Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Hoe stuur je op effectieve informatiebeveiliging?

Leg de verbinding met jouw organisatie en maak afspraken

versie 1.0 | oktober 2024

Effectieve informatiebeveiliging vereist een samenspel van verschillende disciplines, rollen en informatie in (en rondom) de organisatie. Als CISO (Chief Information Security Officer) heb je een sturende en aanjagende rol in het realiseren van een passend niveau van digitale weerbaarheid. Dit doe je bijvoorbeeld door het (laten) uitvoeren van risicoanalyses en het opstellen van het informatiebeveiligingsbeleid. Belangrijk hierbij is dat je de verbinding zoekt met jouw organisatie. Effectieve informatiebeveiliging vergt immers dat genomen beveiligingsmaatregelen passen bij de risico's die jouw organisatie loopt, maar ook past bij de werkwijzes, cultuur en mogelijkheden van jouw organisatie. Hoe krijg en houd jij de verbinding met jouw organisatie? Wat is jouw rol hierin, en hoe maak jij stapsgewijs verbetering in de informatiebeveiliging? En wat is het nut en noodzaak van het inrichten van governance? In dit artikel geven we een aantal concrete handvatten waarmee je jouw organisatie kan meenemen in het realiseren van effectieve informatiebeveiliging.

Achtergrond

De afgelopen jaren zien we dat diverse ontwikkelingen in de (digitale) 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 zijn er immers nu ook al. Door nu te beginnen, beveiligen organisaties zich niet alleen tegen deze bestaande risico's, maar zijn ze straks ook beter voorbereid op de komst van de nieuwe wetgeving.

De handvatten in deze publicatie zijn ter voorbereiding op de NIS2-richtlijn geschreven, maar kunnen ook in bredere context gebruikt worden om te sturen op effectieve informatiebeveiliging.[1]

Doelgroep

Deze publicatie is geschreven voor personen die binnen hun organisatie verantwoordelijk zijn voor het opstellen van het informatiebeveiligingsbeleid en handvatten zoekt om de organisatie stapsgewijs mee te nemen in het realiseren van effectieve informatiebeveiliging.

Aan deze publicatie hebben bijgedragen

CISO's en adviseurs van Ministerie van Onderwijs, Cultuur en Wetenschap, Enexis en Veiligheidsregio Utrecht.

[1] 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

Effectieve informatiebeveiliging vereist samenwerking

De digitale weerbaarheid van een organisatie vereist een samenspel van iedereen in de organisatie. Of het nu gaat om het (HR-) screeningsbeleid, het volgen van awareness training, het doorvoeren van beveiligingspatches of het vaststellen en accepteren van risico's: meerdere personen in de organisatie hebben een rol in of een belang bij.

In praktijk is nog niet iedere organisatie zo ver dat iedereen bewust is van zijn of haar verantwoordelijkheid, dat er een duidelijk beeld is bij de risico's en weerbaarheid van de organisatie en dat de beveiligingsmaatregelen volledig zijn. De CISO is doorgaans een belangrijke speler om hier inzicht in te krijgen. Bijvoorbeeld door het (laten) uitvoeren van risicoanalyses en het vormgeven van het informatiebeveiligingsbeleid.

Effectieve informatiebeveiliging vereist een samenspel van verschillende disciplines, rollen en informatie in (en rondom) de organisatie. Als CISO heb je een sturende en aanjagende rol in het realiseren van passende digitale weerbaarheid. Bijvoorbeeld door het (laten) uitvoeren van risicoanalyses en het opstellen van het informatiebeveiligingsbeleid. Het is belangrijk dat je hierbij de verbinding zoekt met jouw organisatie. Effectieve informatiebeveiliging vergt immers dat de getroffen beveiligingsmaatregelen passen bij de risico's die jouw organisatie loopt, maar ook de werkwijzes, cultuur en mogelijkheden van jouw organisatie.

Afhankelijk van de organisatie waar jij werkzaam in bent kan er een groot gat zitten tussen de 'ideale' situatie – waarin de juiste personen zich bewust zijn van hun rol in de digitale weerbaarheid van de organisatie – en de praktijk. En toch zal jij als CISO, vanuit jouw eigen context, moeten sturen op effectieve informatiebeveiliging. Hoe doe jij deze sturing effectief? Hoe krijg en houd jij de verbinding met jouw organisatie? Wat is jouw rol hierin, en hoe maak jij stapsgewijs verbetering in de informatiebeveiliging? En wat is het nut en noodzaak van het inrichten van governance? In dit artikel geven we een aantal concrete handvatten waarmee je jouw organisatie kan meenemen in het realiseren van effectieve informatiebeveiliging.

Weet wat jouw (toekomstige) bestuur zoekt in een CISO

Effectieve informatiebeveiliging wordt vaak vormgegeven middels het *three lines (of defense)* model. In dit model wordt er onderscheid gemaakt tussen de volgende rollen:

1. De (eind-) verantwoordelijke: Diegene die de eigenaar is van en verantwoordelijk is voor een bedrijfsproces. Denk bijvoorbeeld aan een bestuurder of een proceseigenaar. De eigenaar van het proces is ook de (eind-) verantwoordelijke voor de beveiliging van dit proces.
2. De risicomanager / kadersteller: Diegene die zich, in het kader van informatiebeveiliging, actief bezig houden met het analyseren van risico's. Hij of zij adviseert de (eind-) verantwoordelijke over deze risico's, heeft een sturende rol bij het identificeren van passende beheersmaatregelen en ondersteunt bij het implementeren van beheersmaatregelen.
3. De (onafhankelijke) auditor: Diegene die de effectiviteit van het risicomanagementproces en de algemene informatiebeveiliging controlleert en hierover rapporteert richting het bestuur. Deze rol kan belegd zijn als onafhankelijk onderdeel van de organisatie, of extern worden vervuld.

Er bestaan in praktijk verschillende opvattingen over wat de rol "CISO" omvat. Organisaties geven vaak een eigen draai bij wat ze zoeken in een CISO. Dit is bijvoorbeeld afhankelijk van de doelstellingen, omvang, cultuur en (digitale) volwassenheid van de organisatie. De meeste (grote) organisaties zien een CISO als adviseur richting risico-eigenaren en ondersteuner bij en/of aanjager van het implementeren van passende beheersmaatregelen. Sommige organisaties hebben behoefte aan een technische CISO die optreedt als eigenaar van (digitale) beveiligingsprocessen, andere organisaties zijn op zoek naar een CISO die invulling geeft aan de (interne) auditkant.

Los van de behoeftes van een organisatie verschillen de kwaliteiten die een CISO heeft. Een CISO kan bijvoorbeeld goed zijn in het behouden van de beveiligings-status-quo, het voldoen aan wet- en regelgeving, of juist sterk zijn in change management. Sommige CISO's zijn sterk in de techniek, waar anderen sterk zijn in bestuurskundinge aspecten of stakeholdermanagement.

Uitdagingen voor effectief CISO-schap

Welk type CISO je ook bent, je zal in ieder geval een passend mandaat en budget nodig hebben om effectief te kunnen zijn. Een aantal indicatoren dat je misschien minder mandaat en budget hebt dan gewenst, zijn:

- De CISO is onderdeel van de IT-organisatie. In dergelijke situaties kan digitale veiligheid gezien worden als een "IT probleem", waarbij de CISO slechts beperkt mandaat heeft.
- De security organisatie heeft geen eigen budget, maar moet dit iedere keer apart aanvragen bij bijvoorbeeld de CIO/CTO.
- Er is geen duidelijke behoefte vanuit het bestuur om geïnformeerd te worden over – of betrokken te zijn bij – de beveiliging in de organisatie.
- De organisatie kent "CISO" als rol, maar deze heeft geen ondersteuning vanuit een security team. Dit kan zijn omdat de organisatie simpelweg aan het groeien is, maar ook omdat de CISO-rol enkel gecreëerd is om te voldoen aan directieve beveiligingskaders (wat niet gelijk staat aan effectieve informatiebeveiliging).
- De CISO heeft naast de adviserende en uitvoerende rol ook een controlerende (audit) rol. Deze rollen zijn niet te combineren.

Om effectief te kunnen zijn moet jouw visie over het CISO-schap dan ook aansluiten bij de visie van het bestuur, de volwassenheid en de behoefte van de organisatie. Zorg ervoor dat je hier een goed beeld van krijgt. Dit doe je bij voorkeur al tijdens jouw sollicitatiegesprekken. Stel vragen om te achterhalen of er een match is tussen jou en de organisatie, zoals:

- Hoe belangrijk is informatiebeveiliging voor jou? En wat maakt dat zo belangrijk?
- Welke verwachtingen heb je voor mij in deze rol? Aan wie rapporteer ik?
- Op welke manier is digitale weerbaarheid ingebed in de organisatie? Hoe wordt hier op samengewerkt?
- Hoe ziet de security organisatie er uit? Uit wie bestaat het team en beschikt het team over een eigen budget?
- Is er een security roadmap? En zo nee, moet die er komen (en waarom, volgens jou)?
- Wat zijn de belangrijkste doelstellingen van de organisatie waar ik een bijdrage aan kan leveren? Welke grote veranderingen komen er aan voor de organisatie?

Afhankelijk van de antwoorden die jij krijgt bij deze vragen kan je een beeld schetsen bij de belangrijkste uitdagingen van de organisatie en of jij de rol passend en naar verwachting in kan vullen.

Ken jouw organisatie

Informatiebeveiligingsbeleid is alleen effectief als het past bij de cultuur, strategie, missie, visie, omvang en werkwijze van de organisatie. Zo kan een omvangrijke organisatie gebaat zijn bij een sterk gedefinieerd bestuursmodel, waar andere organisaties veel meer behoefte hebben aan het creëren van security awareness en informeel contact. Verdiep je in de organisatie om er achter te komen wat het karakter is van jouw organisatie en hoe jij daar het beste op kan aansluiten.

Veel mensen in de organisatie zullen (misschien zonder het te weten) een rol hebben in informatiebeveiliging. Zo heeft IT-beheer een uitvoerende taak op het gebied van patch management en daarmee ook het dichten van kwetsbaarheden. En HR zal, bij de indiensttreding van nieuwe medewerkers, een rol hebben in het informeren over het beveiligingsbeleid. Uiteindelijk zijn al deze medewerkers de oren, ogen en handen van de organisatie. Ze hebben een belangrijke rol in het identificeren en mitigeren van risico's.

Ga in gesprek met de medewerkers en externe partners. Zorg ervoor dat je goed begrijpt waar jouw organisatie voor staat, wat belangrijk is voor jouw organisatie en hoe verschillende afdelingen en technische systemen daaraan bijdragen. Als CISO is het *de facto* jouw taak om mensen te laten beseffen dat ook zij een belangrijk rol hebben ten aanzien van de digitale weerbaarheid. Dit kan je op de volgende manieren in de praktijk brengen:

- **Leg contact met jouw collega's**
  Ga het gesprek aan met de medewerkers. Gebruik hiervoor bijvoorbeeld een lijstje namen dat je hebt meegekregen vanuit het bestuur. Onderzoek welke rol zij hebben in de organisatie en hoe zij hun rol zien ten aanzien van digitale weerbaarheid. Probeer raakvlakken te vinden waar je samen vanuit kan werken. Stel vragen als:

- Waar maak jij je zorgen over? Wat is volgens jou belangrijk voor onze organisatie? [2]
- Wat houdt je nu bezig en welke uitdagingen heb je in jouw werk?
- Hoe kijk jij naar informatiebeveiliging? Hoe zie jij jouw rol ten aanzien van informatiebeveiliging en deel je de mening dat jij hier een rol in hebt?
- Wat vind jij dat er goed gaat (t.a.v. informatiebeveiliging)? Doen we de juiste dingen? En zijn er dingen die er beter kunnen?
- Waar loop je tegenaan (t.a.v. informatiebeveiliging) en hoe kan ik je helpen om jouw werk gemakkelijker te maken?

- **Wie moet ik nog spreken?**
  Uiteindelijk is het belangrijk om een netwerk op te bouwen zodat jij grip krijgt op het wel en wee van de organisatie. Vraag aan het einde van (kennismakings-) gesprekken 'wie zou ik nog meer moeten spreken?' om stapsgewijs de organisatie te leren kennen. Ga vooral ook het gesprek aan met diegene die informatiebeveiliging ervaren als hinderlijk of lastig. Zij kunnen je wijzen op drempels die je mogelijk weg kan of moet halen om effectief te zijn.

- **Houd een *security roadshow***
  Organiseer interactieve sessies met verschillende afdelingen waarbij je het belang van informatiebeveiliging benadrukt. Overweeg een realistische demonstratie te geven, die aansluit bij de dagelijkse praktijk van jouw toehoorders, om het belang van beveiliging te laten zien. Gebruik deze sessies voor het creëren voor bewustwording, maar zoek vooral naar de behoeftes van verschillende afdelingen.

- **Onderzoek wat er al ligt in de organisatie**
  Consulteer GRC (Governance, Risk, Compliance) tooling, risico-registers, en eerder uitgevoerde assessment/audits om grip te krijgen op de huidige weerbaarheid en inrichting van de organisatie. Is er bijvoorbeeld een security roadmap? Zijn er eerder problemen geconstateerd, of afspraken gemaakt over rapporteren en verantwoordelijkheden?

Werk stapsgewijs naar effectieve informatiebeveiliging

De (context van jouw) organisatie is continu in beweging. Ontwikkel een visie en roadmap waar mee je vorm geeft aan de toekomstige informatiebeveiliging. Besef je dat informatiebeveiliging geen bestemming is, maar een reis met verschillende tussenstations. Om de informatiebeveiliging naar het volgende niveau te tillen zal je dan ook stapsgewijs moeten werken. Houd hierbij rekening met het volgende:

- **Meten is weten**
  Het nemen van beveiligingsmaatregelen leidt niet altijd tot een verbetering van de beveiliging van de organisatie. Maak vooraf duidelijk welk effect je wilt bereiken en stel goede KPIs op om dit effect te kunnen meten.

- **Doe het stap-voor-stap:**
  Maak veranderingen in een meerdere kleine stappen om de organisatie hier stapsgewijs in mee te nemen. Op deze manier waarborg je dat de organisatie tijd heeft om veranderingen te absorberen en dat informatiebeveiliging niet als een grote last wordt ervaren.

- **Prioriteer jouw beoogde veranderingen.**
  Afhankelijk van jouw visie en de behoefte van de organisatie zal je de voorkeur hebben om bepaalde stappen eerst te nemen. Prioriteer deze op basis van de meest urgente risico's[3], zodat je gericht kan sturen op de meest effectieve maatregelen.

[2] Wil je meer weten over het in kaart brengen van datgene dat jouw organisatie wil beschermen? Lees dan ook de publicatie: Hoe breng ik mijn te beschermen belangen in kaart?

[3] Wil je meer weten over het prioriteren van risico's? Lees dan ook de publicatie: www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/herkennen/hoe-bepaal-ik-de-meest-relevante-risicos

Effectieve KPI's

Om grip te krijgen over de effectiviteit van (veranderingen in) de informatiebeveiliging is het belangrijk om te meten. Goede Key Performance Indicators (KPI's) kunnen hierbij helpen. Maak KPIs zo volledig mogelijk en fit-for-purpose, waarbij je rekening houdt met de behoefte van de stakeholder die de (rapportage over) KPIs zal gebruiken. Een goede KPI kent context die iets zegt over de (security) performance. Voor de effectiviteit van het proces "patch management" zegt de KPI "het aantal kwetsbaarheden in het softwareportfolio" bijvoorbeeld weinig. Voorbeelden van betere KPI's zijn de "mean-time-to-patch" (de gemiddelde tijd tussen het beschikbaar komen van een patch en het doorvoeren hiervan) of "Het *relatieve* aantal *onverholpen* kwetsbaarheden in het softwareportfolio waar wel een patch voor beschikbaar is". En voor een bestuurder is de KPI "totaal aantal incidenten" niet zo relevant als "De mate van verstoring van de bedrijfsvoering als gevolg van beveiligingsincidenten". KPI's kunnen zowel kwantitatief als ook kwalitatief zijn. Kies de vorm die het beste bij jouw organisatie past.

- **Maak gebruik van momentum.** Niet alle veranderingen die jij wilt doorvoeren zullen op evenveel draagvlak kunnen rekenen. Wanneer er aandacht is voor bepaalde ontwikkelingen – zoals een groot (intern of extern) beveiligingsincident, of een verandertraject, kan het momentum wat hierdoor wordt gecreëerd gebruikt worden voor verbetering van de informatiebeveiliging.

- **Stel je dienstbaar op.** Digitale beveiliging is voor veel mensen een ver-van-je-bed-show is, of kan worden ervaren als een 'last'. Redeneer vanuit de visie dat informatiebeveiliging de bedrijfsvoering moet dienen. Als je iets van anderen verwacht, help ze dan ook omdat mogelijk te maken. Neem een onderzoekende houding aan en kom tot een passende oplossing die aansluit bij de manier van werken van jouw organisatie.

Maak afspraken om effectief te kunnen blijven opereren

(Informeel) contact houden met de organisatie is belangrijk om voldoende zicht te houden op de risico's. Om veranderingen effectief door te voeren is het belangrijk om afspraken te maken over de verantwoordelijkheden en taken. Bijvoorbeeld over het uitvoeren van bepaalde beveiligingsmaatregelen of het rapporteren over hun effectiviteit. Dergelijke afspraken hebben voornamelijk het doel om duidelijkheid te creëren en misverstanden te voorkomen. Ook bieden afspraken handvatten voor escalatie. Bijvoorbeeld als afspraken niet worden nagekomen of als er een onoverkomelijk meningsverschil is tussen jou als CISO en een risico-eigenaar.

Door afspraken te maken en te formaliseren (*governance*) voorkom je gedoe achteraf en zorg je ervoor dat je als CISO een passend mandaat hebt. Maak afspraken over:

- **Reguliere contact-/afstemmomenten.** Om een vinger aan de pols te houden is het verstandig om periodiek af te stemmen met jouw (belangrijkste) stakeholders. Denk bijvoorbeeld aan informatieve gesprekken met bestuurders en overige risico-eigenaren, maar ook overleggen waar besluiten worden genomen.

- **Verantwoordelijkheden en bevoegdheden.** Effectieve informatiebeveiliging vereist dat het voor iedereen duidelijk is wie waarvoor verantwoordelijk en bevoegd is. Overweeg het gebruik van het RA(S)CI model. Met dit model beschrijf je per beheersmaatregel: wie er verantwoordelijk (R) en aansprakelijk (A) is, wie er ondersteuning (S) biedt of geraadpleegd (C) wordt, en hierover geinformeerd (I) dient te worden. Door een dergelijke tabel op te stellen houdt jouw organisatie grip op de verantwoordelijkheden ten aanzien van informatiebeveiliging.

- **Rapportage en KPIs.** Verschillende stakeholders zullen behoefte hebben aan (periodieke) rapportages rondom de beveiliging van de organisatie. Spreek af op welke manier en met welke frequentie er gerapporteerd wordt. Bespreek wat de belangrijkste behoefte is van jouw stakeholders en betrek ze bij het opstellen van passende en haalbare KPI's.

- **Escalatie en escalatielijnen.** Idealiter worden afspraken nagekomen en kan jij als CISO een passende oplossing vinden met de betreffende risico-eigenaar. Helaas kan het gebeuren dat jullie er niet uitkomen. Bijvoorbeeld als beoogde beveiligingsmaatregelen ervaren worden als een te zware belasting op de bedrijfsvoering. In dat geval is het belangrijk om afspraken te hebben over hoe een dergelijk probleem op hoger niveau beslecht kan worden. Maak duidelijk onder welke omstandigheden een dergelijke opschaling *moet* en *kan* plaatsvinden en hoe dat proces eruit ziet, zodat de organisatie profiteert van tijdige besluitvorming.

Afspraken en processen zijn alleen effectief als deze gedragen worden door de organisatie. Zorg ervoor dat afspraken bekrachtigd worden door (schriftelijke) instemming van de relevante onderdelen van de organisatie.

Afspraken vastleggen kan op verschillende manieren. Kies vooral iets dat past bij jouw organisatie. Dat kan specifieke GRC-tooling zijn, maar ook een (bedrijfs-)wiki of simpele spreadsheet kunnen voldoen. Bestaande raamwerken en normenkaders, zoals de ISO27001 of het NIST CSF kunnen je helpen om richting te geven over de noodzakelijke afspraken.

Tot slot

Effectief sturen op informatiebeveiliging vereist zowel informeel contact als ook heldere, formele afspraken. Maak gebruik van jouw sociale vaardigheden en redeneer vanuit de bedrijfsdoelstellingen om jouw organisatie stapsgewijs op een passend niveau van digitaal weerbaarheid te krijgen.

Wil je meer weten over dit onderwerp? Op Risicomanagement Routekaart, Governance en randvoorwaarden geven we nog een aantal aanvullende en verdiepende inzichten voor het inbedden en beheren van het risicomanagementproces in jouw organisatie.

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
@ncsc_nl

Oktober 2024