# Handleiding CISO-niveau: uw organisatie beschermen

## Een risicogebaseerd informatiebeveiligingsprogramma ontwikkelen

**1. Identificeer de soorten informatie die uw bedrijf opslaat en gebruikt**
⇒ Maak een overzicht van alle soorten informatie die uw bedrijf opslaat of gebruikt (bijv. klantnamen en e-mail).

**2. Bepaal de waarde van uw informatie**
⇒ Stel belangrijke vragen voor elke informatiesoort:

- Wat zou er gebeuren als deze informatie openbaar werd gemaakt?
- Wat zou er met mijn bedrijf gebeuren als deze informatie onjuist was, bijvoorbeeld als de integriteit van de gegevens was aangetast?
- Wat zou er met mijn bedrijf gebeuren als ik/mijn klanten geen toegang had(den) tot deze informatie?

**3. Een inventaris opstellen**
⇒ Identificeer welke technologie in contact komt met de informatie die u hebt geïdentificeerd. Dit kan hardware (bijv. computers) en softwareapplicaties (bijv. browsere-mail) omvatten. Voeg het merk, model, serienummer en andere identificatoren toe. Ga na waar elk product zich bevindt. Bepaal voor software op welke computer(s) deze software wordt gebruikt.
⇒ Kijk hierbij, indien van toepassing, ook naar technologieën buiten uw bedrijf (bijv. “de cloud”) en alle beveiligingstechnologieën waarover u beschikt, zoals firewalls.

**4. Weten waar uw dreigingen en zwakke plekken zitten**
⇒ Bespreek regelmatig met welke dreigingen en zwakke plekken de financiële sector te maken kan krijgen en schat in hoe groot de kans is dat u getroffen wordt. (Uw nationale CERT, FS-ISAC, uw lokale InfraGard-afdeling etc. kunnen u hierover meer vertellen.)
⇒ Voer ten minste eenmaal per jaar een kwetsbaarheidsscan of -analyse uit.

**5. Een cyberbeveiligingsbeleid opzetten**
⇒ Werk samen met het senior management van uw organisatie om een cyberbeveiligingsstrategie op basis van internationale, nationale en industrienormen en -richtlijnen te ontwikkelen en uit te voeren die is afgestemd op de bovenstaande risico’s. Richtlijnen zoals het NIST Cybersecurity Framework, de Cybersecurity Assessment Tool van de FFIEC (Federal Financial Institutions Examination Council) en ISO 27001 kunnen de basis vormen voor het uitbouwen en verbeteren van dergelijk beleid.
⇒ Geef alle medewerkers training over de details van het beleid en laat ze documenten ondertekenen waarin ze toezeggen dit beleid te zullen naleven om de cyberbeveiliging van uw organisatie te allen tijde te waarborgen.

## Schade door malware voorkomen

⇒ Activeer uw firewall en stel toegangscontrolelijsten (access control lists, ACL’s) in om een bufferzone te creëren tussen uw netwerk en het internet. Beperk de toegang door gebruik te maken van een whitelisting-instelling, waarbij bepaalde IP-adressen of -services niet op de zwarte lijst komen.
⇒ Gebruik antivirussoftware en antispyware op alle computers en laptops.
⇒ Update alle software en firmware door de nieuwste software-updates van fabrikanten en leveranciers onmiddellijk toe te passen. Maak waar mogelijk gebruik van de optie ‘Automatisch bijwerken’.
⇒ Geef alleen IT-medewerkers met beheerdersrechten de bevoegdheid om nieuwe programma’s te installeren.
⇒ Houd activiteitenlogboeken bij die worden gegenereerd door beveiligings-/detectiehardware of -software en monitor deze. Bescherm logboeken met wachtwoordbeveiliging en encryptie.
⇒ Houd alle hostclocks gesynchroniseerd. Als de apparaten van uw organisatie niet allemaal dezelfde klokinstelling hebben, zal de gebeurteniscorrelatie veel moeilijker zijn als er incidenten plaatsvinden.
⇒ Beheer toegang tot verwijderbare media zoals SD-kaarten en USB-sticks. Moedig medewerkers aan om bestanden via e-mail of cloudopslag over te dragen. Informeer personeel over de risico’s van het gebruik van USB’s van externe bronnen of het uitlenen van hun eigen USB’s aan anderen.
⇒ Stel voor uw e-mailservices e-mailbeveiliging en spamfilters in.
⇒ Beveilig alle pagina’s op uw openbare websites met encryptie en andere beschikbare tools.
⇒ Overweeg om de beveiliging van de activa en systemen van uw organisatie te laten beoordelen door een penetratietestservice.

## Medewerkers trainen

⇒ Laat nieuwe medewerkers verplichte cyberbeveiligingstrainingen volgen en train alle huidige medewerkers op gezette tijden, maar minimaal eenmaal per jaar. Verplicht medewerkers om:

- Sterke wachtwoorden te gebruiken op alle werkapparaten en -accounts en moedig hen aan om hetzelfde te doen op hun eigen apparaten en om een wachtwoordmanager te gebruiken,
- Alle besturingssystemen, software en applicaties actueel te houden op alle apparaten,
- Op alle accounts tweeledige verificatie te gebruiken,
- Accountgegevens en toegangskaarten bij afwezigheid veilig en vergrendeld achter te laten,
- Geen accountgegevens of andere gevoelige gegevens te delen via niet-versleutelde e-mail of andere open communicatie,
- Bijlagen niet direct te openen of op links in ongevraagde of verdachte e-mails te klikken,
- Eerst na te gaan of een verdachte e-mail of verdacht pop-upvenster betrouwbaar is voordat ze persoonlijke informatie verstrekken, en goed te kijken naar het e-mailadres, en
- Mogelijke interne of externe beveiligingsincidenten, dreigingen of verkeerde behandeling van gegevens of apparaten te melden bij het technisch personeel van uw organisatie en/of het hoger management.

⇒Ga na of medewerkers zich bewust zijn van de risico’s door geregeld bij wijze van test zelf phishing-e-mails te verzenden vanaf nepaccounts. Ga niet met vingers wijzen als medewerkers hierin trappen, maar maak er een leermoment van.

# Uw gegevens beschermen

⇒ Maak geregeld back-ups van uw belangrijke gegevens (zoals documenten, e-mails en kalenders) en test of ze hersteld kunnen worden. Zet eventueel een back-up in de cloud.
⇒ Zorg ervoor dat het apparaat waarop uw back-up staat niet permanent is aangesloten op het apparaat waarop de originele gegevens zijn opgeslagen, noch fysiek noch via een lokaal netwerk.
⇒ Installeer overspanningsbeveiligers, gebruik generatoren en zorg ervoor dat al uw computers en kritieke netwerkapparaten zijn aangesloten op een noodstroomvoorziening.
⇒ Gebruik een oplossing voor het beheer van mobiele apparaten (Mobile Device Management [MDM]).

# Uw apparaten veilig houden

⇒ Schakel PIN en wachtwoordbeveiliging voor mobiele apparaten in. Configureer apparaten zo dat ze bij verlies of diefstal kunnen worden getraceerd en op afstand kunnen worden gewist of vergrendeld.
⇒ Houd uw apparaten (en alle geïnstalleerde apps) waar mogelijk up-to-date via de optie 'Automatisch bijwerken'.
⇒ Maak bij het verzenden van gevoelige gegevens geen verbinding met openbare wifihotspots – gebruik mobiele verbindingen (inclusief tethering en draadloze dongles) of VPN's.
⇒ Vervang apparaten die niet langer door fabrikanten worden ondersteund door nieuwe exemplaren.
⇒ Stel meldprocedures in voor verloren of gestolen apparatuur.

# Wachtwoorden gebruiken

⇒ Zorg ervoor dat alle computers versleutelingsproducten gebruiken waarbij een wachtwoord nodig is om het apparaat op te starten. Schakel wachtwoord- of PIN-beveiliging voor mobiele apparaten in.
⇒ Gebruik sterke wachtwoorden en vermijd voorspelbare wachtwoorden (zoals passw0rd) en persoonlijke identificatiegegevens (zoals namen van familieleden of huisdieren). Instrueer alle medewerkers om hetzelfde te doen.
⇒ Gebruik waar mogelijk tweeledige verificatie (two-factor authentication of 2FA).
⇒ Wijzig de door de fabrikant verstrekte standaardwachtwoorden op alle apparaten, inclusief netwerk- en IoT-apparaten, voordat ze aan medewerkers ter beschikking worden gesteld.
⇒ Zorg ervoor dat medewerkers gemakkelijk hun eigen wachtwoorden opnieuw kunnen instellen. U kunt medewerkers ook vragen om hun wachtwoord regelmatig te wijzigen (bijv. driemaandelijks, halfjaarlijks of jaarlijks).
⇒ Maak eventueel gebruik van een wachtwoordmanager. Als u gebruikmaakt van een dergelijke manager, zorg er dan voor dat een sterk hoofdwachtwoord (dat toegang biedt tot al uw andere wachtwoorden) wordt gekozen.

# Bevoegdheden beheren

⇒ Zorg ervoor dat alle medewerkers uniek identificeerbare accounts hebben die telkens wanneer ze inloggen op uw systemen worden geverifieerd.
⇒ Geef alleen beheerdersrechten aan vertrouwde IT-medewerkers en belangrijke personeelsleden en zorg dat standaardgebruikers niet langer beheerdersrechten op werkstations hebben.
⇒ Geef medewerkers alleen toegang tot de specifieke gegevenssystemen die ze nodig hebben voor hun werk en zorg ervoor dat ze geen software zonder toestemming kunnen installeren.
⇒ Controleer de fysieke toegang tot uw computers en creëer voor alle medewerkers gebruikersaccounts.

# Uw wifinetwerken en -apparaten beveiligen

⇒ Zorg ervoor dat uw bedrijfswifi veilig en versleuteld is met WPA2. Encryptie is op routers vaak uitgeschakeld, dus zorg ervoor dat u deze inschakelt. Beveilig de toegang tot de router en zorg ervoor dat het standaard ingestelde wachtwoord wordt bijgewerkt. Schakel alle functies voor het beheer op afstand uit.
⇒ Stel uw draadloze toegangspunt of router zo in dat dit/deze de naam van het netwerk niet uitzendt, ook wel bekend als de Service Set Identifier (SSID).
⇒ Beperk de toegang tot uw wifinetwerk door alleen apparaten toe te staan met bepaalde Media Access Control-adressen. Als klanten wifi nodig hebben, stel dan een apart openbaar netwerk in.
⇒ Schakel het Dynamic Host Configuration Protocol (DHCP) in op uw netwerkapparaten, zodat u eenvoudig alle apparaten kunt traceren die toegang hadden tot uw netwerk.
⇒ Log uit als beheerder nadat u de router hebt geïnstalleerd.
⇒ Houd de software van uw router up-to-date. Blijf op de hoogte van updates door uw router bij de fabrikant te registreren en u aan te melden om updates te ontvangen.

# Phishingaanvallen vermijden

⇒ Zorg ervoor dat het personeel niet op het internet surft of e-mails checkt op servers of vanaf een account met beheerdersrechten.
⇒ Stel web- en e-mailfilters in. Overweeg om de toegang van medewerkers tot websites die vaak in verband worden gebracht met cyberdreigingen te blokkeren.
⇒ Leer medewerkers om duidelijke tekenen van phishing te herkennen, zoals spel- en grammaticafouten of slechte imitaties van bekende logo's. Ziet het e-mailadres van de verzender er legitiem uit?
⇒ Scan op malware en wijzig wachtwoorden zo snel mogelijk als u vermoedt dat er een aanval heeft plaatsgevonden. Straf medewerkers niet als ze het slachtoffer worden van een phishingaanval (ze zullen dan niet snel meer geneigd zijn om dergelijke aanvallen te melden).