Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Hoe krijg ik grip op mijn security controls?

Aan de slag met de NIS2-richtlijn

Factsheet FS 2024 | versie 1.0 | 10 juli 2024

Security controls zijn beheersmaatregelen die erop gericht zijn om beveiligingsrisico's te beperken door een (digitale) aanval te voorkomen, tijdig te detecteren, hier adequaat op te reageren en/of hiervan te herstellen. Grip op jouw security controls is nodig om jouw organisatie passend weerbaar te maken en te houden. Deze publicatie helpt je om grip te krijgen op jouw security controls. Wil je meer weten over hoe je tot een afgeronde risicobeoordeling kan komen? Lees dan ook de publicaties 'Hoe breng ik mijn te-beschermen-belangen in kaart' en 'Hoe breng ik mijn dreigingen in kaart?'.

Achtergrond

De afgelopen jaren zien we dat diverse ontwikkelingen in toenemende mate de veiligheid van onze maatschappij en economie onder druk zetten. Denk daarbij aan COVID-19, de oorlog in Oekraïne en cyberdreigingen. In het licht van deze ontwikkelingen is er sinds 2020 vanuit de Europese Unie gewerkt aan de *Network and Information Security (NIS2) directive.* Deze richtlijn is gericht op een verbetering van de digitale en economische weerbaarheid van Europese lidstaten. In Nederland zal de NIS2-richtlijn geïmplementeerd worden in de vorm van de Cyberbeveiligingswet.

De Rijksoverheid adviseert organisaties om niet af te wachten totdat de wet- en regelgeving volledig in werking zijn. De risico's die organisaties en systemen lopen, zijn er immers nu ook al. Organisaties die nu in actie komen beveiligen zich niet alleen tegen deze bestaande risico's, maar zijn straks ook beter voorbereid op de komst van de nieuwe wetgeving.[1]

Deze publicatie maakt onderdeel uit van een publicatiereeks en biedt praktische handvatten voor het uitvoeren van een risicoanalyse in het kader van de NIS2-richtlijn.[2] De handvatten in deze publicatie zijn ter voorbereiding op de NIS2-richtlijn geschreven, maar kunnen ook in bredere context gebruikt worden om grip te krijgen op jouw security controls.[3]

Doelgroep

Deze publicatie is geschreven voor personen die binnen hun organisatie een rol hebben bij het uitvoeren van een risicoanalyse en behoefte hebben aan basisinformatie rondom het inventariseren van – en zicht houden op – security controls.

Aan deze publicatie hebben bijgedragen

CISO's en adviseurs van Gemeente Amersfoort, Gemeente Noordenveld, CIO Rijk, Ministerie van Onderwijs Cultuur en Wetenschap, de Nederlandse Vereniging van Banken en een partner in de chemische industrie.

[1] Cyberbeveiligingswet (NIS2-richtlijn) | Over het NCSC | Nationaal Cyber Security Centrum

[2] Bereid je voor op de wet | Over het NCSC | Nationaal Cyber Security Centrum

[3] Het doel van deze publicatie is om organisaties te ondersteunen bij de voorbereiding op de NIS2-richtlijn. Deze publicatie biedt geen officiële of juridische basis om aan de NIS2-richtlijn te voldoen

Wat zijn security controls?

Security controls zijn beheersmaatregelen die erop gericht zijn om beveiligingsrisico's te beperken door een (digitale) aanval te voorkomen, tijdig te detecteren, hier adequaat op te reageren en/of hiervan te herstellen. Denk bijvoorbeeld aan het voorkomen dat informatie toegankelijk is voor onbevoegden door regels op te stellen rondom 'clear-desks' voor papieren documenten en verwijderbare opslagmedia (USB's). Of het monitoren van afwijkend gedrag op netwerken en systemen om potentiële incidenten te detecteren.

Er zijn verschillende manieren om security controls te categoriseren. Zo kunnen deze gecategoriseerd worden volgens de (primaire) functie van deze control, zoals het hierboven beschreven voorkomen, detecteren en tegengaan van een aanval, of het hiervan herstellen. Daarnaast zijn er verschillende type controls te onderscheiden. Zo richten *Organisatorische controls* zich op het inrichten van veilige processen. Denk aan beleid rondom dataclassificatie of het scheiden en toebedelen van taken en verantwoordelijkheden. *Fysieke controls* richten zich op het beveiligen van de fysieke omgeving, bijvoorbeeld middels cameratoezicht of het voeren van toegangscontrole op serverruimtes. *Mensgerichte controls* hebben oog voor de interactie tussen mensen en systemen. Denk hierbij aan bewustwordingsprogramma's en training op het gebied van informatiebeveiliging. *Technische (of logische) controls* richten zich op technische aspecten zoals het afschermen van het netwerk (middels firewalls en VPN oplossingen) en het beheren van back-ups.

Security controls zijn onderdeel van een groter plaatje

Er is een aantal belangrijke redenen om zicht te hebben op jouw security controls. Zo kan het nodig zijn dat je moet aantonen dat je bepaalde maatregelen hebt getroffen (bij een audit) om aan te kunnen tonen dat jouw organisatie voldoet aan bepaalde wet- of regelgeving. Compliant zijn is echter nog geen garantie voor een veilige en weerbare organisatie. Een belangrijkere reden om zicht te krijgen op security controls is in het kader van risicomanagement.

De weerbaarheid van jouw organisatie is afhankelijk van de geïmplementeerde controls en hoe deze relateren aan de risico's waaraan de organisatie wordt blootgesteld. Verschillende security controls leveren gezamenlijk een bijdrage om een risico te mitigeren. Zo kunnen risico's die voortkomen uit onbevoegde toegang tot gegevensdragers worden beheerst door een combinatie van een fysieke beheersmaatregel – zoals een 'clear-desk' beleid – en een technische maatregel zoals het vercijferen van gegevensdragers. Het kunnen duiden van — en sturen op – jouw weerbaarheid vereist daarbij dat je grip hebt op die security controls.

Een risico-gebaseerde aanpak is de meest kosteneffectieve manier om jouw organisatie passend digitaal weerbaar te maken. Overtuig het bestuur van de noodzaak van een risico-gebaseerde aanpak en maak met hen afspraken over het hiervoor beschikbare budget, KPI's, beleid en de risicobereidheid van de organisatie. Wijs daarbij op de zorgplicht en de persoonlijke aansprakelijkheid van bestuurders op het gebied van digitale weerbaarheid onder de NIS2.

Stap 1: Gebruik een relevant framework als uitgangspunt

Om grip te krijgen op jouw security controls is het goed om uit te gaan van een framework dat een overzicht geeft van de security controls die het meest relevant zijn voor jouw organisatie. Voorbeelden zijn de ISO 27002, IEC62443-3-3, CIS Controls, NIST SP800-53 en COBIT. Naast deze (generieke) frameworks zijn er ook frameworks die gericht zijn op specifieke sectoren, zoals de Baseline Informatiebeveiliging Overheid (BIO). Ook bestaan er voor verschillende sectoren normenkaders zoals de BIACS (voor de watersector), welke een minimale set aan controls schetst die geïmplementeerd moeten worden om een (basis) beveiligingsniveau te behalen.

Een framework biedt houvast om controls te categoriseren, beveiligingsdoelen en -maatregelen met elkaar te relateren en om de link te leggen met jouw weerbaarheid. Bepaal welk framework passend is voor jouw organisatie. Neem daarin de volgende elementen mee:

- Wettelijke kaders en eisen van toezichthoudende instanties. Je wilt ervoor zorgen dat het door jou gekozen framework ook goed past binnen het kader van wet- en regelgeving waar jouw organisatie aan dient te voldoen.

- Sector-specifieke frameworks. Voor sommige sectoren zullen er al specifieke frameworks zijn die de voorkeur genieten. Onderzoek of er al een standaard framework of norm wordt gebruikt binnen jouw sector, of dat het opportuun is om samen met de sector tot een keuze voor een passend framework te komen.

- Leveranciers. Vraag aan jouw leveranciers om rekening te houden met het door jou gekozen framework in hun producten en diensten.

Wees ervan bewust dat een framework lang niet alles tot in detail afdekt. Het kan zijn dat er in jouw organisatie specifieke maatregelen nodig zijn die niet worden beschreven in het gekozen framework. Neem bijvoorbeeld de opslag van gevoelige informatie. In verschillende

frameworks wordt de suggestie gedaan dat een kluis hier een preventieve, fysieke maatregel voor is. Naast het neerzetten van een kluis zal je echter ook rekening moeten houden met aanvullende processen, zoals onderhoud van de kluis (e.g. het tijdig vervangen van een batterij als de kluis een elektronisch slot heeft). Gebruik het framework dus vooral als uitgangspunt, maar wees bedacht op mogelijk aanvullende zaken die van belang zijn voor de weerbaarheid van je organisatie. Wees er op bedacht dat elk framework beperkingen kent. Het kan daarom nuttig zijn meerdere frameworks te bekijken, om zo mogelijke controls te identificeren die je anders over het hoofd zou zien.

Stap 2: Voer een nulmeting uit

Het bestuur is betrokken en er ligt een framework als uitgangspunt. Hiermee kun je aan de slag om de huidige security controls in kaart te brengen.

2.1 Kijk wat je al hebt.

Mogelijk maakt jouw organisatie al gebruik van tooling voor het beheersen van beveiligingsrisico's. Denk aan Information Security Management System (ISMS) tool of een Governance, Risk & Compliance (GRC) tool. Dergelijke tools bieden een veelvoud aan informatie, waaronder een risicoregister en een beschrijving van de (reeds geïmplementeerde) controls. Mocht deze tooling in het verleden gebruikt zijn, dan biedt dit een uitstekend vertrekpunt voor jouw inventarisatie. Wees er wel op bedacht dat deze mogelijk niet up-to-date, noch compleet is.

2.2 Weet bij wie je moet zijn.

De ervaring leert dat veel security controls in de hoofden van mensen zit, maar dat deze informatie niet altijd even duidelijk is vastgelegd. Je zult dus moeten inventariseren welke personen je moet spreken om deze kennis expliciet te maken.

Het kan helpen om terug te vallen op het toebedeelde risico-eigenaarschap als dit duidelijk belegd is. Indien dit niet het geval is, kan het nodig zijn om het hoger management of de bestuurder in te zetten om te verhelderen welke personen de risico-eigenaren (behoren te) zijn.

2.3 Spreek de taal van je stakeholders.

IT-beheerders, inkopers, leveranciers en andere stakeholders zijn meestal geen securityspecialisten, maar hebben doorgaans wel een rol bij het realiseren van bepaalde security controls. Zo zal een HR-adviseur kennis hebben over het aannamebeleid, het uitvoeren van een antecedentenonderzoek of screening, of het opstellen van een geheimhoudingsovereenkomst. De HR-adviseur zal geen kennis hebben van IT-beheersprocessen, maar kan wel een rol spelen in het controleren of de IT-accounts nog overeenkomen met het personeelsbestand. Probeer aan te sluiten bij hun expertise, om vandaaruit te komen op de voor jou relevante informatie. Het kan namelijk voorkomen dat er wel security controls zijn, maar dat deze niet als zodanig door de stakeholder worden herkend.

2.4 Begin klein.

Het in kaart brengen van je security controls kan een uitdagende klus zijn, zeker als dit nog niet eerder is gedaan of is vastgelegd. Afhankelijk van de organisatie kunnen er zo honderden controls worden toegepast zonder dat daar goed zicht op is. Het is daarom verstandig om klein te beginnen. Begin bijvoorbeeld te redeneren vanuit jouw meest urgente risico's, of door je te richten op bepaalde fysieke of digitale segmenten van jouw organisatie.

2.5 Categoriseer je opbrengst.

Tijdens je zoektocht naar security controls is het goed om deze te categoriseren volgens het door jou gekozen framework. Maak in ieder geval inzichtelijk welke functie(s) jouw controls hebben en hoe deze zich verhouden tot jouw organisatie (zie Tabel 1 als voorbeeld). Het door jou gekozen framework kan daar aanvullende handvatten voor bieden, bijvoorbeeld door deze verder onder te verdelen in beschikbaarheids-, integriteits- of vertrouwelijkheidsmaatregelen. Probeer security controls daarbij zoveel mogelijk hiërarchisch op te delen om dit behapbaar te houden: van proces naar activiteiten, van beheersmaatregel naar beveiligingsmaatregelen. Zorg ervoor dat je ook vastlegt waarom deze controls zijn geïmplementeerd, zodat je later kan valideren of deze nog zinvol zijn.

Audits en assessments

Het uitvoeren van een interne/externe of audit of assessment kan ook een overzicht van de door jouw gebruikte security controls opleveren. Dergelijke opdrachten beogen vaak om de blinde vlekken in de beveiligingsinrichting helder te maken, maar kunnen als neveneffect een overzicht van de getroffen maatregelen opleveren. Mocht er sprake zijn van een dergelijke opdracht, probeer dan van de gelegenheid gebruik te maken om hier extra zicht op te krijgen. Door bijvoorbeeld de geïdentificeerde maatregelen te laten plotten op het gekozen control framework.

Stap 3: Hou grip op je controls

De omgeving verandert snel, zeker in de digitale wereld. Security controls die vandaag effectief geïmplementeerd zijn, kunnen morgen onvoldoende zijn. Het is daarom nodig om grip te houden op je controls en deze up-to-date te houden.

3.1 Check het eigenaarschap.

Verschillende teams of personen in jouw organisatie zijn (allicht stilzwijgend) eigenaar van de invulling van een bepaalde security control. Onderzoek of hier afspraken over zijn gemaakt (e.g. volgens het RACI-model[4]) en of deze nog actueel en geldig zijn. Maak, waar nodig, aanvullende afspraken om hierover te rapporteren, bijvoorbeeld bij wijzigingen in de bedrijfsvoering of infrastructuur.

3.2 Toets je controls periodiek.

Security controls moeten logischerwijs doen waarvoor ze bedoeld zijn. Een firewall moet bijvoorbeeld op de juiste manier geconfigureerd zijn om ongewenst binnenkomend verkeer te blokkeren. Je wilt weten of je wachtwoordbeleid voldoende streng is, om accounts goed te beschermen tegen ongeautoriseerde toegang. En een back-up moet regelmatig getest worden om vast te stellen of je weer kunt beschikken over je data.

De control eigenaar maakt inzichtelijk of de security controls nog actueel zijn, of ze ook werken en of ze goed gebruikt worden. Dat kan bijvoorbeeld door het uitvoeren van een penetratietest of door dit mee te nemen in de evaluatie van een incident. Bij een controle kunnen vaak meerdere tests worden uitgevoerd om te bepalen of de control nog voldoende effectief is. Zodra er afwijkingen worden geconstateerd, wordt er een plan opgesteld om die te adresseren.

3.3 Gebruik tools om je controls vast te leggen.

Een actueel overzicht van en inzicht in de security controls (inclusief het eigenaarschap) en de relatie met jouw risico's is een absolute must om je weerbaarheid te bepalen. ISMS en GRC tools kunnen daar een handig hulpmiddel in zijn.

[4] RACI staat voor Responsible, Accountable, Consulted en Informed. Het RACI-model is een matrix die gehanteerd wordt om de rollen en verantwoordelijkheden weer te geven.

Stap 4: Bepaal je weerbaarheid

De inventarisatie van jouw security controls zijn een belangrijke – maar niet de enige – stap in het bepalen van je weerbaarheid. De exacte invulling van hoe je jouw weerbaarheid bepaalt is buiten scope van deze publicatie, maar hou, vanuit het oogpunt van security controls, in ieder geval rekening met het volgende.

4.1 Meet de effectiviteit en test je controls.

Zoals eerder beschreven is het nodig om security controls (periodiek) te toetsen op effectiviteit. De weerbaarheid van jouw organisatie hangt mede samen met de correcte implementatie van de security controls. Neem het testen van je controls mee in het bredere kader van risicomanagement en de PDCA-cyclus.

4.2 Bepaal of je controls geschikt zijn om jouw risico's mitigeren.

Helaas is het niet mogelijk om volledig vrij te zijn van risico's, zelfs niet na het toepassen van security controls. Het is daarom verstandig te streven naar een passend niveau van weerbaarheid, waarbij je oog hebt voor de proportionaliteit en doeltreffendheid van je security controls. Kies voor een gelaagd ontwerp waarbij onafhankelijk geïmplementeerde controls samen een risico mitigeren. Stel vast of de door jou geïdentificeerde security controls voldoende in staat zijn om de dreigingen op je te beschermen belangen te mitigeren. De eerder genoemde firewall is bijvoorbeeld gangbaar voor het voorkomen van intrusies in jouw netwerk, maar is minder effectief in het kader van een insider threat. Gebruik de inventarisatie om een inschatting te maken van de restrisico's en bespreek samen met de risico-eigenaar of deze acceptabel zijn.

4.3 Voer verbeteringen door

Mogelijk kom je tot de conclusie dat jouw controls niet effectief zijn. Stel, in dat geval, een actieplan op om de maatregelen te actualiseren en je risico's acceptabel te houden. Neem hierin mee wie er verantwoordelijk is voor het uitvoeren van deze acties en wie deze verbeteringen controleert. Maak daarbij gebruik van frameworks om eventuele aanvullende maatregelen te identificeren die de restrisico's verder kunnen mitigeren.

Tot slot

Deze publicatie biedt handvatten om grip te krijgen op jouw security controls. Wil je meer weten over hoe je tot een afgeronde risicobeoordeling kan komen? Lees dan ook de publicaties 'Hoe breng ik mijn te-beschermen-belangen in kaart' en 'Hoe breng ik mijn dreigingen in kaart?'.

Tabel 1: Voorbeeld van enkele relevante security controls (maatregelen) ten aanzien van het risicoscenario "datalek als gevolg van phishing via e-mail". De hieronder beschreven categorisering is gebaseerd op het framework NEN-EN-ISO/IEC 27002:2022 NL.

		Control functies			
		Preventief	*Detectief*	*Repressief*	*Correctief*
Type controls	Proces			*Reageren op informatie-beveiligings-incidenten (incident response plan)*	*Onafhankelijke beoordeling van informatie-beveiliging (audit)*
	Technisch	*Toepassing webfilters (filteren op phishing links)*	*Voorkomen van gegevenslekken (monitorsysteem)*	*Bescherming tegen malware (EDR systeem)*	
	Fysiek				
	Mens	*Bewustwording van informatiebeveiliging (bewustwordings-programma)*	*Melden van gebeurtenissen (meldprocedure)*		

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl

Juli 2024