IT Security Association Germany
Bundesverband IT-Sicherheit e.V.

IT-beveiligingswet (Duitsland) en Algemene wet bescherming persoonsgegevens (EU)

Richtlijn "Stand der techniek"

Technische en organisatorische maatregelen

2023

Nederlands versie

In co-operatie met:

PRIVACY EN BEVEILIGING ADVIES
BREEMAN

Erkenning

TeleTrusT bedankt de volgende personen voor hun deelname aan de TeleTrusT Task Force Stand der Technik en voor hun actieve bijdrage aan deze richtlijn.

Projectmanagement

RA Karsten U. Bartels LL.M. - HK2 Rechtsanwälte
Tomasz Lawicki - Capgemini

Auteurs en deelnemende experts

Bartels, Karsten U. - HK2 Rechtsanwaelte
Barth, Michael - Genua GmbH
Bausewein, Christoph - CrowdStrike GmbH
Dehning, Oliver - Hornetsecurity GmbH
Dominkovic, Dennis - SEC Consult Unternehmensberatung GmbH
Dubbel, Sascha - CrowdStrike GmbH
Falkenthal, Oliver - CCVOSSEL GmbH
Fischer, Marco - Procilon GmbH
Follmer, Nancy - heinzl mobile cloud solutions GmbH
Gehrmann, Mareike - Taylor Wessing Partnergesellschaft mbB
Gora, Stefan - Secorvo Security Consulting GmbH
Heyde, Steffen - secunet Security Networks AG
Hohenkamp, Iris - MTRIX GmbH
Jager, Hubert - Digital Trust Innovations
Kahrs, Malte - MTRIX GmbH
Kippert, Tobias - TÜV Informationstechnik GmbH
Kolmhofer, Robert - FH Oberösterreich Studienbetriebs GmbH
Kowol, Dominik - eperi GmbH
Krosta-Hartl, Pamela - LANCOM Systems GmbH
Lang, Thomas - Intargia Managementberatung GmbH
Lawicki, Tomasz - Capgemini
Leitner, Alexander - UNINET it-consulting GmbH
Liedke-Deutscher, Bernd - TÜV Informationstechnik GmbH
Maier, Janosch - Crashtest Security GmbH
Martin, Karl-Ulrich - Detack GmbH
Menge, Stefan - AchtWerk GmbH & Co. KG
Muehlbauer, Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Mueller, Siegfried - MB connect line GmbH
Paulsen, Christian
Robin, Markus - SEC Consult Unternehmensberatung GmbH
Rost, Peter - secunet Security Networks AG
Schlensog, Alexander - secunet Security Networks AG
Wuepper, Werner - Wupper Management Consulting GmbH
Zingsheim, Andre - TüV TRUST IT GmbH

Dit document dient als leidraad en geeft een overzicht. Zij beweert niet uitputtend te zijn, noch beweert zij een exacte uitlegging van de bestaande wettelijke bepalingen te zijn. Het mag niet in de plaats komen van de studie van de relevante richtlijnen, wet- en regelgeving. Bovendien moet rekening worden gehouden met de bijzondere kenmerken van de respectieve producten en hun verschillende toepassingen. In dit opzicht is een groot aantal andere constellaties denkbaar voor de beoordelingen en procedures die in het document aan de orde komen.

Colofon

Uitgever:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestrasse 17
10115 Berlin
Tel.: +49 30 4005 4310
Fax: +49 30 4005 4311
E-Mail: info@teletrust.de
https://www.teletrust.de

V 2 2023-05 NL

Dutch version: Jan Breeman

Inhoud

Afbeeldingenoverzicht

Tabeloverzicht

Principes van de richtlijn

Toen de Duitse IT-Sicherheitsgesetz (hierna genoemd: ITSiG) in juli 2015 van kracht werd, lanceerde het Bundesverband IT-Sicherheit e.V. (TeleTrusT) de Task Force Stand der Technik (hierna genoemd: AK-SdT), om geïnteresseerde partijen op basis van de stand van de techniek richting en aanbevelingen te geven voor technische en organisatorische maatregelen. Om aan deze hoge eisen te voldoen, heeft de AK-SdT voor het ontwikkelen, de evaluatie en het bijwerken van de richtlijn de volgende beginselen vastgesteld:

1. Basisbegrip van het document
   Deze richtlijnen zijn bedoeld om zowel bedrijven die IT gebruiken als aanbieders (fabrikanten en dienstverleners) te helpen bij het bepalen van de stand van de techniek in de zin van de Algemene Verordening Gegevensbescherming (hierna genoemd: AVG) en de ITSiG. Het document kan dienen als referentie voor contractuele overeenkomsten, aanbestedingsprocedures en voor de classificatie van geïmplementeerde veiligheidsmaatregelen. Deze richtlijnen worden beschouwd als een startpunt voor het identificeren van wettelijke IT-beveiligingsmaatregelen. Zij komen niet in de plaats van technisch, organisatorisch of juridisch advies of van beoordeling van individuele gevallen.
2. Verantwoordelijkheid voor ontwikkeling, evaluatie en actualisering
   De TeleTrusT Task Forces Stand der Technik en Law houden zich bezig met de vraag hoe de stand van de techniek in relatie tot technische en organisatorische maatregelen in de zin van de wet kan worden bepaald en hoe wettelijke vereisten kunnen worden geïmplementeerd.
3. Begrip van de aanpak
   De AK-SdT bereikt haar resultaten in een transparant proces en stelt de aanbevolen acties en richtlijnen in een regelmatige actualiseringsprocedure ter discussie beschikbaar aan het publiek.
4. Evaluatieprocedure
   De AK-SdT baseert haar evaluatie op een gestandaardiseerde methode die voor de afzonderlijke maatregelen wordt ingevuld en gepubliceerd. De methode voor het evalueren van het technologische niveau van technische maatregelen wordt in dit document beschreven.
5. Actualisatie
   Om gelijke tred te houden met de technologische vooruitgang, worden regelmatige updates en uitgaven van deze richtlijnen gepland. Momenteel is het de bedoeling om elke twee jaar een nieuwe versie van de richtlijnen te publiceren. Kleine aanpassingen en aanvullingen op de richtlijnen (zoals nieuwe bijdragen aan technische maatregelen) zullen in de loop van het jaar in de vorm van herzieningen van de richtlijnen verschijnen.

Leeswijzer

Deze richtlijnen worden beschouwd als een startpunt voor het bepalen van wettelijke IT-beveiligingsmaatregelen die overeenkomen met de stand van de techniek. Zij zijn geen vervanging voor technisch, organisatorisch of juridisch advies of beoordeling in individuele gevallen.
De ITSiG is gericht op het leveren van een bijdrage aan het verbeteren van de beveiliging van informatiesystemen en kan één op één worden toegepast in Nederland.

1. Introductie

1.1 Wet op de IT-beveiliging

De IT-Sicherheitsgesetz (ITSiG) is sinds 25/07/2015 van kracht en is bedoeld om bij te dragen aan de verbetering van de beveiliging van informatiesystemen in Duitsland. De voorschriften van deze wet dienen om deze systemen te beschermen in termen van huidige en toekomstige bedreigingen voor de beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van beschermde goederen. Volgens de memorie van toelichting is het doel van de wet het verbeteren van de IT-beveiliging van bedrijven, het verbeteren van de bescherming van burgers op het internet en ook het versterken van het Bundesamt für Sicherheit in der Informationstechnik (verder genoemd: BSI) en het Bundeskriminalamt (BKA).
De IT-beveiligingswet is een zogenaamde artikelwet: De wet zelf diende slechts om verschillende sectorspecifieke wetten aan te passen. De ITSiG heeft in de Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) regels opgesteld voor kritieke infrastructuren (KRITIS) en onder meer wijzigingen aangebracht in de Atomgesetz (AtomG), de Energiewirtschaftsgesetz (EnWiG), de Telemediengesetz (TMG) en de Telekommunikationsgesetz (TKG).

De ITSiG en de bijbehorende memorie van toelichting zijn te vinden op de volgende link:

https://www.teletrust.de/it-sicherheitsgesetz.

Het ITSiG bepaalt de meest uitgebreide wijzigingen voor KRITIS-Exploitanten van kritieke infrastructuren en bedrijven die telemediadiensten leveren. KRITIS-exploitanten houden overeenkomstig BSIG Art. 8a lid 1 een minimumniveau van IT-beveiliging aan dat overeenkomt met de stand van de techniek. Ze zijn ook verplicht om bepaalde IT-beveiligingsincidenten aan de BSI te melden. Het classificeren van een bedrijf als een kritieke infrastructuur vindt plaats op twee niveaus. De ene is om te beoordelen of het kan worden toegewezen aan een sector die inherent als kritiek is geclassificeerd (sectoraffiliatie) en de andere is om te beoordelen of er een bepaalde relatie is met beveiliging (relevantie van gevolgfouten). De dienstverleners en KRITIS-exploitanten worden ook indirect getroffen door wettelijke voorschriften wanneer de KRITIS-exploitanten contractueel de relevante verplichtingen aan hen opleggen.
Op grond van BSIG: § 10 lid 1 is het Bundesministerium des Innern (BMI) bevoegd om een verordening uit te vaardigen waarin wordt gespecificeerd welke apparatuur, systemen of delen daarvan als kritieke infrastructuren worden beschouwd in de zin van deze wet. Bij dit proces wordt rekening gehouden met het belang van de diensten en hun dekkingsniveau. De Duitse federale regering heeft op 13/04/2016 ingestemd met de goedkeuring van de ministeriële regeling die door de minister van het BMI is voorgesteld om kritieke infrastructuren te bepalen op basis van de BSIG (BSI-KRITISV). Het eerste deel van de KRITIS-regeling voor de implementatie van de ITSiG is vervolgens op 03/05/2016 in werking getreden. Het tweede deel van de KRITIS-regeling werd vastgesteld op 31/05/2017 en trad uiteindelijk in werking op 01/06/2017. De regeling regelt de classificatie van bedrijven als kritieke infrastructuren in de sectoren energie, water, voeding, informatietechnologie en telecommunicatie (tranche 1) en de sectoren gezondheid, financiën en vervoer en verkeer (tranche 2).
Op grond van BSIG: Art. 8a lid 1 beschikken KRITIS-exploitanten een termijn van twee jaar na de inwerkingtreding van het besluit om passende technische en organisatorische maatregelen (Hierna genoemd: TOM's) te treffen om verstoringen in de beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van hun IT-systemen, -functies of -processen die essentieel zijn voor de functionaliteit van de kritieke infrastructuren die zij exploiteren te voorkomen.
Aanbieders van telemediadiensten garanderen overeenkomstig de TMG: § 13 lid 7 dat hun technische uitrusting binnen hun technische en economische middelen door TOM's wordt beschermd. Bij het kiezen van deze TOM's moet rekening worden gehouden met de stand van de techniek. Incidenten hoeven niet gemeld te worden. Dit is van invloed op elk bedrijf dat een telemediadienst exploiteert. De bepalingen van de TMG voorzien niet in overgangsperioden of vrijstellingen voor micro-ondernemers in tegenstelling tot de KRITIS-regelingen.

1.2 Duitse BSI-normen voor exploitanten in specifieke sectoren

De ITSiG vereist dat KRITIS-exploitanten voldoen aan of op zijn minst rekening houden met de stand van de techniek van IT-beveiligingsmaatregelen. Dit beveiligingsniveau is echter niet verder gespecificeerd in de wet. Het is echter toegestaan dat KRITIS-sectoren beveiligingsnormen voor specifieke sectoren voorstellen (hierna B3S). Het is aan de BSI om de veiligheidsnormen voor specifieke sectoren, die door vertegenwoordigers van die sectoren worden voorgesteld, goed te keuren.
De eerste aanwijzingen voor de ontwikkeling van de B3S zijn te vinden door de KRITIS-exploitanten en -verenigingen in kwestie in het door de BSI is gepubliceerde ontwerp Orientierungshilfe zu Inhalten und

Anforderungen an branchenspezifische Sicherheitsstandards (B3S) volgens BSIG: Art. 8a lid 2[1]. Het ontwerp bevat de volgende methodologie:

1. Definitie van het toepassingsgebied en de beschermingsdoelstellingen van de B3S.
2. Beoordeling van de kwetsbaarheden in de specifieke sector.
3. Uitvoering van een risicoanalyse voor de kwetsbaarheden in de specifieke sector.
4. Afleiding van passende en adequate maatregelen voor de specifieke sector.

Volgens dit artikel moet de B3S helpen bij het kiezen van adequate maatregelen, door bepalingen en maatregelen aan te geven op basis van best practices die typisch zijn voor de sector. De B3S moet waar nodig ook zijn grenzen aangeven, bijvoorbeeld als er meer bescherming en dus aanvullende maatregelen nodig zijn en deze aanvullende bepalingen en maatregelen aanbevelen.
Wat de kwestie van het toereikend zijn betreft, moet in de eerste plaats rekening worden gehouden met de economische kosten die van de KRITIS-exploitant verlangd worden, met name de uitvoeringskosten. Ten slotte mogen de kosten die nodig zijn voor de implementatie niet onevenredig zijn aan de gevolgen van een storing of schade aan de kritieke infrastructuur in kwestie[2]. Of een maatregel adequaat of economisch is, kan echter alleen op individuele basis worden bepaald, rekening houdend met hun unieke beschermingsbehoeften en de uitvoeringskosten voor eventuele vereiste maatregelen.
De richtlijn noemt vervolgens een lijst met onderwerpen (zoals asset management, leveranciers, dienstverleners en derden) die de B3S moet behandelen. De betrokken KRITIS-exploitanten en -verenigingen ontvangen vervolgens nadere informatie over het detailniveau waarop voorstellen in de B3S moeten worden beschreven. Ten slotte noemt de richtlijn andere opties voor het verifiëren van de implementatie.
De richtlijn verduidelijkt nogmaals dat het vaststellen van een minimumnorm voor een bepaalde sector afhankelijk is van een aantal individuele factoren. Een exacte bepaling van de minimumnorm moet daarom worden gemaakt op basis van individuele omstandigheden. Dit geldt met name voor gereguleerde sectoren waarvoor speciale wettelijke voorschriften gelden, zoals de Telecommunicatiewet.
Een sectorspecifieke norm (B3S WA) voor de sectoren watervoorziening en afvalverwijdering werd door de BSI voor het eerst gedefinieerd en goedgekeurd op 01/08/2017. De B3S WA bestaat uit een informatieblad en een IT-beveiligingshandleiding die jaarlijks worden bijgewerkt. De B3S WA is gebaseerd op de BSI-Grundschutz-Kompendium (Basic beschermingscatalogus) en branche specifieke beveiligingseisen. De B3S WA bestaat uit een informatieblad en een IT-beveiligingsrichtlijn die jaarlijks worden bijgewerkt. De B3S WA is gebaseerd op de BSI Grundschutz-Kompendium en van sectorspecifieke beveiligingseisen.
Het blijft echter onduidelijk welke criteria werden gebruikt om de voorgestelde veiligheidsnormen voor de watersector te selecteren en welke criteria vervolgens door de BSI werden gebruikt om het in de zin van stand van de techniek goed te keuren als de B3S WA.

1.3 Europese implicaties

Aan de BSIG worden andere Europese richtlijnen toegevoegd. Daartoe heeft de Europese Commissie de richtlijn betreffende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de hele Europese Unie (NIS-richtlijn) aangenomen, dat in nationale wetgeving moet worden omgezet. Dit leidt niet tot fundamentele wijzigingen, aangezien de nationale wetgever al heeft geanticipeerd op een meerderheid van de vereisten die de Europese wetgevers met de vaststelling van het ITSiG hebben beoogd. De overeenkomstige NIS-richtlijn implementatiewet van 27/04/2017 leidt dus slechts tot een uitbreiding van de BSIG.
Op basis van de Richtlijn werd onder andere BSIG: Art. 8c in het leven geroepen om extra verplichtingen te creëren voor aanbieders van digitale diensten. Digitale diensten zijn vervolgens online marktplaatsen, online zoekmachines en cloud-computing-diensten met een genormaliseerde waarde. Deze diensten moeten ook technische en organisatorische maatregelen (TOM's) implementeren om IT-beveiliging te garanderen die rekening houden met de stand van de techniek. De maatregelen zijn bedoeld om een adequaat beschermingsniveau te waarborgen dat in verhouding staat tot het risico en daarbij rekening te houden met de beveiliging van systemen en installaties, de afhandeling van beveiligingsincidenten en het beheer van de bedrijfscontinuïteit.

1.4 Algemene Verordening Gegevensbescherming (AVG)

De Europese Algemene Verordening Gegevensbescherming (AVG) werd in 2016 aangenomen en trad op 25/05/2018 definitief in werking. Het primaire doel van de AVG is het beschermen van de

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/b3s_Orientierungshilfe.html.
[2] BSIG: Art. 8a lid 1 zin 3

persoonsgegevens van Europese burgers. Tegelijkertijd is de verordening gebaseerd op een op risico's gebaseerde benadering wat betreft de beschermingsdoelstellingen. Er moeten passende technische en organisatorische maatregelen worden genomen om op het gebied van technische gegevensbescherming de rechten en vrijheden van natuurlijke personen te beschermen. Deze moeten ook rekening houden met het samenstellende element stand van de techniek. In het bijzonder bepaalt AVG: Art. 32 dat in het kader van de beveiliging van de gegevensverwerking rekening moet worden gehouden met de stand van de techniek. Daartoe moeten verwerkingsverantwoordelijken en verwerkers passende technische en organisatorische maatregelen nemen. Net als het ITSiG geeft de AVG geen definitie van het samenstellende element stand van de techniek. Hetzelfde geldt voor de EU Data Protection Adaptation and Implementation Act (DSAnpUG-EU) en de daaruit voortvloeiende nieuwe versie van de BDSG (BDSG-nieuw).
Bovendien moeten volgens AVG: Art. 25 de beginselen van gegevensbescherming worden nageleefd door middel van gegevensbescherming als opzet (privacy by design) en door gegevensbescherming als standaardinstellingen (privacy by default). Deze beginselen moeten ook worden toegepast door middel van passende technische en organisatorische maatregelen.
Bij de uitvoering van de richtlijnen moet echter niet alleen rekening worden gehouden met de stand van de techniek, maar moet ook volledig worden gedocumenteerd. Hiertoe zijn uitgebreide en verstrekkende documentatievereisten in het leven geroepen, met name de verplichting om een gegevensbescherming-effectbeoordeling (DPIA) uit te voeren en het beginsel van verantwoording. De verordening stelt in dit verband documentatievereisten vast als haar eigen wettelijke verplichtingen. Technische en organisatorische maatregelen moeten dus afzonderlijk worden vastgesteld en in detail worden beschreven en gedocumenteerd.

1.5 Toepasselijkheid van de maatregelen

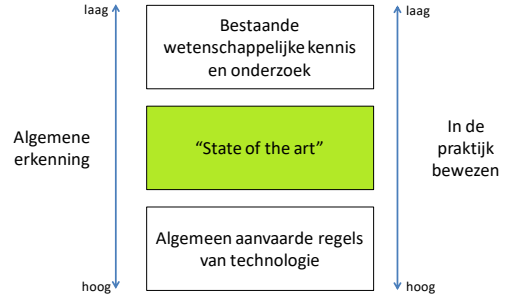
De in deze richtlijn beschreven stand van de techniek richt zich op de inhoud die vanuit de ITSiG en de GDPR wordt vereist. In het kader van de ITSiG is het echter toegestaan om bij de keuze van beschermende maatregelen ook rekening te houden met economische factoren[3]. Of een maatregel economisch is, kan echter alleen worden bepaald door individueel onderzoek van de unieke beschermingsbehoeften en de uitvoeringskosten die de maatregelen vereisen. Daarom is de doelmatigheidscontrole (performance audit) buiten deze richtlijn gelaten.

[3] Voor de vereisten van juridische overwegingen, zie Bartels/Backer, Die Berücksichtigung des Standes der Technik in der DSGVO, DuD 4-2018, 214.

2. Het bepalen van de stand van de techniek

2.1 Definitie

De stand van de techniek[4] voor techniek moet inhoudelijk worden gedefinieerd als afzonderlijke termen met betrekking tot de stand van de techniek, zoals de algemeen aanvaarde regels van de technologie (hierna genoemd: GART) en bestaande wetenschappelijke kennis en onderzoek (hierna genoemd: ESKaR)[5] en moet onafhankelijk meetbaar zijn. Dit onderscheid is de essentiële basis voor het definiëren van de vereiste stand van de techniek. Zoals uit de praktijk blijkt worden deze drie begrippen in gelijke mate door elkaar gehaald of zelfs verward in de jurisprudentie en in het publiek[6].
Deze drie begrippen werden, net als de daaruit volgende driestappentheorie, in 1978 geïntroduceerd met de Kalkar-besluit[7] van het Bundesverfassungsgericht. Op basis van dit besluit kunnen de drie technologie-toestanden als volgt grafisch worden weergegeven:



Afbeelding 1: De drietrapstheorie volgens het Kalkar-besluit

Het niveau van technologie stand van de techniek bevindt zich tussen het meer innovatieve niveau van bestaande wetenschappelijke kennis en onderzoek en het meer gevestigde niveau de algemeen aanvaarde regels voor de techniek. Deze drie niveaus worden geflankeerd door de categorieën algemeen erkend en bewezen in de praktijk.

De classificatie van de wetten vereist een duidelijk onderscheid tussen subjectieve en objectieve criteria. Het criterium v is puur objectief. De subjectieve aspecten houden, in het geval van een overtreding, rekening met de wetten; ze hebben echter geen betrekking op de definitie van de stand van de techniek zelf.

Als gevolg hiervan kan de stand van de techniek worden omschreven als de procedures, uitrusting of werkwijzen die beschikbaar zijn in de handel in goederen en diensten waarvoor de toepassing ervan het meest effectief is om de respectieve doelstellingen van rechtsbescherming te bereiken[8].

Kortom: De stand van de techniek verwijst naar de beste prestaties van een IT-beveiligingsmaatregel die op de markt beschikbaar is om de wettelijke IT-beveiligingsdoelstelling te bereiken.

Technische maatregelen in de fase van bestaande wetenschappelijke kennis en onderzoek zijn zeer dynamisch in hun ontwikkeling en gaan over in de fase stand van de techniek wanneer zij marktrijp worden (of op zijn minst zodra zij op de markt worden gebracht).

Daar neemt de dynamiek af, bijvoorbeeld door processtandaardisatie. In de fase algemeen aanvaarde regels van technologie zijn technische maatregelen ook beschikbaar op de markt. Hun mate van innovatie neemt af, hoewel ze in de praktijk zijn bewezen en vaak in overeenkomstige normen worden beschreven.

Hoewel de overgang van stand van de techniek in wetenschap en onderzoek naar stand van de techniek relatief eenvoudig te identificeren is via markttoegang, is de afbakening tussen de stand van de techniek en algemeen aanvaarde regels van technologie nogal moeilijk. In het geval van technische maatregelen zijn het, in het kader van een productlevenscyclus, vaak nieuwe versies van een beveiligingsoplossing of software die duidelijk zijn gelokaliseerd. In het geval van organisatorische maatregelen zijn het echter

---

[4] De term "niveau van technologie" wordt gebruikt als vervanging voor "stand van de technologie".
[5] "Bestaande wetenschappelijke kennis en technologie" kan als alternatief worden gebruikt. "Bestaande wetenschappelijke kennis en onderzoek" zullen vervolgens in deze richtlijn worden gebruikt zodat een onderscheid kan worden gemaakt tussen dit en stand van de techniek
[6] Dr Mark Seibel, Higher Regional Court Judge, https://www.dthg.de/resources/Definition-Stand-der-Technik.pdf
[7] BVerfGE, 49, 89 (135 f)
[8] Bartels/Backer: Die Berücksichtigung des Stands der Technik in der DSGVO, DuD 4-2018, 214; Bartels/Backer/ Schramm, Der "Stand der Technik" im IT-Sicherheitsrecht, Tagungsband zum 15. Deutschen IT-Sicherheitskongress 2017, Bundesamt für Sicherheit in der Informationstechnik, 503.

vaak geschreven normen die elders worden aangeduid als best practice. Ze hebben zich in de praktijk bewezen en zijn nauwelijks aan modernisering onderhevig.

Bovendien zijn er maatregelen op de markt beschikbaar, waarvan is de erkenning door experts met betrekking tot hun effectiviteit afgenomen. Dit is bijvoorbeeld het geval bij maatregelen die gecompromitteerd zijn of niet meer door de fabrikant (end of life, of eol) worden ondersteund. Deze maatregelen mogen niet langer worden gebruikt.

Als gevolg van vooruitgang (innovatieve verschuiving) kan een verschuiving worden waargenomen tussen de individuele stadia van technologie.

1. Een maatregel zal in eerste instantie het stadium van de bestaande wetenschappelijke kennis en onderzoek bereiken dat bij de oorsprong ervan is ontstaan.
2. Wanneer het op de markt wordt gebracht, gaat het over naar het stadium van de stand van de techniek,
3. En naarmate het op grotere schaal op de markt wordt verspreid en wordt erkend, zal het op een gegeven moment worden gekwalificeerd als algemeen aanvaarde regels van technologie
4. Als de erkenning verloren gaat, kan deze maatregel niet meer worden gebruikt.

Om het vereiste bewijs te leveren op basis van de oriëntatie van hun eigen maatregelen op het niveau van stand van de techniek, is het niet voldoende om de geïmplementeerde maatregelen eenmaal te evalueren en bij te werken door patches te installeren. Dit soort bewijs kan alleen succesvol zijn door de uitgevoerde maatregel op gezette tijden en middels transparante methoden te vergelijken met de alternatieven die op de markt beschikbaar zijn.

2.2 Methode voor het bepalen van de stand van de techniek

De in hoofdstuk 3.2 beschreven technische maatregelen werden geëvalueerd met behulp van een uitvoerbare methode die gebaseerd is op een eenvoudig principe van het beantwoorden van kernvragen over de erkenning door het vak-deskundigen en bewijs in de praktijk. De gebruikte kernvragen zijn bewust eenvoudig geformuleerd en bieden een meer gedetailleerd beeld van de twee dimensies van het onderzoek.

Op elk van de centrale vragen zijn drie antwoorden mogelijk. De antwoorden werden gekozen om indeling in een van de drie niveaus van technologie mogelijk te maken. Elk antwoord moet ook worden gemotiveerd. Hoewel de afzonderlijke vragen indeling in een van de drie technologieniveaus mogelijk maken, omvat elk van hen slechts gedeeltelijke aspecten, wat betekent dat de stand van de technologie van een maatregel pas wordt bepaald door alle vragen voor beide dimensies te beantwoorden.

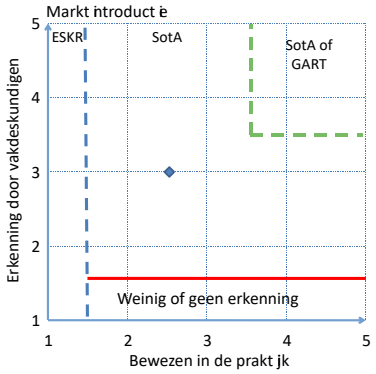
De volgende afbeelding toont het door de AK-SdT gebruikte sjabloon voor alle kernvragen om de stand van de techniek voor een technische maatregel te evalueren:

1.1 Vragen over de mate van erkenning			Beoordeling moet worden ingevuld door werkgroep SotA
1) Welke documentatie met betrekking tot de maatregel is openbaar beschikbaar? (beantwoord de vraag door de vakjes aan te vinken)			
☐ Wetenschappelijke publicatie	☐ Technische publicatie	☐ Massamedia	1 - Wet. publ. 2 - Techn. publ. 3 - Massamedia
(Licht uw antwoord hier toe)			
2) Verwijst de maatregel naar nationale of internationale standaarden? (beantwoord de vraag door de vakjes aan te vinken)			
☐ Nee, niet gestandaardiseerd	☐ Ja, één	☐ Ja, meer dan één	Nee - niet gestandaardiseerd Ja - één Ja - meer dan één
(Licht uw antwoord hier toe)			
3) Wordt de maatregel aanbevolen door erkende gremia/commissies? (beantwoord de vraag door de vakjes aan te vinken)			
☐ Nee	☐ Ja, grote	☐ Ja, veel	Nee Ja - grote Ja - veel
(Licht uw antwoord hier toe)			
4) Wordt de geschiktheid van de maatregel regelmatig onderzocht? (beantwoord de vraag door de vakjes aan te vinken)			
☐ Nee	☐ Ja, door de fabrikant	☐ Ja, door een onafhankelijke instantie	Nee Ja - fabrikant Ja - onafh. instantie
(Licht uw antwoord hier toe)			
		Gemiddelde	

1.2 Vragen over het testen in de praktijk			Beoordeling moet worden ingevuld door werkgroep SotA
1) hoe wordt de mogelijkheid tot innovatie van de maatregel geclassificeerd? (beantwoord de vraag door de vakjes aan te vinken)			
☐ Hoog	☐ Midden	☐ Laag	Hoog Midden Laag
(Beantwoord de vraag door de vakjes aan te kruisen)			
2) Waar is de huidige versie van de maatregel getest? (beantwoord de vraag door de vakjes aan te vinken)			
☐ Nee, niet gestandaardiseerd	☐ Ja, één	☐ Ja, meer dan één	Nee - niet gestandaardiseerd Ja - één Ja - meer dan één
(Beantwoord de vraag door de vakjes aan te kruisen)			
3) Zijn vergelijkbare maatregelen in de markt beschikbaar? (beantwoord de vraag door de vakjes aan te vinken)			
☐ Nee	☐ Weinig	☐ Veel	Nee Weinig Veel
(Licht uw antwoord hier toe)			
4) Hoe vaak wordt de maatregel conceptueel door de fabrikant bijgewerkt? (beantwoord de vraag door de vakjes aan te vinken)			
☐ Meer dan één keer per jaar	☐ Eén keer per jaar	☐ Minder frequent	Nee Ja - grote Ja - veel
(Licht hier uw antwoord toe)			
		Gemiddelde	

Afbeelding 2: Evaluatiecriteria

Met behulp van een puntensysteem wordt op basis van de gegeven antwoorden een gemiddelde score gegenereerd. Aan de hand van de verkregen waarden kan de classificatie in het diagram worden weergegeven.



ESKR	Stand van wetenschap en onderzoek
SotA	Stand van de techniek
GART	Algemeen erkende regels van de technologie

Afbeelding 3: Voorbeeld van classificatie voor stand van de technologie

In het diagram kunnen de hierboven beschreven technologieniveaus, stand van de techniek in science and research, stand van de techniek in technology en generally recognized rules of technology worden ingedeeld.

De stand van wetenschap en onderzoek moet links van de markttoetreding worden geplaatst, maar kan, vanwege de mogelijke erkenning door experts, zich over de hele Y-as uitstrekken.

Als de bovenstaande definitie van stand van de techniek als uitgangspunt wordt gebruikt, wordt onder stand van de techniek in wetenschap en onderzoek de processen, apparatuur of werkwijzen verstaan, waarvan de toepassing de verwezenlijking van de respectieve wettelijke beschermingsdoelstellingen kan waarborgen, maar waarvan het effect nog niet in de praktijk is getest.

Bij het op de markt komen worden dergelijke maatregelen stand van de techniek. Zij zijn geavanceerd en kunnen de verwezenlijking van de respectieve doelstellingen op het gebied van rechtsbescherming op de meest doeltreffende wijze garanderen.

Met de toenemende standaardisatie schuift de classificatie van de maatregel naar rechtsboven. Daar vindt u beproefde, gestandaardiseerde maatregelen die volstaan om aan de wettelijke doelstellingen te voldoen. Ze vormen vaak het basiskader van IT-beveiliging, maar dreigen te worden vervangen door

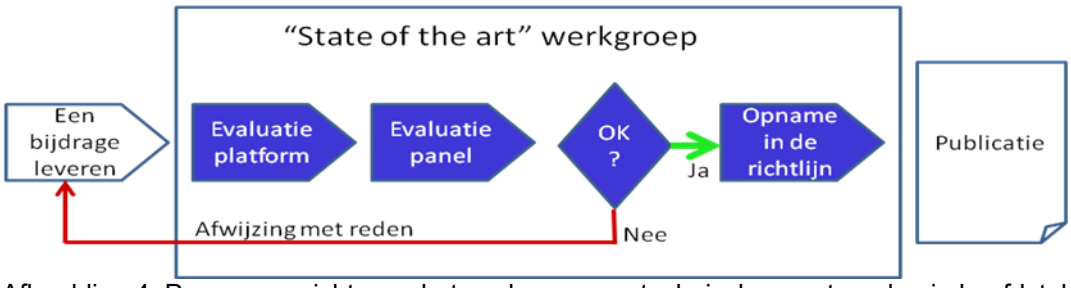
meer geavanceerde maatregelen. Hun herkenning kan snel veranderen, waardoor ze naar het onderste gedeelte van de grafiek schuiven (geen of nauwelijks herkenning).

Deze richtlijn beschrijft technologieën en maatregelen en classificeert ze volgens de hierboven beschreven methode. Er worden geen veiligheidsproducten in engere zin beschreven. Daarom wordt bijvoorbeeld aangenomen dat voor het respectieve doel aan de geschiktheid van de hier beschreven maatregelen is voldaan en is dit voor het individuele gevallen niet verder is gevalideerd.

In de praktijk moet een geschikte methode (bijvoorbeeld vergelijkbaar met die welke hier wordt beschreven) worden aangepast aan de bestaande omstandigheden in de organisatie om de uitgevoerde maatregelen objectief te evalueren, ze te vergelijken met alternatieven en ze als bewijsmateriaal te documenteren[9].

2.3 Proces voor kwaliteitsborging van de richtlijn

De AK-SdT streeft naar een hoge kwaliteit van de inhoud van de richtlijn. Om hierin te slagen, is in de AK-SdT een proces opgezet waarin bijdragen in verschillende fasen succesvol moeten zijn:



Afbeelding 4: Procesoverzicht voor het evalueren van technische maatregelen in hoofdstuk 3.2

Nadat een nieuwe of gewijzigde bijdrage in een gestandaardiseerd model is ingediend (zie afbeelding 4), dan wordt de bijdrage via een evaluatieplatform anoniem geëvalueerd door IT-beveiligingsexperts.

De resultaten hiervan worden besproken en goedgekeurd door het reguliere evaluatiepanel van de AK-SdT[10]. De in het sjabloon gedefinieerde kernvragen en hun antwoorden dienen onder andere als evaluatiecriteria, samen met technische correctheid en de valuta van de inhoud.

Als het beoordelingspanel tot de conclusie komt dat een bijdrage niet aan de vereiste kwaliteit voldoet, wordt deze gemotiveerd afgewezen voor opname in de richtlijn en wordt de auteur hiervan op de hoogte gesteld. De auteur heeft dan de mogelijkheid om zijn bijdrage bij te werken of aan te vullen en voor te bereiden op een nieuwe toetsingsronde.

Bijdragen die deze uitgebreide procedure doorstaan worden in de richtlijn opgenomen.

2.4 Vereiste beschermingsdoelstellingen

De door ITSiG ingevoerde wetswijzigingen richten zich op de beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van beschermingsdoelstellingen.

- Beschikbaarheid
  IT-systemen en -componenten worden als beschikbaar beschouwd wanneer deze altijd voor het beoogde doel en binnen hun bereik van functionaliteit kunnen worden gebruikt.
- Integriteit
  Integriteit verwijst in het bijzonder naar de gegevens. Integriteit wordt geacht aanwezig te zijn wanneer verzekerd wordt dat verzonden gegevens volledig en ongewijzigd de ontvangers worden ontvangen.
- Vertrouwelijkheid
  Er is sprake van vertrouwelijkheid wanneer gevoelige gegevens alleen op de toegestane wijze aan bevoegde personen ter beschikking worden gesteld.
- Authenticiteit (echtheid)
  Er is sprake van authenticiteit wanneer de unieke identiteit van de

[9] Lawicki, "Was bedeutet Stand der Technik?", gepubliceerd in de TeleTrusT speciale bijlage "Sicherheit & Datenschutz" in het tijdschrift iX 6/2018

[10] Op de webpagina van TeleTrusT wordt een lijst van de leden die actief zijn in de Task Force (evaluatie panel) gepubliceerd: https://www.teletrust.de/arbeitsgremien/recht/stand-der-technik/ (Engelse versie: https://www.teletrust.de/en/arbeitsgremien/recht/task-force-state-of-the-art-in-it-security/)

communicatiepartners (en die van de communicerende componenten) is gewaarborgd.

Naast deze IT-beveiligingsdoelstellingen waarop het ITSiG zich richt, zijn er nog andere beschermingsdoelstellingen, die hier met name worden genoemd vanwege de eerdergenoemde AVG[11]:

- Ontkoppelbaarheid (doelbinding)
  Persoonsgegevens mogen alleen worden verwerkt voor het aangegeven doel. De persoonsgegevens mogen niet of alleen in geval van onevenredig hoge inspanningen worden verzameld, verwerkt en gebruikt voor een ander doel dan voor het aangegeven doel.
- Transparantie van de verwerking
  De verwerking van persoonsgegevens moet traceerbaar, verifieerbaar en met redelijke inspanning te beoordelen zijn.
- Interventiecapaciteit
  De verwerking moet zo worden vormgegeven dat het verlenen van de toegangsrechten waarop zij recht hebben, op korte termijn mogelijk wordt gemaakt.

Sommige van deze aanvullende doelstellingen concurreren met de hierboven genoemde doelstellingen op het gebied van IT-beveiliging. Omdat de wettelijke vereisten van het ITSiG en de AVG gelijktijdig van toepassing zijn, is het doel in de organisatie om een gemeenschappelijke, duurzame oplossing te bereiken voor een hoog niveau van de IT-beveiliging en gegevensbescherming. Dit kan alleen door samenwerking tussen de functionarissen voor IT-beveiliging en gegevensbescherming.

Terwijl vanuit het oogpunt van IT-beveiliging het hoofddoel de bescherming van gegevens en infrastructuur is, is vanuit het oogpunt van gegevensbescherming het belangrijkste doel de bescherming van de mensenrechten. Het is belangrijk om deze verschillende gezichtspunten te begrijpen om beschermende maatregelen vast te stellen en deze daarmee in overeenstemming uit te voeren.

3 Technische en organisatorische maatregelen (TOM2)

De ITSiG en AVG vereisen technische en organisatorische maatregelen om te voldoen aan of op zijn minst rekening te houden met de stand van de techniek. De wetgever heeft de relevante systemen en bevoegdheden niet nader gespecificeerd. Daarom moet de naleving van de stand van de techniek gebaseerd zijn op alle relevante onderdelen van de gegevensverwerking, met inbegrip van alle opties voor gegevens-portabiliteit en -opslag.

Omdat IT-infrastructuren sterk afhankelijk zijn van toepassing en sector, is het niet mogelijk om de afzonderlijke componenten in deze richtlijn volledig op te sommen. De auteurs hebben zich daarom gericht op het beschrijven van de essentiële componenten en processen.

3.1 Algemene informatie

Toepassingen met betrekking tot gebruik in het kader van de ITSiG zijn soms zeer specifiek. Dit varieert van gangbare normen, zoals veilige e-mailcommunicatie, tot zeer strenge eisten als dat nodig is, bijvoorbeeld voor veilige besturingsfunctionaliteit in een energiecentrale. Hierdoor is het erg moeilijk om in deze studie een volledige lijst van toepassingen op te stellen en ook toepassing ervan te beschrijven. Omdat er veel manieren zijn om een doel te bereiken kan IT-beveiliging ook op meerdere manieren worden geïmplementeerd en bestaat er niet ÉÉN implementatie van veilige architectuur. Het is daarom bedoeld om essentiële elementen te identificeren die kunnen worden opgevat als stand van de techniek in de zin van de hedendaagse bruikbaarheid van IT-beveiliging.

De beveiligingsbehoeften zijn in elk geval afhankelijk van de toepassing. Volgens de ITSiG moeten de IT-veiligheidsdoelstellingen van beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit worden nageleefd, zelfs als ze worden beoordeeld voor het individuele beeld, naar gelang het geval, met verschillende beschermingsbehoeften, Dit betekent dat met name rekening moet worden gehouden met de volgende beschermingsdoelstellingen:

- Bescherming tegen aanvallen met als doel het ongeoorloofd lezen, wijzigen of verwijderen van verzonden en opgeslagen gegevens
- Bescherming tegen aanvallen van de beschikbaarheid van de betreffende diensten en gegevens voor de exploitant of gebruiker

[11] Geïnspireerd door het Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ICPP), https://www.datenschutzzentrum.de/

- Bescherming tegen ongeoorloofde manipulatie van besturings- en applicatiesystemen, enz.

Naast het implementeren van adequate beschermingsmaatregelen, moet de detectie van aanvallen op IT-systemen, diensten en gegevens worden gegarandeerd volgens de stand van de techniek.

Functionaliteit die de gewenste IT-beveiligingstoepassing realiseert, moet te allen tijde volledig en correct worden geïmplementeerd. Dit zou door een onafhankelijke auditor geverifieerd moeten worden. De implementatie moet altijd stand van de techniek -methoden bevatten. Deze omvatten:

- multi-factor authenticatie;
- wederzijdse authenticatie;
- versleuteling van communicatie tijdens transport;
- gegevensversleuteling (bijvoorbeeld tijdens opslag);
- bescherming van de privésleutel tegen ongeoorloofd kopiëren;
- gebruik van veilige opstartprocessen;
- veilig softwarebeheer inclusief patchbeheer;
- veilige gebruikersadministratie met actieve vergrendelingsoptie;
- veilige mapping van netwerkzones voor extra bescherming op netwerkniveau;
- veilige datacommunicatie tussen verschillende netwerkgebieden;
- veilig surfen op internet;
- realisatie van het need-to-know principe;
- realisatie van de minimale aanpak (inclusief hardening);
- realisatie van logging, monitoring, rapportage en response managementsystemen;
- realisatie van malware bescherming;
- gebruik van veilige back-up-systemen om gegevensverlies te voorkomen;
- meerdere systeemlay-outs voor het implementeren van hoge beschikbaarheid, enz.

Naast de individuele technische applicatiefunctionaliteiten moet ook gekeken worden naar de beveiligingsarchitectuur als geheel. Onder de voorwaarden voor dit doel moeten de volgende punten moeten worden beoordeeld. (Het BNetzA vereist met betrekking tot de IT-beveiligingscatalogus een risicobeoordeling voor implementatie volgens de EnWG sectie 11 met HOOG als standaard of KRITIS voor kritieke processen en toepassingen):

- Het moet voor de gebruiker duidelijk zijn onder welke voorwaarden hij het betreffende systeem in de respectieve veilige configuratie kan gebruiken en toepassen. Als er op één apparaat verschillende operationele scenario's mogelijk zijn (bijvoorbeeld toegang tot kantoor-IT via sessie 1 en toegang tot de proces-IT via sessie 2), dan moet dit in elk geval duidelijk worden weergegeven aan de gebruiker.
- Voor het product of de dienst moet een holistische beveiligingsarchitectuur en bijbehorende documentatie voor evaluatie door onafhankelijke derden bestaan en worden geïmplementeerd.
- De gebruikte cryptografie moet op een veilige en moderne manier in kaart kunnen worden gebracht tot het einde van de levenscyclus van het product. Hiervoor beveelt de BSI up-to-date algoritmen aan in een catalogus voor cryptografiestandaarden.
- Het product of de dienst mag geen achterdeurtjes bevatten die kunnen worden meegelezen of zelfs manipulatie van gegevens en toepassingen mogelijk maken.
- De fabrikant mag niet beschikken over toegangsinterfaces die onafhankelijk van de exploitant kunnen worden gebruikt.
- Het is raadzaam om de uitvoering van de beveiligingsfunctie te laten verifiëren door vertrouwde derden.
- De processen die in de applicatie worden geïmplementeerd (bijvoorbeeld gebruikersautorisatie, sleutelbeheer, enz.) moeten veilig in kaart worden gebracht.

Er zijn andere criteria waaraan moet worden voldaan om een product te beoordelen in termen van stand van de techniek, deze zijn als volgt:

- Het product of de dienst moet rekening houden met internationale normen en moet interoperabel zijn met standaardprotocollen.
- Als er voor de specifieke sector normen bestaan, dan moeten deze in aanmerking worden genomen bij de implementatie.
- Het product of de dienst moet een betrouwbare werking van de componenten vergemakkelijken (marktrijpheid).
- Het product of de dienst moet in de praktijk met succes zijn getest.

- Bij de evaluatie moet de oplossing worden beschouwd als een eenheid waarin hardware en software met elkaar verbonden zijn.
- Het product moet veilig kunnen worden bijgewerkt in termen van beveiliging en toepassingsfunctionaliteit.

De fabrikant van de oplossing is ook onderworpen aan criteria voor de evaluatie van de oplossing waarmee rekening moet worden gehouden bij het kiezen van stand van de techniek implementaties. De fabrikant kan de investeringszekerheid voor de betreffende implementatie garanderen. Dit betekent dat de volgende controles moeten worden uitgevoerd:

- De financiële achtergrond van de fabrikant garandeert verdere levenscycli voor het product.
- Voor het betreffende product is een vastgesteld productbeheer en een routekaart voor verdere ontwikkeling voor de gebruiksperiode van gebruiker aanwezig.
- Het product is tijdens de gebruiksperiode niet gemarkeerd als een uit de handel genomen product.
- De fabrikant reageert proactief op kwetsbaarheden die onder zijn aandacht komen en zijn product beïnvloeden, lost deze op korte termijn op en maakt noodzakelijke software-updates snel beschikbaar.
- De fabrikant produceert de betreffende oplossing in een omgeving met vertrouwd personeel.
- De fabrikant heeft onafhankelijke controle over alle beveiligingsfuncties en vertrouwt met betrekking tot de beveiligingsfuncties niet op andere leveranciers.

Als producten van derden worden gebruikt die minder betrouwbaar zijn, dan moeten de beveiligingsarchitectuur voor het product en de maatregelen van de fabrikant in het productieproces ervoor zorgen dat de volledige beveiligingsarchitectuur op zijn plaats blijft in termen van de gedefinieerde beschermingsbehoeften.

3.2 Technische maatregelen

3.2.1 Authenticatiemethoden en -procedures

Er zijn verschillende procedures en verschillende factoren voor authenticatie en voor het voldoen aan IT-beveiligingsdoelstellingen. Deze factoren kunnen worden onderverdeeld in drie categorieën: op kennis gebaseerde, op bezit gebaseerde en biometrische factoren.
In principe zijn, afhankelijk van het toepassingsgebied en de (technische) eisen deze factoren afzonderlijk of in combinatie geschikt voor een procedure.

De op kennis gebaseerde factoren omvatten bijvoorbeeld wachtwoord, pincode en wachtwoordzin. Het wachtwoord is de meest voorkomende authenticatiemethode en bestaat idealiter uit een willekeurige reeks cijfers, letters en speciale tekens. Het persoonlijk identificatienummer (PIN) daarentegen bestaat meestal uit een 4- of 6-cijferige reeks cijfers waarmee de gebruiker zich op een apparaat kan identificeren. Beide methoden worden meestal in combinatie met een gebruikersnaam gebruikt. In vergelijking met een wachtwoord bestaat een wachtwoordzin uit een langere tekenreeks (maximaal 100 tekens). Deze methode wordt vaak gebruikt voor versleuteling of handtekeningen.

Op bezit gebaseerde factoren omvatten FIDO- en OTP-beveiligingstokens, evenals smartphones en klassieke smartcards. Security tokens worden meestal als tweede factor gebruikt voor extra bescherming van gebruikersaccounts, vaak in de vorm van een USB-stick. Ze kunnen uniek worden toegewezen aan een gebruiker en zijn daarmee gepersonaliseerd. Beveiligingstokens genereren een eenmalig wachtwoord (OTP) en reageren op aanraking of gebruiken aanvullend een biometrische functie. De smartphone dient als veelzijdig authenticatiemedium. Het kan worden gebruikt om OTP's te genereren via een app, om sms-berichten te ontvangen en als een out-of-band authenticator. Hierbij krijgt de gebruiker een verzoek om een aanmelding via zijn app te bevestigen of te weigeren. Klassieke smartcard/PKI-gebaseerde methoden zijn vandaag nog steeds op veel gebieden in gebruik, maar worden momenteel meestal aangevuld met andere methoden vanwege hun inherente complexiteit.

De derde categorie authenticatiemethoden wordt gevormd door biometrische factoren. Denk bijvoorbeeld aan vingerafdruk- en irisscanners, bloedvat- gezicht, typegedrag- en spraakherkenning. Daarvan hebben vingerafdruk- en gezichtsherkenning de overhand gekregen. Procedures kunnen worden onderverdeeld in methode en aantal gebruikte factoren, bijvoorbeeld single-factor of multi-factor authenticatie. Deze procedures worden herhaaldelijk toegepast met de eenmaal vastgestelde factoren.

Een andere procedure is de zogenaamde conditionele/adaptieve authenticatie.

Dit is een combinatie van een authenticatiefactor met verificatie van individuele gedragspatronen of andere contextuele informatie. Alleen als afwijkingen worden gedetecteerd van deze combinatie is een andere factor vereist.

3.2.2 Evaluatie en handhaving van sterke wachtwoorden

De maatregel simuleert real-world aanvallen op veilig opgeslagen/gehashte inloggegevens en meet objectieve de veerkracht op basis van wiskundige methoden, persoonlijk gedrag, enz. De maatregel maakt een grondige inventarisatie van alle wachtwoorden, inclusief onbekende wachtwoorden. De maatregel omvat een uitgebreide inventarisatie en evaluatie van alle wachtwoorden, inclusief onbekende. Daarbij wordt de mate van naleving van het interne bedrijfsbeleid bepaald en worden veiligheidsmaatregelen genomen, zoals het informeren van medewerkers wanneer onveilige wachtwoorden worden gebruikt.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

- Het raden van zwakke wachtwoorden door derden.
- Het gebruik van gecompromitteerde wachtwoorden door derden.
- Ongeautoriseerde toegang tot gebruikersaccounts.

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?
Bedrijfsnetwerken gebruiken doorgaans een centrale opslagplaats voor de gebruikersreferenties (repository) die worden gebruikt om gebruikers te verifiëren (bijvoorbeeld Microsoft Active Directory).

Alle moderne opslagsystemen voor verificatiegegevens (credentials) maken gebruik van de zogenaamde hashing-functies voor wachtwoorden, die bedoeld zijn om te voorkomen dat een aanvaller met toegang tot de centrale database platte tekst (plaintext) wachtwoorden kan herstellen. In zeer vereenvoudigde bewoordingen: de wachtwoorden worden niet opgeslagen in platte tekst (zoals Password123) maar als een hash (zoals ########).

Hoewel deze hashing-functionaliteit een cruciale bescherming van de wachtwoorden is tegen ongeoorloofde toegang, voorkomt het ook dat een organisatie de wachtwoorden evalueert in termen van hun sterkte. Dit is echter noodzakelijk om passende maatregelen te nemen tegen mogelijke aanvallen, zoals het uitproberen van wachtwoorden met woorden uit het woordenboek, het gebruik van bekende gecompromitteerde wachtwoorden of het raden van wachtwoorden op basis van persoonlijke informatie over de beoogde gebruiker.

Het eerste deel van de maatregel, wachtwoordbeveiligingsbeoordeling, identificeert de veerkracht van wachtwoorden door een echte aanval te simuleren die potentiële kwetsbaarheden exploiteert en blootlegt, zoals voorspelbare, zwakke wachtwoorden die door meerdere gebruikers worden gebruikt en gebrekkige cryptografische implementaties.

De gehashte wachtwoorden worden teruggezet naar in platte tekst en beoordeeld op basis van objectieve wiskundige en structurele entropie, subjectief wachtwoordbeleid en nalevingscriteria. Dit gebeurt in overeenstemming met de toepasselijke regelgeving inzake gegevensbescherming. Platte-tekstgegevens worden op geen enkel moment opgeslagen of weergegeven. Zodra de beoordeling is voltooid, worden de “platte tekst” wachtwoorden verwijderd en wordt een zinvol rapport gegenereerd.

De geaggregeerde resultaten van de wachtwoordbeoordeling maken het mogelijk om de beveiligingsrisico's van de wachtwoorden die in de verschillende, meervoudige en heterogene systemen worden gebruikt, te meten. Zo kunnen passende bewustmakings- en opleidingsmaatregelen worden gedefinieerd en kunnen centrale handhavingsmethoden voor sterke wachtwoorden worden geïdentificeerd. Dit maakt ook de beoordeling en optimalisatie mogelijk van de effectiviteit van reeds bestaande maatregelen met objectieve statistieken.

Het tweede deel van de maatregel is het afdwingen van sterke wachtwoorden. Het dwingt het gebruik van sterke en veilige wachtwoorden af in alle technische en organisatorische maatregelen die door een organisatie worden gebruikt.

De vereiste sterkte van elk nieuw wachtwoord wordt aangepast aan het beveiligingsniveau van het betreffende gebruikersaccount door middel van een reeks regels. Het gedefinieerde beveiligingsniveau is gebaseerd op de potentiële impact van een compromitteren van de beveiliging van dat account.

Nieuw ingestelde wachtwoorden worden gecontroleerd aan de hand van een set regels die overeenkomen met het beveiligingsniveau en aan elk account worden toegewezen. Deze regels omvatten vereisten voor samenstelling (lengte, tekenset, symbolen, letterreeksen en herhalingen), wiskundige en structurele entropiewaarden, uniciteit (het wachtwoord mag niet worden gebruikt door een ander account op hetzelfde systeem in de organisatie), het gebruik van bekende standaardwachtwoorden en historisch wachtwoordhergebruik. De regels zijn niet beperkt tot de klassieke zwarte lijst (blacklist), maar kunnen individueel worden geparametriseerd.

Platte tekstgegevens worden op geen enkel moment opgeslagen of weergegeven. Als het wachtwoord wordt geweigerd wanneer een wachtwoordwijziging vereist is, dan wordt de gebruiker geïnformeerd door middel van een met redenen omkleed individueel bericht.

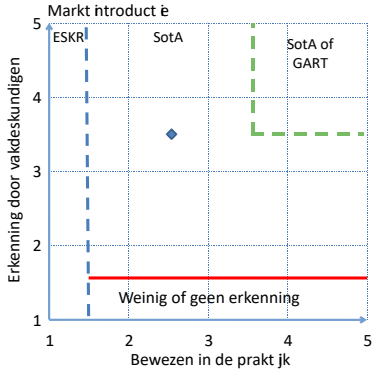
Idealiter wordt deze maatregel centraal toegepast en beheerd voor alle systemen binnen de organisatie vanuit één interface. Hierdoor kan coherent, systeem overschrijdend beleid effectief van kracht worden, wordt meervoudig gebruik van wachtwoorden in verschillende systemen voorkomen en wordt een centrale registratie van de wachtwoordgeschiedenis mogelijk.

De beschreven maatregel leidt tot de centrale handhaving van de respectieve juiste wachtwoordsterkte en geeft de organisatie volledige controle, beheer en documentatie van de sterkte van de wachtwoorden die in de organisatie worden gebruikt. Regelmatige toepassing van de maatregelen maakt het mogelijk om te meten of de regels werken zoals verwacht of dat ze indien nodig moeten worden gecorrigeerd om in de gehele organisatie de juiste wachtwoordsterkte te bereiken.

Welke beschermingsdoelen vallen onder deze maatregel?

☐ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.3 Multifactor authenticatie

In de context van dit artikel wordt authenticatie opgevat als bewijs van een bepaalde identiteit van een computersysteem. Al geruime tijd is de combinatie van gebruikersnaam en wachtwoord de meest gebruikte methode om tijdens het inloggen een gebruiker te authentiseren. Het is nog steeds de meest gebruikte single-factor authenticatiemethode voor het bewijzen van identiteit[12].

Multi-factor authenticatie (MFA) is de term die wordt gebruikt om het proces te beschrijven van het bewijzen van de identiteit van een gebruiker met meer dan één factor (zoals wachtwoord + eenmalig wachtwoord (OTP) of wachtwoord + vingerafdruk + beveiligingstoken).

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

Als een systeem is beveiligd met slechts één factor (single-factor authenticatie), is de gebruikersidentiteit onderhevig aan een verhoogd risico op:

- identiteitsdiefstal;
- misbruik van identiteiten;
- identiteitsfraude.

Eén factor alleen is niet genoeg om computertoegang/gebruikersaanmeldingen die bescherming vereisen te beveiligen - de methoden van digitale aanvallers worden steeds geavanceerder en de potentiële schade wordt steeds drastischer als gevolg van voortdurende netwerken en digitalisering. 81% van alle datalekken wordt veroorzaakt door gestolen of zwakke wachtwoorden (d.w.z. single-factor authenticatie)[13]. Dit zeer hoge percentage wordt met name veroorzaakt door:

- menselijke risico's bij het omgaan met wachtwoorden:
    - onvoldoende kwaliteit van wachtwoorden;
    - te vaak hetzelfde wachtwoord gebruiken;
    - opzettelijke openbaarmaking van wachtwoorden (zoals het delen ervan met andere

[12] Omwille van de eenvoud, deze overweging is uitsluitend gebaseerd op het wachtwoord als enige factor.
[13] Bron: Verizon Data Breach Investigations Report 2017

mensen); of
    - onbedoelde openbaarmaking van wachtwoorden (zoals het opschrijven ervan);
- technische risico's bij het omgaan met wachtwoorden:
    - man in the middle aanvallen;
    - phishing-aanvallen;
    - keylogger-gebaseerde aanvallen;
    - brute force aanvallen, enz.

Het gebruik van MFA-oplossingen kan deze risico's aanzienlijk verminderen.

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?
Naast het conventionele wachtwoord zijn er verschillende authenticatiemethoden en -oplossingen (MFA-systemen) beschikbaar. Ze kunnen worden onderverdeeld in drie hoofdcategorieën:

- op kennis gebaseerde factoren (bijvoorbeeld wachtwoord, pincode, wachtwoordzin, enz.);
- op bezit gebaseerde factoren (bijvoorbeeld beveiligingstoken, smartcard, enz.);
- biometrische factoren (bijvoorbeeld vingerafdruk, iris, enz.).

MFA-systemen combineren meestal twee methoden uit verschillende categorieën in een authenticatieketen, hoewel sommige MFA-systemen ook een willekeurig aantal methoden aan elkaar kunnen koppelen. Het combineren van methoden uit slechts één categorie is niet aan te raden. Let wel: niet alle methoden van deze drie categorieën zijn noodzakelijkerwijs gelijkwaardig, zelfs wanneer ze worden gecombineerd. Elke combinatie is echter een verbetering ten opzichte van het gebruiken van alleen maar een wachtwoord. De beslissing welke authenticatiemethoden moeten worden gecombineerd, hangt af van de beveiligingsbehoeften van de toepassing of gebruikersidentiteit en van de technische vereisten.

Bovendien bieden sommige MFA-systemen een dynamische benadering van gebruikersauthenticatie (adaptieve authenticatie). In dit geval is de combinatie van de authenticatieketen niet langer statisch, maar situatieonafhankelijk en flexibel. De volgende factoren kunnen bijvoorbeeld worden opgenomen: geografische locatie van de gebruiker, unieke apparaat-ID en/of apparaat-IP, typische werktijd van de gebruiker, enz.

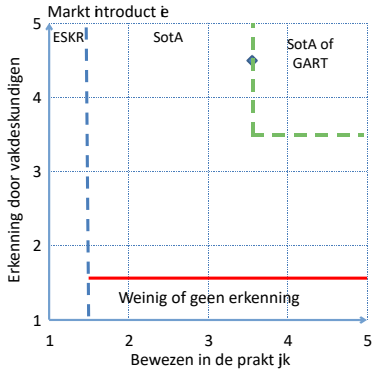
MFA kan nu in veel toepassingen worden geactiveerd of maakt deel uit van de productopties. Als dit niet het geval is voor toepassingen die beveiliging vereisen of als een organisatie meerdere toepassingen gebruikt die beveiliging vereisen, wordt een centrale verificatieoplossing voor alle toepassingen en gebruikers aanbevolen. Het gelijktijdige gebruik van verschillende oplossingen moet worden vermeden vanwege de toenemende complexiteit, hogere kosten en grotere administratieve inspanningen. Moderne MFA-oplossingen bieden een breed scala aan bruikbare methoden en ondersteunde eindapparaten, evenals een centrale authenticatie-instantie voor alle gebruikers, applicaties en systemen.

Vanwege de bovengenoemde menselijke en technische risico's van single-factor authenticatie, vereisen verschillende nationale en internationale regelgeving zoals NIST, PSD2, KRITIS, AVG en BAFIN het gebruik van MFA om gebruikerstoegang tot een te beschermen computersysteem te beveiligen.

Welke beschermingsdoelen vallen onder deze maatregel

☐ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.4 Cryptografische methoden

Cryptografie in de zin van informatiebeveiliging houdt zich bezig met het ontwerpen, definiëren en bouwen van informatiesystemen die zo goed mogelijk bestand zijn tegen manipulatie en ongeoorloofd lezen.

Zogenaamde cryptografische methoden zijn toepasbare methoden om gevoelige inhoud te beschermen. De kwaliteit van de cryptografische methoden hangt met name af van de gebruikte coderingsmethode (bijvoorbeeld AES, ECIES), de geselecteerde sleutellengte (bijvoorbeeld 512 bits) en de geïmplementeerde beveiligingsconfiguratie van de gebruikte producten. Naarmate de sleutellengte toeneemt, groeit het aantal manieren om een gecodeerd bericht te decoderen, waardoor de beveiliging toeneemt

Cryptografie in de zin van informatiebeveiliging houdt zich bezig met het ontwerpen, definiëren en bouwen van informatiesystemen die zo goed mogelijk bestand zijn tegen manipulatie en ongeoorloofd lezen.

In de moderne cryptografie moeten de gebruikte methoden voldoen aan het zogenoemde principe van Kerckhoffs. Hierin staat dat de beveiliging van een versleutelingsmethode is gebaseerd op de geheimhouding van de sleutel. Daarom kan de gebruikte procedure publiekelijk bekend worden gemaakt.

Er wordt onderscheid gemaakt tussen symmetrische en asymmetrische encryptiemethoden:

Symmetrische methodes	**Asymmetrische methodes**
▪ Gecompliceerde sleuteldistributie (als geen beveiligd communicatiekanaal beschikbaar is). ▪ Alle deelnemers die bij betrokken zijn bij dezelfde communicatie gebruiken slechts één (dezelfde) sleutel. Dezelfde sleutel wordt dus gebruikt voor encryptie en ontsleuteling. Voor elke nieuwe communicatie-instantie moet een nieuwe sleutel worden gegenereerd: n instanties vereisen (n*(n-1))/2-sleutels. ▪ Snelle versleuteling van massagegevens. ▪ De enige aantoonbaar veilige versleutelingsmethode is Vernam-Cipher/one-time-pad. ▪ Spontane versleutelde communicatie zonder voorafgaand vertrouwen (tenminste om de sleutel uit te wisselen) is onmogelijk tenzij kwantumcryptografie wordt gebruikt.	▪ Voor onafhankelijk gecodeerde communicatiekanalen neemt het vereiste aantal sleutels lineair toe met het aantal deelnemers (met symmetrische codering neemt dit aantal met het aantal onafhankelijke communicatie-instanties zeer snel toe). ▪ Alle bekende asymmetrischer methoden zijn in vergelijking met symmetrische methoden met een vergelijkbare sleutellengte erg traag. ▪ Om dezelfde mate van veiligheid te bereiken is de vereiste sleutellengte meestal groter dan bij symmetrische cryptografie. ▪ Digitale handtekeningen zijn mogelijk. ▪ Eenvoudige sleuteluitwisseling; er zijn twee sleutels (public en private). De public sleutel wordt gebruikt voor versleuteling, de private sleutel alleen voor ontsleuteling. Private sleutels worden niet uitgewisseld. ▪ Niet geschikt voor grote hoeveelheden gegevens.

In de hybride methode, die meestal in de praktijk wordt toegepast, worden symmetrische en asymmetrische codering gecombineerd om de voordelen van elke techniek te benutten. In de praktijk wordt het uit te wisselen bericht symmetrisch versleuteld met een sessiesleutel. Deze moet groot genoeg zijn om brute forcering van de gehele sleutelruimte te voorkomen. Deze sessiesleutel wordt vervolgens asymmetrisch gecodeerd met de openbare sleutel van de ontvanger en toegevoegd aan het gecodeerde bericht.

Met de toenemende technische ontwikkeling en de daaruit voortvloeiende toename van de rekenkracht, bestaat het risico dat de geheime sleutelinformatie wordt achterhaald en de tot nu toe gebruikte methoden daarmee worden doorbroken.

Dit is precies wat er verwacht wordt bij de inmiddels legendarische kwantumcomputers. De verwachting is dat zodra kwantumcomputers beschikbaar zijn, de tot nu toe gebruikte methoden worden gebroken of dat hun effectiviteit op zijn minst gehalveerd zal zijn.

Onlangs is de ontwikkeling naar kwantumcomputers begonnen. Over de hele wereld werken veel

onderzoeksgroepen aan het bouwen van een kwantumcomputer die de rekenkracht voor bepaalde taken aanzienlijk zou verbeteren. In 2019 kondigde een van de spelers bijvoorbeeld trots aan dat het een kwantumcomputer had gebouwd met 100 miljoen keer snellere rekenkracht in vergelijking met een klassieke computer. Zelfs als deze computer nog niet kan worden gebruikt voor universele taken, laat dit voorbeeld zien dat dit slechts een kwestie van tijd is.

Om deze ontwikkeling aan de encryptiekant tegen te gaan, werkt het National Institute of Standards and Technology (NIST) al aan de standaardisatie van methoden voor kwantumresistente cryptografie. De normen worden in 2023 verwacht.

Los hiervan wordt aanbevolen dat de gebruikte versleutelingsmethoden regelmatig (bijvoorbeeld jaarlijks) worden gecontroleerd op hun doeltreffendheid en actualiteit en indien nodig naar behoren worden aangepast. Dit kan bijvoorbeeld door de sleutellengte te wijzigen (bijvoorbeeld van 128 bits naar 256 bits). Tegen de achtergrond van de hierboven geschetste ontwikkeling moet er nu voor worden gezorgd dat cryptografische procedures ook in de toekomst kunnen worden uitgewisseld. Deze crypto-wendbaarheid is absoluut noodzakelijk om het vereiste beveiligingsniveau in de toekomst te garanderen. Op deze manier kan rekening worden gehouden met de vraag van veel organisaties om verifieerbare algoritmen (zoals open source bibliotheken) te gebruiken. Dit stelt hen, of experts, in staat om te controleren of er achterdeurtjes of opzettelijke zwakheden in de algoritmes zijn ingebouwd.

In de BSI Technical Guideline (BSI TR-02102-1) worden de coderingsmethoden op een specifieke manier gepresenteerd en wordt, afhankelijk van de gebruikte sleutellengte, de gebruiksduur ervan aanbevolen[14]. Meer aanbevelingen over instrumenten en methoden zijn verkrijgbaar bij Enisa[15] en NIST[16].

Welke beschermingsdoelen vallen onder deze maatregel

☒ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

3.2.5 Schijfversleuteling

Volledige schijfversleuteling beschermt gegevensopslagapparaten, zoals magnetische harde schijven en op flashgeheugen gebaseerde SSD's, die in een systeem zijn geïnstalleerd tegen onbevoegde toegang (lezen, wijzigen) door derden. De informatie die daar is opgeslagen, is niet toegankelijk als leesbare tekst, tenzij de gebruiker is geverifieerd voordat het besturingssysteem van de pc of smartphone wordt opgestart.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

Deze maatregel beschermt gegevens op de harde schijven van onbeheerde, uitgeschakelde eindapparaten zoals pc's, laptops, tablets en smartphones (gegevens in rust of data in rest). In het geval van verlies door onoplettendheid of diefstal, of tijdelijke beschikbaarheid voor onbevoegde derden (hotelkamers), kunnen aanvallers de inhoud niet inzien of de opgeslagen informatie manipuleren. Het kopiëren van de Read Only geheugens van apparaten die op deze manier zijn beveiligd, levert omdat deze zijn gecodeerd, dan alleen nutteloze gegevens op.

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

De gegevensdrager(s) die in een systeem zijn geïnstalleerd, zoals magnetische harde schijven en op flashgeheugen gebaseerde SSD's waarop het besturingssysteem en bedrijfsvertrouwelijke gegevens zijn opgeslagen, worden door de maatregel zodanig versleuteld, dat het ongeoorloofd lezen ervan geen platte tekst oplevert. Dit geldt zowel voor het uitlezen van het uitgeschakelde systeem of van de verwijderde harde schijf, als tijdens het gebruik voor het aftappen van de gegevens op de interne interface van de harde schijf (eSATA enz.).

Als symmetrische codering moet ten minste AES-256 in XTS-modus worden geselecteerd. Een centrale beheertool vergemakkelijkt het gebruik op alle pc's van een organisatie aanzienlijk. De cryptografische sleutels mogen nooit in de cloud worden opgeslagen, zelfs niet voor back-updoeleinden.

Bij de keuze van de authenticatiefuncties moet veel belang worden gehecht aan moeilijk te kraken wachtwoorden en 2-factor authenticatie, idealiter gebaseerd op kennis en bezit, bijvoorbeeld met een extra token. Dit maakt ook het gebruik van hardware-ondersteunde vertragingsmechanismen mogelijk bij meerdere onjuiste wachtwoordinvoer. Het verwijderen van de gegevensdrager voor analyse in een

[14] https://www.bsi.bund.de/de/publikationen/technischerichtlinien/tr02102/tr02102_node.html
[15] https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data/cryptographic-protocols-and-tools
[16] https://www.nist.gov/cryptography

aanvallersysteem wordt zinloos.

Voor zover het apparaat dit toelaat, bijvoorbeeld bij Windows 10-systemen, moet ook de zogenaamde Secure Boot worden ondersteund. Dit beschermt het hele opstartproces, inclusief 2-factor authenticatie, tegen manipulatie en behoudt de integriteit van het systeem en de coderingsmechanismen.

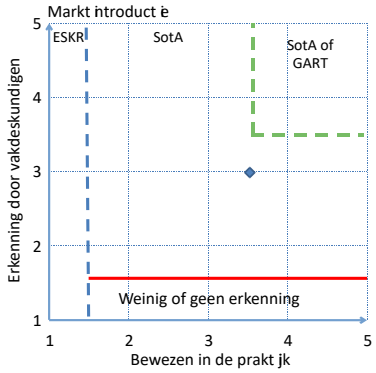
Sommige beschikbare oplossingen ondersteunen ook volledige of map-gebaseerde (folder-based) versleuteling van verwisselbare media. Binnen organisaties heeft automatische, gebruikerstransparante encryptie voor bedrijfsgegevens de voorkeur om platte tekst opslag als gevolg van bedieningsfouten te voorkomen.

Er zijn oplossingen voor Windows 7, 8 en 10 beschikbaar die door de BSI voor gebruik door overheidsinstanties zijn goedgekeurd, maar die ook kunnen worden gebruikt in kritieke infrastructuren en bedrijven.

Welke beschermingsdoelen vallen onder deze maatregel

☐ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☐ Authenticiteit

Stand der techniek classificatie



3.2.6 Versleuteling van bestanden en mappen

Bestand- en map-versleuteling omvatten de versleuteling van afzonderlijke objecten, zoals containers, mappen en individuele bestanden, daarom wordt dit type versleuteling ook wel objectversleuteling genoemd. De programma's die hiervoor beschikbaar zijn, werken vaak transparant, wat betekent dat gebruikers met de objecten kunnen werken alsof ze niet versleuteld zijn.

Objectversleuteling biedt de mogelijkheid om bestanden en mappen veilig van de ene locatie naar de andere te transporteren en te voorkomen dat onbevoegde gebruikers er toegang toe krijgen. Daarom moet ervoor worden gezorgd dat niemand anders dan de bevoegde personen toegang heeft tot de beschermde informatie. Dit kan in individuele gevallen persoonsgegevens of, in het ergste geval, het levensonderhoud van een organisatie in gevaar brengen.

Bovendien is objectversleuteling nuttig bij het gebruik van cloud-services omdat het effectief voorkomt dat gegevens toegankelijk zijn voor de operator.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

1. Onderschepping en misbruik van gegevens tijdens transport, zoals via e-mail.
2. Verlies en diefstal van verwisselbare media met daaropvolgende ongeoorloofde toegang tot gevoelige gegevens.
3. Misbruik van gegevens die zijn opgeslagen in de cloud.

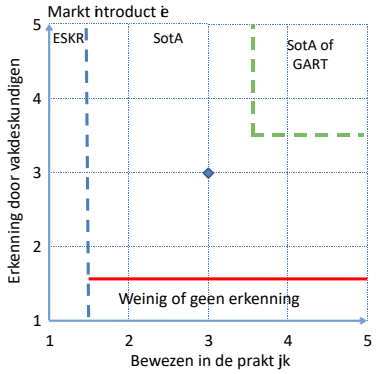
Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

Bestands- en map-versleuteling omvat en de versleuteling van afzonderlijke objecten, zoals containers, mappen en individuele bestanden, daarom wordt dit type versleuteling ook wel objectversleuteling genoemd. De programma's die hiervoor beschikbaar zijn, werken vaak transparant, wat betekent dat gebruikers met de objecten kunnen werken alsof ze niet versleuteld zijn.
Objectversleuteling biedt de mogelijkheid om bestanden en mappen veilig van de ene locatie naar de andere te transporteren en te voorkomen dat onbevoegden er toegang toe krijgen.

Welke beschermingsdoelen vallen onder deze maatregel

☐ Beschikbaarheid ☐ Integriteit ☒ Vertrouwelijkheid ☐ Authenticiteit

Stand der techniek classificatie



3.2.7 E-mail versleuteling

Zakelijke e-mailsberichten bevatten vaak belangrijke en gevoelige gegevens en e-mailadressen zijn vaak ook gepersonaliseerd, en bevatten daarom over het algemeen persoonsgegevens die beschermd moeten worden tegen ongeoorloofde toegang of wijziging. Doorgaans kunnen de beschermingsdoelstellingen worden bereikt door de overdracht van e-mailberichten/of e-mailinhoud te versleutelen.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

- Het bespioneren of manipuleren van e-mailberichten tijdens transport.
- Het bespioneren of manipuleren van opgeslagen e-mailberichten.

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

- Versleutelde e-mailoverdracht (transportversleuteling), TLS.
- Versleuteling van de inhoud van emailberichten; S/MIME of PGP.

De beveiligingseisen voor e-mail zijn onder andere gebaseerd op het type gegevens dat wordt verzonden en opgeslagen in het e-mailsysteem. Bij zakelijke transacties kan er over het algemeen van worden uitgegaan dat e-mailberichten in ieder geval voor de organisatie belangrijke informatie bevatten. E-mailadressen, indien gepersonaliseerd, blijven beschouwd als persoonsgegevens; Er kan daarom van worden uitgegaan dat per e-mail persoonsgegevens worden verzonden en opgeslagen. In individuele gevallen en afhankelijk van het gebruik van e-mail kunnen ook gegevens met speciale beschermingsbehoeften, zoals gegevens over gezondheid, klantgegevens van advocaten, en bijzonder waardevolle bedrijfsgeheimen zoals ontwerpgegevens, worden verzonden.

Dit resulteert in de volgende beveiligingsvereisten voor e-mail:

- Bescherming tegen ongeoorloofde toegang of wijziging van e-mailberichten tijdens transport en opslag (beschermingsdoelstelling: vertrouwelijkheid),
- Bescherming tegen latere wijziging van e-mailberichten die langdurig worden gearchiveerd (beschermingsdoelstelling: integriteit).

Deze beveiligingsdoelstellingen kunnen over het algemeen worden bereikt met versleuteling. Voor e-mailversleuteling moet een onderscheid worden gemaakt tussen het versleutelen van de verzending (transportversleuteling) en het versleutelen van het e-mailbericht zelf (met end-to-end encryptie). De beschermingsdoelstellingen vereisen het gebruik van transport-versleuteling, althans bij het verzenden van e-mailberichten via openbare netwerken. De protocollen die worden gebruikt bij het verzenden van e-mailberichten via internet, namelijk SMTP, POP3 en IMAP, bieden echter in hun basisvorm, onversleutelde gegevensoverdracht Grote delen van het e-mailverkeer worden dus nog steeds onversleuteld verzonden, terwijl er al lang genoeg tools beschikbaar zijn voor e-mailversleuteling.

De huidige versie van TLS (Transport Layer Security, gedefinieerd in RFC 5246) moet worden gebruikt voor transportversleuteling in e-mailverkeer. Er moeten veilige versleutelingsmethoden (zoals momenteel AES-256) worden gebruikt; onveilige versleutelingsmethoden (zoals RC4) mogen niet worden gebruikt. Als algemene regel: forward secrecy moet worden geactiveerd. Het is ook verstandig om de certificaten die door de betreffende andere partij voor TLS worden gebruikt, te controleren op echtheid en geldigheid, bijvoorbeeld met behulp van DANE (RFC 7671). De BSI's Technical Guidelines

TR-02102-02, deel 2, biedt een uitgebreide lijst met aanbevelingen voor TLS.

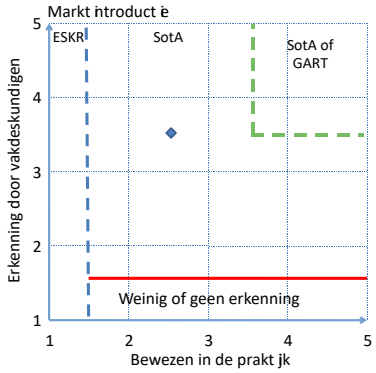
End-to-end encryptie wordt aanbevolen om bijzonder gevoelige gegevens te beschermen. Hiervoor zijn twee standaarden opgesteld: S/MIME (Secure/Multipurpose Internet Mail Extensions, gedefinieerd in RFC 5751) en OpenPGP (Pretty Good Privacy, gedefinieerd in RFC 4880). Beide gebruiken in wezen dezelfde cryptografische mechanismen. Ze verschillen echter in de certificering van openbare sleutels en dus in vertrouwelijkheidsmodellen en zijn niet compatibel met elkaar.

Bij het gebruik van end-to-end versleuteling heeft geen enkel systeem in het transmissiepad toegang tot de inhoud van het e-mailbericht Dit betekent echter dat het gebruik van inhoudsfilters, antivirusprogramma's, antispam, preventie van gegevensverlies en archivering volledig moet worden vermeden. Daarom kan inhoudsversleuteling (content encryptie) alleen zinvol worden gebruikt tussen organisaties; Dit betekent dat e-mailberichten worden versleuteld en onversleuteld worden verzonden via het openbare internet naar het particuliere netwerk (gateway) van de organisatie (end-to-end versleuteling van de organisatie), of indien nodig worden gecombineerd met interne versleuteling van bedrijfsinhoud.

Welke beschermingsdoelen vallen onder deze maatregel

☐ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.8 Beveiligen van elektronische datacommunicatie met PKI

Bij elektronische datacommunicatie is het belangrijk dat de identiteit van de communicatiepartners en de authenticiteit van de verzonden inhoud worden gewaarborgd. Het bewijs van elektronische identiteit van personen, organisaties of apparaten kan worden gewaarborgd door het gebruik van elektronische certificaten. Elektronische handtekeningen zijn geschikt om de authenticiteit van verzonden documenten en berichten te bewijzen. Op certificaten gebaseerde oplossingen worden ook gebruikt voor veilige versleuteling van gegevenstransport. Deze scenario's vereisen een component voor het genereren, beheren en verifiëren van elektronische certificaten die het bewijs van elektronische identiteiten op een betrouwbare manier garanderen: een Public Key Infrastructure (PKI).

De eIDAS-verordening [17]die sinds de zomer van 2016 van kracht is, voorziet ook in het gebruik van een PKI.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

- identiteitsdiefstal / voorwendsel van een valse identiteit;
- manipulatie van de inhoud van digitale berichten of bestanden;
- manipulatie van de timing van berichten of bestanden.

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

De volgende maatregelen zijn verstandig tegen de hierboven beschreven bedreigingen:

- Een interne PKI maken of een externe PKI gebruiken.
- Het gebruik van digitale handtekeningen (handtekeningen, certificaten, stempels) van een geaccrediteerd vertrouwenscentrum.
- Het gebruik van gekwalificeerde tijdstempels om de authenticiteit en timing van berichten en documenten te bewijzen.

De digitale certificaten worden uitgegeven door de certificeringsinstantie van een PKI-organisatie. De term certificate authority of CA wordt hier gebruikt. De geldigheid van openbare

[17] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex:32014R0910

sleutels wordt bevestigd door de digitale handtekeningen van CA's hier. Naast de sleutel zelf bevat het digitale certificaat ook andere informatie, zoals de geldigheidsduur, enz. De CA is verantwoordelijk voor het centrale onderdeel in de Public Key Infrastructure. Om de betrouwbaarheid van de CA's te behouden, moet de identiteit van de aanvrager, of het nu een persoon of organisatie is, worden onderworpen aan een ondubbelzinnige inspectie voordat het elektronische certificaat wordt afgegeven. Dit wordt gedaan door de Registratieautoriteit (RA).

Een validatieautoriteit (VA) is vereist om de geldigheid van digitale certificaten te controleren. Over het algemeen wordt een onderscheid gemaakt tussen de controle aan de hand van een gepubliceerde certificaat-intrekkingslijst (CRL) of real-time validatie via een online certificate status protocol service (OCSP). De keuze van het type inspectie is meestal per geval gebaseerd op het toepassingsscenario.

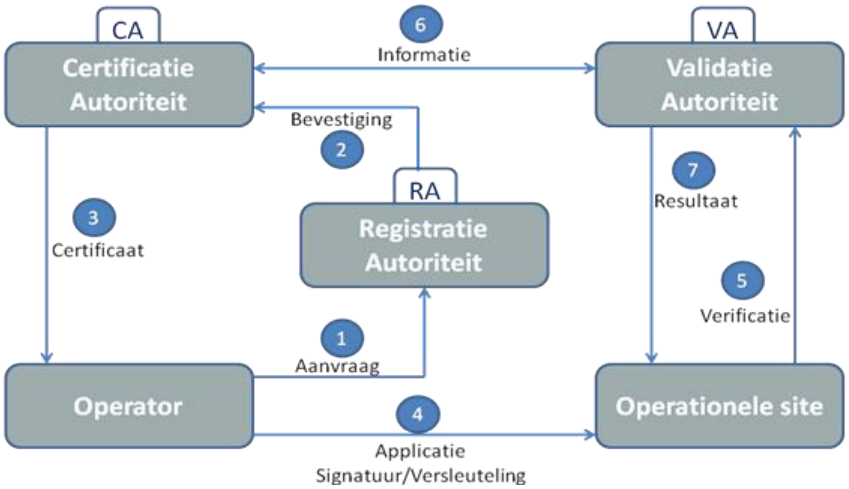
Afhankelijk van de juridische status van de PKI's is het wettelijk toelaatbaar loggen van alle transacties in een PKI verstandig of in de meeste gevallen zelfs noodzakelijk. Ook zijn voor sommige toepassingsgebieden gecertificeerde CA-producten vereist.

De toepassingen van PKI-gebaseerde methoden zijn divers. Als voorbeelden worden de volgende aanvraagprocedures genoemd:

- handtekening en encryptie van e-mailberichten (S/MIME);
- authenticatie en encryptie in het Internet of Things (IOT);
- authenticatie en encryptie op het web (HTTPS);
- authenticatie en encryptie voor VPN-diensten;
- authenticatie en integriteitsbeveiliging voor uitvoerbare code (code signing);
- authenticatie en integriteitsbeveiliging voor documenten (digitale handtekening);
- authenticatie van clients/gebruikers op het internet.

Afhankelijk van de exploitant en de beveiligingsstandaard van het speciale computercentrum kan een breed scala aan oplossingen worden geregeld. Dit varieert van een basis-CA (Root-CA) als een vertrouwensanker (trust-anchor) tot een strikt hiërarchische PKI met verschillende sub-CA's. Ook kan cross-certificering met andere PKI's worden geïmplementeerd.

In de volgende afbeelding ziet u de algemene structuur en interactie van PKI-onderdelen in een werkstroom.



Het gebruik van certificaten is op bijna alle gebieden zinvol en nuttig. Naast toepassingsgebieden in de publieke sector zijn ze ook te vinden in de energie- en gasvoorziening, e-justitie (met beA, beN, beBPO), gezondheidszorg en de industriële en non-profitsector (zoals federaties en verenigingen).

Met name de eIDAS-verordening voorziet in een uitgebreid scala aan gebruiksscenario's. Bewijs van identiteit en vertrouwensdiensten wordt bijvoorbeeld ondersteund door PKI's (zie onderstaande tabel).

eIDAS voorschriften/toepassingen	
Identiteiten	Certificaten
	Elektronische ID's
Vertrouwensdiensten (Trust services)	Elektronische stempels (electronic stamps)
	Elektronische tijdstempels (time stamps)
	Website authenticatie
	Elektronische bezorgdiensten (Delivery services)
	Bewakingsdiensten (preservation services)

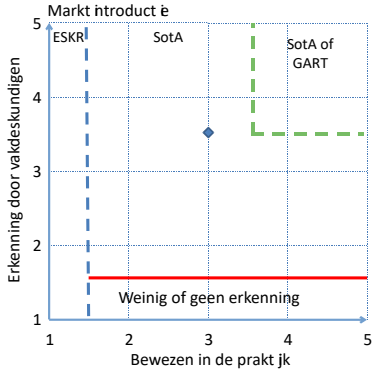
Een voorbeeld van gebruik in de publieke sector is: www.cio.bund.de/Web/DE/IT-Angebot/ITBeratungsdienstleistungen/Public-Key-Infrastruktur-der-Verwaltung/public_key_node.html en in de energievoorzieningssector: www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/PKI/pki_node.html

Voorbeelden van gebruik in de publieke sector zijn: www.cio.bund.de/web/de/it-angebot/it-Beratungsdienstleistungen/public-key-infrastruktur-der-verwaltung/public_key_node.html, in de energievoorziening sector: www.bsi.bund.de/de/themen/digitalegesellschaft/smartmeter/pki/pki_node.html en bij TeleTrusT: https://www.ebca.de.

Welke beschermingsdoelen vallen onder deze maatregel

☐ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.9 Gebruik van VPN's (layer 3)

Een layer 3 VPN beschrijft de verbinding van twee of meer netwerken op laag 3 van het OSI-model[18]. De verzonden gegevens zijn versleuteld. Hierdoor kunnen bijvoorbeeld bedrijfsfilialen in verschillende landen veilig en vertrouwelijk via internet met elkaar verbonden zijn.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

Het gebruik van VPN's beschermt tegen:

- verlies van vertrouwelijkheid door niet-versleutelde/slecht versleutelde verbindingen;
- externe aanvallers;
- verbindingsmanipulatie.

De gebruikte VPN's zijn zelf onderhevig aan andere bedreigingen:

- uitstroom van sleutelmateriaal;
- zwakke cryptografie;
- denial of service: De beschikbaarheid van VPN's wordt bedreigd door fouten of aanvallen.

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

Een layer 3 VPN beschrijft de verbinding van twee of meer netwerken of het koppelen van een client

[18] https://www.itu.int/rec/t-rec-x.200-199407-I/en

aan een netwerk op laag 3 van het OSI-model. De gegevens die in dit proces worden getransporteerd, worden versleuteld en de VPN-eindpunten verifiëren en autoriseren het andere respectieve VPN-eindpunt. Hierdoor kunnen bijvoorbeeld bedrijfsfilialen in verschillende landen veilig en vertrouwelijk via veilige lijnen van derden, zoals internet en diensten die worden ingehuurd door een aanbieder van telecommunicatiediensten, met elkaar worden verbonden. Er worden minder gegevens getransporteerd in vergelijking met een layer 2 VPN omdat layer 2-gegevens, zoals broadcasts, niet worden verzonden. Omgekeerd kan een layer 3 VPN hierdoor niet transparant gebruikt worden voor alle applicaties. Complexe topologieën, zoals on-demand VPN-verbindingen, kunnen soms alleen met een layer 3 VPN worden geïmplementeerd of het is aanzienlijk eenvoudiger om dit te doen. Hetzelfde geldt voor VPN-configuraties met een groot aantal eindpunten. Een layer 3 VPN vereist VPN-toegang voor elke deelnemer. Vaak wanneer een hub-and-spoke VPN-architectuur wordt gebruikt, wordt het centrale knooppunt aangeduid als een VPN-concentrator. Het is aan te bevelen om als oplossing een layer 3 VPN van de fabrikant te kopen.

Als een belangrijk onderdeel van een IT-infrastructuur moet de configuratie en werking van een layer 3 VPN speciale aandacht krijgen. Een layer 3 VPN-oplossing mag alleen worden geleverd door geautoriseerde en vertrouwde leveranciers. Van fabrikanten van veilige VPN-oplossingen kan worden verwacht dat ze actief patchbeheer bieden en snel reageren op beveiligingsproblemen, zodat u te allen tijde de best mogelijke bescherming hebt. Een fabrikant zonder bijbehorend patchbeheer kan niet als een professional worden beschouwd en moet worden uitgesloten van het selectieproces.

Een layer 3 VPN moet de vertrouwelijkheid van de gegevens die erdoorheen worden geleid waarborgen. Voor dit doel moet het apparaat versleuteling en verificatie uitvoeren met algoritmen en parameters die als veilig worden beschouwd. De fabrikant moet kunnen aantonen dat hij actief werkt aan de beveiliging van de gebruikte cryptografie, hetzij door algoritmen te vervangen die onveilig zijn geworden, hetzij door geschikte parameters te kiezen. W ar technisch mogelijk moeten veilige authenticatiemechanismen worden gebruikt. Er moeten verschillende maatregelen worden genomen om extra bescherming te bieden voor de toegang tot het beheer van de layer 3 VPN. Dit omvat versleutelde toegang met beveiligde authenticatie (zoals. HTTPS voor een WebGUI, SSH voor consoletoegang, beschermde authenticatie-informatie in hardware), maar ook de speciale aandacht van de fabrikant voor de beveiliging van het platform voor het VPN-apparaat zelf om ongeoorloofde toegang als gevolg van technische tekortkomingen uit te sluiten. Gevoelige informatie wordt over het algemeen getransporteerd via een VPN.

Een layer 3 VPN met apparaten die backdoors bevatten of softwarebugs laten draaien zodat de apparaten zelf overgenomen kunnen worden is een onacceptabel risico. Daarom moet de voorkeur worden gegeven aan producten die een hoge platformbeveiliging en een hoog niveau van zelfbescherming kunnen aantonen, bijvoorbeeld door middel van onafhankelijke inspecties (certificeringen of zelfs accreditatie). De eisen voor de operationele omgeving moeten ervoor blijven zorgen dat fysieke toegang tot VPN-apparaten alleen mogelijk is voor geautoriseerde personen.

Net als de doelstelling van vertrouwelijkheidsbescherming is de integriteit van het platform cruciaal voor het behoud van de integriteit en authenticiteit van de gegevens die er doorheen worden geleid. Ook hierbij is het belangrijk dat de VPN-apparaten geïnstalleerd zijn op een extra gehard platform, een uitstekende zelfbescherming hebben en geen achterdeurtjes hebben. De beveiligingsprotocollen die een layer 3 VPN gebruiken, garanderen ook de integriteit en authenticiteit van de getransporteerde gegevens. Ook het beheer en het veilig gebruik van belangrijke materialen spelen een cruciale rol. Fabrikanten die kunnen aantonen dat zij het veilig genereren van willekeurige getallen, veilig sleutelbeheer voor private keys (zoals op chipkaarten) en het bijhouden van de leeftijd van gebruikte encryptie-keys mogelijk maken moeten de voorkeur krijgen.

Er zijn passende maatregelen nodig om de beschikbaarheid van layer 3 VPN's voor VPN-endpoint hardware en -software (zoals VPN-concentrators) te waarborgen. Met betrekking tot hardware moet de fabrikant kunnen aantonen dat het platform volgens de eisen is ontworpen en geïmplementeerd voor hoge beschikbaarheid. Dit omvat bijvoorbeeld redundante voedingen, rekenkracht voor de verwerking en ventilatorconfiguratie waarbij het uitvallen van één ventilator niet het hele systeem doet uitvallen. Omdat deze maatregelen in de praktijk nog niet voldoende zijn om hardware-storingen te voorkomen, moet er de mogelijkheid zijn van redundant werking (high availability configuratie). Monitoring speelt hier ook een belangrijke rol, zodat defecte hardware tijdig kan worden gedetecteerd. In dit geval moet de fabrikant passende monitoring ondersteunen, zoals via SNMP. Aan de softwarekant is het om storingen te voorkomen cruciaal om speciale aandacht te besteden aan een correcte implementatie. De voorkeur moet worden gegeven aan fabrikanten die speciale inspanningen leveren bij de ontwikkeling in de vorm van codebeoordelingen. Het is nog steeds belangrijk om je te concentreren op bescherming

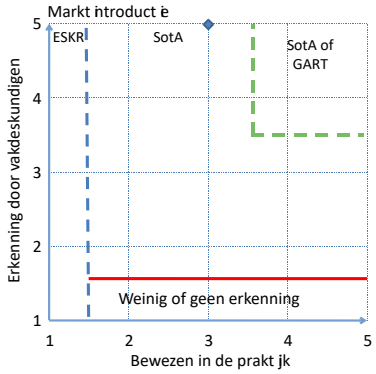
tegen Denial of Service-aanvallen. Een bijzonder veilig platform is natuurlijk ook hier een belangrijke vereiste, naast gecontroleerde toegang tot de gebieden waar de VPN-eindpunten (VPN-concentrators) in het LAN worden bediend.

Loggegevens worden verzameld op de apparaten van een layer 3 VPN. Dit is uiterst belangrijk om aanvallen op het netwerk te kunnen detecteren. Deze gegevens moeten hiervoor echter verplicht zijn. Evenzo is het belangrijk om beheer wijzigingen (admin of beheeracties) te kunnen volgen en dat deze loggegevens verplicht en dienovereenkomstig kunnen worden toegewezen. Dit betekent dat er mogelijkheden moeten zijn om dergelijke loggegevens te archiveren, zodat deze veilig zijn tegen manipulatie (tamper-proof). Dit kan bijvoorbeeld worden gegarandeerd door lokale append-only logs of door een interface te gebruiken naar externe logservers of SIEM-systemen.

Welke beschermingsdoelen vallen onder deze maatregel

☒ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



Opmerking: Hoewel er geen twijfel bestaat over de fundamentele noodzaak om VPN's te gebruiken, leveren fabrikanten regelmatig innovaties om hun niveau van beveiliging, gebruiksvriendelijkheid en bruikbaarheid te verhogen. De stand van de techniek voor VPN's wordt dus niet alleen bepaald door hun bestaan, maar ook door de vorm van deze kwaliteiten.

3.2.10 OSI layer 2 Versleuteling

Layer 2-versleuteling is een beveiliging-oplossingsalternatief voor layer 3 VPN's, die worden gebruikt op de payload van Ethernet-frames in plaats van op IP-pakketten. IP-headers hoeven niet te worden verwerkt (wat tijd bespaart) en de belasting van de lijncapaciteit als gevolg van de coderingsoverhead is veel lager dan versleuteling op laag 3 of hoger.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

Registratie en evaluatie van enorme hoeveelheden gegevens van site-verbindend verkeer via de backbone van het bedrijfsnetwerk of de cloudverbinding via beveiligingslacunes in netwerk-hardware, netwerkserviceproviders en niet-bewaakte ondergrondse of onderzeese kabels en draadloze- of satellietverbindingen, evenals DDoS-aanvallen op gecodeerde layer 3-verbindingen.

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

Versleuteling gebruiken om WAN-communicatie tussen bedrijfslocaties en datacenters te beveiligen. Het gebruik van bandbreedte-neutrale cryptografie-oplossingen met zeer weinig vertraging voor layer 2 WAN-backbones en directe links (zoals dark fiber en Satcom).

Layer 2 versleuteling is een beveiligingsoplossing die in bepaalde applicaties werkt als een geschikt alternatief voor layer 3 VPN's. Het wordt toegepast op de payload van Ethernet-frames in plaats van IP- op de pakketten. IP-headers hoeven niet te worden verwerkt (wat tijd bespaart) en er is geen versleutelingsoverhead (lijnbandbreedte is volledig beschikbaar). Voor het gebruik is een Ethernet-gebaseerd netwerk (point-to-point, hub-spoke of volledig meshed) via speciale kabels (koper/glasvezel) of een layer 2-service van netwerkproviders (zoals Carrier Ethernet-services) vereist.

Typische toepassingen voor layer 2-versleuteling zijn het beschermen van WAN-backbonelijnen (zelfs internationaal) en datacenterverbindingen binnen het bedrijfsnetwerk of met vertrouwde cloud- en collocatieproviders, evenals het beschermen van campus-backbonelijnen die buiten gebouwen en over eigendommen van derden lopen.

De prestatievoordelen zijn de moeite waard, vooral voor het gebruik van centrale IT-diensten, massale desktopvirtualisatie, datacenterconsolidatie en gedistribueerde en redundante opslagsystemen met een

hoog percentage IP-pakketten die klein of relevant zijn voor real time (zoals VoIP, IoT en Smart Grid), en waarvoor IPsec-overhead en vertraging onaanvaardbaar zijn.

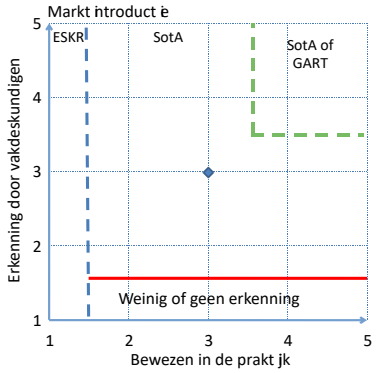
Voor het gebruik van deze netwerkversleutelingstechnologie hoeven bestaande IP-routeringsconfiguraties niet te worden gewijzigd. Dit type versleuteling is transparant voor vrijwel alle netwerkdiensten en toepassingen van OSI layers 3 en hoger en heeft geen meetbare impact op de netwerkprestaties.

Cryptostations op afstand en periodieke wijzigingen van cryptografische sleutels worden automatisch gesynchroniseerd en geverifieerd. Het genereren en distribueren van sleutels in layer 2-encryptieapparaten is gedecentraliseerd, waardoor sleutelservers als single points of failure worden vermeden en de netwerkbeschikbaarheid wordt verhoogd. BSI-goedgekeurde oplossingen zijn beschikbaar.

Welke beschermingsdoelen vallen onder deze maatregel

☒ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.11 Cloud-gebaseerde gegevensuitwisseling

Met de voortschrijdende digitalisering en geografisch verspreide manier van werken vinden zogenaamde op cloud gebaseerde (cloud based) bestand-uitwisselingsdiensten steeds meer toepassing in de IT-omgeving (zoals Dropbox, OneDrive en Google Drive).

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

De gegevens die zijn opgeslagen in een cloud gebaseerde exchange-service voor bestandsuitwisseling zijn onderhevig aan de volgende bedreigingen:

- Ongeautoriseerde toegang en inzage door de exploitant van de dienst
- Onbevoegde toegang en inspectie door derden tijdens verwerking of opslag
- Onbevoegde toegang en inzage door derden terwijl de gegevens via internet worden getransporteerd
- Diefstal of ongeoorloofd gebruik van de identiteit die is overeengekomen met de cloud-service

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

Om de opgeslagen gegevens te beschermen, zijn de volgende maatregelen nuttig:

1. Versleutelde overdracht van bestanden van en naar de bestand-uitwisselingsdienst
2. Versleuteling en pseudonimisering van gegevens die onafhankelijk zijn van de dienst voor bestandsuitwisseling door
   - Aan de client-zijde: end-to-end encryptie van gegevens voor de ontvanger voordat deze naar de cloudopslag worden verzonden (zoals door in de data-exchange-service geïntegreerde versleuteling in client software die bij de cloudopslag hoort of door afzonderlijke end-to-end encryptiesoftware op de client)
   - Gateway encryptie /pseudonimisering (zie hoofdstuk Gegevensopslag in de cloud)

Met name de volgende vragen moeten worden onderzocht:

1. Wie beheert de dienst en heeft de exploitant toegang tot de gegevens?
2. Hoe worden de gegevens beschermd tijdens de verwerking/bestandsopslag?
3. Hoe worden de gegevens beschermd tijdens het transport van en naar de exploitant?

Als de service wordt beheerd door een betrouwbare instantie, dan kan end-to-end versleuteling van de gegevens onder bepaalde omstandigheden worden afgeschaft, maar over het algemeen is het ook verstandig voor vertrouwde exploitanten

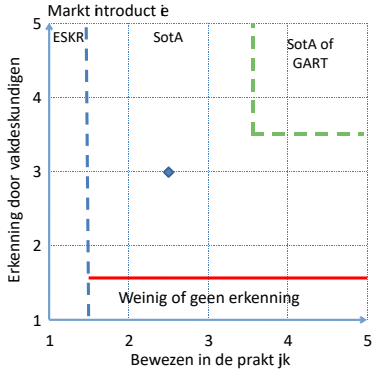
File-exchange diensten zijn beschikbaar waarbij gegevens transparant worden versleuteld voordat ze worden geüpload, dat wil zeggen zonder speciale actie van de gebruiker, en opnieuw worden gedecodeerd na het downloaden. De operator ziet dan alleen versleutelde data. Als alternatief kan client-side encryptiesoftware worden gebruikt, die zorgt voor end-to-end versleuteling van de gegevens nog vóór het uploaden of na het downloaden. Deze oplossingen vereisen echter meestal extra inspanningen van de kant van de gebruiker. Bij het versleutelen moet aandacht worden besteed aan het gebruik van veilige methoden voor versleuteling en aan het genereren en opslaan van sleutels.

In geen geval mag worden afgezien van de versleuteling van gegevens tijdens het transport van en naar de exploitant (transportversleuteling, in de huidige versie meestal TLS).

Welke beschermingsdoelen vallen onder deze maatregel

☐ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.12 Dataopslag in de cloud

Bij het gebruik van cloud-infrastructuren zijn beveiligingsstrategieën die alleen de eigen IT-infrastructuur beveiligen niet voldoende. In een wapenwedloop met aanvallers is de meest basale maatregel de veiligste: het versleutelen van gevoelige data. Om de verwerking van gegevens - waar gewenst - mogelijk te kunnen blijven maken, is een selectieve versleuteling van gegevens op basis van een gegevensclassificatie vereist.

Zodra gevoelige gegevens een veilige, interne omgeving verlaten om in de cloud te worden opgeslagen, moeten ze vóór verzending worden versleuteld. Versleuteling moet, om zelfs door externe beheerders ongeoorloofde toegang tot gegevens, te voorkomen, uitsluitend onder de controle van de gebruikersorganisatie blijven. Eén ding is duidelijk: wie de gegevens versleutelt, moet toegang hebben tot de onversleutelde gegevens. En dat zou alleen de gebruikersorganisatie moeten zijn. Een stand van de techniek oplossing moet daarom een passende, volledig intern gecontroleerde gegevensversleuteling mogelijk maken. Een interne verdeling van beheertaken voor het beheer van cryptografische sleutels naar meerdere personen maakt het nog moeilijker om gevoelige gegevens te compromitteren. Hier is de stand van de techniek de oplossingen die belangrijke functionaliteit zoals het zoeken of filteren van gegevens, rapportage of de geautomatiseerde verwerking van gecodeerde gegevens in cloud toepassingen niet beperken. Om een consistent hoog beveiligingsniveau voor alle cloud toepassingen mogelijk te maken, moet de oplossing ook geschikt zijn voor meerdere clouds, ofwel meerdere cloud providers ondersteunen.

Sinds het wegvallen van het Privacy Shield (Schrems II arrest) is bijzondere voorzichtigheid geboden bij het gebruik van clouddiensten die gegevens buiten Europa opslaan of verwerken.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

Gevoelige gegevens die in de cloud zijn opgeslagen of worden verwerkt, kunnen op vele manieren worden gecompromitteerd, waaronder

1. ongeautoriseerde toegang tot cloudopslag (door zowel externe als interne gebruikers);
2. toegang door externe beheerders van cloud providers of datacenters;
3. onderscheppen tijdens de overdracht tussen de organisatie en de cloud; en
4. diefstal van de cloudopslag.

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?
Een encryption-gateway is een proxy-gebaseerde oplossing die bemiddelt tussen eindgebruikersapplicaties en de cloud. Het versleutelt en pseudonimiseert alle gegevens dat een vooraf gedefinieerde beveiligde interne omgeving verlaat en decodeert informatie die door geautoriseerde eindgebruikers uit de cloud wordt opgevraagd. Bij een dergelijke oplossing moeten de cryptografische sleutels het exclusieve eigendom van de gebruikersorganisatie blijven. Evenzo moeten, om de gegevenssoevereiniteit te waarborgen en de autorisaties voor leestoegang centraal te beheren, versleuteling en decodering ook alleen door de gebruikersorganisatie kunnen worden gecontroleerd. Een dergelijke stand van de techniek oplossing moet daarom een volledig intern sleutelbeheer mogelijk maken, evenals de onafhankelijk van de cloud infrastructuur versleuteling/pseudonimisering van de gegevens. Intern moeten de belangrijkste beheertaken worden verdeeld over verschillende verantwoordelijke personen.

De eigen versleuteling/pseudonimisering van de organisatie maakt deze oplossing veiliger dan de native encryptieoplossingen van derde cloud providers (zoals bring-your-own key). In het laatste geval kan nooit helemaal worden uitgesloten dat derden (zoals databasebeheerders) leestoegang hebben tot gevoelige informatie. Met een encryption-gateway kunnen externe gegevensverwerkers nog steeds beheertaken uitvoeren, maar kunnen geen gevoelige gegevens meer lezen in platte tekst. De oplossing biedt ook bescherming bij gegevensdiefstal: zonder de cryptografische sleutels kunnen aanvallers niets doen met buitgemaakte, versleutelde gegevens.

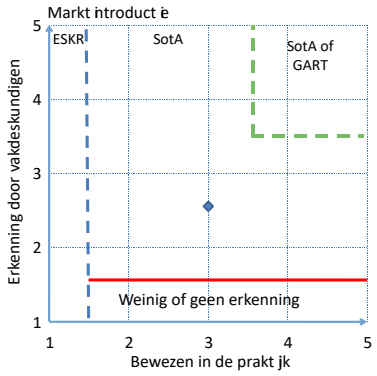
Het centrale criterium voor het gebruik van een encryption-gateway moet zijn dat beschermde gegevens nog steeds kunnen worden verwerkt. Dit kan worden bereikt door gedeeltelijke versleutelingsmethoden.

Met het oog op de toekomst moet een encryption-gateway worden gekozen waarmee de gebruikersorganisatie de gebruikte versleutelingsalgoritmen vrijelijk kan uitwisselen (Crypto Agility). Met de voortschrijdende ontwikkeling van extreem krachtige kwantumcomputers kunnen procedures die vandaag als veilig worden geclassificeerd, in de nabije toekomst verouderd raken. Daarom is een oplossing die al compatibel is met algoritmen van post-kwantum cryptografie (PQC) ideaal.

Welke beschermingsdoelen vallen onder deze maatregel

☐ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.13 Gebruik van mobiele spraak- en datadiensten

Mobiele gesprekken en gegevensoverdrachten zijn gemakkelijker te onderscheppen dan vaste telefonie. Versleuteling van mobiele spraak- en dataoverdracht beschermt hiertegen, net als het harden en configureren van apparaten.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?
Ondanks chat- en web-conference-toepassingen zijn de klassieke vaste en mobiele telefonie tegenwoordig ook een van de meest directe en persoonlijke vormen van communicatie. Het brengt echter verschillende risico's met zich mee en biedt potentiële aanvalsvectoren. De overgrote meerderheid van de telefoongesprekken vanaf vaste lijnen is ook mobiele telefonie betrokken.

- Het hacken van mobiele gesprekken en dataverkeer vanaf vaste lijnen die worden beheerd door mobiele en telefoonnetexploitanten, en waarvoor de basisstations met elkaar en met de vaste verbindingen zijn verbonden en zijn gebaseerd op internettechnologie, enz.
- Hacken van mobiele gesprekken en dataverkeer, en hun overdracht naar command & control aanval-servers via op de mobiele telefoon geïnstalleerde malware die kwetsbaarheden in het

besturingssysteem en apps exploiteert om directe toegang te krijgen tot de microfoon, luidsprekers en touchscreen/toetsenbord en scherm, en op die manier de versleutelingsapp verwijdert.

- Onversleutelde mobiele gesprekken en dataverkeer kunnen worden onderschept met behulp van goedkope hardware op de ether-interface. Aanvallers hoeven hiervoor de mobiele telefoon niet te infecteren of in te breken in het communicatienetwerk. Ze moeten zich echter wel in het ontvangstbereik van de betreffende mobiele telefoon bevinden. Aanvallers kunnen zich bijvoorbeeld voordoen als onderdeel van het mobiele netwerk om de mobiele telefoon op hun afluisterapparaat te registreren en vervolgens gesprekken en dataverkeer direct op te nemen en te analyseren.

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?
De vertrouwelijkheid van gesprekken kan worden gewaarborgd door gebruik te maken van spraak- en gegevensversleuteling op OSI layer 7 (in de communicatie-apps). Gesproken woord- en chatgegevens, samen met eventuele bestandsoverdrachten, worden real time op het apparaat versleuteld en vervolgens, wanneer ze de ontvanger bereiken, gedecodeerd en weergegeven.

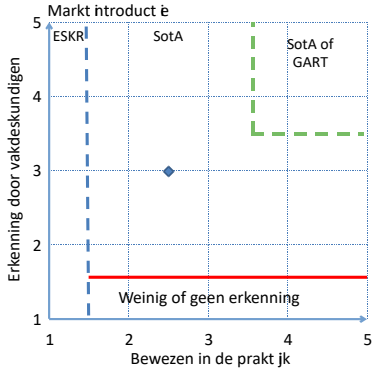
De volgende tegenmaatregelen worden aanbevolen:

- Versleuteling van spraak- en datacommunicatie via geschikte en vertrouwde apps of hardware die voldoen aan de huidige versleutelingsnormen en toepasselijke gegevensbeschermingsregels voor end-to-end versleuteling
- Bovendien centrale configuratie van eindapparatuur door de uitgevende organisatie of een die Bring Your Own Devices (BYOD) ondersteunt via mobile device management (MDM/EMM) - systemen om ongewenste gebruikersacties en app-activiteiten, die leiden tot infectie van mobiele telefoons, te voorkomen
- Voor hogere betrouwbaarheidsniveaus, het gebruik van mobiele telefoons met geharde operating systemen die ervoor zorgen dat microfoon en luidspreker alleen worden gebruikt door de versleutelingsapp en voorkomen dat bestaande malware de coderingssleutel hackt.

Welke beschermingsdoelen vallen onder deze maatregel

☐ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.14 communicatie via Instant Messenger

Instant messaging is de term voor een vorm van digitale communicatie waarbij twee of meer partijen met elkaar converseren door middel van snel verzonden tekst-, beeld- en spraakberichten. De partijen gebruiken hiervoor een gemeenschappelijke Instant Messenger voor het verzenden van de berichten via een netwerk. Als een partij niet online is op het moment dat een bericht wordt verzonden, wordt het over het algemeen op een later tijdstip bij de ontvanger afgeleverd. Secure Instant Messaging probeert chatberichten te beschermen tegen ongeautoriseerde toegang en wijziging.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?
Wanneer informatie wordt uitgewisseld via instant messaging, moet rekening gehouden worden met de volgende bedreigingen:

1. Registreren, analyseren en wijzigen van de inhoud door een onbevoegde derde partij

(man-in-the-middle aanval)
2. Identiteitsdiefstal binnen een communicatiesysteem
3. Diefstal van apparatuur met het oog op het vervolgens zonder toestemming analyseren van instant messaging-gegevens.

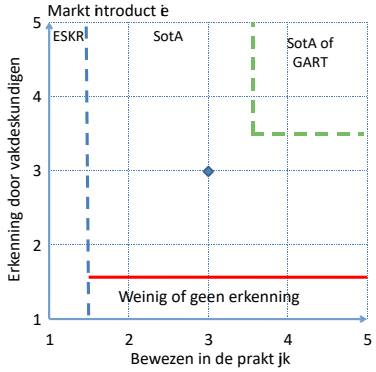
Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

1. Secure Instant Messaging bevat technische beveiligingsmaatregelen om de vertrouwelijkheid en integriteit van de inhoud van communicatie-te behouden:
   - Beveiliging voor berichtoverdracht tijdens het transport met behulp van de nieuwste TLS
   - Gebruik van asymmetrische end-to-end versleuteling met beveiliging dit ten minste vergelijkbaar is met RSA 2048 bit
   - Forward Secrecy moet ook deel uitmaken van de architectuur om de gegevens te beschermen tegen daaropvolgende decodering, ondanks het feit dat ze de lange termijn sleutel hebben.
2. Betrouwbare verificatie/authenticatie van identiteiten
3. Beveiliging van toegangsopties en paden naar inhoud:
   - Schermenvergrendeling op het gebruikte mobiele apparaat (sterk wachtwoord)
   - Geactiveerde apparaat-versleuteling
   - De gebruikte communicatie-app moet onafhankelijke veilige gegevensopslag en bescherming bieden tegen extractie door onbevoegden.

Welke beschermingsdoelen vallen onder deze maatregel

☐ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.15 Beheer van mobiele apparaten

Het gebruik van Mobile Device Management (MDM)-oplossingen reduceert de beveiligingsrisico's die ontstaan door ongecontroleerd gebruik van mobiele apparaten voor zakelijke doeleinden. MDM-oplossingen maken het mogelijk om het beheer en de configuratie van de gebruikte mobiele apparaten te centraliseren.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

1. Gegevensverlies: Als belangrijke gegevens op de mobiele apparaten worden opgeslagen en zo'n apparaat verloren of vernietigd wordt, zal de organisatie moeten accepteren dat deze gegevens in sommige situaties onherroepelijk verloren gaan.
2. Diefstal: Als een mobiel apparaat wordt gestolen, heeft de dief mogelijk toegang tot vertrouwelijke bedrijfsgegevens.
3. Malware: Door openbare WLAN-netwerken te gebruiken, niet installeren van beschikbare updates en het niet controleren van de installatie van applicaties van sommige dubieuze bronnen, raken mobiele apparaten vaak besmet met malware.

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

Met MDM-oplossingen (Mobile Device Management) kunnen beheerders het gebruik van en de toegang tot mobiele apparaten die voor zakelijke doeleinden worden gebruikt, op verschillende manieren en volgens vooraf gedefinieerde beveiligingsrichtlijnen beheren. MDM-oplossingen kunnen de patchstatus van het mobiele apparaat bepalen en gecontroleerd updates installeren zodra ze beschikbaar zijn. Bovendien kunnen adequate wachtwoordbeveiliging, reguliere back-up en apparaat-versleuteling allemaal centraal worden afgedwongen. In geval van diefstal of verlies van het apparaat kan het met geweld worden geschoond (Remote Wipe) om de

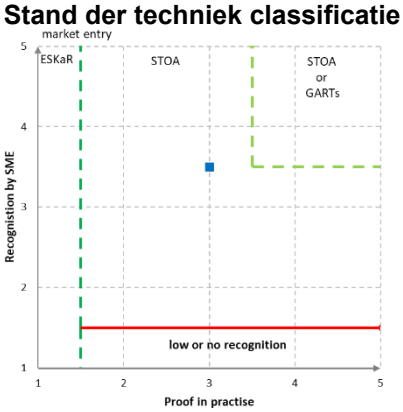
vertrouwelijkheid van bedrijfsgegevens te beschermen. De beheerder kan de gebruikersrechten voor het mobiele apparaat zodanig instellen dat toepassingen van willekeurige en potentieel onveilige bronnen niet kunnen worden geïnstalleerd.

Om te voldoen aan de hogere functionaliteitsvereisten voor het, voor zakelijke doeleinden, gebruik van mobiele apparaten, hebben sommige fabrikanten de huidige MDM-functies uitgebreid met Mobile Application Management (MAM) en Mobile Information Management (MIM) functies, waaronder cloudverbinding met Enterprise Mobility Management (EMM) oplossingen.

Welke beschermingsdoelen vallen onder deze maatregel

☒ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☐ Authenticiteit

Stand der techniek classificatie



3.2.16 Routerbeveiliging

Routers zijn centrale infrastructuurcomponenten die de uitwisseling van netwerkpakketten tussen meerdere netwerken/computers mogelijk maken.

In de business to business -sector (B2B) worden routers niet alleen gebruikt als apparaten voor internettoegang of voor het routeren van gegevens. In de meeste gevallen zetten ze ook VPN-netwerken op. Naarmate de telefonie-infrastructuur is gemigreerd (waarbij ISDN/analoge technologie is vervangen door IP-technologie), zijn routers gebruikt als ISDN-IP-gateways, zodat ISDN-systemen die nog steeds aanwezig zijn, nog steeds kunnen worden gebruikt in IP-netwerken. Beide toepassingen maken de router een cruciaal onderdeel voor een organisatie, met specifieke beveiligingsvereisten.

Vanwege de wereldwijde prevalentie in zowel bedrijfs-, organisatie- als particuliere netwerken, is de router een doelwit voor verschillende soorten aanvallen die moeten worden voorkomen door adequate beschermingsmaatregelen. In dit gedeelte worden de bedreigingen voor routers en de huidige beveiligingsmaatregelen beschreven en beoordeeld.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

Routers zijn bedoeld om gegevens betrouwbaar en veilig om te leiden en tegelijkertijd te beschermen tegen ongeoorloofde toegang. De volgende bedreigingen/risico's kunnen deze doelstellingen in gevaar brengen:

1. configuratiemanipulatie;
2. aanvallen waarbij gebruik wordt gemaakt van bekende gaten in de beveiliging en aanvallen op niet gedichte gaten in de beveiliging;
3. aanvallen met nieuw ontdekte beveiligingslekken (zero-day exploits);
4. aanvallen via IP-telefonieverbindingen;
5. diefstal (vooral outdoor/mobiele communicatierouters);
6. beschikbaarheidsaanvallen (DoS-aanvallen);
7. toegang via niet-gedocumenteerde interfaces (zie backdoors);
8. code van derden uitvoeren en integratie in botnets;
9. aanvallen via onvoldoende beveiligde WLAN's.

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

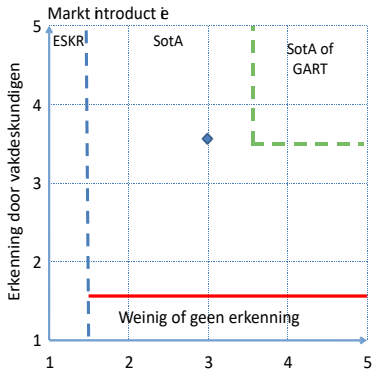
Er zijn meerdere beveiligingsmaatregelen om het risico van de bovenstaande bedreigingen te minimaliseren, die hieronder kunnen worden samengevat als een pakket van routerbeveiligingsmaatregelen:

1. Wachtwoordbeveiliging: het gebruik van beveiligde toegangsgegevens die zijn beveiligd tegen toegang door derden en het vermijden van het gebruik van standaardaanmeldingen
2. Regelmatige firmware-updates van de router
3. Servicecontracten met de fabrikant en een vastgestelde maximale responstijd in het geval dat een ernstige lacune bekend wordt.
4. Als een routerfabrikant geen updates verstrekt nadat hij zich bewust is geworden van een beveiligingslek, is het noodzakelijk om alternatieve apparaten van andere fabrikanten te gebruiken die niet door het lek worden beïnvloed.
5. De router moet op een beveiligde locatie worden opgesteld, bijvoorbeeld een afsluitbare ruimte met toegang die door verantwoordelijke beheerders wordt bewaakt. Het is zelden mogelijk om een router buiten op te stellen op een locatie met beveiligde toegang. De router moet daarom worden uitgerust met een GPS-functie. De router moet zo worden geconfigureerd dat deze na bijvoorbeeld een stroomstoring wordt gecontroleerd om er zeker van te zijn dat deze zich nog steeds op locatie bevindt. Als dit niet het geval is, moet de werking ervan worden verstoord.
6. Er moeten filters zijn voor ongeldige adressen volgens RFC 2267 en in de firewall moeten blacklists worden ingesteld ter bescherming tegen DoS-aanvallen.
7. Alle poorten en interfaces die open of niet nodig zijn, moeten worden gesloten.
8. Indien mogelijk moet de router automatisch worden gedeactiveerd tijdens inactiviteit (bijvoorbeeld 's nachts) om het blootstellingsvenster te verminderen. Deze maatregel mag de installatie van updates niet beperken.
9. Er moeten verschillende netwerkzones worden ingesteld om de impact van succesvolle aanvallen op routers tot een minimum te beperken (netwerksegmentatie).
10. WLAN-routers: geen open netwerken of alleen voor toegang voor gasten (directe uitgaande lijn), gebruik anders de hoogste coderingsstandaarden
11. VPN-routers: Maak geen VPN-verbindingen via vooraf gedeelde sleutels, maar waar mogelijk op basis van een certificaat
12. Router als all-IP/ISDN-gateway: gebruik apparaten met geïntegreerde session border controllers. Firewalls zijn niet in staat om Session Initiation Protocol (SIP) gebaseerde spraakpakketten te verwerken, wat resulteert in het risico van een aanval via voice-over-IP-verbindingen. De werking van de router moet centraal worden bewaakt.

Welke beschermingsdoelen vallen onder deze maatregel

☒ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.17 Netwerkbewaking met behulp van IDS (inbraakdetectiesysteem)

Een inbraakdetectiesysteem (IDS) of inbraakpreventiesysteem (IPS) identificeert en registreert afwijkingen in het IT-netwerk. Het doel van beide systemen is om inbraak en de verspreiding van malware te detecteren voordat er schade optreedt, indien mogelijk. In tegenstelling tot IDS, dat alleen informatie van afwijkend gedrag rapporteert en alarmen genereert, kan een IPS ook automatisch ingrijpen. Dit moet voorkomen dat malware zich verder door het netwerk verspreidt. Opgemerkt moet worden dat directe interventie door een IPS een directe impact kan hebben op de beschikbaarheid in onder andere industriële en productiesystemen, of volledig geautomatiseerde bestel-/leveringsprocessen en rapportage- en beveiligingsprocessen (inclusief brandveiligheid)

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

1. Informatielekken door onderschepping van gevoelige gegevens
2. Misbruik van diensten en communicatieprotocollen
3. Toegang van het IT-systeem van derden tot het IT-netwerk
4. Benutting van de mogelijkheden om toegang te krijgen tot gekoppelde IT-systemen
5. Manipulatie van informatie of software
6. Verspreiding van malware in het IT-netwerk

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?
Er is een onderscheid tussen netwerk gebaseerde en host gebaseerde IDS/IPS. Netwerk gebaseerde IDS/IPS maakt gebruik van interne componenten en/of de netwerkinfrastructuur om de communicatie te bewaken. Host-gebaseerde IDS en IPS gebruiken informatie uit IT-systemen (via software agents, logfile analyses, enz.). In een gedistribueerde systeemarchitectuur moeten de gegevens worden versleuteld en ondertekend voor uitwisseling of opslag.

Detectie is gebaseerd op twee verschillende methoden. Pattern matching identificeert bekende malware op basis van patronen (handtekeningen). Nieuwe aanvalspatronen moeten zo snel mogelijk worden geanalyseerd en hun handtekeningen moeten onmiddellijk worden bijgewerkt als veilig tegen manipulatie, omdat anders aanvallen op basis van deze patronen onopgemerkt blijven.

De tweede methode is gebaseerd op het detecteren van veranderingen in de communicatiepatronen van netwerkbedrijven veroorzaakt door een aanval. Alle communicatie buiten het verwachte dataverkeersprofiel wordt beoordeeld als een anomalie. Hierdoor kunnen ook nieuwe aanvallen worden gedetecteerd. Het is niet nodig om aanvalspatronen in een database te onderhouden. De communicatiepatronen die deel uitmaken van het normale dataverkeer moeten echter worden gedefinieerd.

Als malware wordt gedetecteerd of als er afwijkingen zijn van de geldige nominale communicatievoorwaarde, moet een IDS automatisch relevante incidentrapporten genereren. Alle incidentmeldingen moeten lang genoeg in het systeem worden bewaard om ze te analyseren en indien nodig in een open of gestandaardiseerd formaat kunnen worden geëxporteerd.

Incidentmeldingen moeten alle relevante informatie bevatten voor incidentanalyse en om tegenmaatregelen, zoals een erkende handtekening of een afwijkende communicatieverbinding, te nemen. Alarmberichten moeten zichtbaar zijn op de beheerconsole, als e-mail worden verzonden naar opgegeven accounts en via een exportinterface beschikbaar zijn op een algemeen alarmsysteem (zie SIEM).

Een IPS moet ook zelfstandig alle communicatie in het netwerk waarop een aanvalspoging is gebaseerd. Er moet voor worden gezorgd dat zoveel mogelijk geen communicatie, die niet duidelijk aan aanvalsgedrag kan worden toegeschreven, wordt voorkomen.

Een IDS/IPS moet componenten leveren voor het analyseren van alle communicatie met gateways en/of binnen IT-systemen (hosts) die na een tijdelijke storing voor een stabiele werking automatisch opnieuw synchroniseren.

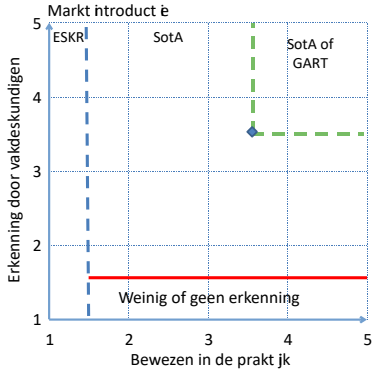
Ongewenste communicatie van IDS/IPS-componenten met derden kan niet worden toegestaan. Bovendien mogen alle IDS- en IPS-componenten niet identificeerbaar zijn, mogen ze geen invloed hebben op het dataverkeer of diensten aanbieden en moeten ze zelf worden beschermd.

Naast handtekening- en sleutellengtes voor gebruikte certificaten, moeten volgens de huidige aanbevelingen van de BSI symmetrische en asymmetrische algoritmen worden gebruikt.

Welke beschermingsdoelen vallen onder deze maatregel

☒ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.18 Bescherming van webverkeer

Webservers zijn een van de belangrijkste manieren om malware te verspreiden. In de meeste gevallen zijn gebruikers zich niet bewust wanneer geïnfecteerde websites malware op het systeem laden en uitvoeren. Als dataverkeer tijdens het surfen door een webfilter wordt geleid, kunnen deze aanvallen worden gedetecteerd en geblokkeerd.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

Webservers zijn een van de belangrijkste manieren om malware te verspreiden. Vaak worden geïnfecteerde webservers gebruikt waarbij de exploitant niet direct betrokken is bij de aanval. Een groot percentage van de webservers heeft permanente beveiligingsgaten waardoor ze kunnen worden aangevallen door hackers en die vervolgens malware op het systeem opslaan, meestal zogenaamde rootkits.

Deze websites worden normaal gesproken beheerd door de gebruiker. Bij het bezoeken van een geïnfecteerde website wordt de malware geladen en op het lokale systeem geactiveerd zonder opgemerkt te worden door de gebruiker (drive-by-downloads).

Aanvallers gebruiken ook speciaal daarvoor ingerichte webservers die vaak een andere website imiteren. In het geval van phishing, worden deze valse kopieën van bekende websites ingezet met het doel om gevoelige informatie van de gebruiker, meestal gebruikersnamen en wachtwoorden, naast bankgegevens, creditcardgegevens, adressen, enz., af te tappen.

Het werkelijke bestemmingsadres (URL met kwaadaardige code of de URL van een geïnfecteerde of valse webpagina) wordt vaak vermomd door automatische omleiding (redirecting) en vaak door URL-shorteners (zoals bit.ly en TinyURL), hoewel deze niet direct betrokken zijn bij de daadwerkelijke aanval. Gebruikers worden via links die in e-mails, op sociale media, enz. worden geplaatst, naar speciale websites doorgeleid.

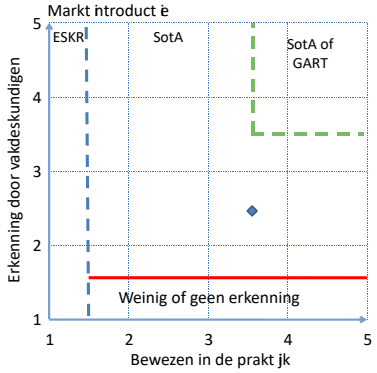
Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

Web dataverkeer wordt door web filters geleid tegen om dit soort aanvallen te beschermen. Web filters beschermen tegen deze aanvallen door de betreffende websites te blokkeren en de gegevens die door websites worden geladen te analyseren op kwaadaardige code. Web filters kunnen centraal worden gebruikt als web filters in de cloud of als on-premise applicaties, of als software die wordt gebruikt op het systeem van de eindgebruiker.

Welke beschermingsdoelen vallen onder deze maatregel

☒ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.19 Bescherming van webapplicaties

Een Web Application Firewall (WAF) beschermt webapplicaties (homepages, online winkels, thuisbankieren portals, enz.) tegen aanvallen. De WAF inspecteert de communicatie tussen gebruikers en webapplicaties op applicatieniveau en blokkeert potentieel schadelijk dataverkeer, zoals SQL-injecties en cross-site scripting. De term Web Service Firewall (WSF) wordt ook veel gebruikt voor machine-to-machine communicatie.

In tegenstelling tot een netwerkfirewall, die werkt op OSI-lagen 3 en 4, behandelen WAF's OSI layer 7 - gegevensverkeer en beschermen ze dus tegen bedreigingen die zich richten op de exploitatie van beveiligingskwetsbaarheden in de applicaties.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?
Aanvallen op webapplicaties of webservice-interfaces, zoals

- SQL-injectie;
- cross-site scripting (XSS);
- lekken van informatie;
- command-injection;
- andere OWASP-bedreigingen.

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?
Met behulp van een Web Application Firewall (WAF) of Web Service Firewall (WSF) die nog vóór de webserver (upstream) actief is.

Een Web Application Firewall (WAF) beschermt webapplicaties (homepages, online winkels, thuisbankier portals, enz.) tegen aanvallen. De WAF analyseert de communicatie tussen gebruikers en webapplicaties op applicatieniveau en blokkeert potentieel schadelijk dataverkeer. In de meeste gevallen volstaat het aanpassen van de WAF voor gaten in de beveiliging van webapplicaties die op korte termijn moeten worden gedicht. Het aanpassen of patchen van de te beveiligen webapplicatie kan vervolgens achteraf worden gepland en met voldoende kennisgeving voor tests worden uitgevoerd. Vaak wordt een combinatie van verschillende kwetsbaarheden misbruikt voor aanvallen. Het blokkeren van één centrale kwetsbaarheid per WAF kan dus snel veel aanvallen afweren.

De Web Services Firewall (WSF) is een speciaal geval van de WAF voor machine-to-machine communicatie en wordt ook via http/https verwerkt. De aanvalsvectoren voor WAF en WSF lijken erg op elkaar. Voor zowel de WSF als de WAF geldt het volgende.

Moderne webapplicaties en -services bieden vaak een programmeerinterface (API) die een breed scala aan functies biedt voor flexibel machinegebruik, wat echter zelden de beste vorm van bescherming is.

De WAF beëindigt versleuteld dataverkeer aan de gebruikerszijde, analyseert de inhoud en leidt deze om naar de webserver als versleutelde verzoeken die als onschadelijk worden geclassificeerd. Schadelijke verzoeken worden geblokkeerd.

Het bedienen van webapplicaties zonder gebruik te maken van een appliance of virtuele upstream WAF kan niet langer worden beschouwd als stand van de techniek.

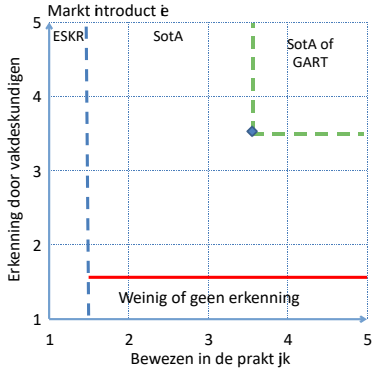
Een WAF moet de volgende kenmerken hebben:

- loggegevensoverdracht naar SIEM- en anomalie detectiesystemen met de optie om wachtwoordwoorden, creditcardgegevens, enz. te verbergen;
- clustering mogelijkheden voor hoge beschikbaarheid en belastingverdeling (load-balancing);
- bescherming tegen OWASP top 10 aanvallers, zoals SQL injection, cross-site scripting (XSS) en directory traversal door middel van blacklisting, whitelisting en patroonherkenning;
- sterke authenticatie van gebruikers van webapplicaties en diensten;
- sessiebeheer, d.w.z. inspectie en manipulatiebescherming van sessiecookies;
- Broken Access Control voorkomt ongeautoriseerde toegang tot paden (path traversal), bestanden en API-functies;
- filters voor onnodige http-headers;
- bescherming tegen cross-site request forgery (CSRF) door header evaluatie van http-requests, zoals referrer informatie.

Welke beschermingsdoelen vallen onder deze maatregel

☒ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.20 Externe netwerktoegang/onderhoud op afstand

Externe netwerken moeten voor onderhoud of software-updates bereikbaar zijn via het internet.

In een industriële omgeving zijn deze deelnemers machinebesturingscomponenten zoals PLC, aandrijfeenheden en bedieningspanelen. In het geval van onderhoud of een software-update moet de externe gebruiker online toegang krijgen tot deze systemen met de tools van de fabrikant (zoals PLC-programmeersoftware).

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

- Ongeautoriseerde toegang tot het bedrijfsnetwerk
- Ongeautoriseerde toegang tot doelsystemen
- Toegang op afstand kan niet worden getraceerd
- Tappen of blootstellen van data tijdens een onderhoudssessie op afstand

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

Om onderhoud op afstand mogelijk te maken zijn de doelsystemen meestal via routers met internet verbonden. Ze gebruiken dit vervolgens om een VPN-verbinding tot stand te brengen met wat een intermediate (tussenliggende) server wordt genoemd. Dit tussenliggende punt is de link tussen het doelsysteem en de externe gebruiker, die eveneens een VPN-verbinding met de intermediate server tot stand heeft gebracht. Omdat beide locaties hun eigen verbinding hebben, kan elke deelnemer deze op elk moment beëindigen. In dit proces is de taak van de intermediate server om alleen de goedgekeurde doelsystemen voor de respectieve externe gebruiker toe te staan. Idealiter kan dit worden beperkt tot externe gebruikers en doelsystemen tot laag 3 (IP, poort, protocol). Dit garandeert de aansluiting voor de specifieke toepassing op het doelsysteem. Afhankelijk van de toepassing kunnen door middel van onderhoud op afstand ook zuivere terminalverbindingen tot stand worden gebracht. Denk hierbij bijvoorbeeld aan web-, RDP-, VNC- en SSH-toegang. Dit is afhankelijk van de beschikbaarheid van het doelsysteem. Met name een directe 1:1-netwerkkoppeling van de externe gebruiker naar het doelsysteem-netwerk moet echter worden vermeden.

Versleutelde VPN-verbindingen garanderen gegevensintegriteit en bescherming tegen het

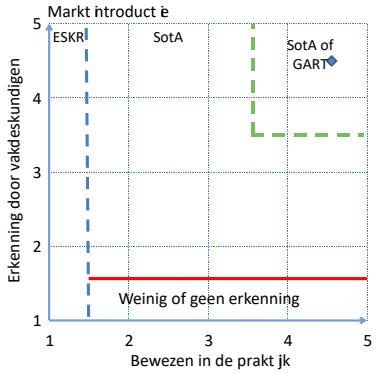
aftappen van gegevens. T2-Factorauthenticatie moet beschikbaar zijn voor autorisatie van de externe gebruiker.

Elke remote onderhoudssessie moet worden geregistreerd. Dit is nodig om de meest recente toegang tot het netwerk of de router te identificeren in het geval van een beveiligingsincident. Als dit gebeurt, moeten de identiteit van de externe gebruiker (IP-adres en naam), de tijd en de duur van de verbinding worden geregistreerd. Dit wordt idealiter opgeslagen op de intermediate server.

Welke beschermingsdoelen vallen onder deze maatregel

☐ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.21 Harden van servers

Aangezien serversystemen de essentiële (vaak gevoelige) gegevens en persoonsgegevens van de organisatie verwerken en opslaan, moeten de gebruikte systemen speciaal worden beschermd. Server hardening is een zeer effectieve beveiligingsmaatregel. Het beschermt het besturingssysteem, ongeacht of het een fysieke, virtuele of cloud gebaseerde server is.

Gangbare server besturingssystemen zoals Microsoft Windows Server en verschillende Linux Server-systemen hebben standaard geen zeer beperkende beveiligingsconfiguratie en zijn mogelijk uitgerust met onnodige componenten. Vaak worden deze ongebruikte en niet-geconfigureerde functionaliteiten door aanvallers gebruikt om het besturingssysteem te compromitteren.

Door server hardening worden deze functies en hun interfaces uitgeschakeld of strikter geconfigureerd, wat het beveiligingsniveau van de serversystemen aanzienlijk verhoogt. Daarom moet het harden van servers een integraal onderdeel zijn van de technische beveiligingsstrategie van de organisatie.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?
De belangrijkste bedreigingen van niet-geharde serversystemen zijn:

- Gegevensmanipulatie van persoonsgegevens en gevoelige bedrijfsgegevens
- Gegevensverlies (zoals volledige databasesystemen)
- Manipulatie van applicaties of aangesloten systemen
- Manipulatie, sabotage of spionage van operationele en productieprocessen
- Identiteitsdiefstal (zoals aanvallen op domeincontrollers)
- Malware van welke aard dan ook opslaan en malware verspreiden naar andere systemen
- Misbruik van servercapaciteit voor tot nut van aanvaller (zoals crypto-mining)
- Misbruik van servers voor laterale beweging (host jumping) om andere systemen aan te vallen

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?
Om serversystemen te harden, moeten met name de volgende maatregelen worden geïmplementeerd:

1. Deactiveren van componenten
    - Periodieke verificatie of actieve diensten noodzakelijk zijn voor de werking
    - Deactiveren of de-installatie van onnodige componenten/-services, inclusief achtergrondservices van het besturingssysteem
    - Deactiveren van onnodige opstart- en tijd-gecontroleerde processen
    - Deactiveren van onnodige, technisch verouderde en onveilige interfaces of protocollen
    - Deactiveren van het kunnen overdragen van telemetriegegevens, tenzij deze

volgens een centraal beleid nodig zijn voor centrale monitoring
    - Deactiveren van onnodige bestandsshares
    - Deactiveren of beperking van de toegang tot beheer-websites

2. Activering van hardware-gerelateerde beveiligingsfuncties
    - Activering van CPU-beveiligingsfuncties en testen van de juiste werking van toepassingen (zoals Address Space Layout Randomization (ASLR) en Data Execution Prevention (DEP))
    - Activering van een BIOS-wachtwoord, beperking van de opstartvolgorde tot noodzakelijke apparaten
    - Indien van toepassing, activering van bescherming tegen zijkanalen (side-channel) aanvallen
    - Indien van toepassing, activering van procedures voor veilig opstarten

3. Beveiligingsconfiguraties
    - Gebruik van beveiligde communicatieprotocollen om ervoor te zorgen dat gevoelige gegevens en authenticatie-informatie versleuteld worden verzonden
    - Gebruik van certificaten voor de uitwisseling van cryptografische sleutels
    - Deactivering van auto-start mechanismen (zoals voor USB-media)
    - Activering van een screensaver met wachtwoordbeveiliging
    - Activering van sterke gebruikersaccount-controle (user account control)
    - Activering van antivirusbescherming op het systeem al tijdens het opstartproces
    - Verwijderen van onnodige certificaten uit trust-stores
    - Het voorkomen van het lekken van informatie met betrekking tot geïnstalleerde services en versienummers
    - Uitschakelen van fout- en foutopsporingsberichten voor eindgebruikers of deze vervangen door neutrale foutmeldingen
    - Diensten uitvoeren met minimale rechten en een servicegebruiker, processen indien mogelijk uitvoeren in een geïsoleerde omgeving
    - Activeer logging

4. Minimale toewijzing van machtigingen (need-to-know-en least-privilege-principes)
    - Regelmatige controle van toegewezen toegangsrechten
    - Minimale rechten toekennen voor beheeractiviteiten
    - Minimale rechten toekennen voor bestandssysteem en externe data-interfaces
    - Minimale rechten toekennen voor onderhoudsinterfaces/toegang
    - Beperk de toegang tot configuratiebestanden van het besturingssysteem, beperk de toegang tot fysieke servers (vooral om te voorkomen dat ongeautoriseerde externe schijfstations worden aangesloten)

5. Accounts en wachtwoorden
    - Gebruik sterke wachtwoorden en mechanismen (juiste wachtwoordlengte, complexiteit, accountvergrendeling, wijzigingsinterval, enz.), hergebruik wachtwoorden niet voor andere toepassingen of gebruik geen 2-factor authenticatie (zie Paragraaf 3.2.1 e.v.)
    - Bescherm alle accounts met een wachtwoord conform het wachtwoordbeleid
    - Vervang alle bestaande standaardwachtwoorden conform het wachtwoordbeleid door eigen wachtwoorden
    - Vergrendel lokaal beheerder (Local admin) account na meerdere onjuiste pogingen
    - Gebruik van persoonsgebonden beheerdersaccounts (admin) voor beheeractiviteiten
    - Deactiveer of hernoem de standaardgebruikersaccounts
    - Deactiveer lokale gastaccounts
    - Gebruik non-privileged serviceaccounts (accounts met beperkte rechten) om processen uit te voeren
    - Deactiveer de remote login via netwerken) van lokale gebruikers (local guest) accounts
    - Deactiveer standaard-, test- en anonieme accounts voor alle geïnstalleerde **services/softwarecomponenten**

6. Netwerkcomponenten
    - Stel netwerkbeperkingen in (bijvoorbeeld TCP/IP-configuratie), schakel ongebruikte netwerkprotocollen uit of verwijder ze
    - Beperk verbindingen met services tot een minimum
    - Activeer indien van toepassing pakketfilters/firewalls om de communicatie te beperken tot de minimaal vereiste toegang

Voor veelgebruikte server besturingssystemen zijn meer gedetailleerde hardening-richtlijnen publiekelijk beschikbaar:

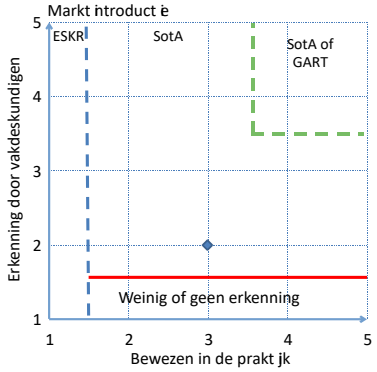
- Security Technical Implementation Guides (STIG's): **https://iase.disa.mil/stigs**
- CIS Benchmarks (Center for Internet Security Inc.): **https://www.cisecurity.org/cis-benchmarks**
- Microsoft-beveiligingsrichtlijnen: **https://blogs.technet.microsoft.com/secguide/**

De meeste hardening-maatregelen kunnen worden gerealiseerd door technische aanpassingen. Deze instellingen kunnen met een hardening-pakket (zoals hardening scripts) geautomatiseerd worden gedistribueerd naar alle serversystemen van de organisatie. Nieuwe serversystemen moeten onmiddellijk na installatie met het betreffende pakket worden gehard. Bij het harden van bestaande systemen kan hardening leiden tot functionele storingen, zodat een back-up gemaakt moet worden en de geharde serversystemen uitgebreid moeten worden getest.

Welke beschermingsdoelen vallen onder deze maatregel

☒ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.22 Eindpuntdetectie en -respons platform (EDR)

De bescherming van eindapparaten (bijvoorbeeld pc's, laptops, smartphones of tablets) vereist nu veel meer dan alleen een antivirusprogramma. Moderne oplossingen (Endpoint Detection & Response Platforms, EDR) combineren de nieuwste beveiligingstechnologieën om alle soorten cyberaanvallen op client- en serversystemen in verschillende besturingssystemen te stoppen en de initiators te identificeren. In tegenstelling tot conventionele oplossingen is hiervoor geen specifieke voorkennis, zoals handtekeningen of een eerste slachtoffer, vereist.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

- Malware
- Exploitatie
- Kwaadaardige scripts
- Hacker activiteiten
- Misbruik van beheertools en tools met kwade bedoelingen

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

EDR-platforms combineren effectieve detectie- en preventietechnieken om het compromitteren van clients en servers ook over computers en besturingssystemen heen te voorkomen en zelfs actieve aanvallers in computernetwerken bloot te stellen.

Lichtgewicht agents leveren de aanvalsrelevante procestelemetriegegevens, gebruiken lokaal effectieve machine learning-modellen (kunstmatige intelligentie) en correleren en visualiseren wijze tactieken, technieken en procedures op holistische.

Dankzij state-of-the-art sensorarchitectuur gebruiken Next Generation EPP-oplossingen slechts tot een

fractie van de computercapaciteit vergeleken met een klassieke AV-scanner en zijn regelmatige downloads van handtekeningen niet langer nodig. Dit betekent

- signatuur loze detectie en actieve blokkering van kwaadaardige code door machine learning modellen (bij voorkeur lokale runtime);
- controle en registratie van programma-activiteit in procesketens en optioneel het blokkeren van kwaadaardig gedrag;
- bescherming tegen misbruik van kwetsbaarheden in legitieme applicaties (exploits en geheugenmanipulatie);
- idealiter worden detecties gecorreleerd en worden de techniek en tactieken weergegeven (inclusief gebruikte tools zoals malware, Trojaanse paarden, PowerShell scripting en het doelwit van de aanvaller (exfiltratie van gegevens, het opzetten van een backdoor, zijwaartse (crossside) beweging binnen de organisatie, escalatie van rechten, enz.);
- aanvullende dreigingsinformatie laat zien wie de vermoedelijke actor/vijand is (cybercriminaliteit of nationaal gemotiveerde aanval) en welke doelen en industrieën de aanvallers aanvallen;
- Een volledig geïntegreerde sandbox-verbinding maakt het veilig onschadelijk maken van gevonden kwaadaardige code mogelijk voor verdere analyse zonder de productie in gevaar te brengen.

EDR-platforms behandelen de volledige levenscyclus van een aanvalspoging. Dit is de enige manier om conclusies te trekken over de actoren en hun motivatie, die idealiter contextueel zijn aangevuld met actuele dreigingsinformatie. Bovendien kunnen systeem-telemetriegegevens door externe deskundigen worden gecontroleerd op schadelijk bewijs.

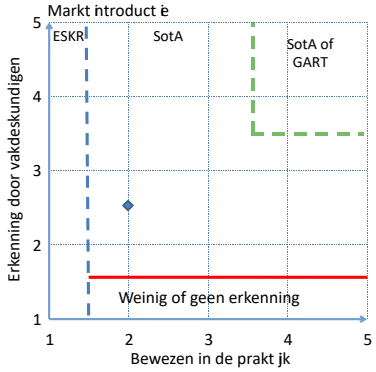
Bovendien moet hieraan worden toegevoegd dat voor een holistische bescherming van eindapparaten met name de volgende punten in aanmerking moeten worden genomen als deze aspecten niet door de respectieve EDR-oplossing zelf worden geboden:

- Autorisaties/rollen (trefwoord: beheerautorisaties)
- Update mechanismen (besturingssysteem en software)
- Beperkingen/controle van de geïnstalleerde software
- Versleuteling van eindapparaten
- Bescherming tegen zoals hierboven beschreven bedreigingen/malware
- Voorschriften/richtlijnen voor toegestaan gebruik (privégebruik, gebruik in externe netwerken, reizen, gebruik van gegevensdragers, opslag van gegevens, back-up enz.); in het bijzonder als de gebruiker beheerrechten heeft
- Gebruik van authenticatieprocedures (gebruikersnaam/wachtwoord, pincode, biometrie, enz.)

Welke beschermingsdoelen vallen onder deze maatregel

☒ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.23 Gebruik van internet met web-isolatie

Web-isolatie scheidt het bureaublad van de gebruiker van browsersessies en maakt veilig internetgebruik mogelijk zonder de inhoud of functionaliteit te beperken. Browser ondersteunde cyberaanvallen, gegevensstroom/-verlies en de bijbehorende productiviteitsbeperkingen en imagoschade worden effectief voorkomen.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?
Infectie van de werkstation-computer, bijvoorbeeld door:

- browser kwetsbaarheden, drive-by-downloads, geïnfecteerde websites;
- ransomware, APT, Trojaanse paarden, virussen, wormen;
- zero-day exploits;
- kwaadaardige links in e-mailberichten;

en dus verspreiding van malware in het bedrijf kritische netwerk.

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?
Er zijn verschillende manieren om browsersessies te isoleren. De gebruikte architectuur en de beveiligingsmechanismen zijn hierbij bepalend. Voorbeelden zijn de zogenaamde remote controlled browseromgevingen of lokale meer-laags browserisolaties.

Een eenvoudige isolatie van de browseromgeving (bijvoorbeeld via eenvoudige virtualisatie op basis van Hyper-V of zogenaamde browser sandboxing) biedt onvoldoende hoog niveau van bescherming tegen de bovengenoemde bedreigingen, omdat het bijvoorbeeld geen veilig gehard besturingssysteem heeft waarin de browser standaard draait; maakt geen gebruik van extra beveiligde netwerksegmentatie; ondersteunt gen veilig kopiëren en plakken of maakt geen gebruik van extra beveiligingsfuncties zoals datasloten (gegevensvergrendelingen.) Dit is de reden waarom deze methode niet geschikt is om de bedreigingen tegen te gaan.

Remote controlled browser omgevingen gebaseerd op ReCoBS
Het ReCoBS scheidt het internetgebruik fysiek van de werkcomputer van de gebruiker. Elke browsersessie wordt buiten het gevoelige netwerkgebied uitgevoerd in een speciaal geïsoleerde omgeving binnen een speciaal gehard systeem op een afzonderlijke hardware in een afzonderlijk netwerksegment (DMZ).

Via een technisch beveiligd communicatiekanaal wordt de browser vanaf het werkstation via videostream op het externe systeem op afstand bestuurd.

De meeste aanvallen gericht op Windows-gebaseerde kwetsbaarheden worden al met succes afgeweerd in de geharde Linux-omgeving. Verdere beveiligingsmechanismen en zones in de overall architectuur bieden betrouwbare bescherming tegen aanvallen, zelfs als de browser is gecompromitteerd. De fysieke scheiding van het werkstation en het browsersysteem biedt ook bescherming tegen hardware-gerelateerde aanvallen (spectre, meltdown, zombieload en kwetsbaarheden in de hypervisor).

Met regelmatige tussenpozen (standaard eenmaal per dag) moet het externe systeem via een systeemkopie in zijn oorspronkelijke staat worden hersteld, zodat eventuele schadelijke code effectief wordt verwijderd en ervoor moet worden gezorgd dat de systeemkopie met integriteit wordt bewaard.

Het werkstation van de gebruiker vereist op geen enkel moment directe toegang tot internet en is daarom extra beschermd, bijvoorbeeld tegen het opnieuw laden van kwaadaardige code door geïnfecteerde documenten die de computer op andere manieren hebben bereikt, bijvoorbeeld via e-mail of USB-stick.

Aangezien de ReCoBS-architectuur het mogelijk maakt om gemeenschappelijke standaard browserfuncties op het externe-systeem uit te voeren, zijn aanvullende ontwikkelingen nodig voor acceptatie van de gebruikers, zodat de op afstand bestuurde browser niet significant verschilt van lokaal browsergebruik en alle gangbare functies zoals persoonlijke bladwijzers, kopiëren en plakken, afdrukken of up- en downloaden in principe beschikbaar worden gesteld.

Voor de optionele overdracht van bestanden (browser up- en download) tussen extern systeem en werkstation moeten extra controlemechanismen worden voorzien die opvallende bestanden in quarantaine plaatsen en beheerders op de hoogte stellen. Een voorbeeld van een dergelijk controlemechanisme is virusbescherming in de gegevensgateway.

Daarnaast wordt een centraal beheer van de overall oplossing aanbevolen, zodat bijvoorbeeld een bestaande directoryservice kan worden gekoppeld en gebruikt om gebruikersrollen te beheren.

Webisolatie gebaseerd op lokale virtualisatie van de browser applicatie
Een andere benadering van web-isolatie is gebaseerd op lokale inkapseling van de browsertoepassing door middel van veilige virtualisatie in combinatie met een Windows-gebruikersaccount met beperkte rechten, een gehard gast-besturingssysteem en internet/intranetscheiding via afzonderlijke VPN-tunnels naar de internetgateway. Dit voorkomt directe toegang van de browsersessie tot de hardware

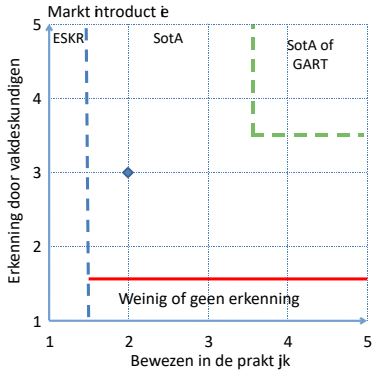
van de PC.

Een voordeel van lokale browserisolatie is de mogelijkheid van standalone gebruik op mobiele werkstations. De niet-bestaande fysieke scheiding tussen het gevoelige werkstation en het browsersysteem kan er echter voor zorgen dat lokale beveiligingshiaten in de processor hardware of -software worden misbruikt om via een exploit-pakket dat alle beschermende lagen dekt (all-Layer exploit package) in te breken in het eindapparaat.

Welke beschermingsdoelen vallen onder deze maatregel

☐ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.24 Aanval detectie en analyse (SIEM)

Security Information and Event Management Systems (SIEM) worden gebruikt om afwijkingen te evalueren en aanvallen op de bedrijfsinfrastructuur te voorkomen. Ze maken holistische, real-time herkenning van beveiligingskritieke gebeurtenissen in de IT-infrastructuur en de implementatie van passende maatregelen (gedeeltelijk geautomatiseerd) mogelijk.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

SIEM kan helpen tegen de volgende bedreigingen:

- Aanvalsactiviteiten door externe partijen (hackeraanvallen)
- Bedreigingen door insiders (zoals ongeautoriseerde toegang tot gegevens van andere afdelingen, computersabotage)
- Compliance schendingen

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

Een SIEM wordt gebruikt om log- en gebeurtenisgegevens van apparaten, netwerkcomponenten, applicaties en beveiligingssystemen centraal te verzamelen. De SIEM kan bijvoorbeeld de volgende gegevensbronnen in kaart brengen:

- Logbestanden van besturingssystemen
- Firewallgebeurtenissen van netwerkfirewalls
- Alarmen van inbraakdetectie- en preventiesystemen (IDS/IPS)
- Intelligente netwerksensoren/netwerkmonitorsystemen met informatie over gevonden assets/apparaten, kwetsbaarheden, nalevingsovertredingen of abnormale netwerkgedrag
- Directory services Authenticatiediensten (zoals Single Sign on-systemen)
- Endpoint Detection & Response Systemen (EDR/XDR)
- Indicatoren om aanvallers en aanvallen te identificeren, zoals IP-adressen, hashes, hostnamen, enz. (Threat Intelligence Feeds), bijvoorbeeld zoals contextinformatie om aanvallers aan te pakken

In de organisatie heeft het beveiligingsteam de mogelijkheid om in real time een holistisch beeld te krijgen van de processen in haar IT-oplossing/infrastructuur door de gerichte aggregatie en analyse van beveiligingsrelevante gebeurtenis- en systeemlogboeken. Dit maakt aanvallen, ongebruikelijke patronen en gevaarlijke processen zichtbaar. Op basis van de opgedane kennis zijn organisaties in staat om snel en accuraat te reageren op acute dreigingen. Op basis van de beschikbare data kunnen in de nasleep van een aanval patronen worden geanalyseerd (forensisch onderzoek) en kunnen bestaande maatregelen worden verbeterd.

Moderne SIEM-tools bevatten betrouwbare en direct toepasbare detectieregels die kunnen worden

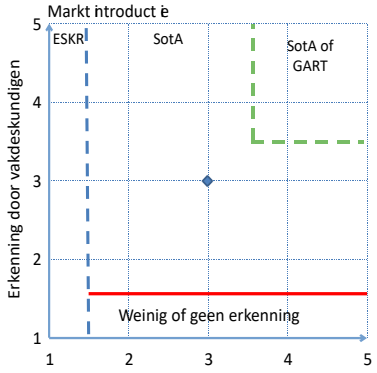
aangepast aan nieuwe dreigingsscenario's. De werking van een SIEM-oplossing vereist de integratie van geschikte bronnen, maar ook het verstrekken van aanzienlijke systeembronnen (zoals grafiekdatabases, data meren en servers voor exploitatie en beheer). Tegelijkertijd wordt door continue gegevensuitwisseling wordt een aanzienlijk bandbreedtebenutting bereikt. De bijbehorende beheercomplexiteit, aanschaf- en exploitatiekosten zijn vrij hoog, waardoor de klassieke SIEM-oplossingen meestal worden gebruikt in grote en zeer grote bedrijven.

Cloud gebaseerde en door derden beheerde oplossingen zoals SIEM as a Service (SIEMaaS) zijn een modern alternatief met eenvoudig te berekenen kosten. Ze maken het mogelijk om de technologie ook in kleine en middelgrote bedrijven te gebruiken. Ook kan een modern endpoint detection & response platform (DER/XDR) met zijn interfaces naar Security Orchestration, Automation and Response (SOAR), netwerkbeveiligingsproducten zoals next-generation firewalls en geïntegreerde threat intelligence een verstandig alternatief zijn.

Welke beschermingsdoelen vallen onder deze maatregel

☐ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.25 Vertrouwelijk gegevensverwerking

Traditioneel wordt geprivilegieerde toegang van beheerders tot gegevens tijdens de verwerking alleen beveiligd met organisatorische of reactieve maatregelen tegen misbruik van de bevoegdheid. Met behulp van vertrouwelijke gegevensverwerking (confidential computing) worden deze gegevens fraudebestendig en preventief beschermd tegen ongeoorloofde toegang. Dit is met name van belang voor toepassingen op het gebied van cloud computing. Het verwerken van vertrouwelijke gegevens komt overeen met de beschermingsvereisten wanneer clouddiensten worden gebruikt voor kritieke infrastructuren of voor gevoelige gegevensverwerkingsprocessen, zoals in de geneeskunde, industrie of in gereguleerde gebieden (zoals regTech).

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

Cloudbeheerders zijn verantwoordelijk voor de probleemloze werking van hun systemen. Om deze taak te kunnen vervullen, krijgen ze tal van bevoegdheden. Ze kunnen bijvoorbeeld de systeemconfiguratie aanpassen en de inhoud van het geheugen uitlezen. Dit betekent dat gegevens kunnen worden gecompromitteerd op weg naar de cloud, opgeslagen in de cloudopslag en tijdens verwerking in de cloud, niet alleen door aanvallen van derden, maar ook door illegaal handelend van de medewerkers van cloud service-providers.

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

Eerdere benaderingen van gegevenstoegang-beveiliging hebben betrekking op gegevens in rust (opslag) en gegevens in transit (netwerk). Confidential computing richt zich op de bescherming van gegevens tijdens de verwerking. Dit is een van de buitenwereld afgeschermde omgeving of capsule waarin alle gegevensverwerking in onversleutelde toestand plaatsvindt. Deze afscherming kan direct op de processorchip van de server en/of via meerdere servers worden geïmplementeerd.

Om de gegevens te kunnen verwerken, moet de benodigde sleutel beschikbaar zijn in de capsule. Als een aanvaller zou proberen toegang te krijgen tot de ingekapselde omgeving, zouden de gegevens die daar zonder codering worden verwerkt, onvermijdelijk uit voorzorg worden verwijderd. Om een verhoogde veiligheid te bereiken, kunnen de capsules na voorafgaand onderzoek door onafhankelijke auditors worden verzegeld met behulp van bekende cryptografische geheimen.

In gegevensverwerkingssystemen die zijn uitgerust met de maatregelen die zijn samengevat onder het kopje vertrouwelijk computergebruik, kan geen enkele beheerder toegang krijgen tot de gegevens die

op de server worden verwerkt. Alleen een kwaadwillende coalitie van meerdere onafhankelijke partijen (bijvoorbeeld systeembeheerder samen met hun onafhankelijke auditors) kan de technische maatregelen terzijde schuiven. Dit vermindert de kans op kwaadaardige toegang met verschillende ordes van grootte.

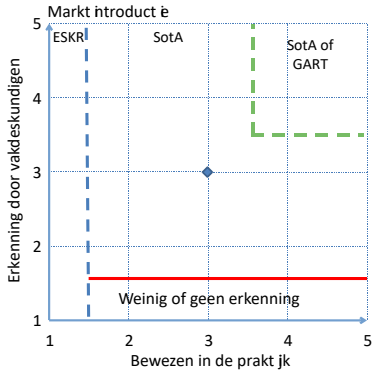
Vertrouwelijk computergebruik

- Maakt het mogelijk gegevens te verwerken in centrale infrastructuren zonder ze bloot te stellen aan de mogelijkheid om door de exploitanten van deze centrale infrastructuren te worden gelezen;
- Biedt gebruikers meer controle en, afhankelijk van de audit, ook transparantie
- Biedt nieuwe vrijheidsgraden, aangezien nieuwe toepassingen denkbaar zijn die onder conventionele gegevensbescherming- en veiligheidsoverwegingen niet op een juridisch conforme wijze kunnen worden uitgevoerd.

Welke beschermingsdoelen vallen onder deze maatregel

☐ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.26 Sandboxing voor analyse op kwaadaardige code

Sandbox-technologie wordt gebruikt om potentieel gevaarlijke bestanden in een geïsoleerde omgeving uit te voeren en te controleren op kwaadaardig gedrag. Het uitvoeren in een separate omgeving voorkomt mogelijke infectie.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

- Hacker activiteiten (generiek)
- Malware (virussen, Trojaanse paarden, enz.)
- Phishing

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

Het gebruik van de sandboxing-methode voor geautomatiseerde malware-analyse is gebruikelijk in twee use cases:

Perimeter sandboxing

Bij perimeter sandboxing worden bestandsbijlagen (zoals documenten uit de actieve omgeving en ingesloten inhoud zoals scripts) uit e-mails meestal automatisch uitgevoerd. Sandbox-analyse op de e-mailgateway genereert voor de gebruiker meestal een latentie in de toegang tot de onderzochte bestandsbijlage, van enkele seconden tot minuten.
Sandboxes kunnen ook worden gebruikt bij de webgateway (next-generation firewall of proxy) om bijvoorbeeld gedownloade programma's te controleren. Ook hier wordt een vertraging veroorzaakt voordat het bestand bij de gebruiker wordt afgeleverd. Daarnaast heeft het gebruik ook invloed op het gedrag van de browser en web-gebaseerde software. Daarom wordt het bestand naast de klassieke sandboxing-functie (controleer eerst of de levering vertraagd is) ook met parallelle controle aan het eindapparaat afgeleverd.
Als tijdens de laatste procedure kwaadaardige code wordt geïdentificeerd, worden daaropvolgende maatregelen genomen. Deze omvatten netwerkisolatie en het blokkeren van command and control-adressen die tijdens sandboxing zijn geïdentificeerd.

Sandbox voor forensisch onderzoek van bestanden die tijdens het onderzoek werden ontdekt of geïdentificeerd

Door sandboxes te verbinden met next-generation antivirusproducten (op machine learning

gebaseerde antivirus) en EDR-oplossingen (eindpuntdetectie en -respons), kunnen bestanden met een schadelijke prognose of van gedetecteerde en actief onderdrukte aanvalsketens veilig buiten de actieve omgeving worden uitgevoerd. Het uitvoeren maakt vervolgens de extractie van verdere relevante indicatoren (zoals bestanden/hashes, URL's, IP-adressen, registeractiviteiten, enz.) mogelijk en die meer context bieden aan de zaak die wordt onderzocht en zelfs de toewijzing van een vermoedelijke aanvaller mogelijk maakt.

Omdat sandbox-oplossingen vrij wijdverspreid zijn, proberen aanvallers altijd detectie in een sandbox te voorkomen. Bij het uitvoeren van hun kwaadaardige code proberen ze bijvoorbeeld, met bepaalde programma's/processen en andere specifieke functies, te bepalen of het een gevirtualiseerde runtime-omgeving is, zoals gebruikelijk is bij sandboxes, of een actieve omgeving. Om detectie ervan te voorkomen zal de kwaadaardige code zich dan meestal onschadelijk gedragen. Dit gedrag kan echter ook worden gedetecteerd in de sandbox en worden gebruikt om verdachte inhoud te identificeren (kat-en-muisprincipe).
De exploitatie van zogenaamde Day-0 Exploits/Zero-Day Threats, ofwel zwakke punten die nog niet bekend zijn bij het publiek, kan ook leiden tot sandbox-ontduiking (bypasses). Het kan ook voorkomen dat de geëmuleerde runtime-omgeving niet overeenkomt met het slachtoffersysteem en dus het gedrag bij het uitvoeren in de sandbox verschilt van dat op het doelsysteem van een aanval. Het is daarom noodzakelijk om deze tactieken bekend als sandbox-ontduiking (sandbox evasion) onder de knie te krijgen, bijvoorbeeld door statische en dynamische analyse te combineren.

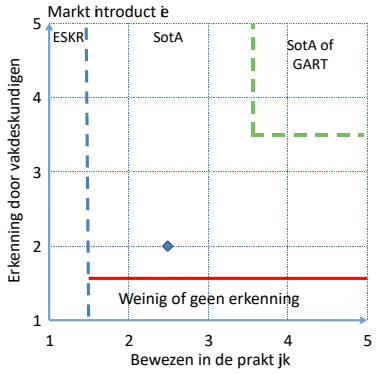
Sandboxes bieden ook een groot voordeel vanwege hun hoge mate van automatisering, waardoor de noodzaak voor handmatige analyse van kwaadaardige code (zogenaamde malware reverse engineering) door een expert enorm wordt verminderd.

Er zijn veel open source en commerciële sandboxes beschikbaar. Veelal woerden deze aangeboden als veelal kosten-intensieve hardware-oplossingen, of als publieke of private cloudoplossingen. Sand-box-technologie wordt ook al enige tijd in browsers gebruikt om veelvoorkomende soorten aanvallen in een vroeg stadium te detecteren.

Welke beschermingsdoelen vallen onder deze maatregel

☐ Beschikbaarheid ☒ Integriteit ☒Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.27 cyberdreiging intelligentie (cyberthreat intelligence)

Cyber Threat Intelligence is een belangrijk element van moderne verdedigingsstrategieën en biedt indicatoren, rapporten en diensten om op de hoogte te blijven van huidige aanvallen, cyberaanvallen te identificeren, hun vermoedelijke auteurs te bepalen en tegenmaatregelen af te leiden.

Cyber Threat Intelligence is onderverdeeld in drie toepassingsgebieden:

- Tactische Cyber Threat Intelligence omvat malware-analyse en de import van individuele, statische en gedragsmatige dreigingsindicatoren in defensieve IT-beveiligingsoplossingen zoals netwerk-, endpoint- en applicatie-beveiligingsoplossingen om hun effectiviteit te vergroten. Indicatoren verkregen via Cyber Threat Intelligence kunnen een belangrijke rol spelen bij maatregelen zoals systeempatching.
- Operationele Cyber Threat Intelligence wordt gebruikt om de kennis over een aanvaller, zijn vaardigheden, infrastructuur en aanvalstactieken, evenals technieken en procedures (TTP's) te verbeteren. Deze informatie kan worden

gebruikt om significante meer gerichte cyberbeveiligingsmaatregelen te implementeren, zoals incidentanalyse, incidentrespons en proactieve opsporing van bedreigingen. Dit verbetert de prestaties van cybersecurity-medewerkers (bijvoorbeeld van het Security Operation Center of CERT), zoals experts op het gebied van het opsporen van bedreigingen, kwetsbaarheidsmanagers, incidentresponsanalisten en insider threat prevention-experts.

- Strategische Threat Intelligence biedt een beter inzicht in de huidige dreigingssituatie (dreigingsanalyse), de afleiding van trends en de motivatie van individuele aanvallersgroepen. Het ondersteunt strategische zakelijke beslissingen om de cyberbeveiliging te verbeteren.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?
Cyber Threat Intelligence biedt informatie over alle soorten huidige en potentiële cyberdreigingen en helpt zich daartegen te verdedigen.

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

1. **Tactische Cyber Threat Intelligence (TM)**

Integratie van bedreigingsindicatoren (feeds) in bestaande endpoint- en netwerkdetectie- en respons systemen, systeembeheeroplossingen, firewalls, IDS/IPS- en SIEM/SOAR-oplossingen met als doel echte aanvallen te identificeren en analyse te ondersteunen (inclusief retro hunting), evenals het voorkomen van compromitteren. Voor een optimale effectiviteit moet het mogelijk zijn om de indicatoren automatisch te gebruiken voor de detectie en preventie van cyberaanvallen. De bronnen voor Threat Intelligence Indicators maken het mogelijk om conclusies te trekken over hun betrouwbaarheid en worden onderscheiden in:

- open source intelligence (OSINT);
- gebeurtenissen van particuliere honeypot-systemen;
- inzichten uit aanvalsanalyses uit echte klantomgevingen; of
- onderzoekswerk door deskundigen die door de inlichtingendiensten zijn opgeleid.

2. **Operationele Cyber Threat Intelligence (TM/OM)**

Organisaties die een Security Operation Centre (SOC) exploiteren en mogelijk hun eigen Computer Emergency Response Team (CERT) hebben, gebruiken Threat Intelligence om zichzelf continu op de hoogte te houden van de actoren en hun TTP's. Voor dit doel bieden uitgebreide Threat Intelligence-platforms toegang tot indicatoren, verschillende rapportindelingen (korte rapporten, situatierapporten, aanvallerprofielen), toegang tot malwaredatabases, sandbox-technologie voor geautomatiseerde malware-analyse en reverse engineering van malware. De aanbieder moet in staat zijn om aan klant specifieke eisen te voldoen. Bovendien moet het mogelijk zijn om rechtstreeks toegang te krijgen tot analisten bij de aanbieder en om onderzoeksvragen (RFI's) in te dienen.

3. **Strategische Threat Intelligence (OM)**

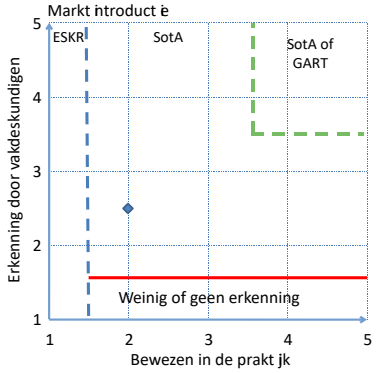
Zowel de informatiebeveiligingssector als de overall/corporate security van grote bedrijven maken gebruik van Threat Intelligence om een zo compleet mogelijk beeld van de situatie te krijgen. De geopolitieke situatie en sectorspecifieke en mondiale trends in het dreigingslandschap staan hierbij centraal. Door toegang te hebben tot een toegewijde medewerker bij de provider wordt het eigen team virtueel uitgebreid en wordt ervoor gezorgd dat directe toegang tot de datapool van de provider mogelijk is en dat klant specifiek onderzoekswerk optimaal wordt uitgevoerd.

Aanbieders van moderne IT-beveiligingsoplossingen leveren, integreren en automatiseren Threat Intelligence, zodat dreigingsindicatoren en relevante aanvalstelemetrie zinvol worden gekoppeld, preventieve maatregelen automatisch worden gekoppeld en aanvallerattributie mogelijk wordt gemaakt zonder dat de gebruiker extra systemen of personeel nodig heeft.

Welke beschermingsdoelen vallen onder deze maatregel

☒ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☐ Authenticiteit

Stand der techniek classificatie



3.2.28 Beveiligen van IT-beheersystemen

IT-beheersystemen zijn clients en servers die andere IT-systemen beheren en bewaken met behulp van beheertoepassingen. In vergelijking met standaardwerkstations bevinden IT-beheersystemen zich meestal in speciale netwerksegmenten waarin aanvullende netwerkprotocollen worden gebruikt en van waaruit de beheerinterfaces van systemen kunnen worden bereikt. Door dit bijzondere gebruik van IT-beheersystemen vormen deze systemen een groot risico op schade (zoals toegang door onbevoegden). Daarom moeten risicobeperkende voorschriften en maatregelen, tegen ongeoorloofde toegang en om een veilig beheer van IT-systemen te handhaven, worden genomen; met name met betrekking tot de bescherming van accounts met speciale bevoegdheden die op de systemen en de noodzakelijke verbindingen worden gebruikt

Eisen aan IT-beheersystemen

IT-beheersystemen moeten overeenkomstig de server-hardening maatregel (zie hoofdstuk 3.2.21) worden gehard.

Voor het gebruik en de omgang met IT-beheersystemen en voor de bescherming ervan moeten regels en maatregelen worden vastgesteld. Alvorens toegang te verlenen aan een gebruiker, moet de gebruiker eerst dit reglement aanvaarden en zich ertoe verbinden deze na te leven. Een overtreding van de vastgestelde voorschriften moet worden verklaard en moet zo nodig gevolgen hebben.

Toegang tot IT-beheersystemen mag alleen worden verleend of vrijgegeven voor gekwalificeerde medewerkers. IT-beheersystemen mogen alleen worden gebruikt voor het beheer van systemen en moeten volgens hun beveiligingsvereisten worden beveiligd met hardening-maatregelen en sterke authenticatiemethoden. Hun beschermingseisen moeten met passende maatregelen worden vastgesteld en beschermd.

Toegang tot IT-beheersystemen moet alleen, na succesvolle authenticatie via een beveiligde inlogprocedure, mogelijk zijn voor geautoriseerde beheerders. Dit vereist een geschikte authenticatiemethode om de gebruiker te identificeren en die voldoet aan de beveiligingseisen van het te beheren systeem (zoals meervoudige authenticatie, zie hoofdstuk 3.2.3). Bij het invoeren van toegangsgegevens zoals wachtwoorden of pincodes mogen deze gegevens niet door het systeem worden weergegeven. Bij het via het netwerk inloggen op IT-beheersystemen moeten de gegevens voor het verifiëren van de gebruiker met behulp van beveiligde protocollen in gecodeerde vorm worden verzonden. Inactieve externe sessies moeten na een bepaalde periode automatisch worden afgemeld/beëindigd.

Als voor het beheer een verbinding met een netwerksegment met systemen met een hoge of zeer hoge beveiligingsvereiste vereist is (zoals een netwerksegment met SCADA/ICS-systemen), moet de beheer- of netwerkverbinding via een jump server/proxy server in een DMZ tussen deze netwerksegmenten worden gemaakt.

Er moeten minimumnormen komen voor wachtwoorden voor IT-beheersystemen. Deze systemen moeten ook worden geïntegreerd in “stand van de techniek” autorisatiesystemen en waarbij de aansluiting en het autorisatiesysteem zelf speciaal moeten worden beveiligd/gehard. Verder moeten gepersonaliseerde accounts worden gebruikt, die duidelijk aan een persoon kunnen worden toegewezen. Standaardgebruikers en wachtwoorden mogen niet worden gebruikt.

Er moet voor worden gezorgd dat op IT-beheersystemen alleen toegestane softwarecomponenten, programma's en scripts worden uitgevoerd. Als een aanvulling op softwarecomponenten, programma's of scripts noodzakelijk is, moet in het kader van een passend proces toestemming worden verleend

voordat zij worden gebruikt en moet het gebruik ervan worden gedocumenteerd en gecontroleerd.

Op IT-beheersystemen moeten de inlogprocessen en activiteiten van beheerders worden gelogd, zodat kan worden getraceerd welke activiteiten door welke personen zijn (accounts) zijn uitgevoerd. Om de verifieerbaarheid van de uitgevoerde activiteiten te waarborgen, mogen beheerders de logboeken en auditfiles van hun eigen activiteiten met hun accounts niet wijzigen of verwijderen. Voor kritieke beheeractiviteiten moet het meer-ogen-principe worden toegepast.

Aanbeveling/implementatie
Voor de inrichting worden als voorbeelden voor een adequate bescherming de volgende maatregelen aanbevolen:

- ISO/IEC 27002:2013

De norm bevat aanbevelingen voor de implementatie van de in ISO/IEC 27001:2013 Annex A vereiste maatregelen voor toegangscontrole en voor de operationele beveiliging van systemen, die ook van toepassing zijn op IT-beheer. Als certificering volgens ISO/IEC 27001:2013 wordt nagestreefd, moeten deze maatregelen worden geïmplementeerd in het kader van het ISMS. Uitvoeringsinstructies voor deze maatregel zijn vooral te vinden in paragrafen 9 Toegangscontrole en 12 Operationele beveiliging.

- BSI IT-Grundschutz Compendium (februari 2021)

Het BSI IT-Grundschutz Compendium beschrijft in de modules SYS.1, SYS.2 en IND.1 tal van maatregelen voor de bescherming van systemen. Deze modules zijn ook relevant en van toepassing op IT-beheersystemen. In de bouwstenen wordt de implementatie van de genoemde eisen voor een hoge of zeer hoge beschermingsbehoefte aanbevolen.

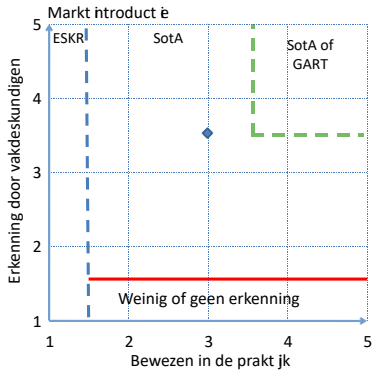
- De BDEW Whitepaper: Anforderungen an sichere Steuerungs- und Telekommunikationssysteme 2.0 geeft ondersteunend advies voor het beveiligen van IT-beheersystemen, zoals het gebruik van secure protocollen en jump servers voor (remote) access, en ook het in afgeschermde netwerkzones (DMZ) plaatsen van systemen.

De specificaties voor de operationele beveiliging en toegangsbeveiliging van IT-beheersystemen moeten periodiek (ten minste jaarlijks) op volledigheid en geschiktheid worden gecontroleerd en worden bijgewerkt in overeenstemming met een toegangs- of toegangscontrolebeleid.

Welke beschermingsdoelen vallen onder deze maatregel

☒ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.29 Monitoring van directoryservices en op identiteit gebaseerde segmentatie

Bij een groot deel van de ernstige cyberaanvallen van door de overheid gemotiveerde actoren en cybercriminelen zijn directory-services en gebruikersaccounts betrokken. Deze omvatten complexe supply chain-aanvallen en daaropvolgende spionage en sabotage. Daarom is het essentieel voor bedrijven en organisaties om hun aanvalsoppervlak te verkleinen en onnodige risico's in een vroeg stadium te identificeren en te elimineren, om aanvalspogingen en ongebruikelijke toegangen vanaf het begin te detecteren en in real time in te dammen, zelfs als de aanvaller buitgemaakte geldige toegangsgegevens gebruikt en eindpuntbeveiliging en IPS-systemen falen.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

- Aanvallen die gebruikmaken van vastgelegde/gelekte gebruikersnamen en wachtwoorden (zoals toegang krijgen tot gegevens die op het dark web worden verhandeld) en waarbij

geen malwarecomponent betrokken is.

- Misbruik van kwetsbaarheden in directory services (onvoldoende beveiligde serviceaccounts (kruisverwijzing naar het hoofdstuk Beschermen van beheerdersaccounts?)
- Verspreiding en beweging (laterale beweging) van een aanvaller binnen de organisatie
- Misbruik van accounts met speciale bevoegdheden, escalatie van autorisatie

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?
Monitoring en bescherming van directoryservices en controle van gebruikersaccounts (op identiteit gebaseerde risico gebaseerde Conditional Access)

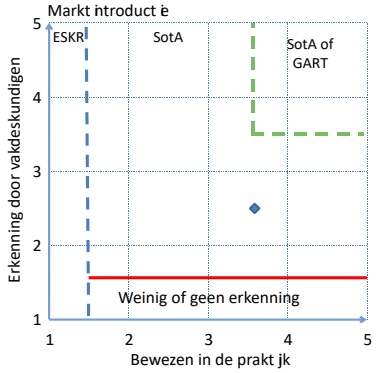
1. Beoordeling/audit van directoryservices: Moderne beveiligingsoplossingen combineren de hygiënestatus van directory services zoals Active Directory, Azure Active Directory en andere 'Identity as a Service'-oplossingen om kwetsbaarheden profylactisch te behandelen en risicoprofielen te maken. Deze omvatten:
   - Detectie van slecht beveiligde serviceaccounts
   - Identificatie van verborgen bevoegdheden die verder gaan dan het groepslidmaatschap, zoals delegatie, verkeerd gebruik van SID's met speciale bevoegdheden,
   - Detectie van aanvalspaden naar accounts met speciale bevoegdheden die doorgaans alleen worden ontdekt tijdens uitgebreide audits (zoals via tools zoals SharpHound/Bloodhound).
2. Real-time monitoring en analyse van al het relevante authenticatieverkeer, zowel lokaal, (zoals Kerberos, NTLM, LDAP, RDP, RPC enz.), als van cloud gebaseerde IDaaS- en Federation-services, om aanvalspogingen en het gebruik van zogenaamde verkenningstools te detecteren en in een uitgebreide en verrijkte vorm aan het Security Operation Centre (SOC) te presenteren. Door integratie met cloud gebaseerde diensten kunnen ook geolocatie gerelateerde afwijkingen worden geregistreerd en afwijkingen van normaal gebruik worden gedetecteerd.
3. Op basis van de individuele beschermingsbehoeften van de betreffende organisatie en vanaf punt één rekening houdend met de risicoprofielen, kan een identiteit-gerelateerde reeks regels worden geïmplementeerd, die bijvoorbeeld voorkomt dat gebruikersaccounts met een slechte risicoscore toegang krijgen tot kritieke toepassingen of tot lokale kritieke servers. Het moet ook mogelijk zijn om automatisch te reageren op ongewoon gebruikersgedrag en maatregelen te eisen, zoals het verzoek om een extra authenticatiefactor (MFA). Dit maakt bescherming mogelijk die de focus van gespecialiseerde klassieke oplossingen zoals Privileged Access Management (beheer van speciale bevoegdheden) combineert met die van User & Entity Behavior Analytics en die tegelijkertijd eenvoudig in de praktijk kan worden toegepast, zoals door een sensortoepassing in de directoryservers te implementeren, en API-gebaseerde integratie in federation-services en cloud directory-diensten. De toepassing van machine-learning-modellen vermindert de inspanning hier aanzienlijk.

Opmerking: Alle drie de deelgebieden zijn belangrijke bouwstenen en dragen actief bij aan de implementatie van een Zero Trust Framework. Beleid kan effectief worden geïmplementeerd zonder dat koppelingen met bijvoorbeeld netwerkfirewalls hoeven te worden geïmplementeerd.

Welke beschermingsdoelen vallen onder deze maatregel

☐ Beschikbaarheid ☒ Integriteit ☒Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.2.30 Netwerk segmentatie en scheiding

Het partitioneren van netwerken door middel van netwerksegmentatie en -scheiding is een effectieve maatregel om bedreigingen voor de beschikbaarheid, vertrouwelijkheid en integriteit van netwerken en de daarin opgenomen systemen te verminderen. Segmentatie en scheiding ondersteunen ook, als onderdeel van de defense-in-depth-aanpak, bescherming.

Bij netwerksegmentatie is een netwerk verdeeld in verschillende segmenten, die elk fungeren als een eigen subnetwerk. De communicatie tussen deze segmenten wordt beperkt via gedefinieerde zonegrenzen (koppelpunten) met een controle/bewaking van de netwerkverbindingen. Zonegrenzen tussen netwerken, zoals tussen informatietechnologie (IT) en operationele technologie (OT), verminderen veel risico's die verband houden met het IT-netwerk, zoals malwarebedreigingen. Zonescheiding of segmentatie beperkt de toegang tot systemen, gegevens en toepassingen en beperkt de communicatie tussen netwerken. Deze aanpak beschermt segmenten in het netwerk tegen aanvallen van andere (al getroffen) segmenten.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

- Laterale beweging van aanvallers in het netwerk (Network Lateral Movement)
- Ongehinderde verspreiding van malware in netwerken.
- Bedreigingen van binnenuit (zoals ongeautoriseerde toegang tot systemen van andere afdelingen of locaties).
- Vanwege netwerkgroottes en gegevensvolumes moeilijker te identificeren ongeautoriseerd of kwaadaardig verkeer
- Exploitatie van de toegang tot genetwerkte IT-systemen
- Verlies van beschikbaarheid, integriteit en vertrouwelijkheid van veel systemen als ze op een plat netwerk werken en worden gecompromitteerd
- Verlies van beschikbaarheid van kritieke systemen op het netwerk als gevolg van aanvallen op niet-kritieke systemen met minder beveiligingsmaatregelen

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

Voor netwerksegmentatie moet een netwerk worden verdeeld in verschillende zogenaamde netwerkzones (of subnetwerken), waarbij een netwerkzone een logische groep apparaten, toepassingen en systemen vormt met gemeenschappelijke beveiligingsvereisten (dezelfde beveiligingsbehoeften). Het gebruik van kritieke en niet-kritieke systemen in een netwerkzone, zelfs als ze thematisch kunnen worden gegroepeerd of een hoog niveau van communicatie met elkaar hebben, is niet toegestaan.

Netwerkzones kunnen logisch (zoals door VLAN's) en/of fysiek (zoals door een speciaal daarop gerichte switchinfrastructuur worden gescheiden. De beslissing of fysieke scheiding vereist is, moet worden genomen op basis van wettelijke vereisten of met een op risico's gebaseerde benadering.

Al het verkeer tussen de verschillende netwerkzones verloopt via gedefinieerde en passende zoneovergangen (koppelpunten) en moet vooraf worden goedgekeurd. In het geval van zoneovergangen moet beperking, controle en monitoring van netwerkverkeer met bijvoorbeeld firewalls/IPS/ACL worden geïmplementeerd. Mechanismen voor het detecteren van beveiligingsrelevante gebeurtenissen in het netwerkverkeer (zoals firewall/IPS, inloggen op netwerkapparaten en sensoren/IDS) moeten op basis van risicoafweging worden geïmplementeerd en kunnen bijvoorbeeld door een SIEM worden geanalyseerd en geëvalueerd.

Voor zoneovergangen wordt een whitelisting-aanpak toegepast. Al het dataverkeer wordt standaard

geblokkeerd en alleen gedefinieerd dataverkeer is toegestaan (standaard weigeren, bij uitzondering toestaan). Netwerkverbindingen tussen systemen in verschillende netwerkzones (met name met verschillende beschermingseisen) moeten tot het noodzakelijke minimum worden beperkt en, indien nodig, moeten afzonderlijke overdrachtsinterfaces worden geïmplementeerd in afzonderlijke zones (zoals DMZ).

Voor netwerksegmentatie moet een architectuur op basis van het defense-in-depth-principe worden gepland en geïmplementeerd. Hiervoor moeten zones voor externe of niet-vertrouwde netwerken (zoals internet- en WLAN's voor bezoekers), zones voor DMZ-systemen (zoals proxysystemen en jumpservers voor externe toegang) en zones voor interne systemen (zoals servers, clients, printers, enz.) worden voorzien. Voor systemen die moeten worden geïsoleerd (zoals systemen zonder beveiligingsupdates/onderhoud) moeten aparte zones worden ingericht. Industriële netwerken, iSCSI/opslagnetwerken en IT-netwerken moeten altijd fysiek van elkaar gescheiden zijn.

Al het netwerkverkeer met netwerken van derden (zoals internet voor het downloaden van updates en externe toegang van externe dienstverleners) moet in een DMZ-zone worden beëindigd door proxy's, jumpservers, VDI-omgevingen, enz. en het netwerkverkeer moet worden gecontroleerd. Directe communicatie van netwerken van derden naar interne netwerkzones is niet toegestaan.

Afhankelijk van de beschermingseisen en de kritikaliteit moeten de vereiste beschermings-/harding-maatregelen voor de afzonderlijke zones worden gedefinieerd en geïmplementeerd.

Afgezien van actieve netwerkapparaten, zou elk systeem zich logischerwijs in slechts één zone moeten bevinden. Routering van netwerkverkeer op hosts/VM's tussen netwerkadapters of de plaatsing van systemen in meerdere netwerken (multi-homing) moet in principe worden vermeden en mag alleen, na een eerder uitgevoerde risicoanalyse en met de nodige beschermende maatregelen en zoneovergangen om geen ongecontroleerde overgangen tussen zones te creëren, worden uitgevoerd in vrijgegeven en gedocumenteerde situaties. Bovendien moet, voor externe apparaten die verbinding maken met bedrijfssystemen, split tunneling worden voorkomen. Split-tunneling stelt een externe persoon of extern apparaat in staat om verbinding te maken met een beveiligd netwerk terwijl hij via een andere verbinding communiceert met een bron op een extern/onveilig netwerk. Uitzonderingen waar split-tunneling is bedoeld, zoals voor videoconferentie oplossingen die zonder tunnel toegang hebben tot centrale cloud systemen, moeten worden gedefinieerd.

Voor beheersystemen moeten speciale netwerken beschikbaar worden gesteld, die alleen voor beheertaken mogen worden gebruikt. Beheerderstoegang tot out-of-band netwerken op beheerinterfaces van servers, netwerkapparaten of KVM-systemen mag alleen mogelijk zijn vanaf netwerken voor beheersystemen.

In relatie tot het Zero Trust Principe wordt steeds vaker gebruik gemaakt van zogenaamde microsegmentatie. Hier wordt het aanvalsoppervlak verkleind door het netwerk op te delen in segmenten die nodig zijn om een toepassing uit te voeren (bijvoorbeeld virtuele machines, containers, services).

Voor de uitvoering van de maatregel worden de volgende normen aanbevolen:

BSI IT-Grundschutz Compendium
: De BSI IT-Grundschutz Compendium beschrijft in module NET.1.1 Netwerkarchitectuur en -ontwerp vereisten voor de specificatie, planning, implementatie en het testen van netwerksegmentatie en voor het beveiligen van de netwerkcommunicatieverbindingen die plaatsvinden via de zones.

ISO/IEC 27002:2022
: De ISO/IEC 27002:2022-norm bevat aanbevelingen voor de implementatie van netwerkbeveiligingsmaatregelen (Control 8.20), netwerk service security (Control 8.21) en netwerk scheiding (Control 8.22).

IEC 62443-3-3:2013
: De IEC 62443-3-3:2013-norm bevat specificaties voor netwerksegmentatie en voor de controle van netwerkzone-overgangen in industriële communicatienetwerken in FR 5 Restricted Data Flow.

Periodiek en indien nodig moeten audits worden uitgevoerd om na te gaan of de bestaande netwerken en netwerksegmenten aan de vastgestelde specificaties en voorschriften en aan de huidige documentatie voldoen.

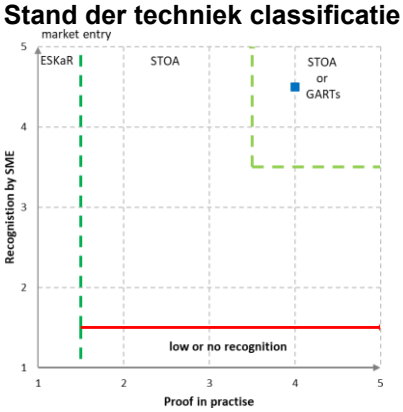
De gedocumenteerde richtlijnen, procedures en controlemaatregelen voor netwerkscheiding die essentieel zijn voor de exploitatie, moeten periodiek worden gecontroleerd op volledigheid,

doeltreffendheid, geschiktheid en op gewijzigde randvoorwaarden en zo nodig worden bijgewerkt.

Welke beschermingsdoelen vallen onder deze maatregel

☒ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.3 Organisatorische maatregelen

Omdat informatie- en communicatiefaciliteiten niet altijd in beginsel zijn ontworpen voor beveiliging en technische beveiliging alleen effectief is als deze adequaat gepaard gaat met organisatorische en personele maatregelen, heeft elke organisatie een systeem van methoden, procedures en regels nodig voor het beheer van de beveiliging van bedrijfsinformatie, met andere woorden: een Information Security Management System (ISMS).

Een ISMS stelt regels vast en implementeert deze voor het classificeren en omgaan met gevoelige informatie. Het ISMS is een belangrijk onderdeel van het managementsysteem en loopt door alle belangrijke gebieden van de organisatie. Het ISMS omvat methoden voor regelmatige inspectie en documentatie van organisatorische en technische veranderingen.

Een belangrijk aandachtspunt van het ISMS is het overwegen van veranderingen in de informatiebeveiliging wanneer belangrijke elementen van de IT-structuur gepland zijn om te worden gewijzigd of gehandhaafd. Een ander aspect is regelmatige training en bewustmaking van het personeel. Het ISMS bepaalt ook hoe noodpreventie moet worden uitgevoerd en hoe moet worden gereageerd op potentiële beveiligingsincidenten. Het doel van het ISMS is om op lange termijn een efficiënt en voortdurend adequaat veiligheidsniveau te garanderen en te handhaven.

TeleTrust heeft in haar document Informationssicherheitsmanagement - Praxisleitfaden für Manager een bruikbare richtlijn gegeven voor het beheren van de informatiebeveiliging. Het document laat zien dat informatiebeveiligingsbeheer en de daaraan gekoppelde compliance- en risicocultuur een strategisch controle-instrument kan zijn dat de beveiligingssituatie in één oogopslag zichtbaar maakt.

3.3.1 Normen en standaarden

Er zijn een aantal internationale standaarden en normen die als basis kunnen dienen voor de implementatie van een ISMS. Anders dan bij technische maatregelen zijn de voortdurende veranderingen in organisatorische maatregelen een permanent fenomeen, wat betekent dat verwijzing naar normen en standaarden zelfs in de context van stand van de techniek mogelijk is. De ISO/IEC 27000-reeks wordt gebruikt als referentiepunt voor verdere normen en standaarden. Er zijn enkele overlappingen, hoewel deze over het algemeen worden gebruikt als synergiën, wat in de zin van informatiebeveiliging resulteert in een positief effect op de gebruikte normen. Voor zover aanvullende normen of standaarden worden geïmplementeerd voor het beheer van IT-diensten, -processen en -risico's, moeten de geadresseerde overlappingen worden geïdentificeerd en gebruikt.

De ISO 27000 normen

De ISO/IEC 27000-reeks (ook bekend als ISO27K) is een reeks normen voor IT-beveiliging. Deze normen worden uitgegeven door de International Organization for Standardization (ISO) en de International Electrotechnical Commission (IEC).

ISO/IEC 27001 is de bekendste norm uit de ISO/IEC 27000-reeks. Het formuleert de eisen waaraan een ISMS moet voldoen. Voor de concrete uitvoering bestaan ook andere normen en richtlijnen.

De ISO/IEC 27000-reeeks bevat de volgende belangrijke items, die elk functioneren als een onafhankelijke norm en gegroepeerd zijn als een reeks normen.

ISO/IEC norm	Gebruikt voor de volgende taken
ISO/IEC 27000	Information technology - Security techniques - Information security management systems - Overview and vocabulary (Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Overzicht en woordenschat)
ISO/IEC 27001	Information security management systems - Requirements (Managementsystemen voor informatiebeveiliging - Eisen)
ISO/IEC 27002	Recommendations for various information security control mechanisms - Information security, cybersecurity and privacy protection - Information security controls (Aanbevelingen voor verschillende controlemechanismen voor informatiebeveiliging - Informatiebeveiliging, cyberbeveiliging en privacybescherming - Informatiebeveiligingscontroles)
ISO/IEC 27003	Information technology - Security techniques - Information security management systems - Guidance (Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Richtsnoeren)
ISO/IEC 27004	Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation (Informatietechnologie - Beveiligingstechnieken - Beheer van informatiebeveiliging - Monitoring, meting, analyse en evaluatie)
ISO/IEC 27005	Information technology - Security techniques - Information security risk management (Informatietechnologie - Beveiligingstechnieken - Risicobeheer op het gebied van informatiebeveiliging)
ISO/IEC TR 27019	Information technology - Security techniques - Information security controls for the energy utility industry (Informatietechnologie - Beveiligingstechnieken - Informatiebeveiligingscontroles voor de energiesector)
ISO/IEC 27031	Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity (Informatietechnologie - Beveiligingstechnieken - Richtsnoeren voor de gereedheid van informatie- en communicatietechnologie voor bedrijfscontinuïteit)
ISO/IEC 27034	Information technology - Security techniques - Application security (6½ parts) (Informatietechnologie - Beveiligingstechnieken - Toepassingsbeveiliging 6 ½ delen)
ISO/IEC 27035	Information technology - Security techniques - Information security incident management (parts 1-3 published, part 4 DRAFT) (Informatietechnologie - Beveiligingstechnieken - Beheer van informatiebeveiligingsincidenten (deel 1-3 gepubliceerd, deel 4 in ontwerpfase)

Tabel 1: Overzicht van de ISO/IEC 27000 serie

Andere normen en standaarden
Informatiebeveiligingsnormen en -criteria kunnen afhankelijk van het niveau waarop ze worden beschouwd, worden geclassificeerd als bedrijfs-, systeem- en productnormen. Ze kunnen op basis van hun formulering worden gegroepeerd in technische, minder technische en niet-technische normen.

De hierboven genoemde structuurniveaus kunnen, op basis van een eerdere beschrijving van initiatief D21, als volgt worden geschetst:

	Technisch	Minder technisch	Niet technisch
Bedrijf		BSI Standard 200 BSI Grundschutz	ISO 9000 ISO 20000 ISO 27000 ISO 22301 CobiT SoGP
Systeem		ICPP data protection seal of approval, EuroPriSe, TÜViT Trusted Process/Site/Product	
Product	ITSEC ISO 15408 (CC) ISO 19790 (FIPS 140)		

Afbeelding 5: Structuurniveaus van voor Informatiebeveiliging relevante standaarden

De, niet-in technische taal geformuleerde, eisen voor bedrijven en publieke instellingen beschreven in ISO 27001 onderscheiden zich van ISO 9001, ISO 20000-1, ISO 22301, CoBIT en Standard of Good Practice for Information Security (SoGP).

ISO 27000 e.v.
: De reeks normen in ISO 27000 e.v. omvat verschillende normen met betrekking tot ISMS. Een cruciale norm in deze serie is ISO/IEC 27001, die eisen beschrijft voor een functionerend ISMS in de context van een organisatie (zie 3.3.1.1).

ISO 27001 gebaseerd op BSI IT-Grundschutz
: Dit is de implementatie van ISO 27001 óp basis van de IT-basisbeschermingscatalogus (IT Grundschutz) van het Duitse federale bureau voor informatiebeveiliging (ook gedocumenteerd in BSI-norm 200-2).

De BSI-standaard 200-1 stelt de algemene vereisten voor een ISMS. In principe is het compatibel met ISO-norm 27001 en houdt het bovendien rekening met de aanbevelingen van andere ISO-normen van de ISO 2700x-familie, zoals ISO 27002. Het biedt iedereen die geïnteresseerd is, ongeacht welke methode ze willen gebruiken om de vereisten te implementeren, een gemakkelijk te begrijpen en systematische introductie en een reeks instructies.

BSI Standard 200-2 biedt met de procedure volgens IT-Grundschutz het volgende:

- specifieke en methodische ondersteuning bij de stapsgewijze invoering van een ISMS;
- aandacht voor de afzonderlijke fasen van het informatiebeveiligingsproces;
- oplossingen die zijn afgeleid van praktijkervaring, d.w.z. best practice-benaderingen;
- mogelijkheid tot certificering.

Het onderscheid in de implementatie tussen de originele ISO 27001-implementatie en de basisbeschermingsaanpak van BSI is te vinden in onderstaande tabel:

Categorie	ISO27001	BSI IT-basisbescherming
Toepassingsgebied	Relevante normen <100 blz.	Basisbescherming catalogus > 4000 pagina's
Eisen	Abstracte en generieke randvoorwaarden	Specifiek model voor praktische maatregelen
Risicoanalyse	Volledige analyse van elk doelobject	Vereenvoudigde analyse in geval van verhoogde beschermingsvereisten
Maatregelen	Ca. 150 conceptuele eisen	> 1100 specifieke maatregelen
Certificering	Certificering	Auditor certificaat + certificering
Geldigheid	3 jaar, jaarlijkse monitoring audits	3 jaar, jaarlijkse monitoring audits

Tabel 2: Differentiatie van ISO 27001 versus BSI IT-Basisbescherming

ISO 20000-1

Deze norm specificeert eisen aan (interne of externe) organisaties met betrekking tot het uitvoeren van procesgerichte diensten. Sommige van de vereiste processen (voornamelijk informatiebeveiligingsbeheer, incident- & eventmanagement en servicecontinuïteitsbeheer) overlappen met ISO 27001. Conventioneel wordt ISO 20000-1 toegepast op IT-organisaties, terwijl het toepassingsgebied van ISO 27001 alle soorten organisaties kan omvatten.

ISO 22301

Deze standaard houdt zich bezig met het borgen van bedrijfscontinuïteit (BCM) en specificeert eisen aan BCM-systemen in organisaties. Zoals in ISO 22301 beschreven, verwijzen BCM-systemen ook naar IT (maar niet alleen naar IT). Het toepassingsgebied van ISO 27001 omvat ook BCM, maar alleen vanuit het oogpunt van informatiebeveiliging (d.w.z. in hoeverre de bedrijfscontinuïteit in gevaar kan worden gebracht door informatiebeveiligingsincidenten).

ISO 9001

Deze norm specificeert de eisen van kwaliteitsmanagementsystemen, maar bevat ook een ongelooflijk aantal informatiebeveiligingsoverwegingen, bijvoorbeeld sommige gerelateerd aan verplichtingen in relatie tot:

- het waarborgen van de beschikbaarheid van middelen en informatie over de implementatie en monitoring van processen;
- de etikettering, opslag, bescherming en opvraagbaarheid van stammen;
- de vaststelling, terbeschikkingstelling en onderhoud van infrastructuur zoals gebouwen, werkplekken en bijbehorende pensioeninstellingen, procesapparatuur (bv. hardware en software) en ondersteunende diensten (bv. communicatie- en informatiesystemen);
- de bescherming van eigendommen van klanten, zoals intellectueel eigendom, persoonsgegevens enz.

CobiT

Control Objectives for Information and related Technology (CobiT) is een methode om, ter ondersteuning van bedrijfsrelevante processen, risico's die voortvloeien uit het gebruik van IT te beheersen. Het is een op revisie en controlling gerichte toolbox voor het management die resultaten en prestatiemetingen voor alle IT-processen definieert. CobiT beschrijft verschillende procesgebieden, elk met gedefinieerde controledoelen, volwassenheidsmodellen en maatregelen. CobiT heeft betrekking op alle IT-processen, terwijl ISO 27001 zich richt op het beheersen van informatiebeveiligingsprocessen.

SoGP

De Standard of Good Practice for Information Security (SoGP) van het ISF's is een goede praktijkbenadering voor bedrijfsinformatiebeveiliging en die ook benchmarking van beveiliging mogelijk maakt. De SoGP behandelt vanuit een zakelijk perspectief verschillende gebieden van informatiebeveiliging (bijvoorbeeld IT-beveiligingsbeheer, bedrijf kritische toepassingen, informatieverwerking, communicatie/netwerken, systeemontwikkeling) en biedt alternatieven, deels aanvullend, deels complementair aan ISO 27001.

3.3.2 Processen

Volgens het BSI is het onmogelijk om industriële normen te beschrijven op een manier die definitief is en van toepassing is op alle gebieden. In plaats daarvan kunnen ze worden bepaald met behulp van bestaande nationale en internationale normen, zoals DIN- of ISO-normen, of met behulp van sjablonen die in de praktijk met succes op het relevante gebied zijn toegepast.

Voor bedrijven die direct of indirect door ITSiG worden getroffen, betekent dit dat naleving, testen en certificeren van een groot aantal algemene en sectorspecifieke normen vereist is.

De onderstaande secties bevatten een korte beschrijving van de vereiste organisatorische maatregelen, en een beoordeling van welke normen uit de ISO/IEC 27000-serie moeten worden geïmplementeerd om aan de stand van de techniek te voldoen. De inhoud van dit hoofdstuk dient hierbij als leidraad. Constante technologische vooruitgang zorgt er echter voor dat ook officiële kaders en normen voortdurend moeten worden bijgewerkt.

Daarom vereist de afweging van stand van de techniek individueel onderzoek in hoeverre een individuele maatregel of bundel van maatregelen op een bepaald moment geschikt, noodzakelijk en redelijk is.

In tegenstelling tot de technische maatregelen volgens welke systemen of technische processen ervoor zorgen dat informatie wordt beschermd, beschrijven organisatorische maatregelen (als voorbeeld) zoals processen, werkinstructies, richtlijnen en dergelijke en die organisaties zichzelf opleggen en bedoeld zijn om de veiligheid te verhogen. Het implementeren en het naleven zijn meestal de verantwoordelijkheid van de betrokken personen en worden het best ondersteund door technische maatregelen. Regelmatige controle en training zorgen ervoor dat de geplande maatregelen correct worden uitgevoerd.

De actieve ondersteuning van het management en de samenwerking van gespecialiseerde afdelingen is van cruciaal belang bij het invoeren van een ISMS. Risico's die van invloed zijn op de bedrijfsinfrastructuur, persoon, IT, processen en informatie en die een negatief effect hebben op een of meer basiswaarden van informatiebeveiliging (zoals beschikbaarheid integriteit en vertrouwelijkheid) moeten worden geïdentificeerd en beoordeeld.

Hieronder volgen de primaire organisatorische processen en maatregelen die kunnen worden afgeleid uit stand van de techniek praktijken.

3.3.2.1 Beveiligingsorganisatie

De beveiligingsorganisatie streeft naar een beheerskader. De beveiligingsorganisatie omvat de taken en verantwoordelijkheden om de implementatie en werking van informatiebeveiliging binnen de organisatie te initiëren en te bewaken.

Om ervoor te zorgen dat een ISMS met succes kan worden geïntroduceerd en geëxploiteerd, moet het hoogste management:

- de eindverantwoordelijkheid voor het ISMS en informatiebeveiliging in de organisatie op zich nemen;
- gesensibiliseerd te zijn en alle relevante verantwoordelijke personen en medewerkers informeren over mogelijke risico's, persoonlijke aansprakelijkheid in geval van het niet-naleven van de vereisten en de mogelijkheden voor de organisatie met een ISMS, en hen verplichten tot informatiebeveiliging;
- definiëren, implementeren en continu verbeteren van een effectieve beveiligingsorganisatie in de vorm van rollen, verantwoordelijkheden en autorisaties;
- tegelijkertijd, met het oog op het beheer van de informatiebeveiliging, de volgende structuren vaststellen: organisatiestructuren (zoals afdelingen, groepen en competentiecentra), rollen en taken.
  Als minimumvereisten voor een beveiligingsorganisatie gelden:

- het benoemen van een verantwoordelijke manager (welke voorzitter of bestuurder is direct verantwoordelijk voor informatiebeveiliging?); en
- het benoemen van een Chief Information Security Officer (CISO) als centrale rol binnen een IS-organisatie.

Onder alle omstandigheden moeten de volgende basisregels in acht worden genomen:

- De eindverantwoordelijkheid ligt op managementniveau
- Iedere medewerker is verantwoordelijk voor informatiebeveiliging in zijn/haar werkomgeving.

De belangrijke rollen en verantwoordelijkheden binnen een beveiligingsorganisatie zijn:

Hoger management (bestuurders, Raad van Bestuur)
- strategische (toegewijde) verantwoordelijkheid en in laatste instantie ook eindverantwoordelijkheid voor informatiebeveiliging;
- verantwoordelijkheid voor alle risico gerelateerde beslissingen.

Chief Information Security Officer (CISO)
- tactische of (soms) operationele controle van informatiebeveiliging;
- ondersteuning van het management bij informatiebeveiliging-taakbewustzijn;
- stafpositie met direct recht en verplichting om te rapporteren aan het hoogste managementniveau.

Information Security Officer (ISO)
- operationele controle van informatiebeveiliging, waar nodig tactische taken voor individuele bedrijfsonderdelen;
- organisatorisch direct toegewezen aan CISO.

Functionaris voor gegevensbescherming (FG of DPO)
- moet niet noodzakelijkerwijs worden gezien als onderdeel van het IS-managementteam, maar in plaats daarvan als een belangrijk contact in zaken met betrekking tot compliance, en idealiter regelmatig betrokken bij het IS-managementproces.

Audit Manager
- centraal aanspreekpunt voor interne en externe audits;
- coördineert en controleert planning en uitvoering van audits;
- ondersteunt CISO in hun taken.

IS Management Team/IS Management Forum/Stuurgroep Veiligheid
- permanent gremium voor de coördinatie van de planning en uitvoering van informatiebeveiligingsmaatregelen;
- bestaat uit CISO, ISO('s), plaatsvervangers voor implementatie, gespecialiseerde beheerders, FG, vertegenwoordigers van het hoger management;
- advies- en controlefunctie voor CISO.

Organisatorische maatregelen komen overeen met de stand van de techniek, als de implementatie ervan voldoet aan de momenteel geldende normen. Bij de uitvoering van deze maatregelen moeten ten minste de normen ISO/IEC 27000 tot ISO/IEC 27005 van de ISO/IEC 27000-serie in acht worden genomen. Als andere toepasselijke eisen, normen of resultaten van risicobeoordelingen dit vereisen, kunnen ook andere organisatorische maatregelen noodzakelijk zijn.

3.3.2.2 Vereistenbeheer (Requirements management)

Een gericht en effectief ISMS kan alleen binnen de context van de specifieke organisatie en haar informatiebeveiligingseisen worden ingevoerd. Daarom moeten beveiligingsvereisten worden bepaald en moet de implementatie ervan worden gepland, gerealiseerd, gecontroleerd en voortdurend worden verbeterd.

Vereistenbeheer vormt als proces de basis voor het uitlijnen van informatiebeveiliging binnen de organisatie.
Het continu voldoen aan de vereisten garandeert dat belanghebbenden in een ISMS (se stakeholders) tevreden zijn. Vanwege de complexiteit hiervan is het opzetten van een vereistenbeheerproces aan te raden.

De eisen van een organisatie zijn onder te verdelen in:

- wettelijke vereisten;

- contractuele vereisten; en
- andere vereisten.

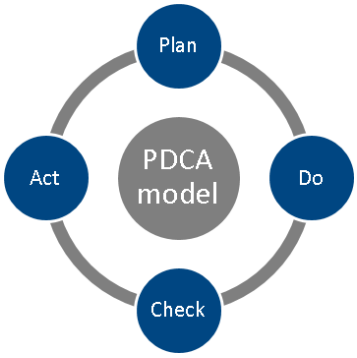
Wettelijke vereisten vloeien voort uit verschillende rechtsgebieden, zoals gegevensbeschermingsrecht, arbeidsrecht, IT-recht, strafrecht en nog veel meer (een uniforme informatiebeveiligingswetgeving is er niet). In toenemende, mate met betrekking tot traceerbare informatiebeveiliging, kunnen echter ook eisen (en verwachtingen) worden gesteld door verschillende zakenpartners van de organisatie (zoals door klanten, leveranciers, dienstverleners, uitbestedingspartners, samenwerkingspartners, verzekeringsmaatschappijen enz.).

Wettelijke en contractuele vereisten worden vaak primaire of basis vereisten genoemd omdat ze de basis vormen van het informatiebeveiligingsproces.

Andere vereisten (en/of verwachtingen/beperkingen) vloeien doorgaans voort uit de volgende entiteiten:

- markt;
- publiek (openbaarheid);
- bedrijf, hoofdkantoor;
- aandeelhouders;
- medewerkers;
- bedrijfsprocessen (incl. intern gedefinieerd beleid);
- technologie.

Een state-of-the-art vereistenbeheerproces kan in een PDCA-model als volgt worden weergegeven:



Afbeelding 6: PDCA-model

PLAN: Alle soorten eisen en verwachtingen van de organisatie,
- vastleggen;
- analyseren;
- beoordelen; en
- omzetten in interne (veiligheids-)specificaties voor de organisatie.

DO: Voldoen aan informatiebeveiligingsspecificaties van de organisatie (en dus impliciet ook aan de eisen en verwachtingen van de organisatie), bijvoorbeeld in de vorm van:
- organisatorische maatregelen: beleid, regelgeving, richtlijnen;
- personeel gerelateerde maatregelen, waaronder personeelsevaluatie, sensibilisering, permanente opleiding;
- technische maatregelen van toegangscontrole, encryptie enz.;
- infrastructurele maatregelen voor toegangscontrole, veiligheidszones.

CHECK: Monitoren en beoordelen van de mate waarin aan de institutionele informatiebeveiligingsspecificaties wordt voldaan (en dus impliciet ook aan de eisen en verwachtingen van de organisatie):
- het opvragen van indicatoren en parameters;
- het identificeren van tekortkomingen (in interactie met de stakeholders);
- het plannen van corrigerende maatregelen.

ACT: Het continu verbeteren van de mate waarin aan institutionele informatiebeveiligingsspecificaties wordt voldaan (en daarmee impliciet ook aan de eisen en verwachtingen van de organisatie):
- het implementeren van corrigerende maatregelen en het controleren van de doeltreffendheid ervan;
- het communiceren van verbeteringen.

Effectief vereistenbeheer garandeert de naleving van wettelijke, contractuele en andere vereisten en

zorgt ervoor dat schendingen van wettelijke, regelgevende, contractuele en andere verplichtingen met betrekking tot informatiebeveiliging worden vermeden.

Een positieve beoordeling van het ISMS en de informatiebeveiliging die hiermee wordt bereikt, zorgt ervoor dat ze op de juiste manier worden geïmplementeerd en worden uitgevoerd in overeenstemming met bedrijfsrichtlijnen, processen en relevante vereisten.

3.3.2.3 Beheer van het toepassingsgebied

Bij het toepassingsgebied van een ISMS moet altijd rekening gehouden worden met de informatiebeveiligingsvereisten van de organisatie. Het toepassingsgebied moet daarmee in overeenstemming worden ontwikkeld. Overeenkomstige wijzigingen moeten zorgvuldig worden gepland en geïmplementeerd en documentatie en motivering, waaruit blijkt dat het voldoet aan de strengste industrienormen voor het toepassingsgebied, moeten worden bewaard.

3.3.2.4 Beheer van informatiebeveiligingsrichtlijnen

Als basis voor een ISMS moet de aandacht van het management gericht zijn op informatieveiligheid. Het doel is dat het management richting geeft en dat de beschermende doelen in verhouding staan tot de vereisten van de organisatie en de relevante wetten en voorschriften.

Om te voldoen aan de stand van de techniek, moeten informatiebeveiligingsbeleid en informatiebeveiligingsdoelstellingen in de vorm van een richtlijn worden gedefinieerd en binnen de organisatie kenbaar worden gemaakt. Bovendien moeten er voldoende middelen beschikbaar worden gesteld en moet het belang van het voldoen aan de eisen worden uitgedragen. Het leidende beginsel (met inbegrip van de informatiebeveiligingsdoelstellingen) moet ten minste eenmaal per jaar worden gecontroleerd om ervoor te zorgen dat ze up-to-date zijn en zo nodig worden verbeterd.

3.3.2.5 Risicobeheer

Risicomanagement bestaat uit systematische risicobeoordeling en identificatie, monitoring en behandeling van risicogebieden. Het doel is om systematisch kansen en risico's voor de organisatie te identificeren en deze risico's te beoordelen aan de hand van de waarschijnlijkheid dat ze zich zullen voordoen en hun kwantitatieve effecten op de bedrijfswaarden.

Voor state-of-the-art risicomanagement moeten richtlijnen worden opgesteld om de waarden, zwakke punten, bedreigingen, effecten en waarschijnlijkheid van gebeurtenissen op de organisatie en de toelaatbare omvang van het restrisico te bepalen. De methodologie voor het implementeren van risicobeoordeling en -behandeling en het aannemen van restrisico's door het hoger management, moet ook worden vastgesteld.

Op basis hiervan moeten bestaande risico's worden geanalyseerd, beoordeeld en behandeld. Restrisico's moeten op een aantoonbare manier door het hoger management worden opgepakt en de algehele risicoblootstelling van de organisatie moet voortdurend worden geoptimaliseerd. Verdere details worden uitgelegd in het hoofdstuk Beheer van informatiebeveiligingsrisico's.

3.3.2.6 Beheer van Verklaring van toepasselijkheid

Een verklaring van toepasselijkheid moet voortdurend zijn bijgewerkt en waarin wordt vastgelegd welke controls van bijlage A van ISO 27001 (en indien van toepassing ook andere beveiligingsmaatregelen) van toepassing zijn en welke niet, en ook de redenen voor dit besluit en een beschrijving van de wijze waarop deze maatregelen moeten worden geïmplementeerd. De verklaring van toepasselijkheid toont een actueel beeld van de beoogde en actuele staat van de informatiebeveiliging in de organisatie in de relevante beoordelingscyclus en in overeenstemming met de stand van de techniek.

3.3.2.7 Middelenbeheer (resource management)

De organisatie moet bepalen welke middelen nodig zijn voor de ontwikkeling, implementatie, onderhoud en voortdurende verbetering van het ISMS en voortdurend de werkelijke vereisten bijsturen.

State-of-the-art praktijken vereisen dat de verstrekte middelen ten minste voldoen aan de basisvereisten.

3.3.2.8 Beheer van kennis en competentie

Om een ISMS professioneel te beheren, moeten de personen die ervoor verantwoordelijk zijn de bijbehorende competenties hebben of door middel van verdere opleiding tot dit niveau worden opgeleid. Om te voldoen aan state-of-the-art moet de behoefte aan kennis en competenties worden bepaald, moeten bijbehorende competenties worden verworven en moet de werkelijke behoefte voortdurend worden bijgewerkt.

3.3.2.9 Beheer van documentatie en communicatie

Het doel hierbij is om zowel de beoordelingen als de actuele staat van het ISMS en de informatiebeveiliging te documenteren, inclusief het behalen van doelen, hoe met risico's wordt omgegaan en hoe aan eisen wordt voldaan en dit te communiceren naar belanghebbenden, rekening houdend met de eisen van doelgroepen.

Om te voldoen aan de stand van de techniek, moet de nodige documentatie worden gemaakt en aantoonbaar worden gecommuniceerd voor alle controls die worden gecontroleerd.

3.3.2.10 Beheer van IT-diensten

IT-Dienstenbeheer (IT-Service management) biedt een aanpak op alle IT-beheerniveaus en op alle feitelijke niveaus, te beginnen met bedrijfsoriëntatie, servicemethodologie en informatiebeveiliging, tot implementatie en infrastructuurbeheer en het gebruik van technologie die hiermee samenhangt. Het is belangrijk om het beveiligingsproces te verankeren in het proceslandschap van de organisatie.

Naast de in het TeleTrusT-document Informationssicherheitsmanagement - Praxisleitfaden für Manager beschreven interfaces en processen moeten, om te voldoen aan de modernste praktijken, de volgende processen worden gevolgd.

3.3.2.11 Middelenbeheer (Asset management

Middelenbeheer beschrijft drie aspecten die voor de waarden van de organisatie van belang zijn en vormt de basis voor de analyse en beoordeling van risico's (zie ook 3.3.2.5): verantwoordelijkheden, classificatie en omgang van media.

Om verantwoordelijkheden te bepalen, worden bedrijfswaarden geïdentificeerd en wordt een passende verantwoordelijkheid voor bescherming gedefinieerd. Zodra de waarden en rollen van verantwoordelijkheid zijn gedefinieerd, moet aan de hand van de classificatie ervoor worden gezorgd dat de informatie onderworpen is aan een passend beveiligingsniveau en dat in verhouding staat tot het belang ervan voor de organisatie. Een richtlijn voor het omgaan met media zorgt ervoor dat ongeoorloofde verspreiding, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen, wordt vermeden.

3.3.2.12 Training en bewustwording

Het gevoelig maken van medewerkers voor IT-beveiliging is een belangrijke voorwaarde voor de implementatie van het gewenste beveiligingsniveau. Medewerkers moeten weten hoe belangrijk informatiebeveiliging is voor de organisatie en hoe zij persoonlijk kunnen bijdragen aan het bereiken van dit doel. Ze moeten ook weten hoe ze zich moeten gedragen als ze een beveiligingsincident vermoeden of ontdekken. Om deze taken doeltreffend te kunnen uitvoeren, moeten de medewerkers periodiek in het belang van de informatiebeveiliging worden opgeleid, zodat zij op de hoogte zijn van alle relevante organisatorische en technische omstandigheden. Training helpt medewerkers om (IT-)systemen goed te bedienen en om te voldoen aan alle benodigde regelgeving. Deze aspecten moeten, indien van toepassing, worden gecontroleerd als onderdeel van het middelenbeheerproces (zie 3.3.2.7).

3.3.2.13 Operatie

De werking van een beveiligingsorganisatie en -omgeving dient om alles wat nodig is om het netwerk, computer- en serversystemen, applicaties en oplossingen in een veilige en beschermde staat te houden, te onderhouden. Het zorgt ervoor dat medewerkers, applicaties en servers de juiste toegangsrechten hebben voor de bronnen die ze nodig hebben en dat monitoring, audits en rapportage worden gecontroleerd. De bediening vindt plaats na implementatie en systeemtesten en zorgt voor continu onderhoud, updates en monitoring.

Referentiemodellen en IT-dienstenbeheer (zoals ITIL) bieden een kader voor een succesvolle werking, hierdoor kunnen processen voor informatiebeveiligingsbeheer nauw worden gecoördineerd met andere IT-processen.

3.3.2.14 Incidentbeheer

Incidentbeheer combineert technische en organisatorische maatregelen als reactie op geïdentificeerde of potentiële beveiligingsincidenten. Naast het opsporen, analyseren en beheren van zwakke punten, problemen en gerichte aanvallen, worden ook methoden beschreven en gepland om met dit soort incidenten om te gaan en waarbij ook organisatorische en juridische overwegingen zijn opgenomen. Het doel van incidentbeheer is het bevorderen van het identificeren, plannen en implementeren van vereisten, zodat in het geval van een incident zonder vertraging effectieve en efficiënte maatregelen kunnen worden geïmplementeerd ter bescherming van de organisatie.

3.3.2.15 Continuïteitsbeheer

In het kader van continuïteitsmanagement worden technische en organisatorische maatregelen om operationele storingen te voorkomen samengevat.

Naast het vastleggen, analyseren en beheren van de risico's op falen en het, langs de tijdlijn, beschrijven van de effecten daarvan, plant het ook hoe, in voorkomende situaties, om te gaan met de escalatie van incidenten, inclusief organisatorische en juridische kwesties.

Het doel van continuïteitsbeheer is het bevorderen van het planning, identificeren en implementeren van vereisten, zodat in geval van nood zonder vertraging effectieve en efficiënte maatregelen kunnen worden geïmplementeerd ter bescherming van de organisatie.

3.3.2.16 Aanschaf (procurement)

Voorafgaand aan de daadwerkelijke aanschaf van IT-systemen of -diensten zijn er enkele voorbereidende stappen die moeten worden genomen om ervoor te zorgen dat het resultaat voldoet aan de vereisten van de organisatie. Dit geldt voor aspecten die zowel betrekking hebben op inhoud als op beveiliging; deze punten omvatten:

- analyse van de gestelde eisen (requirements);
- analyse van de risico’s;
- analyse van de beveiligingseisen (eisen met betrekking tot functie en betrouwbaarheid);
- test- en acceptatieplan.

Als leveranciers op langere termijn betrokken zijn bij het leveren van software, oplossingen of diensten, dan moet ervoor worden gezorgd dat bedrijfsmiddelen, die toegankelijk zijn voor leveranciers, gegarandeerd worden beschermd. Dit omvat met name het dienstenleveringsniveau en het beveiligingsniveau zoals beschreven in de leveranciersovereenkomsten.

3.3.2.17 Software-ontwikkeling en IT-projecten

IT-projecten moeten vanaf het begin het probleem van informatiebeveiliging transparant en kwantificeerbaar aanpakken. Binnen organisaties moeten projectorganisaties toe naar een meer rigoureus en herhaalbaar proces dat in elke fase de kwestie van beveiliging als basiscomponent omvat en in elke fase van het project bindende verantwoordelijkheden voor de beveiligingsmanager bepaalt. Deze doelstellingen moeten door de bedrijfsleiding worden versterkt en gelegitimeerd. Met name tijdens faseovergangen moet een formele regel voor goedkeuring worden ingesteld om het verplichte aspect van secure by design in het IT-proces te benadrukken.

De ervaring leert dat het beveiligingsteam in het bijzonder in de plannings- en implementatiefase nauw moet samenwerken met het projectteam. Het beveiligingsteam moet aanvullende beveiligingsvereisten, een bindende beveiligingsarchitectuur definiëren en een dreigingsanalyse uitvoeren. De resultaten worden vervolgens verwerkt in het totaalconcept, waardoor dure correcties in latere fasen van het project worden voorkomen (zie hoofdstuk 3.3.3).

3.3.2.18 Prestatiebewaking

Dit proces omvat alle monitoring-, meet-, analyse- en beoordelingsactiviteiten met betrekking tot het ISMS en de informatiebeveiliging die in dit verband wordt geproduceerd. Deze moeten worden gecontroleerd en geïnspecteerd op naleving van stand van de techniek. Dit betekent onder andere het vastleggen en regelmatig evalueren van protocollen, maar ook het op gezette tijdstippen uitvoeren van interne audits en technische systeemaudits om informatie te verkrijgen over de vraag of het ISMS en de daardoor geproduceerde informatiebeveiliging (nog) voldoen aan de eisen geïmplementeerd en effectief zijn en worden gehandhaafd. Het hoogste managementniveau moet het ISMS ten minste eenmaal per jaar evalueren om te bepalen of en in welke mate het zijn gedefinieerde doel vervult en bijdraagt aan de implementatie van informatiebeveiligingsdoelstellingen. Dit vormt de basis voor verdere beslissingen.

Technische systeemaudits, interne en externe audits kunnen worden beschouwd als subprocessen (zie hieronder) van het hier besproken proces. Hetzelfde geldt voor alle andere categorieën van monitoring-, meet-, analyse- en beoordelingsactiviteiten.

3.3.2.19 Technische systeemaudits

Technische systeemaudits (inspecties op netwerk-, systeem- en applicatieniveau) moeten regelmatig door of namens de organisatie worden uitgevoerd. Deze audits worden meestal uitgevoerd als penetratietests of als web controls:

- Voor een kleine penetratietest worden willekeurig, met betrekking tot beveiliging, beleid en configuraties in de gebruikte IT-systemen, onderzocht in de vorm van een technische controle en

worden aanbevelingen gegeven voor het elimineren van eventuele kwetsbaarheden. De inspectie van het IT-systeem wordt samen met de beheerders uitgevoerd.
- Voor een uitgebreide penetratietest worden, naast de technische audit, kwetsbaarheden in de geteste IT-systemen verwijderd door middel van technisch onderzoek met behulp van onder andere speciale beveiligingstools. Daarbij krijgen de testers, onder toezicht van de beheerders, toegang tot de IT-systemen om ter plaatse te inspecteren.
- Met een informatiebeveiliging web check wordt de beveiligingsstatus van de internet-, intranet- en/of extranet aanwezigheid van de organisatie geïnspecteerd. In dit proces wordt het merendeel van de tests met behulp van geautomatiseerde methoden e via internet uitgevoerd en, indien van toepassing via het interne netwerk (voor intranet en extranet).

3.3.2.20 Interne en externe controles (audits)
ISMS-certificatie en ISMS-audits dienen de volgende doelen:

- Het controleren van de voortgang van de implementatie van het ISMS
- Het bepalen van het, met de auditcriteria van de organisatie, naleven van de ISMS.
- Het bepalen van het vermogen van het ISMS om te voldoen aan wettelijke, regelgevende en contractuele vereisten.
- Het controleren van het gebruik en de effectiviteit van de ISMS.
- Het identificeren van kwetsbaarheden in en potentieel voor verbetering van het ISMS.

Binnen het toepassingsgebied van het ISMS moeten interne audits in de regel ten minste eenmaal per jaar door of namens de organisatie worden uitgevoerd. Om aan de stand van de techniek te voldoen, wordt elke organisatie-eenheid of elk onderdeel van het toepassingsgebied, zoals locatie, gebouw, enz., minstens eens in de drie jaar intern gecontroleerd.

Externe ISMS-audits worden uitgevoerd door partijen die betrokken zijn in de organisatie (zoals klanten met second party audits) of door externe, onafhankelijke auditororganisaties (third party audits).

Als onderdeel van het uitvoeren van ISO 27001-certificeringsaudits controleert het auditteam of aan de vereisten van ISO 27001 wordt voldaan, die eisen moeten worden geïmplementeerd met inachtneming van de normen uit ISO 27002 en ISO 27005. Auditors van certificatie-instellingen zijn, in de loop van de auditprocedure, verplicht om te voldoen aan de ISO 19011- en ISO 27007-normen. ISO/IEC TR 27008 bevat een handleiding voor het controleren van ISMS-controles en is eveneens van toepassing.

De certificatie-instelling voert als onderdeel van een certificeringsprocedure de volgende taken uit:

- het controleren van de auditresultaten, inclusief auditconclusies;
- het documenteren van de beoordeling van de auditresultaten, inclusief auditconclusies;
- het leveren van een certificeringsrapport met certificaatgoedkeuring;
- de afgifte van het certificaat.

Voor ISO 27001 geaccrediteerde certificatie-instellingen hebben accreditatie volgens ISO 17021 en ISO 27006 Een overzicht van in Duitsland geaccrediteerde instellingen voor ISMS-certificering is te vinden op de website van de nationale accreditatie instantie (DAkkS).

Certificering volgens ISO 27001 is drie jaar geldig en wordt als onderdeel van bewakingsaudits ten minste eenmaal per jaar opnieuw beoordeeld. Als het certificaat na drie jaar wordt verlengd, moet voordat de periode is verstreken de organisatie van drie jaar met succes slagen voor het her-certificering-audit.

3.3.2.21 Verbetermanagement (doorgaand verbeterproces)
De organisatie moet de adequaatheid, geschiktheid en effectiviteit van hun ISMS voortdurend verbeteren. De essentiële activiteiten met betrekking tot onderhoud en voortdurende verbetering van het ISMS zijn bedoeld om de ISMS-prestaties te evalueren en voortdurend te optimaliseren. In het bijzonder moeten hierbij de volgende aspecten aan de orde komen:

- het omgaan met non-conformiteiten als gevolg van het monitoren, meten, analyseren en beoordelen van het ISMS en de informatiebeveiliging die in dit kader wordt geproduceerd;
- het definiëren en implementeren van corrigerende maatregelen om de oorzaak van non-conformiteiten weg te nemen;
- het voortdurende verbeteren van de adequaatheid, geschiktheid en effectiviteit van het ISMS en de informatiebeveiliging die het oplevert.

3.3.3 Veilige softwareontwikkeling (Secure Software Development, SSD)

De beveiliging van een applicatie moet gedurende het hele softwareontwikkelingsproces worden overwogen. Ongeacht de gebruikte ontwikkelingsmethode moet rekening worden gehouden met maatregelen voor veilige applicatieontwikkeling. Procedurele modellen en best practices voor veilige softwareontwikkeling worden beschreven in BSIMM, OWASP SAMM, OWASP ASVS, BSI Leitfaden zur Entwicklung sicherer Webanwendungen en ISO/IEC 27034 en onderwezen in TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E). In de afzonderlijke hoofdstukken worden de essentiële beschermende maatregelen voor het softwareontwikkelingsproces vermeld.

3.3.3.1 Behoefteanalyse (Requirements analysis)

Veilige applicatieontwikkeling begint met een analyse van de behoeften. De basis van de behoefteanalyse is een dreigingsanalyse. De te beschermen (bedrijfs-)middelen en de bedreigingen die voor deze activa bestaan moeten worden gedefinieerd en worden beschreven. Er moet rekening worden gehouden met de architectuur van de applicatie, met name de gegevensstromen en het bewaren van gegevens en met hun betrouwbaarheidsgrenzen. De risico's van deze geïdentificeerde bedreigingen moeten vervolgens worden beoordeeld en voor de toepassing moeten tegenmaatregelen en beveiligingsvereisten worden afgeleid. Een nuttige methode voor het identificeren van concrete bedreigingen is een definitie van zogenaamde misbruikgevallen. Deze beschrijven zowel concrete aanvallen als het gewenste gedrag van de applicatie in het geval van een aanval. Verdere veiligheidseisen voor de applicatie vloeien bijvoorbeeld voort uit wettelijke voorschriften of contractuele verplichtingen. Net als de functionele vereisten werken deze beveiligingsvereisten door in de daaropvolgende ontwerpfase van het softwareontwikkelingsproces en ook in de specificatie van de testcases voor de latere tests van de toepassing.

Het Volere-sjabloon[19], dat vaak wordt gezien als de standaard voor de algemene vereistenspecificatie, definieert al een aantal beveiligingsvereisten waarmee rekening moet worden gehouden:

- 15a toegangseisen;
- 15b integriteitseisen;
- 15c privacy eisen;
- 15d auditeisen;
- 15e immuniteitseisen.

3.3.3.2 Software ontwerp

Om de geïdentificeerde bedreigingen tegen te gaan moet een veilig ontwerp rekening houden met alle beveiligingsvereisten. Een resultaat van het ontwerpproces is de beveiligingsarchitectuur en een dataverwerkingsstrategie. Een veilig ontwerp houdt rekening met aspecten zoals veilige authenticatie, cryptografische vereisten, foutafhandeling, systeemconfiguratie, vertrouwensrelatie tussen applicatiecomponenten en de bedrijfslogica van de applicatie. Onvoldoende aandacht voor veiligheid bij het ontwerp van een applicatie is vaak de oorzaak van zwakke punten in de applicatie, zoals ontbrekende of onjuiste authenticatie en autorisatie, en kan achteraf alleen met grote inspanning worden verholpen. Andere oorzaken zijn in de code zijn ingebouwde codesleutels en wachtwoorden, onjuiste verwerking van gevoelige gegevens en onveilige foutafhandeling, waarmee de aanvaller nuttige informatie wordt geboden.

Het naleven van Secure Design principes helpt de architect om een robuust ontwerp voor zijn toepassing te maken. Voorbeelden van dergelijke bewezen ontwerpprincipes zijn Least Privilege, Defense in Depth en Secure by Default. Ontwerpprincipes zoals Privacy by Default worden steeds belangrijker, vooral in relatie tot de AVG. Daarnaast kan een architect gebruik maken van zogenaamde ontwerppatronen en best practices op het gebied van veiligheid die, in tegenstelling tot ontwerpprincipes, een meer concrete, maar taalonafhankelijke benadering bieden voor het oplossen van terugkerende problemen. Het ontwerp, of ten minste de ontwerpaspecten die relevant zijn vanuit veiligheidsoogpunt, moeten worden onderworpen aan een ontwerpbeoordeling voordat de implementatie van de aanvraag begint.

3.3.3.3 Implementatie

Typische implementatiefouten, zoals het ongecontroleerd verwerken van invoer, het exporteren van deze gegevens en het mengen van code en gegevens, kunnen leiden tot beveiligingskwetsbaarheden zoals injecties, cross-site scripting en bufferoverflows. Specifieke programmeerrichtlijnen helpen ontwikkelaars om zich al tijdens de implementatie te concentreren op beveiliging. Deze richtlijnen moeten individueel worden afgestemd op de gebruikte programmeertalen, bibliotheken en frameworks. Bij het gebruik van frameworks moeten deze, om hun beveiligingsfuncties niet te ondermijnen, correct

[19] https://www.volere.org/templates/volere-requirements-specification-template/

worden gebruikt. Zo kan bijvoorbeeld worden aangegeven dat bepaalde functies en objecten pas mogen worden gebruikt, of dat softwaremodules alleen mogen worden ingeschakeld na succesvol met een code-analysetool te zijn getest. Met behulp van statische codecontroles moet de broncode geautomatiseerd worden gecontroleerd op typische implementatiefouten. De broncode of ten minste de beveiligingsrelevante delen van de broncode (volgens de resultaten van de dreigingsanalyse) moeten bovendien aan een handmatige code review worden onderworpen.

Zwakke punten in de applicatie kunnen echter ook het gevolg zijn van het gebruik van onveilige componenten van andere fabrikanten. Daarom moeten dergelijke onderdelen zorgvuldig worden geselecteerd en moeten de beveiligingsbulletins, die door deze leveranciers worden gepubliceerd, en de CVE-database met bekende kwetsbaarheden voortdurend worden gecontroleerd. Dergelijke controles van componenten van derden moeten geautomatiseerd worden uitgevoerd met behulp van een afhankelijkheid controlerende tool. Wanneer programma's, zoals containeroplossingen, worden gebruikt om de toepassing te implementeren, dan moeten ook deze worden gecontroleerd op bekende beveiligingsproblemen.

3.3.3.4 Software tests

Met behulp van blackbox/greybox/whitebox tests en statische en dynamische security scans wordt gezocht naar kwetsbaarheden in de applicatie. Om de hoogst mogelijke efficiëntie te bereiken, moet - voor zover van toepassing - de voorkeur worden gegeven aan een combinatie van blackbox, greybox en whitebox-tests en aan statische en dynamische beveiligingsscans. Zo kunnen de gebruikte versleutelingsalgoritmen eenvoudig door middel van statische analyse van de broncode worden geïdentificeerd en geëvalueerd, terwijl beveiligingsgaten die voortvloeien uit integratie van verschillende componenten of alleen tijdens runtime (zoals in communicatie met een authenticatiedienst) door middel van dynamische scans van het systeem goed worden gedetecteerd. In tegenstelling tot handmatige penetratietests, kunnen beveiligingsscans als onderdeel van het softwareontwikkelingsproces worden geautomatiseerd om een beveiligingsaudit van elke softwareversie te garanderen. Bovendien moeten de vereiste beveiligingsmaatregelen van de applicatie tijdens de testfase worden gecontroleerd, d.w.z. de mate waarin de applicatie is beschermd tegen de aanvallen die in de dreigingsanalyse zijn geïdentificeerd. Een goede bron voor het maken van testcases zijn de gedefinieerde misbruikgevallen (defined abuse cases).

Deze beveiligingstests geven echter geen absolute zekerheid over de beveiliging van de applicatie. Veiligheid kan niet, zoals bij functionaliteitstests, worden vastgesteld op basis van verwacht gedrag komt overeen met waargenomen gedrag. Veiligheid is een negatief criterium; Het bestaat meestal uit het voorkomen van ongewenst gedrag. De creativiteit van een aanvaller is bijna oneindig; er kunnen dus nog meer dreigingen zijn en dus ook meer testcases waar nog geen rekening mee is gehouden. Toch zijn beveiligingstests een belangrijk onderdeel van het veilige softwareontwikkelingsproces.

3.3.3.5 Bescherming van source code en resources

Om de integriteit van code en bronnen te behouden en zo de applicatie te beschermen tegen manipulatie zoals backdoors, Trojaanse paarden en wijzigingen in de logica van de processtroom, moeten broncode-beheersystemen worden gebruikt en, zo nodig, mogen afzonderlijke codeonderdelen alleen aan specifieke ontwikkelaars worden toegewezen. Gevoelige informatie mag niet worden opgeslagen in broncode-controlesystemen om te voorkomen dat deze onbedoeld publiekelijk wordt. Daarnaast moet een veilige ontwikkelomgeving worden gewaarborgd door onder andere toegangsrechten te beperken en systemen te harden, ervoor te zorgen dat ontwikkelaars alleen persoonlijke gebruikersaccounts gebruiken en niet met beheerrechten werken en dat zij getraind zijn in beveiliging.

3.3.3.6 Software certificatie

Voorafgaand aan de levering van de software is het zinvol om deze te laten controleren en certificeren door een neutrale instantie. Hoewel de functionaliteit van de software door tests is gewaarborgd, zorgt certificering ervoor dat de architectuur, behoeftebeheer, configuratiebeheer en risicobeheer geschikt zijn voor een veilig ontwikkelings- en vooral probleemoplossingsproces.

Om later zwakke punten te kunnen elimineren, moeten architectuur en ontwerp zo worden ontworpen dat niet alleen bugs kunnen worden geëlimineerd, maar in geval van nood ook defecte componenten kunnen worden vervangen.

Vereistenbeheer is essentieel voor complexere software. Voor oplevering moeten de eisen (opnieuw) worden gecontroleerd of ze duidelijk volgens IREB (International Requirements Engineering Board) zijn gedefinieerd. De implementatie van eisen moet herleidbaar zijn tot de broncode. In het eenvoudigste geval kan dit worden gedaan door ID's toe te wijzen, die vervolgens ook worden gebruikt in code

comments. Dit maakt het mogelijk om snel te reageren op zwakke punten die bekend worden.

Configuratiebeheer is nauw verbonden met vereistenbeheer. Hier moet worden gecontroleerd of een softwareversie met broncode en alle bijbehorende documenten duidelijk kan worden toegewezen aan een versiestatus (en later aan een softwarerelease). Wanneer eisen worden gewijzigd, moet duidelijk zijn welke documenten al een nieuwe status hebben en welke rekening houden met de vereisten en welke niet. Omdat documenten individueel verder worden ontwikkeld, hebben documenten meestal verschillende versies, daarom moet naast versiebeheer van de documenten ook een zogenaamde baseline worden gedefinieerd, die bepaalt welke documenten in welk versienummer bij elkaar horen en dus overeenkomen met een release. Dit maakt het mogelijk om te zien welke fouten en zwakheden in welke softwareversie zijn gecorrigeerd.

In de eerste stap dient risicomanagement om je bewust te maken van mogelijke risico's en gevaren die zich onder andere kunnen voordoen door zwakke punten. Risicobeheer is vooral essentieel wanneer mensenlevens in gevaar kunnen worden gebracht. In het geval van softwarecertificering moet vóór de levering worden gecontroleerd of een risicobeheersysteem aanwezig is dat

- risico's identificeert;
- risico's indeelt naar waarschijnlijkheid van optreden en ernst;
- risicobeperkende maatregelen definieert;
- de risico's te opnieuw classificeert nadat de maatregelen zijn geïmplementeerd;
- met regelmatige tussenpozen en in geval van wijzigingen wordt voortgezet.

Als de software in een systeemverband wordt uitgevoerd, moet ook het hele systeemverband worden gecertificeerd.

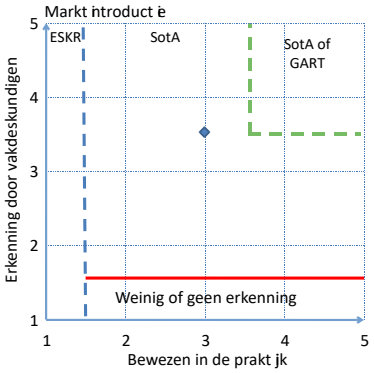
3.3.3.7 Software delivery

Een kwetsbaarheid in de levering en setup van de software vernietigt het resultaat van alle eerdere beveiligingsmaatregelen in het softwareontwikkelingsproces. Daarom moet, om te voorkomen dat de productieve toepassingsomgeving wordt aangetast, een veilig levering- en implementatieproces de integriteit van de geïmplementeerde software waarborgen. Hiervoor kunnen codehandtekeningen worden gebruikt. Aanvallen op de geïmplementeerde applicatie kunnen ook mogelijk zijn door een onveilige configuratie van de applicatie zelf. Daarom moet een veilige configuratie van de software in de productieomgeving worden gewaarborgd en moeten ongeoorloofde wijzigingen in de configuratie worden voorkomen. Als beveiligingsmaatregelen zijn hier geschikte standaardinstellingen (Secure by Default) en handleidingen voor beheerders beschikbaar. Om de potentiële schade van een aanval te minimaliseren, moet de applicatie zo min mogelijk rechten hebben (Least Privilege). Vooral in containeromgevingen worden applicaties vaak onnodig uitgevoerd als rootgebruiker, wat ten koste van alles moet worden vermeden. Ook voor de beveiliging van de applicatie zelf is het essentieel dat deze altijd met beveiligingsupdates up-to-date wordt gehouden.

3.3.3.8 Beveiligingsreactie (Security response)

Aangezien zwakke punten nooit volledig kunnen worden uitgesloten, moet elke fabrikant voorbereid zijn op dergelijke meldingen en snel kunnen reageren. Het zogenaamde Security Response Process van een fabrikant beschrijft zijn aanpak bij het omgaan met beveiligingsproblemen die bij hem bekend zijn geworden. Beveiligingspatches zijn tijd-kritisch en moeten daarom snel worden geleverd. Dit omvat zowel zelf ontwikkelde componenten als bekende kwetsbaarheden in standaardsoftware zoals bibliotheken en frameworks. Om beveiligingsonderzoekers te motiveren om de kwetsbaarheid te melden, zijn Responsible Vulnerability Disclosure of Bug-Bounty programma's beschikbaar. Het is essentieel dat gemelde kwetsbaarheden zodanig terugvloeien in het softwareontwikkelingsproces dat ze worden geëlimineerd.

Stand der techniek classificatie



3.3.4 Proces certificatie

Om informatiebeveiliging en gegevensbescherming met succes binnen de organisatie te implementeren, moeten hiervoor processen worden geïdentificeerd en passende maatregelen worden geïmplementeerd. Het uitvoeren van dergelijke maatregelen zal echter alleen doeltreffend zijn, als de effectiviteit ervan regelmatig wordt geëvalueerd. Deze beoordeling kan worden uitgevoerd door interne en externe bronnen. Een speciaal extern effect, maar niet verplicht voor alle bedrijven, wordt bereikt door certificering volgens de huidige normen. In dit hoofdstuk worden de mogelijkheden van procescertificering beschreven.

Context Informatiebeveiliging

In het kader van informatiebeveiliging kan een ISMS gecertificeerd worden volgens ISO 27001 of (in ieder geval in Duitsland op basis van de BSI IT-Grundschutz).

De ISMS-certificeringsaudits hebben de volgende doelstellingen:

- het controleren van de voortgang van de implementatie van een ISMS;
- het bepalen van de conformiteit van het ISMS met de auditcriteria van de organisatie;
- het bepalen van het vermogen van het ISMS om te voldoen aan wettelijke, regelgevende en contractuele vereisten;
- het beoordelen van de toepassing en effectiviteit van het ISMS;
- het identificeren van zwakke punten/potentieel voor verbetering van het ISMS.

Binnen de scope van het ISMS moeten interne audits (zogenaamde First Party Audits) in beginsel ten minste eenmaal per jaar door of namens de organisatie worden uitgevoerd. Voor ISMS-certificering zijn deze audits verplicht. Elke organisatorische eenheid (of elk onderdeel van het toepassingsgebied zoals locatie, gebouw, enz.) wordt regelmatig onderworpen aan interne audits. In het geval van een interne audit is het essentieel om ervoor te zorgen dat de afdelingen niet zelf auditeren, maar dat de audits altijd worden uitgevoerd door een onafhankelijke persoon.

De zogenaamde second party audits zijn externe ISMS-audits die worden uitgevoerd door partijen die betrokken zijn bij de organisatie (zoals eigen klanten). Als de externe audits worden uitgevoerd door onafhankelijke auditorganisaties, dan worden ze Third Party Audits genoemd. In het geval van een uitbestedingscontract kunnen ook passende leveranciersaudits vereist zijn.

De leverancier (of uitbesteder) kan echter ook aantonen dat aan de informatiebeveiligingseisen wordt voldaan door middel van een geschikt certificaat (zoals ISO 27001 of ISO 27001 op basis van BSI IT-Grundschutz).

Als een ISMS moet worden gecertificeerd, moet de auditprocedure worden uitgevoerd door een geaccrediteerde certificatie-instelling. Certificatie-instellingen voor ISO 27001 hebben een accreditatie volgens ISO 17021 en ISO 27006. Een overzicht van in Duitsland geaccrediteerde ISMS-certificatie-instellingen is te vinden op de website van de Duitse accreditatieinstelling (DAkkS). Het BSI is de verantwoordelijke certificeringsinstantie voor de basisbescherming van de informatica.

Bij de certificeringsaudit controleert het auditteam of wordt voldaan aan de eisen van ISO 27001 of de BSI IT-Grundschutz. Bij ISO 27001 moeten de audits worden uitgevoerd met inachtneming van de normen ISO 27002 en ISO 27005 (en zo nodig met verdere branche specifieke aanvullingen van de normen van de 27-serie). Auditors van certificatie-instellingen voor ISO 27001 zijn verplicht om binnen de auditprocedure de normen ISO 19011 en ISO 27007 in overweging te nemen. Voor audits volgens BSI IT-Grundschutz moet het betreffende geldige certificatieschema van de BSI in acht worden genomen.

Certificeringen volgens ISO 27001 of ISO 27001 op basis van BSI IT-Grundschutz hebben een geldigheidsduur van 3 jaar en worden minimaal één keer per jaar in het kader van zogenaamde surveillance audits gecontroleerd. Om het certificaat na 3 jaar te kunnen laten verlengen, dan moet de organisatie nog voor het einde van de periode van 3 jaar met succes een her-certificeringsaudit hebben doorstaan.

Afhankelijk van de sector kan het zijn dat ook aan zogenaamde sectorspecifieke eisen moet worden voldaan. Daarbij moet worden nagegaan of de relevante sectorspecifieke eisen een bewijs van een gecertificeerd ISMS vereisen. Daarnaast kunnen verdere eisen worden gedefinieerd, die volgens de specificatie moeten worden geïmplementeerd en bewezen. Een overzicht van de gepubliceerde sectorspecifieke normen (voor Duitsland) is te vinden op de website van BSI.

Daarnaast zijn er andere, deels sectorspecifieke normen, standaarden en richtlijnen die ook betrekking hebben op individuele aspecten van informatiebeveiliging (zoals VdS10000, ISIS12, IDW980, HIPAA, EuroCloud Star Audit, CSA CCM en ITIL).

Verdere voordelen die spreken voor ISMS-certificering zijn

- bewijs van passende risicobeoordeling en -behandeling;
- bevestiging van de functionaliteit van het ISMS door onafhankelijke derden;
- bewijs van de continue verbetering van het ISMS;
- vermindering van de aansprakelijkheid in geval van incidenten, omdat naleving van een geharmoniseerde norm in de EU een vermoeden van conformiteit met de erkende technische regels (normen) en de stand van de techniek geeft;
- externe presentatie in het kader van corporate marketing/ voor de reputatie naar anderen toe.

Context Gegevensbescherming
De implementatie van een gegevensbescherming beheersysteem (data protection management system, DSMS) leent zich ook voor het controleren van de effectiviteit van maatregelen in verband met de vereisten van de AVG. Hoewel de AVG een dergelijk systeem niet expliciet voorschrijft, toont het toch op veel plaatsen de noodzaak van een dergelijk systeem aan. AVG: Art. 32 lid 1 sub d[20] vereist bijvoorbeeld een procedure voor de regelmatige toetsing, beoordeling en evaluatie van de doeltreffendheid van technische en organisatorische maatregelen om de beveiliging van de verwerking te waarborgen.

Aangezien een dergelijke procedure een geplande en gestructureerde aanpak binnen de organisatie vereist, d.w.z. implementatie van het klassieke PDCA-model, is het opzetten van een DSMS een logische stap. Als het op hoog niveau is afgestemd op de elementen van de ISO-structuur, dan kan het ook op basis van ISO 27001worden geïntegreerd in een bestaand ISMS.

Net als een ISMS kan ook het DSMS worden gecontroleerd en op deze wijze kan de mate van volwassenheid van een dergelijk systeem worden bepaald. Op basis van de ISO 19011-richtlijnen kunnen audits worden uitgevoerd op basis van een auditprogramma en een auditplan. Een audit kan worden uitgevoerd door de Functionaris Gegevensbescherming. In grotere organisaties kunnen de audits ook worden uitgevoerd door deskundig opgeleide medewerkers van de organisatie of door consulting bedrijven die gespecialiseerd zijn in gegevensbescherming.

In het kader van de zogenaamde leveranciersaudits kunnen ook eventuele contractverwerkers van de organisatie worden gecontroleerd.

Ongeacht het bovenstaande bestaat in de context van gegevensbescherming ook de mogelijkheid van certificering om bewijs te verkrijgen van naleving van de bepalingen van de AVG (zie AVG: Art. 42 lid 1). Volgens AVG: Art. 4 lid 5 moeten echter gegevensbescherming specifieke certificeringsprocedures en gegevensbeschermingszegels en -testmerken eerst op grond van AVG: Art. 43 door geaccrediteerde certificatie-instellingen worden goedgekeurd (in Duitsland bijvoorbeeld de DAkkS) of de bevoegde toezichthoudende autoriteit. Dat is nog niet gebeurd.

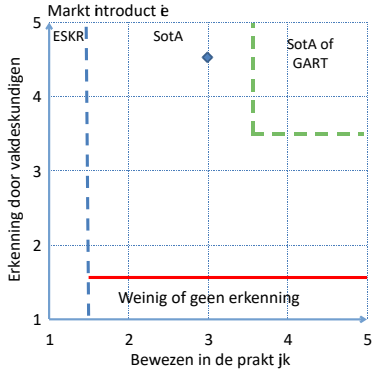
Dergelijke gegevensbescherming specifieke certificeringsprocedures, gegevensbeschermingszegels en -testmerken hebben, zoals blijkt uit de bewoordingen van AVG: Overweging 100, echter alleen betrekking op product-, proces- en dienstencertificering (zie ISO/IEC 17065). In dit verband noemt de AVG zelf bijvoorbeeld

[20] Zie ook AVG: Art. 5 lid 2, DPA "De verwerkingsverantwoordelijke (...) moet (...) de naleving aantonen" en AVG: Art. 24 lid 1 "(...) ervoor te zorgen en het bewijs te leveren (...) dat de verwerking overeenkomstig deze verordening wordt uitgevoerd".

- bewijs van het vervullen van de plichten van een verantwoordelijke persoon (zie AVG: Art. 24 lid 3);
- bewijs van het naleven van het ontwerp van de technologie en gegevensbeschermingsvriendelijke voorinstellingen (zie FADP: Art. 25 lid 3);
- bewijs van voldoende garanties van een verwerker (conform Art. 28, leden 5 en 6);
- bewijs van de veiligheid van de verwerking (zie AVG: Art. 32 lid 3);
- bewijs van passende garanties in verband met gegevensverwerking in een derde land (zie AVG: Art. 46 lid 2, onder f).

Een DSMS kan niet in de zin van de AVG worden gecertificeerd door middel van gegevensbescherming specifieke certificeringsprocedures en gegevensbescherming zegels en testmerken. Niettemin zijn deze aanvullend op een DSMS en kunnen ze in principe bij het controleren van een DSMS in aanmerking worden genomen als bewijs van het naleven van de bepalingen van de AVG.

Stand der techniek classificatie



3.3.5 Beheer van kwetsbaarheden- en patches

Het doel van kwetsbaarheids- en patchbeheer is het identificeren en corrigeren van zwakke plekken in de functionaliteit en beveiliging in firmware en software. Patches zijn bedoeld om geïdentificeerde kwetsbaarheden te elimineren en om misbruik ervan te voorkomen. Het kwetsbaarheids- en patchbeheerproces omvat identificatie, beoordeling, implementatie en evaluatie voor alle producten en systemen van de organisatie. Voor het kwetsbaarheids- en patchbeheerproces moeten de verantwoordelijkheden voor implementatie en effectiviteitstesten binnen de organisatie worden gedefinieerd.

3.3.5.1 Beoordeling (Assessment)

Om patches en kwetsbaarheden efficiënt te beheren, moet eerst het IT-landschap van de organisatie worden geïnventariseerd. Omdat het landschap in de loop van de tijd kan veranderen, moet een dergelijk onderzoek regelmatig worden uitgevoerd en up-to-date worden gehouden. Componenten die zich niet in het interne netwerk bevinden (zoals smartphones en notebooks van serviceproviders) moeten met behulp van speciale richtlijnen worden beheerd. Deze richtlijnen zijn bedoeld om de eigenaren van deze onderdelen aan te moedigen de softwarestatus op hun apparaten zelf bij te werken of om ze regelmatig voor updates te verbinden met het bedrijfsnetwerk.

3.3.5.2 Identificatie en evaluatie

Om kwetsbaarheden, bedreigingen en software fixes te identificeren, moeten relevante informatiebronnen (websites van leveranciers, CERT's, CVSS-databases, mailinglijsten van software- en hardware-leveranciers, nieuwsgroepen van derden, enz.) worden gemonitord, ook moeten professionele tools voor het beheer van bedrijfspatches worden overwogen. Alle verantwoordelijken voor IT-systemen, applicaties, netwerkcomponenten, enz. moeten periodiek een overzicht/samenvatting van de huidige patchstatus geven. Daarmee moet een rapport worden gemaakt voor de evaluatie van de huidige patchsituatie en voor de beoordeling van het huidige risico (zoals CVSS-score). De volgende oplossingen zijn als behandelingsopties beschikbaar:

- De overdracht aan patchbeheer om geïdentificeerde kwetsbaarheden te dichten met een geschikte patch (update).
- Het definiëren van tijdelijke oplossingen (configuratieaanpassing, code-analyse, enz.) om de kwetsbaarheid aan te pakken.
- Het afsluiten of isoleren van het getroffen systeem.

Als, om het beveiligingslek te verhelpen, patches handmatig worden gedownload, moet met behulp van gestandaardiseerde methoden (cryptografische checksums, handtekeningen of digitale certificaten) de authenticiteit ervan worden geverifieerd, in het bijzonder voor downloads vanaf het internet. Patches moeten in de eerste plaats rechtstreeks worden opgehaald vanaf de bronnen van de fabrikant. Alleen in uitzonderlijke gevallen zijn patches van andere vertrouwde bronnen toegestaan (bijvoorbeeld met geïntegreerde producten van derden, zoals runtimebibliotheken).

3.3.5.3 Bevoorrading (Provisioning)

Voorbereiding
Zodra de authenticiteit van de patches is geverifieerd, moeten ze worden geverifieerd in testsystemen. Zo mogelijk moeten de testsystemen op dezelfde of vergelijkbare wijze als het productiesysteem worden uitgerust en geconfigureerd.

Voordat de patches definitief in de productieomgeving worden geïmplementeerd, moet, om herinstallatie van de patches mogelijk te maken in geval van een fout, een back-up van de getroffen systemen worden gemaakt. Als de prestaties ongewenst zijn of als de functionaliteit beperkt is, moeten maatregelen voor probleemoplossing worden geïdentificeerd en uitgevoerd.

Implementatie
Om het uitvoeringsproces goed te laten verlopen, moeten passende voorbereidingen worden getroffen. Dit omvat bijvoorbeeld het informeren van alle systeembeheerders en het definiëren van de voor het implementeren van patches benodigde tijd. De installatie moet ook aan de gebruikers worden aangekondigd, zodat zij tijdig vóór de aangekondigde installatieperiode hun operationele processen kunnen voltooien.

Normaal gesproken moeten patches automatisch worden gedistribueerd (zoals met een Enterprise Patch Management Tool). Het is echter mogelijk dat beheerders afzonderlijke patches lokaal moeten installeren. In dit geval moet de communicatie veilig worden gehouden en moeten bestanden worden uitgewisseld met authenticatiecontrole.

Zodra patches worden uitgerold, moet de voortgang worden gemonitord en gecommuniceerd om bijvoorbeeld mislukte implementatiepogingen tijdig op te sporen en dan moeten onmiddellijk passende corrigerende maatregelen worden genomen.

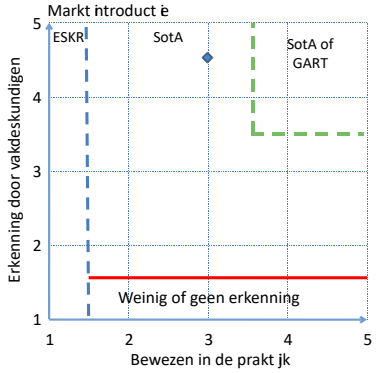
3.3.5.4 Behandeling van uitzonderingen

Niet patchbare systemen
Voor systemen of toepassingen, waarvoor

- updates van de fabrikant niet meer beschikbaar zijn (zogenaamde legacy-systemen);
- door de fabrikant nog geen updates van het besturingssysteem zijn uitgebracht;
- om operationele redenen een onderhoudsvenster niet op korte termijn beschikbaar kan worden gesteld (zoals geautomatiseerd in procestechnologie);
- tijdens een update een her-certificering van het hele systeem noodzakelijk wordt, technische maatregelen moeten worden geïdentificeerd en geïmplementeerd;
  aangezien een uitschakeling of eenvoudige her-configuratie meestal niet compatibel is met de operationele vereisten, moet rekening worden gehouden met het volgende
- scheiding, zonering, inkapseling of applicatie-firewalls; en
- netwerkmonitoring via inbraakdetectiesysteem worden gebruikt om te beschermen tegen en om misbruik van bestaande kwetsbaarheden te detecteren.

Goedkeuring van de fabrikant
Als voor de invoer van patches de goedkeuring van de fabrikant vereist is, zoals bij releases voor het patchen van databases of besturingssystemen, kunnen de meeste beschikbare patches niet worden geïmporteerd omdat een verlies van functionaliteit mogelijk zou zijn en door de fabrikant geen garantie zou worden gegeven. Om deze reden moeten de voorwaarden voor het verstrekken en vrijgeven van patches en updates en voor alternatieve oplossingen voor kwetsbaarheden contractueel met de fabrikant worden overeengekomen.

Stand der techniek classificatie



3.3.6 Beheer van informatiebeveiligingsrisico's

Risicobeheer is een essentieel instrument voor het beheer van bedrijfsrisico's en daarmee de voorwaarde voor het selecteren van passende risico-verlagende beveiligingsmaatregelen. In de praktijk wordt het gebruik van beveiligingsmaatregelen bepaald door het afwegen van de kosten en baten. Om de voordelen te bepalen, moeten beveiligingsrisico's worden geïdentificeerd en geëvalueerd. Een goed en gestructureerd beheersing van informatiebeveiligingsrisico's (ISRM) creëert de nodige transparantie die het management in staat stelt om in deze context passende beslissingen te nemen.

Bovendien is het beheer van informatiebeveiligingsrisico's[21] een kernelement bij de implementatie en herhaalde actualisering van informatiebeveiligingsbeheersystemen (ISMS) of gegevensbeschermingsbeheersystemen (DSMS).

Standaarden

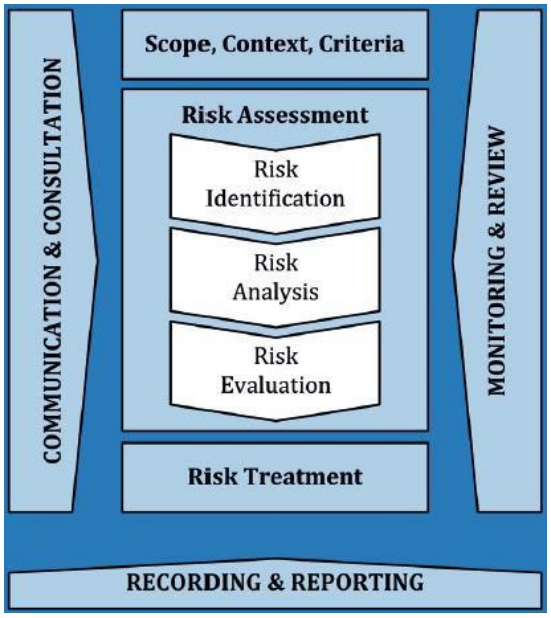
In het algemeen geldt ISO 31000 als de belangrijkste internationale norm voor risicomanagement, terwijl ISO/IEC 27005[22] specifiek van toepassing is op informatiebeveiligingsrisico's. ISO/IEC 27005 sluit nauw aan op ISO 31000, maar bevat aanvullende (niet-normatieve) informatie over de identificatie en evaluatie van activa, voorbeelden van bedreigingen en kwetsbaarheden, en methoden voor risicobeoordeling in het kader van informatiebeveiliging. In Duitsland is de BSI-Grundschutz ook relevant, met name BSI 200-3 (afgekort: BSI-GS). Voor industriële automatiseringssystemen is ook IEC 62443 Part 3-2 voor Security Risk Assessment and System Design beschikbaar.

Afhankelijk van de regelgeving moeten organisaties mogelijk voldoen aan aanvullende specifieke maatregelen, zoals de AVG en de IT-Sicherheitskatalog van het Bundesnetzagentur (IT-SiKat), die beiden aanvullende specificaties voor risicobeheer bevatten. Ook voor individuele sectoren zijn met betrekking tot de IT-beveiligingswet sectorspecifieke beveiligingsstandaarden gedefinieerd, de zogenaamde B3S, en worden aanbevelingen gedaan voor de implementatie van risicomanagement voor KRITIS-exploitanten.

Proces

Risicomanagement is een cyclisch proces (volgens Plan, Do, Check, Act). Naarmate omstandigheden zoals de dreigingssituatie, systeemzwaktes en de technologische omgeving veranderen, moet de risicobeoordeling up-to-date worden gehouden en de effectiviteit ervan worden bewaakt. Afbeelding 1 toont het risicoproces volgens ISO 31000.

[21] In deze zin verwijzen "IT-risico's" en "IT-beveiliging" naar risico's en beveiliging van alle typen informatie en niet alleen elektronisch verwerkte data.
[22] De ISO/IEC 27005 standard is op dit moment in herziening



Afbeelding 7: Risicobeheer proces conform ISO 31000

In de eerste stap (het **creëren van de context**) worden de basisvereisten voor ISRM gemaakt. Allereerst wordt bepaald op welke onderdelen van de organisatie het ISRM van toepassing is; als het ISRM wordt ingevoerd als onderdeel van een ISMS, wordt dit over het algemeen bepaald door het toepassingsgebied van het ISMS. De bedrijfsprocessen die in ISRM moeten worden opgenomen, moeten worden geselecteerd. Op basis van de bedrijfsprocessen wordt gekeken naar de bijbehorende organisatieonderdelen, IT- en OT-systemen en -applicaties, data- en spraakcommunicatiefaciliteiten, dienstverleners en ook vastgoed en gebouwen. Er wordt een ISRM-organisatie met bijbehorende taakverdeling gecreëerd (bijvoorbeeld onder voorzitterschap van een risicomanager), tenzij dit al binnen een ISMS of DSMS is gebeurd. Het is ook raadzaam om, indien beschikbaar, interfaces te definiëren tussen ISRM en centraal bedrijfsrisicobeheer.

Gevaren worden bepaald tijdens de **risico-identificatie**. Gevaren werken tegen waarden (assets/middelen). In een ISRM zijn waarden voornamelijk informatie en in tweede instantie systemen en componenten voor de verwerking en bescherming ervan. Tijdens de risico-identificatie worden de gevaren bepaald aan de hand van de waarden. Volgens de definitie van BSI [Glossary] zijn bedreigingen de interactie van bedreigingen (zoals natuurrampen, pandemieën, inbraak, hackers, criminelen) en zwakke punten (zoals softwarefouten, organisatorische tekortkomingen en technische defecten). De uitdaging is om zoveel mogelijk van deze bedreigingen te identificeren. Gestandaardiseerde gevarencatalogi zoals die in bijlage D van ISO/IEC 27005 of het gevarenoverzicht van het BSI Grundschutzkompendium bieden hierbij ondersteuning. Deze catalogi moeten echter worden aangepast aan de geselecteerde context en bestaande waarden. In dit proces is de samenwerking van informatiebeveiligingsmanagers en technische experts, zoals in een werkgroep, belangrijk.

Risicoanalyse betekent het beoordelen van het gevaar in termen van het potentieel voor schade en de waarschijnlijkheid dat het zich voordoet. Zoals gezegd is het zelden mogelijk om terug te vallen op solide cijfers voor IT-risico's. Ook hier zijn de beoordelingen van technische experts, zo mogelijk uit meerdere disciplines, doorslaggevend. Verliezen kunnen van verschillende aard zijn (zoals financiële verliezen, gevaar voor lijf en leden, aantasting van het aanbod of de productie/productie, reputatieschade, enz.). Aangezien waarschijnlijkheidscijfers onderhevig zijn aan een hoge mate van onzekerheid en schade niet altijd duidelijk kan worden gekwantificeerd, kunnen IT-risico's normaal gesproken niet worden uitgedrukt als een concreet getal (kardinaal), maar eerder binnen een ordinale schaal, bijvoorbeeld hoog, gemiddeld (of midden) en laag. ISO/IEC 27005 Bijlage E biedt nuttige richtlijnen voor dit type classificatie. Een gevaar dat op deze manier wordt geclassificeerd, wordt een risico genoemd.

Risico's moeten worden **beoordeeld** en op passende wijze worden **aangepakt**, en daarvoor bestaan verschillende opties. Men kan ze bijvoorbeeld bewust dragen (accepteren), zich ertegen verzekeren of tegenmaatregelen nemen (zie ISO 31000 hoofdstuk 6.4.4), maar men mag ze niet negeren. Op deze manier wordt een bewuste keuze gemaakt. Deze beslissing moet worden genomen door een persoon die verantwoordelijkheid neemt, of het nu gaat om de kosten van maatregelen of schade wanneer zich

een risico voordoet. Deze persoon wordt meestal de risico-eigenaar genoemd[23]. Om het risico te verminderen, stellen technische deskundigen tegenmaatregelen voor, waarvan de kosten en de vermindering van het risico de basis vormen voor de beslissing om de maatregelen al dan niet uit te voeren. De risico-eigenaar neemt vervolgens het besluit over de uitvoering ervan en het aanvaarden van het restrisico dat overblijft na het implementeren van de maatregelen. Vanwege wettelijke vereisten bij KRITIS-exploitanten of voor het aandachtsgebied van de AVG, is de risico-eigenaar niet volledig vrij om risico's zonder verdere behandeling te accepteren of over te dragen.

Communicatie, **rapportage** (met name richting management) en monitoring zijn ondersteunende processen. Binnen een ISMS of DSMS zijn ze sowieso vastgesteld en moeten ze overeenkomstig op ISRM worden toegepast. Als er een centraal bedrijfsrisico beheersysteem is, is efficiënte communicatie en wederzijdse complementariteit tussen dit systeem en het ISRM belangrijk, en worden criteria voor de escalatie van informatiebeveiligingsrisico's naar het centrale bedrijfsrisico beheersysteem gedefinieerd die voor beide partijen begrijpelijk en aanvaardbaar zijn.

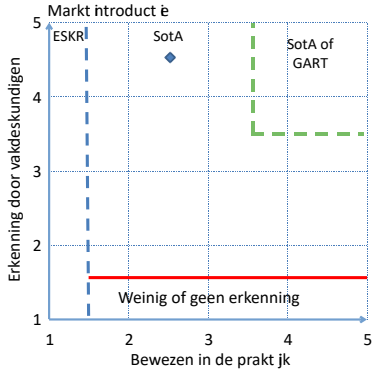
Praktische tips

Het compleet nieuw inrichten van een ISRM is voor organisaties vaak een veelomvattende taak (in termen van tijd en kosten). Net als andere processen is ISRM onderhevig aan een continu verbeteringsproces, wat betekent dat je niet kunt verwachten dat je bij de eerste poging een perfect proces kunt vaststellen. Integendeel, een te zwaarwichtige aanpak kan een last voor de toekomst blijken te zijn: er is dan het gevaar dat het proces op de lange termijn "in slaap valt" of alleen zal worden geïmplementeerd als een formeel noodzakelijk relikwie zonder enig herkenbaar voordeel. In dit opzicht is het raadzaam om in het begin te kiezen voor een pragmatische aanpak, waarbij minder aandacht wordt besteed aan volledigheid dan aan kwaliteit. Het is belangrijk dat risico's met een hoge prioriteit worden geïdentificeerd, geanalyseerd en op passende wijze worden aangepakt, en dat hierover een zo groot mogelijke consensus bestaat onder de beslissende partijen.

De identificatie van bedreigingen en de juiste categorisering ervan zijn op het eerste gezicht bijzonder uitdagend. Hiervoor kunnen standaard dreigingscatalogi zoals die in ISO/IEC 27005 worden gebruikt. Toch is er zelden een duidelijk antwoord op de vraag of de dreiging van blikseminslag onder overmacht moet worden geplaatst en bijvoorbeeld als een groot algemeen risico moet worden behandeld, en of risico's onafhankelijk van elkaar kunnen worden behandeld, d.w.z. of bijvoorbeeld blikseminslag niet samen met het risico van stroomuitval moet worden behandeld. De onderlinge relaties kunnen zo complex worden als je wilt, zodat je bepaalde onnauwkeurigheden moet accepteren. Onnauwkeurigheden spelen sowieso een rol bij het schatten van de waarschijnlijkheid van optreden. Hierbij is het van belang om het doel niet uit het oog te verliezen, namelijk dat de resultaten van de risicoanalyse gebruikt kunnen worden om een begrijpelijke beslissing te nemen of er al dan niet actie nodig is.

Nauwelijks minder moeilijk is het inschatten van waarschijnlijkheden van optreden. Het is raadzaam om zoveel mogelijk externe en interne informatiebronnen te gebruiken. De eerste omvatten CVE[24]-lijsten, leveranciersinformatie, CERT-services (zoals van BSI), en de laatste omvatten de evaluatie van informatiebeveiligingsincidenten, penetratietests, audits of bewustmakingsmaatregelen. De waarden moeten regelmatig, bijvoorbeeld ten minste eenmaal per jaar, worden aangepast aan de huidige situatie.

Stand der techniek classificatie



[23] Met begrip "risico-eigenaar van ISO 27001 wordt, afhankelijk van de verantwoordelijkheid van de betrokken person, vaak de risicomanager of risicodrager bedoeld.

[24] Common Vulnerabilities and Exposures (CVE) is een gestandaardiseerde lijst van kwetsbaarheden en beveiligingsrisico's van computersystemen.

3.3.7 Persoonlijke certificering

De organisatorische maatregelen omvatten onder meer de inzet van gekwalificeerde specialisten. Dit geldt met name voor bedrijf kritische gebieden en kritieke infrastructuren (KRITIS). Alleen op deze manier kan het bedrijfsvermogen worden beschermd en kan worden voldaan aan de vele wettelijk verankerde eisen met betrekking tot het bewijs van kwaliteit van het ingezette personeel.

Door de toenemende verscheidenheid aan technische oplossingen is het noodzakelijk dat alle medewerkers die werkzaam zijn in de IT-sector continu in de basis en innovaties worden bijgeschoold. De medewerkers moeten worden opgeleid en gecertificeerd in overeenstemming met de respectieve activiteit en de vereisten die daaruit moeten worden afgeleid, zowel met betrekking tot de te vervullen rol (zoals beheerder, ontwikkelaar, IT-architect, auditor, informatiebeveiligingsfunctionaris, functionaris voor gegevensbescherming) als met betrekking tot de branche specifieke (zoals telecommunicatie, transport) en oplossing specifieke (zoals on-prem (lokaal geïnstalleerde automatiseringssoftware) en cloud) functies.

Met de persoonlijke certificering wordt de beroepskwalificatie bewezen. Een persoonlijk attest wordt namelijk meestal pas afgegeven nadat een beroepsopleiding is afgerond, en op basis daarvan met goed gevolg het examen is afgelegd.

Afhankelijk van het doel en het toepassingsgebied zijn er verschillende certificeringsprogramma's op de markt. Hieronder vindt u enkele voorbeelden:

Beheerders (Administrators)

- Er bestaan verschillende fabrikantafhankelijke certificeringsprogramma's die gericht zijn op het gebruik, de configuratie en het beheer van het betreffende product.
Het gaat hierbij met name om certificaten van Microsoft, Linux, Oracle, Cisco, IBM, maar ook certificeringsprogramma's van cloud serviceproviders zoals Microsoft, AWS en Google.

Software ontwikkelaars

- TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.) van TeleTrusT.
De focus van de T.P.S.S.E.-certificering ligt op de expertise over hoe en waar beveiligingsaspecten worden geïntegreerd in softwareontwikkeling.
(https://www.teletrust.de/tpsse/)
- Certified Secure Software Lifecycle Professional (CSSLP) van ISC2.
Dit is een leveranciers-neutrale certificering die de expertise van een individu aantoont in het binnen de levenscyclus van softwareontwikkeling implementeren van beveiliging.
(https://www.isc2.org/Certifications/CSSLP)

IT-architecten

- Certified Professional for Software Architecture (CPSA) door iSAQB
De International Software Architecture Qualification Board (iSAQB) is een vereniging van software-architectuurexperts uit de industrie, advies- en trainingsbedrijven, de academische wereld en andere organisaties (https://www.isaqb.org/certifications/)

IT-beveiligingsauditors

- Certified Information Systems Auditor (CISA) door ISACA
CISA is een wereldwijd geaccepteerde certificering op het gebied van audit, controle en beveiliging van informatiesystemen.
- ISO/IEC 27001 lead auditor
Hierbij ligt de focus op het voorbereiden en uitvoeren van een audit van het ISMS. De certificering wordt aangeboden door verschillende aanbieders.
- BSI IT-Grundschutz-Auditor
Certificering om in overeenstemming met de BSI-normen en het BSI IT-Grundschutz compendium audits uit te voeren.

IT-beveiliging experts

- TeleTrusT Information Security Professional (T.I.S.P.) door TeleTrusT
De inhoud van het T.I.S.P.-certificaat omvat de belangrijkste aspecten van informatiebeveiliging, technische en organisatorische maatregelen en Duitse en Europese wetgeving (https://www.teletrust.de/tisp/.
- Certified Information Systems Security Professional (CISSP) door ISC^2
Om het certificaat te behalen, moet expertise op het gebied van veiligheidsrelevante aspecten

uit verschillende gebieden van het zogenaamde Common Body of Knowledge (CBK) worden aangetoond (https://www.isc2.org/Certifications/CISSP).

- Comptia Security+ by Computing Technology Industry Association (COMPTIA)

Dit certificaat richt zich op basiskennis van beveiligingsconcepten en technische en organisatorische maatregelen (https://www.comptia.org/de/zertifizierungen/security).

- Certified Information Security Manager (CISM) door ISACA

De focus ligt op planning, implementatie en controle en monitoring van IT-beveiligingsconcepten voor specialisten en managers (https://www.isaca.de/de/zert-start/international/cism1).

Functionaris Gegevensbescherming (DPO/FG)/Gegevensbescherming Coördinator/Gegevensbescherming Adviseur

- Tot op heden is voor een van de adviserende, ontwerpende en controlerende beroepen op het gebied van gegevensbescherming nog geen certificering beschikbaar volgens een erkende onafhankelijke certificeringsprocedure, door een onafhankelijke certificerende instantie en in overeenstemming met ISO/IEC 17024. Adequate expertise op het gebied van gegevensbescherming is afhankelijk van een groot aantal factoren en kan niet worden overgedragen door een enkelvoudige cursus[25]. Een uitgebreidere opleiding op het gebied van gegevensbescherming wordt aanbevolen, zoals:
- Certified Information Privacy Professional (CIPP)
  De IAPP-training richt zich op gegevensbeschermingswetten, -beleid en -normen in belangrijke internationale rechtsgebieden, de vaardigheden die nodig zijn om gegevensbeschermingsoperaties te beheren en de voorbereiding op het certificeringsexamen (https://iapp.org/train/).

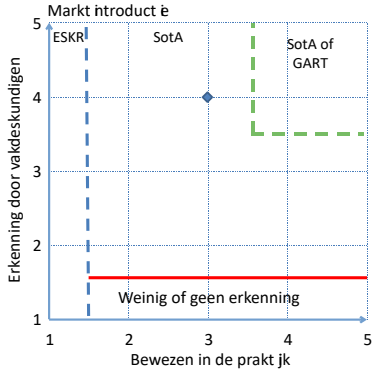
Industrie-specifieke certificaten

- Telecommunications
- Zero-Outage (Geen uitval)
  De inhoud van de Zero-Outage-certificeringen omvat normen en best practices voor het leveren van veilige, betrouwbare en maximaal beschikbare end-to-end IT-diensten en -oplossingen in de telecommunicatiesector (https://zero-outage.com/).
- Transport
- Certificaten voor operationele ICT in spoorwegactiviteiten
  De inhoud van de certificeringen voor operationele ICT in spoorwegactiviteiten omvat normen, standaarden en best practices waarmee rekening moet worden gehouden in IT-projecten en IT-toepassingen bij spoorwegactiviteiten (http://www.hmocs.de/).
- RCS Academie (SBB)
  De inhoud van de RCS Academy-certificeringen omvat de normen, standaarden en best practices waarmee, met name in Zwitserland, rekening moet worden gehouden bij IT-projecten en IT-toepassingen op het gebied van dispatching van spoorwegactiviteiten.

Op de Duitse markt heeft het BSI bovendien een opleidingsreeks voor deskundigen opgezet die zich richt op de BSI IT Grundschutz compendium. Naast de hierboven genoemde auditors zijn dit de BSI IT-Grundschutz-Practitioners en BSI IT-Grundschutz- Advisors[26].
Andere Europese landen hebben hun eigen individuele certificeringsprogramma's die nog niet onderworpen zijn aan uniforme regelgeving. Een overzicht van de certificeringsprogramma's van de Europese landen is samengesteld door de European Cyber Security Organization (ECSO)[27].

[25] BvD, Professional profile of data protection officers, https://www.bvdnet.de/wp-content/uploads/2018/04/BvD-Berufsbild_Auflage-4_dt_en.pdf
[26] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/ITGrundschutzBerater/itgrund-schutzberater.html;jsessionid=3DE1AE0E2759C0AA3373341257ECAC85.1_cid500
[27] https://www.ecs-org.eu/documents/publications/5fad54a94cfac.pdf

Stand der techniek classificatie



3.3.8 Omgaan met providers

Het uitbesteden van diensten kan voordelig zijn als dienstverleners gerichter, innovatiever en beter of goedkoper zijn dan de klant bij het verlenen van de opdracht of een speciale technologie in gebruik hebben.

Het inschakelen van dienstverleners gaat echter soms gepaard met niet onaanzienlijke risico's (zoals: afhankelijkheid, verlies van controle en sturingsopties en risico's voor de informatiebeveiliging). In het ergste geval kunnen deze risico's het voortbestaan van de klant in gevaar brengen. Hoe vertrouwelijker, kwetsbaarder of beperkter (zoals veiligheid en gegevensbescherming) de gegevens, hoe groter het risico. Tegen deze achtergrond zijn de selectie, controle, monitoring en toetsing van dienstverleners als organisatorische maatregel van centraal belang.

Het uitbesteden van diensten (zoals netwerkbeheer) gaat gepaard met verschillende bedreigingen voor de IT-veiligheid, zoals:

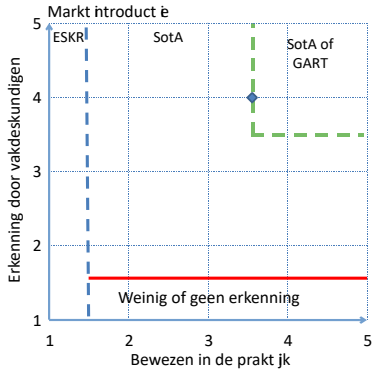
- Inbreuk op de beveiliging die resulteert in de vernietiging, het verlies, de wijziging of ongeoorloofde openbaarmaking van of toegang tot gegevens.
- Niet-contractuele of ongepaste verwerking door derden van de verstrekte gegevens met het oog op de uitvoering van het contract.
- Misbruik van toegangsrechten verkregen door de dienstverlener en de daaruit voortvloeiende diefstal, verlies of ongeoorloofde openbaarmaking van de verstrekte gegevens
- Menselijk en organisatorisch falen of wangedrag als gevolg van het niet naleven van overeengekomen technische en organisatorische maatregelen
- Juridische risico's (zoals schade als gevolg van handelen of nalaten van dienstverleners, boetes of gevangenisstraffen, officiële bevelen)

Om deze bedreigingen tegen te gaan, worden de volgende maatregelen aanbevolen:

- Maatregelen voor het selecteren van serviceproviders
- Het ontwerpen of aanpassen van het aankoopproces met als doel zich te concentreren op gegevensbescherming en informatiebeveiliging, zoals door relevante instanties in een vroeg stadium bij het selectieproces te betrekken en op basis van individuele of algemeen erkende normen (bijvoorbeeld Trusted Computer System Evaluation Criteria (TCSEC)) minimumnormen (basisnormen) vast te stellen.
- Het in een gestructureerde vorm uitvoeren van informatieverzoeken (RFI) met vragen over informatiebeveiliging en gegevensbescherming met een verzoek om een bindende verklaring van de dienstverlener
- Biedingsverzoeken (Request for Proposal of RFP) van verschillende dienstverleners op basis van een gedetailleerde beschrijving van diensten en specificaties, evenals de individuele vereisten voor gegevensbescherming en informatiebeveiliging.
- Zorgvuldig onderzoek (due diligence) dat een beoordeling van alle relevante juridische risico's in verband met een juridische transactie omvat.
- Maatregelen om dienstverleners te controleren en te monitoren
- In ieder geval wordt een interne definitie en delegatie van verantwoordelijkheden met betrekking tot het toezicht op dienstverleners aanbevolen.
- Het type en de omvang van de maatregelen zijn afhankelijk van verschillende factoren, zoals de grootte van de organisatie, de complexiteit van de dienstenniveau overeenkomst (SLA) en de organisatiestructuur, evenals al binnen de organisatie bestaande processen.

- Opstellen en toepassen van criteria om de capaciteit van dienstverleners voortdurend in overeenstemming met de gedefinieerde en contractueel overeengekomen vereisten (in overeenstemming met de bepaling in ISO 9001 sub-sectie 8.4) te controleren.
- De maatregelen worden idealiter geïntegreerd in een IT-risicobeheer dat is ingebed in de bestaande bedrijfsprocessen (zoals IT-beveiligingsbeheer, compliance beheer, gegevensbeschermingsbeheer).
- Maatregelen voor het toezicht op dienstverleners
- Risicobeheer van dienstverleners om taken te prioriteren, auditintervallen te bepalen, het type en de reikwijdte van auditmaatregelen te bepalen (zoals auditmaatregelen ter plaatse, gebruik van vragenlijsten en commerciële databases voor risicobeheer van dienstverleners), enz. door het individuele risico in verband met de inbedrijfstelling van de respectieve dienstverlener te beoordelen op basis van de mate van waarschijnlijkheid dat bepaalde risico's zich zullen voordoen, de mate waarin het risico kan worden beïnvloed en de inspanning die daarvoor nodig is.
- Audits van dienstverleners/leveranciers (IT-beveiligingsaudits, gegevensbeschermingsaudits, fysieke beveiligingsaudits) tijdens de uitvoering van het contract
- Beheer van contracten, certificaten en andere documentatie

Stand der techniek classificatie



3.3.9 Informatiebeveiliging beheersysteem (ISMS

Een ISMS is ontworpen om binnen het toepassingsgebied de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te waarborgen door het binnen de organisatie vaststellen van procedures en regels en de bijbehorende implementatie van beveiligingsmaatregelen. Op deze manier wordt informatiebeveiliging permanent gepland, beheerd en gecontroleerd om het vereiste beveiligingsniveau te bereiken, te behouden en continu te verbeteren.

Vereisten

De basis voor het ISMS is de definitie van het toepassingsgebied en de context waarin het ISMS moet worden ingericht en geëxploiteerd. Voor de definitie van het toepassingsgebied moeten interne en externe vereisten, verwachtingen met betrekking tot de ISMS-doelstellingen, betrokken partijen en wettelijke en reglementaire vereisten worden overwogen.

Een ISMS vereist een continu verbeteringsproces (CIP), dat in de vorm van de PDCA-cyclus wordt geïmplementeerd om het onderhouden van de informatiebeveiliging in de organisatie te waarborgen. Om een effectief en efficiënt ISMS te realiseren, moeten de volgende vereisten worden geïmplementeerd.

De steun van het hoogste managementniveau (raad van bestuur, uitvoerend management, enz.) voor het inrichten en verdere ontwikkelen van een ISMS moet worden gewaarborgd, aangezien beslissingen moeten worden genomen over de doelstellingen, de reikwijdte en het uitvoeren van het ISMS en middelen vrijgemaakt moeten worden door het hoogste managementniveau. De ondersteuning van het hoogste managementniveau voor het ISMS vindt plaats door de adoptie (ondertekening) van de informatiebeveiligingsrichtlijn. Deze richtlijn definieert de informatiebeveiligingsdoelstellingen van de organisatie in het toepassingsgebied van het ISMS, die zijn afgestemd op de bedrijfsdoelstellingen en -strategieën, en stelt de verbintenis van het hoogste managementniveau vast om het ISMS voortdurend te verbeteren. Dit is essentieel, omdat de algehele verantwoordelijkheid voor informatiebeveiliging altijd bij het hoogste managementniveau blijft. De richtlijn moet worden gecommuniceerd naar alle medewerkers in het toepassingsgebied.

Om een ISMS op te zetten en technische en organisatorische beveiligingsmaatregelen te implementeren, moet in het toepassingsgebied een geschikte, overkoepelende organisatiestructuur voor informatiebeveiliging aanwezig zijn. De rollen en verantwoordelijkheden van alle betrokken partijen en personen moeten duidelijk worden omschreven. Alle personen in het toepassingsgebied moeten voldoende worden betrokken bij een opleidings- en bewustmakingsprogramma dat in overeenstemming is met hun taken, rollen en verantwoordelijkheden.

Voor de succesvolle werking van het ISMS en ter ondersteuning van het informatiebeveiligingsproces moeten interne/externe communicatievereisten en een documentcontroleproces voor de vereiste documentatie van het ISMS (gedocumenteerde informatie en records) worden gedefinieerd.

Een zwaartepunt van het ISMS is risicomanagement om (IT)risico's voor de organisatie te identificeren en te analyseren en deze door middel van passende maatregelen zo beheersbaar mogelijk te maken of terug te brengen tot een aanvaardbaar niveau. Risicobeheer moet worden aangepast aan de organisatie en worden geïntegreerd in het informatiebeveiligingsproces.

Aanbevelingen/implementatie
De volgende normen worden aanbevolen voor de implementatie van een ISMS:

- ISO/IEC 27001:2013
  Deze norm geeft eisen voor een te certificeren ISMS en beschrijft noodzakelijke processen voor implementatie, beheer, controle en continue verbetering.
  Als certificering van het ISMS wordt aangevraagd, moeten aanvullende eisen van de in aanhangsel A vermelde controles worden toegepast.
- BSI Standaard 200
  Deze-norm beschrijft de algemene vereisten voor een ISMS en combineert de IT- Grund-schutz -methodologie met de vereisten van ISO/IEC 27001 om compatibel te zijn met de laatste en waardoor ISO/IEC 27001-certificering op basis van IT-Grundschutz mogelijk wordt.
- BSI IT- Grundschutz Compendium (februari 2021)
  Het BSI IT- Grundschutz Compendium beschrijft gevaren in verband met administratieve accounts en daaruit voortvloeiende vereisten voor de behandeling daarvan in module in de OPS.1.1.2.
- VdS Guidelines 10000 (VdS 10000)
  VdS Schadenverhütung GmbH, een dochteronderneming van de Duitse Vereniging van Verzekeraars, biedt een praktische, compacte catalogus van maatregelen voor het opzetten van een ISMS speciaal voor kleine en middelgrote bedrijven.
  Certificering door VdS is ook mogelijk, de richtlijnen zijn gebaseerd op de normen van ISO/IEC 27001 en BSI- Grundschutz.
- Information Security Management System in 12 stappen (ISIS12)
  Het Network for Information Security in SMEs, met leden zoals de Beierse IT Security Cluster e.V. en de Universiteit van Regensburg, biedt een wetenschappelijk onderbouwd model voor kleine en middelgrote instellingen voor de, in 12 stappen, praktische invoering van een ISMS op basis van de ISO/IEC 27001 en BSI-Grundschutz normen. Certificering is mogelijk.
- Austrian Information Security Handbook
  Het Oostenrijkse handboek voor informatiebeveiliging beschrijft en ondersteunt de procedure voor het opzetten van een uitgebreid ISMS en biedt, vanwege de gekozen structuur, een implementatiehulpmiddel voor de implementatie volgens ISO/IEC 27001.

Kwaliteitsbewaking (Quality assurance)
Voor de implementatie van de PDCA-cyclus binnen het ISMS moeten periodieke audits (ten minste jaarlijks) worden uitgevoerd om na te gaan of technische en organisatorische maatregelen effectief zijn en worden geïmplementeerd en toegepast in overeenstemming met het informatiebeveiligingsbeleid. Hiertoe moet een verordening voor de evaluatie en verbetering van het informatiebeveiligingsproces en een regelmatig, ten minste driejarig auditplan voor de uitvoering van interne en externe audits worden vastgesteld. Periodiek moeten door professioneel gekwalificeerde personen audits worden uitgevoerd in overeenstemming met het auditplan en op ad-hoc basis. Aanleiding voor audits zijn bijvoorbeeld proceswijzigingen,

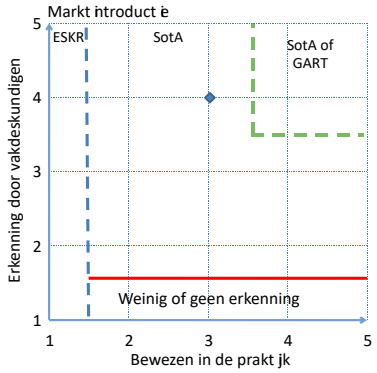
scopewijzigingen, infrastructuurwijzigingen of het signaleren van nieuwe, kritieke risico's.

Het hoogste managementniveau moet periodiek en regelmatig worden geïnformeerd over de status, die bijvoorbeeld is afgeleid van interne/externe audits, van informatiebeveiliging en moet het ISMS evalueren in de vorm van managementbeoordelingen om de, toepasbaarheid, geschiktheid, effectiviteit en voortdurende verbetering van het ISMS te waarborgen.

Welke beschermingsdoelen vallen onder deze maatregel

☒ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☐ Authenticiteit

Stand der techniek classificatie



3.3.10 Beschermen van accounts met speciale bevoegdheden

Voor het beheer van systemen zijn geprivilegieerde accounts (accounts met verstrekkende bevoegdheden) vereist. Door mogelijk ongeoorloofd of oneigenlijk gebruik brengen deze accounts en bijbehorende rechten een risico met zich mee met grote kans op schade. Daarom moet er passende regelgeving zijn om een goed IT-systeembeheer te garanderen, met name met betrekking tot het toewijzen, het gebruik en intrekken van administratieve toegangsrechten.

Naast interactieve accounts met beheerderstoegangsrechten worden serviceaccounts meestal gebruikt voor toepassingen of toepassingsservices die geen directe interactie van de administratieve gebruiker vereisen. Hieronder vallen ook de zogenaamde taak(gerichte)accounts (bijvoorbeeld voor cronjobs). De onjuiste (meestal te genereuze) toewijzing van rechten aan de serviceaccounts is een groot zwak punt in de meeste organisaties en waar aanvallers ook bijzondere aandacht aan besteden.

Vereisten voor beheerdersaccounts en toegangsrechten

Er moeten richtlijnen en voorschriften worden vastgesteld voor het gebruik en de behandeling van administratieve rechten en accounts. Alvorens een beheerdersaccount aan een gebruiker toe te kennen, moet de gebruiker eerst deze richtlijnen en voorschriften accepteren en zich ertoe verbinden deze na te leven. Elke schending van de gedefinieerde richtlijnen en voorschriften moet worden verklaard en moet zo nodig gevolgen hebben.

Er moet een restrictieve autorisatiestrategie worden gevolgd, volgens welke de toegang tot hulpbronnen in principe verboden is, tenzij deze uitdrukkelijk is toegestaan en goedgekeurd. Hiertoe moet voor het toewijzen van rechten een bepaald model of een welbepaalde procedure worden toegepast. Een mogelijkheid is bijvoorbeeld het Role Based Access Control (RBAC) model. RBAC is een functie gebaseerde toegangscontrole, waarbij autorisatie wordt verleend op basis van gedefinieerde rollen. Gebruikers worden toegewezen aan een of meer rollen en ontvangen dus de toegangsrechten van deze rollen. De respectievelijke rollen worden in RBAC gedefinieerd op basis van activiteitenprofielen.

Voor het toekennen van beheerrechten (administratieve rechten) moeten de beginselen van need-to-know en least-privilege in acht worden genomen. Met het need-to-know principe krijgt ieder persoon alleen de kennis, machtiging en/of het bezit van vertrouwelijke informatie die nodig is om zijn of haar eigen taken te vervullen. Met het least privilege principe krijgt elke gebruiker precies die rechten die absoluut noodzakelijk zijn voor het uitvoeren van zijn of haar taken.

Het verlenen van beheerrechten moet worden uitgevoerd in een gedefinieerd en gecontroleerd proces en waarin elk verzoek wordt beoordeeld en gedocumenteerd. Beheerrechten kunnen niet worden verleend zonder eerst dit proces te hebben doorlopen en te zijn goedgekeurd.

Voor beheerderstoegangsrechten roeten speciale beheerdersaccounts worden gemaakt en

gebruikt en die verschillen van gebruikersaccounts voor normaal gebruik (niet zijnde beheertaken). Activiteiten die zonder beheerrechten kunnen worden uitgevoerd, mogen niet worden uitgevoerd door beheerdersaccounts (geprivilegieerde accounts.)

Beheerdersaccounts mogen alleen die rechten kunnen krijgen die nodig zijn om de activiteiten uit te voeren die voor dat account zijn opgegeven. Het uitgeven van rechten voor “superbeheerders" met machtigingen voor alle systemen moet worden vermeden. In het geval van bestaande standaardaccounts voor beheertaken moeten deze worden gedeactiveerd, hernoemd en zo mogelijk niet op beperkte wijze worden gebruikt.

Elk beheerdersaccount moet duidelijk aan een persoon kunnen worden toegewezen. Als dit vanwege de systeemkenmerken niet mogelijk is, moet het gebruik van een niet op de persoon herleidbare beheerdersaccount worden beveiligd met aanvullende organisatorische en/of technische maatregelen en moet de afhandeling ervan worden vastgelegd. Vereiste groepsaccounts voor beheeractiviteiten moeten nauwkeurig worden gespecificeerd (met name de toegestane groep personen) en het gebruik ervan moet ook worden gedocumenteerd en is alleen in uitzonderlijke gevallen toegestaan. Het gebruik van groepsaccounts moet consequent worden geregistreerd.

Voor alle beheertaken moeten vervangingsregels worden gedefinieerd. Daarnaast moeten noodaccounts met beheerrechten worden aangemaakt en moeten hun toegangsgegevens veilig worden bewaard. Het gebruik van deze accounts moet worden beperkt en gecontroleerd (zoals het beginsel van dubbele controle) en moet worden gedocumenteerd. In het geval van noodaccounts met multifactor-authenticatie (MFA) moet worden opgemerkt dat alle factoren voor authenticatie ook in noodsituaties beschikbaar en operationeel en toegankelijk moeten zijn.

Als tijdelijke beheerrechten worden verleend, dan moeten deze een tijdelijke/logische beperking hebben en opnieuw worden ingetrokken wanneer de noodzaak ophoudt te bestaan.

Beheerdersaccounts met uitgebreide toegangsrechten moeten worden beschermd met een sterke authenticatieprocedure (koppeling van verschillende authenticatiefuncties, challenge-response of op certificaten gebaseerde procedures) waarin de identiteit van de gebruiker duidelijk kan worden vastgesteld. Gebruikersaccounts met uitgebreide toegangsrechten moeten worden beveiligd met ten minste twee authenticatiefuncties. Als een passende authenticatieprocedure niet mogelijk is, moet worden nagegaan of vanwege het risico aanvullende technische of organisatorische maatregelen nodig zijn voor de bescherming. Het gebruik van dezelfde wachtwoorden voor meerdere beheerdersaccounts is niet toegestaan.

Er moet een actuele en volledige documentatie van alle beheerdersaccounts met hun respectieve toegangsrechten worden bijgehouden. Dit geldt zowel voor systemen die in gebruik zijn, zoals besturingssystemen en (apparaat)firmware, als voor gespecialiseerde toepassingen, zoals centrale applicaties.

Voor veiligheidskritieke activiteiten wordt, conform het beginsel van scheiding van taken, een taakverdeling of een scheiding van taken uitgevoerd. Deze scheiding moet zodanig zijn ontworpen dat het uitvoeren van veiligheidskritieke activiteiten gebonden is aan de aanwezigheid van meerdere gebruikers (zoals door het beginsel van dubbele controle) of dat een activiteit wordt verdeeld over meerdere personen die elkaar mogelijk niet vertegenwoordigen. In ieder geval moeten beheerdersrollen worden gescheiden van controlerende rollen zoals interne audit.

Alle logins en activiteiten die door beheerdersaccounts worden uitgevoerd, moeten worden geregistreerd zodat kan worden getraceerd welke activiteiten door welke accounts zijn uitgevoerd. Om de verifieerbaarheid van de door de beheerdersaccounts uitgevoerde activiteiten te waarborgen, mogen beheerders geen log- en controleprocedures van hun eigen activiteiten kunnen wijzigen of verwijderen. Regelmatig moet een beoordeling van deze logboeken en auditlogboeken plaatsvinden om de activiteiten van de administraties op naleving te controleren.

Machine-2-Machine-serviceaccounts (M2M)
Beheerdersaccounts zijn vaak goed beveiligd, maar serviceaccounts niet. Door gebruik te maken van deze omstandigheid slagen aanvallers heel vaak in de zogenaamde laterale beweging, d.w.z. de beweging van het ene gecompromitteerde systeem naar het volgende (vaak meer kritieke) systemen.

Het bijzondere hierbij is dat deze accounts bijzonder kwetsbaar zijn omdat:

- deze accounts geen gebruik maken van multifactor authenticatie (MFA);
- opgeslagen wachtwoorden van deze accounts (uitgaande van beheerrechten) zeer eenvoudig gelezen kunnen worden;
- de wachtwoorden van deze accounts vaak niet gewijzigd worden en niet zijn onderworpen aan nieuwe wachtwoordrichtlijnen en dus, vanwege hun leeftijd, vaak nog steeds erg eenvoudig zijn;
- de wachtwoorden van deze accounts zijn vaak bij veel mensen bekend, waarbij niet duidelijk is wie deze wachtwoorden precies kent.

Alle serviceaccounts moeten worden gemaakt en gedocumenteerd volgens een gedefinieerde procedure. Voor deze accounts moeten sterke, vaak gegenereerde wachtwoorden worden gebruikt en deze mogen alleen toegankelijk worden gemaakt voor een klein, welbepaald aantal personen. Als personen met kennis van de toegangsgegevens voor deze accounts de organisatie verlaten of van functie veranderen, dan moeten de wachtwoorden na een passende risicobeoordeling worden gewijzigd.

Om serviceaccounts te beveiligen, mag interactieve toegang tot deze accounts niet worden toegestaan en elke poging om interactief in te loggen met een dergelijk account moet onmiddellijk worden onderzocht. Voor elke taak en service moeten, speciale separatie accounts worden gemaakt (en niet bijvoorbeeld slechts één account per systeem) en het principe van de minste bevoegdheden (least-privileges) moet strikt worden nageleefd. Om niet per ongeluk aanvullende rechten van andere accounts over te nemen, mogen serviceaccounts ook niet van andere accounts worden gekopieerd.

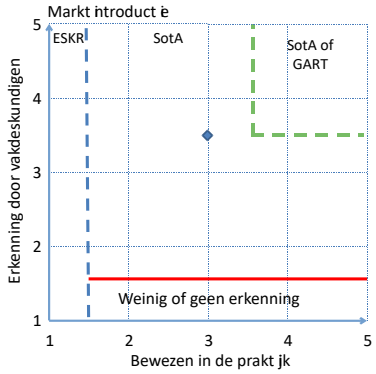
Aanbevelingen/implementatie
De volgende normen worden aanbevolen voor het beheer van beheerdersaccounts en hun toegangsrechten, evenals voor de uitvoering van regelgeving:

- ISO/IEC 27002:2013
  De norm bevat aanbevelingen voor de implementatie van de in ISO/IEC 27001:2013 Annex A vereiste maatregelen voor het toewijzen, het beheer en de audit/controle van beheerdersaccounts. Als certificering conform ISO/IEC 27001:2013 wordt aangevraagd, dan moeten deze maatregelen binnen het kader van het ISMS worden geïmplementeerd. Uitvoeringsinstructies voor deze maatregel zijn vooral te vinden in de punten 9.2.3 Beheer van speciale toegangsrechten en 12.4.3 Logboeken van beheerders en exploitanten.
- BSI IT-Grundschutz Compendium (februari 2021)
  Het BSI IT- Grundschutz -Compendium beschrijft in module OPS.1.1.2 bedreigingen in verband met beheerdersaccounts en afgeleide vereisten voor de afhandeling ervan.
- Oostenrijks handboek voor informatiebeveiliging 4.1.1
  Het Oostenrijkse handboek voor informatiebeveiliging bevat aanbevelingen voor het beheer van gebruikers, waaronder ook beheerdersaccounts. Er zijn aanbevelingen te vinden over het toewijzen, het beheer en de documentatie van toegangsrechten en over de regulering van toegangsmogelijkheden in geval van vertegenwoordiging en noodsituaties.
- BDEW Whitepaper: Vereisten voor veilige besturings- en telecommunicatiesystemen 2.0
  Naast de eis om te voldoen aan het need-to-know principe in de algemene vereisten, beveelt de BDEW white paper ook aan dat applicaties en gespecialiseerde applicaties gebruikersconcepten moeten implementeren waarin beheerdersrollen kunnen worden toegewezen met granulaire toegangscontrole.

Welke beschermingsdoelen vallen onder deze maatregel

☒ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand der techniek classificatie



3.3.11 Dark web bewaking

Het verlies van bedrijf kritische informatie kan ernstige gevolgen hebben. Wie op de hoogte is van het verlies, kan daarop reageren. Net als in de echte wereld, waar gestolen goederen op de zwarte markt worden verhandeld, wordt gestolen bedrijfsinformatie (zoals informatie over kwetsbaarheden, bevindingen van gebruikte cookies, gestolen inloggegevens, betalingstransactie-informatie) verhandeld op het zogenaamde dark web[28]. Dit verwijst naar veel afzonderlijke netwerken (darknets) binnen het internet.

Het Dark Web wordt door aanvallers gebruikt om informatie met elkaar uit te wisselen en gestolen bedrijfsinformatie te presenteren en/of te verkopen. Dit gebeurt meestal direct na de aanval. Het technisch compromitteren van bedrijven, systemen en netwerken vindt vaak ongemerkt plaats en leidt tot een datalek of kan dienen om een gerichte aanval voor te bereiden. Daarom kan het observeren van het dark web helpen om de voortgang van een aanval op een bedrijf, die heeft plaatsgevonden of op handen is, te identificeren, en om p op basis van de beschikbare informatie passende corrigerende maatregelen te nemen.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

Het regelmatig en gericht monitoren van het dark web[29] en de ontdekking van gestolen bedrijfsinformatie kan helpen bij het voorkomen van geplande of toekomstige aanvallen op een bedrijf (bijvoorbeeld door een ransomware-aanval, illegale gegevensdiefstal of vervolgaanvallen door andere aanvallers). De maatregel draagt daarmee bij aan risico-minimalisatie. Het kan ook worden gebruikt om zogenaamde supply chain-aanvallen te detecteren (ook bekend als aanvallen op de supply chain, aanvallen van derden, aanvallen op de waardeketen) om te voorkomen dat een aanval op de eigen omgeving indirect wordt uitgevoerd via externe leveranciers of leveranciers of via de supply chain.

Dark web-monitoring beschermt niet tegen de dreiging van compromitteren (inbraak door daders) zelf. De inzichten die volgen uit Dark Web Monitoring kunnen echter de risico's voor de getroffen organisatie minimaliseren door passende responsmaatregelen te nemen om verdere schade te voorkomen of op zijn minst te beperken.

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

Handmatige analyses van de openbaar beschikbare informatie over een organisatie en de huidige dreigingssituatie voor de respectieve industrie worden uitgevoerd om vervolgens geautomatiseerde sets regels op te zetten die individueel zijn aangepast aan de betreffende organisatie. Deze zorgen voor regelmatige (minimaal dagelijkse) monitoring van bijvoorbeeld:

- marktplaatsen en forums op het dark web (onder andere mogelijk via speciale providers);
- gepubliceerde datalekken (zoals Identity Leak Checker van het Hasso Plattner Instituut[30]);
- publieke en niet-openbare communicatie op het World Wide Web en op social media platforms en relevante gesloten gebruikersgroepen;
- waarschuwingen van de relevante autoriteiten en officiële instanties (zoals BSI en US-Cert);

---

[28] Ook Darknet of Deep Web genoemd

[29] 27 Als een special soort van Cyber Threat Intelligence (zie ook hoofdstuk 3.2.27)

[30] 28 https://sec.hpi.de/ilc/search

- berichtgeving in de media.

De handmatige analyses van de informatie- en dreigingssituatie worden zo nodig herhaald om een continue optimalisatie van de regels en voorschriften te garanderen.

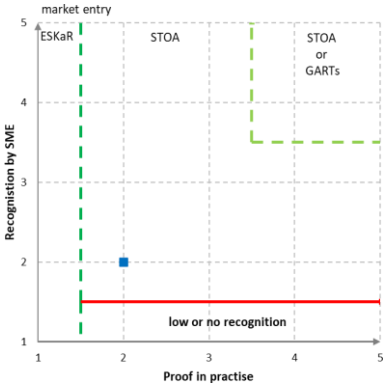
De handmatige analyses van de informatie- en dreigingssituatie worden indien nodig herhaald om een continue optimalisatie van de regelgeving te garanderen.

Vanwege de grote hoeveelheid te verwachten data kan een hoge mate van automatisering en professionalisering meestal alleen worden bereikt via een beheerde service. Daarnaast moeten gespecialiseerde data-analisten met een achtergrond in onderzoek tactieken bij de taken worden betrokken.

Welke beschermingsdoelen vallen onder deze maatregel

☒ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☐ Authenticiteit

Stand van de techniek classificatie



3.3.12 Software stuklijst (SBOM)

Een Software Bill of Materials of SBOM is een lijst met componenten en afhankelijkheden die voor een IT-toepassing of IT-service vereist zijn. Deze lijst is machine-leesbaar en biedt transparantie over componenten van derden die in de toepassing of dienst worden gebruikt. Het maakt het mogelijk om potentiële kwetsbaarheden die worden veroorzaakt door onderliggende componenten te identificeren.

Tegen welke IT-beveiligingsdreiging(en) wordt de maatregel gebruikt?

De maatregel dient ter bescherming tegen zogenaamde supply chain-aanvallen die worden uitgevoerd door het benutten van beveiligingsgaten in gebruikte componenten (zoals softwarebibliotheken). Zonder SBOM is er geen informatie over welke componenten worden gebruikt in een IT-applicatie of een IT-dienst, waardoor het identificeren van potentiële kwetsbaarheden veel moeilijker, zo niet onmogelijk is.

Welke maatregel (procedure, apparatuur of bedrijfsmodus) wordt in dit punt beschreven?

SBOM biedt een complete stuks lijst van alle componenten die worden gebruikt in een IT-toepassing of IT-service. Deze informatie maakt een vergelijking mogelijk met een lijst met beveiligingslekken die zich in een specifiek onderdeel kunnen bevinden en dus informatie over de vraag of de gebruikte IT-toepassing of IT-service ook door dit beveiligingslek kan worden getroffen.

Voor SBOM zijn verschillende dataformats ontwikkeld. Er zijn ISO-normen voor de SPDX[31] en SWID[32] en door OWASP is de CycloneDX[33]-standaard goedgekeurd. SWID en SPDX worden voornamelijk gebruikt om software uniek voor verschillende doeleinden te identificeren (niet alleen beveiliging). CycloneDX richt zich daarentegen op de beveiliging van applicaties en de analyse van de componenten van de supply chain, ook buiten software, waaronder hardwarecomponenten en clouddiensten. De formats zijn niet compatibel met elkaar.

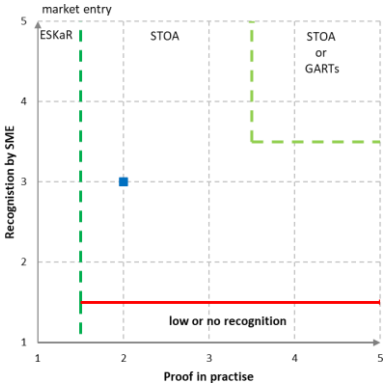
[31] Software Package Data Exchange; ISO/IEC 5962:2021 - SPDX Specification V2.2.1
[32] Software Identification Tag; ISO/IEC 19770-2:2015
[33] OWASP CycloneDX Software Bill of Materials Standard; (https://cyclonedx.org/)

SBOM is een belangrijke maatregel om zich te verdedigen tegen supply chain-aanvallen. De Amerikaanse regering heeft door middel van een uitvoeringsbesluit in mei 2021[34], verder onderbouwd door het Amerikaanse ministerie van Handel (juli 2021)[35] en NIST (februari 2022)[36], de levering en het gebruik van SBOM door leveranciers van de Amerikaanse overheid verplicht gesteld. De Europese Commissie werkt als onderdeel van de Cyber Resilience Act[37] aan een soortgelijke regeling.

Welke beschermingsdoelen vallen onder deze maatregel

☒ Beschikbaarheid ☒ Integriteit ☒ Vertrouwelijkheid ☒ Authenticiteit

Stand van de techniek classificatie



[34] U.S. White House Executive Order 14028 on Improving the Nations Cybersecurity (12. Mai 2021)
[35] U.S. Department of Commerce: "The Minimum Elements for an SBOM" (12. Juli 2021)
[36] NIST SP 800-218 Secure Software Development Framework (SSDF) Version 1.1 (Februari 2022)
[37] Europese Commissie: Proposal for a Regulation on cybersecurity requirements for products with digital elements - Cyber resilience Act (15.9.2022)

4. Appendix

4.1 Toelichting: Maatregelen tegen ransomware-aanvallen

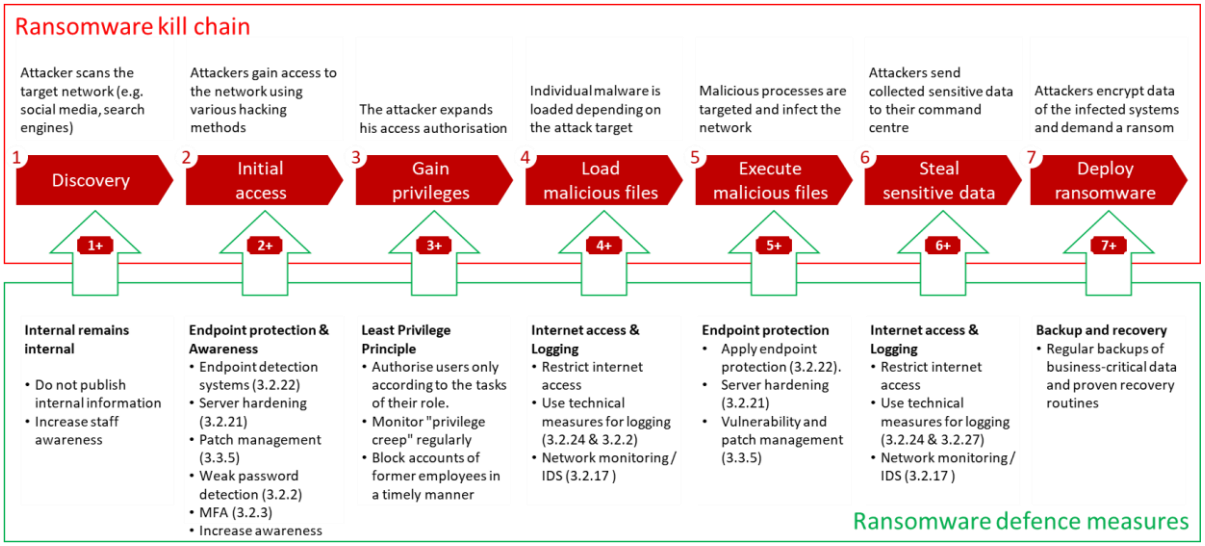
Ransomware beschrijft een type aanval dat de toegang tot persoonlijke en bedrijfsgegevens blokkeert (meestal door middel van versleuteling) en losgeld eist om deze gegevens vrij te geven. In de meeste gevallen is het niet mogelijk om zonder het losgeld te betalen de originele gegevens te reconstrueren. Vaak gaat een ransomware-aanval gepaard met de dreiging om gevoelige of geheime gegevens van het slachtoffer van de aanval te publiceren om de losgeld-eis te ondersteunen. Andere algemene termen voor ransomware zijn afpersing/crypto Trojan of chantage-software. Het publiek verwijst vaak naar een ransomware-aanval.

De dreiging van ransomware is de afgelopen jaren gestaag gegroeid en is een van de grootste bedreigingen voor zowel particulieren als bedrijven.

De procedure van een dergelijke aanval is echter complex en begint veel eerder dan op het eerste gezicht lijkt. Elke ransomware -aanval verschilt in afzonderlijke stappen, maar in algemeenheid is de procedure vergelijkbaar.

Om de complexiteit van een ransomware -aanval tegen te gaan, is het gebruik van slechts één maatregel (bijvoorbeeld antivirussoftware of proxyfilters) onvoldoende. Er moeten meerdere maatregelen tegelijk worden uitgevoerd en dus moeten er meerdere verdedigingslinies worden opgezet. Voorbeelden van dergelijke activiteiten zijn detectie van gecompromitteerde accounts en zwakke wachtwoorden, gebruik van MFA, systemen voor aanvalsdetectie, enz.

In het volgende diagram tonen we voorbeelden van de afzonderlijke stappen en de bijbehorende beschermende maatregelen die afhankelijk van de respectieve stap moeten worden gebruikt:



Ransomware kill chain	Ransomware verdedigingsmaatregelen
1) Ontdekking Aanvallers verzamelen zoveel mogelijk informatie over de organisatie onder attack, bijvoorbeeld in openbare zoekacties (Shodan, Censys) of sociale netwerken.	**1+) Intern blijft intern** Publiceer geen informatie die alleen bedoeld is voor intern gebruik (netwerkplannen, IP-adressen, organigrammen, contactgegevens, enz.). Als mogelijke benadering kan een classificatie van documenten en gegevens (openbaar, intern, geheim) worden gemaakt. Ook medewerkers moeten hierop getraind worden.
2) Initiële toegang Aanvallers gebruiken verschillende hacking methodes om toegang te krijgen tot het netwerk. Een eerste infectie treedt op, vaak via phishing-e-mails of schadelijke websites. Op dit moment is de eigenlijke kwaadaardige code nog niet geladen.	**2+) Endpoint bescherming & Awareness** Implementeer maatregelen voor de bescherming van eindapparaten (3.2.22 HR SdT); Sensibiliseer medewerkers door middel van regelmatige bewustwordingstrainingen. Schakel de uitvoering van macro's uit of beperk ze tot alleen ondertekende macro's. Gebruik maatregelen om gecompromitteerde accounts en zwakke wachtwoorden te detecteren (3.2.2 HR SdT). Gebruik indien mogelijk MFA (3.2.3 HR SdT). Maar ook andere maatregelen, zoals server hardening (3.2.21 HR SdT) en kwetsbaarheden en patchmanagement (3.3.5 HR SdT).
3) Verkrijg privileges Aanvallers vergroten de rechten waarmee ze handelen om tot verdergaande acties te komen en daarmee een hogere kans op schade.	**+) Least Privilege Principe (PoLP)** Zorg ervoor dat gebruikers alleen de toegangsrechten krijgen die ze nodig hebben om hun taken uit te voeren. Controleer regelmatig het autorisatiemodel op privilege creep. Stem maatregelen af op de gebruikersaccount-cyclus en blokkeer accounts van voormalige medewerkers op korte termijn. Bescherm geprivilegieerde accounts via MFA.
4) **Laad schadelijke bestanden** De druppelaar laadt nu de eigenlijke kwaadaardige code (payload). Deze payload is vaak individueel geprogrammeerd en wordt niet herkend door antivirussoftware.	**4+) Internettoegang & Logging** Sta internettoegang toe tot goedgekeurde pagina's, blokkeer andere. In afwachting van de beschermingsvereisten kan het gebruik van ReCoBS (3.2.23 HR SdT) nuttig zijn. Voor logging en monitoring kunnen verdere technische maatregelen zoals SIEM (3.2.24 HR SdT) of CTI (3.2.27 HR SdT) en netwerkmonitoring door middel van IDS (3.2.17 HR SdT) worden gebruikt.
5) Voer schadelijke bestanden uit Verdere kwaadaardige code wordt gedownload, de aanvallers verspreiden zich over het netwerk (laterale beweging)	**5+) Endpoint-bescherming** Pas maatregelen toe voor terminalbeveiliging (3.2.22 HR SdT). Implementeer verdere maatregelen zoals server hardening (3.2.21 HR SdT) en vulnerability en patch management (3.3.5 HR SdT).
6) Gevoelige gegevens stelen Gevoelige gegevens zoals toegangsgegevens worden verzonden naar de command-and-control-server van de aanvallers.	**6+) Internettoegang & Logging** Sta internettoegang toe tot goedgekeurde pagina's, blokkeer andere. Afhankelijk van de beschermingseisen kan het gebruik van ReCoBS (3.2.23 HR SdT) nuttig zijn. Voor logging en monitoring kunnen verdere technische maatregelen zoals SIEM (3.2.24 HR SdT) of CTI (3.2.27 HR SdT) en netwerkmonitoring door middel van IDS (3.2.17 HR SdT) worden gebruikt.
7) Ransomware implementeren De eigenlijke kwaadaardige code die de gegevens versleutelt, wordt uitgevoerd.	**7+) Back-up en herstel** Bij een succesvolle aanval moeten er natuurlijk eerst veel maatregelen worden genomen om de infectievector te vinden en te sluiten en de schade te beperken. Huidige, niet-geïnfecteerde back-ups zijn vereist voor de daaropvolgende herinstallatie van de systemen en het herstel van de gegevens.

IT Security Association Germany (TeleTrusT)

Het Bundesverband IT-Sicherheit e.V. (TeleTrusT) is een wijdverspreid competentienetwerk voor IT-beveiliging bestaande uit leden uit de industrie, administratie, consultancy en onderzoek, evenals nationale en internationale partnerorganisaties met vergelijkbare doelstellingen. Met een breed scala aan leden en partnerorganisaties belichaamt TeleTrusT het grootste competentienetwerk voor IT-beveiliging in Duitsland en Europa. TeleTrusT biedt interdisciplinaire fora voor IT-beveiligingsexperts en vergemakkelijkt informatie-uitwisseling tussen leveranciers, gebruikers, researchers en autoriteiten. TeleTrusT becommentarieert technische, politieke en juridische kwesties met betrekking tot IT-beveiliging en is organisator van evenementen en conferenties.

TeleTrusT is een vereniging zonder winstoogmerk, met als doel de professionaliteit van informatiebeveiliging te bevorderen, het bewustzijn en de beste praktijken op alle domeinen van informatiebeveiliging te vergroten. TeleTrusT is drager van de "European Bridge CA" (EBCA; PKI-netwerk van vertrouwen), de IT-expertcertificering "TeleTrusT Information Security Professional" (T.I.S.P.) en "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) en biedt het vertrouwenszegel "IT Security made in Germany". TeleTrusT is lid van het European Telecommunications Standards Institute (ETSI). Het hoofdkantoor van de vereniging is gevestigd in Berlijn, Duitsland.

Contact:

IT Security Association Germany (TeleTrusT)
Dr. Holger Muehlbauer
Managing Director Chausseestrasse 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.