Bijlage CSR 1 Omgaan met vertrouwelijke informatie en documenten

CSR 1.1 Doelstelling

Alle medewerkers moeten op de juiste wijze omgaan met vertrouwelijke informatie (documenten en gegevens). Dit is van groot belang voor de beveiliging van de ICT infrastructuur en de primaire processen tegen cybercriminaliteit. Beveiliging van de informatievoorziening en bedienketens in het primaire proces is afhankelijk van de beveiliging van de documentatie van de ICT-infrastructuur. De vertrouwelijkheid van informatie wordt uitgedrukt in een classificatie. De classificatie geeft de aard van de documentatie weer en helpt de gebruiker bij het bepalen hoe een document verwerkt dient te worden.

Organisaties gebruiken hun eigen rubricering, of houden ten minste de volgende rubricering of informatieclassificatie aan:

a. Departementaal Vertrouwelijk;
b. Bedrijfsvertrouwelijk;
c. Bedrijfsinformatie.

Departementaal Vertrouwelijk

Deze informatie dient strikt vertrouwelijk te worden behandeld en mag uitsluitend op basis van need-to-know worden verstrekt. Informatie met deze classificatie mag niet worden uitgewisseld met externen en valt buiten de scope van dit document.

Bedrijfsvertrouwelijk

Deze informatie is uitsluitend toegankelijk voor diegenen die de informatie nodig hebben om hun werkzaamheden uit te kunnen voeren en wordt op basis van need-to-know verstrekt.

Bedrijfsinformatie

Deze informatie is voor iedereen vrij toegankelijk.

CSR 1.2 Best practice

CSR 1.2.1 Uitwisselen van informatie

In de overeenkomst met externen zijn eisen opgenomen voor geheimhouding en het vertrouwelijk omgaan met documenten.

Voorbeelden van bedrijfsvertrouwelijke informatie (gerelateerd aan cybersecurity) zijn:

a. Ontwerpdocumenten, constructietekeningen en -berekeningen;
b. Bediening en beheer handleidingen, veiligheidsinstructies en documentatie;
c. Configuratiedocumentatie van ICT en ICS/SCADA-systemen;
d. Datanetwerkschema's en IP adressen;
e. Informatie over de ligging van kabels en leidingen;
f. Informatie over accounts en wachtwoorden.

Uitwisseling van informatie kan op meerdere manieren plaatsvinden. Voor elke wijze van uitwisseling zijn specifieke voorwaarden en regels van kracht:

Informatie uitwisseling via email

a. Informatie met de classificatie Bedrijfsvertrouwelijk mag onversleuteld via email worden uitgewisseld met externen.
b. Informatie met de classificatie TLP AMBER mag onversleuteld via email worden uitgewisseld met BAW partners.

Informatie uitwisseling via bestand-uitwisselingsservices

a. Informatie met de classificatie Bedrijfsvertrouwelijk via een bestandenuitwisselservice (b.v. Wetransfer) mag uitsluitend versleuteld worden uitgewisseld met externen, waarbij bestanden worden versleutel met AES 256 encryptie. Het gekozen wachtwoord is uniek voor elke bestandsuitwisseling en dient te voldoen aan de wachtwoordrichtlijn en via een ander communicatiekanaal (b.v. via SMS) aan de ontvangende partij te worden verzonden.
b. Informatie met de classificatie TLP AMBER via Wetransfer (of vergelijkbare service) mag uitsluitend versleuteld worden uitgewisseld met BAW partners, waarbij bestanden worden versleutel met AES 256 encryptie. Het gekozen wachtwoord is uniek voor elke bestandsuitwisseling en dient te voldoen aan de wachtwoordrichtlijn en via een ander communicatiekanaal (b.v. via SMS) aan de ontvangende partij te worden verzonden.

Informatie uitwisseling via eigen of externe servers

Informatie met de classificatie Bedrijfsvertrouwelijk of TLP AMBER mag onversleuteld via eigen of externe servers worden uitgewisseld, mits er een voldoende authenticatie van de gebruiker en zijn bevoegdheden plaatsvindt.

CSR 1.2.2 Versleutelen van gegevens

Wanneer versleuteling van informatie nodig is, dient dit te gebeuren met een versleutelingsprogramma dat ten minste AES 256 encryptie ondersteunt en een sterk wachtwoord dat voldoet aan de vereisten voor wachtwoorden. Een voorbeeld van zo een programma is 7-Zip, een eenvoudig te gebruiken computerprogramma, waarmee bestanden versleuteld ingepakt kunnen worden.

7-Zip is gratis voor (thuis)gebruik (zie www.7-zip.org). Bij gebruik van AES-256 versleuteling en sterke wachtwoorden (zie hiervoor de wachtwoordrichtlijn) biedt 7-Zip een veilige manier voor gegevensversleuteling.

Documenten versleutelen met 7-Zip

a. Start 7-Zip via de Start toets links onderin Windows.
b. Ga naar de folder waar de te versleutelen bestanden staan.
c. Selecteer de bestanden en klik op de Add button (het groene + symbool).
d. Selecteer:
    i. Archive format: zip
    ii. Encryption method: AES-256
e. Kies een wachtwoord dat voldoet aan de wachtwoordrichtlijn en voer dit in.
f. Klik op de OK button en sluit 7-Zip af.
g. Het versleutelde bestand is klaar om te versturen.

Documenten ontsleutelen met 7-Zip

a. Open het bestand in 7-zip.
b. Selecteer de Extract button (het blauwe – symbool).
c. Selecteer de folder waar het bestand uitgepakt dient te worden.
d. Voer het wachtwoord in en klik de OK button.

CSR 1.2.2.1 Overdracht en vernietiging van vertrouwelijke data bij einde contract

Bij het aflopen en beëindiging van een contract met een externe partij, draagt externe partij alle objectinformatie -met de classificatie Bedrijfsvertrouwelijk- over aan opdrachtgever.

Daarna vernietigt/verwijdert de externe partij de Bedrijfsvertrouwelijke informatie van opdrachtgever van de eigen systemen.

Bijlage CSR 2 Personele toegang

CSR 2.1 Doelstelling

Het van belang inzicht te hebben in wie fysieke toegang heeft tot de IA systemen binnen de objecten. Van onderhoudspersoneel dient te worden vastgesteld dat verwacht kan worden dat zij op juiste wijze zullen omgaan met informatie waartoe men toegang heeft.

CSR 2.2 Best practice

Best practices voor personele toegang zijn als volgt (indachtig naleving van AVG regels):

a. Voorafgaand aan de operationele inzet dient al het vast onderhoudspersoneel:
    i. een persoonlijke geheimhoudingsverklaring te hebben ondertekend;
    ii. zich daarbij te kunnen legitimeren met een officieel geldig legitimatiemiddel met een goed gelijkende pasfoto;
    iii. een Verklaring Omtrent Gedrag (VOG) in bezit te hebben welke is gerelateerd aan de beoogde Werkzaamheden;
b. Hangende de aanvraag voor een VOG kan volstaan worden met een eigen verklaring van de betreffende medewerker gedurende een periode van maximaal zes weken welke niet verlengd kan worden.

Er dient op toe gezien dat al het onderhoudspersoneel dat niet structureel verschijnt:

a. Zich legitimeert;
b. In specifieke gevallen op eerste verzoek van de objecteigenaar bereid is een eigen verklaring en een geheimhoudingsovereenkomst te ondertekenen.

Alle medewerkers worden nadrukkelijk geïnformeerd over het feit dat het doorgeven van informatie over de werking, inrichting, organisatie rondom de objecten in welke vorm dan ook NIET zal geschieden dan na uitdrukkelijke toestemming van de objecteigenaar.

Iedere geconstateerde afwijking van bovenstaande eisen dient te worden behandeld als security incident.

Bijlage CSR 4 Het veilig koppelen van beheer- en onderhoudsapparatuur aan ICT- en IA-systemen

CSR 4.1 Doelstelling

Tijdens het verrichten van beheer- onderhoudswerkzaamheden wordt door medewerkers van de Objectbeheerder soms tijdelijk apparatuur (bijvoorbeeld draagbare media, waaronder USB-sticks, externe disks, laptop, tablet, CD's, DVD's, enz.)gekoppeld aan de ICT- en IA-omgeving (PLC's, servers, routers, switches, enz.) van de Objecteigenaar. Hierdoor ontstaan cybersecurity risico's zoals b.v. malwarebesmetting of binnendringing van het netwerk. De Objectbeheerder dient deze risico's te mitigeren.

CSR 4.2 Best practice

CSR 4.2.1 Soorten apparatuur

Met betrekking tot het koppelen van apparatuur wordt er onderscheid gemaakt tussen een tweetal soorten apparaten:

a. Actieve apparaten;
b. Passieve apparaten.

Actieve apparaten

Onder actieve apparaten wordt verstaan apparaten die zelfstandig kunnen opereren en over een Operating System beschikken, zoals b.v. een laptop of tablet.

Passieve apparaten

Onder passieve apparaten wordt verstaan apparaten die een actief apparaat nodig hebben voor informatie-uitwisseling. Dit zijn gegevensdragers en opslagmedia, zoals b.v. USB-sticks, externe disks, DVD's, CD-ROM's.

CSR 4.2.2 Instructies voor gebruik van actieve apparaten

Initieel

a. Zorg dat het apparaat gehardend is;
b. Versleutel de harde schijf van het apparaat;
c. Beveilig de toegang tot het apparaat met een sterk wachtwoord;
d. Installeer een malwarescanner;
e. Zet de interne firewall aan op het apparaat.

Vóór en tijdens elk gebruik

a. Gebruik het apparaat uitsluitend voor beheer en onderhoud van IA systemen van Objecteigenaar;
b. Alvorens verbinding te maken met het IA netwerk op de objecten, controleer of de laatste updates en patches zijn geïnstalleerd op de aan te sluiten randapparatuur en installeer deze indien nodig;
c. Alvorens verbinding te maken met het IA netwerk op de objecten, installeer de laatste updates van de malwarescanner op aan te sluiten apparaat en scan deze;
d. Alvorens verbinding te maken met het IA netwerk op de objecten, download op de randapparatuur de benodigde te installeren updates en patches voor de betreffende ICT en IA systemen;
e. Alvorens verbinding te maken met het IA netwerk op de objecten, download ICT of IA-software (updates en patches) uitsluitend vanaf een betrouwbare bron en via een beveiligde verbinding;
f. Alvorens verbinding te maken met het IA netwerk op de objecten, controleer de integriteit van downloads van ICT en IA software met de meegeleverde hashcode;
g. Alvorens verbinding te maken met het IA netwerk op de objecten, controleer de downloads op malware voordat deze worden geïnstalleerd binnen de ICT of IA omgeving;

h. Alvorens verbinding te maken met het IA netwerk op de objecten, zet 3G, 4G, 5G, WiFi, Bluetooth uit (koppelingen tussen IA en andere netwerken zijn niet toegestaan) en laat deze gedurende de koppeling met het IA netwerk uit staan;
i. Alvorens verbinding te maken met het IA netwerk op de objecten, dienen mobiele gegevensdragers door Objectbeheerder ter controle gescand te worden op malware.

CSR 4.2.3 Instructies voor gebruik van passieve apparaten

a. Gebruik uitsluitend de voorgeschreven opslagmedia voor de koppeling met ICT- of IA-systemen;
b. Zorg dat alle gegevens op USB-sticks en externe harde schijven versleuteld zijn, volgens de richtlijn voor het omgaan met vertrouwelijke gegevens;
c. Scan gegevensdragers zoals b.v. USB-sticks, externe harde schijven, CD-ROM's, DVD's en diskettes elke keer vóór gebruik binnen de ICT- of IA-omgeving op malware;
d. Vervang een gegevensdrager waarop malware is ontdekt door een nieuwe gegevensdrager;
e. Alvorens verbinding te maken met het IA netwerk op de objecten, dienen gegevensdragers door Objectbeheerder ter controle gescand te worden op malware.

CSR 4.2.4 Smartphones en Tablets

Voor beheer en onderhoudswerkzaamheden mogen smartphones en tablets uitsluitend na een risicoanalyse en -afweging worden ingezet.

Bijlage CSR 7 Wachtwoorden

CSR 7.1 Doelstelling

Wachtwoorden zijn een essentiële authenticatiemethode om personen, assets of processen toegang te geven tot die functionaliteit en gegevens die noodzakelijk zijn voor het uitvoeren van de beoogde functie, alsook om deze te beschermen tegen oneigenlijk gebruik door anderen. In deze richtlijn zijn de minimale best practices opgenomen voor het gebruik, wijzigen en beschermen van wachtwoorden in IA systemen.

Met de steeds verder toenemende rekenkracht van computers is het van belang dat wachtwoorden complex genoeg zijn en blijven, om weerbaar te blijven tegen tools om wachtwoorden te kraken. Het gebruik van sterke wachtwoorden met een voldoende complexiteit maakt het economisch onrendabel en in de praktijk onhaalbaar om wachtwoorden binnen de IA-omgeving van objecten te achterhalen.

Het is van groot belang iedereen in lijn werkt met de minimale vereisten voor wachtwoordcomplexiteit en ervoor zorgt dat de complexiteit van alle gebruikte wachtwoorden met de tijd meegaat. Biometrische authenticatie biedt een alternatief voor wachtwoorden, of kunnen worden toegepast voor 2-factor authenticatie.

CSR 7.2 Best practice

CSR 7.2.1 Vereisten aan wachtwoorden

Aan wachtwoorden voor alle gebruikers (zowel personen als processen en apparaten) worden eisen gesteld m.b.t. lengte, complexiteit, geldigheidsduur en hergebruik:

a. Wachtwoorden hebben een minimale lengte, passend bij het soort account;
b. Wachtwoorden hebben een minimale complexiteit (verplichte karakterset) waaruit het wachtwoord moet bestaan:
    i. Hoofdletters;
    ii. Kleine letters;
    iii. Cijfers;
    iv. Speciale karakters, bijvoorbeeld: “;’:<>,.?!@#$%&*()+=_-^/\;
c. Wachtwoorden hebben een maximale geldigheidsduur;
d. Wachtwoorden kunnen niet worden hergebruikt.

Deze eisen zijn afhankelijk van het soort gebruikersaccount en gebruik. In algemeenheid geldt: hoe meer rechten aan een account zijn toegekend, hoe zwaarder de eisen.

De volgende zaken dienen niet te worden opgenomen in, of onderdeel uit te maken van, wachtwoorden:

a. Namen van familieleden, huisdieren, vrienden, collega’s, stripfiguren, etc.;
b. Computernamen en -termen, commando’s, naam van de software of hardware, naam van het bedrijf dat het heeft geleverd;
c. Woorden verwijzend naar organisatie, object of locatie, bijvoorbeeld: Rijkswaterstaat, Waterschap, Amaliasluis, gemaalDeHeining, Rotterdam;
d. Geboortedata en andere persoonlijke informatie als adres en telefoonnummers;
e. Eén van de voorafgaande woordsoorten, gevolgd door een getal (bijvoorbeeld: geheim01, welkom123, GuustFlater13, etc.).

CSR 7.2.2 Gegevensversleuteling

Voor versleuteling van gegevens t.b.v. gegevensuitwisseling dienen wachtwoorden te voldoen aan:

a. Wachtwoordlengte: minimaal 8 karakters;
b. Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.

CSR 7.2.3 Soorten accounts

Voor de IA-omgeving van objecten worden verschillende accounts onderkend, met elk hun eigen vereisten voor wachtwoordgebruik.

Standaardaccount fabrikant: Standaard accounts en -wachtwoorden die toegepast worden in ICT- en IA-producten van fabrikanten mogen niet worden gebruikt en dienen te zijn uitgeschakeld.

SCADA-Operatoraccount
Een persoonlijk account dat wordt gebruikt voor de bediening van SCADA systemen
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 180 dagen
Wachtwoordlengte: minimaal 20 karakters

Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.

SCADA-applicatiebeheeraccount
Een persoonlijk account dat wordt gebruikt om de applicatie op het SCADA systeem te beheren
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 180 dagen
Wachtwoordlengte: minimaal 20 karakters

Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.

SCADA-Systeemaccount (service/applicatie account)
Een account dat ervoor zorg draagt dat een applicatie zonder menselijke interventie applicatieopdrachten kan uitvoeren onder speciale rechten.
Soort: service
Wachtwoord vervanging: 365 dagen
Wachtwoordlengte: minimaal 20 karakters

Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.

SCADA-Administratoraccount
Een persoonlijk account dat op de systemen volledig beheer heeft d.m.v. administrator rechten.
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 180 dagen
Wachtwoordlengte: minimaal 20 karakters

Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 2 van elk.

Kantoorautomatiseringsaccount (KA-account)
Het persoonlijke gebruikers account waarmee men kan werken op de organisaties Kantoorautomatiseringsomgeving.
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 90 dagen
Wachtwoordlengte: minimaal 8 karakters

Wachtwoord complexiteit: combinatie van hoofdletters, kleine letters, cijfers en leestekens, tenminste 1 van elk.

CSR 7.2.4 Tips voor het omgaan met wachtwoorden

Enkele tips:

a. Gebruik een wachtwoord dat is gebaseerd op een zin, een songtekst of een rijmpje. Zet de eerste letters van ieder woord achterelkaar, en probeer letters door cijfers te vervangen (Bijvoorbeeld: Het rijmpje “Als het regent in mei is april voorbij en leggen alle vogels een ei!” wordt “Ahri5i4velavee!”, waarbij de maanden zijn vervangen door cijfers).

Bijlage CSR 8 Patchmanagement

CSR 8.1 Doelstelling

Vrijwel alle apparatuur aanwezig op een object heeft te maken met software en/of firmware. Om het aantal kwetsbaarheden in deze apparatuur tot een minimum beperkt te houden, is het van belang om de software en firmware up-to-date te houden en regelmatig te patchen.

Goed patchmanagement draagt bij aan het voorkomen van ongeautoriseerde toegang tot systemen. Door bekende kwetsbaarheden tijdig te repareren, kan een kwaadwillende hiervan niet langer misbruik maken.

Deze richtlijn helpt een effectief patch management beleid op te stellen en te volgen, waarbij aandacht is voor de risicobeoordeling van de patch op de functies van het object en daarmee ook de business impact voor het (al dan niet) uitvoeren van patches.

CSR 8.2 Best practice

CSR 8.2.1 Bepalen van uit te rollen patches

Tenminste de volgende zaken behoren te worden opgenomen in de patch management procedures, om te bepalen welke patches relevant zijn voor het object en uitgerold dienen te worden:

a. Inventariseer voor het object welke software en firmware er op elk apparaat draait en neem dit op in het (bij voorkeur centrale) CMDB of asset management systeem;
b. Houd bij welke kwetsbaarheden er zijn en worden ontdekt voor de systemen die in gebruik zijn. Beoordeel de risico's van de kwetsbaarheden voor het object (zie paragraaf CSR 8.2.2);
c. Houd bij welke patches er uitkomen voor alle apparaten en controleer welke relevant zijn. Indien patches een invloed kunnen hebben op de werking van (b.v. SCADA-) software, houdt bij welke patches zijn goedgekeurd door de leverancier/fabrikant en rol alleen goedgekeurde patches uit;
d. Maak een alternatief mitigatievoorstel indien een patch nog niet is goedgekeurd of besloten wordt om een specifieke patch niet te installeren. Bepaal de risico's die overblijven indien wordt gekozen voor de alternatieve migratie;
e. Houd voor beheer en onderhoud een lijst bij met alle te installeren patches en de systemen waarop dit dient te gebeuren.

CSR 8.2.2 Risicobeoordeling

Zolang een kwetsbaarheid niet is verholpen door installatie van een patch of door een andere vorm van mitigatie, is er kans op misbruik van die kwetsbaarheid. Bepaal het risico op misbruik door het beschouwen van kans en impact.

Kans

De kans dat een kwetsbaarheid wordt uitgebuit is afhankelijk van de blootstelling van de kwetsbaarheid en de uitvoerbaarheid van het exploiteren van de kwetsbaarheid.

De kans dat de kwetsbaarheid wordt uitgebuit		Omschrijving kans en daarmee het benutten van de kwetsbaarheid
1	Verwaarloosbaar t > 5 jaar	De kans en daarmee het falen of misbruik van de functie van het object wordt niet binnen 5 jaar verwacht.
2	Klein (3 jaar < t ≤ 5 jaar)	De kans en daarmee het falen of misbruik van de functie van het object wordt tussen 3 jaar en 5 jaar na nu verwacht.
3	Middelmatig (2 jaar < t ≤ 3 jaar)	De kans en daarmee het falen of misbruik van de functie van het object wordt tussen 2 jaar en 3 jaar na nu verwacht.
4	Groot (1 jaar < t ≤ 2 jaar)	De kans en daarmee het falen of misbruik van de functie van het object wordt tussen 1 jaar en 2 jaar na nu verwacht.
5	Zeker (t ≤ 1 jaar)	De kans en daarmee het falen of misbruik van de functie van het object wordt tussen nu en 1 jaar verwacht.

€	Uitstel patch geeft < 50 k Euro aan extra onderhoudskosten	Uitstel patch geeft < 500 k Euro aan extra onderhoudskosten	Uitstel patch geeft < 1000 k Euro aan extra onderhoudskosten.	Uitstel patch geeft > 1000 k Euro aan extra onderhoudskosten
P	Het niet patchen leidt tot een niet compliancy registratie en rapportage en heeft verder geen politieke consequenties.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en is mogelijk aanleiding voor verscherpte controles door toezichthouders.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en is mogelijk aanleiding voor negatieve media berichtgeving die tot kamer vragen kunnen leiden.	Het niet patchen leidt tot een niet compliancy registratie en rapportage en de positie van Dijkgraaf, DG, de Minister of Staatssecretaris staat ter discussie.

Risico

Het uiteindelijke risico wordt gepaald door het combineren van kans en impact in een risicomatrix.

		Impact			
		Verwaarloosbaar (1)	Beperkt (2)	Groot (3)	Ernstig (4)
Kans	Verwaarloosbaar (1)	Acceptabel (1)	Acceptabel (2)	Acceptabel (3)	Acceptabel (4)
	Klein (2)	Acceptabel (2)	Acceptabel (4)	Ongewenst (6)	Ongewenst (8)
	Gemiddeld (3)	Acceptabel (3)	Ongewenst (6)	Ongewenst (9)	Ongewenst (12)
	Groot (4)	Acceptabel (4)	Ongewenst (8)	Ongewenst (12)	Onacceptabel (16)
	Zeker (5)	Ongewenst (5)	Ongewenst (10)	Onacceptabel (15)	Onacceptabel (20)

De risicoscore wordt bepaald door kans- en impactscore met elkaar te vermenigvuldigen. De hoogte van dit getal geeft aan hoe noodzakelijk een beheersmaatregel in de vorm van een patch is. Hierin worden drie niveaus onderscheiden: onacceptabel (rood), ongewenst (oranje) of acceptabel (groen).

1. Onacceptabel — Risicoscore 15 t/m 20:

Er moeten direct beheersmaatregelen worden getroffen om het risico te beheersen. Dat kan door de patch zo snel mogelijk te implementeren of minimaal (tijdelijk) compenserende maatregelen te treffen.

2. Ongewenst — Risicoscore 5 t/m 12:

De patch moet worden doorgevoerd om het risico te beheersen ofwel worden aangetoond waarom dit nu niet haalbaar/noodzakelijk is. Een planning voor het doorvoeren van de patch is vereist naast tijdelijke compenserende maatregelen om zolang het risico te reduceren.

3. Acceptabel — Risicoscore 1 t/m 4:

De patch hoeft niet direct doorgevoerd te worden en kan gewoon worden doorgevoerd binnen het geplande reguliere onderhoudsmoment van de systemen.

CSR 8.2.3 Inplannen van patches

Afhankelijk van de urgentie van de patches, kunnen deze tijdens regulier periodiek onderhoud worden geïnstalleerd. Het is soms noodzakelijk apparatuur opnieuw op te starten na installatie van patches. Tijdens zulke herstarts is het mogelijk dat het object niet kan worden bediend. Inplannen van patches dient dan ook altijd te gebeuren in overleg zodat de operatie niet wordt verstoord.

CSR 8.2.4 Testen van patches

CSR 1.1.1 Om te voorkomen dat de uitrol van patches problemen geeft op het object, dienen patches vooraf te worden getest op werking en integriteit. Bij voorkeur gebeurt dit in een OTA-omgeving.

CSR 8.2.5 Verantwoord uitrollen van ingeplande en geteste patches

Plan voor roll-back bij falende patches

a. Zorg voor een actuele en goed werkende back-up, waarop kan worden teruggevallen indien een patch problemen geeft na installatie;
b. Overweeg een extra back-up te maken vlak voordat patches worden geïnstalleerd;
c. Reserveer bij de geplande onderhoudswerkzaamheden tijd voor een eventuele roll-back van back-up op apparatuur.

Controleer voorafgaand aan de uitrol van een patch de systeem eventlog. (het is belangrijk eventueel aanwezige problemen vooraf te kennen om na de uitrol van een patch te kunnen bepalen welke eventuele problemen door de patch veroorzaakt zijn en welke al bestonden).

Controleren of patches succesvol zijn uitgerold

a. Controleer na de uitrol van de patch of de uitrol is geslaagd en goed is afgerond (controleer de system eventlog op mogelijke fouten);
b. Indien de patch succesvol is uitgerold, controleer de werking van het object niet is aangetast en of alle toepassingen nog functioneren als verwacht.

Controleren of systeem hardening niet is aangetast

a. controleer of de systeem hardening niet is aangetast door het installeren van de patch. Bijvoorbeeld:
    i. Zijn afgesloten poorten niet opengezet;
    ii. Zijn uitgeschakelde of verwijderde programma's en/of DLL's niet opnieuw geïnstalleerd of geactiveerd;
b. Indien de hardening is aangetast, dient het niveau van hardening te worden hersteld.

Bijlage CSR 9 Hardening

CSR 9.1 Doelstelling

Hardening betreft het verwijderen of uitschakelen van overbodige en/of ongebruikte functionaliteit van een apparaat en is van toepassing op software, hardware en netwerk. Hardening zorgt ervoor dat systemen minder kwetsbaar zijn voor malware en minder snel gecompromitteerd kunnen worden. Hardening wordt toegepast op zowel IT als IA componenten.

Er worden drie methoden van hardening toegepast, te weten software hardening, hardware hardening en netwerk hardening:

a. Software hardening is van toepassing op operating systemen (bijvoorbeeld Microsoft Windows, Linux, iOS, Android) en applicaties (bijvoorbeeld HMI of engineering software, configuratietools, maar ook MS Office, Acrobat reader, Active-X controls en Adobe Flash);
b. Hardware hardening is van toepassing op bijvoorbeeld firmware, alsook het uitschakelen van niet gebruikte communicatiepoorten, antennes, en overige niet gebruikte functionaliteit;
c. Netwerk (Process Control Network) hardening is van toepassing op bijvoorbeeld uitschakelen van onveilige en niet gebruikte protocollen, het beperken van netwerkverkeer (firewalls) en segmentatie/zonering van het netwerk.

Maak indien mogelijk gebruik van de aanwezig security opties van de fabrikant/leverancier.

CSR 9.2 Best practices

CSR 9.2.1 Basistips

Enkele basistips voor hardening zijn:

a. Software
   i. Operating System;
      - De operationele OS versie dient altijd te worden ondersteund door de OS leverancier;
      - Gebruik waar mogelijk de nieuwste (mogelijke) versie[4];
      - Installeer de laatste (mogelijke) patches[1];
      - Schakel niet-gebruikte system services uit of verwijder deze[5];
   ii. Virtualization layer;
      - Gebruik de nieuwste (mogelijke) versie[1]; Deze versie dient wel te worden ondersteund door de softwareleverancier;
      - Installeer de laatste (mogelijke) patches[1];
      - Schakel niet-gebruikte functionaliteit uit of verwijder deze;
   iii. Applicaties
      - Verwijder alle niet noodzakelijke applicaties;
      - Installeer de nieuwste versie van applicaties[1]; Deze versie dient wel te worden ondersteund door de softwareleverancier;
      - Installeer de laatste (mogelijke) patches[1];
      - Zorg voor secure coding tijdens ontwikkeling van eigen software[6];
   iv. Firmware
      - Installeer de laatste (mogelijke) firmware[1];
b. Hardware
   v. Schakel niet-gebruikte poorten uit
      - Gebruik portblockers als niet-gebruikte poorten niet kunnen worden uitgeschakeld om abusievelijk gebruik te voorkomen en tamper-evident stickers (void stickers) om manipulatie te detecteren;

[4] Download alleen van gevalideerde vendorlocaties en controleer de integriteit van downloads middels een checksum.
[5] Zie ook Hardeningprofielen zoals hierna behandeld.
[6] Zie SSD document van CIP (Center for Information security and Privacy protection)

- Beperk de gebruiksmogelijkheden van de nog openstaande poorten (bv. USB alleen voor hid (muis/keyboard)); Gebruik tamper-evident stickers (void stickers) om manipulatie te detecteren;

vi. Schakel niet noodzakelijke draadloze toegang uit (bv. WiFi, Bluetooth, IR, NFC, 4G, 5G, LoRa);

vii. Schakel niet gebruikte functionaliteit uit en verwijder deze waar mogelijk (bv. ingebouwde 4G/5G modem, antennes, I/O);

c. Netwerk

viii. Schakel niet-noodzakelijke communicatieprotocollen uit (bv. FTP, SMB, telnet);

ix. Pas netwerksegmentatie toe. Scheidt hierbij essentiële delen voor de besturing van niet essentiële delen;

x. Beperkt netwerkverkeer tussen verschillende netwerkzones middels firewalls.

CSR 9.2.2 Hardening-profielen

Op Internet zijn de nodige hulpmiddelen te vinden ter ondersteuning van het hardening-proces. Hardening (en tooling daarvoor) kan en mag alleen ingezet worden wanneer met zekerheid gesteld kan worden dat de inzet hiervan geen risico vormt voor de continuïteit van werking van het systeem. Het is van belang dit zowel vooraf als achteraf te testen.

Enkele van deze hulpmiddelen zijn:

CIS

De ‘Security Benchmarks’ van CIS heeft op internet standaard hardening-profielen beschikbaar voor de meeste platformen: http://www.cisecurity.org/

CIS Benchmarks: https://www.cisecurity.org/cybersecurity-best-practices/

Microsoft

Microsoft Security Baselines (Security Compliance Toolkit - SCT): https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10

Microsoft Baseline Security Analyzer (MBSA): https://www.microsoft.com/en-us/download/details.aspx?id=19892

Defense Information System Agency (DISA)

Security Technical Implementation Guides (STIGs): https://public.cyber.mil/stigs/downloads/

Bijlage CSR 11 Malware scanning en opschoning middels een USB

CSR 11.1 Doelstelling

Malware besmettingen zijn vandaag de dag niet meer uit te sluiten. Derhalve worden voor de bescherming van ICT en IA systemen tegen malware oplossingen gevraagd. Bij nieuwbouw systemen dient vanaf het ontwerp hier voldoende aandacht en uitwerking aan gegeven te worden. Echter de maatregelen voor de detectie van en preventie tegen malware kunnen bij de ontwerpkeuzes dilemma's opleveren. In die situaties dient contact en afstemming gezocht te worden voor de uiteindelijke keuze. Ook kunnen er bestaande omgevingen zijn waar (nog) geen antimalware voorzieningen op de ICT en IA systemen zijn getroffen maar waar u meer zekerheid wilt verkrijgen over eventuele aanwezigheid van malware.

Het is van belang dat in deze gevallen malware gedetecteerd en opgeschoond kan worden, door medewerkers die beheer- en onderhoudswerkzaamheden uitvoeren aan ICT en IA systemen.

CSR 11.2 Best practice

CSR 11.2.1 Randvoorwaarden

Een risico bij malware scanning en opschoning is dat wanneer er daadwerkelijk een besmetting heeft plaatsgevonden u niet vooraf weet in welke mate (of met welk soort malware) de computers zijn besmet. Het installeren van een conventionele antivirus oplossing brengt een nieuw risico met zich mee, indien de antivirus software een besmet bestand aantreft op de computer zullen de meeste antivirus software oplossingen (bij standaardinstellingen) deze bestanden proberen op te schonen, in quarantaine te plaatsen of te verwijderen. Dit is uiteraard onwenselijk aangezien de besmette bestanden mogelijk vitaal zijn of noodzakelijk voor de juiste werking voor de bediening van het object.

Randvoorwaarde is dat de ingezette oplossing voor malware scanning zo ingesteld wordt dat het alleen detecteert en rapporteert. Er mag niets verwijderd worden.

De volgende paragrafen schetsen een goede manier om het scannen aan te pakken.

CSR 11.2.2 Voorbereiden USB-stick met antimalware software

a. Gebruik **bij voorkeur een nieuwe USB stick** waar de malwarescan software op geïnstalleerd gaat worden;
b. Als extra beveiliging voor de USB-stick met antimalware software dient bij voorkeur een USB stick met **schrijfbeveiliging** (of een SD-kaart met schrijfbeveiliging, in combinatie met een SD-kaart lezer) gebruikt te worden. Door de schrijfbeveiliging te activeren voordat de USB-stick in het besmette systeem geplaatst wordt, wordt besmetting van de USB-stick voorkomen;
c. Scan de USB stick **voor elk gebruik** op een computer buiten het object met een actuele malwarescan software;
d. De USB-stick moet **voor elk gebruik** voorzien worden van de juiste –en meest actuele- **antimalware** software en malwaredefinities.

Een voorbeeld van een dergelijke antimalware software is de vrij verkrijgbare software van ClamAV welke als portable applicatie kan worden geïnstalleerd op een USB stick en kan worden voorzien van updates op een andere computer.

Voor Windows computers kunt u bijvoorbeeld de nieuwste versie van ClamWin downloaden via http://nl.clamwin.com/ (Voor Linux computers is deze via de website http://www.clamav.net/ verkrijgbaar).

Installeer de software via het installatie programma op een USB stick en na dat de software is voorzien van de laatste versie antivirus definities kan de USB stick gebruikt worden op de object computers welke niet zijn aangesloten op internet.

Standaard staat ClamWin zo ingesteld dat een besmetting alleen zal worden gerapporteerd, indien u er zeker van bent dat een eventueel besmet bestand geen cruciale rol heeft voor de werking van het bedieningssysteem kunt u vanuit het programma het virus verwijderen.

Uiteraard kunnen ook andere antimalware programma's worden gebruikt, mits zo ingesteld dat besmettingen uitsluitend worden gerapporteerd en niet in quarantaine worden geplaatst.

Om er zeker van te zijn dat alle bestanden kunnen worden gescand is het noodzakelijk het scanprogramma met verhoogde rechten op te starten. In Windows is dit "Als administrator starten" of "Run as administrator" en in Linux als "Root" of "Sudo".

CSR 11.2.3 Voorbereiden op malwarescanning

Handel volgens onderstaande werkwijze:

a. Update de USB stick met de laatste antimalware software en laatst beschikbare malwaredefinities;
b. Scan de USB stick met antimalware software **voor elk gebruik** op een computer buiten het object met een actuele malwarescan software;
c. Zet op deze USB stick een malwarescan tool/software die **uitsluitend een rapportage** geeft over de besmetting zonder automatische handelingen;
d. Gebruik een malwarescanner welke **geen verbinding met internet** nodig heeft om op te kunnen starten (bijvoorbeeld i.v.m. licentie controle);
e. Gebruik een USB stick waar de antimalware software als een **portable applicatie** op kan worden geïnstalleerd;
f. De rapportage dient verzameld te worden op los media zoals een USB-stick. Gebruik hiervoor bij voorkeur een nieuwe andere stick dan die waarop de malwarescan software staat;
g. Scan de USB stick met antimalware software ook **na elk gebruik** op een computer buiten het object met een actuele malwarescan software.

CSR 11.2.4 Scannen en opschonen

In onderstaand schema wordt een bedoelde werkwijze getoond om een dergelijk object te schonen. Het proces kent de volgende stappen:

Identificeren

Gebruik de offline malwarescan tool om het systeem te controleren op virussen. Zorg voor correcte rapportage op een centrale plaats. Deze rapportage moet op een apart systeem weggeschreven worden, zodat het proces minimaal verstoord wordt.

Rapporteren

Verzamel de rapportage op aparte media zoals een USB-stick. Gebruik hiervoor bij voorkeur een **nieuwe andere stick** dan die waarop de malwarescan software staat.

Houdt ook bij de verzameling van rapportage rekening met voldoende controle op verwisselbare media: Bij plaatsen van een USB-stick in een besmet object is de kans op besmetting van de USB-stick reëel aanwezig. Herhaal hiertoe stap 6 van de instructie voorbereiding malwarescanning.

Maatregelen treffen

Bij constatering van malware dient gekeken te worden naar mogelijke oplossingen voor het opschonen. Na autorisatie kunnen de te nemen stappen gepland en uitgevoerd worden. Houdt bij het treffen van de maatregelen weer rekening met de mogelijke besmetting van verwisselbare media. Extra aandachtspunt in dit geval is ook: Zorg dat de vervangen / vernieuwde bestanden (als daarvan sprake is) bij plaatsing niet besmet worden. Gebruik zo mogelijk checksums op bron en bestemming om de juistheid van de bestanden te controleren.

Controleren

Herhaal ter controle ten minste de eerste stap (Identificeren).

Bijlage CSR 21 Uniform aanleveren van incidentrapportages

Cybersecurityincidenten dienen te worden gerapporteerd. Daarnaast dient maandelijks een overzicht te worden gestuurd van alle incidenten. Een voorbeeld van de rapportagestructuur is te vinden in de hiernavolgende paragrafen. De objecteigenaar kan kiezen een eigen rapportagestructuur te gebruiken voor interne rapportages. Voor rapportage naar een CERT of vergelijkbaar dienen tenminste de in het onderstaand formulier opgenomen informatie te worden verstrekt.

CSR 21.1 Formulier voor rapportage van een cybersecurityincident

Dit formulier dient zo volledig mogelijk te worden ingevuld. Na invulling dit formulier versturen naar de objecteigenaar.

ALGEMENE INFORMATIE	
Datum rapport:	dd-mm-jjjj
Objectnaam en locatie:	
Naam rapporteur:	
Functie rapporteur:	
Organisatie rapporteur:	
Telefoonnummer:	

Rapporteert hiermee het volgende cybersecurityincident:

ALGEMENE INFORMATIE INCIDENT	
Soort incident[7]:	
Incident is opgemerkt op:	[jjjjmmdd/uu:mm]
Incident opgemerkt door:	[indien ander dan rapporteur]
Is het object nog operationeel:	Ja/Nee
Opschaling incident response team nodig:	Ja/Nee

DETAIL INFORMATIE INCIDENT	
Beschrijving van het incident[8]:	
Analyse van het incident:	
Is de dreiging ingesloten:	Ja/Nee
Hoe is de dreiging ingesloten:	
Is de dreiging bestreden:	Ja/Nee
Hoe is de dreiging bestreden:	

[7] Voorbeelden van incidenten zijn: malware, (D)DoS, verlies van controle over proces/bediening, verlies van zicht op proces/bediening, verlies van toegang tot systemen, hack, ongeoorloofd verschaffen van toegang, ongeoorloofde wijziging van configuratie/instellingen/rechten, verwijderen/wijzigen van logfiles.

[8] Een korte, duidelijke beschrijving van het incident, verwijzing naar overige beschikbare documentatie (b.v. logfiles, communicatie met leverancier en interne en externe stakeholders) betreffende het incident.

Is herstel nodig:	Ja/Nee
Welk herstel is nodig:	

CSR 21.2 Formulier voor periodieke rapportage van cybersecurityincidenten

Dit formulier dient aan het begin van elke maand zo volledig mogelijk te worden ingevuld. Na invulling dit formulier versturen naar de objecteigenaar.

Datum rapport:	dd-mm-jjjj
Objectnaam en locatie:	
Rapporteur:	[naam, functie en bedrijf van degene die het rapport opmaakt]
Periode:	[maand waarop deze rapportage betrekking heeft]

De volgende cybersecurityincidenten (inclusief hun afhandeling) hebben plaatsgevonden in de hiervoor genoemde periode:

No	Datum/tijd incident: [jjjjmmdd/uu:mm]	Soort incident[9]:	Afgehandeld (J/N):	Datum/tijd afgehandeld:	Uitleg/opmerkingen m.b.t. incident en afhandeling[10]:
1					
2					
3					
4					
5					

[9] Voorbeelden van incidenten zijn: malware, (D)DoS, verlies van controle over proces/bediening, verlies van zicht op proces/bediening, verlies van toegang tot systemen, hack, ongeoorloofd verschaffen van toegang, ongeoorloofde wijziging van configuratie/instellingen/rechten, verwijderen/wijzigen van logfiles.

[10] Een korte, duidelijke beschrijving van het incident, incident afhandelingsnummer/verwijzing naar overige beschikbare documentatie (b.v. logfiles, communicatie met leverancier en interne en externe stakeholders) betreffende het incident, en hoe het incident is opgelost.

Bijlage CSR 23 Verwijdering en vernietiging van informatie en apparatuur

CSR 23.1 Doelstelling

Indien apparatuur uit de PA/IA-omgeving met opslagmedia wordt verwijderd of hergebruikt, moet er op toegezien worden dat er geen gevoelige gegevens of in licentie gegeven software op de opslagmedia achterblijft. Denk hierbij bijvoorbeeld aan gegevensdragers zoals harde schijven, maar ook aan PLC's of IoT apparatuur. Het is van belang dat alle informatie die aanwezig is op apparatuur op zorgvuldige wijze wordt verwijderd wanneer een apparaat uit de PA/IA-omgeving wordt gehaald en afgevoerd of hergebruikt. Daarnaast dient vertrouwelijke informatie in de PA/IA-omgeving die niet meer nodig is vernietigd te worden.

CSR 23.2 Best Practice

Bij de best practices wordt er onderscheid gemaakt tussen apparatuur die wordt hergebruikt, apparatuur die wordt vernietigd en fysieke documenten. De volgende minimale best practices zijn van toepassing:

CSR 23.2.1 Verwijdering gegevens bij hergebruik apparatuur

Indien apparatuur wordt hergebruikt is het van belang de op het apparaat aanwezige informatie te verwijderen. Hierbij geldt het volgende:

a. Vertrouwelijke informatie wordt tenminste 3 maal volledig overschreven met verschillende bitpatronen, waaronder 2 vaste patronen en één random patroon;
b. Niet vertrouwelijke informatie wordt tenminste 1 maal volledig overschreven met een random bitpatroon;
c. Er wordt gecontroleerd of de gegevens zijn verwijderd;
d. Indien volledig overschrijven van de informatie niet mogelijk is, dient de gegevensdrager te worden vernietigd.

CSR 23.2.2 Verwijdering gegevens bij vernietiging apparatuur of digitale media

Indien apparatuur niet wordt hergebruikt is het van belang de op het apparaat aanwezige informatie te verwijderen. Hierbij geldt het volgende:

a. De informatie wordt middels een degausser verwijderd door een hiertoe gecertificeerd bedrijf, of;
b. Het apparaat wordt versnipperd door een hiertoe gecertificeerd bedrijf.

CSR 23.2.3 Verwijdering van fysieke informatie (documenten)

Verwijdering van fysieke documenten met daarop vertrouwelijke informatie vindt plaats op een veilige manier, bijvoorbeeld door verbranding of versnippering. Bij versnippering wordt er gebruik gemaakt van apparatuur waarbij de mate van versnippering (snippergrootte) in overeenstemming is met het vertrouwelijkheidsniveau van de informatie. Gebruik hiervoor bij voorkeur een gecertificeerd bedrijf.