

Een gewaarschuwd mens telt voor twee

Handreiking strategische digitale veiligheid



Adviescollege
ICT-toetsing

Een gewaarschuwd mens telt voor twee

Handreiking strategische digitale veiligheid

Informatiebeveiliging staat al lange tijd op de agenda van menig bestuurder. Inmiddels heeft iedere organisatie van enig formaat een Chief Information Security Officer (CISO), zijn er verschillende normatieve kaders die aangeven waar informatiebeveiliging aan moet voldoen en zijn medewerkers zich meer bewust van dit onderwerp. Toch blijkt uit het meest recente Cybersecuritybeeld van Nederland¹ dat dit niet genoeg is. Het aantal incidenten neemt nu al toe en de strategische digitale veiligheid van Nederland staat steeds meer onder druk. Deze handreiking is bedoeld om die situatie te keren en bestuurders van overheidsorganisaties te helpen effectief toezicht te houden. Dat is noodzakelijk, omdat cyberbeveiligingsrisico's een strategisch risico zijn².

De Baseline Informatiebeveiliging Overheid (BIO-2) beschrijft de maatregelen die overheidsorganisaties moeten nemen om zich tegen toenemende dreiging te verweren. Het Adviescollege ICT-toetsing (AcICT) constateert echter dat veel overheidsorganisaties moeite hebben de juiste maatregelen uit te voeren.

Effectieve weerbaarheid tegen statelijke en criminele actoren (hierna: *kwaadwillenden*) vereist dat het risicobeheer voor strategische digitale veiligheid onderdeel uitmaakt van de bedrijfsvoering. Om dit in te richten adviseren wij te werken op basis van actuele inzichten en vervolgens concrete maatregelen te implementeren om de strategische digitale veiligheid te verbeteren. Zorg daarbij dat alle medewerkers hun verantwoordelijkheid nemen en stel bij op basis van periodieke evaluaties.

De cyclus moet regelmatig worden herhaald, omdat de strategieën van kwaadwillenden veranderen. Daardoor veranderen niet alleen de risico's, maar ook de effectiviteit van maatregelen. Het landschap van een organisatie is bovendien continu in beweging, bijvoorbeeld door veranderingen in processen, software en hardware. Maatregelen van gisteren zijn vandaag achterhaald en risico's moeten voortdurend opnieuw worden ingeschat.

De adviezen in deze handreiking komen voort uit recente onderzoeken van het AcICT en uit publieke casussen. Ze sluiten aan bij bestaande informatiebeveiligingsrichtlijnen. De voorbeelden in de kaders laten zien waarom aandacht voor informatiebeveiliging top-prioriteit zou moeten zijn. Immers, een gewaarschuwd mens telt voor twee.

1. Werk op basis van actuele inzichten

Een effectieve bescherming van cruciale systemen (applicaties, gegevens, enzovoort), waaronder systemen die vallen onder de vitale infrastructuur, begint met inzicht in het te beschermen landschap. Welke informatiesystemen heeft een organisatie, wie is daarvan de eigenaar en welke functie vervullen ze? De beschrijving hiervan noemen we de *inventaris*. De inventaris bevat systemen, maar ook mensen of organisaties. De inventaris beschrijft iets waardevols: het gaat om datgene waarmee de organisatie doelen bereikt en taken vervult. Dit kan worden bedreigd en dat is een risico. De hoogte van het risico is afhankelijk

¹ Nationaal Coördinator Terrorismebestrijding en Veiligheid. *Cybersecuritybeeld Nederland 2025 (CSBN 2025)*. <https://www.nctv.nl/documenten/2025/11/26/cybersecuritybeeld-nederland-2025>

² Cybersecurityraad. Handreiking Cybersecurity voor bestuurders en bedrijfseigenaren (4 juni 2025). <https://www.cybersecurityraad.nl/actueel/nieuws/2025/06/04/handreiking-geeft-bestuurders-en-bedrijfseigenaren-meer-grip-op-cybersecurity>

van de dreiging en het beschermingsniveau van het landschap. Ingewikkeld? Niet als je steeds de inventaris en de dreigingsbeelden gebruikt om de risico's te bepalen.

Wij constateren in de praktijk dat organisaties hun inventaris onvoldoende op orde hebben. Daardoor weten bestuurders niet welke risico's ze lopen met hun informatiesystemen of waarom deze interessant kunnen zijn voor kwaadwillenden. Daarnaast is er onvoldoende kennis van de werkwijzen van kwaadwillenden en weet men niet goed welke maatregelen hiertegen genomen moeten worden.

Wij adviseren de volgende drie stappen regelmatig te doorlopen met als doel de beschermende maatregelen te baseren op actuele inzichten.

Breng in kaart wat beschermd moet worden

In de inventaris dient een organisatie onderscheid te maken tussen reguliere systemen, cruciale systemen voor het eigen functioneren en systemen die vallen onder de vitale infrastructuur. Daarnaast kent iedere organisatie kritieke afhankelijkheden die bij uitval kunnen leiden tot ernstige verstoringen van hun (cruciale) systemen. De organisaties en de mensen waarvan een organisatie afhankelijk is, horen ook bij de inventaris.

Als systemen die vallen onder de vitale infrastructuur uitvallen of aangetast worden, is dat ontwrichtend voor de overheidsorganisatie en/of samenleving. De NCTV³ geeft op haar website een definitie van vitale infrastructuur. De RIVM Leidraad risicobeoordeling⁴ bevat een vragenlijst. Samengevat moet een organisatie zich de volgende vragen stellen om te bepalen welke systemen onderdeel zijn van de vitale infrastructuur:

- Is het systeem een kritieke of essentiële entiteit – in de zin van de Cyberbeveiligingswet en de Wet Weerbaarheid Kritieke Entiteiten – voor het ongestoord functioneren van Nederland als onafhankelijke staat?
- Kan een aanval op het systeem resulteren in ernstig letsel, sterfte of gebrek aan primaire levensbehoeften van burgers?
- Kan een aanval op het systeem resulteren in grote economische schade of ernstige toename van de staatschuld?

Het in kaart brengen van systemen en afhankelijkheden is onderdeel van de risicoanalyse voor informatiebeveiliging. De CISO coördineert dit proces en zorgt ervoor dat ten minste de volgende acties worden uitgevoerd:

- Inventariseer periodiek welke cruciale informatiesystemen de organisatie heeft en leg het eigenaarschap vast. Betrek hierbij de organisatie (bestuurders, proceseigenaren en experts) door workshops en scenario-oefeningen. Zo ontstaat een gedeeld en gedragen beeld van wat de cruciale systemen zijn.
- Identificeer de informatiesystemen die specifiek beschermd moeten worden tegen kwaadwillenden. Hanteer hierbij het uitgangspunt: wat is de schade als kwaadwillenden toegang krijgen?
- Maak afhankelijkheden expliciet, met name de organisatorische (belanghebbenden, ketenpartners, leveranciers, specialisten), operationele (processen, diensten) en technische (systemen, infrastructuur, externe diensten).
- Analyseer de gevolgen van mogelijke verstoringen voor de continuïteit van de dienstverlening. Dit kan bijvoorbeeld volgens de methodiek van de Business Impact Analyse (BIA) waarbij de impact in kaart wordt gebracht van verlies van vertrouwelijkheid, integriteit en beschikbaarheid.
- Leg alle informatie uit de analyse gestructureerd vast, bijvoorbeeld in een Configuratie Management Database (CMDDB) voor de registratie van systeem- en afhankelijkheidsgegevens of in BIA-rapportages conform ISO 22301.

³ Nationaal Coördinator Terrorismebestrijding en Veiligheid definieert Vitale infrastructuur. Geraadpleegd op 12 december 2025: <https://www.nctv.nl/onderwerpen/v/vitale-infrastructuur>. Zie ook de nieuwe Cyberbeveiligingswet (Cbw) – de Nederlandse implementatie van de Europese NIS2 richtlijn – voor de bepalingen in het digitale domein.

⁴ RIVM: *Leidraad risicobeoordeling 2022* (26 sep. 2022). <https://www.rivm.nl/documenten/leidraad-risicobeoordeling-2022>

2020: Aanval op Amerikaanse overheidsinstellingen en bedrijven

Als gevolg van een geavanceerde aanval op SolarWinds vanuit Rusland, zijn duizenden klanten besmet met malware. Veel computernetwerken in de VS zijn geïnfiltrerd en vertrouwelijke gegevens zijn buitgemaakt, waaronder die van het ministerie van Justitie (3 procent van de mailboxen), het federale rechtbankstelsel (geheime aanklachten, namen van informanten), Microsoft (gevoelige broncode) en het gerenommeerde beveiligingsbedrijf FireEye. Volgens Microsoft was de aanval zó complex dat er honderden IT-engineers aan moeten hebben gewerkt.

Benutte kwetsbaarheid: een gebrekkige beveiliging en integriteitscontrole in de ontwikkelomgeving van SolarWinds.

2023: Wereldwijd misbruik TeamCity

Hackers kregen toegang tot de softwarecode op de servers van TeamCity van JetBrains: een product voor het geautomatiseerd compileren, testen en releasen van software. Alhoewel Russische staatshackers soortgelijke kwetsbaarheden in het verleden hebben benut voor het verkrijgen van vertrouwelijke gegevens (zoals bij de aanval via SolarWinds), lijkt dat nu nog niet het geval. Deze hack lijkt eerder een investering, bedoeld voor toekomstig misbruik: er is toegang verkregen tot veel netwerken, ook buiten de overheid.

Benutte kwetsbaarheid: het kunnen omzeilen van authenticatie bij het uitvoeren van instructies.

De Cyber Security Raad en het Nationaal Cyber Security Centrum (NCSC)⁵ hebben meerdere interessante publicaties uitgebracht over de samenwerking tussen bestuurder en CISO.

Koppel de inventaris aan actuele dreigingsbeelden

Als de inventaris bekend is, breng dan voor elk onderdeel het dreigingsbeeld in kaart:

- Gebruik erkende dreigingsbeelden, zoals het Dreigingsbeeld Statelijke Actoren (DBSA)⁶ van de AIVD en het eerder genoemde Cybersecuritybeeld van de NCTV.
- Vertaal deze dreigingsbeelden naar relevante dreigingen voor de eigen organisatie. Betrek specialisten en domeindeskundigen om te bepalen welke dreigingen realistisch zijn. Houd bij statelijke actoren rekening met speciale kwetsbaarheden en aanvallen op delen van de organisatie. In tabel 1 geven we daar voorbeelden van op basis van onze ervaringen.
- Houd rekening met kwetsbaarheden die gestapeld worden: kleine risico's tezamen kunnen een groot risico vormen.
- Zorg voor inzicht in de 'fitheid' van systemen, want dat bepaalt mede het risico dat een organisatie loopt.

⁵ NCSC: *Vragen die je als bestuurder kunt stellen aan de CISO*. Geraadpleegd op 12 december 2025:

<https://www.ncsc.nl/risicomanagement/vragen-die-je-als-bestuurder-kunt-stellen-aan-de-ciso>

⁶ Algemene Inlichtingen- en Veiligheidsdienst: *Dreigingsbeeld Statelijke Actoren 2025* (2025, 17 juli)

<https://www.aivd.nl/documenten/publicaties/2025/07/17/dreigingsbeeld-statelijke-actoren-2025>

Inventarisatie-onderdeel	Voorbeeld van een bedreiging
Personeel	Gebruikers of beheerders met geprivilegieerde toegang worden doelgericht benaderd en omgekocht, verleid of gechanteed, afgeluisterd of gehackt.
Leverancier	Leverancier met geprivilegieerde toegang wordt specifiek voor een aanval omgekocht, verleid, gechanteed, afgeluisterd of gehackt. Een aanvaller richt een nieuwe entiteit op die als leverancier in een keten functioneert met als eigenlijke doel een specifieke aanval uit te voeren.
IT-procedures	Aanvaller kan authenticatiemiddel op naam van ander verkrijgen (hiaten in uitgifteproces). Niet-geautoriseerde USB-sticks worden geaccepteerd.
IT-diensten	Beheerssoftware met geprivilegieerde toegang bevat kwetsbaarheid die benut wordt.
IT-infrastructuur	Toegang tot een systeem vanaf een ander, minder goed beveiligd, systeem. Aanvaller heeft toegang tot platforms bij hosting-/cloudpartijen.
Data	Cryptografische sleutels die geprivilegieerde toegang geven kunnen worden gekopieerd.
Fysiek	Aanvaller is in staat communicatie af te luisteren en te manipuleren via apparaten, telecombedrijven of internetproviders. Aanvaller heeft fysiek toegang tot hardwarecomponenten, bijvoorbeeld door deze te onderscheppen bij transport of door inbraak.

Tabel 1: Mogelijke bedreigingen per inventarisatie-onderdeel

Kwaadwillenden gaan soms verder dan men voor mogelijk houdt. Zo blijkt uit onderstaande voorbeelden van een aantal spraakmakende aanvallen dat zij:

- een grote aanvalskracht hebben - een aanval kent dikwijls een extreme inspanning, in termen van voorbereidingstijd (meerdere jaren, soms wel tien jaar), expertise, capaciteiten en kosten (vaak tientallen miljoenen);
- opportunistisch zijn - een aanval kan toegang tot systemen of gegevens verlenen voor toekomstig gebruik en hoeft geen directe operationele waarde of noodzaak te kennen.

Als kwaadwillenden kiezen voor een langdurige, dure en complexe aanval, wordt deze zonder meer gericht op dat deel van de inventaris dat grote waarde heeft voor de organisatie. Beveiliging hiertegen is deels een kwestie van gezond verstand en moet in balans zijn met de waarde van dat wat je beveiligt: je gaat je dure fiets niet met een klein slotje bij het station zetten. Zo'n geavanceerde aanval moet zo moeilijk en onaantrekkelijk mogelijk zijn voor de aanvaller.

Uit het nieuws: overheidssystemen doelwit van geavanceerde aanvallen

2021: Spyware op mobiele apparaten van Europarlementariërs

In 2021 kwam een schandaal aan het licht: er was via WhatsApp spyware op mobiele telefoons van Europarlementariërs geïnstalleerd die gebruik maakte van kwetsbaarheden in mobiele besturingssystemen. Sommige kwetsbaarheden waren nog onbekend. Er waren meer dan tien leveranciers betrokken; met name het Israëlische bedrijf NSO Group dat de spyware Pegasus heeft ontwikkeld wordt met deze hack geassocieerd. Via het afluisterplatform van Pegasus hadden de klanten van NSO, natiestaten binnen en buiten de EU, toegang tot interne discussies, beleidsvorming en stemstrategieën binnen het Europees Parlement.

2024: Contactgegevens van de politie buitgemaakt

In september 2024 werd een grote cyberaanval op de Nederlandse politie uitgevoerd, waarbij werkgerelateerde contactgegevens van praktisch alle 63.000 politiemensen zijn buitgemaakt. Dit blijkt uit onderzoek van de inlichtingendiensten AIVD en MIVD. De gegevens konden worden gestolen doordat accounts van medewerkers werden gehackt. Bij de hack werd gebruikgemaakt van een zogenaemde pass-the-cookie-aanval, waarbij een aanvaller een actieve sessie overneemt met de bijbehorende rechten. Deze aanval werd ontdekt en onderzocht door gespecialiseerde teams binnen de Politie en is door de inlichtingendiensten toegeschreven aan de Russische hackersgroep Laundry Bear. De impact op de organisatie was groot: de Politie erkent dat het lek aanzienlijke gevolgen had voor de organisatie én de collega's.

Werk risico's uit

De koppeling van de inventaris aan dreigingsbeelden maakt duidelijk wat de risico's zijn voor de systemen, de daarin opgeslagen data of de infrastructuur. Daaruit volgt welke kwaadwillenden de grootste dreiging vormen en wat hun werkwijze is. Een bekende methodiek om risico's in te schatten is de risicobeoordelingsmatrix uit ISO 27005 (tabel 2). Ook de Britse NCSC heeft hier een goed hanteerbare methodiek voor⁷. Wij adviseren om een methodiek te kiezen en deze door de organisatie te laten adopteren.

In de praktijk zien we dat met name de risico's waarvan de kans groot is dat ze optreden veel aandacht krijgen. Binnen de context van strategische digitale veiligheid moet echter ook expliciet rekening worden gehouden met lage risico's: onwaarschijnlijke aanvallen die catastrofale gevolgen kunnen hebben. De vraag is dus steeds of een informatiesysteem zó interessant is voor kwaadwillenden dat ze bereid zijn om een extreem krachtige aanval uit te voeren. Soms zijn het risico's waar organisaties zich niet of nauwelijks tegen kunnen beschermen. Ondanks dat deze niet vaak voorkomen, zijn ze wel direct catastrofaal en is extra bescherming nodig.

		Consequentie				
		Catastrofaal	Kritisch	Serius	Significant	Klein
Kans	Bijna zeker	Erg hoog risico	Erg hoog risico	Hoog risico	Hoog risico	Matig risico
	Erg waarschijnlijk	Erg hoog risico	Hoog risico	Hoog risico	Matig risico	Laag risico
	Waarschijnlijk	Hoog risico	Hoog risico	Matig risico	Laag risico	Laag risico
	Nogal waarschijnlijk	Matig risico	Matig risico	Laag risico	Laag risico	Erg laag risico
	Onwaarschijnlijk	Extra aandacht	Laag risico	Laag risico	Erg laag risico	Erg laag risico

Tabel 2: Risicobeoordelingsmatrix: deze tabel bepaalt het risiconiveau voor een systeem op basis van de kans op een aanval en de consequenties van deze aanval.

Het eindresultaat van de drie stappen uit dit hoofdstuk is een lijst van risicobeelden per onderdeel van de inventaris. Deze lijst moet compact en goed leesbaar voor bestuurders zijn.

2. Implementeer concrete maatregelen om de strategische digitale veiligheid te verbeteren

Als de actuele risico's voor de systemen in kaart zijn gebracht (advies 1), is het zaak deze te ondervangen met concrete beveiligingsmaatregelen (advies 2). Het onderscheid tussen cruciale en reguliere systemen is belangrijk, maar voorkom dat alle aandacht naar de cruciale systemen gaat en de reguliere worden vergeten. Helaas blijkt uit de praktijk dat de basisbeveiliging veelal niet op orde is doordat hier geen aandacht voor is of omdat de budgetten voor beheer en onderhoud te laag zijn ingeschat. Beide categorieën moeten adequaat beveiligd worden. Wij adviseren daartoe het volgende.

Ontwikkel en implementeer een passend basisbeveiligingsniveau voor alle systemen

Voor een goede beveiliging tegen kwaadwillenden moet in elk geval het basisbeveiligingsniveau op orde zijn. Kwaadwillenden gebruiken immers bekende zwakheden voor hun acties. Dit betekent concreet dat alle maatregelen uit de BIO-2 nageleefd moeten worden voor de reguliere systemen.

Voor cruciale systemen en systemen met een extra hoog risicoprofiel is extra aandacht nodig. In het kader hieronder staan de aanvullende noodzakelijke maatregelen die geïmplementeerd moeten worden om een cruciaal systeem te beveiligen.

⁷ Brits National Cyber Security Centre. *A basic risk assessment and management method*. (2023, 23 juni): <https://www.ncsc.gov.uk/collection/risk-management/a-basic-risk-assessment-and-management-method>

Aanvullende noodzakelijke maatregelen voor de beveiliging van cruciale systemen en systemen met een extra hoog risicoprofiel

Gebruik alleen producten van betrouwbare origine

Computers, routers, switches of CPU's kunnen bewerkt zijn door kwaadwillenden waardoor er informatie kan lekken of waardoor hackers gemakkelijk toegang kunnen krijgen. Gebruik dus alleen vertrouwde producten (o.a. door de leverancier gevalideerde softwarecomponenten) en controleer afhankelijkheden op kwetsbaarheden.

Screen leveranciers en monitor continu hun activiteiten

Leveranciers kunnen overgenomen worden, failliet gaan of onder druk staan van kwaadwillenden. Screen ze dus regelmatig. Denk daarbij onder andere aan een audit op de broncode van software, haalbaarheid van data-overdracht, plausibiliteitscontrole op de jaarrekening, concernrelaties en eigenaren in het buitenland, en een VOG voor medewerkers. Of laat ethische hackers proberen een cruciaal systeem binnen te dringen.

Monitor alle randapparatuur

Routers en sensoren geven data door aan een centrale cloud of datacenter en kunnen hackers zo toegang geven tot een computernetwerk. Zorg dat altijd de meest recente patches zijn geïnstalleerd en monitor de werking van randapparatuur op verdachte patronen.

Beveilig toegang tot systemen met sterke authenticatie en beperkte zichtbaarheid

Wachtwoorden kunnen met snelle computers gemakkelijk gevonden worden. Daarom is een extra beveiligingsmethode om de identiteit van een gebruiker vast te stellen belangrijk. Stel strenge eisen aan authenticatie: gebruik meerdere factoren en, waar nodig, hardwaretokens of cardreaders. Beperk daarnaast de zichtbaarheid van systemen. Zorg ervoor dat alleen geauthentiseerde en geautoriseerde gebruikers een systeem kunnen benaderen. Zo wordt het aanvalsoppervlak sterk verkleind en wordt ongeautoriseerde toegang structureel bemoeilijkt. Een goede manier om dit te realiseren, is met een Software Defined Perimeter (SDP). Deze geeft een hogere beveiliging dan VPN.

Train en toets geprivilegieerde ICT-beheerders en versterk toezicht op hun handelingen

Beheerders hebben noodzakelijkerwijs toegang tot gevoelige gegevens en systemen; ze zijn daardoor een potentieel doelwit van kwaadwillenden. Zorg voor een gerichte training met periodieke toetsing van hun handelingsbekwaamheid en weerbaarheid, en ondersteun deze training met praktijkvoorbeelden van relevante incidenten. Beperk bovendien het aantal beheerders en geef hun alleen toegang tot kritieke systemen via intermediaire servers die een beveiligde brug vormen tussen het streng beveiligde en het reguliere landschap. Log alle handelingen uitvoerig, zorg dat de logs integer zijn en richt toezicht in.

Train medewerkers in het veilig gebruiken van hun apparaten

Plaats alle mobiele apparaten buiten de ruimte of in een goed af te sluiten ijzeren trommel bij vertrouwelijke gesprekken. Zorg dat medewerkers PC's, laptops en mobiele apparaten regelmatig (het liefst dagelijks) herstarten, om ongewenste processen door mogelijke malware te beëindigen en softwareupdates te installeren. Dit verkleint de kans dat malware actief blijft en dat beveiligingslekken niet worden gedicht.

Beperk netwerkcommunicatie tot strikt noodzakelijke communicatie met bekende partijen

Via gegevensuitwisseling kunnen gegevens binnen worden gehaald die de beschikbaarheid en integriteit van het systeem beschadigen. Zorg er daarom voor dat er alleen gecommuniceerd kan worden met bekende partijen, dat de uitwisseling van gegevens beperkt blijft tot het noodzakelijke, en dat de identiteit van de andere partij en context voor iedere transactie wordt vastgesteld (*zero-trust*).

Beperk websurfen vanaf werkplek

Als iemand een browser gebruikt, kunnen anderen toegang krijgen tot diens computer en daarmee tot het netwerk waarmee de computer is verbonden. Zorg er daarom voor dat websurfen uitsluitend plaatsvindt op een computer die niet betrokken is bij cruciale systemen of via een gevirtualiseerde werkplek die dagelijks wordt geschoond. Als het noodzakelijk is om documenten van internet binnen te halen, installeer dan een apparaat dat uitsluitend dataverkeer in één richting toestaat (*datadiode*).

Monitor het netwerkverkeer op alle dagen en alle tijdstippen (24/7)

Een hack kan leiden tot onregelmatigheden in het patroon van dataverkeer; bijvoorbeeld meer dataverkeer op ongebruikelijke momenten en vanaf ongebruikelijke servers. Verhoog het toezicht door continue monitoring via een Security Operations Center (SOC). Introduceer specifieke detectieregels om afwijkingen van normale systeem- of gebruikerspatronen vroegtijdig te signaleren. Plaats daarnaast loksystemen (*honeypots*) die bedoeld

zijn om aanvallers te misleiden en hun gedrag te analyseren. Zo worden aanvallen vroegtijdig zichtbaar. Actualiseer de respons op deze aanvallen en verbeter de verdedigingstechnieken.

Oefen met realistische aanvalsscenario's

Zorg ervoor dat medewerkers oefenen met het detecteren van en reageren op een aanval. Bijvoorbeeld door *red teaming*: twee teams met tegengestelde rollen oefenen om de weerbaarheid van een organisatie tegen realistische aanvalsscenario's te verbeteren. Voer bovendien periodiek specifieke securitytoetsen uit zoals pentesten en crisisoefeningen. Test ook systeemherstelscenario's (*failover*) waarbij - om de systemen in de lucht te houden - wordt uitgeweken naar een andere locatie met een back-up of synchronisatie.

Maak onderscheid tussen cruciale en reguliere systemen

Aan strenge beveiligingsmaatregelen kleven ook nadelen, zoals een afgenomen gebruiksgemak en hogere kosten. Het is daarom niet reëel om aan alle systemen in een organisatie de allerhoogste beveiligingsmaatregelen toe te kennen. Door een strikte scheiding aan te brengen tussen reguliere en cruciale systemen kunnen het extra ongemak en de extra kosten beperkt worden. Het landschap moet dan zo ingericht worden dat cruciale systemen en data met een hoog rubriceringsniveau gescheiden zijn van de reguliere systemen. Dit kan door systemen fysiek (op een andere locatie) of logisch (in een ander netwerk) onder te brengen met minimale en strikt gecontroleerde koppelingen naar reguliere systemen.

3. Zorg dat alle medewerkers hun verantwoordelijkheid nemen

Strategische digitale veiligheid krijgt alleen gestalte als mensen zich eraan gedragen. Iedere medewerker - van werkvloer tot de bestuurskamer - heeft hierin een rol. In het kader hierboven staat al een aantal noodzakelijke maatregelen dat hierop betrekking heeft. Daarnaast moet het bestuur van een organisatie participatie actief stimuleren. Het doel daarvan is dat de hele organisatie begrijpt waarom er extra stappen worden genomen om cruciale systemen te beschermen en dat iedereen actief aan die bescherming moet bijdragen. Zo dragen alle medewerkers hun verantwoordelijkheid en voelt de CISO zich geen roepende in de woestijn, zoals wij regelmatig horen. De adviezen in dit hoofdstuk zijn erop gericht dat voor elkaar te krijgen.

Uit het nieuws: verstreckende gevolgen voor organisaties die de basis niet op orde hebben

2025: Misbruik netwerkapparatuur Openbaar Ministerie

In juli 2025 werd het Openbaar Ministerie (OM) door het Nationaal Cyber Security Centrum (NCSC) gewaarschuwd voor actief misbruik van een ernstige kwetsbaarheid in Citrix NetScaler-apparatuur. Naar aanleiding hiervan heeft het OM zijn systemen van het internet losgekoppeld en een onderzoek ingesteld. Uit onderzoek bleek dat aanvallers de kwetsbaarheid mogelijk hadden benut om toegang te krijgen tot de systemen van het OM. Het OM startte daarom een gefaseerde hersteloperatie en nam aanvullende beveiligingsmaatregelen. De digitale dienstverlening was daardoor tijdelijk beperkt, onder meer doordat medewerkers niet extern konden inloggen en bepaalde systemen niet beschikbaar waren.

2025: Hackers kregen toegang tot de systemen van TU Eindhoven

De Technische Universiteit Eindhoven (TU/e) kreeg in januari 2025 te maken met een cyberaanval waarna het netwerk volledig moest worden uitgezet. Daardoor lag het onderwijs aan de TU/e een paar dagen stil. Onderzoek op verzoek van de TU/e toonde aan dat de aanvallers inlogden via VPN met gestolen inloggegevens. Ongeautoriseerde toegang was mogelijk door het ontbreken van een aanvullende verificatiestap voor VPN-toegang zoals multifactor authenticatie (MFA). De universiteit meldt dat er geen indicatie is dat er data zijn gestolen; het bereik van de aanval bleef beperkt omdat systemen na detectie snel werden afgekoppeld.

Zorg dat verantwoordelijkheden voor informatiebeveiliging duidelijk zijn

Alleen met een duidelijke verdeling van verantwoordelijkheden voor strategische digitale veiligheid biedt een organisatie weerstand aan steeds complexer wordende digitale dreigingen. De eindverantwoordelijkheid voor informatiebeveiliging binnen een organisatie ligt formeel bij het verantwoordelijke bestuursorgaan, meestal de directie of het bestuur. Het wordt daarbij ondersteund door een sterke en goed toegeruste leiderschapsstructuur. De CISO speelt een belangrijke rol in de coördinatie en organiseert dat:

- de verantwoordelijkheid (eigenaarschap) voor concrete aspecten van digitale veiligheid op het juiste niveau belegd is;
- alle medewerkers van de organisatie - niet alleen teams die verantwoordelijk zijn voor doorontwikkeling, onderhoud of beheer van software - in staat zijn hun verantwoordelijkheden uit te voeren;
- beleid, procedures en controles regelmatig worden herzien en aangepast aan actuele dreigingsbeelden.

Veranker risicobeheer in de aansturing van de organisatie door dit onderwerp vast op de agenda van periodieke overleggen te plaatsen, op alle niveaus. Laat de afspraken over het risicobeheersingsproces vastleggen in een beheersysteem voor informatiebeveiliging (een ISMS⁸) en zorg dat de vastgelegde keuzes en regels voor alle medewerkers toegankelijk zijn. Zorg er wel voor dat een dergelijk systeem, evenals de CMDB, toegankelijk en hanteerbaar blijft. Een groot risico is namelijk dat deze systemen zoveel, deels automatisch gegenereerde, gegevens bevatten dat niemand er meer iets aan heeft. Om het voor mensen behapbaar te houden, is het zinvol om te sturen op een beperkte set van systemen en data, de risico's daarvan en de te nemen maatregelen.

Zorg dat de medewerkers zich veilig gedragen

Medewerkers veranderen hun gedrag alleen als duidelijk is wat het nieuwe gedrag moet zijn en welke middelen daarvoor voorhanden zijn. Het lijnmanagement van een organisatie heeft hierbij een belangrijke voorbeeldfunctie. Bovendien moeten medewerkers gemotiveerd zijn om te investeren in het gewenste nieuwe gedrag. Alleen een training is niet genoeg om mensen te motiveren. Onderstaande adviezen vergroten de kans dat medewerkers hun verantwoordelijkheid nemen.

- Communiceer de risico's en dreigingen voor de organisatie expliciet en zo concreet als mogelijk.
- Wees duidelijk over de kwetsbaarheid van systemen en de genomen maatregelen. Laat zien hoe zij de inventaris beschermen. Concrete gedragsregels rondom zaken zoals toegang, datagebruik en meldplicht behoren bij deze maatregelen.
- Train medewerkers regelmatig op cyberbewustzijn. Denk hierbij aan het herkennen van phishingmail, omgaan met gevoelige data en het strikt naleven van informatiebeveiligingsrichtlijnen. Oefen ook social-engineering-scenario's, zoals gesimuleerde CEO-fraude, om medewerkers te leren verdachte verzoeken en valse e-mails te herkennen en te melden.
- Zorg dat medewerkers weten hoe ze moeten handelen bij een incident (groot of klein). Zorg dat het als vanzelfsprekend wordt gezien om melding te maken. Oefen de respons op incidenten ook regelmatig.
- Zorg dat het topmanagement het belang van een sterke beveiligingscultuur uitdraagt.
- Beloon goed gedrag.

Deel kennis over cruciale systemen

Bij cruciale systemen denken medewerkers al snel alleen aan systemen die vertrouwelijke gegevens verwerken of industriële automatisering van bijvoorbeeld een waterkering. Maar ook andere systemen kunnen extra bescherming nodig hebben, bijvoorbeeld als het gaat om risico's bij foutieve of onvolledige data (integriteit) of problemen die ontstaan als systemen uitvallen (beschikbaarheid). Om ervoor te zorgen dat de juiste mensen verantwoordelijkheid nemen voor deze systemen is het belangrijk kennis erover te delen.

⁸ Beheersysteem voor informatiebeveiliging: Nationaal Cyber Security Centrum. (2025, 17 juli). *Beginnen met een ISMS*. Geraadpleegd op 12 december 2025, van <https://www.ncsc.nl/risicomanagement/beginnen-met-een-isms>

Uit het nieuws: de menselijke factor is vaak onderschat

2010 - 2013 Aanval op de Belgische telecomprovider Belgacom

Medewerkers van Belgacom – Belgische aanbieder van telecomdiensten – werden in 2010 naar vervalste LinkedIn-pagina's gelokt. Hierdoor kregen aanvallers toegang tot computers van deze medewerkers, waarop aftapsoftware werd geplaatst. Na nog een aantal acties kon malware op de netwerkinfrastructuur worden geïnstalleerd en kon de mobiele communicatie (spraak, internet) tussen Europa, het Midden-Oosten en Noord-Afrika worden afgeluisterd. Klokkenluider Edward Snowden onthulde in 2013 dat deze aanval onderdeel was van spionage door de Amerikaanse en Britse inlichtingendiensten NSA en GCHQ.

2015: Datalek US Office of Personnel Management (OPM)

Door een mail te sturen aan een medewerker kregen hackers toegang tot de inlognaam en het wachtwoord van een gedeeld beheerdersaccount. Dat ontsloot de persoonlijke informatie van ongeveer 21,5 miljoen federale werknemers en andere betrokkenen. Ook hadden de hackers inzage in screeningformulieren van medewerkers van de geheime dienst en in circa 5,6 miljoen vingerafdrukgegevens. Het vermoeden is dat China met deze hack een database wilde opbouwen van overheids personeel. De grondoorzaak van de aanval was dat het management van OPM onvoldoende prioriteit gaf aan cyberbeveiliging. Als gevolg van het incident trad de directeur van OPM af en verliet later ook de CIO haar functie.

Zorg voor voldoende technische kennis bij bestuurders en leidinggevenden

De verantwoordelijkheid voor beveiliging ligt vaak bij personen met een juridische achtergrond of met een bestuurdersprofiel. Dit zorgt weliswaar voor sterke compliance, maar niet noodzakelijk voor voldoende paraatheid tegen kwaadwillenden. De overheid moet ervoor zorgen dat bestuurders, toezichthouders en CISO een profiel hebben waarin technische kennis, bestuurlijke vaardigheid en juridische sensitiviteit samengaan. We pleiten er niet voor dat bestuurders een soort CISO-light worden, maar wel dat ze in staat zijn om risico's goed te beoordelen met input van technische functionarissen. Een CISO moet kunnen leunen op een sterke IT-organisatie die achter het beleid staat en voldoende capaciteit heeft om het uit te voeren.

4. Stel bij op basis van periodieke evaluaties

Het evalueren en verbeteren van cyberweerbaarheid is een proces dat de organisatie versterkt. Het naleven van beveiligingsmaatregelen zorgt voor leermomenten die daartoe kunnen worden benut. Medewerkers zijn daarvoor een belangrijke bron. Zij leren in de praktijk van incidenten, van risico-afwegingen en van het nut van bepaalde tegenmaatregelen. Dit gaat van operationeel technische activiteiten – bijvoorbeeld het correct en veilig configureren van een firewall – tot communicatie tijdens een crisis. Leveranciersmanagers kunnen voor dilemma's staan: producten van leveranciers die een jaar geleden nog vertrouwd waren, kunnen door veranderde geopolitieke verhoudingen opeens geen optie meer zijn. Ook klachten van medewerkers over tijdrovende procedures zijn relevant. Het is belangrijk om alle informatie te verzamelen, te structureren en bruikbaar te maken. Samen met evaluaties van incidenten, bijna-incidenten en oefeningen moeten leermomenten vertaald worden naar concrete verbeteringen. Zo leert de organisatie van de praktijk.

Naast evaluaties uit de praktijk zijn periodieke evaluaties essentieel. We missen deze vaak en adviseren daarom het volgende.

Zorg voor een gedegen audit

Bij doeltreffende beveiligingsmaatregelen hoort controle op de effectiviteit en naleving daarvan. Richt daartoe een goede interne auditfunctie in die wordt aangevuld met externe audits. Een audit levert een meting op, op basis waarvan de organisatie kan verbeteren. Het herhaald uitvoeren van een audit zorgt ervoor dat de organisatie grip op de maatregelen houdt en deze bij kan stellen als ze onvoldoende blijken of niet worden nageleefd door de medewerkers. Voer de interne audit uit volgens een gestructureerd proces en zorg dat auditbevindingen een eigenaar krijgen die een plan opstelt om ze te verhelpen. Dit plan wordt beoordeeld door de auditor.

Periodieke audits zijn niet voldoende. Continu toezicht is een manier van samenwerken tussen een bestuur, de CISO en de uitvoerders waarbij niet alleen de voortgang op het implementeren van maatregelen wordt gemeten (de inspanning), maar ook het effect daarvan (de effectiviteit). De Handreiking van de Cyber

Security Raad , voor bestuurders⁹, beschrijft de inrichting van deze samenwerking. Naast periodieke audits kunnen geautomatiseerde audits continu controleren of systemen voldoen aan de gestelde eisen.

Uiteindelijk is het doel om de weerbaarheid van de organisatie te verhogen. Een audit heeft dus niet als doel om vinkjes te verzamelen in een rapport. Als het zo wordt ervaren, moet er nog veel gebeuren aan de opzet van de audit en de betrokkenheid van de medewerkers.

Neem het risicobeheer mee in de managementreview

Cybersecurity moet worden besproken in de bestuurskamer als vast agendapunt, met een budget en een verbeterprogramma. De Cyberbeveiligingswet schrijft voor dat de besluitvorming en verantwoordelijkheid voor cybersecurity op het hoogste niveau belegd moeten worden. Een goede manier om dit voor elkaar te krijgen, is om het risicobeheer mee te nemen in de jaarlijkse managementreview op het bestuur of de directie. De managementreview is een ISO9001-activiteit – onderdeel van de Plan Do Check Act-cyclus¹⁰ – waarbij met een bepaalde frequentie (per kwartaal, half jaar of jaar) de directie systematisch het eigen kwaliteitsmanagement onder de loep neemt. Een organisatie kan natuurlijk ook een vergelijkbare methodiek inzetten om cybersecurity op de directietafel te krijgen.

Toets regelmatig of medewerkers de maatregelen naleven en stuur bij

Het is nodig om regelmatig te toetsen in hoeverre medewerkers het gewenste gedrag laten zien als het gaat om beveiliging en waar nodig bij te sturen:

- Toets medewerkers regelmatig op cyberbewustzijn.
- Analyseer de nalevingsgraad van de gedragsmaatregelen en bepaal welke factoren de naleving van maatregelen beïnvloeden.
- Stimuleer het lerende vermogen van de medewerkers door openlijk lessen te trekken uit de in- en externe audits en scenario-oefeningen.
- Waarborg dat de geleerde lessen worden vertaald naar bijgesteld beleid en versterkte beveiligingsmaatregelen, zodat de cyberweerbaarheid continu verbetert.

⁹ Cybersecurityraad. Handreiking Cybersecurity voor bestuurders en bedrijfseigenaren (4 juni 2025):

<https://www.cybersecurityraad.nl/actueel/nieuws/2025/06/04/handreiking-geeft-bestuurders-en-bedrijfseigenaren-meer-grip-op-cybersecurity>

¹⁰ Toelichting op de PDCA cyclus in <https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso9001-2015-process-appr.pdf>

Bijlagen bronnen bij “Uit het nieuws”

Voorbeeld	Referenties
2010 - 2013 Aanval op de Belgische telecomprovider Belgacom	<ul style="list-style-type: none"> • Belgacom surveillance case europarl.eu • Belgacom hacking case europarl.eu • Belgium ISP under attack by British Intelligence edri.org
2015: Datalek US Office of Personnel Management (OPM)	<ul style="list-style-type: none"> • Data Breach – House of Representatives Committee oversight.house.gov • OPM has Improved Controls, but Further Efforts Are Needed gao.gov
2020: Aanval op Amerikaanse overheidsinstellingen en bedrijven vanuit Rusland	<ul style="list-style-type: none"> • Active Exploitation of SolarWinds Software cisa.gov • Advanced Persistent Threat Compromise of Government Agencies cisa.gov • SolarWinds hack was ‘largest and most sophisticated attack’ ever reuters.com
2021: Spyware op mobiele apparaten van Europarlementariërs	<ul style="list-style-type: none"> • Verslag enquêtecommissie om het gebruik van Pegasus europarl.eu • Europe’s PegasusGate europarl.eu
2023: Wereldwijd misbruik TeamCity kwetsbaarheid vanuit Rusland	<ul style="list-style-type: none"> • Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE cisa.gov
2024: Contactgegevens politie buitgemaakt door Russische hackers	<ul style="list-style-type: none"> • Stand van zaken onderzoek en veiligheidsmaatregelen datalek politie politie.nl • Ontwikkelingen rond datalek bij Nederlandse politie politie.nl • Onbekende Russische groep achter hacks Nederlandse doelen aivd.nl
2025: Hackers kregen toegang tot de systemen van TU/e	<ul style="list-style-type: none"> • Samen sterk: Hoe onze universiteit de cyberaanval trotseerde tue.nl
2025: Misbruik netwerkapparatuur Openbaar Ministerie	<ul style="list-style-type: none"> • Onderzoek naar aanleiding van signaal NCSC om.nl • Informatie over kwetsbaarheden in Citrix Netscaler ncsc.nl • OM gaat stapsgewijs online om.nl

Deze publicatie is een uitgave van:

Adviescollege ICT-toetsing

info@adviescollegeicttoetsing.nl
www.adviescollegeicttoetsing.nl
Postbus 16292 | 2500 BG Den Haag

januari 2026



De tekst van deze publicatie is gelicentieerd onder de Creative Commons Naamsvermelding 4.0-licentie (CC-BY 4.0), de rechten op afbeeldingen, lettertypen en logo's liggen bij hun respectievelijke eigenaren. De volledige licentie-tekst is te lezen op: <https://creativecommons.org/licenses/by/4.0/>. Wanneer je gebruik wilt maken van dit werk, hanteer dan bij voorkeur de volgende methode van naamsvermelding:
Adviescollege ICT-toetsing (2026), Een gewaarschuwd mens telt voor twee. Den Haag, januari 2026, CC-BY 4.0 gelicentieerd.



**Adviescollege
ICT-toetsing**