Capaciteitsopbouw cyberbeveiliging Toolbox voor financiële organisaties

Handleiding directieniveau: Leiderschap in cyberbeveiliging

Grondbeginselen van het beheer van cyberrisico's

Bevestig dat u de volgende vragen met ja kunt beantwoorden:

1. Voldoet uw organisatie aan de **toepasselijke vereisten van wet- en regelgeving**?

2. Heeft uw organisatie **haar cyberblootstellingen gekwantificeerd en haar financiële veerkracht** getest?

3. Heeft uw organisatie een **verbeterplan** om te zorgen dat blootstellingen binnen uw afgesproken risicobereidheid vallen?

4. Bespreekt de raad van bestuur regelmatig **beknopte, duidelijke en bruikbare informatie met betrekking tot de cyberveerkracht van de organisatie die het management heeft aangeleverd**?

5. Heeft uw organisatie **incidentresponsplannen die onlangs zijn geoefend**, ook op directieniveau?

6. Zijn de **rollen van degenen die verantwoordelijk zijn voor het beheer van cyberrisico's** duidelijk en in overeenstemming met de drie verdedigingslijnen?

7. Beschikt u over een **onafhankelijke validatie en waarborg** van de beveiligingsmentaliteit van uw organisatie ten aanzien van cyberrisico's?

Toezicht

Als het hoogste leiderschapsniveau binnen uw organisatie heeft de raad van bestuur de eindverantwoordelijkheid voor het beheersen van cyberrisico's en moet daarom toezicht houden op de strategie, het beleid en de activiteiten van de organisatie op dit gebied. De raad van bestuur moet specifiek:

⇒ De eindverantwoordelijkheid nemen voor het toezicht op cyberrisico en veerkracht, hetzij als volledige raad of door het delegeren van toezicht aan een specifieke commissie van de raad van bestuur.
⇒ Eén bedrijfsfunctionaris aanwijzen, meestal de centrale informatiebeveiligingsfunctionaris (CISO), die verantwoording aflegt over de capaciteit van uw organisatie om cyberveerkracht en vooruitgang bij het implementeren van doelstellingen op het vlak van cyberveerkracht te beheren. Ervoor zorgen dat deze functionaris standaard toegang heeft tot de raad en voldoende bevoegdheid, kennis van het onderwerp, ervaring en middelen heeft om deze taken uit te voeren.
⇒ Jaarlijks de risicotolerantie van uw organisatie bepalen en zorgen dat deze is afgestemd op uw bedrijfsstrategie en risicobereidheid.
⇒ Ervoor zorgen dat er jaarlijks een formele, onafhankelijke cyberveerkrachtbeoordeling van uw organisatie wordt uitgevoerd.
⇒ Toezicht houden op de opzet, de implementatie, het testen en de voortdurende verbetering van de plannen voor cyberveerkracht, zodat uw organisatie op één lijn ligt en uw CISO of een andere verantwoordelijke functionaris regelmatig verslag hierover uitbrengt aan de raad van bestuur.
⇒ Cyberveerkracht en risicobeoordeling in de algemene bedrijfsstrategie van uw organisatie, in het risicobeheer, de budgettering en de toewijzing van middelen integreren, met als doel ervoor te zorgen dat cyberrisico's volledig worden meegenomen in het totale operationele risico.
⇒ Regelmatig uw prestaties op bovenstaande punten beoordelen en eventueel onafhankelijk advies voor continue verbetering inwinnen.

Op de hoogte blijven

De effectiviteit van het toezicht op cyberrisico's door de raad van bestuur hangt af van de aanwezige kennis van het onderwerp bij de leden en het op de hoogte zijn van actuele informatie.

⇒ Ervoor zorgen dat alle leden die toetreden tot de raad beschikken over de juiste en actuele vaardigheden en kennis om de risico's van cyberaanvallen te begrijpen en te beheren.
⇒ Het management regelmatig om advies vragen over de huidige en toekomstige risicoblootstelling van uw organisatie, relevante regelgevingsvereisten, en benchmarks voor risicobereidheid uit de branche en de maatschappij als geheel. Daarnaast houdt de raad regelmatig briefings over de laatste ontwikkelingen met betrekking tot bedreigingen en het regelgevingsklimaat, plant en overlegt samen met collega's en leiders in de cyberbeveiliging en wisselt op directieniveau informatie over governance en rapportage uit.
⇒ Het management herinneren aan zijn verantwoordelijkheid om een gekwantificeerde en begrijpelijke beoordeling van cyberrisico's, bedreigingen en gebeurtenissen te geven als standaard agendapunt tijdens raadsvergaderingen.
⇒ Ervoor zorgen dat iedereen op de hoogte is van voortdurende uitdagingen voor systemen, zoals kwetsbaarheden in de toeleveringsketen, wederzijdse afhankelijkheden en het onvoldoende delen van informatie over cyberrisicobeheer tussen raden onderling.

De toon zetten

Naast het senior management moet de raad van bestuur de kernwaarden, risicocultuur en verwachtingen van uw organisatie met betrekking tot cyberveerkracht vaststellen en uitdragen.

⇒ Een cultuur bevorderen waarin medewerkers op alle niveaus hun belangrijke verantwoordelijkheden voor het behoud van cyberveerkracht in uw organisatie kennen. Het goede voorbeeld geven.
⇒ Toezien op de rol van het management bij het bevorderen en onderhouden van de risicocultuur van uw organisatie. De risicocultuur promoten, bewaken en beoordelen, rekening houdend met de impact van cultuur op veiligheid en gezondheid en waar nodig veranderingen doorvoeren.
⇒ Duidelijk maken dat van alle medewerkers wordt verwacht dat zij integer handelen en geconstateerde gevallen van niet-naleving binnen of buiten uw organisatie onmiddellijk melden.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE

Capaciteitsopbouw cyberbeveiliging Toolbox voor financiële organisaties

Handleiding CEO-niveau: Leiderschap in cyberbeveiliging

Bestuur

De cyberbeveiliging van uw organisatie staat of valt met het hoogste managementniveau. De CEO moet samen met de raad van bestuur de risico's begrijpen en de eindverantwoordelijkheid nemen voor de cyberbeveiligingsactiviteiten en -medewerkers in de organisatie. U moet:

⇒ Een centrale informatiebeveiligingsfunctionaris (chief information security officer [CISO]) aanwijzen indien dit nog niet gebeurd is of, als de middelen hiervoor niet toereikend zijn, iemand binnen uw organisatie aanwijzen om de rol van CISO op zich te nemen.
⇒ Samenwerken met de CISO of ander technisch personeel om een cyberbeveiligingsstrategie en -kader op te stellen en toe te passen die is afgestemd op de specifieke cyberrisico's van de organisatie op basis van internationale, nationale en industrienormen en -richtlijnen.
⇒ Duidelijke rollen en verantwoordelijkheden formuleren voor medewerkers die de cyberbeveiliging van de organisatie implementeren en beheren.

- Samenwerken met de CISO om de juiste cyberbeveiligingsrollen en toegangsrechten voor alle personeelsniveaus vast te stellen.
- In goede banen leiden van communicatie en samenwerking om ervoor te zorgen dat cyberbeveiligingsmanagement holistisch is, vooral als verantwoordelijkheden op het gebied van cyberbeveiliging worden gedeeld door meerdere medewerkers of divisies binnen de organisatie (zoals het hebben van aparte verticale structuren voor informatiebeveiliging, risico's en technologie).

⇒ Ervoor zorgen dat de CISO weet bij wie hij moet zijn om u en de raad van bestuur tijdig op de hoogte te brengen van bedreigingen.
⇒ De CISO of ander technisch personeel vragen om het senior management geregeld te briefen.
⇒ Ervoor zorgen dat het beveiligingsbeleid, de normen, handhavingsmechanismen en procedures van de organisatie uniform zijn in alle teams en bedrijfsonderdelen.

Risicobeoordeling en -beheer

Om te zorgen voor een sterk bewustzijn van cyberbeveiliging en voorbereid zijn voor als het misgaat, moeten risico's continu geanalyseerd worden. De cyberbeveiliging van uw organisatie kan worden verbeterd door:

⇒ Risicobeoordeling en beheer van cyberbeveiliging als prioriteit vast te stellen binnen de bredere risicobeheer- en bestuursprocessen van uw organisatie. Samen te werken met uw CISO of ander technisch personeel aan een plan voor uitvoering van een risicobeoordeling die het volgende omvat:

- Beschrijven van de activa van uw organisatie en de mate waarin deze afhankelijk zijn van technologie,
- Beoordelen van de volwassenheid van uw organisatie en de inherente risico's die aan de technologische afhankelijkheid van haar activa kleven,
- Bepalen van de gewenste volwassenheid van uw organisatie,
- Begrijpen waar cyberdreigingen in de lijst met risicoprioriteiten van uw organisatie staan,
- Vaststellen in hoeverre uw huidige cyberbeveiligingsstatus overeenkomt met de gewenste doelstatus,
- Implementeren van plannen om volwassenheid te bereiken en in stand te houden,
- Voortdurend opnieuw evalueren van de volwassenheid, risico's en doelen van uw organisatie op het vlak van cyberbeveiliging, en
- Overwegen om derden penetratietesten of 'red teaming-oefeningen' te laten uitvoeren,
- Overwegen om beveiligingsmaatregelen te nemen, zoals de aanschaf van een cyberverzekering.

⇒ De inspanningen van werknemers tijdens het risicobeoordelingsproces te kanaliseren om ervoor te zorgen dat de organisatie snel kan reageren.
⇒ De resultaten van de risicobeoordeling te analyseren en presenteren zodat het management, maar ook de belangrijke stakeholders en de raad van bestuur, toezicht kunnen uitoefenen.
⇒ Toezicht te houden op alle veranderingen zodat de organisatie zoals gewenst of adequater kan reageren op cyberdreigingen, waarbij alle maatregelen die worden genomen om de cyberbeveiliging te verbeteren afgestemd moeten zijn op de risico's en betaalbaar moeten zijn voor uw organisatie.
⇒ Toe te zien op de effectiviteit van continue monitoring om slagvaardig en flexibel te kunnen blijven reageren op cyberrisico's die zich voordoen.

Organisatiecultuur

De cyberbeveiliging van uw organisatie is geen eenmalige klus die door een handjevol medewerkers geklaard kan worden; het is een factor om rekening mee te houden bij alle zakelijke beslissingen en activiteiten en iets waar alle medewerkers een rol in blijven spelen. Doe het volgende om ervoor te zorgen dat de cyberbeveiliging door de hele organisatie heen continu op peil blijft:

⇒ Voer cyberbeveiligingsgesprekken met het leiderschapsteam en communiceer regelmatig met het personeel dat verantwoordelijk is voor het beheer van cyberrisico's.
⇒ Geef alle nieuwe medewerkers een cyberbeveiligingstraining, zorg ervoor dat alle medewerkers op de hoogte zijn van het cyberbeveiligingsbeleid van uw organisatie – en laat ze documenten ondertekenen waarin ze toezeggen dit beleid na te leven – en zorg ervoor dat uw IT-afdeling of ander technisch personeel hen heeft ingelicht over best practices.
⇒ Laat alle medewerkers periodiek cyberbeveiligingstrainingen volgen met betrekking tot hun beveiligingsverantwoordelijkheden op korte en lange termijn.
⇒ Zorg ervoor dat uw organisatie cyberbeveiliging altijd laat meewegen bij de keuze van potentiële leveranciers en het delen van gegevens met derden.
⇒ Beoordeel jaarlijks het cyberbeveiligingsbeleid van uw organisatie.
⇒ Stimuleer de vrijwillige informatie-uitwisseling over cyberdreigingen en incidenten binnen uw organisatie en met betrouwbare concurrenten.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE

Capaciteitsopbouw cyberbeveiliging Toolbox voor financiële organisaties

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).

Capaciteitsopbouw cyberbeveiliging Toolbox voor financiële organisaties

Handleiding CISO-niveau: uw klanten beschermen

Individueel advies voor klanten en medewerkers om financiële gegevens te beschermen

Adviseer uw medewerkers en klanten om de onderstaande richtlijnen voor cyberbeveiliging in hun eigen gedrag te volgen zodat ze beter voorbereid zijn op cyberdreigingen en hun financiële gegevens hiertegen beschermen.

1. Implementeer basispraktijken voor cyberhygiëne op uw apparaten.
⇒ Gebruik sterke wachtwoorden op alle persoonlijke en werkapparaten en overweeg het gebruik van een wachtwoordmanager.
⇒ Houd besturingssystemen en andere software en applicaties op uw computers en mobiele apparaten up-to-date.
⇒ Installeer antivirus-, anti-malware- en anti-ransomware-software die kwaadaardige programma's tegenhoudt, detecteert en verwijdert.
⇒ Gebruik een firewallprogramma om onbevoegde toegang tot uw computer te voorkomen.
⇒ Gebruik alleen beveiligingsproducten van gerenommeerde bedrijven. Lees beoordelingen uit computer- en consumentenbladen en overleg eventueel met de fabrikant van uw computer of besturingssysteem.

2. Ga zorgvuldig om met gevoelige informatie.
⇒ Stuur geen bankrekeningwachtwoorden of andere gevoelige gegevens van financiële accounts via niet-versleutelde e-mail.
⇒ Denk goed na over waar en hoe u verbinding maakt met het internet om te bankieren of berichten met gevoelige persoonlijke gegevens te versturen. Openbare wifinetwerken en computers op plaatsen zoals bibliotheken of businesscenters in hotels kunnen riskant zijn.

3. Ga niet in op phishinge-mails.
⇒ Open niet meteen e-mailbijlagen en klik niet op links in ongevraagde of verdachte e-mails. Stop. Denk na. Klik.
⇒ Wees argwanend als iemand u onverwacht online of telefonisch contacteert en u om persoonlijke gegevens vraagt. Zelfs wanneer u met bekende adressen communiceert, doet u er goed aan zo min mogelijk persoonlijke gegevens via e-mail te delen.
⇒ Vergeet niet dat geen enkele financiële instelling u zal e-mailen of bellen en om vertrouwelijke informatie zal vragen die ze al over u hebben.
⇒ Ga ervan uit dat een verzoek om informatie van een bank waar u nog nooit een rekening hebt gehad frauduleus is.
⇒ Controleer of een verdachte e-mail of een verdacht pop-upvenster legitiem is voordat u persoonlijke gegevens verstrekt. Let goed op het e-mailadres.

Accounts beheren

⇒ Vraag klanten om sterke gebruikers-ID's en wachtwoorden te gebruiken om in te loggen op uw diensten. Adviseer hen niet hetzelfde wachtwoord te gebruiken als voor andere accounts.
⇒ Gebruik directe verificatie, realtimeverificatie, verificatie door een testbetaling, identiteitsverificatie en/of out-of-wallet-vragen om na te gaan of het om echte klanten gaat en de kans op fraude te verminderen.
⇒ Bied klanten idealiter tweeledige verificatie aan bij het inloggen op uw diensten.
⇒ Controleer de gebruikersaccounts regelmatig op tekenen van fraude.

Gegevens beschermen

⇒ Bedenk welke klantgegevens uw organisatie *moet* verzamelen om haar diensten uit te voeren, en verzamel bij voorkeur geen klantgegevens die daar niet voor nodig zijn.
⇒ Stel beleid voor gegevensbewaring op en verspreid dit binnen de organisatie. Verwijder klantgegevens wanneer ze niet meer nodig zijn.
⇒ Versleutel klantgegevens tijdens verzending en opslag.
⇒ Stel gegevensbeveiligingsbeleid op om duidelijk te maken welke methoden voor gegevensoverdracht worden goedgekeurd of beperkt en om te specificeren wat acceptabel is voor alle medewerkers bij hun omgang met klantgegevens. Zorg ervoor dat alle medewerkers op de hoogte zijn van dit beleid en zich eraan houden; evalueer het beleid geregeld en werk het waar nodig bij.

Openbare webapplicaties beveiligen

⇒ Implementeer HTTPS in de webapplicatie(s) van uw organisatie en leid al het HTTP-verkeer om naar HTTPS.
⇒ Maak op uw website(s) gebruik van een contentbeveiligingsbeleid om cross-site scripting-aanvallen, clickjacking en andere code-injectie te voorkomen.
⇒ Schakel koppeling van openbare sleutels op uw website(s) in om man-in-the-middle-aanvallen te voorkomen.
⇒ Zorg ervoor dat uw publieksgerichte webapplicatie(s) nooit cookies gebruiken om zeer gevoelige of kritieke klantinformatie (zoals wachtwoorden) op te slaan en dat de cookies niet te lang blijven staan. Versleutel eventueel de informatie die is opgeslagen in de cookies die u plaatst.
⇒ Overweeg om de beveiliging van uw publieksgerichte webapplicatie(s) minimaal eenmaal per jaar te laten beoordelen door een penetratietestservice.

Medewerkers trainen

⇒ Leer uw medewerkers verantwoordelijkheid op zich te nemen en reik strategieën aan om menselijke fouten waarbij klantgegevens zouden kunnen worden blootgesteld zoveel mogelijk te voorkomen. Adviseer ze dus om:

- Hun toegang tot en doorgifte van klantgegevens tot een minimum beperken tot wat nodig is om hun taken uit te voeren,
- Sterke beveiligingspraktijken toe te passen op alle apparaten en accounts waarop klantgegevens worden verwerkt door sterke wachtwoorden en tweeledige verificatie te gebruiken, software bijgewerkt te houden en niet op verdachte links te klikken, en
- Mogelijke interne of externe beveiligingsincidenten, dreigingen of verkeerde verwerking van gegevens aan het technisch personeel van uw organisatie en/of hoger management te melden.

⇒ Zorg ervoor dat uw werknemers documenten waarin ze toezeggen zich te zullen houden aan de beleidsregels inzake gegevensbescherming en beveiliging van uw organisatie begrijpen en hebben ondertekend, zodat ze deze niet overtreden, weten hoe ze moeten omgaan met klanten en dus niet op een onveilige manier met klanten communiceren.

Klanten informeren

⇒ Zorg dat u de regelgeving die voor uw organisatie van toepassing is als het gaat om de omgang met gegevensinbreuken van klanten kent zodat u weet wat de regels zijn als zich incidenten voordoen.
⇒ Wanneer uw organisatie kennis krijgt van een geval van onbevoegde toegang tot gevoelige klantinformatie, stel dan snel een onderzoek in om te bepalen hoe groot de kans is dat de informatie is of zal worden misbruikt. Volg de beste praktijken op het gebied van kennisgeving en breng de betrokken klant(en) zo snel mogelijk op de hoogte met:

- Een algemene beschrijving van het incident en de informatie waarop de gegevensinbreuk betrekking heeft,
- Een telefoonnummer voor meer informatie en hulp,
- Een herinnering om de komende 12 tot 24 maanden “waakzaam te blijven”,
- Een aanbeveling om gevallen van vermoede identiteitsdiefstal onmiddellijk te melden,
- Een algemene beschrijving van de stappen die de financiële instelling heeft genomen om de informatie te beschermen tegen verdere onbevoegde toegang of onbevoegd gebruik,
- Contactgegevens van kredietinformatiebureaus, en
- Alle overige informatie die uw organisatie overeenkomstig de regelgeving moet verstrekken.

Capaciteitsopbouw cyberbeveiliging Toolbox voor financiële organisaties

Handleiding CISO-niveau: verbindingen met derden beveiligen

Leveranciers kiezen met cyberbeveiliging in gedachten

Stel potentiële leveranciers de volgende vragen om hun bescherming tegen en bewustzijn van cyberaanvallen te meten en daarmee de impact die ze zouden hebben op het risicoprofiel van uw organisatie:

1. **Hoeveel ervaring hebben zij?** Achterhaal voor welke klanten de leverancier heeft gewerkt. Zitten er klanten bij met een soortgelijke organisatie als de uwe?
2. **Geven ze aan de gangbare cyberbeveiligingsnormen na te leven** zoals het NIST Framework of ISO 27001, of kunnen ze een SOC2-rapport tonen?
3. **Tot welke van uw gegevens en/of bedrijfsmiddelen moeten ze toegang hebben om hun diensten te kunnen leveren?** Vragen ze om kennelijk onnodige toegang?
4. **Hoe willen ze de bedrijfsmiddelen en gegevens van uw organisatie die in hun bezit zijn beschermen?**
5. **Hoe beheren ze hun eigen cyberrisico door derden?** Kunnen ze informatie geven over hun toeleveringsketen?
6. **Wat is hun plan voor herstel na noodgevallen en bedrijfscontinuïteit?** in geval van een incident dat invloed heeft op de bedrijfsmiddelen en/of gegevens van uw organisatie?
7. **Hoe houden ze uw organisatie op de hoogte?** Hoe willen ze trends, dreigingen en veranderingen binnen hun organisatie communiceren?

Risico's via derden identificeren

⇒ Houd een actuele lijst bij van alle relaties met leveranciers en de bedrijfsmiddelen en gegevens die in elk van deze relaties worden blootgesteld.
⇒ Bekijk de gegevens waartoe elke leverancier of derde toegang heeft. Zorg ervoor dat dit toegangsniveau tot het strikte minimum wordt beperkt (principe van 'least privilege').
⇒ Classificeer uw relaties met leveranciers en derden (laag, gemiddeld, hoog) op basis van de impact die een inbreuk op hun systemen zou hebben op uw organisatie.
⇒ Evalueer in hoeverre de leveranciers cyberbeveiliging waarborgen, en begin daarbij met de leveranciers met het hoogste risico. Naleving van relevante normen is een goed uitgangspunt. Ontwikkel een plan voor regelmatige veiligheidsbeoordelingen. Het kan soms zinvol zijn om leveranciers met het hoogste risico en/of de meest uitgebreide toegang tot klantgegevens ter plaatse te beoordelen.

Beveiliging door derden beheren

⇒ Voer grondige due diligence uit. Neem in uw offerteaanvragen, contracten, bedrijfscontinuïteit, incidentrespons en service level agreements met leveranciers de verwachtingen van uw organisatie ten aanzien van cyberbeveiliging op. Leg samen vast wie verantwoordelijk en aansprakelijk is in geval van een cyberincident.

- Informeer naar de cyberbeveiligingspraktijken van andere derden zoals financiële organisaties waarmee u samenwerkt of gegevens deelt. Alle cyberbeveiligingseisen waaraan uw organisatie moet voldoen, moeten ook gelden voor uw leveranciers en alle andere organisaties waarmee u gegevens deelt of die toegang hebben tot bedrijfsmiddelen.

⇒ Gebruik vastgestelde en overeengekomen maatregelen om de naleving van de cyberbeveiligingsnormen van uw leveranciers te controleren.
⇒ Controleer bij uw leveranciers die gevoelige gegevens behandelen of ze gebruikmaken van tweeledige verificatie, encryptie of andere beveiligingsmaatregelen voor de accounts die u bij hen hebt.
⇒ Zorg ervoor dat alle door u geïnstalleerde software en hardware van derden een beveiligingshandshake heeft zodat de opstartprocessen beveiligd zijn via verificatiecodes en niet worden uitgevoerd als codes niet worden herkend.
⇒ Als u leveranciersproducten tegenkomt die namaak zijn of niet voldoen aan de specificaties, werk dan samen aan een oplossing of anders een exitstrategie.
⇒ Evalueer leverancierscontracten jaarlijks en zorg ervoor dat ze blijven voldoen aan uw strategische koers en de wettelijke vereisten inzake gegevensbeveiliging. Bij beëindiging van het contract moet u bepalingen opnemen over het retourneren van uw bedrijfsmiddelen of gegevens, nagaan of de bedrijfsmiddelen of gegevens die in het bezit waren van de leverancier volledig zijn gewist en zorgen dat hij niet langer toegang heeft tot uw systemen of servers.

Informatie delen

⇒ Zorg ervoor dat u duidelijke communicatiekanalen en contactpunten hebt om te communiceren over beveiligingsproblemen met de leveranciers en concurrenten van uw organisatie.
⇒ Het tijdig delen van betrouwbare, bruikbare cyberbeveiligingsinformatie met interne en externe belanghebbenden (inclusief organisaties en overheidsinstanties binnen en buiten de financiële sector).
⇒ Volg relevante updates over de ervaringen van andere organisaties met hun derden op het gebied van dreigingen, zwakke plekken, incidenten en respons zodat uw organisatie beter gewapend is, zich beter bewust is van de situatie en meer te weten komt. Als uw organisatie deelneemt aan informatie-uitwisseling met andere organisaties, bijvoorbeeld in het kader van de FS-ISAC, kunt u gemakkelijk op de hoogte blijven.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE

Capaciteitsopbouw cyberbeveiliging Toolbox voor financiële organisaties

Handleiding incidentrespons

Voorbereiding

⇒ Werk samen met het senior management van uw organisatie en andere betrokken medewerkers om een incidentrespons en bedrijfscontinuïteitsplan op te stellen op basis van de meest urgente risico's die geïdentificeerd zijn in de cyberrisicobeoordeling van uw organisatie.

- Ontwikkel dreigingsscenario's voor de soorten incidenten die verband houden met de cyberrisico's die binnen uw organisatie de hoogste prioriteit hebben. Focus op capaciteitsopbouw om te reageren op die scenario's.
- Stel een lijst met contactpunten voor incidentrespons samen en verspreid deze binnen uw organisatie.
- Verzamel contactgegevens van relevante lokale en federale wetshandhavingsinstanties en -functionarissen.
- Stel bepalingen vast die aangeven welke soorten incidenten moeten worden gemeld, wanneer ze moeten worden gemeld en aan wie.
- Stel schriftelijke richtlijnen vast die aangeven hoe snel medewerkers moeten reageren op een incident en welke handelingen nodig zijn op basis van relevante factoren zoals de functionele en informatie-impact van het incident en de waarschijnlijkheid van herstel na het incident.
- Laat alle medewerkers contact opnemen met uw technische team – dit zijn meestal de IT-medewerkers en/of de CISO/CIO/een andere vergelijkbare manager – wanneer zich een incident voordoet.
- Implementeer oplossingen om de handelingen van werknemers te monitoren en om dreigingen en incidenten te kunnen identificeren.
- Voeg bedrijfscontinuïteitsplannen toe om de samenwerking van uw organisatie met leveranciers en primaire klanten tijdens een zakelijk noodgeval te coördineren. Vermeld indien nodig ook hoe handmatige of alternatieve bedrijfswerkzaamheden uitgevoerd zouden moeten worden.
- Stel schriftelijke procedures op voor het uitschakelen en herstarten van het systeem in noodgevallen.
- Ontwikkel en test methoden voor het ophalen en herstellen van back-upgegevens; test back-upgegevens periodiek om de validiteit ervan te verifiëren.
- Zorg dat er overeenkomsten en procedures zijn voor het uitvoeren van bedrijfsactiviteiten op een alternatieve locatie.
- Zorg dat er een duidelijk kanaal is voor de verspreiding naar alle klanten.

Oefening

⇒ Organiseer kleine tafeloefeningen met alle medewerkers of vertegenwoordigers van alle personeelsniveaus, inclusief leidinggevenden van de organisatie, PR/communicatiemedewerkers en juridische en nalevingsteams.
⇒ Zoek tafeloefeningen in de branche die relevant zijn voor uw organisatie en neem hieraan als het even kan deel.
⇒ Stel een proces vast om ervoor te zorgen dat de geleerde lessen van de oefeningen worden opgenomen en aan de orde komen in de cyberbeveiligingsstrategie van uw bedrijf.

Respons

⇒ Implementeer een incidentresponsplan om de impact te minimaliseren, ook op het vlak van reputatieschade.
⇒ Identificeer betrokken/aangetaste systemen en beoordeel de schade.
⇒ Verminder de schade door de betrokken bedrijfsmiddelen te verwijderen (loskoppelen).
⇒ Begin met het opnemen van alle informatie zodra het team vermoedt dat er een incident heeft plaatsgevonden. Probeer bewijs van het incident te bewaren tijdens het loskoppelen/scheiden van aangetaste geïdentificeerde bedrijfsmiddelen. Verzamel bijvoorbeeld de logboeken van de systeemconfiguratie, het netwerk en inbraakdetectie uit de betrokken bedrijfsmiddelen.
⇒ Breng de juiste interne partijen, externe leveranciers en autoriteiten op de hoogte en vraag indien nodig om hulp.
⇒ Breng klanten op de hoogte en bied ondersteuning in overeenstemming met wet- en regelgeving en richtlijnen tussen instanties.
⇒ Gebruik platforms voor het delen van informatie over dreigingen zoals FS-ISAC of MISP om de branche op de hoogte te stellen van de dreiging.
⇒ Documenteer alle stappen die tijdens het incident werden genomen om deze later te beoordelen.

Herstel

⇒ Herstel herstelde bedrijfsmiddelen naar periodieke "herstelpunten" (indien beschikbaar) en gebruik back-upgegevens om systemen te herstellen naar de laatst bekende "goede" status.
⇒ Creëer bijgewerkte "schone" back-ups van herstelde bedrijfsmiddelen en zorg ervoor dat alle back-ups van kritieke bedrijfsmiddelen op een fysieke locatie in een veilige omgeving worden opgeslagen.
⇒ Test en controleer of geïnfecteerde systemen volledig zijn hersteld. Bevestig dat de betrokken systemen normaal functioneren.

Beoordeling

⇒ Voer een discussie over "geleerde lessen" nadat het incident heeft plaatsgevonden – overleg met senior medewerkers, vertrouwde adviseurs en de leverancier(s) van computerondersteuning om mogelijke zwakke plekken te beoordelen of nieuwe stappen aan te bevelen die moeten worden geïmplementeerd.
⇒ Identificeer, indien mogelijk, de zwakke plekken (in software, hardware, bedrijfsactiviteiten of gedrag van medewerkers) die tot het incident hebben geleid en ontwikkel een plan om hierin verbetering aan te brengen.
⇒ Ontwikkel een plan voor controle om soortgelijke of verdere incidenten met betrekking tot de geïdentificeerde problemen te detecteren.
⇒ Deel geleerde lessen en informatie over het incident op platformen voor het delen van informatie over dreigingen zoals FS-ISAC.
⇒ Integreer de geleerde lessen in de protocollen voor respons op incidenten van uw organisatie.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE