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

TeleTrusT
Pioneers in IT security.

IT-Sicherheitsgesetz en General EU Data Protection Regulation:

Richtlijn "State of the Art"

Technische en organisatorische maatregelen

2021

Nederlandse versie

in co-operatie met

PRIVACY EN BEVEILIGING ADVIES
BREEMAN

Erkentelijkheid

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

Projectleiding

RA Karsten U. Bartels LL.M. - HK2 Rechtsanwälte
Tomasz Lawicki - m3 management consulting GmbH

Auteurs en deelnemende experts

Alsbih, Amir
Bartels, Karsten U. - HK2 Rechtsanwälte
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 IT-Solutions GmbH
Föllmer, Nancy - heinzl mobile cloud solutions GmbH
Gehrmann, Mareike - Taylor Wessing Partnergesellschaft mbB
Gora, Stefan - Secorvo Security Consulting GmbH
Heyde, Steffen - secunet Security Networks AG
Jäger, Hubert - Digital Trust Innovations
Kahrs, Malte - MTRIX GmbH
Kerbl, Thomas - SEC Consult Unternehmensberatung GmbH
Kippert, Tobias - TÜV Informationstechnik GmbH
Kolmhofer, Robert - FH Oberösterreich Studienbetriebs GmbH
Kowol, Dominik - eperi GmbH
Krosta-Hartl, Pamela - LANCOM Systems GmbH
Lawicki, Tomasz - m3 management consulting GmbH
Liedke-Deutscher, Bernd - TÜV Informationstechnik GmbH
Maier, Janosch - Crashtest Security GmbH
Menge, Stefan - AchtWerk GmbH & Co. KG
Mühlbauer, Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Müller, 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
Wallaschek, Felix - DETACK GmbH
Wüpper, Werner - Wüpper Management Consulting GmbH

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

Colofon

Uitgever:
Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
E-Mail: info@teletrust.de
https://www.teletrust.de

V 1.8_2021-02 NL

Dutch version: Jan Breeman

Inhoud

Afbeeldingenoverzicht

Tabeloverzicht

Principes van de richtlijn

Toen de Duitse IT-Sicherheitsgesetz (ITSiG) in juli 2015 van kracht werd, lanceerde het Bundesverband IT-Sicherheit e.V. (TeleTrusT) de werkgroep Stand der Technik (hierna AK-SdT genoemd), om geïnteresseerden richting en aanbevelingen te geven te geven op de *state of the art*, ofwel stand van de techniek, voor de 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 richtlijn is bedoeld om bedrijven en leveranciers (fabrikanten en dienstverleners) te helpen bij het bepalen van de *state of the art* in de zin van de General Data Protection Regulation (GDPR) en de ITSiG. Het document kan dienen als referentie voor contractuele overeenkomsten, aanbestedingsprocedures en voor de classificatie van geïmplementeerde beveiligingsmaatregelen.
   Deze richtlijn is een uitgangspunt voor het bepalen van wettelijk voorgeschreven IT-beveiligingsmaatregelen. Deze richtlijn is een uitgangspunt voor het bepalen van juridische IT-beveiligingsmaatregelen; ze vormen geen vervanging voor technisch, organisatorisch of juridisch advies of voor individuele adviezen.
2. ***Verantwoordelijkheid voor de ontwikkeling, evaluatie en actualisering***
   De AK-SdT en de TeleTrusT werkgroep Recht zijn gericht op het beantwoorden van de vraag, hoe de desbetreffende *state of the art* relevant is in de zin van de wet met betrekking tot de technische en organisatorische maatregelen, en hoe wettelijke eisen kunnen worden geïmplementeerd.
3. ***Begrip van de aanpak***
   De AK-SdT verwerkt haar resultaten op transparante wijze en stelt de aanbevelingen voor actie en oriëntatie, met een reguliere bijwerkprocedure, publiekelijk ter discussie.
4. ***Evaluatieprocedure***
   De AK-SdT baseert haar evaluatie op een gestandaardiseerde methode, die voor elke afzonderlijke maatregelen is ingevuld en bekend gemaakt. De methode voor het beoordelen van de *state of the art* van technische maatregelen wordt beschreven in hoofdstuk 2.2.
5. ***Actualisatie***
   Om gelijke tred te houden met de technologische vooruitgang, s het de bedoeling dat deze richtlijn regelmatig wordt bijgewerkt en gepubliceerd. Momenteel is het doel om tweejaarlijks een update van de richtlijnen te publiceren.
   Kleine aanpassingen van en toevoegingen aan de richtlijn (zoals nieuwe bijdragen aan technische maatregelen) zullen gedurende het jaar als een zogenaamde herziening van de richtlijn verschijnen.

Aanwijzing voor gebruik

Deze richtlijn is uitgangspunt voor het bepalen van de wettelijke IT-beveiligingsmaatregelen die overeenkomen met de *state of the art.* Ze vormt geen vervanging voor technisch, organisatorisch of juridisch advies of specifieke adviezen.
De ITSiG is gericht op het leveren van een bijdrage aan het verbeteren van de beveiliging van informatiesystemen in Duitsland en is van kracht sinds 25/07/2015; het kan één op één ook worden toegepast in Nederland.

1 Introductie

1.1 Wet op de IT-beveiliging (IT-Sicherheitsgesetz)

De IT-Sicherheitsgesetz (ITSiG) is van kracht sinds 25 juli 2015 en is bedoeld om bij te dragen aan de verbetering van de beveiliging van informatiesystemen in Duitsland. De regelgeving van deze wet dient ter bescherming van deze systemen in termen van huidige en toekomstige bedreigingen voor de beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van beschermde goederen. Volgens de toelichting is het doel van de wet om de IT-beveiliging van bedrijven te verbeteren, de bescherming van burgers op het internet te verhogen en ook het Bundesamt für Sicherheit in der Informationstechnik (BSI) en het Bundeskriminalamt (BKA) in dit verband te versterken.

De ITSiG is een zogenaamde artikelwet: de wet zelf werd alleen gebruikt om verschillende sectorspecifieke wetten aan te passen. De ITSiG heeft in de Bundesamt für die Sicherheit in der Informationstechnik (BSIG) regelgeving voor kritieke infrastructuren (KRITIS) opgesteld en heeft onder meer wettelijke wijzigingen aangebracht in de Atomgesetz (AtomG), de Energiewirtschaftsgesetz (EnWiG), de Telemediengesetz (TMG) en de Telekommunikationsgesetz (TKG).

De ITSiG en de bijbehorende toelichting zijn beschikbaar via de link: https://www.teletrust.de/it-sicherheitsgesetz.

De ITSiG voorziet in de meest uitgebreide veranderingen voor KRITIS -exploitanten en bedrijven die telemediadiensten aanbieden. Exploitanten van kritieke infrastructuren dienen conform BSIG Art. 8a lid 1 een minimumniveau van IT-beveiliging aan te houden, dat overeenkomt met de *state of the art*. Ze zijn ook verplicht om bepaalde IT-beveiligingsincidenten te melden aan het BSI. Het classificeren van een organisatie als kritieke infrastructuur vindt plaats op twee niveaus. Een daarvan is om te beoordelen of de organisatie valt binnen een sector die inherent is geclassificeerd als kritisch (sector aansluiting) en de andere is om te beoordelen of er een bijzondere relatie is met de veiligheid (relevanties van de daaruit voortvloeiende fouten). Dienstverleners en leveranciers worden indirect getroffen door deze wettelijke voorschriften, wanneer de KRITIS-exploitanten de desbetreffende verplichtingen contractueel aan hen opleggen.

Op grond van BSIG Art. 10, lid 1 is het Bundesministerium des Innern (BMI) bevoegd een wettelijke regeling uit te werken, waarin wordt bepaald welke apparatuur, systemen of delen daarvan als kritieke infrastructuren in de zin van deze wet worden beschouwd. Voor dit proces wordt rekening gehouden met de betekenis van de diensten en het dekkingsniveau ervan. De Duitse regering heeft ingestemd met de goedkeuring van de ministeriële regeling die op 13 april 2016 door de minister van Binnenlandse Zaken is ingediend om kritieke infrastructuren te bepalen op basis van de BSIG (BSI-KritisV).

Het eerste deel van de Kritis-verordening voor de uitvoering van de ITSiG is vervolgens in werking getreden op 3 mei 2016. Het tweede deel van de verordening werd vastgesteld op 31 mei 2017 en trad uiteindelijk in werking op 01 juni 2017. De verordening regelt de classificatie van bedrijven als kritieke infrastructuren in de energie-, water-, voedsel-, informatietechnologie- en telecommunicatiesector (korf 1) en de sectoren gezondheid, financiën en vervoer en verkeer (korf 2).

Op grond van de BSIG Art.8 lid 1 hebben exploitanten van kritieke infrastructuren een periode van twee jaar nadat het wettelijke regeling in werking is getreden om adequate technische en organisatorische maatregelen (TOMs) te treffen om verstoringen in beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van hun IT-systemen, componenten of processen die zij exploiteren en die essentieel zijn voor de functionaliteit van de kritieke infrastructuren, te voorkomen.

Aanbieders van telemediadiensten moeten conform TMG Art. 13 lid 7 garanderen dat hun technische voorzieningen binnen hun technische en economische middelen door TOMs wordt beschermd. Bij het kiezen van deze TOMs moet rekening worden gehouden met de *state of the art*. Er is geen verplichting om incidenten te melden. Dit heeft gevolgen voor elke organisatie die een telemediadienst exploiteert. In tegenstelling tot de KRITIS-regelgeving voorzien de bepalingen van de Telemediawet niet in overgangsperioden of vrijstellingen voor micro-ondernemers.

1.2 Duitse BSI-beveiligingsnormen voor KRITIS exploitanten in specifieke sectoren

De ITSiG vereist dat KRITIS-exploitanten voldoen aan of op zijn minst rekening houden met de state *state of the art* van IT-beveiligingsmaatregelen. Dit beveiligingsniveau wordt echter niet verder gespecificeerd in de wet. KRITIS sectoren mogen voor specifieke sectoren beveiligingsnormen voorstellen (hierna B3S). Het is aan het BSI om beveiligingsnormen voor specifieke sectoren, die door vertegenwoordigers van de sectoren zijn voorgesteld, goed te keuren.

De eerste aanwijzingen voor het ontwikkelen van B3S zijn door de betrokken KRITIS-exploitanten en -verenigingen te vinden in het door het BSI gepubliceerde concept: “Orientierungshilfe zu Inhalten und Anforderungen an B3S gemäß § 8a Abs. 2 BSIG”[1].

Het ontwerp bevat de volgende methodologie:

1. Definitie van het toepassingsgebied en de beschermingsdoelstellingen van de B3S.
2. Beoordeling van de sectorspecifieke risicosituatie.
3. Risicoanalyse van de sectorspecifieke risicosituatie.
4. Afleiding van geschikte en adequate sectorspecifieke maatregelen.

De B3S is bedoeld om te helpen bij het kiezen van adequate maatregelen door het vermelden van bepalingen en maatregelen op basis van *best practices* welke typisch zijn voor de sector. Het B3S moet waar nodig ook grenzen aantonen, bijvoorbeeld als "meer" bescherming en dus aanvullende maatregelen nodig zijn, en vervolgens deze aanvullende bepalingen en maatregelen aanbevelen.

Wat toereikendheid betreft, moet in de eerste plaats rekening worden gehouden met de economische kosten voor de KRITIS-exploitant, met name met de kosten van de uitvoering.

Ten slotte mogen de benodigde uitvoeringskosten niet onevenredig zijn aan de gevolgen van een tekortkoming of aantasting van de betrokken kritieke infrastructuur[2].

Of een maatregel echter adequaat of economisch is, kan alleen op individuele basis worden vastgesteld rekening houdend met hun unieke beschermingsbehoeften en uitvoeringskosten voor de vereiste maatregelen.

De richtlijn noemt vervolgens een lijst van onderwerpen (zoals middelenbeheer (asset management), leveranciers, dienstverleners en derden) die de B3S moet behandelen. De betrokken KRITIS-exploitanten en -verenigingen ontvangen vervolgens nadere informatie over de mate van gedetailleerdheid waarop voorstellen in het B3S moeten worden beschreven. Tot slot, worden in de richtlijn andere opties genoemd voor het verifiëren van de uitvoering.

Uit de richtlijn blijkt nogmaals dat het vaststellen van een minimumnorm voor een bepaalde sector afhankelijk is van een aantal individuele factoren. Daarom moet de minimumnorm nauwkeurig worden vastgesteld op basis van individuele voorwaarden. Dit geldt in het bijzonder voor gereguleerde sectoren die onderworpen zijn aan speciale wettelijke voorschriften, zoals de Telecommunicatiewet.

---

1 "Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG"; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/b3s_Orientierungshilfe.html.
2 BSI Art. 8a lid 1 zin 3

Op 1 augustus 2017 heeft het BSI voor het eerst, voor de sector water van de sectoren watervoorziening en afvalwaterzuivering is, een sectorspecifieke norm (BS3 WA) vastgesteld en goedgekeurd. De BS3 WA bestaat uit een informatieblad en een IT-beveiligingsrichtlijn die jaarlijks worden bijgewerkt. De BS3 WA is gebaseerd op de BSI Grundschutzkatalog (basisbescherming-catalogus) en van sectorspecifieke beveiligingseisen.

Het blijft echter onduidelijk welke criteria werden gebruikt om de voorgestelde beveiligingsnormen voor de watersector te selecteren en welke criteria vervolgens door het BSI werden gebruikt om het in de zin van *state of the art* goed te keuren als de BS3 WA.

1.3 Europese implicaties

De BSIG wordt aangevuld met andere Europese richtlijnen. Daartoe heeft de Europese Commissie de richtlijn betreffende maatregelen voor een hoog gemeenschappelijk niveau voor de beveiliging van netwerk- en van informatiesystemen aangenomen voor de hele Europese Unie (NIOS-richtlijn), dat in het nationale recht moet worden doorgevoerd. Dit leidt niet tot fundamentele veranderingen, aangezien de nationale wetgever al heeft geanticipeerd op een meerderheid van de vereisten die de Europese wetgevers voor de goedkeuring van de ITSiG hadden gesteld. De overeenkomstige op 27 april 2017 aangenomen uitvoeringswet NIS-Richtlinien leidt dus alleen maar tot een uitbreiding van de BSIG.

Onder meer op basis van de richtlijn is BSIG Art. 8c in het leven geroepen met extra verplichtingen voor aanbieders van *digitale diensten*. Digitale diensten zijn online marktplaatsen, online zoekmachines en cloudcomputing-diensten van een genormaliseerde waarde. Deze diensten moeten ook technische en organisatorische maatregelen (TOMs) implementeren om de IT-beveiliging te waarborgen en die rekening houdt 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 houdt met de veiligheid van systemen en installaties, de behandeling van beveiligingsincidenten en het beheer van de bedrijfscontinuïteit.

1.4 General Data Protection Regulation (GDPR)

De Europese General Data Protection Regulation[3] (GDPR) is in 2016 aangenomen en op 25 mei 2018 definitief in werking getreden. Het primaire doel van de GDPR is het beschermen van de persoonsgegevens van Europese burgers. De verordening is gebaseerd op een op risico's gebaseerde benadering in termen van haar beschermingsdoelstellingen. Passende technische en organisatorische maatregelen moeten worden genomen op het gebied van de technische gegevensbescherming om de rechten en vrijheden van natuurlijke personen te beschermen.

Hierbij moet rekening worden gehouden met het criterium *state of the art*. In het bijzonder bepaalt GDPR Art. 32, dat de beveiliging van de verwerking regelt en, Art. 9 en bijlage 1 van de Duitse Federale Wet bescherming gegevens (BDSG) vervangt, dat *state of the art* in aanmerking moet worden genomen als onderdeel van de beveiliging van gegevensverwerking. Daartoe moeten controllers en verwerkers passende technische en organisatorische maatregelen treffen. Naast de ITSiG biedt de GDPR geen definitie voor het criterium *state of the art*. Hetzelfde geldt voor de EU-wet op aanpassing en tenuitvoerlegging van gegevensbescherming (DSAnpUG-EU) en de herziene versie van de BDSG die daaruit voortvloeit, de BDSG-nieuw.

Bovendien moeten, op grond van GDPR Art. 25, de beginselen van gegevensbescherming in acht worden genomen door middel van gegevensbescherming bij opzet (privacy by design) en gegevensbescherming als standaard (privacy by default). Deze beginselen moeten ook worden toegepast door middel van passende technische en organisatorische maatregelen.

3 Europese Algemene Verordening Gegevensbescherming (AVG)

State of the art moet echter niet alleen in overweging worden genomen bij het toepassen van de richtlijnen, maar moet ook volledig worden gedocumenteerd. Hiervoor zijn uitgebreide en vergaande documentatievereisten opgesteld, in het bijzonder de verplichting om een effectbeoordeling van gegevensbescherming[4] (DPIA) uit te voeren en invulling te geven aan de verantwoordingsplicht. De verordening bevat in relatie tot deze kwestie documentatievereisten als haar eigen wettelijke verplichtingen. Zo moeten technische en organisatorische maatregelen individueel worden vastgesteld en in detail worden beschreven en gedocumenteerd.

1.5 Toereikendheid van de maatregelen

De *state of the art* beschreven in deze richtlijn) richt zich op de inhoud die door de ITSiG en de GDPR wordt gevraagd. Het is echter vanuit de ITSiG toegestaan, inzake beveiliging en gegevensbescherming, ook rekening te houden met economische factoren, onder andere bij de keuze van beschermende maatregelen(safeguards)[5]. . Of een maatregel echter economisch is, kan alleen worden bepaald door individueel onderzoek naar de unieke beschermingsbehoeften en de uitvoeringskosten die door de maatregelen worden verlangd. Daarom is de doelmatigheidscontrole (performance audit) buiten deze richtlijn gehouden.

4 DataProtection ImpactAssessment

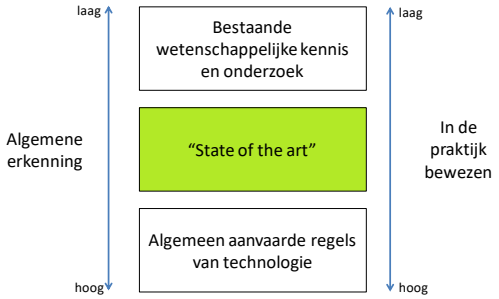
5 Zie voor van juridische overwegingen bij de wettelijke eisen Bartels/Backer: “Die Berücksichtigung des Standes der Technik in der DSGVO”, DuD 4-2018, 214.

2 Bepaling van State of the Art

2.1 Definitie

De *state of the art* van technologie[6] moet in conceptueel vergelijkbare technologische begrippen worden gedefinieerd, zoals de "algemeen aanvaarde regels van de technologie" (GART) en "bestaande wetenschappelijke kennis en onderzoek" (ESKR) [7] en moet onafhankelijk meetbaar zijn. Dit onderscheid is de essentiële basis voor het definiëren van de vereiste stand van de technologie. Zoals uit vele praktijkvoorbeelden blijkt, worden deze drie begrippen in gelijke mate door elkaar gehaald of zelfs verward, zowel in de jurisprudentie en in het openbaar[8].

Deze drie begrippen werden in 1978 geïntroduceerd met het Kalkar-besluit van het Bundesverfassungsgericht[9], evenals de *drietrapstheorie* als gevolg daarvan. Op basis van dit besluit kunnen de drie technologieniveaus grafisch worden afgebeeld:



Afbeelding 1: De drietrapstheorie volgens het Kalkar-besluit

Het technologieniveau *state of the art* ligt tussen het meer innovatieve "bestaande wetenschappelijke kennis en onderzoek" technologieniveau en het meer gevestigde "algemeen aanvaarde technologieniveau". Deze drie technologieniveaus 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 *state of the art* t is puur objectief. De subjectieve aspecten houden in geval van een strafbaar feit rekening met de wetten, zij hebben echter geen betrekking op de definitie van *state of the art* zelf.

Bijgevolg kan State of the Art worden omschreven als de procedures, apparatuur of werkmethoden die beschikbaar zijn in de handel in goederen en diensten waarvan de toepassing het meest effectief is bij het bereiken van de respectieve doelstellingen op het gebied van rechtsbescherming[10].

Kortom kan worden gezegd dat de *state of the art* de beste prestaties beschrijft van een onderwerp dat beschikbaar is op de markt om een object te bereiken. Het onderwerp is de IT-beveiligingsmaatregel; het doel is de wettelijke IT-beveiligingsdoelstelling.

Technische maatregelen in de fase "bestaande wetenschappelijke kennis en onderzoek" zijn zeer dynamisch in hun ontwikkeling en gaan over in de fase *state of the art* wanneer ze marktrijpheid bereiken (of op zijn minst op de markt worden gelanceerd). De dynamiek neemt daar af, bijvoorbeeld door processtandaardisatie. In de fase "algemeen aanvaarde technologieregels" zijn ook technische maatregelen op de markt beschikbaar. Hun mate van innovatie neemt af, hoewel ze in de praktijk zijn bewezen en vaak in overeenkomstige

---

6 De term technologieniveau wordt gebruikt als vervanging voor State of Technology.
7 Als alternatief kan “Bestaande wetenschappelijke kennis en technologie” worden gebruikt. In deze richtlijn zal “bestaande wetenschappelijke kennis en onderzoek” (ESKR) wordt gebruikt, zodat onderscheid kan worden gemaakt tussen dit en 'state of the art'.
8 Dr Mark Seibel, rechter in hoger beroep: https://www.dthg.de/resources/Definition-Stand-der-Technik.pdf
9 BVerfGE, 49, 89 (135 f)
10 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.

normen worden beschreven.

Als gevolg van vooruitgang kan een verschuiving tussen de afzonderlijke technologische fasen worden waargenomen ("innovatieve verschuiving").

1. Een maatregel zal in initieel de fase "bestaande wetenschappelijke kennis en onderzoek" stadium bereiken.
2. Wanneer het op de markt wordt gebracht, zal het overgaan naar de fase *state of the art*,
3. en aangezien het meer op de markt wordt gedistribueerd en erkend, zal het op een bepaald moment worden gekwalificeerd als "algemeen aanvaarde regels van technologie."

Om het vereiste bewijsmateriaal te leveren oriëntatie van hun eigen maatregelen op basis van het niveau van de *state of the art* volstaat het niet om de toegepaste maatregelen eenmalig te evalueren en bij te werken door patches te installeren. Een dergelijk bewijs kan alleen succesvol zijn door de uitgevoerde maatregel op gezette tijden met transparante methoden te vergelijken met de op de markt beschikbare alternatieven.

2.2 Methode voor het bepalen van de State of the Technologie

De technische maatregelen beschreven in hoofdstuk 3.2 van deze richtlijn werden geëvalueerd met behulp van een uitvoerbare methode gebaseerd op een eenvoudig beginsel van het beantwoorden van centrale vragen over de "mate van erkenning" en "mate van bewijs in de praktijk". De gebruikte centrale vragen zijn bewust geformuleerd en zorgen voor een meer gedetailleerd beeld van de twee dimensies van het onderzoek.

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

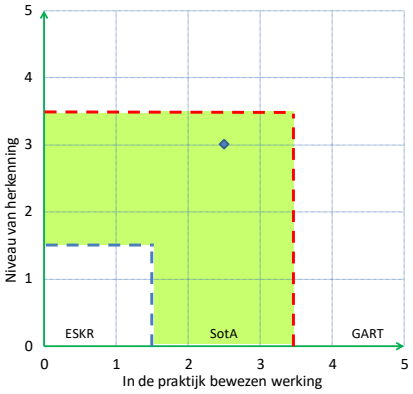
De volgende afbeelding toont het door de AK-SdT gebruikte sjabloon met de centrale vragen om de stand van de technologie voor een technische maatregel te evalueren:

1.1 Vragen over de mate van erkenning			Beoordeling moet worden ingevuld door SotA werkgroep
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	☐ j a, 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 SotA werkgroep
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	☐ één keer per jaar	☐ minder frequent	nee ja - grote ja - veel
(licht hier uw antwoord toe)			
		Gemiddelde	

Afbeelding 2: Evaluatiecriteria

Op basis van een puntensysteem wordt met de antwoorden een gemiddelde gevormd. Met deze verkregen waarden kan de actie in het diagram worden gegroepeerd:



ESKR	stand wetenschappelijk en onderzoek
SotA	stand van de techniek (
GART	algemeen erkende regels van de technologie

Afbeelding 3: Voorbeeld van State of the Art classificatie

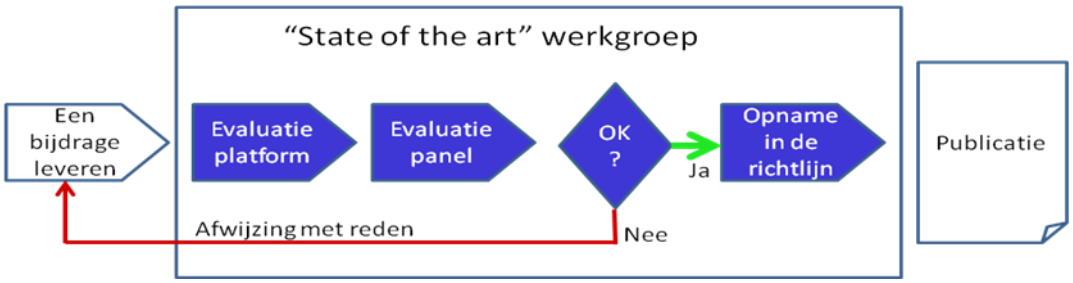
Zoals te zien is in het diagram, wordt een maatregel geclassificeerd als *state of the art,* als deze zich op basis van de gebruikte methoden binnen het groene veld bevindt.

In deze richtlijn worden technologieën en methoden beschreven en geëvalueerd, maar geen specifieke beveiligingsproducten. Daarom wordt bijvoorbeeld de geschiktheid van de hier beschreven maatregelen geacht te zijn vervuld voor het desbetreffende doel.

In de bedrijfspraktijk moet een geschikte methode (zoals vergelijkbaar met de hier beschreven methoden) worden aangepast aan de bestaande omstandigheden in de organisatie om zo op objectieve wijze de uitgevoerde maatregelen objectief te evalueren, te vergelijken met alternatieven en deze als bewijs te documenteren[11].

2.3 Proces voor kwaliteitsborging van de richtlijn

De werkgroep *state of the art* streeft ernaar om een hoge kwaliteit van de inhoud in de richtlijn te waarborgen. Om dit te bereiken is in de AK-SdT een proces opgezet waarin de 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 gestandaardiseerde sjabloon is ingediend (zie Afbeelding 4), wordt de bijdrage via een evaluatieplatform anoniem geëvalueerd door IT-beveiligingsexperts. De resultaten hiervan worden besproken en vastgesteld door het reguliere evaluatiepanel van de AK-SdT[12]. Als evaluatiecriteria dienen onder andere de in het sjabloon gedefinieerde centrale vragen en de antwoorden, tezamen met technische correctheid en de valuta van de inhoud.

Als het evaluatiepanel tot de conclusie komt dat een bijdrage niet voldoet aan de vereiste kwaliteit, wordt deze voor opname in de richtlijn met motivering afgewezen en wordt de

11 Lawicki, "Was bedeutet Stand der Technik?", gepubliceerd in het TeleTrusT Sonderbeilage "Sicherheit & Datenschutz" in het tijdschrift IX 6/2018

12 Op de webpagina van TeleTrusT wordt een lijst met leden die actief zijn in de Task Force (evaluatiepanel) 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/)

auteur op de hoogte gebracht. 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 alomvattende 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 hun beoogde doel en binnen hun werkingssfeer kunnen worden gebruikt.
- ***Integriteit***
  Integriteit verwijst in het bijzonder naar de gegevens. Integriteit wordt beschouwd als aanwezig te zijn, wanneer het zeker is, dat verzonden gegevens volledig en ongewijzigd door de ontvangers worden ontvangen.
- ***Vertrouwelijkheid***
  Vertrouwelijkheid wordt geacht te bestaan wanneer gevoelige gegevens alleen beschikbaar worden gesteld aan geautoriseerde personen en wel op toegestane wijze.
- ***Authenticiteit***
  Authenticiteit bestaat wanneer de unieke identiteit van de communicatiepartners (en die van de communicerende componenten) is gewaarborgd.

Naast deze op ITSiG gerichte IT-beveiligingsdoelstellingen, zijn er andere beschermingsdoelstellingen, die hier, vanwege de eerder genoemde GDPR[13], met name worden genoemd:

- ***ontkoppelbaarheid (+ gegevensminimalisatie);***
- ***transparantie;***
- ***interventievermogen***.

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

Terwijl het hoofddoel vanuit het oogpunt van IT-beveiliging de bescherming van gegevens en infrastructuur is, is de belangrijkste doelstelling vanuit het perspectief van de gegevensbescherming de bescherming van de mensenrechten. Het is belangrijk om deze verschillende standpunten te begrijpen om beschermende maatregelen vast te stellen en dienovereenkomstig uit te voeren.

13 Geïnspireerd door het onafhankelijke centrum voor privacybescherming Schleswig-Holstein (ICPP): https://www.datenschutzzentrum.de/

3 Technische en organisatorische maatregelen (TOMS)

De ITSiG en de GDPR vereisen naleving van, of op zijn minst het rekening houden met, de stand van de techniek van de technische en organisatorische maatregelen. De wetgever specificeert de relevante systemen en componenten niet verder. 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 gegevensoverdracht en gegevensopslag.

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

3.1 Algemene informatie

Toepassing met betrekking tot het gebruik in het kader van de ITSiG zijn soms zeer specifiek. Dit varieert van gemeenschappelijke normen, zoals veilige e-mailcommunicatie, tot veeleisende vereisten, zoals, als dat nodig is veilige controlefunctionaliteit in een elektriciteitscentrale.

Als gevolg hiervan is het zeer moeilijk om een volledige lijst van toepassing in deze studie op te stellen en ook dit toepassen te beschrijven. Omdat er vele manieren zijn om een doel te bereiken, kan IT-beveiliging veelal ook anders worden geïmplementeerd en bestaat er dus niet ÉÉN implementatie van veilige architectuur. Het is daarom bedoeld om essentiële elementen te identificeren die kunnen worden opgevat als *state of the art* in de zin van bruikbaar in de huidige IT-beveiliging.

De beschermingsbehoeften zijn in elk geval afhankelijk van de toepassing. Volgens de ITSiG moeten de IT-beveiligingsdoelstellingen van beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit worden nageleefd, zelfs als ze worden beoordeeld op individuele situaties met verschillende van toepassing zijnde beschermingsbehoeften. Dit betekent dat met name rekening moet worden gehouden met de volgende beschermingsdoelstellingen:

- Bescherming tegen aanvallen gericht op het ongeoorloofd lezen, wijzigen of verwijderen van verzonden en opgeslagen gegevens.
- Bescherming tegen aanvallen op de beschikbaarheid van de respectieve diensten en gegevens van de operator en gebruik
- Bescherming tegen ongeoorloofde manipulatie van bedrijf- en applicatiesystemen, enz.

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

Functionaliteit die de gewenste IT-beveiligingsapplicatie realiseert, moet te allen tijde volledig en correct worden geïmplementeerd. Dit moet worden geverifieerd door een onafhankelijke accountant. Implementatie moet altijd *state of the art* methoden bevatten, deze omvatten:

- 2-factor-authenticatie (2FA);
- Wederzijdse authenticatie
- Versleuteling van de communicatie tijdens het transport
- Versleuteling van de gegevens (bijvoorbeeld tijdens opslag)
- Bescherming van de privésleutel tegen ongeoorloofd kopiëren
- Gebruik van veilige opstartprocessen
- Veilig softwarebeheer inclusief patchbeheer
- Veilig gebruikersbeheer met actieve vergrendelingoptie
- Veilig toewijzen van netwerkzones voor extra bescherming op netwerkniveau
- Veilige datacommunicatie tussen verschillende netwerkgebieden
- Veilig surfen op het internet
- Realisatie van het need-to-know principe
- Realisatie van de minimale aanpak (inclusief hardening)

- Realisatie van logging, monitoring, rapportage en response management systemen
- Realisatie van malwarebescherming
- Gebruik van beveiligde back-upsystemen om verlies van gegevens te voorkomen
- Meerdere systeemlay-outs voor het implementeren van hoge beschikbaarheid, enz.

Naast de individuele technische applicatiefuncties moet ook de beveiligingsarchitectuur als geheel in aanmerking worden genomen. Hiertoe moeten onder de voorwaarden voor dit doel de volgende punten moeten worden geëvalueerd (Voor de implementatie van de IT-beveiligingscatalogus in overeenstemming met EnWG Sectie 11 vereist BNetzA[14] een hoge risicobeoordeling als standaard of kritiek voor kritieke processen en applicaties.):

- Het moet de gebruiker duidelijk zijn onder welke voorwaarden hij het betreffende systeem in de desbetreffende veilige configuratie kan gebruiken en toepassen. Als er op één apparaat verschillende operationele scenario's mogelijk zijn (zoals toegang tot kantoor-IT via sessie 1 en toegang tot een IT-proces via sessie 2), dan moet dit in elk geval duidelijk aan de gebruiker worden getoond.
- 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 tot het einde van de levenscyclus van het product op een veilige en moderne manier in kaart kunnen worden gebracht. Hiervoor beveelt het BSI up-to-date algoritmen aan in een catalogus voor cryptografiestandaarden.
- Het product of de desbetreffende dienst mag geen achterdeuren bevatten die manipulatie van gegevens en applicaties mogelijk maken.
- De fabrikant mag geen toegangsinterfaces hebben die onafhankelijk van de bediener kunnen worden gebruikt.
- Het is raadzaam om de implementatie van de beveiligingsfunctie te laten verifiëren door vertrouwde derden.
- De processen die in de aanvraag worden geïmplementeerd (zoals gebruikersautorisatie, sleutelbeheer, enz.) moeten veilig in kaart worden gebracht.

Andere criteria waaraan moet worden voldaan om een product te evalueren in termen van *state of the art* zijn als volgt:

- Het product of de dienst moet rekening houden met internationale normen en moet inter-operabel zijn met standaardprotocollen.
- Als er branchespecifieke normen bestaan, dan moet hiermee rekening worden gehouden bij de implementatie.
- Het product of de dienst moet een betrouwbare werking van de componenten versoepelen (marktrijpheid).
- Het product of de dienst moet in de praktijk met succes zijn getest.
- Evaluatie moet de oplossing beschouwen als een eenheid waar hardware en software aan elkaar gekoppeld zijn.
- Het product moet op het gebied van beveiliging en applicatiefunctionaliteit veilig kunnen worden bijgewerkt

De fabrikant van de oplossing is ook onderworpen aan criteria voor het evalueren van de oplossing die moet worden overwogen bij het kiezen van *state of the art* implementaties. De fabrikant kan investeringszekerheid garanderen voor de betreffende implementatie, dit betekent dat de volgende controles moeten worden uitgevoerd:

- De financiële achtergrond van de fabrikant garandeert verdere levensduur van het product.
- Voor het betreffende product een vastgesteld productbeheer en voor verdere ontwikkeling voor de gebruiksperiode van de gebruiker bestaat een routekaart.
- Het product is tijdens de gebruiksperiode niet aangemerkt als een beëindigd product.

14 Het Bundesnetzagentur is het Duitse Federale Netwerk Agentschap

- De fabrikant reageert proactief op kwetsbaarheden die onder haar aandacht komt en haar product beïnvloeden, lost ze op korte termijn op en stelt de nodige software-updates snel beschikbaar.
- De fabrikant produceert de betreffende oplossing in een omgeving met vertrouwd personeel.
- De fabrikant heeft onafhankelijk de controle over alle beveiligingsfuncties en vertrouwt niet op andere leveranciers met betrekking tot de beveiligingsfuncties.

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

3.2 Technische maatregelen

3.2.1 Beoordelen van de wachtwoordsterkte

De maatregel simuleert praktische aanvallen op veilig opgeslagen/gehashte inloggegevens en meet de objectieve veerkracht op basis van wiskundige methoden, persoonlijk gedrag, enz. De maatregel maakt een grondige inventarisatie en evalueert alle, zelfs onbekende, wachtwoorden. De maatregel bepaalt het niveau van naleving van de interne richtlijnen binnen het bedrijf en ondersteunt of faciliteert, in overeenstemming met de GDPR, de implementatie van beveiligingsmaatregelen, zoals het attenderen van werknemers als onveilige wachtwoorden worden gebruikt.

Tegen welke dreiging(en) wordt deze maatregel ingezet?
De maatregel moet het risico van misbruik van accountgegevens (inloggegevens) voorkomen.

80% van de IT-beveiligingsincidenten die leiden tot openbaarmaking van accountgegevens - privégegevens, persoonlijke gegevens en bedrijfsgegevens, kan worden toegeschreven aan zwakke en/of gestolen wachtwoorden (Verizon Report, 2017).

Het naleven van statisch wachtwoordbeleid voor gebruikersaccounts blijkt daarom geen adequate maatregel te zijn voor het implementeren van sterke, veilige wachtwoorden. Het wachtwoordbeleid misleidt en creëert zo een schijnzekerheid.

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?
Over het algemeen gebruiken bedrijfsnetwerken een centrale opslag voor inloggegevens van gebruikers en die worden gebruikt om gebruikers te verifiëren die toegang hebben tot services en/of werkstations (bijvoorbeeld Microsoft Active Directory).

Alle moderne inloggegevens-registratiesystemen gebruiken hash-functies voor wachtwoorden die bedoeld zijn om te voorkomen dat aanvallers met toegang tot de centrale database in platte tekst wachtwoorden kunnen ophalen.

Hoewel deze hash-functionaliteit biedt cruciale bescherming van wachtwoorden tegen ongeautoriseerde toegang, voorkomt het ook dat een organisatie wachtwoorden kan evalueren. Dit is echter nodig om maatregelen te treffen tegen mogelijke aanvallen - zoals het als wachtwoord uitproberen van woorden uit het woordenboek, het gebruik van wachtwoorden waarvan bekend is dat ze zijn gecompromitteerd of het raden van wachtwoorden met behulp van persoonlijke informatie over het doelwit.

De beoordeling van de wachtwoordbeveiliging definieert de veerkracht van een wachtwoord door een daadwerkelijke aanval te simuleren die verschillende potentiële zwakke punten gebruikt en exploiteert, zoals voorspelbare/zwakke wachtwoorden, wachtwoorden die door meerdere gebruikers worden gebruikt, defecte cryptografische implementaties, enz.

Op deze manier worden opgehaalde wachtwoorden verwerkt volgens nationale, regionale en interne regels voor gegevensbescherming zonder informatie over specifieke gebruikers of wachtwoorden bekend te maken of op te slaan.

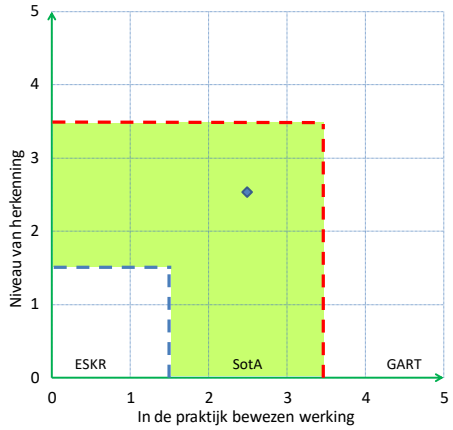
Verkregen wachtwoorden worden vervolgens beoordeeld op basis van objectieve wiskundige en structurele entropie - en subjectieve – het naleven van de wachtwoordrichtlijn - criteria. Zodra de beoordeling is voltooid, worden de (platte tekst)-wachtwoorden verwijderd en wordt een zinvol rapport gegenereerd.

De resultaten van het beoordelen van de wachtwoordbeveiliging - het auditrapport - stellen de organisatie in staat om de exacte beveiligingsrisico's van de wachtwoorden die in verschillende veelvoudige en heterogene systemen worden gebruikt, te meten. Zo kunnen de beste bewustmaking- en opleidingsmaatregelen voor gebruikers worden gedefinieerd en kunnen centrale handhavingmethoden worden geïdentificeerd voor sterke wachtwoorden. Hierdoor kan ook de doeltreffendheid van de al ingevoerde maatregelen worden herzien en verbeterd.

Welke beschermingsdoelen worden met deze maatregel bereikt?

☐ Beschikbaarheid
☐ Integriteit
☐ Vertrouwelijkheid
☐ Authenticiteit

Classificatie van het technologieniveau



3.2.2 Afdwingen van sterke wachtwoorden

De maatregel dwingt het gebruik van sterke, veilige wachtwoorden af, voor alle technische en organisatorische maatregelen die door de organisatie worden genomen.

De sterkte van het wachtwoord wordt door middel van een regelmechanisme geschaald naar het beveiligingsniveau van het betreffende gebruikersaccount. Het gedefinieerde beveiligingsniveau is gebaseerd op de potentiële impact van het compromitteren van de beveiliging van dit account.

Tegen welke dreiging(en) wordt deze maatregel ingezet?

80% van de IT-beveiligingsincidenten die leiden tot de openbaarmaking van accountgegevens - privégegevens, persoonlijke gegevens en bedrijfsgegevens - kan worden toegeschreven aan zwakke en/of gestolen wachtwoorden (Verizon Report 2017).

Daarom is gebleken dat het naleven van het statische wachtwoordbeleid voor gebruikersaccounts geen adequate maatregel is voor het handhaven van sterke, veilige wachtwoorden - de wachtwoordrichtlijn geeft een schijnzekerheid wat betreft het beveiligingsniveau.

De beschreven maatregel verhoogt het beveiligingsniveau van de gebruikte wachtwoorden tot een wachtwoord dat overeenkomt met het beveiligingsrisico (controle en detectie).

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?

Nieuw ingestelde wachtwoorden worden gecontroleerd aan de hand van een reeks regels die aan elk account zijn toegewezen en afzonderlijk voor verschillende categorieën worden

geparametriseerd.

De regels omvatten maatregelen voor: samenstelling (lengte, tekenset, symbolen, tekensequenties en herhalingen), wiskundige en structurele entropiewaarden, uniciteit (het wachtwoord mag niet worden gebruikt door een ander account op hetzelfde systeem binnen de organisatie), het gebruik van bekende standaardwachtwoorden en hergebruikte wachtwoorden (historisch). De regels zijn niet beperkt tot een zwarte lijst (blacklisting), maar kunnen individueel worden geparametriseerd.

De oplossing wordt centraal gebruikt en beheerd door één interface voor alle systemen binnen de organisatie.

Dit maakt coherent, systeembreed beleid effectief. Dit voorkomt ook meervoudig gebruik van wachtwoorden in verschillende systemen en maakt het mogelijk om centrale registratie van de wachtwoordgeschiedenis bij te houden.

Gegevens in platte tekst worden nooit opgeslagen of weergegeven. De eindgebruiker ontvangt een duidelijk bericht als zijn nieuwe wachtwoord wordt geweigerd, met uitleg over de reden. Dit ontlast het callcenter en beschermt de privacy van de gebruiker.

Alle communicatie tussen servers en systemen voor het afdwingen van sterke wachtwoorden wordt beveiligd met behulp van versleuteling.

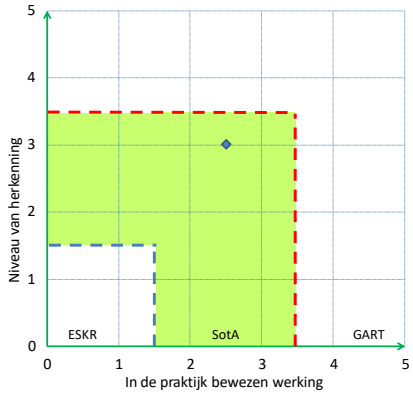
De beschreven maatregel zal voor elk geval resulteren in de centrale handhaving van voldoende wachtwoordsterkte en geeft de organisatie volledige toezicht, controle en documentatie van de wachtwoorden die in het bedrijf worden gebruikt. Het kan, met het gebruik van wachtwoorden, ook een adequaat niveau van beveiliging in bereiken voor verificatie (authenticatie).

De handhaving moet worden geëvalueerd aan de hand van een maatregel voor het beoordelen en evalueren van wachtwoorden. De veerkracht van de wachtwoorden die worden gebruikt voor daadwerkelijke aanvallen moet worden gemeten en bepaald en moet worden of de regels zoals verwacht effectief zijn of dat ze moeten worden bijgesteld om, zoals de omstandigheden kunnen vereisen, het gebruik van zwakke wachtwoorden te voorkomen.

Welke beschermingsdoelen worden met deze maatregel bereikt?

☐ Beschikbaarheid
☐ Integriteit
☐ Vertrouwelijkheid
☐ Authenticiteit

Classificatie van het technologieniveau



3.2.3 Multi-factor authenticatie

In de context van dit artikel wordt authenticatie gezien als bewijs van een bepaalde identiteit van een computersysteem. Al geruime tijd is de combinatie van gebruikersnaam en wachtwoord de meest voorkomende methode voor het authenticeren van een gebruiker

tijdens het inloggen. Het is nog steeds de meest gebruikte single-factor authenticatie methode voor het bewijzen van identiteit.12

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

Tegen welke dreiging(en) wordt deze maatregel ingezet?
Als een systeem met slechts één factor (single-factor authenticatie) is beveiligd, is de gebruikersidentiteit onderhevig aan een verhoogd risico op

- identiteitsdiefstal,
- misbruik van identiteit en
- identiteitsfraude.

Een factor alleen is niet genoeg om de login voor de toegang tot de computer/gebruiker die bescherming te beschermen - de methoden van digitale aanvallers worden steeds geavanceerder en de potentiële schade wordt, als gevolg van het toenemend gebruik van netwerken en van digitalisering, steeds drastischer. 81% van alle datalekken wordt veroorzaakt door gestolen of zwakke wachtwoorden (d.w.z. single-factor authenticatie)[15]. Deze zeer hoge waarden worden met name veroorzaakt door:

- Menselijke risico's bij het omgaan met wachtwoorden:
  - onvoldoende kwaliteit van wachtwoorden,
  - te vaak van hetzelfde wachtwoord gebruiken,
  - opzettelijke openbaarmaking van wachtwoorden (zoals delen met andere mensen) of
  - onbedoelde openbaarmaking van wachtwoorden (zoals opschrijven).
- Technische risico's bij het omgaan met wachtwoorden:
  - Man in the Middle aanvallen,
  - phishing-aanvallen,
  - keylogger gebaseerde aanvallen,
  - brute force aanvallen, enz.

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?
Naast het conventionele wachtwoord zijn verschillende andere authenticatiemethoden en -oplossingen (MFA-systemen) beschikbaar. Ze kunnen worden onderverdeeld in drie hoofdcategorieën:

- Op kennis gebaseerde factoren (zoals wachtwoord, pincode, wachtwoordzin, enz.)
- Op bezit gebaseerde factoren (zoals beveiligingstokens, smartcards, enz.)
- Op biometrie gebaseerde factoren (zoals vingerafdruk, iris, enz.)

MFA-systemen combineren meestal twee methoden uit verschillende categorieën in een authenticatieketen, hoewel sommige MFA-systemen ook toestaan dat een willekeurig aantal methoden aan elkaar worden gekoppeld. Het combineren van methoden uit slechts één categorie is niet aan te raden. Let wel: niet alle methoden uit deze drie categorieën zijn noodzakelijkerwijs gelijkwaardig, zelfs wanneer zij worden gecombineerd. Echter, elke combinatie is een verbetering ten opzichte van het gebruik alleen maar een wachtwoord. De beslissing welke authenticatiemethoden moeten worden gecombineerd, hangt af van de beschermingsbehoeften van de applicatie, van de gebruikersidentiteit en van de technische vereisten.

Bovendien bieden sommige MFA-systemen een dynamische benadering van gebruikersverificatie (adaptieve authenticatie). In dat geval is de combinatie van de verificatieketen niet langer statisch, maar situatieafhankelijk en flexibel. De volgende factoren kunnen bijvoorbeeld worden opgenomen: de geografische locatie van de gebruiker, het

15 Bron: Verizon Data Breach Investigations Report 2017

unieke ID en/of IP van het apparaat, de typische werktijd van de gebruiker, enz.

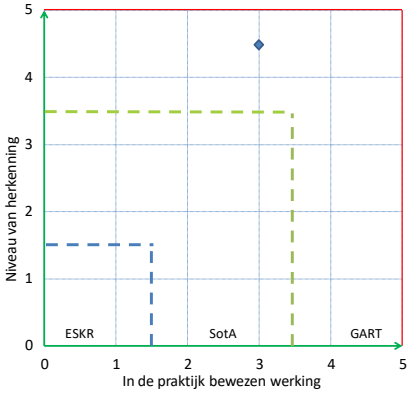
MFA kan nu in veel applicaties worden geactiveerd of maakt deel uit van de productopties. Als dit niet het geval is voor applicaties die bescherming vereisen, of als een bedrijf meerdere applicaties die bescherming vereisen gebruikt, wordt een centrale verificatieoplossing voor alle applicaties en gebruikers aanbevolen. Het gelijktijdig gebruik van verschillende oplossingen moet worden vermeden uit het oog op toenemende complexiteit, hogere kosten en grotere administratie-inspanning. Moderne MFA-oplossingen bieden een breed scala aan bruikbare methoden en ondersteunde eindapparaten, evenals een centraal authenticatie-exemplaar voor alle gebruikers, applicaties en systemen.

Vanwege bovengenoemde menselijke en technische risico's van single-factor authenticatie, stellen verschillende nationale en internationale regelgeving, zoals NIST, PSD2, kritische infrastructuur beschermingsprogramma's en de GDPR, evenals de Federal Financial Supervisory Authority (BaFin), het gebruik van MFA als eis voor het beschermen van de toegang van gebruikers tot een computersysteem dat bescherming vereist.

Welke beschermingsdoelen worden met deze maatregel bereikt?

☐ Beschikbaarheid
☐ Integriteit
☐ Vertrouwelijkheid
☐ Authenticiteit

Classificatie van het technologieniveau



3.2.4 Cryptografische toepassingen

De beschermingsdoelstellingen kunnen alleen worden doorgevoerd voor de aspecten integriteit, vertrouwelijkheid en authenticiteit en wel door een passende combinatie van alle drie de factoren. Dit hoofdstuk bevat aanbevelingen voor het gebruik en het kiezen van cryptografische toepassingen.
Cryptografische toepassingen worden voor verschillende doeleinden gebruikt en vormen de basis voor veel IT-beveiligingsmaatregelen. Moderne cryptografie wordt gebruikt in:

- Authenticatie procedures;
- Waarborgen van de authenticiteit;
- Toegangscontrole;
- Implementatie van weerlegbaarheid en onweerlegbaarheid;
- Delen van geheimen;
- Implementeren van anonimeringprocedures;
- Verkiezing en stemming (committment procedures);
- Crypto-currencies;
- +Digital Rights Management (DRM);

en veel andere scenario's.

Een gemeenschappelijk kenmerk van deze toepassingen is, dat ze in de eerste plaats dienen om vertrouwelijkheid en authenticiteit te garanderen. Dit betekent bijvoorbeeld het voorkomen van diefstal van vertrouwelijke gegevens of onopgemerkte manipulatie van

gegevens.

Cryptografische toepassingen zijn bedoeld om het principe van Kerckhoff te vervullen. Open algoritmen kunnen systematisch door een grote, wereldwijde gemeenschap van experts worden geëvalueerd op zwakke punten en worden geoptimaliseerd. Dit is ongeveer hoe de huidige standaard voor symmetrische encryptie, AES, werd en wordt gemaakt, in een openbare wedstrijd. Het wordt als zeer veilig beschouwd.

Het beveiligingsniveau van een cryptografische methode geeft aan, welke inspanning een aanvaller moet leveren, om platte tekst te produceren. Eenvoudig gezegd: dit neemt toe met het aantal beschikbare opties voor het kiezen van de sleutel (de bit-lengte).

Als gevolg van de toenemende rekenkracht, analytische vooruitgang en technische mogelijkheden, bestaat het risico dat met een aanval op een cryptografische methode, deze bekend zal worden en het niveau van beveiliging tot praktisch haalbaar wordt teruggebracht. Het is ook mogelijk dat iemand er in slaagt een kwantum computer te bouwen, waarmee veel sneller een *brute force* opdracht kan worden uitgevoerd en het niveau van bescherming van de symmetrische encryptie drastisch naar beneden haalt. Veel asymmetrische encryptie zou met behulp van beschikbare kwantum computers volledig worden gebroken.

Voor zekerheid of de gebruikte cryptografische methoden effectief zijn, moeten ze ongeveer één keer per jaar worden gecontroleerd.

De huidige versie van de aanbevelingen is door het BSI gepubliceerd als Technical Guidelines TR-02102[16]. In documenten van het Amerikaanse NIST, ENISA en andere organisaties zijn nadere aanbevelingen te vinden [17][18][19][20][21][22].

Op dit moment kunnen en met name worden de volgende aanbevelingen gedaan:

- Symmetrische versleutelingmethoden: AES-128, AES-192, AES-256 idealiter met GCM als bedrijfsmodus. EAX-modus wordt ook aanbevolen als omwille van resources een stream cipher is vereist en een iets hogere vertraging als gevolg van het versleutelen aanvaardbaar is. In moderne systemen moet als de bedrijfsmodus Authenticated Encryption met Associated Data (AEAD) worden gebruikt.
  Bedrijfsmodi zonder extra Message Authentication Code (MAC) en zonder verdere integriteitbescherming worden over het algemeen als onveilig beschouwd en mogen niet worden gebruikt.
- Asymmetrische versleutelingmethoden: ten minste ECIES-250, DLIES-2000, RSA 2000, curve25519, curve448 of ECC Brainpool. ECIES moet worden gebruikt met 384 of meer bits. Als DLIES of RSA wordt gebruikt, moet 3072 bits of meer bits worden gebruikt.
- Hash-functies: Let op SHA-256, SHA-384, SHA-512, SHA3-256, SHA3-384 en SHA3-512. De SHA1 en MD5 algoritmen zijn niet langer *state of the* art.
- Sleutelafleiding functies (KDF) en wachtwoord-hashes: Huidige geschikte algoritmen zijn[23]: Argon2, PBKDF2, scrypt en bcrypt. Nieuwe systemen moeten het Argon2 algoritme gebruiken.

---

16 Zie: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html
(Engelse versie: https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/tr02102/tr02102_node.html)
17 BSI TR-02102-1 "Cryptographic Mechanisms: Recommendations and Key Lengths" version: 2018-02
18 NIST Special Publication 800-57 Part 1 Revision 4: Recommendation for Key Management Part 1: General
19 NIST Special Publication 800-175B: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
20 European Union Agency for Network and Information Security: Algorithms, key size and parameters report – 2014
21 https://eprint.iacr.org/2015/1018.pdf
22 https://safecurves.cr.yp.to/
23 https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet

- (Random number generators:
  - fysieke generatoren voor willekeurige getallen, functionaliteitklasse PTG.2 of PTG.3[24]
  - deterministische generatoren voor willekeurige getallen, functionaliteitklasse DRG.3 en DRG.4
- TLS[2526]: TLS 1.3 gecombineerd met forward secrecy met behulp van veilige algoritmen volgens BSI TR-02102-2, tabel 1[27]. Het gebruik van hulpmiddelen zoals: https://www.owasp.org/index.php/O-Saft en https://www.ssllabs.com/ssltest/ helpt bij het inspecteren van de TLS-configuratie.

Opmerking:
Side-channel aanvallers zijn een relevant probleem voor cryptografie. Het kiezen van "aanbevolen" algoritmen beschermt wel tegen analytische aanvallen, maar niet tegen side-channel aanvallen. Deze aanvallen worden doorgaans gemaakt aan de hand van het meten van fysieke parameters zoals looptijden, stroomverbruik, warmte en trillingen.

Potentiële side-channels zijn vooral afhankelijk van de implementatie van het algoritme en het gebruikte platform. De side-channel bestendigheid van IT-beveiligingsproducten varieert per provider. Werk bij twijfel samen met gespecialiseerde dienstverleners.

3.2.5 Versleuteling van harde schijven

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

Tegen welke dreiging(en) wordt deze maatregel ingezet?
Deze maatregel beschermt gegevens op de harde schijven van onbeheerde, uitgeschakelde eindapparaten zoals PC's, laptops, tablets of 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. Als apparaten op deze manier worden beschermd, levert het kopiëren van de Read-Only geheugens, omdat deze versleuteld zijn, alleen nutteloze gegevens.

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?
De gegevensdrager(s) die in een systeem zijn geïnstalleerd, zoals magnetische harde schijven of op flashgeheugen gebaseerde SSD's waarop het besturingssysteem en vertrouwelijke bedrijfsgegevens zijn opgeslagen, worden door de maatregel zodanig versleuteld dat het ongeautoriseerd lezen ervan geen platte tekst biedt. Dit geldt zowel voor het geval van het uitlezen met het systeem uitgeschakeld of als de harde schijf is verwijderd en ook voor het tijdens het gebruik aftappen van de gegevens aan de interface van de interne harde schijf (eSATA etc.).

Bij symmetrische versleuteling moet ten minste AES-256 in de XTS-modus worden

---

24 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf
25 Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths Part 2 - Use of Transport Layer Security (TLS)
26 NIST Special Publication 800-52 Revision 1 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
27 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf (Engelse versie: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-2.pdf)

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 het kiezen 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 het ook mogelijk om hardwareondersteunde vertragingsmechanismen te gebruiken bij meerdere onjuiste wachtwoordvermeldingen. Het maakt het zinloos om de schijf uit te breiden voor analyse in een systeem van de aanvaller.

Voor zover het apparaat het toelaat, zoals met 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 versleutelingmechanismen.

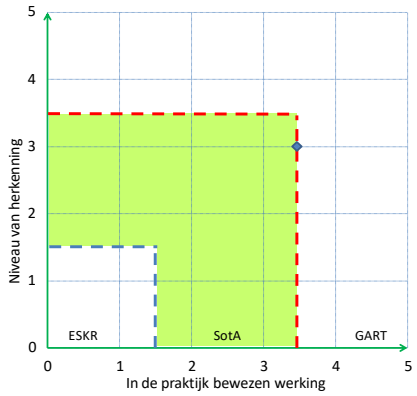
Sommige beschikbare oplossingen ondersteunen ook volledige of mapgebaseerde (folder-based) versleuteling van verwisselbare media. Binnen organisaties heeft automatische, voor de gebruiker transparante, versleuteling van bedrijfsgegevens de voorkeur om platte tekst opslag als gevolg van bedrijfsfouten te voorkomen.

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

Welke beschermingsdoelen worden met deze maatregel bereikt?

- ☐ Beschikbaarheid
- ☐ Integriteit
- ☐ Vertrouwelijkheid
- ☐ Authenticiteit

Classificatie van het technologieniveau



3.2.6 Versleuteling van bestanden en mappen

Bestands- en mapversleuteling omvatten de versleuteling van afzonderlijke objecten, zoals containers, mappen of afzonderlijke bestanden, daarom wordt dit type versleuteling ook wel objectversleuteling genoemd. De voor dit doel beschikbare programma's 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. Er moet dus voor worden gezorgd dat niemand anders dan de gemachtigde personen toegang heeft tot de beschermde informatie. Dit kan in individuele gevallen persoonsgegevens of, in het ergste geval, het voortbestaan van een organisatie in gevaar brengen.

Bovendien is objectversleuteling handig bij het gebruik van cloudservices, omdat het effectief voorkomt dat gegevens door operators worden geopend.

Tegen welke dreiging(en) wordt deze maatregel ingezet?

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

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?

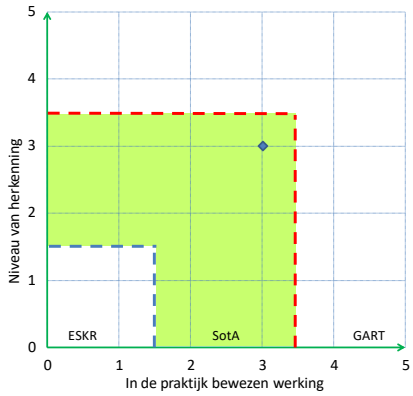
Bestand- en mapversleuteling omvatten de versleuteling van afzonderlijke objecten, zoals containers, mappen of afzonderlijke bestanden, daarom wordt dit type versleuteling ook wel objectversleuteling genoemd. De programma's die hiervoor beschikbaar zijn, werken vaak transparant, wat betekent dat gebruikers 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 vervoeren en te voorkomen dat onbevoegden er toegang toe krijgen.

Welke beschermingsdoelen worden met deze maatregel bereikt?

☐ Beschikbaarheid
☐ Integriteit
☐ Vertrouwelijkheid
☐ Authenticiteit

Classificatie van het technologieniveau



3.2.7 E-mailversleuteling

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

Tegen welke dreiging(en) wordt deze maatregel ingezet?

- het bespioneren of manipuleren van e-mailberichten tijdens transport;
- het bespioneren of manipuleren van opgeslagen e-mailberichten.

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?

Versleutelde e-mailtransmissie (transportversleuteling); TLS

Versleuteling van e-mailinhoud; S/MIME of PGP

De beveiligingseisen voor e-mail zijn onder andere gebaseerd op het type gegevens dat in het mailsysteem wordt verzonden en opgeslagen. Bij zakelijke transacties kan over het algemeen worden aangenomen dat e-mailberichten voor de organisatie op zijn minst belangrijke informatie bevatten. Gepersonaliseerde e-mailadressen blijven als persoonsgegevens worden beschouwd; er kan dus van worden uitgegaan dat per e-mailbericht persoonsgegevens zullen worden verzonden en opgeslagen. In individuele

gevallen en afhankelijk van het gebruik van e-mail kunnen ook gegevens met speciale beschermingsbehoeften worden verzonden, zoals gegevens over gezondheid of cliëntgegevens van advocaten of bijzonder waardevolle bedrijfsgeheimen zoals ontwerpgegevens.

Dit resulteert in de volgende beveiligingseisen voor e-mail:

- Bescherming tegen ongeoorloofde toegang tot of wijziging van e-mailberichten tijdens transport en opslag (beschermingsdoelstelling: vertrouwelijkheid);
- Bescherming tegen latere wijziging van e-mailberichten die voor lange termijn worden gearchiveerd (beschermingsdoelstelling: integriteit).

Deze beschermingsdoelstellingen kunnen doorgaans worden bereikt met versleuteling. Voor e-mailversleuteling moet onderscheid worden gemaakt tussen het versleutelen van de transmissie (transportversleuteling) en het versleutelen van het e-mailbericht (of end-to-end encryptie). De beschermingsdoelstellingen vereisen het gebruik van transportversleuteling, althans bij het verzenden van e-mailberichten via openbare netwerken. De protocollen die worden gebruikt bij het verzenden van e-mailberichten via het internet, namelijk SMTP, POP3 en IMAP, bieden echter in hun basisvorm ongecodeerde gegevensoverdracht. Grote delen van het e-mailverkeer worden daarom nog steeds onversleuteld verzonden, hoewel er al lange tijd veel 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 momenteel veilige versleutelingmethoden (bijvoorbeeld AES-256) worden gebruikt; onveilige versleutelingmethoden (bijvoorbeeld RC4) mogen niet worden gebruikt. Als algemene regel moet forward geheimhouding worden geactiveerd. Het is ook verstandig om de certificaten die voor TLS door de respectieve andere kant worden gebruikt, te inspecteren op echtheid en geldigheid, bijvoorbeeld met behulp van DANE (RFC 7671). De technische richtlijn TR-02102-02 van het BSI deel 2 van het BSI bevat een uitgebreide lijst met aanbevelingen voor TLS.

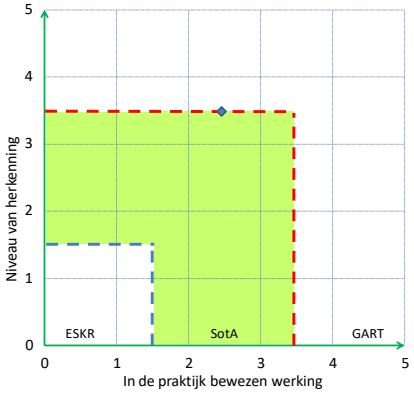
End-to-end encryptie wordt aanbevolen om bijzonder gevoelige gegevens te beschermen. Hiervoor zijn twee standaarden vastgesteld: S/MIME (Secure/Multipurpose Internet Mail Extensions, gedefinieerd in RFC 5751) en OpenPGP (Pretty Good Privacy, gedefinieerd in RFC 4880). Beide gebruiken in wezen dezelfde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

Bij het gebruik van end-to-end encryptie heeft geen enkel systeem in het transmissiepad toegang tot de inhoud van het e-mailbericht. Dit betekent echter dat het gebruik van inhoudsfilters, antivirus programma's, anti-spam, preventie van gegevensverlies en archivering volledig moet worden vermeden en daarom kan inhoudsversleuteling (content encryptie) alleen zinvol worden gebruikt tussen organisaties; dit betekent dat e-mailberichten versleuteld en ongecodeerd zijn in de overdracht van het openbare internet naar het particuliere netwerk (gateway) van de organisatie (end-to-end encryptie van de organisatie), of zo nodig worden gecombineerd met interne versleuteling van bedrijfsinhoud.

Welke beschermingsdoelen worden met deze maatregel bereikt?

- ☐ Beschikbaarheid
- ☐ Integriteit
- ☐ Vertrouwelijkheid
- ☐ Authenticiteit

Classificatie van het technologieniveau



3.2.8 Beveiligen van elektronisch dataverkeer met PKI

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

De eIDAS-verordening28 die sinds de zomer van 2016 van kracht is, voorziet ook in het gebruik van een PKI.

Tegen welke dreiging(en) wordt deze maatregel ingezet?

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

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?

De volgende maatregelen zijn zinvol tegen de hierboven beschreven bedreigingen:

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

De digitale certificaten worden afgegeven door de certificaatautoriteit (CA) van een PKI-organisatie. De geldigheid van openbare sleutels wordt bevestigd door de digitale handtekeningen van de CA. Samen met 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 te behouden, moet de identiteit van de aanvrager, ongeacht of hij of zij een persoon of organisatie heeft, worden onderworpen aan een ondubbelzinnige inspectie voordat het elektronische certificaat wordt afgegeven. Dit wordt gedaan door de Registratie Autoriteit (RA).

Een Validatie autoriteit (VA) is vereist om de geldigheid van digitale certificaten te controleren. In het algemeen wordt een onderscheid gemaakt tussen de controle op een gepubliceerde certificaatintrekking lijst (certificate revocation list of CRL) en real-time

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

validatie via een Online Certificate Status Protocol (OCSP) service. De keuze van het type inspectie is meestal per geval gebaseerd op het toepassingsscenario.

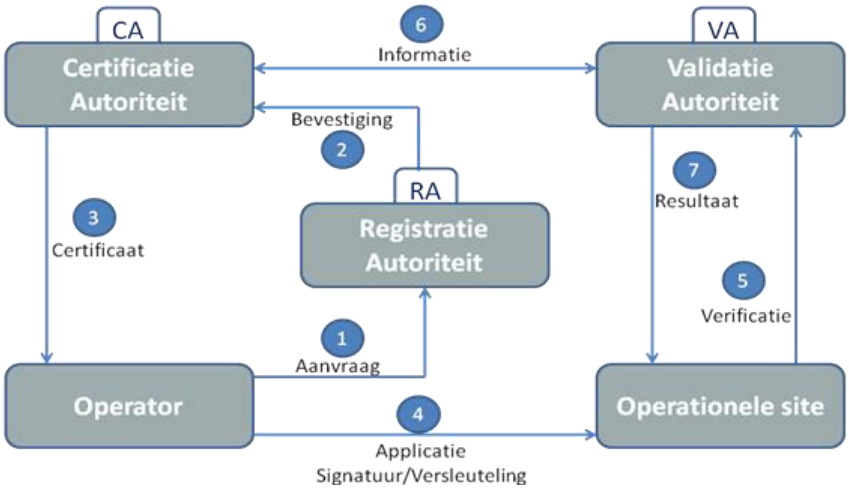
Afhankelijk van de juridische status van de PKI is in de meeste gevallen de wettelijk toelaatbare registratie van alle transacties in een PKI verstandig of zelfs noodzakelijk. Voor sommige toepassingsgebieden zijn ook gecertificeerde CA -producten vereist.

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

- Handtekening en versleuteling van e-mailberichten (S/MIME)
- Authenticatie en encryptie in het Internet of Things (IoT)
- Authenticatie en versleuteling op het web (HTTPS)
- Authenticatie en versleuteling voor VPN-diensten
- Verificatie- en integriteitbeveiliging voor uitvoerbare code (codeondertekening of code signing))
- Beveiliging van verificatie en integriteit voor documenten (digitale handtekening of digital signature)
- authenticatie van gebruikers/clients 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 Root-CA als een *trust anchor* tot een strikt hiërarchische PKI met verschillende sub-CA's. Ook kan cross certificering met andere PKI s worden geïmplementeerd. Dit varieert van een Root-CA als een zo genoemd vertrouwensanker tot een strikt hiërarchische PKI met meerdere sub-CA's. Ook kan een crosscertificering met andere PKI s worden geïmplementeerd.

Het volgende diagram toont in een werkstroom de structuur en interactie van de PKI -componenten.



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- n gasvoorziening, e-justitie (met beA, beN, beBPO), gezondheidszorg en de industrie- en non-profit sector (zoals federaties en verenigingen).

De eIDAS-verordening voorziet in het bijzonder in een uitgebreid scala aan gebruiksscenario's. Zo wordt een bewijs van identiteit en vertrouwensservices ondersteund door PKI's (zie onderstaande tabel).

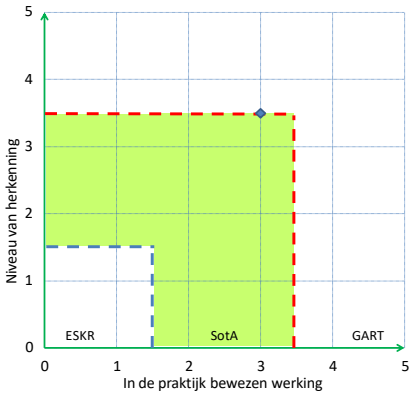
eIDAS voorschriften/toepassingsgevallen	
Identiteiten	Certificaten
	Elektronische ID's
Vertrouwensdiensten (Trust services)	Elektronische stempels (Electronic stamps)
	Elektronische tijdstempels (Time stamps)
	Website authenticatie
	Elektronische bezorgdiensten (Delivery services)
	Bewakingsdiensten (Preservation services)

Voorbeeld 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 zelfs bij TeleTrusT: https://www.ebca.de.

Welke beschermingsdoelen worden met deze maatregel bereikt?

☐ Beschikbaarheid
☐ Integriteit
☐ Vertrouwelijkheid
☐ Authenticiteit

Classificatie van het technologieniveau



3.2.9 Inzet van VPN (OSI layer 3)

Een layer 3 VPN beschrijft de verbinding van twee of meer netwerken op layer 3 van het OSI-model[29]. De verzonden gegevens worden versleuteld, hierdoor kunnen bijvoorbeeld bedrijfskantoren in verschillende landen veilig en vertrouwelijk via internet met elkaar worden verbonden.

Tegen welke dreiging(en) wordt deze maatregel ingezet?

Het gebruik van VPN's beschermt tegen:

- Verlies van vertrouwelijkheid als gevolg van ongecodeerde/slecht versleutelde verbindingen
- Externe aanvallers
- Verbindingsmanipulatie

29 https://www.itu.int/rec/T-REC-X.200-199407-I/en

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

- Uitstroom van sleutelmateriaal
- Zwakke cryptografie
- Denial of service: De beschikbaarheid van de VPN wordt bedreigd door fouten of aanvallen

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?

Een layer 3 VPN beschrijft de verbinding van twee of meer netwerken of de koppeling van een client aan een netwerk op OSI layer 3. De gegevens die in dit proces worden vervoerd, worden versleuteld en de VPN-eindpunten verifiëren en machtigen het andere respectievelijke VPN-eindpunt. Hierdoor kunnen bijvoorbeeld bedrijfskantoren in verschillende landen veilig en vertrouwelijk met elkaar worden verbonden via onveilige lijnen van derden, zoals internet of diensten die door een telecom provider worden ingehuurd. In vergelijking met een layer 2 VPN worden minder gegevens vervoerd, omdat layer 2-gegevens, zoals broadcasts, niet worden verzonden. Omgekeerd kan een layer 3 VPN hierdoor niet transparant worden gebruikt voor alle toepassingen.

Complexe topologieën, zoals on-demand VPN-verbindingen, kunnen soms alleen worden geïmplementeerd met een layer 3 VPN of het is aanzienlijk gemakkelijker 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 wordt aanbevolen om een layer 3 VPN van de fabrikant als oplossing te vinden.

Als 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. Hiervoor moet het apparaat versleuteling en verificatie uitvoeren met algoritmen en parameters die als veilig worden beschouwd. De fabrikant moet kunnen bewijzen dat hij actief werkt aan de beveiliging van de gebruikte cryptografie, hetzij door het vervangen van algoritmen die onveilig zijn geworden of door het kiezen van geschikte parameters. Waar dat technisch haalbaar is, moeten veilige mechanismen voor authenticatie 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 verificatie (zoals HTTPS voor een WebGUI, SSH voor consoletoegang, beveiligde authenticatie-informatie in hardware), maar ook de speciale aandacht van de fabrikant voor de beveiliging van het platform voor het VPN-apparaat zelf om ongeautoriseerde toegang vanwege technische tekortkomingen uit te sluiten.

Gevoelige informatie wordt doorgaans via een VPN getransporteerd.

Een layer 3 VPN met apparaten die backdoors bevatten of toestaan dat softwarebugs draaien, zodat de apparaten kunnen worden overgenomen, is een onaanvaardbaar risico. Daarom moeten producten die in staat zijn om een hoog niveau van platformbeveiliging en zelfbescherming aan kunnen tonen, zoals door middel van onafhankelijke inspecties (certificeringen of zelfs accreditatie), de voorkeur krijgen. De vereisten voor de operationele omgeving moeten blijvend waarborgen dat fysieke toegang tot VPN-apparaten alleen mogelijk is voor geautoriseerde personen.

Net als de doelstelling voor het beschermen van de vertrouwelijkheid is de integriteit van het

platform van cruciaal belang voor het behoud van de integriteit en authenticiteit van de gegevens die erdoorheen worden doorgegeven. Het is ook belangrijk dat de VPN-apparaten zijn geïnstalleerd op een extra gehard platform, uitstekende zelfbescherming hebben en geen backdoors hebben. De beveiligingsprotocollen die een layer 3 VPN gebruiken, garanderen ook de integriteit en authenticiteit van de getransporteerde gegevens. Ook het beheer en het veilige gebruik van sleutelmaterialen spelen een cruciale rol. De voorkeur moet worden gegeven aan fabrikanten die kunnen aantonen dat ze het genereren van willekeurige nummers, veilig sleutelbeheer voor private verificatiesleutels (zoals op chipkaarten) vergemakkelijken en de leeftijd van gebruikte coderingssleutels bijhouden.

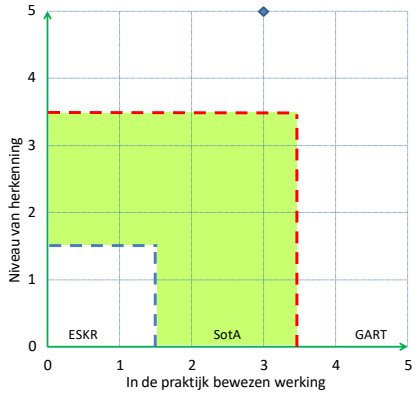
Om de beschikbaarheid van layer 3 VPN's voor VPN-endpoint-hardware en -software (zoals VPN-concentrators) te garanderen, zijn passende maatregelen nodig. Wat hardware betreft, moet de fabrikant kunnen aantonen dat het platform volgens de vereisten is ontworpen en geïmplementeerd voor hoge beschikbaarheid. Dit omvat bijvoorbeeld redundante voedingen, rekenkracht voor de verwerking en ventilatorconfiguratie waarbij het uitvallen van één ventilator niet het hele systeem laat uitvallen. Omdat deze maatregelen in de praktijk nog niet voldoende zijn om hardwarefouten te voorkomen, moet er de mogelijkheid van redundante werking zijn (configuratie met hoge beschikbaarheid). Monitoring speelt ook hier een belangrijke rol, opdat defecte hardware tijdig kan worden gedetecteerd. In dit geval moet de fabrikant passende monitoring ondersteunen, zoals met SNMP. Aan de softwarekant is het, om storingen te voorkomen, van cruciaal belang om speciale aandacht te besteden aan de juiste implementatie. De voorkeur moet worden gegeven aan fabrikanten die code reviews uitvoeren. Het is nog steeds belangrijk om te focussen op de bescherming tegen Denial of Service aanvallen. Een bijzonder veilig platform is ook hier een belangrijke vereiste, naast gecontroleerde toegang tot de gebieden waar de VPN-eindpunten (VPN-concentrators) in het LAN worden bediend.

De apparaten van een Layer 3 VPN maken loggegevens aan. Deze zijn uiterst belangrijk voor het opsporen van aanvallen op het netwerk. Deze gegevens moeten voor dit doel verplicht zijn, evenzo is het belangrijk om administratieve wijzigingen te kunnen volgen en dat deze loggegevens verplicht en dienovereenkomstig kunnen worden toegewezen. Dit betekent dat er opties moeten zijn zodat dergelijke loggegevens veilig worden opgeslagen en beschermd zijn tegen manipulatie (tamper-proof). Dit kan bijvoorbeeld worden gegarandeerd door lokale append-only logs, of door gebruik te maken van een interface naar externe logservers of SIEM-systemen.

Welke beschermingsdoelen worden met deze maatregel bereikt?

- ☐ Beschikbaarheid
- ☐ Integriteit
- ☐ Vertrouwelijkheid
- ☐ Authenticiteit

Classificatie van het technologieniveau



Opmerking: Hoewel er geen twijfel bestaat over de fundamentele noodzaak om VPN's te gebruiken, leveren fabrikanten regelmatig innovaties om hun beveiligingsniveau,

gebruiksvriendelijkheid en performance te verhogen. Zo wordt 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 Versleuteling op OSI 2

Layer 2- versleuteling is een beveiligingsoplossing alternatief aan layer 3 VPN's en wordt gebruikt op de payload van Ethernet-frames in plaats van op de IP-pakketten. IP-headers hoeven niet te worden verwerkt (wat tijd bespaart) en de belasting op de lijncapaciteit als gevolg van de overhead door het (de-)coderen is veel lager dan versleuteling op OSI 3 of hoger.

Tegen welke dreiging(en) wordt deze maatregel ingezet?
Het verzamelen en beoordelen van de enorme datavolumes van locatieverbindend verkeer (koppelpunten) via de (bedrijfsnetwerk-) backbone of de cloudverbinding als gevolg van beveiligingsproblemen in de netwerkhardware, netwerkproviders en niet-bewaakte ondergrondse of onderwater kabels en draadloze of satellietverbindingen, evenals DDoS-aanvallen op versleutelde layer 3-verbindingen.

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?
Het gebruik van versleuteling om WAN-communicatie tussen bedrijfslocaties en datacenters te beveiligen. Het gebruik van bandbreedteneutrale cryptografieoplossingen met zeer weinig vertraging voor layer 2 WAN-backbones en directe koppelingen (zoals dark fiber of Satcom). Layer 2-versleuteling is een beveiligingsoplossing die in bepaalde applicatie als een geschikt alternatief werkt voor layer3 VPN's. Het wordt toegepast op de payload van Ethernet-frames in plaats van op IP-pakketten. IP-headers hoeven niet te worden verwerkt (wat tijd bespaart) en er is geen encryptie overhead als gevolg van versleuteling (de lijnbandbreedte is volledig beschikbaar). Een Ethernet-gebaseerd netwerk (Point-to-Point, Hub-Spoke of Fully Meshed) via speciale kabels (koper/glasvezel) of een layer 2-service van netwerkproviders (zoals Carrier Ethernet-services) is vereist voor gebruik.

Typische toepassingen voor layer2-versleuteling zijn het beschermen van WAN-backbone lijnen (ook internationaal) en datacenter verbindingen binnen het bedrijfsnetwerk of voor vertrouwde cloud- en collocation-providers, evenals het beschermen van backbone-lijnen voor de campus die buiten gebouwen en over eigendommen van derden lopen.

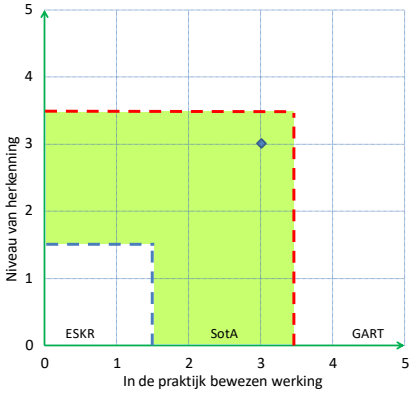
De prestatievoordelen zijn de moeite waard, vooral voor het gebruik van centrale IT-diensten, massale desktop-virtualisatie, datacenter-consolidatie en gedistribueerde en redundante opslagsystemen (SAN/NAS), met veel kleine of real-time relevante IP-pakketten (zoals VoIP, IoT of Smart Grid) en waarvoor overhead en -vertraging veroorzaakt door IPsec onaanvaardbaar zijn.

Het gebruik van deze netwerkversleutelingtechnologie vereist geen wijziging van bestaande IP-routeringconfiguraties. Dit type versleuteling is transparant voor vrijwel alle netwerkdiensten en -applicaties van OSI 3 en hoger en heeft geen meetbare invloed op de netwerkprestaties.

Externe cryptostations en het periodiek wijzigingen van cryptografische sleutels worden automatisch gesynchroniseerd en geverifieerd. Sleutelgeneratie en -distributie in layer 2-encryptieapparaten is gedecentraliseerd, waardoor sleutel-servers als single points of failure worden vermeden en zo de beschikbaarheid van het netwerk toeneemt. BSI-goedgekeurde oplossingen zijn beschikbaar

Welke beschermingsdoelen worden met deze maatregel bereikt?
- Beschikbaarheid
- Integriteit
- Vertrouwelijkheid
- Authenticiteit

Classificatie van het technologieniveau



3.2.11 Cloud-gebaseerde gegevensuitwisseling

Met de voortschrijdende digitalisering en geografisch verspreide manier van werken hebben zogenaamde cloud-gebaseerde gegevensuitwisseling steeds vaker toepassing gevonden in de IT-omgeving (met file exchange services, zoals Dropbox, OneDrive en, Google Drive).

Tegen welke dreiging(en) wordt deze maatregel ingezet?

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

- Ongeoorloofde toegang tot en bezichtiging door de exploitant van de dienst
- Ongeoorloofde toegang tot en inspectie door derden tijdens verwerking of opslag
- Ongeoorloofde toegang tot en inspectie door derden terwijl de gegevens via internet worden vervoerd
- Diefstal of ongeoorloofd gebruik van de identiteit die is overeengekomen met de cloud-service.

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?

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

1. versleutelde verzending van bestanden van en naar de data exchange service
2. versleuteling en pseudonimisering van gegevens die onafhankelijk zijn van de file exchange service door
    - end-to-end versleuteling aan cliëntzijde van gegevens voor de ontvanger voordat deze naar de cloud-opslag wordt verzonden (bijvoorbeeld door versleuteling geïntegreerd in de exchange service in clientsoftware die tot de cloud-opslag behoort of door afzonderlijke end-to-end encryptie-software op de client)
    - Gateway encryptie / pseudonimisering (zie hoofdstuk "Gegevensopslag in the cloud")

Met name de volgende vragen moeten in overweging worden genomen:

1. wie de service beheert en heeft de exploitant toegang tot de gegevens?
3. hoe worden de gegevens beschermd tijdens de verwerking / bestandsopslag?
4. hoe worden de gegevens beschermd tijdens het vervoer van en naar de exploitant?

Als de service wordt beheerd door een vertrouwde instantie, dan is end-to-end versleuteling van de gegevens zelf in sommige gevallen niet nodig, maar in principe is het ook bij vertrouwde exploitanten nuttig.

Er zijn data exchange services beschikbaar, waar gegevens transparant worden versleuteld voordat ze worden geüpload, dat wil zeggen zonder speciale actie van de gebruiker, en opnieuw gedecodeerd na het downloaden. De operator ziet dan alleen versleutelde gegevens. Als alternatief kan encryptie software aan clientzijde worden toegepast, die ervoor zorgt dat de gegevens end-to-end worden versleuteld voordat ze worden geüpload of na het downloaden. Deze oplossingen vereisen echter meestal extra inspanning van de kant van de

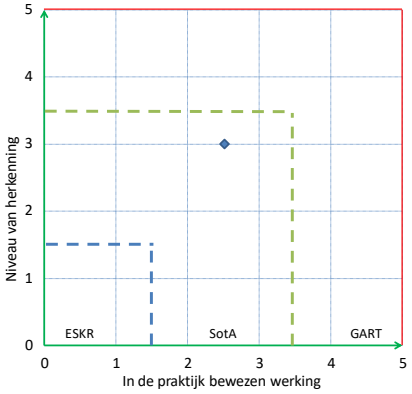
gebruiker. Bij het versleutelen, moet aandacht worden besteed aan het gebruik van veilige procedures voor versleuteling en aan sleutelgeneratie en sleutelopslag.

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

Welke beschermingsdoelen worden met deze maatregel bereikt?

☐ Beschikbaarheid
☐ Integriteit
☐ Vertrouwelijkheid
☐ Authenticiteit

Classificatie van het technologieniveau



3.2.12 Gegevensopslag 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 elementaire maatregel de meest veilige: de versleuteling van gevoelige gegevens. Om de verwerking van gegevens - waar gewenst - mogelijk te kunnen blijven maken, is een selectieve versleuteling van gegevens volgens een gegevensclassificatie vereist.

Zodra gevoelige gegevens een veilige, interne omgeving verlaten om in de cloud opgeslagen te worden, moet deze worden versleuteld nog voordat ze worden verzonden. Versleuteling moet, om ongeoorloofde toegang tot gegevens te voorkomen, uitsluitend binnen het controlegebied van de gebruikersorganisatie blijven, zelfs voor externe beheerders. Eén ding is duidelijk: wie de gegevens versleutelt, moet toegang hebben tot de onversleutelde gegevens. En dat zou alleen de gebruikersorganisatie moeten zijn. Een *state of the art* oplossing moet daarom zorgen voor passende, volledig intern gecontroleerde gegevensversleuteling. Een interne verdeling van administratieve taken bij het beheren van cryptografische sleutels aan meerdere personen, maakt het nog moeilijker om gevoelige gegevens te compromitteren. *State of the art* oplossingen vormen geen beperking voor belangrijke functionaliteit, zoals het zoeken of filteren van gegevens, rapportage of de geautomatiseerde verwerking van versleutelde gegevens in cloud-applicaties. Om een consistent hoog beveiligingsniveau voor alle cloud-applicaties mogelijk te maken, moet de oplossing ook multi-cloud geschikt zijn, d.w.z. ondersteuning bieden voor meerdere cloud-providers.

Bijzondere voorzichtigheid is geboden bij het gebruik van cloudservices die gegevens buiten Europa opslaan of verwerken sinds het wegvallen van het Privacy Shield (Schrems II arrest).

Tegen welke dreiging(en) wordt deze maatregel ingezet?

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

1. Ongeoorloofde toegang tot cloud-opslag (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
5. Diefstal van de cloud-opslag

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?
Een encryption-gateway is een proxy-gebaseerde oplossing die bemiddelt tussen eindgebruikerapplicaties en de cloud. Het versleutelt en pseudonimiseert alle gegevens die een vooraf gedefinieerde beveiligde interne omgeving verlaten en decodeert informatie uit de cloud die wordt gevraagd door geautoriseerde eindgebruikers. Met een dergelijke oplossing moeten de cryptografische sleutels het exclusieve eigendom van de gebruikersorganisatie blijven. Op dezelfde manier moeten, om de soevereiniteit van gegevens te garanderen en de toegangsautorisaties centraal te controleren, encryptie en decryptie ook alleen door de gebruikersorganisatie kunnen worden bestuurd. Daarom moet een dergelijke *state of the art* oplossing een volledig intern sleutelbeheer mogelijk maken, evenals de versleuteling / pseudonimisering van de gegevens die onafhankelijk zijn van de cloud-infrastructuur. Intern moeten de belangrijkste beheerstaken worden verdeeld over verschillende verantwoordelijke personen.

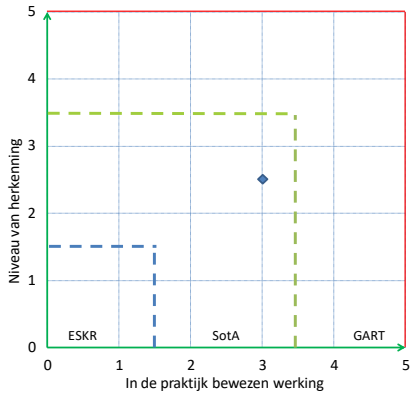
De bedrijfseigen encryptie /pseudonimisering maakt deze oplossing veiliger dan de native encryptie-oplossingen van derde cloud-providers (Bring-Your-Own Key, enz.). In het laatste geval kan nooit volledig worden uitgesloten dat derden (zoals databasebeheerders) toegang hebben tot gevoelige informatie. Met een encryption-gateway kunnen gegevensverwerkers van derden nog steeds administratieve taken uitvoeren, maar kunnen ze gevoelige gegevens niet meer in platte tekst lezen. Deze oplossing biedt ook bescherming in het geval van gegevensdiefstal: zonder de cryptografische sleutels kunnen aanvallers niets doen met vastgelegde, versleutelde gegevens.

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

Met het oog op de toekomst moet een encryption-gateway worden geselecteerd waarmee de gebruikersorganisatie vrij de gebruikte encryptie-algoritmen (Crypto Agility) kan uitwisselen. Met de progressieve ontwikkeling van extreem krachtige kwantumcomputers kunnen procedures die vandaag als veilig worden geclassificeerd, in de nabije toekomst achterhaald raken. Daarom is een oplossing die al compatibel is met algoritmen van postkwantum cryptografie (PQC) ideaal.

Welke beschermingsdoelen worden met deze maatregel bereikt?
- ☐ Beschikbaarheid
- ☐ Integriteit
- ☐ Vertrouwelijkheid
- ☐ Authenticiteit

Classificatie van het technologieniveau



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 gegevensoverdracht beschermt

hiertegen, net als het hardenen van apparaten en configuratie.

Tegen welke dreiging(en) wordt deze maatregel ingezet?
Ondanks chat en webconference applicaties zijn vandaag de klassieke vaste en mobiele telefonie de meest directe en persoonlijke vormen van communicatie. Het brengt echter verschillende risico's met zich mee en biedt potentiële aanvalsvectoren. Bij de overgrote meerderheid van de telefoongesprekken met vaste telefoons is ook een mobiele telefoon betrokken.

- Het op de vaste lijnen, van telefonie en netwerk exploitanten die de basisstations onderling via vaste lijnen verbinden, afluisteren van mobiele telefoongesprekken en dataverkeer, welke onder andere zijn op internettechnologie gebaseerd zijn.
- Het hacken van mobiele gesprekken en dataverkeer en via malware hun overdracht naar Command & Control aanval-servers die op de mobiele telefoon is geïnstalleerd en die kwetsbaarheden in het besturingssysteem en apps misbruikt om direct toegang te krijgen tot microfoon, luidsprekers en touchscreen toetsenbord en scherm, en op deze wijzer de encryptie-app verwijdert.
- Onversleutelde mobiele gesprekken en dataverkeer kunnen met behulp van goedkope hardware op de etherinterface worden onderschept. Om dit te doen, hoeven aanvallers de mobiele telefoon niet te infecteren of in te breken in het communicatienetwerk. Ze moeten echter binnen het ontvangstbereik van de betreffende mobiele telefoon bevinden. Aanvallers kunnen zich bijvoorbeeld voordoen alsof ze deel uitmaken van het mobiele netwerk om de mobiele telefoon op hun luisterapparaat te registreren en vervolgens rechtstreeks gesprekken en dataverkeer opnemen en analyseren.

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?
De vertrouwelijkheid van gesprekken kan door(in de communicatie-app layer) spraak- en gegevensversleuteling op OSI 7 te gebruiken worden gewaarborgd. Gesproken woord- en chatgegevens en eventuele bestandsoverdrachten worden in real-time op het apparaat versleuteld en vervolgens wanneer ze de ontvanger bereiken gedecodeerd en weergegeven.

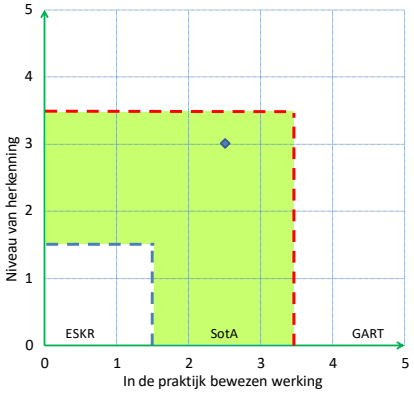
De volgende tegenmaatregelen worden aanbevolen:

- Versleuteling van spraak- en datacommunicatie via geschikte en vertrouwde apps of hardware die voldoen aan de huidige coderingsstandaarden en toepasselijke beveiligingsregels voor end-to-end encryptie
- Bovendien, centrale configuratie van eindapparatuur door de uitgevende organisatie of een die Bring Your Own Devices (BYOD) ondersteunt door middel van Mobile Device Management systemen (MDM / EMM) om ongewenste acties van gebruikers en app-activiteiten die leiden tot mobiele telefoon infectie te voorkomen
- Voor hogere niveaus van betrouwbaarheid, het gebruik van mobiele telefoons met gehardende operation systemen die ervoor zorgen dat microfoon en luidspreker alleen worden gebruikt door de encryptie-app en voorkomen dat bestaande malware van het hacken van de encryptiesleutel.
- voor hogere betrouwbaarheidsniveaus het gebruik van mobiele telefoons met gehardende bedieningssystemen, welke garanderen dat microfoon en luidspreker alleen gebruikt kunnen worden door de encryptie-app en dat voorkomen wordt, dat willekeurig welke malware de encryptiesleutel kan hacken.

Welke beschermingsdoelen worden met deze maatregel bereikt?

- ☐ Beschikbaarheid
- ☐ Integriteit
- ☐ Vertrouwelijkheid
- ☐ Authenticiteit

Classificatie van het technologieniveau



3.2.14 Communicatie via Instant Messenger

Instant Messaging is de term voor een vorm van digitale communicatie waarin twee of meer partijen converseren door middel van snel verzonden tekst, beeld en spraakberichten. De partijen gebruiken hierbij een gemeenschappelijke Instant Messenger voor het via een netwerk versturen van de berichten. Als één partij op het moment dat een bericht wordt verzonden niet online is, wordt het bericht doorgaans op een later tijdstip aan de ontvanger bezorgd. Secure Instant Messaging probeert chatberichten te beschermen tegen ongeautoriseerde toegang en wijziging.

Tegen welke dreiging(en) wordt deze maatregel ingezet?

Wanneer informatie wordt uitgewisseld via Instant Messaging, moeten de volgende bedreigingen in aanmerking worden genomen:

1. Het 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 chatgegevens

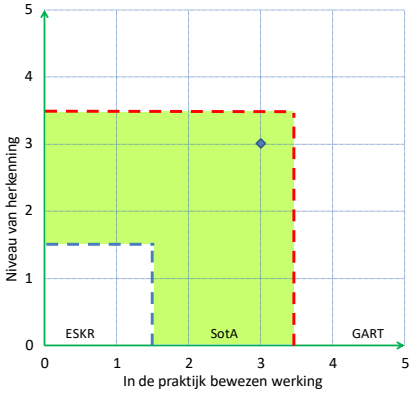
Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?

1. Secure Instant Messaging bevat technische beveiligingsmaatregelen om de vertrouwelijkheid en integriteit van de inhoud van de communicatie te bewaren:
   - Bescherming voor gegevensoverdracht tijdens het transport met behulp van de nieuwste TLS
   - Gebruik van asymmetrische end-to-end versleuteling met beveiliging die ten minste vergelijkbaar is met RSA 2048 bit
   - Forward Secrecy moet deel uitmaken van de architectuur om de gegevens te beschermen tegen latere decryptie, ondanks het bezit van de lange termijn sleutel.
2. Betrouwbare verificatie/verificatie van identiteiten
3. Beveiliging van toegangsopties en toegangswegen naar inhoud:
   - Schermvergrendeling op het gebruikte mobiele apparaat (met sterk wachtwoord)
   - Geactiveerde apparaatversleuteling
   - De gebruikte communicatie-app moet onafhankelijke veilige gegevensopslag en bescherming bieden tegen decodering door onbevoegde partijen.

Welke beschermingsdoelen worden met deze maatregel bereikt?

- ☐ Beschikbaarheid
- ☐ Integriteit
- ☐ Vertrouwelijkheid
- ☐ Authenticiteit

Classificatie van het technologieniveau



3.2.15 Beheer van mobiele apparaten

Het gebruik van Mobile Device Management (MDM) oplossingen reduceert de beveiligingsrisico's die ontstaan als gevolg van 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 dreiging(en) wordt deze maatregel ingezet?

4. Gegevensverlies: Als belangrijke gegevens worden opgeslagen op de mobiele apparaten en het apparaat verloren gaat of wordt vernietigd, moet het bedrijf accepteren dat deze gegevens in sommige situaties onherroepelijk verloren gaan.
5. Diefstal: Als een mobiel apparaat wordt gestolen, kan de dief toegang hebben tot vertrouwelijke bedrijfsgegevens.
6. Malware: Door het gebruik van openbare WiFi-netwerken (WLAN), het niet installeren van beschikbare updates en het niet controleren van de installatie van applicaties uit sommige twijfelachtige bronnen, zijn mobiele apparaten vaak besmet met malware.

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?

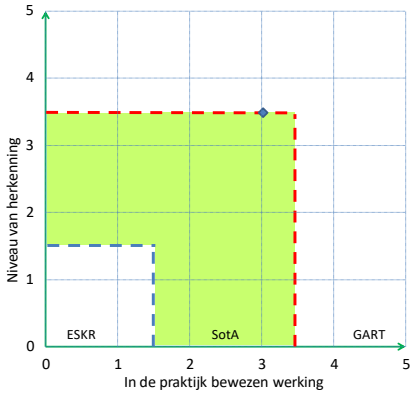
MDM-oplossingen stellen beheerders in staat om de toegang tot en het gebruik van mobiele apparaten die voor zakelijke doeleinden worden gebruikt, op verschillende manieren en volgens vooraf gedefinieerde beveiligingsrichtlijnen te beheren. MDM-oplossingen kunnen de patch-status van het mobiele apparaat bepalen en een melding doen om updates te installeren zodra deze beschikbaar en gecontroleerd zijn. Bovendien kunnen adequate wachtwoordbeveiliging, regelmatige back-up en apparaatversleuteling allemaal centraal worden afgedwongen. In het 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 gebruikersrechten voor het mobiele apparaat zo instellen dat applicaties uit willekeurige en mogelijk onveilige bronnen niet kunnen worden geïnstalleerd.

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

Welke beschermingsdoelen worden met deze maatregel bereikt?

- ☐ Beschikbaarheid
- ☐ Integriteit
- ☐ Vertrouwelijkheid
- ☐ Authenticiteit

Classificatie van het technologieniveau



3.2.16 Routerbeveiliging

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

In de business to business (B2B)-sector worden routers niet alleen gebruikt als internet-toegangsapparaten of voor het routeren van gegevens. In de meeste gevallen bouwen ze ook VPN-netwerken op. Aangezien de telefonie-infrastructuur is gemigreerd (ter vervanging van ISDN/analoge technologie door IP-technologie), zijn routers gebruikt als ISDN-IP-gateways, zodat de bestaande ISDN-systemen, nog steeds in IP-netwerken kunnen gebruiken. Beide applicaties maken de router voor een organisatie een essentieel onderdeel met specifieke beveiligingsvereisten.

Vanwege de wereldwijde prevalentie in zowel bedrijf- en organisatie- als particuliere netwerken is de router een doelwit voor verschillende soorten aanvallen die moeten worden voorkomen door adequate beschermende maatregelen. In deze sectie worden de bedreigingen voor routers en de huidige beschermende maatregelen beschreven en beoordeeld.

Tegen welke dreiging(en) wordt deze maatregel ingezet?
Routers zijn bedoeld om gegevens betrouwbaar en veilig om te leiden en tegelijkertijd te beschermen tegen ongeautoriseerde toegang.
De volgende bedreigingen/risico's kunnen deze doelstellingen in gevaar brengen:

1. Configuratiemanipulatie
2. Aanvallen met gebruikmaking van bekende en nog niet gesloten gaten hiaten in de beveiliging
3. Aanvallen met gebruikmaking van nieuw ontdekte beveiligingsgaten (zero-day exploits)
4. Aanvallen via IP-(telefonie)verbindingen
5. Diefstal (vooral outdoor/ mobiele communicatie routers)
6. Beschikbaarheidaanvallen (DoS-aanvallen)
7. Toegang via ongedocumenteerde interfaces (backdoors)
8. Uitvoeren van code van derden en integratie in botnets
9. Aanvallen via onvoldoende beveiligde WLAN's

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?
Er zijn meerdere beveiligingsmaatregelen om het risico van de bovenstaande bedreigingen tot een minimum te beperken, die hieronder kunnen worden samengevat als een pakket router beveiligingsmaatregelen:

1. Wachtwoordbeveiliging: Gebruik van beveiligde toegangsgegevens die zijn beveiligd tegen toegang door derden en het vermijden van het gebruik van standaardaanmeldingen
2. Regelmatige firmware-updates uitvoeren voor routers
3. Servicecontracten met de fabrikant en een vastgestelde maximale responstijd in het

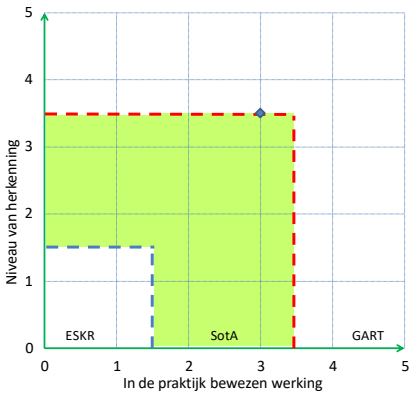
geval dat een ernstig beveiligingsgat bekend wordt.

4. Als een routerfabrikant geen updates verstrekt nadat hij zich bewust is geworden van een beveiligingslek, is het noodzakelijk om te overwegen alternatieve apparaten van andere fabrikanten die niet door het lek worden beïnvloed te gebruiken.
5. De router moet worden ingesteld op een beveiligde locatie, zoals een afsluitbare ruimte met toegang die wordt bewaakt door verantwoordelijke beheerders. Het is zelden mogelijk dat een router buitenshuis op een locatie met beveiligde toegang wordt ingesteld. De router moet daarom zijn uitgerust met een GPS-functie. De router moet zo worden geconfigureerd dat deze bijvoorbeeld na een stroomstoring wordt gecontroleerd, om te controleren of deze zich nog steeds op de site bevindt. Als dit niet het geval is, moet de werking ervan worden verstoord.
6. In de firewall moeten filters voor ongeldige adressen volgens RFC 2267 en blacklists worden ingesteld ter bescherming tegen DoS-aanvallen.
7. Alle poorten en interfaces die open en niet nodig zijn, moeten worden gesloten.
8. Indien mogelijk, moet de router automatisch tijdens inactiviteit (bijvoorbeeld 's nachts) deactiveren, om het blootstellingvenster te verkleinen. Deze maatregel mag de installatie van updates niet beperken.
9. Er moeten verschillende netwerkzones worden ingesteld, om de impact van succesvolle aanvallen op routers (netwerksegmentatie) tot een minimum te beperken.
10. WLAN-routers: Geen open netwerken of alleen voor gasttoegang (directe uitgaande lijn), anders de hoogste versleutelingnormen gebruiken
11. VPN-routers: Bouw geen VPN-verbindingen op met vooraf gedeelde sleutels, maar, waar mogelijk, op basis van 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. Bediening van routers moet centraal worden gecontroleerd.

Welke beschermingsdoelen worden met deze maatregel bereikt?

- ☐ Beschikbaarheid
- ☐ Integriteit
- ☐ Vertrouwelijkheid
- ☐ Authenticiteit

Classificatie van het technologieniveau



3.2.17 Netwerkbewaking met behulp van IDS (inbraak detectiesysteem)

Een inbraak detectiesysteem (IDS) of inbraak preventiesysteem (IPS) identificeert en registreert afwijkingen in het IT-netwerk. Het doel van beide systemen is om indien mogelijk inbraak en de verspreiding van malware te detecteren voordat schade optreedt. In tegenstelling tot IDS, dat alleen informatie rapporteert over afwijkend gedrag en alarmen genereert, kan een IPS ook automatisch ingrijpen. Dit moet voorkomen dat malware verder via het netwerk wordt verspreid. Er zij op gewezen dat directe interventie door een IPS een directe impact kan hebben op de beschikbaarheid van onder andere industriële en productiesystemen, volledig geautomatiseerde bestel- en leveringsprocessen en rapportage-

en beveiligingsprocessen (inclusief brandveiligheid)

Tegen welke dreiging(en) wordt deze maatregel ingezet?

1. Informatielekken als gevolg van het onderscheppen van gevoelige gegevens
2. Misbruik van diensten en communicatieprotocollen
3. Toegang van derden IT-systemen tot het IT-netwerk
4. Benutting van mogelijkheden van toegang tot gekoppelde IT-systemen
5. Manipulatie van informatie of software
6. Verspreiding van malware in het IT-netwerk

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?

Er is een onderscheid tussen netwerkgebaseerde en host-gebaseerde IDS/IPS. Network-based IDS/IPS maakt gebruik van interne componenten en/of de netwerkinfrastructuur om de communicatie te monitoren. Host-based IDS en IPS gebruiken informatie van IT-systemen (via software agents, logfile analyses, enz.). In gedistribueerde systeemarchitectuur moeten de gegevens worden versleuteld en voor uitwisseling of opslag worden ondertekend.

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

De tweede methode is gebaseerd op het detecteren van veranderingen in de communicatiepatronen van netwerkcomponenten veroorzaakt door een aanval. Alle communicatie buiten het verwachte dataverkeerprofiel wordt geëvalueerd 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 normaal dataverkeer moeten echter worden gedefinieerd.

Als malware wordt gedetecteerd of als er verschillen zijn met de geldige nominale staat van communicatie, moet een IDS automatisch relevante incidentrapporten genereren. Alle incidentmeldingen moeten lang genoeg voor analysedoeleinden in het systeem worden bewaard en indien nodig in een open of gestandaardiseerd formaat kunnen worden geëxporteerd.

Incidentrapporten moeten alle relevante informatie bevatten voor incidentanalyse en voor het nemen van tegenmaatregelen, zoals herkende handtekening of afwijkende communicatieverbinding. Alarmberichten moeten zichtbaar zijn op de beheerconsole, als e-mailbericht worden verzonden naar bepaalde accounts en via een exportinterface beschikbaar zijn op een algemeen alarmsysteem (zie SIEM).

Een IPS moet ook onafhankelijk alle communicatie in het netwerk waarop een poging tot aanval is gebaseerd, onafhankelijk blokkeren. Voor zover mogelijk moet geen communicatie voorkomen wordt, dat duidelijk aan niet-aanvalsgedrag kan worden toegeschreven.

Een IDS/IPS moet componenten leveren om alle communicatie naar gateways en/of binnen IT-systemen (hosts) te analyseren en die na een tijdelijke storing automatisch opnieuw synchroniseren voor een stabiele bewerking.

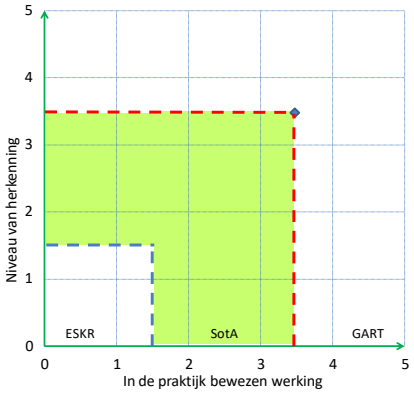
Ongewenste communicatie van IDS/IPS-componenten naar derden kan niet worden toegestaan. Bovendien moeten alle IDS- en IPS-componenten niet-identificeerbaar zijn, mogen ze geen invloed hebben op het dataverkeer of diensten aanbieden en zelf moeten ze worden beschermd.

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

Welke beschermingsdoelen worden met deze maatregel bereikt?

- ☐ Beschikbaarheid
- ☐ Integriteit
- ☐ Vertrouwelijkheid
- ☐ Authenticiteit

Classificatie van het technologieniveau



3.2.18 Bescherming van het 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 tijdens het surfen dataverkeer via een webfilter wordt geleid, kunnen deze aanvallen worden gedetecteerd en geblokkeerd.

Tegen welke dreiging(en) wordt deze maatregel ingezet?

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

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

Aanvallers maken ook gebruik van speciaal hiervoor ingerichte webservers die vaak een andere website imiteren. In het geval van phishing, worden deze valse kopieën van bekende websites ingezet met als doel van het aftappen van gevoelige informatie van de gebruiker, meestal gebruikersnamen en wachtwoorden, als ook bankgegevens, credit card informatie, adressen, enz.

Het werkelijke bestemming adres (de URL met kwaadaardige code of de URL van een geïnfecteerde of valse webpagina) is vaak vermomd door middel van automatische omleiding(redirecting), en vaak ook URL-shorteners (bit.ly, TinyURL, enz.), hoewel deze niet direct betrokken zijn bij de werkelijke aanval. Gebruikers worden, via links in e-mailberichten, op sociale media, enz., doorgeleid naar speciale websites

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?

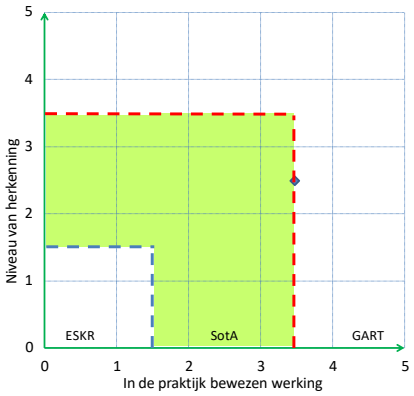
Webgegevensverkeer wordt via webfilters geleid om tegen dit soort aanvallen te beschermen. Webfilters beschermen tegen deze aanvallen door de betreffende websites te blokkeren en de gegevens die door websites worden geladen voor schadelijke code te analyseren. Webfilters kunnen centraal worden gebruikt als webfilters in de cloud of als on-premise apparaten, of als software die wordt bediend op het systeem van de eindgebruiker.

Welke beschermingsdoelen worden met deze maatregel bereikt?

- ☐ Beschikbaarheid
- ☐ Integriteit

- Vertrouwelijkheid
- Authenticiteit

Classificatie van het technologieniveau



3.2.19 Bescherming van webapplicaties

Een Web Application Firewall (WAF) beschermt webapplicaties (homepages, online winkels, thuisbankier portals, enz.) tegen aanvallen. De WAF inspecteert de communicatie tussen gebruikers en webapplicaties op toepassingsniveau en blokkeert mogelijk schadelijk dataverkeer, zoals SQL-injectie of 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-layers 3 en 4, behandelen WAFs OSI 7 (gegevensverkeer) en beschermen ze zo tegen bedreigingen die zich richten op de exploitatie van beveiligingskwetsbaarheden in de applicaties.

Tegen welke dreiging(en) wordt deze maatregel ingezet?

Aanvallen op webapplicaties of webservice-interfaces, zoals

- SQL-injectie
- Cross-Site Scripting (XSS)
- Informatielekken
- Command-injection
- Andere OWASP-bedreigingen

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?

Met behulp van een Web Application Firewall (WAF) of Web Service Firewall (WSF) die actief is voor de webserver (upstream).

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 mogelijk schadelijk dataverkeer. Veelal is een aanpassing van de WAF is voldoende om korte termijn gaten in de beveiliging van de webapplicatie te dichten. Vervolgens kan achteraf het aanpassen of patchen van de te beschermen webapplicatie worden gepland en met voldoende aandacht voor de uit te voeren tests. Bij aanvallen wordt vaak een combinatie van verschillende kwetsbaarheden gebruik gemaakt, zo kunnen met het blokkeren van een centrale kwetsbaarheid in de WAF veel aanvallen snel worden afgewend.

De Web Services Firewall (WSF) is een speciale vorm van de WAF voor gericht op machine-to-machine communicatie en werkt vergelijkbaar via http/https. De aanvalsvectoren voor WAF en WSF lijken erg op elkaar. Het volgende geldt voor zowel de WSF als de WAF.

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 biedt.

De WAF beëindigt versleuteld gegevensverkeer aan de gebruikerszijde, analyseert de inhoud en stuurt deze door naar de webserver als de versleutelde berichten als onschadelijk zijn geclassificeerd. Schadelijke berichten worden geblokkeerd.

De werking van webapplicaties zonder gebruik te maken van een fysieke of virtuele upstream WAF kan niet langer worden beschouwd als *state of the art*.

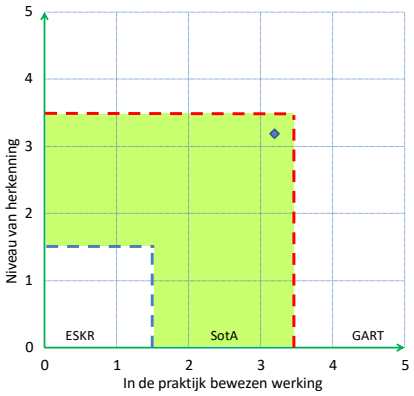
Een WAF moet de volgende prestatiekenmerken hebben:

- Overdracht van log gegevens naar SIEM- en anomaliedetectie systemen met de mogelijkheid om wachtwoorden, creditcardgegevens, enz. te verbergen
- Clustering mogelijkheden voor hoge beschikbaarheid en belastingsverdeling(load-balancing)
- Bescherming tegen OWASP top 10 aanvallers, zoals SQL injectie, cross-site scripting (XSS) en Directory Traversal door middel van blacklisting, whitelisting en patroonherkenning
- Sterke authenticatie van webapplicaties en gebruikers van diensten
- Sessiebeheer, d.w.z. inspectie- en manipulatiebescherming van sessiecookies
- Broken Access Control dat ongeautoriseerde toegang tot paden (Path Traversal), bestanden en API-functies voorkomt
- Filters tegen onnodige http-headers
- Bescherming tegen Cross-Site Request Forgery (CSRF) door evaluatie van headers van http-verzoeken, zoals verwijsinformatie (referrer-information)

Welke beschermingsdoelen worden met deze maatregel bereikt?

☐ Beschikbaarheid
☐ Integriteit
☐ Vertrouwelijkheid
☐ Authenticiteit

Classificatie van het technologieniveau



3.2.20 Externe toegang tot netwerken / onderhoud op afstand

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

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 met de tools van de fabrikant(zoals PLC-programmeersoftware) toegang krijgen tot deze systemen.

Tegen welke dreiging(en) wordt deze maatregel ingezet?

- Ongeoorloofde toegang tot het bedrijfsnetwerk
- Ongeoorloofde toegang tot doelsystemen

- Externe toegang op afstand dat niet kan worden getraceerd
- Het aftappen of blootstelling tijdens een externe onderhoudssessie

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?

De doelsystemen zijn meestal via routers verbonden met het internet om onderhoud op afstand mogelijk te maken. Vervolgens gebruiken wordt een VPN-verbinding tot stand gebracht met wat een intermediate server (tussenliggende server) wordt genoemd. Dit tussenpunt (koppelpunt) is de koppeling tussen het doelsysteem en de externe gebruiker, die eveneens een VPN-verbinding met de intermediate server heeft opgezet. Aangezien beide deelnemers hun eigen verbinding hebben, kan elke deelnemer de verbinding op elk gewenst 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 op layer 3 (IP, poort, protocol). Dit garandeert de verbinding van de specifieke applicatie met het doelsysteem. Afhankelijk van de applicatie kunnen met onderhoud op afstand ook zuivere terminalverbindingen worden tot stand gebracht, met inbegrip van web-, RDP-, VNC- en SSH-verbindingen. Dit is afhankelijk van de beschikbaarheid van het doelsysteem. Met name moet een directe 1:1-netwerkkoppeling van een externe gebruiker aan het netwerk van het doelsysteem worden voorkomen.

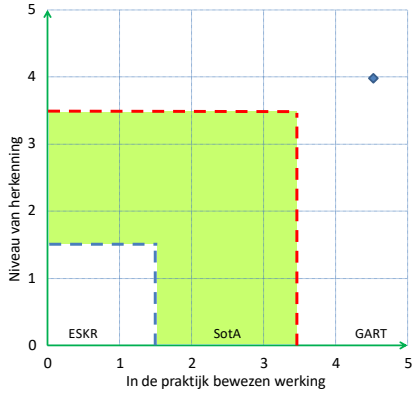
Versleutelde VPN-verbindingen garanderen gegevensintegriteit en bescherming tegen het aftappen van gegevens. Voor autorisatie van de externe gebruiker moet 2-factor authenticatie beschikbaar zijn.

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

Welke beschermingsdoelen worden met deze maatregel bereikt?

☐ Beschikbaarheid
☐ Integriteit
☐ Vertrouwelijkheid
☐ Authenticiteit

Classificatie van het technologieniveau



3.2.21 Serverhardening

Aangezien op serversystemen de essentiële (vaak gevoelige) gegevens en persoonsgegevens van de organisatie worden verwerkt en opgeslagen, 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 of meerdere Linux

Serversystemen hebben standaard geen zeer restrictieve 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 middel van server hardening worden deze functies en hun interfaces uitgeschakeld of meer restrictief geconfigureerd, wat het beveiligingsniveau van de serversystemen aanzienlijk verhoogt. Daarom moet server hardening een integraal onderdeel zijn van de technische beveiligingsstrategie van organisaties.

Tegen welke dreiging(en) wordt deze maatregel ingezet?
De belangrijkste bedreigingen van niet-gehardende serversystemen zijn:

- Gegevensmanipulatie, zoals van persoonsgegevens en gevoelige bedrijfsgegevens
- Gegevensverlies (bijv. hele databasesystemen)
- Manipulatie van applicaties of aangesloten systemen
- Manipulatie, sabotage of spionage van operatie- en productieprocessen
- Identiteitsdiefstal (bijv. aanvallen op domeincontrollers)
- Invoegen van malware van welke aard, om deze malware naar andere systemen te distribueren
- Misbruik van servercapaciteit voor tot nut van de aanvallers (zoals Crypto-Mining)
- Misbruik van servers voor zijdelingse beweging (Host-jumping) om andere systemen aan te vallen

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?
Om serversystemen te hardenen, moeten met name de volgende maatregelen worden genomen:

1. Deactivering van componenten
    - Controleer periodiek of actieve services noodzakelijk zijn voor de werking
    - Deactiveer of de-installeer onnodige onderdelen/services van het besturingssysteem, met inbegrip van achtergrondservices
    - Deactiveer onnodige opstart- of tijdgestuurde processen
    - Deactiveer onnodige, technisch verouderde of onveilige interfaces of protocollen
    - Deactiveren de overdracht van telemetriegegevens, tenzij deze volgens centraal beleid nodig zijn voor centrale monitoring
    - Deactiveer onnodige bestand-shares
    - Deactiveer of beperk toegang tot administratieve websites
2. Activering van hardwaregerelateerde beveiligingsfuncties
    - Activeer CPU-beveiligingsfuncties en test de juiste werking van applicaties, zoals Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP)
    - Activeer het BIOS-wachtwoord en de beperk de opstart(volgorde) tot noodzakelijke apparaten
    - Activeer, indien van toepassing, bescherming tegen Side-Channel aanvallen
    - Activeer, indien van toepassing, veilige opstartprocedures
3. Beveiligingsconfiguraties
    - Gebruik beveiligde communicatieprotocollen om ervoor te zorgen dat gevoelige gegevens en authenticatie-informatie versleuteld worden verzonden
    - Gebruik certificaten voor het uitwisselen van cryptografische sleutels
    - Deactiveer auto-start mechanismen voor zoals voor USB-media)
    - Activeer schermbeveiliging met wachtwoordbeveiliging
    - Activeer sterk gebruikersaccount beheer (User Account Control)
    - Activeer, al tijdens het opstartproces, antivirus beveiliging op het systeem
    - Verwijder onnodige certificaten uit Trust Stores
    - Voorkom informatielekken met betrekking tot geïnstalleerde services en versienummers

- Schakelen fout- en foutopsporingsberichten voor eindgebruikers uit, of vervangen deze door neutrale foutberichten
- Voer services uit met minimale rechten en een servicegebruiker voer processen, indien mogelijk, uit in een geïsoleerde omgeving
- Actief loggen

4. Toekenning van minimale toegangsrechten (autorisatie op basis van need-to-know en least privilege principes):
   - Verifieer regelmatig verleende toegangsrechten
   - Ken minimale rechten toe voor administratieve activiteiten;
   - Ken minimale rechten toe voor bestandssysteem en externe gegevensinterfaces;
   - Ken minimale rechten toe voor onderhoudsinterfaces/-toegangen;
   - Beperk de toegang tot de configuratie van het besturingssysteem tot fysieke servers (specifiek het voorkomen van ongeautoriseerd aansluiten van externe gegevensdragers)
5. Accounts en wachtwoorden:
   - Gebruik sterke wachtwoorden en mechanismes (zoals wachtwoordlengte, complexiteit, accountvergrendeling, wijzigingsinterval), gebruik wachtwoorden niet opnieuw voor andere applicaties of gebruik 2-factor authenticatie (zie hoofdstuk 3.2.1 e.v.)
   - Bescherm alle accounts met ten minste een wachtwoord, conform het wachtwoordbeleid
   - Vervang alle bestaande standaard (default) wachtwoorden door eigen wachtwoorden, conform het wachtwoordbeleid
   - Blokkeer het lokale beheeraccount (Local Administrator Account) na meerdere keren verkeerd invoeren van het wachtwoord
   - Gebruik eigen persoonsgebonden beheeraccounts (Administrator Accounts)
   - Deactiveer of hernoem standaard gebruikersaccounts
   - Schakel lokale gastaccounts (Local Guest Accounts) uit
   - Gebruik non-privileged serviceaccounts om processen uit te voeren
   - Blokkeer het remote (over netwerken) aanmelden van lokale gebruikersaccounts
   - Schakelen standaard (default), test- en anonieme accounts uit voor alle geïnstalleerde services wen softwarecomponenten
6. Netwerkcomponenten
   - Stel netwerkbeperkingen in (zoals TCP/IP-configuratie), schakel niet-gebruikte netwerkprotocollen uit of verwijder ze
   - Beperk verbindingen tot services tot een minimum
   - Activeer, indien van toepassing, pakketfilters/firewalls om communicatie te beperken tot minimaal benodigde toegang

Voor algemene besturingssystemen van servers zijn meer gedetailleerde hardening richtlijnen openbaar beschikbaar:

- Security Technical Implementation Guides (STIGs): https://iase.disa.mil/stigs
- CIS Benchmarks (Center for Internet Security, Inc.): https://www.cisecurity.org/cisbenchmarks
- Microsoft Security Guidance: https://blogs.technet.microsoft.com/secguide/

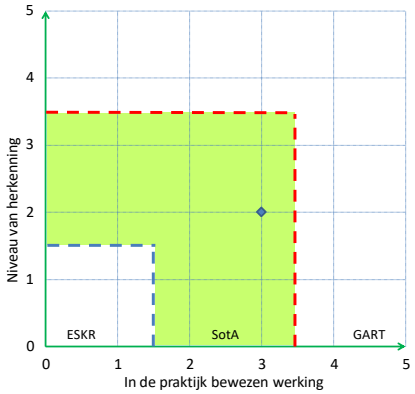
De meeste hardening maatregelen kunnen worden gerealiseerd met technische aanpassingen. Deze instellingen kunnen geautomatiseerd met een hardening pakket (zoals hardening-scripts) worden gedistribueerd naar alle serversystemen van de organisatie.

Nieuwe serversystemen moeten onmiddellijk na de installatie worden gehard met het desbetreffende pakket. Bij het hardenen van bestaande systemen kan hardening leiden tot functionele storingen, dus moet een back-up worden gemaakt en de gehardende serversystemen moeten uitgebreid worden getest.

Welke beschermingsdoelen worden met deze maatregel bereikt?

- Beschikbaarheid
- Integriteit
- Vertrouwelijkheid
- Authenticiteit

Classificatie van het technologieniveau



3.2.22 Eindpuntdetectie en respons platform

De bescherming van eindapparaten (zoals PC's, laptops, smartphones of tablets) vereist nu veel meer dan alleen een antivirus programma. 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 geen specifieke voorkennis, zoals handtekeningen of een eerste slachtoffer, vereist.

Tegen welke dreiging(en) wordt deze maatregel ingezet?

- Malware
- Uitbuiting (Exploit)
- Kwaadaardige scripts
- Hacker activiteit
- Misbruik van beheertools en tools met kwade bedoelingen

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?

EDR-platforms combineren effectieve detectie- en preventietechnieken om het compromitteren van client- en servers, over computers en besturingssystemen, te voorkomen en zelfs actieve aanvallers in computernetwerken bloot te ontmaskeren.

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

Dankzij de *state of the art* sensorarchitectuur gebruiken EPP-oplossingen van de volgende generatie slechts een computer tot een fractie van de capaciteit van een klassieke AV-scanner en het regelmatig downloaden van handtekeningen is niet langer nodig. Dit betekent dat:

- Signature-loze detectie en actieve blokkering van kwaadaardige code door machine learning-modellen (bij voorkeur lokale runtime),
- Controle en registratie van programma activiteit over procesketens heen 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 (waaronder gebruikte tools, zoals malware, trojans, PowerShell scripting en het doel van de aanvaller, exfiltratie van gegevens, het opzetten van een backdoor, zijdelingse beweging binnen de organisatie, escalatie van rechten, enz.)

- Aanvullende bedreigingintelligentie laat zien wie de vermoedelijke acteur/vijand (cybercriminaliteit of nationaal gemotiveerde aanval) is en welke doelen en industrieën de aanvallers nastreven.
- Een volledig geïntegreerde sandbox-verbinding maakt veilige detonatie van gevonden kwaadaardige code en verdere analyse mogelijk zonder de productie in gevaar te brengen.

EDR-platformen 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 dreiginginformatie. Bovendien kunnen systeem-telemetriegegevens door externe deskundigen op schadelijk bewijs worden gecontroleerd.

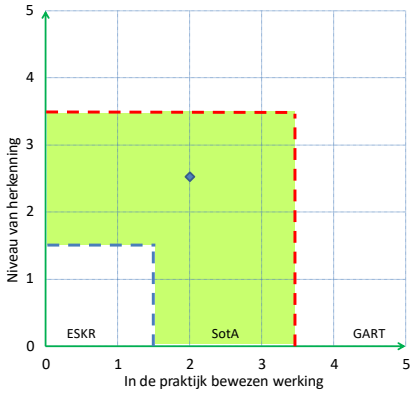
Bovendien moet worden vermeld, dat voor een holistische bescherming van eindapparatuur, voor zover deze aspecten niet geboden worden door de desbetreffende EDR-oplossing, met name rekening gehouden moet worden met de volgende punten:

- Autorisaties/rollen (trefwoord: administratieve autorisaties)
- Update mechanismen (besturingssysteem en software)
- Beperkingen/controle van de geïnstalleerde software
- Versleuteling van eindapparaten
- Bescherming tegen hierboven beschreven bedreigingen/malware
- Verordeningen/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 administratieve rechten heeft
- Gebruik van authenticatieprocedures (gebruikersnaam/wachtwoord, pincode, biometrie, enz.)

Welke beschermingsdoelen worden met deze maatregel bereikt?

☐ Beschikbaarheid
☐ Integriteit
☐ Vertrouwelijkheid
☐ Authenticiteit

Classificatie van het technologieniveau



3.2.23 Internetgebruik met web-isolatie

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

Tegen welke dreiging(en) wordt deze maatregel ingezet?

Infectie van het 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 bedrijfskritische netwerk.

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?
Er zijn verschillende manieren om browsersessies te isoleren. De gebruikte architectuur en de beveiligingsmechanismen zijn hierbij doorslaggevend. Voorbeelden hiervoor zijn de zogenaamde remote controlled browseromgevingen of meerlaagse lokale browserisolaties.

Een eenvoudige isolatie van de browseromgeving (zoals via eenvoudige virtualisatie op basis van Hyper-V of zogenaamde browser sandboxing) biedt onvoldoende hoog niveau van bescherming tegen bovengenoemde bedreigingen, omdat het bijvoorbeeld niet een veilig gehard besturingssysteem heeft waarin de browser standaard wordt uitgevoerd; geen gebruik maakt van extra veilige netwerksegmentatie; geen secure copy & paste mogelijk maakt of geen extra beveiligingsfuncties zoals datasloten gebruikt. Dit is de reden waarom deze methode niet geschikt is voor het tegengaan van de bedreigingen.

Op afstand bestuurde browseromgevingen op basis van ReCoBS
Het op afstand bestuurde browser systeem (Remote-Controlled Browser System of ReCoBS) scheidt het internetgebruik fysiek van de werkcomputer van de gebruiker. Elke browsersessie wordt buiten het gevoelige netwerkgebied in een speciaal geïsoleerde omgeving, binnen een speciaal gehardend systeem, op een aparte hardware en in een separaat netwerksegment (DMZ) uitgevoerd.

Via een technisch beveiligd communicatiekanaal wordt de browser op afstand vanaf het werkstation via videostream op het externe systeem bediend. Het merendeel van de aanvallen gericht op Windows-gebaseerde kwetsbaarheden worden al met succes afgeweerd in de gehardende Linux-omgeving. In de overall architectuur bieden andere beveiligingsmechanismen en zones betrouwbare bescherming tegen aanvallen, zelfs als de browser is gecompromitteerd. De fysieke scheiding van werkstation en browsersysteem biedt ook bescherming tegen hardwaregerelateerde aanvallen (Spectre, Meltdown, ZombieLoad en kwetsbaarheden in de hypervisor).

Op gezette tijden (standaard eenmaal per dag) moet het externe systeem via een image van het systeem teruggezet naar de oorspronkelijke staat, zodat schadelijke code effectief wordt verwijderd; Het is belangrijk dat de image van het systeem integer wordt bewaard.

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

Aangezien de ReCoBS-architectuur het mogelijk maakt om algemene standaard browserfuncties uit te voeren op het externe systeem, zijn aanvullende ontwikkelingen noodzakelijk voor de acceptatie van gebruikers, zodat de op afstand bestuurbare browser niet significant verschilt van het lokale browsergebruik en alle gangbare functies zoals persoonlijke bladwijzers, copy & paste, afdrukken of het up- en downloaden in principe beschikbaar gesteld worden.

Voor de optionele overdracht van bestanden (browser up- en download) tussen het externe systeem en werkstation moeten aanvullende controlemechanismen worden verstrekt die opvallende bestanden in quarantaine plaatsen en beheerders waarschuwen. Een voorbeeld van een dergelijk controlemechanisme is virusbescherming in de DTA-gateway.

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

Webisolatie op basis van lokale virtualisatie van de browserapplicaties
Een andere benadering van webisolatie is gebaseerd op het lokaal inkapselen van de browserapplicatie door middel van veilige virtualisatie in combinatie met een in rechten

beperkt Windows-gebruikersaccount, een gehard gastbesturingssysteem en het via afzonderlijke VPN-tunnels scheiden van internet / intranet naar de Internet gateway. Dit voorkomt directe toegang van de browsersessie tot de hardware van de PC.

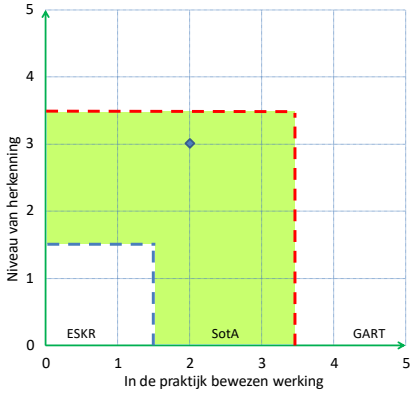
Een van de voordelen van lokale browserisolatie is de mogelijkheid van stand-alone gebruik op mobiele werkstations.

Met de niet- aanwezige fysieke scheiding tussen het gevoelige werkstation en het browsersysteem zouden echter lokale beveiligingshiaten in de processorhardware of -software kunnen worden gebruikt om via een exploitpakket dat alle beschermende lagen bestrijkt (all-Layer exploit package), in te breken.

Welke beschermingsdoelen worden met deze maatregel bereikt?

☐ Beschikbaarheid
☐ Integriteit
☐ Vertrouwelijkheid
☐ Authenticiteit

Classificatie van het technologieniveau



3.2.24 Detectie en evaluatie van aanvallen (SIEM)

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

Tegen welke dreiging(en) wordt deze maatregel ingezet?

SIEM kan helpen tegen de volgende bedreigingen:

- Aanvalactiviteiten door externe partijen (hacker aanvallen
- Insider-bedreigingen (zoals ongeoorloofde toegang tot gegevens van andere afdelingen en computersabotage)
- Schendingen van de naleving

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie 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:

- Log bestanden van besturingssystemen
- Firewall gebeurtenissen van netwerkfirewalls
- Alarmen van Intrusion Detection & Prevention Systems (IDS/IPS)
- Intelligente netwerksensoren/netwerk-monitoringsystemen met informatie over gevonden assets / apparaten, kwetsbaarheden, schending van de naleving en abnormaal netwerkgedrag
- Directory services Authentication services (zoals Single Sign on systems)

- Endpoint Detection & Response Systems (EDR/XDR)
- Indicatoren voor het identificeren van aanvallers en aanvallen zoals IP-adressen, hashes, hostnamen, enz.

In de organisatie heeft het security team de mogelijkheid om real-time een holistisch beeld te krijgen van de processen van 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 organisatie in staat om snel en accuraat te reageren op acute bedreigingen. Op basis van de beschikbare gegevens kunnen in de nasleep van een aanval patronen worden geanalyseerd (forensisch onderzoek) en bestaande maatregelen kunnen worden verbeterd.

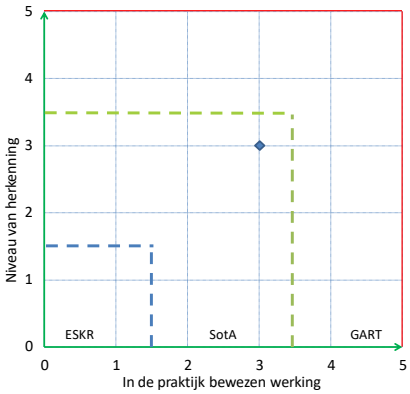
Moderne SIEM-tools bevatten betrouwbare en onmiddellijk toepasbare detectieregels die kunnen worden aangepast aan nieuwe dreigingscenario's. De werking van een SIEM-oplossing vereist de integratie van geschikte bronnen, maar ook het verstrekken van aanzienlijke systeembronnen (zoals grafiekdatabases, gegevensmeren en servers voor exploitatie en beheer). Tegelijkertijd wordt een aanzienlijke voor continue gegevensuitwisseling bandbreedtebenutting gebruikt. De bijbehorende administratieve complexiteit en de acquisitie- en exploitatiekosten zijn vrij hoog, daarom worden bij grote en zeer grote organisaties meestal de klassieke SIEM-oplossingen gebruikt.

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

Welke beschermingsdoelen worden met deze maatregel bereikt?

☐ Beschikbaarheid
☐ Integriteit
☐ Vertrouwelijkheid
☐ Authenticiteit

Classificatie van het technologieniveau



3.2.25 Vertrouwelijke gegevensverwerking

Traditioneel worden de uitgebreide toegangsrechten tot gegevens van beheerders tijdens de verwerking alleen beveiligd met organisatorische of reactieve maatregelen tegen misbruik van deze bevoegdheden. Met behulp van vertrouwelijke gegevensverwerking (Confidential Computing) worden deze gegevens fraudebestendig en preventief beschermd tegen ongeautoriseerde toegang. Dit is vooral belangrijk voor cloud-computing applicaties. Gegevensverwerking komt overeen met de beschermingseis *Vertrouwelijk* wanneer cloudservices worden gebruikt voor kritieke infrastructuren of voor gevoelige gegevensverwerkingsprocessen, bijvoorbeeld in de geneeskunde, de industrie of in

gereguleerde gebieden (bijvoorbeeld regTech).

Tegen welke dreiging(en) wordt deze maatregel ingezet?
Cloudbeheerders zijn verantwoordelijk voor de probleemloze werking van hun systemen. Om deze taak te kunnen vervullen, krijgen ze tal van privileges. 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 cloud en tijdens de verwerking in de cloud niet alleen door aanvallen van derden, maar ook door illegaal handelende werknemers van cloud-serviceproviders.

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?
Eerdere benaderingen van gegevenstoegang beveiliging hebben betrekking op gegevens in rust (opslag) en gegevens in transit (netwerk). Vertrouwelijke gegevensverwerking richt zich op de bescherming van gegevens tijdens de verwerking. Dit is een gebied of capsule afgeschermd van de buitenwereld waarin de volledige gegevensverwerking in een ongecodeerde toestand plaatsvindt. Deze afscherming kan direct worden geïmplementeerd op de processorchip van de server en/of via meerdere servers. Om de gegevens te kunnen verwerken, moet de benodigde sleutel beschikbaar zijn in de capsule. Als een aanvaller zou proberen om toegang te krijgen tot het ingekapselde gebied, zouden de gegevens die daar worden verwerkt zonder versleuteling onvermijdelijk uit voorzorg worden verwijderd. Om meer veiligheid te bereiken, kunnen de capsules na voorafgaand onderzoek door onafhankelijke auditors worden verzegeld met behulp van bekende cryptografische geheimen.

Bij gegevensverwerkingsystemen die zijn uitgerust met de maatregelen die zijn samengevat onder het kopje "vertrouwelijke gegevensverwerking", kan één beheerder geen toegang krijgen tot de gegevens die in de server worden verwerkt. Alleen een kwaadaardige coalitie van verschillende onafhankelijke partijen (zoals systeembeheerder samen met een onafhankelijke auditor) kan de technische maatregelen breken. Dit vermindert de kans op kwaadaardige toegang door verschillende ordes van grootte.

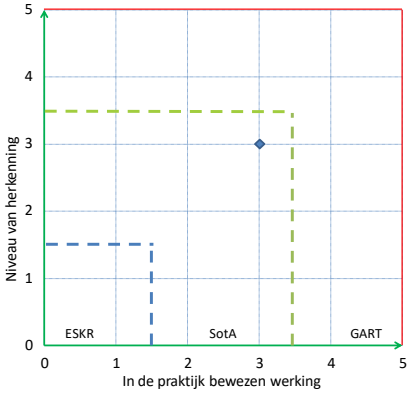
Vertrouwelijke gegevensverwerking

- maakt het mogelijk gegevens in centrale infrastructuren te verwerken zonder ze bloot te stellen aan de mogelijkheid van kennisname (kunnen lezen) door de exploitanten van deze centrale infrastructuren;
- biedt gebruikers meer controle en, afhankelijk van de audit, ook transparantie
- biedt nieuwe vrijheidsgraden, aangezien nieuwe applicaties denkbaar zijn die niet, op grond van conventionele overwegingen op het gebied van gegevensbescherming en beveiliging, op een juridisch conforme manier kunnen worden geïmplementeerd.

Welke beschermingsdoelen worden met deze maatregel bereikt?

☐ Beschikbaarheid
☐ Integriteit
☐ Vertrouwelijkheid
☐ Authenticiteit

Classificatie van het technologieniveau



3.2.26 Sandbox-analyse ter detectie van schadelijke code

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

Tegen welke dreiging(en) wordt deze maatregel ingezet?

- Algemene hacker activiteiten
- Malware (virussen, Trojaanse paarden enz.)
- Phishing

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?

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

Perimeter Sandbox

Bij perimetersandboxing worden bestandsbijlagen, zoals documenten uit de actieve (werk)omgeving, maar ook ingesloten inhoud zoals scripts) van e-mailberichten meestal automatisch uitgevoerd. Sandbox-analyse op de e-mailgateway genereert meestal een latentie voor de gebruiker van enkele seconden tot minuten bij de toegang tot de onderzochte bestandsbijlage.

Sandboxes kunnen ook worden gebruikt op de webgateway (firewall of proxy van de volgende generatie) om bijvoorbeeld gedownloade programma's te controleren. Ook hier wordt een vertraging veroorzaakt voordat het bestand aan de gebruiker wordt geleverd. Daarnaast beïnvloedt het gebruik hiervan ook het gedrag van de browser en webgebaseerde software. Daarom wordt het bestand, naast de klassieke werking van sandbox (eerst controleren of de levering vertraagd is) ook - met parallelle control - aan het eindapparaat afgeleverd. Als kwaadaardige tijdens de laatste procedure code wordt geïdentificeerd, worden aanvullend maatregelen getroffen. Deze omvatten netwerkisolatie, het blokkeren van *command and control* adressen die zijn geïdentificeerd tijdens het sandboxen.

Sandbox voor forensisch onderzoek van tijdens het onderzoek ontdekte of geïdentificeerde bestanden

Door sandboxes te verbinden met volgende -generatie antivirusproducten (machine-learning gebaseerde antivirus) en EDR-oplossingen (endpointdetectie en -respons), kunnen bestanden met een schadelijke prognose of van gedetecteerde en actief onderdrukte aanvalsketens veilig buiten de actieve omgeving worden uitgevoerd. De uitvoering maakt het vervolgens mogelijk om verder relevante indicatoren (bestanden/hashes, URL's, IP-adressen, registeractiviteiten, enz.) te extraheren, wat een onderzochte zaak meer context biedt en zelfs het toeschrijven aan een verdachte aanvaller mogelijk maakt.

Omdat sandbox-oplossingen al aardig wijdverspreid zijn, proberen aanvallers altijd sanbox-detectie te voorkomen. Bij het uitvoeren van hun kwaadaardige code, proberen ze

bijvoorbeeld te bepalen of het een gevirtualiseerde runtime omgeving betreft, zoals gebruikelijk is met sandboxes, of een actieve omgeving met specifieke programma's/processen en andere specifieke functies. De kwaadaardige code zal zich dan meestal onschadelijk gedragen om de detectie ervan te voorkomen. Ook dit gedrag kan echter in de sandbox worden gedetecteerd en worden gebruikt om verdachte inhoud (kat-en-muisprincipe) te identificeren.

De exploitatie van zogenaamde 0-Day (Zero-Day) exploits/bedreigingen, d.w.z. zwakke punten die nog onbekend zijn bij het publiek, kunnen ook leiden tot sandbox-ontduiking (bypasses). Het kan ook gebeuren, dat de geëmuleerde runtime omgeving niet overeenkomt met het slachtoffersysteem en dus kan het gedrag bij het uitvoeren in de sandbox afwijken van dat op het doelsysteem van de aanval. Het is daarom noodzakelijk om deze tactieken, die bekend staan als sandbox evasion, te beheersen, bijvoorbeeld door statische en dynamische analyse te combineren.

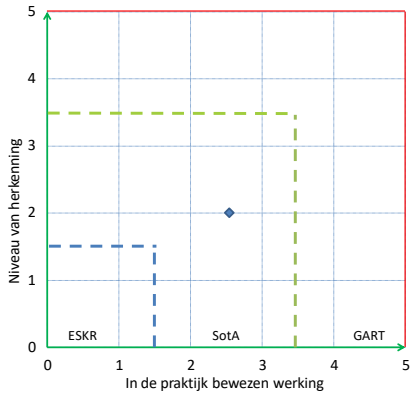
Sandboxes bieden ook een groot voordeel: het, als gevolg van hun hoge mate van automatisering, enorm verminderen van de noodzaak van handmatige door een expert analyse van kwaadaardige code (zogenaamde malware reverse engineering).

Een groot aantal commerciële en open source sandbox oplossingen is beschikbaar.
Deze worden aangeboden als meetal kostenintensieve hardwareoplossingen, maar ook als publieke of private geleverde cloud-oplossingen. Sandbox-technologie wordt ook al geruime tijd gebruikt in de browsers, om veelvoorkomende aanvallen vroegtijdig te detecteren.

Welke beschermingsdoelen worden met deze maatregel bereikt?

☐ Beschikbaarheid
☐ Integriteit
☐ Vertrouwelijkheid
☐ Authenticiteit

Classificatie van het technologieniveau



3.2.27 Cyber threat intelligence

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

Cyber Threat Intelligence is ingedeeld in drie toepassingsgebieden:

- Tactische Cyber Threat Intelligence omvat malware-analyse en de import van individuele, statische en gedragsdreigingindicatoren in defensieve IT-beveiligingsoplossingen zoals netwerk-, endpoint- en applicatiebeveiligingsoplossingen om hun effectiviteit te vergroten. Indicatoren verkregen via Cyber Threat Intelligence kunnen een belangrijke rol spelen in maatregelen zoals systeempatching.
- Operationele Cyber Threat Intelligence wordt gebruikt om kennis over een aanvaller, zijn vaardigheden, infrastructuur en aanvalstactieken, evenals technieken en

procedures (TTP's) te verbeteren. Deze informatie kan worden gebruikt om significant meer gerichte cyberbeveiligingsmaatregelen te implementeren, zoals incidentanalyse, incidentrespons en proactieve opsporen van bedreigingen. Dit verbetert de prestaties van cybersecurity-werknemers (bijvoorbeeld van het Security Operation Center of CERT) zoals experts op gericht zoeken naar bedreigingen, kwetsbaarheidmanagers, incidentresponse-analisten en experts op het gebied van insider bedreigingspreventie.
- Strategic Threat Intelligence biedt een beter begrip van de huidige dreigingsituatie (dreigingsanalyse), het afleiden van trends en het motiveren van individuele aanvallergroepen. Het ondersteunt strategische zakelijke beslissingen om de cyberveiligheid te verbeteren.

Tegen welke dreiging(en) wordt deze maatregel ingezet?
CTI biedt informatie over alle soorten huidige en potentiële cyberbedreigingen en helpt zich daartegen te verdedigen.

Welke maatregelen (procedures, faciliteiten of werkingswijzen) worden in deze sectie beschreven?

Tactical Cyber Threat Intelligence (TM)
Integratie van threat indicators (feeds) in bestaande endpoint- en netwerkdetectie & responsesystemen, systeembeheeroplossingen, firewalls, IDS/IPS- en SIEM/SOAR-oplossingen met als doel het identificeren van echte aanvallen en ondersteunende analyses (inclusief retrojacht) en het voorkomen van het compromitteren. Voor een optimale effectiviteit moet het mogelijk zijn om de indicatoren voor detectie en preventie van cyberaanvallen geautomatiseerd te gebruiken. De bronnen voor Threat Intelligence Indicators maken het mogelijk conclusies te trekken over hun betrouwbaarheid en worden gedifferentieerd in:

- Open Source Intelligence (OSINT),
- Evenementen van privatr honeypotsystemen,
- inzichten uit aanvalsanalyses uit echte klantomgevingen, en
- Onderzoekswerk door inlichtingendiensten opgeleide deskundigen

Operationele Cyber Threat Intelligence (TM/OM)
Organisaties die een Security Operation Centre (SOC) exploiteren en mogelijk hun eigen Computer Emergency Response Team (CERT) hebben, passen Threat Intelligence toe om continu op de hoogte te blijven van de actoren en hun TTP's. Hiervoor bieden uitgebreide Threat Intelligence-platforms toegang tot indicatoren, verschillende rapportformaten (korte berichten, situatierapporten, aanvallerprofielen), toegang tot malwaredatabases, sandbox-technologie voor geautomatiseerde malware-analyse en malware reverse engineering. De aanbieder moet in staat zijn om klantspecifieke eisen te dekken, bovendien moet het mogelijk zijn om rechtstreeks bij de aanbieder toegang te krijgen tot analisten en om onderzoeksverzoeken (RFI's) in te dienen.

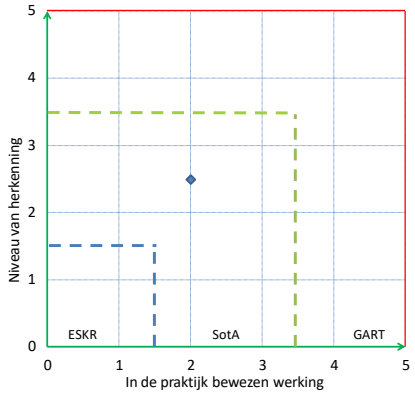
Strategische Threat Intelligence (OM)
Zowel de informatiebeveiligingssector als de algehele/bedrijfsbeveiliging van grote bedrijven gebruiken Threat Intelligence om een zo compleet mogelijk beeld van de situatie te krijgen. De geopolitieke situatie en sectorspecifieke en mondiale trends in het dreigingslandschap lopen daarbij voorop. Door toegang te hebben tot een toegewijde werknemer bij de provider wordt het eigen team virtueel uitgebreid en zorgt voor directe toegang tot de datapool van de provider en dat klantspecifiek onderzoekswerk optimaal wordt uitgevoerd.

Aanbieders van moderne IT-beveiligingsoplossingen leveren integratie en automatiseren Threat Intelligence, zodat dreigingindicatoren en relevante aanvalstelemetrie zinvol met elkaar verbonden zijn, preventieve maatregelen geautomatiseerd worden en het toewijzen aan een aanvaller mogelijk wordt gemaakt, zonder dat de gebruiker extra personeel of systemen nodig zijn.

Welke beschermingsdoelen worden met deze maatregel bereikt?

- ☐ Beschikbaarheid
- ☐ Integriteit
- ☐ Vertrouwelijkheid
- ☐ Authenticiteit

Classificatie van het technologieniveau



3.3 Organisatorische maatregelen

Omdat informatie- en communicatievoorzieningen in beginsel niet altijd zijn ontworpen voor beveiliging en technische beveiliging alleen effectief is wanneer 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).

Vanuit een ISMS worden regels gesteld en geïmplementeerd voor het classificeren en omgaan met gevoelige informatie. Het ISMS is een belangrijk onderdeel van het managementsysteem en loopt door alle belangrijke geledingen van de organisatie. Het ISMS omvat procedures voor regelmatige inspectie en documentatie van organisatorische en technische veranderingen.

Een belangrijke focus van het ISMS is het overwegen van veranderingen in de informatiebeveiliging wanneer belangrijke elementen van de IT-structuur moeten worden gewijzigd of onderhouden. Een ander aspect is regelmatige training en het bewustmaken van het personeel. Het ISMS bepaalt ook hoe noodpreventie moet worden uitgevoerd en hoe te reageren op mogelijke beveiligingsincidenten. Het doel van het ISMS is om een lange termijn beveiligingsniveau te garanderen en te handhaven dat efficiënt en consistent adequaat is.

TeleTrusT geeft met haar document “Informationssicherheitsmanagement - Praxisleitfaden für Manager" een bruikbare richtlijn voor het beheer van informatiebeveiliging. Het document toont dat het beheer van informatiebeveiliging en bijbehorende nalevings- en risicocultuur een strategisch controle-instrument beschikbaar kan zijn dat de veiligheidssituatie 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 het implementeren van een ISMS. In tegenstelling tot technische maatregelen zijn de voortdurende veranderingen in organisatorische maatregelen een permanent fenomeen, wat betekent dat verwijzing naar standaarden en normen zelfs in de context van state of the art mogelijk is. De ISO/IEC 27000 reeks wordt gebruikt als referentiepunt voor verdere standaarden en normen. Er zijn enkele overlappingen, deze worden over het algemeen gebruikt als synergieën, wat resulteert in een positief effect op de gebruikte standaarden, in de zin van informatiebeveiliging. Voor zover aanvullende standaarden of normen worden toegepast voor het beheer van IT-diensten, -processen of -risico's, moeten de geadresseerde overlappingen worden geïdentificeerd en gebruikt.

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

ISO/IEC 27001 is de meest bekende standaard in de ISO/IEC 27000 serie. Het formuleert de eisen waaraan een ISMS moet voldoen. Voor concrete implementatie zijn ook andere normen en richtlijnen beschikbaar.

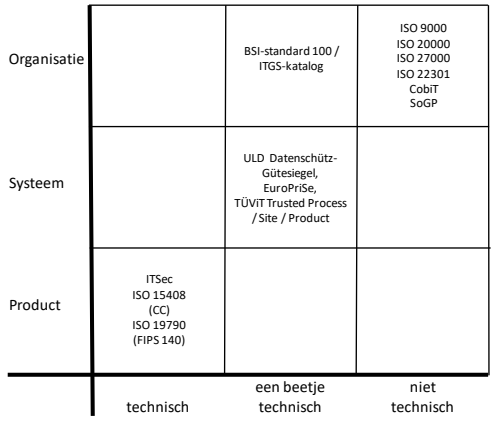
De ISO/IEC 27000-reeks bevat de volgende belangrijke items, elk functionerend als zelfstandige standaard en gegroepeerd als een reeks van standaarden.

Standaard	Gebruikt voor de volgende taken
NEN-ISO/IEC 27000	Managementsystemen voor informatiebeveiliging, Overzicht en woordenlijst
NEN-ISO/IEC 27001	Managementsystemen voor informatiebeveiliging, Eisen (voor een ISMS)
NEN-ISO/IEC 27002	Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging
NEN-ISO/IEC 27003	Managementsystemen voor informatiebeveiliging, Handleiding
NEN-ISO/IEC 27004	Managementsystemen voor informatiebeveiliging, Monitoring, meting, analyse en evaluatie
NEN-ISO/IEC 27005	Beveiligingstechnieken, Risicobeheer voor informatiebeveiliging
NEN-ISO/IEC TR 27019	Beveiligingstechnieken, Besturingselementen voor informatiebeveiliging voor de energiesector
NEN-ISO/IEC 27031	Beveiligingstechnieken, Concepten en principes met betrekking tot IT-ondersteuning voor bedrijfscontinuïteit
NEN-SO/IEC 27034	Informatietechnologie, Applicatiebeveiliging deel 3: beheerproces
NEN-ISO/IEC 27035	Beveiligingstechnieken, Incidentbeheer deel 1: principes

Tabel 1: Overzicht van de ISO/IEC 27000-reeks

Andere normen en standaarden
Informatiebeveiligingsstandaarden en criteria kunnen, afhankelijk van het niveau waarop ze worden beschouwd, worden geclassificeerd als bedrijfs-, systeem- en productstandaarden. 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 weergegeven:



Afbeelding 5: Structuurniveaus van voor Informatiebeveiliging relevante standaarden

Als norm voor organisaties (bedrijven en overheidsinstellingen), die in een niet-technische

taal, geformuleerd is, ontstaat met name behoefte aan afbakening van de ISO 27001 van ISO 9001, ISO 20000-1, ISO 22301, COBIT en de Standard of Good Practice (SoGP).

ISO 27000 e.v.
De reeks standaarden in de ISO 27000 e.v. bevat verschillende standaarden met betrekking tot het ISMS. Een cruciale standaard in deze serie is ISO/IEC 27001, waarin de vereisten voor een goed functionerend ISMS in de context van een organisatie zijn beschreven (zie 3.3.1.1).

ISO 27001 op basis van de BSI IT-Grundschutz
Dit is de implementatie van ISO 27001 met behulp van de IT-basisbeschermingscatalogus (IT Grundschutz) van het Duitse Federale Bureau voor Informatiebeveiliging (BSI) (ook gedocumenteerd in BSI-norm 100-2).

De BSI -norm 100-1 definieert algemene eisen voor een ISMS. In principe is deze compatibel met de standaard ISO- 27001 en verder worden de aanbevelingen van andere standaarden in de ISO 2700x-familie, zoals ISO 27002, in overweging genomen. Het biedt iedereen die geïnteresseerd is een gemakkelijk te begrijpen en systematische introductie en set van instructies, ongeacht welke methode ze zouden willen gebruiken om invulling te geven aan de vereisten.

Met de in de IT-Grundschutz beschreven procedure biedt BSI -norm 100-2:
- specifieke en methodische hulp voor het stapsgewijs invoeren van een ISMS
- het overwegen van de individuele stappen van het informatiebeveiligingsproces
- oplossingen die zijn afgeleid van de praktijkervaring, d.w.z. best practice benaderingen
- mogelijkheid tot certificering

De afbakening van de originele ISO 27001 implementatie versus de basisbescherming aanpak van het BSI is te vinden in de onderstaande tabel:

categorie	**ISO 27001**	**BSI** Grundschutz
reguleringsgebied (scope)	relevante normen <100 pagina's	BSI Grundschutz-Katloge > 4000 pagina's
eisen (requirements)	abstracte en generieke randvoorwaarden	concrete voorbeelden van praktische maatregelen
risicoanalyse	volledige analyse van elk doelobject	vereenvoudigde analyse in geval van verhoogde beschermingseis
maatregelen	ongeveer 150 conceptuele eisen	> 1100 concrete maatregelen
certificering	certificering	auditcertificaat + certificering
geldigheid	3 jaar, jaarlijkse observatie-audits	3 jaar, jaarlijkse observatie-audits

Tabel 2: Differentiatie van ISO 27001 versus de BSI IT-Grundschutz

ISO 20000-1
Deze standaard specificeert eisen van (interne of externe IT) organisaties met betrekking tot de prestaties van procesgerichte diensten. Sommige van de vereiste processen, voornamelijk informatiebeveiligingsbeheer, incidentbeheer (incident & event management) en continuïteitsbeheer) overlappen met ISO 27001. Conventioneel wordt ISO 20000-1 toegepast op IT-organisaties, terwijl de scope van ISO 27001 alle soorten organisaties kan bestrijken.

ISO 22301
Deze standaard houdt zich bezig met het waarborgen van bedrijfscontinuïteit (BCM) en specificeert de eisen van bedrijfscontinuïteit beheersystemen in organisaties. BCM-systemen zoals beschreven in ISO 22301 verwijzen ook naar (maar niet beperkt tot) IT. Het toepassingsgebied van ISO 27001 heeft ook betrekking op BCM, maar alleen vanuit het perspectief informatiebeveiliging (d.w.z. in hoeverre de bedrijfscontinuïteit in gevaar kan worden gebracht door IT-beveiligingsincidenten).

ISO 9001

Deze standaard specificeert de eisen aan kwaliteitsbeheer systemen (KMS), maar omvat ook een ongelooflijk aantal overwegingen op het gebied van informatiebeveiliging, bijvoorbeeld sommige gerelateerd aan verplichtingen ten aanzien van:

- het waarborgen van de beschikbaarheid van middelen en informatie over implementatie en monitoring van processen
- labeling, opslag, bescherming en het kunnen ophalen van logboeken
- onderzoek, levering en onderhoud van infrastructuur zoals gebouwen, werkplekken en bijbehorende nutsvoorzieningen, procesapparatuur (zoals hardware en software) en ondersteuningdiensten (zoals communicatie- en informatiesystemen)
- bescherming van het eigendom van de klant, zoals intellectuele eigendom, persoonsgegevens enz.

COBIT

COBIT is een methode om risico's, als gevolg van het gebruik van IT om bedrijfsrelevante processen te ondersteunen, te beheersen. Het is een toolkit voor het management gericht op revisie en controle dat voor alle IT-processen resultaten en prestatiemeting definieert. COBIT beschrijft verschillende procesgebieden, elk met gedefinieerde controledoelstellingen, volwassenheidsmodellen en maatregelen. COBIT heeft betrekking op alle IT-processen, terwijl ISO 27001 gericht is op het beheersen van informatiebeveiligingsprocessen.

SoGP

De Standard of Good Practice for Information Security (SoGP) van ISF is een goede praktijkbenadering voor bedrijfsinformatiebeveiliging die ook benchmarking van de beveiliging mogelijk maakt. De SoGP behandelt verschillende gebieden binnen de informatiebeveiliging (zoals IT-beveiligingsbeheer, bedrijfskritieke applicaties, informatieverwerking, communicatie/netwerken en systeemontwikkeling) vanuit een zakelijk perspectief en biedt een alternatief, soms met het oog op het aanvullen van de ISO 27001.

3.3.2 Processen

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

Voor organisaties die direct of indirect te maken hebben met ITSiG betekent dit, dat naleving met testen en certificering aan een veelheid aan algemene en sectorspecifieke standaarden vereist is.

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

De beoordeling van state of the art vereist derhalve een individueel onderzoek in hoeverre een individuele maatregel of bundel van maatregelen op een bepaald tijdstip 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 (zoals) processen, werkinstructies, richtlijnen of vergelijkbaar die door de organisatie zelf worden opgelegd en bedoeld zijn om de beveiliging te verhogen. Implementatie en naleving zijn meestal de verantwoordelijkheid van de betrokkenen en worden het best ondersteund door technische maatregelen. Regelmatige controle en opleiding zorgen ervoor dat de geplande maatregelen correct worden uitgevoerd.

De actieve ondersteuning van het management en de samenwerking van gespecialiseerde

afdelingen is cruciaal bij de invoering van een ISMS. Risico's die van invloed zijn op de bedrijfsinfrastructuur, het personeel, IT, processen en informatie, en die een negatief effect hebben op een of meer basiswaarden van informatiebeveiliging (bijvoorbeeld, beschikbaarheid, integriteit en vertrouwelijkheid), moeten worden geïdentificeerd en beoordeeld.

Hieronder volgen de primaire organisatorische processen en maatregelen die kunnen worden afgeleid uit state of the art praktijken.

3.3.2.1 Beveiligingsorganisatie

De beveiligingsorganisatie streeft naar een beheerskader. De beschrijving van de beveiligingsorganisatie omvat de taken en verantwoordelijkheden die betrokken zijn bij het initiëren en bewaken van de implementatie en werking van informatiebeveiliging binnen de organisatie.

Om een ISMS met succes te kunnen invoeren en exploiteren, moet het hoogste management:

- de algehele verantwoordelijkheid op zich nemen voor het ISMS en de informatiebeveiliging binnen de organisatie
- alle relevante verantwoordelijke personen en werknemers op de hoogte te stellen van de mogelijke risico's en persoonlijke aansprakelijkheid in geval van het niet naleven van de vereisten, en de mogelijkheden van een ISMS voor de organisatie zelf en zij moeten ook verantwoordelijkheden met betrekking tot informatiebeveiliging doorgeven
- het definiëren, implementeren en voortdurend verbeteren van een effectieve beveiligingsorganisatie in de vorm van rollen, verantwoordelijkheden en autorisaties.
- Ondertussen moeten met het oog op het beheer van informatiebeveiliging de volgende gegevens worden vastgesteld: organisatiestructuren (bijvoorbeeld afdelingen, groepen, competentiecentra), rollen en taken.

Het volgende zijn de minimumvereisten voor een beveiligingsorganisatie:

- het benoemen van een verantwoordelijke manager (lid van de Raad van Bestuur of directeur en rechtstreeks verantwoordelijk is voor de informatiebeveiliging?) en
- het benoemen van een Chief Information Security Officer (CISO) als centrale rol binnen de IS organisatie.

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

- de algehele verantwoordelijkheid ligt op managementniveau
- elke werknemer is binnen de eigen werkomgeving verantwoordelijk voor de informatiebeveiliging.

De belangrijke rollen en verantwoordelijkheden binnen een beveiligingsorganisatie zijn:

Hoger bestuur (directeuren, raad van bestuur)

- Strategische verantwoordelijkheid (toegewijd), en in laatste instantie ook de algehele verantwoordelijkheid voor informatiebeveiliging
- Verantwoordelijkheid voor alle risicogerelateerde beslissingen

Chief Information Security Officer (CISO)

- Tactische of (soms) operationele controle op de informatiebeveiliging
- Ondersteuning van het management in IS-taakbewustzijn
- Leidinggevende functie met directe recht en plicht om aan het hoogste management te rapporteren

Information Security Officer (ISO)

- Operationele controle van informatiebeveiliging, waar nodig tactische taken voor individuele organisatieonderdelen
- Organisatorisch rechtstreeks toegewezen aan CISO

IS Management Team/IS Management Forum/Security Steering Committee

- Permanent comité voor de planning en implementatie van maatregelen voor

informatiebeveiliging
- Bestaat uit CISO, ISO(s), vertegenwoordigers van de implementatie, gespecialiseerde managers, functionaris gegevensbescherming, vertegenwoordigers van het senior management
- Overleg- en controlefunctie voor CISO

Functionaris gegevensbescherming
- niet noodzakelijkerwijs onderdeel van het IS management team, maar in plaats daarvan een belangrijk contactpersoon op het gebied van compliance, idealiter regelmatig betrokken bij het IS-beheer proces

Audit Manager
- Centraal aanspreekpunt voor interne en externe audits
- Coördinatie en controle van de planning en uitvoering van audits
- Ondersteunt CISO bij hun taken.

Organisatorische maatregelen zijn state of the art, als de uitvoering ervan voldoet aan de huidig geldende normen. Bij de uitvoering van deze maatregelen moeten ten minste de van de ISO/IEC 27000-reeks (normen ISO/IEC 27000 t/m ISO/IEC 27005) in acht worden genomen. Als andere toepasselijke eisen, normen of resultaten van risicobeoordelingen dit vereisen, kunnen andere organisatorische maatregelen noodzakelijk zijn.

3.3.2.2 Beheer van de vereisten (Requirements management)

Een gericht en effectief ISMS kan alleen worden ingevoerd in de context van de specifieke organisatie en haar eisen voor informatiebeveiliging. Daarom moeten de eisen die relevant zijn voor de beveiliging worden vastgesteld en moet de uitvoering ervan worden gepland, gerealiseerd, gecontroleerd en voortdurend worden verbeterd.

Requirements management vormt de basis voor het uitlijnen van informatiebeveiliging als een conditie en proces binnen de organisatie.

Het voortdurend voldoen aan de eisen garandeert tevredenheid van belanghebbenden in een ISMS (d.w.z. stakeholders). Vanwege de complexiteit hiervan wordt het opzetten van een requirements management proces aanbevolen.

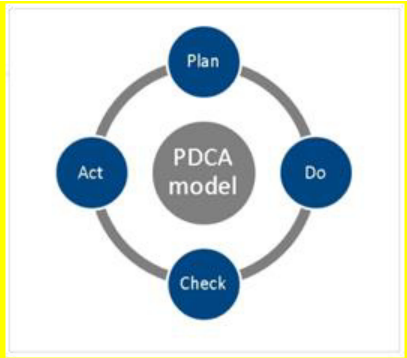
De eisen aan een organisatie kunnen worden onderverdeeld in:
- wettelijke vereisten,
- contractuele vereisten en
- andere eisen.

In toenemende mate kunnen echter vereisten (en verwachtingen) met betrekking tot traceerbare informatiebeveiliging door verschillende zakenpartners van de organisatie kunnen worden ingevoerd (zoals door klanten, leveranciers, dienstverleners, outsourcing-partners, samenwerkingspartners, verzekeringsmaatschappijen enz.).

Wettelijke en contractuele eisen worden vaak primaire of basiseisen genoemd omdat ze de basis vormen van het IS-proces.

Andere eisen (en/of verwachtingen/beperkingen) vloeien doorgaans voort uit de volgende entiteiten:
- markt;
- publiek (in het algemeen);
- de organisatie, het hoofdkantoor;
- aandeelhouders;
- werknemers;
- bedrijfsprocessen (inclusief intern gedefinieerd beleid);
- technologie.

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



Afbeelding 6: PDCA model

PLAN: Alle soorten eisen en verwachtingen van de organisatie,

- de registratie,
- de analyse
- de beoordeling en
- de vertaling naar interne (beveiligings)specificaties voor de organisatie.

DO: Het voldoen aan de informatiebeveiliging specificaties van de organisatie (en impliciet ook aan de eisen en verwachtingen van de organisatie), zoals in de vorm van:

- de organisatorische maatregelen: beleid, regelgeving, richtlijnen
- personeelsgerelateerde maatregelen, waaronder personeelsbeoordeling, (informatiebeveiliging-) bewustzijn, permanente opleiding
- de technische maatregelen van toegangscontrole, encryptie enz.
- de infrastructurele maatregelen voor toegangscontrole, veiligheidszones

CHECK: Toezicht op en herziening van de mate waarin de specificaties voor institutionele informatiebeveiliging wordt voldaan (en daarmee impliciet aan de eisen en verwachtingen van de organisatie):

- het opvragen van indicatoren en parameters
- het identificeren van tekorten (in interactie met de stakeholders)
- het plannen van corrigerende maatregelen.

ACT: Voortdurende verbetering van de mate waarin aan de institutionele informatiebeveiliging specificaties wordt voldaan (en daarmee impliciet ook de eisen en verwachtingen van de organisatie):

- het implementeren van corrigerende maatregelen en de werkzaamheid ervan controleren
- het communiceren van verbeteringen.

Effectief requirements management garandeert de naleving van wettelijke, contractuele en andere eisen en zorgt ervoor dat schending van wettelijke, regelgevende, contractuele en andere verplichtingen met betrekking tot informatiebeveiliging wordt vermeden.

Positieve beoordeling van het ISMS en de daarmee bereikte informatiebeveiliging zorgen ervoor, dat ze op de juiste manier worden geïmplementeerd en worden uitgevoerd in overeenstemming met de richtlijnen, processen en relevante vereisten van de organisatie.

3.3.2.3 Beheer van het toepassingsgebied

Bij de reikwijdte van een ISMS moet altijd rekening worden gehouden met de eisen aan de informatiebeveiliging van de organisatie. Het toepassingsgebied wordt dienovereenkomstig ontwikkeld. Overeenkomstige wijzigingen moeten zorgvuldig worden gepland en uitgevoerd. Documentatie en verantwoording voor het toepassingsgebied moeten worden bewaard om aan te tonen dat het voldoet aan de strengste industrienormen.

3.3.2.4 Beheer van de informatiebeveiligingsrichtlijnen

Als basis voor een ISMS moet de focus van het management van de organisatie gericht zijn op informatiebeveiliging. Het doel is dat het management richting geeft en dat de

beschermende doelstellingen in verhouding staan tot de eisen van de organisatie en de relevante wet- en regelgeving.

Om te voldoen aan de state of the art moeten de doelstellingen voor informatiebeveiliging en het informatiebeveiligingsbeleid worden gedefinieerd in de vorm van een richtlijn en binnen de organisatie bekend worden gemaakt. Bovendien moeten voldoende middelen worden verstrekt en moet het belang van het voldoen aan de eisen worden gecommuniceerd.

Dit richtinggevende beginsel (met inbegrip van de doelstellingen op het gebied van informatiebeveiliging) moet ten minste eenmaal per jaar worden gecontroleerd, om ervoor te zorgen dat ze up-to-date zijn en indien nodig worden verbeterd.

3.3.2.5 Beheer van de risico's (Riskmanagement)

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

Voor state of the art risicobeheer moeten regels worden opgesteld om de waarden, kwetsbaarheden, dreigingen, effecten en waarschijnlijkheid van gebeurtenissen en de toelaatbare omvang van het restrisico te bepalen. Ook moet de methodologie voor het uitvoeren van risicobeoordeling en -behandeling en de vaststelling van de restrisico's door het hoger management worden vastgesteld.

Bestaande risico's moeten op deze basis worden geanalyseerd, beoordeeld en behandeld. Restrisico's moeten door het hoger management aantoonbare wijze worden geaccepteerd en de algehele risicoblootstelling van de organisatie moet voortdurend worden geoptimaliseerd.

Verdere details worden toegelicht in het hoofdstuk "Beheer van Informatiebeveiligingrisico's".

3.3.2.6 Beheer van de verklaring van toepasselijkheid

In een verklaring van toepasselijkheid moet continue de documentatieregistratie worden bijgewerkt, waarin de van toepassing zijnde controls van ISO 27001 Bijlage A (en indien van toepassing andere beveiligingsmaatregelen) benoemd zijn en welke niet van toepassing zijn, de redenen voor de beslissing hiervoor en een beschrijving van de wijze waarop deze maatregelen moeten worden uitgevoerd. De verklaring van toepasbaarheid geeft een actueel beeld van het doel en de feitelijke stand van de informatiebeveiliging in de organisatie in de relevante beoordelingscyclus in overeenstemming met de state of the art praktijken.

3.3.2.7 Beheer van bedrijfsmiddelen (Resourcebeheer)

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

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

3.3.2.8 Beheer van kennis- en competenties

Om een ISMS professioneel te kunnen beheren, moeten de personen die daarvoor verantwoordelijk zijn, over de bijbehorende competenties beschikken of via bijscholing naar dit kennisniveau worden gebracht. Om te voldoen aan de state of the art praktijk, moet de behoefte aan kennis en competenties worden bepaald, de competenties moeten worden verworven en de werkelijke behoefte voortdurend worden aangepast.

3.3.2.9 Beheer van documentatie- en communicatie

Het doel is hier om zowel de beoordelingen als de feitelijke toestand van het ISMS en de informatiebeveiliging vast te leggen, met inbegrip van het verwezenlijken van doelstellingen, hoe risico's worden behandeld en hoe aan de eisen wordt voldaan, en dit te communiceren naar belanghebbenden, rekening houdend met de behoeften van de doelgroepen.

Om te voldoen aan de state of the art praktijk, moet de nodige documentatie worden aangemaakt en aantoonbaar worden gecommuniceerd voor alle gecontroleerde controls.

3.3.2.10 Beheer van de IT-diensten (IT-servicemanagement)

IT-servicebeheer biedt een aanpak op alle niveaus van IT-beheer en op alle expertiseniveaus, te beginnen met bedrijfsoriëntatie en met inbegrip van servicemethodologie en informatiebeveiliging, tot en met implementatie en beheer van de infrastructuur en het gebruik van de bijbehorende technologie. Het is belangrijk om het beveiligingsproces in te bedden in het proceslandschap van de organisatie.

Aanvullend op de interfaces en processen die worden beschreven in het TeleTrusT document "Informationssicherheitsmanagement - Praxisleitfaden für Manager", moeten de volgende processen worden gevolgd om te voldoen aan de state of the art praktijk:

3.3.2.11 Bedrijfsmiddelenbeheer (Asset Management)

Asset management beschrijft drie aspecten die belangrijk zijn voor waarden van de organisatie en vormt de basis voor analyse en beoordeling van risico's (zie ook 3.3.2.5), de verantwoordelijkheden, classificatie en behandeling van media.

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

3.3.2.12 Training en bewustzijn

Het verhogen van de bewustwording van werknemers is een belangrijke voorwaarde voor de implementatie van het gewenste beveiligingsniveau. Werknemers moeten weten hoe belangrijk informatiebeveiliging is voor de organisatie en hoe ze 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 uit te kunnen voeren, moeten werknemers periodiek worden getraind op het belang van de informatiebeveiliging en zodat zij op de hoogte zijn van alle relevante organisatorische en technische omstandigheden. Training helpt werknemers om (IT)systemen goed te bedienen en om te voldoen aan het naleven van alle noodzakelijke richtlijnen. Deze aspecten moeten, indien van toepassing, worden gecontroleerd als onderdeel van het bedrijfsmiddelenbeheer proces, (zie 3.3.2.7).

3.3.2.13 Bedrijfsvoering (Operatie)

De werking van een beveiligingsorganisatie en -omgeving dient om alles in stand te houden wat nodig is om netwerk, de computer- en serversystemen, applicaties en oplossingen in een veilige en beschermde staat te houden. Het zorgt ervoor dat werknemers, servers en applicaties de juiste toegangsrechten hebben om toegang te krijgen tot de bronnen (resources) die ze nodig hebben en dat monitoring, audits en rapportage worden gecontroleerd plaatsvinden. De werking vindt plaats na implementatie en systeemtesten en zorgt voor onafgebroken onderhoud, updates en monitoring.

Referentiemodellen en IT-servicemanagement (bijvoorbeeld ITIL) bieden een raamwerk voor succesvolle werking.

Op deze manier kunnen informatiebeveiliging beheerprocessen nauw worden gecoördineerd met andere IT-processen. Op deze manier kunnen de informatiebeveiliging beheerprocessen nauw verbonden zijn met overige IT-processen.

3.3.2.14 Incidentbeheer

Incidentbeheer combineert technische en organisatorische maatregelen in reactie op geïdentificeerde en potentiële beveiligingsincidenten. Naast detectie, analyse en beheer van problemen, kwetsbaarheden en gerichte aanvallen, worden ook methoden voor het omgaan

met dit soort incidenten beschreven en gepland, waaronder ook organisatorische en juridische overwegingen.

Het doel van incidentbeheer is het bevorderen van planning en identificatie en implementatie van voorwaarden, zodat in geval van een incident zonder tijdverlies efficiënte en effectieve maatregelen ter bescherming van de organisatie kunnen worden uitgevoerd.

3.3.2.15 Continuïteitsbeheer

Continuïteitsbeheer omvat een samenvatting van technische en organisatorische maatregelen om bedrijfsonderbrekingen te voorkomen. Naast registratie, analyse en beheer van de risico's van falen en de (eventuele latere) gevolgen daarvan, beschrijft en wordt met continuïteitsbeheer gepland hoe om in noodsituaties te gaan met escalatie van incidenten, waaronder organisatorische en juridische kwesties.

Het doel van continuïteitsbeheer is het bevorderen van planning, identificatie en implementeren van eisen, zodat in geval van nood en zonder tijdverlies efficiënte en effectieve maatregelen kunnen worden uitgevoerd ter bescherming van de organisatie.

3.3.2.16 Aanschaf (procurement)

Voorafgaand aan de daadwerkelijke aanschaf van IT-systemen of -diensten zijn enkele voorbereidende stappen te nemen, om ervoor te zorgen dat het resultaat voldoet aan de vereisten van de organisatie. Dit geldt voor aspecten die verband houden met zowel inhoud als beveiliging. Deze punten omvatten:

- Normanalyse (requirements analysis)
- Risicoanalyse
- Beveiligingsanalyse (eisen met betrekking tot functionaliteit en betrouwbaarheid)
- Test- en acceptatieplan.

Als leveranciers betrokken zijn bij langere termijn levering van software, oplossingen of diensten, moet ervoor worden gezorgd dat de bescherming van de waarden van de organisatie en die toegankelijk zijn voor leveranciers, gewaarborgd is. In het bijzonder omvat dit het in een leveranciersovereenkomst beschreven service- en beveiligingsniveau.

3.3.2.17 Softwareontwikkeling en IT-projecten

IT-projecten moeten het vraagstuk van informatiebeveiliging van meet af aan en op transparante en kwantificeerbare wijze aanpakken.

Projectorganisaties moeten toewerken naar een rigoureus, herhaalbaar proces dat in elke fase de beveiliging als elementaire bouwsteen (basiscomponent) omvat en voor elke fase van het project bindende verantwoordelijkheden bepaalt voor de beveiligingsmanager (Security Manager). Deze doelstellingen moeten door het management van de organisatie worden bevestigd en gelegitimeerd. Met name bij faseovergangen moet, om het verplichte aspect van "secure by design" in het IT-proces te benadrukken, een formele goedkeuringsregel worden opgesteld. De ervaring leert dat het beveiligingsteam nauw moet samenwerken met het projectteam, in het bijzonder in de planning- en implementatiefase. Het beveiligingsteam moet aanvullende beveiligingseisen en een bindende beveiligingsarchitectuur definiëren en een dreigingsanalyse uitvoeren. De resultaten worden vervolgens opgenomen in het totaalconcept, waardoor dure correcties in latere fasen van het project worden voorkomen (zie hoofdstuk 3.3.3).

3.3.2.18 Beheer van de performance (prestatie bewaking)

Dit proces omvat alle activiteiten op het gebied van monitoren, meten, analyseren- en beoordelen met betrekking tot het ISMS en de in deze context geproduceerde informatiebeveiliging. Deze activiteiten moeten worden bewaakt en gecontroleerd op naleving van state of the art. Dit betekent onder andere het registreren en regelmatig evalueren van protocollen, maar ook het regelmatig uitvoeren van interne audits en technische systeemaudits om informatie te verkrijgen over de vraag of het ISMS en de door haar geproduceerde informatiebeveiliging (nog) voldoen aan de eisen, effectief zijn uitgevoerd en worden gehandhaafd. Het hoogste niveau management moet het ISMS

minstens eenmaal per jaar evalueren, om te bepalen of en in welke mate het ISMS voldoet aan de gedefinieerde doel en bijdraagt tot de uitvoering van de informatiebeveiligingsdoelstellingen. Dit vormt de basis voor verdere besluiten.

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

3.3.2.19 Technische systeemaudits

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

- Voor een kleine penetratietest worden willekeurig configuraties en beleid met betrekking tot beveiliging in de gebruikte IT-systemen onderzocht in de vorm van een technische audit en worden aanbevelingen gedaan 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 ook met behulp van onder andere speciale beveiligingstools de geteste IT-systemen onderzocht naar kwetsbaarheden, door technische onderzoeken. Daarbij krijgen de testers toegang tot de IT-systemen die ter plaatse onder toezicht van de beheerders moeten worden geïnspecteerd.
- Met een IS-webcheck wordt de beveiligingsstatus van de aanwezigheid van internet, intranet en/of extranet van de organisatie gecontroleerd.
  In dit proces wordt het merendeel van de tests en uitgevoerd met behulp van via het internet beschikbare geautomatiseerde methoden en, waar van toepassing, via het interne netwerk (voor intranet en extranet).

3.3.2.20 Interne en externe audits, *ISMS*-certificering

ISMS-audits dienen de volgende doeleinden:

- Het controleren van de voortgang van de implementatie van het ISMS
- Het bepalen of het ISMS voldoet aan de auditcriteria van de organisatie
- Het bepalen of het ISMS in staat om te voldoen aan wettelijke, regelgevende en contractuele eisen
- Het controleren van het gebruik en effectiviteit van het ISMS
- Het identificeren van kwetsbaarheden/potentie voor het verbeteringen in het ISMS

Interne audits moeten in het kader van het toepassingsbereik van het ISMS doorgaans ten minste eenmaal per jaar door of namens de organisatie worden uitgevoerd. Om aan de state of the art te voldoen, wordt elke organisatie-eenheid (of elk onderdeel van het toepassingsgebied, zoals locatie, gebouwen, enz.) ten minste eenmaal in de drie jaar intern gecontroleerd.

Externe ISMS-audits worden als tweede partij audit uitgevoerd door in de organisatie belanghebbende partijen (bijvoorbeeld klanten) of als audit van derden (third party audit)door een externe, onafhankelijke auditororganisatie.

Als onderdeel van het uitvoeren van certificeringaudits controleert het auditteam of aan de eisen van ISO 27001 is voldaan, die moeten worden uitgevoerd met inachtneming van de normen ISO 27002 en ISO 27005. Auditors van de certificeringinstanties moeten gedurende de auditprocedure voldoen aan de -normen ISO 19011 en ISO 27007. ISO/IEC TR 27008 bevat een richtlijn voor het auditen van ISMS-controls en is eveneens van toepassing.

De certificeringinstantie voert het kader van de certificeringprocedure de volgende taken uit in:

- Controle van de auditresultaten inclusief auditconclusies
- Documentatie van de evaluatie van de auditresultaten, inclusief de auditconclusies
- Certificeringrapport met certificaatgoedkeuring

- Uitgifte van het certificaat.

Geaccrediteerde certificeringinstanties voor ISO 27001 hebben accreditatie volgens ISO 17021 en ISO 27006 Een overzicht van de in Nederland geaccrediteerde ISMS-certificerende instanties is te vinden op de website van de Raad voor Accreditatie (https://www.rva.nl); een overzicht van in Duitsland geaccrediteerde instanties is te vinden op de website van de (Duitse) Nationale Accreditatie-instantie (DAkkS).

ISO 27001 certificering is drie jaar geldig en wordt ten minste eenmaal per jaar als onderdeel van surveillance audits opnieuw beoordeeld. Om het certificaat na drie jaar verlengd te krijgen, moet de organisatie, nog voordat de periode van drie jaar is verstreken, met succes een hercertificeringaudit hebben doorstaan.

3.3.2.21 Continu verbeteringsproces (Improvement Management)

De organisatie moet de toereikendheid, geschiktheid en effectiviteit van hun ISMS voortdurend verbeteren.

De essentiële activiteiten op het gebied van onderhoud en voortdurende verbetering van een ISMS zijn bedoeld om voortdurend de ISMS-prestaties te evalueren en te optimaliseren. Hierbij moeten in het bijzonder de volgende aspecten aan de orde komen:

- Het omgaan met non-conformiteiten die voortvloeien uit het monitoren, meten, analyseren en beoordelen van het ISMS en de in dit verband bereikte informatiebeveiliging
- Het vaststellen en uitvoeren van corrigerende maatregelen om de oorzaak van non-conformiteit te elimineren

Voortdurende verbetering van de toereikendheid, geschiktheid en effectiviteit van het ISMS en de daarmee gegenereerde informatiebeveiliging.

3.3.3 Veilige softwareontwikkeling (Secure Software Development)

Gedurende het hele softwareontwikkelingsproces moet rekening gehouden worden met beveiliging van een applicatie.

Ongeacht de gebruikte ontwikkelingsmethode moet rekening worden gehouden met maatregelen voor een veilige ontwikkeling van toepassingen. Voor veilige softwareontwikkeling zijn procedurele modellen en best practices beschreven in BSIMM, OWASP SAMM, OWASP ASVS, Grip op SSD van het CIP[30]webrichtlijnen van het Forum Standaardisatie[31,] de BSI-richtlijnen voor de ontwikkeling van veilige webapplicaties, in ISO/IEC 27034 en onderwezen in TeleTrusT Professional for Secure Software Engineering T.P.S.S.E. De essentiële beschermende maatregelen binnen het softwareontwikkelingsproces worden vermeld in de afzonderlijke hoofdstukken.

3.3.3.1 Vereistenanalyse (Requirements Analyse)

Veilige applicatieontwikkeling begint met analyse van de eisen (eisen/normen). De basis van deze analyse is een dreigingsanalyse. De te beschermen (bedrijfs)activa moeten worden gedefinieerd en de bedreigingen die voor deze activa bestaan, moeten worden beschreven. De architectuur van de applicatie, in het bijzonder de gegevensopslag en de gegevensstromen en de grenzen aan hun vertrouwelijkheid hun moeten worden overwogen. Vervolgens moeten de risico's van deze geïdentificeerde bedreigingen worden beoordeeld en tegenmaatregelen en beveiligingseisen voor de applicatie worden afgeleid. Een nuttige methode voor het identificeren van concrete bedreigingen is een definitie van zogenaamde misbruikzaken. Deze beschrijven concrete aanvallen en het, in het geval van een aanval, gewenste gedrag van de applicatie. Verdere beveiligingseisen voor de applicatie vloeien bijvoorbeeld voort uit wettelijke of contractuele verplichtingen. Deze beveiligingsvereisten, zoals de functionele vereisten, vloeien voort uit de daaropvolgende ontwerpfase van het softwareontwikkelingsproces en ook de specificatie van de testcases voor de latere tests van

30 grip-op-ssd-het-proces-v20.pdf (cip-overheid.nl)
31 https://www.forumstandaardisatie.nl/standaard/webrichtlijnen

de applicatie.

De Volere template[32,] die vaak wordt gezien als de standaard van de algemene normspecificatie, definieert al een aantal beveiligingsvereisten, die in aanmerking moeten worden genomen:

- 15a toegangsvereisten;
- 15b integriteitvereisten;
- 15c privacyvereisten;
- 15d auditvereisten;
- 15e immuniteitsvereisten.

3.3.3.2 Software ontwerp

Een veilig ontwerp moet, om de geïdentificeerde bedreigingen tegen te gaan, rekening houden met alle beveiligingseisen. Een resultaat van het ontwerpproces is de beveiligingsarchitectuur inclusief een strategie voor gegevensverwerking. Een veilig ontwerp houdt rekening met aspecten zoals veilige verificatie, cryptografische vereisten, foutafhandeling, systeemconfiguratie, vertrouwensrelatie tussen applicatieonderdelen en de bedrijfslogica van de applicatie. Onvoldoende aandacht voor de beveiliging bij het ontwerp van een applicatie is vaak de oorzaak van zwakke punten, zoals ontbrekende, foutieve authenticatie en autorisatie en kan alleen met grote inspanning achteraf worden verholpen. Andere oorzaken zijn in de code ingebouwde sleutels of wachtwoorden, onjuiste verwerking van gevoelige gegevens of onveilige foutafhandeling die de aanvaller nuttige informatie verschaft. Naleving van Secure Design principes helpt een architect om een robuust ontwerp voor zijn applicatie te creëren. Voorbeelden van dergelijke bewezen ontwerpprincipes zijn Least Privilege, Defense in Depth en Secure by Default. Ontwerpprincipes zoals Privacy by Default worden steeds belangrijker, vooral met betrekking tot de EU-verordening inzake gegevensbescherming (de GDPR). Daarnaast kunnen door een architect zogenaamde ontwerppatronen en best practices voor de beveiliging worden gebruikt die, in tegenstelling tot ontwerpprincipes, een meer concrete, maar taalonafhankelijke benadering biedt om terugkerende problemen op te lossen. Het ontwerp, of ten minste de ontwerpaspecten die relevant zijn vanuit beveiligingsperspectief, moet voordat de implementatie van de applicatie begint worden onderworpen aan een ontwerpbeoordeling.

3.3.3.3 Implementatie

Typische implementatiefouten, zoals het ongecontroleerd verwerken van invoer en uitvoer van deze gegevens of het vermengen van code en gegevens, kunnen leiden tot beveiligingsproblemen zoals code-injection, cross-site scripting en/of bufferoverflows. Specifieke programmeerrichtlijnen helpen ontwikkelaars om zich tijdens de implementatie te concentreren op beveiliging. Deze programmeerrichtlijnen moeten individueel worden afgestemd op de gebruikte programmeertalen, bibliotheken en kaders. Gebruikte frameworks moeten correct worden toegepast, om hun beveiligingsfuncties niet te ondermijnen. Er kan bijvoorbeeld worden opgegeven dat alleen bepaalde functies en objecten mogen worden gebruikt of dat softwaremodules alleen na succesvolle controle met een codeanalysetool kunnen worden benaderd. 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 (op basis van de resultaten van de dreiginganalyse) moeten bovendien worden onderworpen aan een handmatige code review.

Zwakke punten in de applicatie kunnen echter ook het gevolg zijn van het gebruik van onveilige componenten van andere fabrikanten. Daarom moeten dergelijke componenten zorgvuldig worden geselecteerd en moeten de beveiligingsbulletins die door deze leveranciers worden gepubliceerd en de CVE-database met bekende kwetsbaarheden voortdurend worden gecontroleerd. Dergelijke “derde-partij component controle” moet automatisch met behulp van een afhankelijkheidscontrole tool worden uitgevoerd. Bij het gebruik van applicatie-implementatie programma's (deployment programma’s, zoals

32 https://www.volere.org/templates/volere-requirements-specification-template/

containeroplossingen), moeten deze ook worden gecontroleerd op bekende kwetsbaarheden.

3.3.3.4 Testen van de software

Met behulp van blackbox/greybox/whitebox testen en statische en dynamische beveiligingsscans wordt gezocht naar kwetsbaarheden in de applicatie. Indien van toepassing moet, om de hoogst mogelijke efficiëntie te bereiken, de voorkeur worden gegeven aan een combinatie van blackbox-, greybox- en whitebox-testen, statische en dynamische beveiligingsscans. Zo kunnen gebruikte versleutelingalgoritmen eenvoudig worden geïdentificeerd en geëvalueerd door statische analyse van de broncode, terwijl beveiligingshiaten die voortvloeien als gevolg van de integratie van verschillende componenten of alleen bij runtime (zoals in communicatie met een verificatieservice) goed worden geïdentificeerd door dynamische scans van het systeem. In tegenstelling tot handmatige penetratietests kunnen beveiligingsscans, om een beveiligingscontrole van elke softwareversie te garanderen, als onderdeel van het softwareontwikkelingsproces worden geautomatiseerd. 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. Gedefinieerde misbruikgevallen zijn een goede bron voor het maken van testcases.

Deze beveiligingstests bieden echter geen absolute garantie over de beveiliging van de applicatie. Beveiliging kan niet worden bewezen, zoals met functionaliteittests, door het feit dat het verwachte gedrag overeenkomt met waargenomen gedrag. Veiligheid is een negatief criterium; het bestaat meestal uit het voorkomen van ongewenst gedrag. Hier is de creativiteit van een aanvaller bijna oneindig. Zo kunnen er nog meer bedreigingen en testgevallen bestaan, die nog niet werden overwogen. Niettemin zijn beveiligingstests een belangrijk onderdeel van het veilige Secure Software proces.

3.3.3.5 Bescherming van broncode en resources

Om de integriteit van (bron)code en middelen (resources) te behouden en zo de applicatie te beschermen tegen manipulatie zoals backdoors, Trojaanse paarden of veranderingen in de verwerkingslogica, moeten broncode controlesystemen worden gebruikt en, indien nodig, mogen afzonderlijke code-onderdelen alleen aan specifieke ontwikkelaars worden toegewezen. Gevoelige informatie mag niet, om te voorkomen dat deze onbedoeld het publiek bereikt, worden opgeslagen in broncode controlesystemen.

Daarnaast moet een veilige ontwikkelomgeving worden gewaarborgd onder meer door toegangsrechten te beperken en systemen te hardenen, ervoor te zorgen dat ontwikkelaars alleen gepersonaliseerde (persoonsgebonden) gebruikersaccounts gebruiken, niet werken met beheerrechten en getraind zijn in beveiliging.

3.3.3.6 Certificatie van de software

Voorafgaand aan de levering van de software, is het zinvol om die te laten controleren en certificeren door een neutrale instantie. Hoewel de functionaliteit van de software is gewaarborgd door tests, zorgt certificering ervoor dat de architectuur, het Vereistenbeheer (Requirements Management), configuratiebeheer en risicobeheer geschikt zijn voor een veilige ontwikkeling en vooral het oplossen van problemen.

Om zwakke punten later te kunnen elimineren, moeten architectuur en ontwerp zodanig worden ontworpen dat niet alleen bugs kunnen worden geëlimineerd, maar ook defecte onderdelen in noodgevallen kunnen worden vervangen. Voor meer complexe software is Vereistenbeheer essentieel. Vóór de levering moet (opnieuw) worden gecontroleerd of de eisen duidelijk volgens IREB (International Requirements Engineering Board) zijn gedefinieerd. Het toepassen van de eisen moet herleidbaar zijn tot de broncode. In het eenvoudigste geval kan dit worden gerealiseerd, door het toewijzen van ID’s, die vervolgens ook als Comments in de code kunnen worden opgenomen. Dit maakt het mogelijk om snel te reageren op bekend geworden kwetsbaarheden.

Configuratiebeheer is nauw verbonden met vereistenbeheer. Hier moet worden

gecontroleerd of een softwareversie met broncode en alle bijbehorende documenten duidelijk kunnen worden toegewezen aan een versiestatus (en later aan een softwarerelease). Wanneer de eisen worden gewijzigd, moet duidelijk zijn welke documenten al actueel zijn en welke eisen in aanmerking komen en welke niet. Aangezien de documenten individueel worden ontwikkeld, hebben documenten gewoonlijk een verschillende status en versie. Daarom moet, naast het toekennen van versies aan documenten, ook een zogenaamde Baseline worden gedefinieerd, die bepaalt welke documenten bij elkaar horen bij welk versienummer en dus bij een bepaalde release. Dit maakt het mogelijk om te zien welke fouten en zwakke punten in welke softwareversie is gecorrigeerd.

In de eerste stap dient risicobeheer zich bewust te zijn van de mogelijke risico's en gevaren die zich, onder andere door zwakke punten, kunnen voordoen. Risicobeheer is vooral noodzakelijk, wanneer mensenlevens in gevaar kunnen komen. 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 en ernst,
- risicomitigerende maatregelen definieert,
- risico's opnieuw indeelt, nadat de maatregelen zijn uitgevoerd;
- op regelmatige tijdstippen en in geval van veranderingen wordt voortgezet.

Als de software in systeemverband (System Group) wordt uitgevoerd, moet het hele systeemverband worden gecertificeerd.

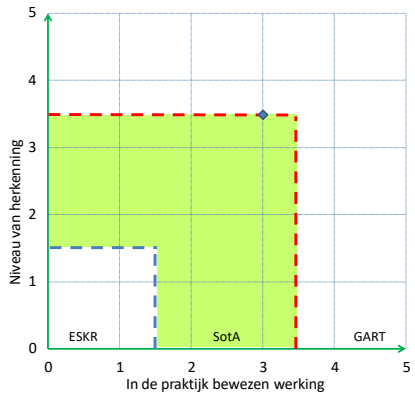
3.3.3.7 Levering van software (Software Delivery)

Een kwetsbaarheid bij de levering en installatie van de software vernietigt het resultaat van alle eerdere beveiligingsmaatregelen in het softwareontwikkelingsproces. Daarom moet een veilig levering- en implementatieproces de integriteit van de geïmplementeerde software waarborgen, om te voorkomen dat de toepassingsomgeving (productieomgeving) wordt aangetast. Voor dit doel kunnen code- signatures worden gebruikt. Aanvallen op de geïmplementeerde applicatie zijn ook mogelijk als gevolg van onveilige configuratie van de applicatie zelf. Daarom moet een veilige configuratie van de software in de productieomgeving worden gewaarborgd en moeten ongeautoriseerde wijzigingen in de configuratie worden voorkomen. Geschikte standaardinstellingen (Security by Default) en handleidingen voor beheerders zijn hier als beveiligingsmaatregelen beschikbaar. Om de potentiële schade van een aanval te minimaliseren, moet de applicatie minimale toegangsrechten hebben (Least Privilge). In het bijzonder worden applicaties in containeromgevingen vaak onnodig als root-gebruiker uitgevoerd, wat koste wat kost moet worden vermeden. Voor de beveiliging van de applicatie is het is essentieel, dat deze altijd met beveiligingsupdates up-to-date wordt gehouden.

3.3.3.8 Beveiligingsresponse

Aangezien kwetsbaarheden nooit volledig kunnen worden uitgesloten, moet elke fabrikant voorbereid zijn op dergelijke meldingen en snel kunnen reageren. Het zogenaamde Security Response proces van een fabrikant beschrijft haar aanpak bij het omgaan met beveiligingsproblemen die bekend zijn geworden. Beveiligingspatches zijn tijdkritisch en moeten daarom snel beschikbaar worden gesteld. Dit betreft zelf ontwikkelde componenten en bekende kwetsbaarheden in standaardsoftware, zoals bibliotheken en frameworks. Om beveiligingsonderzoekers te motiveren om kwetsbaarheid te melden, zijn Responsible Vulnerability Disclosure- of Bug-Bounty-programma's beschikbaar. Het is essentieel dat gemelde kwetsbaarheden terugvloeien in het softwareontwikkelingsproces op een zodanige manier dat ze worden geëlimineerd.

Classificatie van het technologieniveau



3.3.4 Proces certificering

Om in een organisatie de informatiebeveiliging en gegevensbescherming succesvol te implementeren, moeten processen worden geïdentificeerd en passende maatregelen worden genomen. De uitvoering van dergelijke maatregelen is echter alleen doeltreffend als de doeltreffendheid ervan regelmatig wordt geverifieerd. Deze beoordeling kan worden uitgevoerd door interne of externe bronnen. Een speciaal extern effect, maar niet voor alle organisaties verplicht, wordt bereikt door certificering volgens de huidige normen. Dit hoofdstuk beschrijft de mogelijkheden van procescertificering.

Context informatiebeveiliging

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

De ISMS-certificeringaudits hebben de volgende doelstellingen:

- Controle van de voortgang van implementatie van een ISMS
- Bepaling van de compliance van het ISMS met de auditcriteria van de organisatie
- Bepalen Van het vermogen van het ISMS om aan wettelijke, regelgevende en contractuele vereisten te voldoen
- Beoordeling van het toepassen en de effectiviteit van het ISMS
- Identificatie van kwetsbaarheden / verbeteringspotentieel van het ISMS

Interne audits (zogenaamde "First Party Audits") binnen een toepassingsgebied van het ISMS moeten in beginsel ten minste eenmaal per jaar door of namens de organisatie worden uitgevoerd. Deze audits zijn verplicht voor ISMS-certificering. Elke organisatie-eenheid (of elk onderdeel van het toepassingsgebied, zoals locatie, gebouw, enz.) wordt regelmatig intern gecontroleerd. In het geval van een interne audit is het van essentieel belang ervoor te zorgen dat de afdelingen niet zelf controleren, maar dat de audits altijd door een onafhankelijke persoon worden uitgevoerd.

De zogenaamde "second party audits" zijn externe ISMS audits uitgevoerd door partijen die geïnteresseerd zijn in de organisatie (zoals de eigen klanten). Als de externe audits worden uitgevoerd door onafhankelijke auditorganisaties, worden ze derden-audits (third-party audits) genoemd. In het geval van een uitbestedingcontract kunnen passende leverancieraudits nodig zijn.

De leverancier (of outsourcer) kan echter ook aantonen dat hij aan de vereisten voor informatiebeveiliging voldoet door middel van een passend certificaat (bijvoorbeeld ISO 27001 of ISO 27001 op basis van BSI IT-Grundschutz).

Als een ISMSmoet worden gecertificeerd, moet de auditprocedure worden uitgevoerd door een erkende certificeringinstantie. Certificeringinstanties voor ISO 27001 hebben een accreditatie volgens ISO 17021 en ISO 27006. Een overzicht van in Duitsland geaccrediteerde ISMS-certificeringsinstanties is te vinden op de website van de Duitse Accreditatie-instantie (DAkkS). Het Federal Office for Information Security (BSI) is de

verantwoordelijke certificeringinstantie voor elementaire IT-bescherming. Een overzicht van de in Nederland geaccrediteerde ISMS-certificerende instanties is te vinden op de website van de Raad voor Accreditatie (https://www.rva.nl);

Als onderdeel van de certificeringaudit controleert het auditteam of aan de eisen van ISO 27001 of de BSI IT-Grundschutz van het BSI is voldaan. De audits moeten worden uitgevoerd op ISO 27001, met in achtneming van de normen uit ISO 27002 en ISO 27005 (en indien nodig verdere branchespecifieke aanvullingen op de normen van de 27-serie). Auditors van certificeringinstanties voor ISO 27001 moeten, het kader van de auditprocedure,de normen uit ISO 19011 en ISO 27007 in overweging nemen. Voor audits volgens BSI IT-Grundschutz moet de desbetreffende geldige certificeringregeling van het 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 ten minste eenmaal per jaar, in het kader van zogenaamde surveillance audits, gecontroleerd. Indien het certificaat na 3 jaar wordt verlengd, moet de organisatie voor het einde van de periode van 3 jaar met succes een hercertificeringaudit hebben doorstaan. Afhankelijk van de sector kan het zijn dat ook aan zogenaamde sectorspecifieke eisen moet worden voldaan. Nagegaan moet worden of de desbetreffende sectorspecifieke eisen aantoonbaarheid van een gecertificeerd ISMS vereisen. Bovendien kunnen verdere vereisten worden gedefinieerd, die volgens specificatie moeten worden geïmplementeerd en bewezen. Een overzicht van gepubliceerde sectorspecifieke standaarden is te vinden op de BSI website.

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

Andere voordelen die voor ISMS -certificering spreken zijn:

- Bewijs van passende beoordeling en behandeling van risico;'s
- Bevestiging door onafhankelijke derden van de functionaliteit van het ISMS
- Bewijs van de continue verbetering van het ISMS
- Vermindering van de aansprakelijkheid in geval van incidenten, omdat het naleven van een in de EU geharmoniseerde norm doet vermoeden van conformiteit aan erkende technologieregels (normen) en stand van de techniek.
- Externe presentatie in het kader van corporate marketing/ voor de reputatie naar anderen

Context Gegevensbescherming

De invoering van een gegevensbescherming beheersysteem (DSMS) leent zich ook voor het controleren van de effectiviteit van maatregelen in verband met de vereisten van de Europese basisverordening persoonsgegevens (GDPR). Hoewel de GDPR een dergelijk systeem niet expliciet voorschrijft, toont het toch op veel plaatsen de noodzaak van een dergelijk systeem. GDPR vereist bijvoorbeeld[33] een "procedure voor de regelmatige herziening, beoordeling en evaluatie van de effectiviteit van technische en organisatorische maatregelen om de beveiliging van de verwerking te waarborgen[34]".

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

---

33 Zie ook GDPR Art. 5(2) "De controller (...) moeten (...) aantonen dat aan de regels voldoet" en GDPR Art. 24, lid 1, "(...) waarborgen en het bewijs leveren (...) dat de verwerking overeenkomstig deze verordening wordt uitgevoerd.".
34 bijvoorbeeld GDPR Art. 32, lid 1 d

Net als een ISMS kan ook de DSMS worden gecontroleerd en kan zo de mate van volwassenheid van een dergelijk systeem worden bepaald. Op basis van de ISO 19011 richtlijnen kunnen audits op basis van een auditprogramma en een auditplan worden uitgevoerd. Een audit kan worden uitgevoerd door de Functionaris Gegevensbescherming (Data Protection Officer, ook wel FG of PO genoemd). In grotere organisaties kunnen de audits ook worden uitgevoerd door vakkundig opgeleide medewerkers van de organisatie zelf of door adviesbureaus die gespecialiseerd zijn in gegevensbescherming.

Binnen het kader van de zogenaamde leverancieraudits kunnen ook alle (sub-)contracters (contractverwerkers van de organisatie) worden gecontroleerd.

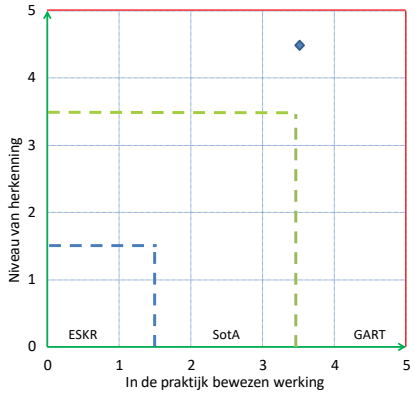
Ongeacht het bovenstaande bestaat, in de context van gegevensbescherming, ook de mogelijkheid van certificering om bewijs te verkrijgen van de naleving van de bepalingen van de GDPR (zie GDPR Art. 42 lid 1). Op grond van GDPR Art. 42 lid 5 moet echter eerst worden goedgekeurd door erkende certificeringinstanties overeenkomstig GDPR Art. 43 (zoals in Duitsland, de DAkks) of de bevoegde toezichthoudende autoriteit. Dit is nog niet gebeurd.

Zoals blijkt uit de formulering van GDPR Overweging 100, hebben dergelijke "procedures voor gegevensbescherming en tests en beproevingsmerken voor gegevensbescherming" echter alleen betrekking op product-, proces- en servicecertificering (conform ISO/IEC 17065). In dit verband noemt de GDPR zelf bijvoorbeeld

- bewijs van het vervullen van taken van een verantwoordelijke persoon (zie GDPR Art. 24 lid 3);
- bewijs van compliancy met het ontwerp van de technologie en gegevensbeschermingsvriendelijke presets (zie FADP Art. 25 lid 3;
- bewijs van voldoende garanties van een verwerker (zie GDPR Art. 28, lid 5 en 6);
- bewijs van de beveiliging van de gegevensverwerking (zie GDPR Art. 32 lid 3);
- bewijs van passende waarborgen in relatie tot gegevensverwerking in een derde land (zie FADP Art. 46 lid 2 sub f)).

Een DSMS kan in de zin van de GDPR niet worden gecertificeerd door middel van "gegevensbeschermingsspecifieke certificeringprocedures en gegevensbeschermingszegels en testmarkers". Deze zijn echter complementair aan een DSMS en kunnen in beginsel bij de audit van een DSMS in aanmerking worden genomen als bewijs van het naleven van de bepalingen van de GDPR.

Classificatie van het technologieniveau



3.3.5 Kwetsbaarheid- en patchbeheer

Het doel van kwetsbaarheid- en patchmanagement is het identificeren en corrigeren van beveiligings- en functionaliteitstekortkomingen in software en firmware. Patches[35] zijn

35 De drie belangrijkste type patches zijn:

- Bugfix: dit is de correctie van fouten (bugs) die optreden in de (programma)broncode.

bedoeld om geïdentificeerde kwetsbaarheden te elimineren en de exploitatie ervan te voorkomen. Het kwetsbaarheids- en patchbeheerproces omvat identificatie , beoordeling, evaluatie en implementatie voor alle producten en systemen van de organisatie. Voor het kwetsbaarheids- en patchbeheerproces moeten binnen de organisatie verantwoordelijkheden voor implementatie- en effectiviteittesten binnen de organisatie worden gedefinieerd.

3.3.5.1 Assessment

Om patches en kwetsbaarheden efficiënt te beheren, moet eerst het IT-landschap van de organisatie worden geïnventariseerd. Aangezien dit in de loop van de tijd kan veranderen, moet een dergelijke inventarisatie regelmatig worden uitgevoerd en up-to-date worden gehouden. Onderdelen die zich niet in het interne netwerk bevinden (zoals smartphones en notebooks van dienstverleners) moeten volgens speciale richtlijnen worden beheerd. Deze richtlijnen zijn bedoeld om de eigenaren van deze componenten aan te moedigen de softwarestatus op hun apparaten zelf bij te werken of deze regelmatig om te worden bijgewerkt aan te sluiten op het bedrijfsnetwerk.

3.3.5.2 Identificatie en evaluatie

Om kwetsbaarheden, softwarefixes en bedreigingen te identificeren, moeten relevante informatiebronnen (websites van leveranciers, CERT's, CVSS-databases, mailinglijsten voor software- en hardwareleveranciers, nieuwsgroepen van derden, enz.) worden gecontroleerd, evenals het overwegen van professionele tools voor het, binnen de organisatie, beheer van patches.

Iedereen die verantwoordelijk is voor IT-systemen, applicaties, netwerkcomponenten, etc. moet periodiek een overzicht/samenvatting geven van de huidige patchstatus. Hieruit moet een rapport worden opgesteld voor de evaluatie van de huidige patchsituatie en worden gebruikt om het huidige risico te beoordelen (bijvoorbeeld CVSS-score). De volgende oplossingen zijn als behandelingsopties beschikbaar:

- Overdracht aan patchbeheer om geïdentificeerde kwetsbaarheden met een geschikte patch te sluiten (update).
- Definiëring van tijdelijke oplossingen (configuratieaanpassing, codeanalyse, enz.) om het beveiligingslek (als work-around) te behandelen.
- Afsluiting of isolatie van het getroffen systeem.

Als patches om het beveiligingslek op te lossen handmatig worden gedownload, moet, vooral voor downloads van het internet de authenticiteit ervan worden geverifieerd met behulp van gestandaardiseerde methoden (cryptografische checksums, handtekeningen of digitale certificaten). Patches moeten in de eerste plaats rechtstreeks uit bronnen van fabrikanten worden verkregen. Alleen in uitzonderlijke gevallen (bijvoorbeeld voor geïntegreerde producten van derden, zoals runtime-bibliotheken) zijn patches van andere vertrouwde bronnen toegestaan.

3.3.5.3 Inrichting (Provisioning)

Voorbereiding

Zodra de echtheid van de patch is geverifieerd, moeten deze in testsystemen geverifieerd worden. Indien mogelijk moeten de testsystemen op dezelfde of vergelijkbare wijze worden uitgerust en geconfigureerd als het productiesysteem.

Voordat patches in de productieomgeving worden uitgerold, moet een back-up van de getroffen systemen worden gemaakt om de patches in geval van een fout het opnieuw te kunnen installeren. Als de prestaties ongewenst zijn of de functionaliteit beperkt is, moeten probleemoplossing maatregelen worden geïdentificeerd en geïmplementeerd.

- Hotfix: dit is de niet uit te stellen correctie van fouten in de toepassingsprogrammatuur.
- Update: dit is de klassieke vorm van het aanpassen van de programmatuur, de update bevat functieverbeteringen, in sommige gevallen ook correcties van fouten.

Implementatie
Om het uitvoeringsproces naar behoren te laten verlopen, moeten passende voorbereidingen worden getroffen. Dit omvat bijvoorbeeld het informeren van alle systeembeheerders en het definiëren van de tijdsperiode voor het utrollen van de patches. Het installeren moet ook aan de gebruikers worden aangekondigd, zodat zij hun operationele processen tijdig voor de aangekondigde installatieperiode kunnen voltooien.

Normaal gesproken moet distributie van patches geautomatiseerd plaatsvinden (bijvoorbeeld met een Enterprise Patch Management Tool). Het is echter mogelijk dat beheerders afzonderlijke patches lokaal moeten installeren. In dat geval moet de communicatie veilig worden gehouden en moeten bestanden worden uitgewisseld met authenticatie controle. Zodra patches worden uitgerold, moet het proces worden bewaakt en gecommuniceerd, om bijvoorbeeld mislukte implementatiepogingen tijdig op te sporen. Passende corrigerende maatregelen moeten snel worden genomen.

3.3.5.4 Behandeling van uitzonderingen

Niet te patchen systemen
Voor systemen of toepassingen, waarvoor

- geen updates meer beschikbaar zijn bij de fabrikant (zogenaamde legacy-systemen),
- geen updates van het besturingssysteem zijn uitgebracht door de fabrikant,
- een onderhoudsvenster, om operationele redenen, niet op korte termijn beschikbaar gesteld kan worden (bijv. automatisering in procestechnologie),
- tijdens een update een hercertificering van het hele systeem noodzakelijk wordt, moeten technische maatregelen worden vastgesteld en uitgevoerd.

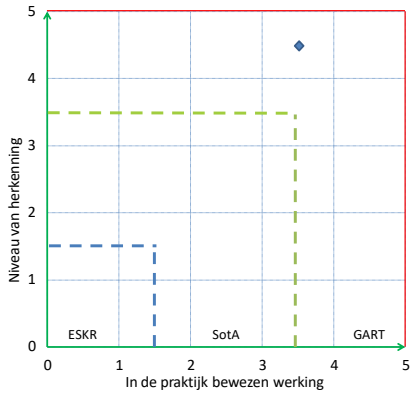
Aangezien een shutdown of eenvoudige herconfiguratie meestal onverenigbaar is met de operationele vereisten, moet rekening worden gehouden met het volgende:

- Scheiding, zonering, inkapseling of applicatie firewalls en
- Netwerkbewaking met een inbraak detectiesysteem (IDS)

om de bescherming te bieden tegen en detectie van exploitatie van bestaande kwetsbaarheden.

Goedkeuringen van fabrikant
Als goedkeuring door de fabrikant vereist is voor de invoer van patches (bijvoorbeeld releases voor patches van database of besturingssystemen), dan kunnen de meeste beschikbare patches, vanwege mogelijk functieverlies en wegvallen van de garantie van de fabrikant, niet worden geïmporteerd. Om deze reden moeten met de fabrikant perioden voor het vrijgeven en leveren van patches en updates of alternatieve tijdelijke oplossingen voor kwetsbaarheden contractueel worden overeengekomen.

Classificatie van het technologieniveau



3.3.6 Beheer van informatiebeveiligingsrisico's

Risicobeheer is een essentieel instrument voor het beheer van bedrijfsrisico's en dus de voorwaarde voor het selecteren van passende risicobeperkende beveiligingsmaatregelen. In

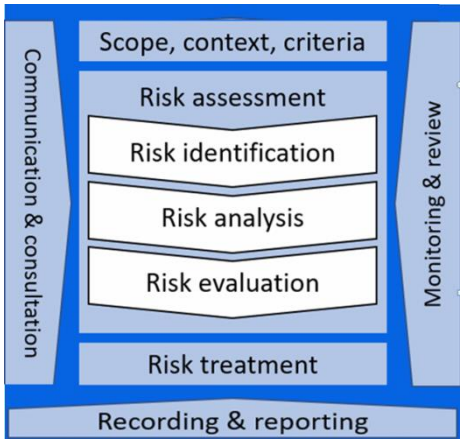
de praktijk wordt het gebruik van beveiligingsmaatregelen bepaald door hun kosten en baten af te wegen. Om de voordelen te bepalen, moeten beveiligingsrisico's worden geïdentificeerd en geëvalueerd. Een goed en gestructureerd informatiebeveiliging risicobeheer (ISRM) creëert de nodige transparantie en stelt het managementniveau in staat om in deze context passende beslissingen te nemen. Bovendien is het beheer van informatiebeveiligingsrisico's[36] een kernelement in de implementatie en herhaalde actualisering van informatiebeveiliging beheersystemen (ISMS) en gegevensbescherming beheersystemen (DSMS).

Standaarden
In het algemeen geldt ISO 31000 als belangrijkste internationale norm voor risicobeheer, terwijl ISO/IEC 27005[37] de norm die specifiek van toepassing is op informatiebeveiligingsrisico's. Het proces van deze laatste is zeer nauw gericht op ISO 31000, maar bevat aanvullende (niet-normatieve) informatie over de identificatie en evaluatie van middelen (assets), voorbeelden van bedreigingen en kwetsbaarheden, en methoden voor risicobeoordeling in het kader van informatiebeveiliging.
In Duitsland is de BSI IT-Grundschutz ook relevant, met name BSI 200-3 (BSI-GS). Voor industriële automatiseringssystemen is ook de standaard IEC 62443 Part 3-2 voor "Security Risk Assessment and System Design" beschikbaar.

Afhankelijk van de regelgeving moeten organisaties mogelijk voldoen aan aanvullende vereisten, zoals de Europese basisverordening gegevensbescherming (GDPR) of de IT-Sicherheitskatalog van het Bundesnetzagentur (IT-SiKat), die beide aanvullende specificaties voor risicobeheer bevatten.

voor afzonderlijke sectoren zijn, met betrekking tot de IT-Sicherheitsgesetz, ook sectorspecifieke veiligheidsnormen, de zogenaamde B3S, gedefinieerd; deze doen aanbevelingen voor de implementatie van risicobeheer voor KRITIS-exploitanten.

Proces
Risicomanagement is een cyclisch proces (volgens PDCA = Plan, Do, Check, Act). Aangezien omstandigheden zoals de dreigingsituatie, kwetsbaarheden in het systeem en technologische omgeving veranderingen, moet de risicobeoordeling up-to-date worden gehouden en de doeltreffendheid ervan worden gecontroleerd. Afbeelding 8: toont het risicoproces volgens ISO 31000.



Afbeelding 7: Risicoproces conform ISO 31000

In de eerste stap (het vaststellen van de context) worden de basisvoorwaarden voor het ISRM gemaakt. Allereerst wordt bepaald op welke delen van de organisatie het ISRM van toepassing is; als het ISRM wordt ingevoerd als onderdeel van een ISMS, wordt dit over het

36 Met IT-risico's en IT-beveiliging verwijst deze tekst naar risico's en beveiliging voor alle soorten informatie, dus niet alleen de elektronisch verwerkte gegevens.
37 De SO/IEC 27005-norm wordt momenteel herzien.

algemeen bepaald door de reikwijdte van het ISMS. De bedrijfsprocessen die in het ISRM moeten worden opgenomen, moeten worden geselecteerd. Op basis van de bedrijfsprocessen worden de bijbehorende organisatie-eenheden, IT- en OT-systemen en -applicaties, data- en spraakcommunicatiefaciliteiten, dienstverleners en ook vastgoed of gebouwen in overweging genomen. Er wordt een ISRM -organisatie opgezet met bijbehorende taaktoewijzing (zoals onder voorzitterschap van een risicomanager), tenzij dit al is gebeurd binnen een ISMS of DSMS. Het is ook raadzaam om, indien beschikbaar, tussen het ISRM en centraal bedrijfsrisicobeheer interfaces te definiëren.

Gevaren worden bepaald tijdens de **risico-identificatie**. Gevaren werken tegen waarden (assets). In een ISRM-systeem zijn deze waarden voornamelijk informatie, en ten tweede systemen en componenten voor de verwerking en bescherming ervan. Tijdens de risico-identificatie worden de risico's tegen de waarden afgezet. Volgens de definitie in de woordenlijst van de BSI: "Bedreigingen zijn de interactie van bedreigingen (zoals. natuurrampen, pandemieën, inbraak, hackers, interne overtreders) en zwakke punten (zoals. softwarefouten, organisatorische tekortkomingen en technische gebreken)". De uitdaging is om zoveel mogelijk van deze gevaren te identificeren." Gestandaardiseerde dreigingencatalogi zoals die in ISO/IEC 27005 Bijlage D of dreigingenoverzicht van het BSI Grundschutz kompendium bieden hierbij ondersteuning. Deze catalogi moeten echter worden aangepast aan de geselecteerde context en de bestaande waarden. Daarbij is de interactie van informatiebeveiligingsmanagers en technische deskundigen, bijvoorbeeld in een werkgroep, belangrijk.

Risicoanalyse houdt in dat het gevaar wordt beoordeeld in termen van de waarschijnlijkheid van het optreden en de kans op schade. Zoals hierboven vermeld, is het zelden mogelijk om terug te vallen op solide cijfers voor IT-risico's. Ook hier is, indien mogelijk, de beoordeling van technische deskundigen uit verschillende disciplines, doorslaggevend. Schade kan van verschillende aard zijn (zoals financiële schade, gevaar voor leven en ledematen, aantasting van het aanbod of fabricage/ 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 normaliter niet worden uitgedrukt als een concreet getal (kardinaal), maar eerder binnen een generieke schaal, bijvoorbeeld Hoog, Midden, Laag. ISO/IEC 27005 Bijlage E biedt nuttige richtlijnen voor dit soort classificaties. Een op deze manier ingedeeld gevaar wordt risico genoemd.

Risico's moeten worden **beoordeeld** (assessed)en op **passende wijze** worden **aangepakt**, waarvoor verschillende opties mogelijk zijn. Men kan ze bijvoorbeeld bewust dragen (accepteren), zich tegen hen verzekeren of tegenmaatregelen nemen (ISO 31000 Hoofdstuk 6.4.4), maar men moet ze niet negeren. Op deze manier wordt een bewuste beslissing genomen. Deze beslissing moet worden genomen door een persoon die verantwoordelijkheid neemt, ongeacht de kosten van de maatregelen of van de schade wanneer zich een risico voordoet. Deze persoon wordt veelal aangeduid als risico-eigenaar[38]. Om het risico te reduceren, worden door de deskundigen tegenmaatregelen voorgesteld, waarvan de kosten en de risicoreductie de basis vormen om te beslissen of de maatregelen al dan niet worden uitgevoerd. De risico-eigenaar neemt vervolgens de beslissing over de uitvoering ervan en het aanvaarden van het risico dat overblijft na de uitvoering van de maatregelen; het restrisico. Vanwege wettelijke vereisten voor KRITIS -exploitanten of in het kader van de GDPR is de risico-eigenaar niet geheel vrij om risico's te accepteren of over te dragen zonder verdere behandeling.

Communicatie, rapportage (met name richting management) en **monitoring** zijn ondersteunende processen. Binnen een ISMS of DSMS worden ze hoe dan ook toegepast en moeten vergelijkbaar ze op het ISRM worden toegepast. Bij een centraal (gecentraliseerd) risicomanagementsysteem is, zijn efficiënte communicatie en wederzijdse

38 De term "risico-eigenaar" van ISO 27001 wordt afhankelijk van de verantwoordelijkheden van de persoon ook vertaald als "risicoverantwoordelijke" of "risiconemer".

complementariteit tussen dat systeem en het ISRM belangrijk, en dat voor het centrale bedrijfsrisicobeheersysteem criteria worden vastgesteld voor de escalatie van informatiebeveiligingsrisico's, welke aan beide kanten begrijpelijk en aanvaardbaar zijn.

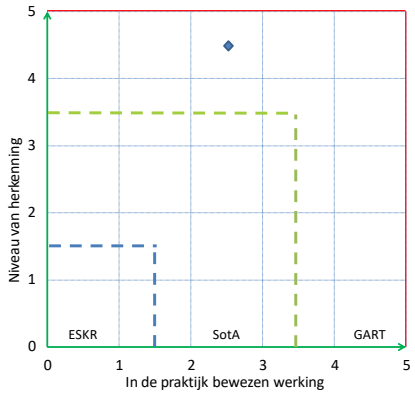
Praktische Tips

Het inrichten van een volledig nieuw ISRM is voor organisaties vaak een uitgebreide taak (in termen van tijd en kosten). Net als andere processen is ISRM onderworpen aan een continu verbeteringsproces, wat betekent dat u bij de eerste poging geen perfect proces kan verwachten. Integendeel, een te zwaarwichtige aanpak kan voor een later tijdstip een belasting vormen. Het gevaar bestaat dat het proces dan zal op de lange termijn "in slaap valt" of zal alleen worden uitgevoerd als een formeel noodzakelijk relikwie zonder enig waarneembaar 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 de risico's met hoge prioriteit worden geïdentificeerd, geanalyseerd en op passende wijze worden aangepakt, en dat hier de grootst mogelijke consensus over is tussen de beslissende partijen.

De identificatie en juiste categorisering van bedreigingen vormen een bijzondere uitdaging bij de start. Hiervoor kunnen standaard dreigingcatalogi zoals die in ISO/IEC 27005 worden gebruikt. Niettemin is er zelden een duidelijk antwoord op de vraag of de dreiging van blikseminslag moet worden aangemerkt als overmacht (force majeure) en bijvoorbeeld moet worden behandeld als een groot algemeen risico, 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 enige onnauwkeurigheid geaccepteerd moet worden. Het inschatten van de waarschijnlijkheid van het voorkomen veroorzaakt hoe dan ook enige onnauwkeurigheid. Op dit punt is het belangrijk om de doelstelling niet uit het oog te verliezen, namelijk dat de resultaten van de risicoanalyse kunnen worden gebruikt om een begrijpelijke beslissing te nemen over de vraag of al dan niet een actie moet worden ondernomen.

Nauwelijks minder moeilijk is dewaarschijnlijkheid van voorkomen in te schatten. Het is raadzaam om zoveel mogelijk externe en interne informatiebronnen te gebruiken. De eerste omvatten CVE[39]-lijsten, leveranciersinformatie, CERT-diensten (bijvoorbeeld van het BSI), en de laatste omvatten de evaluatie van informatiebeveiligingsincidenten, penetratietests, audits en bewustmakingsmaatregelen. De waarden moeten regelmatig, bijvoorbeeld ten minste eenmaal per jaar, worden aangepast aan de huidige situatie.

Classificatie van het technologieniveau



3.3.7 Persoonlijke certificatie

De organisatorische maatregelen omvatten onder meer de inzet van gekwalificeerd gespecialiseerd personeel. Dit geldt met name voor bedrijfskritische omgevingen en kritieke

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

infrastructuren (KRITIS). Alleen op deze wijze is het mogelijk om bedrijfsmiddelen te beschermen en te voldoen aan de vele in wetten verankerde eisen met betrekking tot het bewijs van de kwaliteit van het ingezette personeel.

Vanwege de toenemende verscheidenheid aan technische oplossingen is het noodzakelijk dat alle medewerkers die in de IT-sector werkzaam zijn, voortdurend worden opgeleid in de basis en innovaties. De werknemers moeten in overeenstemming met de desbetreffende activiteiten en de daaruit afgeleide eisen worden opgeleid en gecertificeerd, zowel met betrekking tot de rol waaraan moet worden voldaan (zoals beheerder, ontwikkelaar, IT-architect, auditor, informatiebeveiligingsfunctionaris, functionaris voor gegevensbescherming) als met betrekking tot branchespecifieke (zoals telecommunicatie, vervoer) en oplossingsspecifieke (zoals On-Prem, cloud) functies.

Met persoonlijke certificering wordt de beroepskwalificatie aangetoond. Dit komt omdat een persoonlijk certificaat meestal pas wordt afgegeven nadat een professionele opleiding en een met succes geslaagd examen op basis hiervan is afgerond. Afhankelijk van doel en toepassingsgebied zijn er verschillende certificeringprogramma's op de markt. Hieronder enkele voorbeelden:

- Beheerders
  - Er bestaan verschillende fabrikantafhankelijke certificeringprogramma's die gericht zijn op het gebruik, de configuratie en het beheer van het betreffende product. Deze omvatten met name certificaten van Microsoft, Linux, Oracle, Cisco, IBM, maar ook certificeringprogramma's van cloudservice providers zoals Microsoft, AWS en Google.
- Softwareontwikkelaars
  - TeleTrusT Professional for Secure Software Engineering (TPSSE) van TeleTrusT.
    De focus van de TPSSE-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 leveranciersneutrale certificering die de expertise van een individu voor het implementeren van beveiliging binnen een levenscyclus van softwareontwikkeling aantoont.
    (https://www.isc2.org/Certifications/CSSLP)
- IT-architecten
  - Certified Professional for Software Architecture (CPSA) van iSAQB
    De International Software Architecture Qualification Board (iSAQB) is een vereniging van software architectuur experts vanuit industrie, consulting en training bedrijven, academia en andere organisaties.
    (https://www.isaqb.org/certifications/)
- IT-security auditors
  - Certified Information Systems Auditor (CISA) van ISACA
    CISA is een wereldwijd erkende certificering op het gebied van audit, control en beveiliging van informatiesystemen.
    (https://www.isaca.de/de/zert-start/international/cisa)
  - ISO/IEC 27001 lead auditor
    De focus ligt op het voorbereiden en uitvoeren van een audit van het Information Security Management System (ISMS). De certificering wordt aangeboden door verschillende aanbieders.
  - BSI IT-Grundschutz-Auditor
    Certificering voor het uitvoeren van audits in overeenstemming met de BSI-normen en het BSI "IT-Grundschutz" compendium.
- IT-beveiligingsexperts
  - TeleTrusT Information Security Professional (TISP) van TeleTrusT
    De inhoud die voor het TISP certificaat wordt behandeld, bevat 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) van ISC²
  Om het certificaat te verkrijgen, moet expertise op het gebied van veiligheidsrelevante aspecten uit verschillende gebieden van het zogeheten Common Body of Knowledge (CBK) worden aangetoond.
  (https://www.isc2.org/Certifications/CISSP)
- Comptia Security+ van 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) van ISACA
  De focus ligt op de planning, implementatie en beheersing en monitoring van IT security concepten voor specialisten en managers.
  (https://www.isaca.de/de/zert-start/international/cism1)

- Data Protection Officer / Data Protection Coördinator / Data Protection Advisor
  Tot op heden is er op het gebied van gegevensbescherming geen certificering volgens een erkende onafhankelijke certificeringprocedure door een onafhankelijke certificerende instantie en in overeenstemming met ISO/IEC 17024 voor een van de consulting, designing en controlling beroepen. Adequate expertise op het gebied van gegevensbescherming is afhankelijk van een veelheid aan factoren en kan niet worden doorgeven door een enkelvoudige cursus[40]. Een uitgebreider opleiding op het gebied van gegevensbescherming wordt aanbevolen. Bijvoorbeeld:
  - Certified Information Privacy Professional (CIPP)
    IAPP-training richt zich op wetten, beleidsregels en normen voor gegevensbescherming in grote internationale rechtsgebieden, de vaardigheden die nodig zijn om gegevensbeschermingsoperaties te beheren en de voorbereiding van het certificeringexamen.
    (https://iapp.org/train/)
- Industriespecifieke certificaten
  - Telecommunicatie
    - Zero-Outage
      De inhoud van de Zero-Outage-certificeringen omvat best practices en standaarden voor het leveren van veilige, betrouwbare en zeer 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 operationele ICT in spoorwegactiviteiten certificeringen hebben betrekking op de beste praktijken, standaarden en normen die moeten worden overwogen in IT-projecten en IT-toepassingen in spoorwegactiviteiten.
      (http://www.hmocs.de/)
    - RCS Academy (SBB)
      De inhoud van de RCS Academy-certificeringen heeft betrekking op de beste praktijken, standaarden en normen die in IT-projecten en IT-toepassingen op het gebied van spoorwegverrichtingen moeten worden overwogen, met name in Zwitserland.

Op de Duitse markt heeft het Duitse Federale Bureau voor Informatiebeveiliging (BSI) ook een trainingsreeks gestart voor experts die zich richten op het BSI "IT Grundschutz"

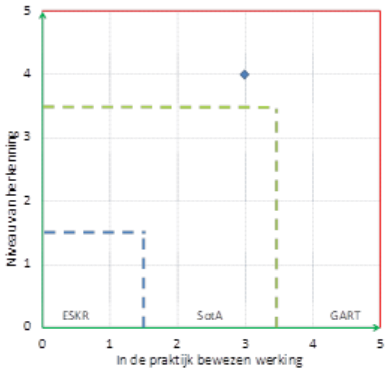
---

40 BvD, professioneel profiel van functionaris voor gegevensbescherming: https://www.bvdnet.de/wp-content/uploads/2018/04/BvDBerufsbild_Auflage-4_dt_en.pdf

compendium. Naast de hierboven genoemde auditors zijn dit de practitioners en adviseurs voor de BSI IT-Grundschutz[41].

Andere Europese landen hebben hun eigen, nog niet aan uniforme regelgeving onderworpen, individuele certificeringprogramma's. De European Cyber Security Organisation (ECSO) heeft een overzicht van de certificeringprogramma's van de Europese landen samengesteld[42].

Classificatie van het technologieniveau



3.3.8 Omgaan met aanbieders

Het uitbesteden van diensten kan voordelig zijn als dienstverleners, bij het leveren van de in opdracht genomen dienst, meer gefocust, innovatiever en beter of goedkoper zijn dan de klant of als zij een speciale technologie in gebruik hebben.

Gebruik maken van dienstverleners gaat echter soms gepaard met niet-onaanzienlijke risico's (zoals afhankelijkheid, verlies van controle en stuuropties, risico's voor de informatiebeveiliging). In het ergste geval kunnen deze risico's het bestaan van de klant in gevaar brengen. Hoe vertrouwelijker, kwetsbaarder of vertrouwelijker de gegevens (zoals geheimhouding, gegevensbescherming), hoe groter het risico. Tegen deze achtergrond staan selectie, controle, monitoring en beoordeling van dienstverleners als organisatorische maatregel centraal.

Het uitbesteden van diensten (zoals netwerkbeheer) gaat gepaard met verschillende bedreigingen voor de IT-beveiliging (met inbegrip van de ook informatiebeveiliging), zoals:

- Inbreuk op de beveiliging met als gevolg vernietiging, verlies, wijziging of ongeoorloofde openbaarmaking van of toegang tot gegevens.
- Niet-contractuele of ongepaste behandeling door derden van de, voor het uitvoeren van de overeenkomst, verstrekte gegevens.
- Misbruik van toegangsrechten verkregen door de dienstverlener, met als gevolg diefstal, verlies of ongeoorloofde openbaarmaking van de verstrekte gegevens
- Menselijk en organisatorisch falen of wangedrag als gevolg van de niet-naleving van overeengekomen technische en organisatorische maatregelen
- Juridische risico's (zoals schade als gevolg van handelingen of nalatigheden van dienstverleners, boetes of opsluiting, officiële bevelen)

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

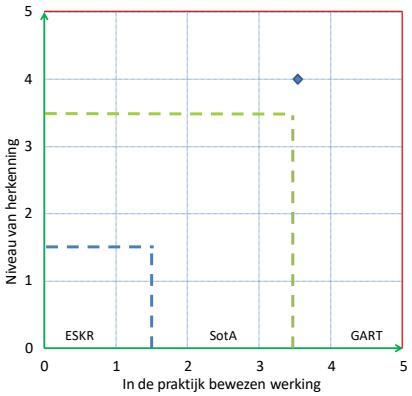
1. Maatregelen voor de selectie van dienstverleners:
    - Het ontwerpen of aanpassen van het aankoopproces, met als doel zich te concentreren op gegevensbescherming en informatiebeveiliging, bijvoorbeeld door relevante instanties in een vroeg stadium bij het selectieproces te betrekken en op

41 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/ITGrundschutzBerater/itgrundschutzberater.html;jsessionid=3DE1AE0E2759C0AA3373341257ECAC85.1_cid500

42 https://www.ecs-org.eu/documents/publications/5fad54a94cfac.pdf

basis van individuele of algemeen erkende normen (zoals Trusted Computer System Evaluation Criteria (TCSEC)), minimumnormen (basisnormen) vast te stellen.
    - Het in een gestructureerde vorm uitvoeren van verzoeken om informatie (RFI) met vragen over informatiebeveiliging en gegevensbescherming met een verzoek om een bindende verklaring van de dienstverlener
    - Het, bij verschillende dienstverleners, aanvragen van een voorstel (RFP), op basis van een gedetailleerde beschrijving van diensten of specificaties, evenals de individuele eisen aan gegevensbescherming en informatiebeveiliging.
    - Due diligence, d.w.z. zorgvuldig onderzoek, inclusief een beoordeling van alle relevante juridische risico's in verband met een juridische transactie.
2. Maatregelen voor de controle en het toezicht op dienstverleners:
    - In ieder geval wordt, voor het toezicht op de dienstverleners, een interne definitie en delegatie van verantwoordelijkheden aanbevolen.
    - De aard en reikwijdte van de maatregelen zijn afhankelijk van verschillende factoren, zoals de grootte van het bedrijf, de complexiteit van de dienstenniveau overeenkomst (SLA) en de organisatiestructuur en al bestaande processen in het bedrijf.
    - Criteria opstellen en toepassen om de capaciteit van dienstverleners, overeenkomstig de vastgestelde en contractueel overeengekomen vereisten (overeenkomstig de bepaling in onderafdeling 8.4 van ISO 9001), continu te controleren.
    - Idealiter worden de maatregelen geïntegreerd in een IT-risicobeheer dat is ingebed in de bestaande bedrijfsprocessen (zoals IT-beveiligingsbeheer, compliance beheer, gegevensbeschermingsbeheer).
3. Maatregelen ter controle van dienstverleners:
    - Risicobeheer van dienstverleners voor het prioriteren van taken, het bepalen van controle-intervallen, het bepalen van de aard en reikwijdte van de controlemaatregelen (zoals. controlemaatregelen op locatie en het gebruik van vragenlijsten of commerciële databanken voor het risicobeheer van de dienstverlener) enz.
    - Audits van dienstverleners/leveranciers (IT-beveiligingsaudits, gegevensbeschermingsaudits, fysieke beveiligingsaudits) tijdens het uitvoeren van het contract
    - Beheer van contracten, certificaten en andere documentatie

Classificatie van het technologieniveau



Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Bundesverband IT-Sicherheit e.V. (TeleTrusT) is een kennisnetwerk dat bestaat uit nationale en buitenlandse leden uit industrie, administratie, consultancy en wetenschap en thematisch gerelateerde thematisch verwante partnerorganisaties. TeleTrusT belichaamt met haar brede scale aan leden en partnerorganisaties TeleTrusT het grootste competentienetwerk voor IT-beveiliging in Duitsland en Europa. TeleTrusT biedt interdisciplinaire forums voor IT-beveiligingsexperts, organiseert evenementen en faciliteert de uitwisseling van IT-beveiliging gerelateerde informatie tussen leveranciers, gebruikers, onderzoekers en autoriteiten. TeleTrusT biedt forums voor experts, organiseert evenementen en conferenties discussies over technische, politieke en juridische kwesties met betrekking tot IT-beveiliging. TeleTrusT is drager van de European Bridge CA (EBCA, PKI Network of Trust), de IT-expert certificatiecertificaten "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 hoofdkwartier van de vereniging bevindt zich in Berlijn.

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.