Tips voor het opstellen van een Cyber response plan

ABN·AMRO

Inhoud

Mij overkomt dat niet... toch?

Vrijwel dagelijks staan er berichten in de media over bedrijven en publieke organisaties die te maken hebben met cyberaanvallen. Toch zijn er nog steeds veel ondernemers die denken dat hun bedrijf niet interessant is voor cybercriminelen.

De praktijk leert dat elk bedrijf in elke branche een potentieel doelwit is. Veel bedrijven die slachtoffer zijn geworden, zijn niet doelbewust gekozen. Een reactie op een phishing mail, een download van een verkeerd bestand of het gebruik van oude software kan al een cyberaanval tot gevolg hebben. Computers worden gehackt, gegevens gestolen of gewist en bedrijfsprocessen vallen stil. Voor veel bedrijven vormt een cyberaanval daarom de grootste en meest directe bedreiging voor de continuïteit.

Hoewel cyberaanvallen niet altijd zijn te voorkomen, kunt u wel maatregelen nemen om de kans erop te verkleinen. En u kunt zich erop voorbereiden, voor het geval u er in de toekomst wel slachtoffer van wordt. Een Cyber response plan kan u daarbij helpen. In dit document leggen we uit hoe u een Cyber response plan opstelt en waarom het verstandig is om er een te maken.

Wat is een Cyber response plan?

Een Cyber response plan is een opsomming van acties die uw bedrijf helpen om voorbereid te zijn op incidenten als gevolg van cybercriminaliteit. Naast preventieve maatregelen geven wij u tips over signalen die kunnen duiden op problemen, hoe te reageren en hoe u de impact minimaliseert. We behandelen aspecten als training en communicatie tijdens een cyberincident. Ook beschrijven we welke stappen u kunt zetten om problemen op te lossen, zodat uw bedrijf de activiteiten kan hervatten.

Waarom heeft u het nodig?

Elke onderneming – hoe klein ook – kan slachtoffer worden van cybercriminaliteit. Met een Cyber response plan bent u beter voorbereid en kunt u gericht acties ondernemen die de kans op een cyberincident verkleinen en de schade bij een incident beperken. Grote multinationals huren experts in of hebben een afdeling om een Cyber response plan op te zetten. Voor mkb'ers is dit niet altijd mogelijk, maar met een aantal eenvoudige stappen voorkomt u al veel risico's.

Tip

Wees voorbereid op internetcriminaliteit. Zo weet u wat u moet doen, als het u overkomt.

Voordat u aan de slag gaat

Voordat u begint, adviseren wij u om één persoon verantwoordelijk te maken voor het Cyber response plan van uw onderneming. In de praktijk is dit vaak de persoon die de IT voor uw bedrijf regelt. Dat kan een medewerker zijn, maar ook iemand buiten uw bedrijf, bijvoorbeeld een vriend of familielid.

Deze persoon wordt eigenaar van het Cyber response plan en bepaalt wie hij of zij nodig heeft om het plan te maken en wie welke activiteiten op zich neemt. Deze persoon moet uiteindelijk ook het Cyber response plan goedkeuren.

Stappenplan

Een Cyber response plan bestaat uit een aantal stappen die u moet doorlopen. Wereldwijd zijn er diverse standaarden voor het opzetten van een Cyber response plan. Wij hebben die gebruikt voor het opzetten van dit document. Hiernaast ziet u een aantal stappen die u moet doorlopen om een goed plan op te kunnen zetten.

Stap 1 – Inventarisatie
Wat moet ik beschermen?

Stap 2 – Identificatie
Welke vormen van cybercriminaliteit vormen een bedreiging?

Stap 3 – Preventie
Hoe bescherm ik mijn bedrijf?

Stap 4 – Detectie
Hoe vind ik het probleem en los ik het op?

Stap 5 – Herstel
Hoe ben ik zo snel mogelijk weer in bedrijf?

Stap 6 – Verbetering
Hoe verbeter ik mijn Cyber response plan?

Stappenplan

1. Inventarisatie
2. Identificatie
3. Preventie
4. Detectie
5. Herstel
6. Verbetering

Stap 1 – Inventarisatie
Wat moet ik beschermen?

Om te kunnen bepalen wat u moet beschermen, hoeft u eigenlijk maar één vraag te stellen: Welke systemen, processen en informatie zijn cruciaal voor het voortbestaan van mijn bedrijf?

Het antwoord op deze vraag verschilt per bedrijf. Voor een webwinkel zijn dat de website en het betaalsysteem, voor een tuinder is dat het programma dat het klimaat in de kassen regelt en voor een huisarts is dat zijn/haar patiëntenadministratie. Bepaal dus eerst voor uzelf welke systemen, processen en informatie voor uw bedrijf onmisbaar zijn.

Cybercriminaliteit komt vrijwel altijd van buitenaf. Het is daarom belangrijk om ervoor te zorgen dat niemand ongewenst toegang krijgt. Daarvoor moet u niet alleen de systemen beschermen, maar ook de data beveiligen en uw medewerkers trainen om uw bedrijfsprocessen overeind te houden.

Bescherm uw systemen

U moet niet alleen de apparatuur beschermen die deel uitmaakt van uw netwerk (computers, servers, routers etc.). Denk ook aan andere systemen die belangrijk zijn voor de continuïteit van uw bedrijf zoals machines, regelapparatuur of robots. En als u vertrouwelijke informatie uitwisselt met externe partijen is het van belang om ook de beveiliging van uw communicatieprotocollen mee te nemen.

Zo beschermt u uw computersystemen:

- Installeer een firewall en een antivirusprogramma en houd die up-to-date.
- Installeer tijdig patches, dat zijn updates die zwakke plekken in uw software herstellen.
- Houd uw software up-to-date en verwijder oude versies. Sta niet toe dat medewerkers op eigen initiatief software kunnen installeren en hardware gebruiken waarvan u niet weet of deze veilig zijn.
- Neemt u diensten of applicaties af van externe leveranciers? Laat dan in het contract vastleggen dat zij de bescherming tegen cybercriminaliteit op orde hebben.
- Laat ethische hackers tests uitvoeren om zwakke plekken te vinden

Tip
Met een IDS (Intrusion Detection System) bent u beter in staat om uw netwerk te monitoren en sneller te reageren op incidenten. Een IDS is overigens niet goedkoop.

Bescherm uw data

Data zoals klantgegevens, login gegevens, offertes en facturen zijn essentieel voor de meeste bedrijven. Als ze worden gestolen, heeft u een datalek. U heeft ze opgeslagen en uw klanten mogen erop vertrouwen dat u zorgt dat ze niet in handen van onbevoegden komen. Daarom is het belangrijk ze goed te beveiligen tegen indringers.

Dit kunt u doen om uw data te beschermen:

- Beperk het aantal mensen dat toegang heeft tot de data.
- Wees selectief in het toekennen van rechten. Niet elke medewerker heeft volledige rechten nodig. Een magazijnmedewerker hoeft bijvoorbeeld geen toegang te hebben tot de personeelsadministratie.
- Beveilig de toegang tot uw systemen. Voeg naast het gebruik van een gebruikersnaam en wachtwoord een extra stap toe (tweefactor authenticatie). Inloggen kan dan alleen door het invoeren van een extra code die bijvoorbeeld naar de smartphone van de gebruiker wordt gestuurd.
- Sla uw data versleuteld op en bescherm de encryptiesleutels goed.
- Maak regelmatig een back-up van uw data en zorg dat de back-up niet direct via het netwerk is te benaderen. Sla deze bijvoorbeeld op een externe harde schijf op. Houd u aan de Algemene verordening gegevensbescherming (AVG). Zo voorkomt u dat bij een computerinbraak persoonsgegevens worden gestolen, die u niet (meer) had mogen bezitten.

Bescherm uw medewerkers

Circa 85% van de cyberaanvallen start met het manipuleren van medewerkers door cybercriminelen. Uw medewerkers worden benaderd via e-mail, social media of telefoon en faciliteren onbedoeld en onbewust toegang tot uw bedrijfsnetwerk. Phishing is veruit de bekendste en meest voorkomende vorm ervan. Hiermee kunnen inloggegevens worden gestolen of kan malware geïnstalleerd worden op een computer of netwerk. Het is daarom van groot belang dat u uw medewerkers regelmatig wijst op de slinkse manieren waarop cybercriminelen te werk gaan.

Dit kunt u doen:

- Train regelmatig uw medewerkers in het herkennen van risicovolle situaties (bijv. het herkennen van phishingmails of verzoeken om het installeren/ updaten van software).
- Gebruik antivirus software en/of installeer een e-mailfilter om kwaadaardige mails te blokkeren.
- Test uw medewerkers regelmatig, bijvoorbeeld door hen test phishing mails te sturen.
- Laat medewerkers meedenken hoe zwakke plekken in de procedures en systemen kunnen worden aangepakt.

Tip

Laat uw medewerkers een wachtwoord manager gebruiken. Die genereert sterke en unieke wachtwoorden en voorkomt dat uw medewerkers wacht-woorden moeten onthouden of ergens opschrijven.

Stap 2 – Inventarisatie
Wat zijn de bedreigingen?

Er zijn vele vormen van cybercriminaliteit. In dit hoofdstuk noemen we een aantal voorbeelden. Wat ze precies inhouden, leest u in bijlage 1.

Ruwweg kunnen we cybercriminaliteit onderverdelen in 3 categorieën:

1. Bedreiging voor de vertrouwelijkheid van uw data
2. Bedreiging voor de integriteit van uw data
3. Bedreiging voor de beschikbaarheid van uw data en systemen

Bedreiging voor de vertrouwelijkheid van uw data

Vertrouwelijke informatie is waardevol voor cybercriminelen. Die kunnen ze verkopen op hacker fora of het darkweb, misbruiken door bijvoorbeeld uw klanten phishing mails te sturen of om u chanteren met publicatie. Er zijn legio methoden om vertrouwelijke informatie te bemachtigen, bijvoorbeeld via phishing, spyware, gehackte e-mailaccounts en diversen vormen van malware. Als vertrouwelijke informatie in handen is van onbevoegden, spreken we van een datalek. De gevolgen datalek kunnen desastreus zijn. Bijvoorbeeld als het gaat om informatie uit medische of juridische dossiers of blauwdrukken voor een nieuw product. Naast directe schade is er vaak reputatieschade, gevolgd door claims van gedupeerden of een boete van de toezichthouder.

Bedreiging voor de integriteit van uw data

Als uw data wordt gewijzigd door cybercriminelen of andere aanvallers (bijvoorbeeld een kwaadwillende medewerker) is die data niet meer betrouwbaar, correct of volledig. Dit kan plaatsvinden door virussen andere vormen van malware en interne fraude door een medewerker. Gewijzigde gegevens kunnen grote gevolgen hebben voor uw bedrijfsprocessen en klanten. Bijvoorbeeld wanneer een cybercrimineel zich toegang heeft verschaft tot het patiëntenbestand en medische informatie wijzigt. Maar ook de financiële administratie of het e-mailsysteem zijn een potentieel doelwit. Een cybercrimineel zou bijvoorbeeld facturen naar uw klanten kunnen sturen met een ander rekeningnummer. De financiële schade kan flink in de papieren lopen en impact hebben op de winstgevendheid en reputatie van uw bedrijf.

Bedreiging voor de beschikbaarheid van uw data en systemen

Een andere, ernstige bedreiging is het niet beschikbaar zijn van systemen en data. Deze bedreigingen worden bijvoorbeeld veroorzaakt door ransomware, DDoS-aanvallen en wiper malware. Een DDoS-aanval zorgt voor tijdelijke onbereikbaarheid van uw website, server of netwerk. Ransomware kan ertoe leiden dat uw data wordt versleuteld en u de toegang tot al uw informatie kwijt bent. Zelfs backupbestanden kunnen worden versleuteld. Wiper malware is agressieve malware die alle data wist en systemen onbruikbaar maakt. De gevolgen kunnen sterk uiteenlopen, van een ernstige verstoring tot een zelfs een faillissement.

Tip

Zorg dat de beveiliging van uw systemen en software altijd up-to-date is.

Stap 3 – Preventie
Hoe bescherm ik mijn bedrijf?

Om uw bedrijf zo goed mogelijk te beschermen, is het belangrijk om te weten wat de zwakke plekken zijn in uw bedrijf en voor welke cyberaanvallen u kwetsbaar bent. Neem uw netwerk en organisatie eens kritisch onder de loep.

Waar bent u kwetsbaar? Waar kan de grootste schade ontstaan? Welke systemen en processen mogen in elk geval niet getroffen worden? Door de verscheidenheid aan cyberaanvallen is dat best lastig te bepalen

Werk scenario's uit

Een veelgebruikte methode om u te beschermen tegen cybercriminaliteit is het ontwikkelen van scenario's. Door te denken in scenario's worden de gevolgen meteen zichtbaar en kunt u beter beoordelen welke maatregelen u moet nemen.

Op basis van de bedreigingen die we in stap 2 hebben gecategoriseerd, kunt u bijvoorbeeld drie scenario's uitwerken. Hier ziet u wat u kunt doen als bepaalde scenario's werkelijkheid worden.

Tip

Wist u dat u zich tegen cybercriminaliteit kunt verzekeren? Vraag uw verzekeraar naar de mogelijkheden.

Scenario 1: datalek

Onbevoegden hebben kritische bedrijfsinformatie in handen gekregen.

Wat moet u doen?

- Achterhaal welke informatie is gelekt.
- Leg digitale sporen vast voor onderzoek en als bewijsmateriaal.
- Doe aangifte bij de politie en neem juridische stappen.
- Meld een datalek bij de Autoriteit Persoonsgegevens. Informeer alle betrokkenen: medewerkers, klanten, leveranciers, media etc.

Scenario 2: diefstal

Een hacker is uw netwerk binnengedrongen en heeft forse bedragen weggesluisd naar externe rekeningen.

Wat moet u doen?

- Bel uw bank.
- Achterhaal welke rekeningen zijn geplunderd en welke inlogcodes zijn gebruikt.
- Onderzoek naar welke rekeningen het geld is weggesluisd.
- Leg digitale sporen vast voor onderzoek en als bewijsmateriaal.
- Doe aangifte bij de politie en neem juridische stappen

Scenario 3: ransomware

Een hacker heeft de systemen en/of data van uw bedrijf versleuteld. U moet binnen 72 uur betalen om dit ongedaan te maken

Wat moet u doen?

- Probeer te achterhalen hoe de hacker heeft kunnen binnendringen.
- Check of uw back-up nog bruikbaar is.
- Leg digitale sporen vast voor onderzoek en als bewijsmateriaal.
- Doe aangifte bij de politie en neem juridische stappen.
- Neem contact op met een computer emergency response team (CERT) voor deskundige hulp en advies.

Tip

Als uw bedrijf onder de NIS2 wetgeving valt, moet u cyberincidenten binnen 24 uur melden bij de toezichthouder in uw branche.

Werk de scenario's uit tot een Cyber response plan

Als u heeft nagedacht over de meest waarschijnlijke scenario's voor uw bedrijf, kunt u concreet een Cyber response plan maken waarin u voor de meest waarschijnlijke scenario's een draaiboek opstelt. Belangrijke aspecten daarbij zijn:

- Besluitvorming – wie heeft mandaat om (soms ingrijpende) beslissingen te nemen?
- Expertise – welke experts heeft u nodig voor technische analyse, het implementeren van maatregelen en wellicht juridische bijstand?
- Taakverdeling – wat kunnen of moeten medewerkers doen bij een cyberincident?

Bescherm uw medewerkers

Het trainen op cyberincidenten is belangrijk. En dat moet u niet één keer doen, maar regelmatig. Alleen zo ontstaat er een routine en leren uw medewerkers hun rol en verantwoordelijkheid kennen. Want tussen weten wat je moet doen en adequaat reageren als het serieus is, zit vaak nog een wereld van verschil. Bovendien vergroot elke training het risicobewustzijn van uw medewerkers. Hoe beter uw medewerkers zijn voorbereid, hoe kleiner de kans dat ze cruciale fouten maken. Door het testen van uw Cyber response plan anticipeert u op toekomstige incidenten, voorkomt u paniek als het gebeurt en vergroot u de weerbaarheid van uw bedrijf.

Communicatie

Communicatie rond een cyberincident is heel belangrijk. Bedenk daarom voor elk scenario welke partijen u moet informeren. Behalve uw medewerkers zijn dat de politie, klanten, leveranciers en wellicht ook de media en de toezichthouder in uw branche. Iedereen die last kan hebben van uw cyberincident moet worden gecommuniceerd. Maar overweeg goed wat u wel en niet wilt communiceren en op welk moment. Zo voorkomt u dat wat u vertelt nog meer vragen oproept en u vervolgens daar veel tijd mee kwijt bent. Wees daarom duidelijk en meld wanneer men eventueel meer informatie kan verwachten. Zijn er persoonsgegevens gestolen? Doe dan aangifte bij de Autoriteit Persoonsgegevens.

Preventieve producten

Op het gebied van cybersecurity is er een breed palet aan producten beschikbaar ter preventie van cybercriminaliteit en zijn er oplossingen voor detectie en herstel op de markt. Vraag in elk geval uw IT-er om periodiek de digitale beveiliging en alle gebruikersrechten door te lichten.

Niet vergeten

Hieronder een paar aandachtspunten om u op weg te helpen:

- Zorg dat alle medewerkers weten waar ze phishing, een datalek of fraude moeten melden.
- Leg de verantwoordelijkheden bij een datalek, fraude of ransomware-aanval vast.
- Zorg voor faciliteiten om malware in quarantaine te plaatsen.
- Bescherm uw back-ups tegen ransomware-aanvallen.
- Oefen periodiek met het terugzetten van back-ups.
- Maak afspraken met leveranciers en afnemers voor het geval systemen niet beschikbaar zijn.

Een aanval in de supply chain

Het kan natuurlijk gebeuren dat uw belangrijkste leverancier slachtoffer wordt van cybercriminaliteit en tijdelijk haar activiteiten moet staken. Dat kan betekenen dat bepaalde services niet worden verleend of producten niet worden geleverd. Het is daarom goed om na te denken wat de impact op uw bedrijfsprocessen is als zich een dergelijke situatie aandient. Heeft een plan B als uw belangrijkste leverancier tijdelijk wegvalt?

Stap 4 – Detectie
Hoe vind ik het probleem en los ik het op?

Voorkomen is altijd beter dan genezen. Een cyberaanval overvalt u meestal, maar u kunt ook preventief zoeken naar signalen. Wist u dat cybercriminelen zich soms wekenlang in een netwerk schuilhouden voordat ze hun slag slaan? U kunt ze voor zijn, door bijvoorbeeld regelmatig een netwerkscan uit te voeren. Dan weet u meteen hoe het met de veiligheid van uw netwerk is gesteld. Als tijdens het uitvoeren van een netwerkscan indringers worden ontdekt, bent u vaak nog niet te laat om maatregelen te nemen. Zo kunt u de schade beperken.

Let ook op onderstaande meldingen. Dit kunnen signalen zijn van cybercriminaliteit:

- Er zijn niet bestaande medewerkers toegevoegd
- Bepaalde medewerkers hebben plotseling veel meer gebruikersrechten
- Uw IT'er constateert afwijkend dataverkeer, er worden bijvoorbeeld veel gegevens naar een extern IP adres verstuurd.
- Er wordt 's nachts ingelogd terwijl uw bedrijf alleen overdag operationeel is
- Een leverancier of klant meldt dat hij een vreemd mailtje van uw bedrijf heeft ontvangen.

Analyseer zwakke plekken

Door regelmatig uw systemen te testen op cyberveiligheid, achterhaalt u wat de zwakke plekken zijn. Zitten er kwetsbaarheden in de beveiliging? Is een beveiligingsupdate op tijd geïnstalleerd? Herkennen medewerkers phishingmails en andere mails waarmee ze onbedoeld malware binnenhalen? Door het identificeren van de bron kunt u maatregelen nemen. Door het analyseren van zwakke plekken, kunt u maatregelen nemen om de beveiliging van uw systemen en processen verbeteren, configuratiefouten herstellen, uw website en e-mailbeveiliging versterken en schaduw IT identificeren.

Cyberaanval? Kom direct in actie

Bent u slachtoffer van een cyberaanval, kom dan meteen in actie. Het volgende is slim om direct te doen:

- Registreer wat er is gebeurd.
- Leg vast in welk deel van uw netwerk de cyberaanval heeft plaatsgevonden.
- Bepaal welke processen en systemen gevaar lopen of al zijn getroffen.
- Als dat kan, koppel dan computers of servers los van internet en van uw netwerk. Hoe meer u kunt loskoppelen, hoe groter de kans dat u de schade beperkt.
- Plaats besmette systemen in quarantaine.
- Verwijder niet direct alle geraakte data, accounts en systemen, want zo wist u mogelijk ook bewijsmateriaal.

Beperk de toegangsmogelijkheden

Hoe meer mensen toegang hebben tot uw netwerk en systemen, hoe groter het risico op cybercriminaliteit. Want zoals al eerder gezegd: in de meeste gevallen geven uw medewerkers zelf onbewust en onbedoeld cybercriminelen toegang tot uw netwerk of systemen.

Zo beperkt u dat risico:

- Geef medewerkers alleen toegang tot systemen die ze echt nodig hebben.
- Bepaal per systeem of computerprogramma wie er volledige en wie er beperkte toegangsrechten moet hebben.
- Inventariseer welke externe partijen toegang hebben tot uw netwerk, wat hun rechten zijn en of die rechten allemaal nodig zijn. Versterk het authenticatieproces.
- Voer tweefactorauthenticatie in voor cruciale systemen of software.
- Bepaal of er mogelijkheden zijn om de beveiliging van uw systemen, externe diensten en data te verbeteren

Back-ups zijn cruciaal

Voor de continuïteit van uw bedrijf is het essentieel dat u beschikt over een recente back-up van uw systeem en data. Bent u slachtoffer van een cyberaanval, dan kunt u uw bedrijfsactiviteiten weer snel hervatten. Leg ook vast hoelang back-ups bewaard moeten blijven.

Realtime online back-up
Een realtime online back-up heeft als voordeel dat u kunt terugvallen op actuele gegevens, maar deze kan vatbaar zijn voor ransomware.

Offline back-up
Een offline back-up, die bijvoorbeeld elke avond wordt gemaakt en los van het netwerk wordt opgeslagen, is een goed alternatief.

Geen back-up
Geen back-up betekent dat u bij een cyberaanval waardevolle gegevens kunt verliezen. En u bent mogelijk aansprakelijk voor de gevolgen daarvan.

Tip
Maak zeer regelmatig back-ups en zet die weg op een veilige plaats, bijvoorbeeld een externe harde schijf. Oefen met het terugzetten van een back-up. Evalueer het proces en los knelpunten op.

Stap 5 – Herstel
Hoe ben ik zo snel mogelijk weer in bedrijf?

Na een cyberaanval wilt u zo snel mogelijk weer aan het werk en alle systemen en software in gebruik nemen. Om de controle over uw netwerk terug te krijgen, is het noodzakelijk om alle malware veilig te verwijderen.

Daarna moeten uw systemen minder kwetsbaar gemaakt worden (in het Engels: system hardening) en getest worden, voordat ze weer in gebruik kunnen worden genomen. Dit proces moet grondig worden uitgevoerd om te voorkomen dat er malware achterblijft en er later opnieuw problemen ontstaan. U kunt eventueel een professionele, externe partij inhuren om dit voor u uit te voeren. Deze reset van systemen is ook een goede gelegenheid om uw systemen bij te werken voor zover dat nog niet gebeurd was.

Houd bij het opstellen van een Cyber response plan rekening met de tijd die u nodig heeft om te herstellen van een cyberincident en de bedrijfsprocessen te hervatten. Ook is het van belang om daarin op te nemen hoeveel gegevens u maximaal mag verliezen. Dat wordt meestal uitgedrukt in uren of minuten, want voor een drukbezochte webwinkel betekent een uur geen omzet iets anders dan voor een schildersbedrijf. Als u die twee aspecten scherp heeft, kunt u bepalen welke maatregelen minimaal noodzakelijk zijn voor uw bedrijfscontinuïteit.

Check het volgende

Voordat u uw netwerk en systemen weer in gebruik neemt, moet u zeker weten dat dit veilig kan. Check onder meer of de volgende zaken op orde zijn:

- Is alle malware verwijderd?
- Is de beveiliging van de systemen gecontroleerd en volledig up-to-date?
- Is de back-up veilig en volledig?
- Zijn maatregelen genomen om herhaling van het cyberincident te voorkomen?
- Zijn externe bestanden (van leveranciers) gecheckt? Zijn extern gehoste systemen gesynchroniseerd met uw processen en systemen?
- Is er een fall-backplan als het misgaat?

Tip

Check na de herstart uw systemen en software en blijf ze volgen. En wees alert op nieuwe incidenten.

Stap 6 – Verbetering
Hoe verbeter ik mijn Cyber response plan?

De daders achter cybercrime zitten niet stil. Ze ontdekken nieuwe kwetsbaarheden in software, ontwikkelen nieuwe malware, en bedenken nieuwe methoden om bedrijven aan te vallen.

Ze zetten kunstmatige intelligentie in om persoonlijke en grammaticaal correcte phishing mails te maken en aanvaller sneller en efficiënter te maken. Dagelijks vinden er cyberincidenten plaats en het is niet uitgesloten dat ook uw bedrijf er vroeg of laat mee te maken krijgt. Het is daarom belangrijk dat u uw Cyber response plan regelmatig test en waar nodig aanpast. Bovendien vergroot elke oefening het bewustzijn van uw medewerkers en vergroot u de kans dat ze op hun hoede zijn voor bijvoorbeeld phishing mails en dubieuze websites.

Evalueer

Na elke oefening en na elk cyberincident is het belangrijk om met alle betrokkenen om de tafel te gaan zitten en de oefening of het incident te bespreken. Loop het hele proces van melding tot herstel door, analyseer, beoordeel en bespreek wat u heeft geleerd. Wat ging er goed, waar is verbetering nodig en wat heeft u geleerd? Vragen die u zichzelf en uw team stelt, zijn onder andere:

- Waren de procedures duidelijk?
- Werden de toegewezen taken door iedereen goed uitgevoerd?
- Welke beveiligingsmaatregelen hebben gewerkt en welke niet?
- Zijn er nieuwe kwetsbaarheden (mens, proces, technologie) aan het licht gekomen?
- Zijn extra beveiligingsmaatregelen nodig?
- Wegen de investeringen in maatregelen op tegen het risico?
- Zijn uw medewerkers zich voldoende bewust van de risico's?
- Kunnen kwetsbaarheden bij leveranciers of partners uw bedrijf raken?

Tot slot

Geen enkel bedrijf wil te maken krijgen met een datalek, ransomware, fraude of een andere vorm van cybercriminaliteit. Daarom is het belangrijk om actief met uw Cyber response plan aan de slag te gaan. Niet alleen bij het opstellen, maar ook bij het trainen van scenario's en het verbeteren van het plan. U leert door te doen. Veel kunt u vooraf bedenken, maar bij een oefening leert u wie in actie moet komen, welke middelen uw medewerkers nodig hebben en welke maatregelen er moeten worden genomen. Na elke oefening bent u beter voorbereid op toekomstige aanvallen.

Een Cyber response plan zorgt er ook voor dat u zich beter bewust wordt van wat er binnen uw bedrijf allemaal nodig is om het draaiende te houden. U krijgt hiermee een duidelijk overzicht van en inzicht in de belangrijke processen en IT-diensten van uw bedrijf. We wensen u veel succes met het opstellen van uw Cyber response plan!

Verbeter uw cybersecurity met Cyber Veilig & Zeker

Op ABN AMRO Doorpakken helpen wij ondernemers met oplossingen die verder gaan dan financiële diensten. Bijvoorbeeld met Cyber Veilig & Zeker: onze cybersecurity- oplossing die uw cyberrisico's verlaagt en aanvullend is op uw huidige IT.

Lees meer over Cyber Veilig & Zeker of plan direct een gesprek in met een van onze cyberadviseurs om erachter te komen hoe Cyber Veilig & Zeker uw bedrijf beschermt tegen dreigingen van buitenaf.

Het is ook mogelijk te mailen voor een aanvraag of meer informatie.
U bereikt ons via: veiligondernemen@abnamro.nl

Bijlage 1
Toelichting op veel voorkomende cyberaanvallen

BEC
Business E-mail Compromise (BEC) is een geavanceerde vorm van phishing via e-mail en richt zich vooral op specifieke medewerkers bij bedrijven, zoals degene die de betalingen uitvoert. Een BEC-aanval begint bij grondig voorwerk door de fraudeur. Kijk voor meer informatie op: abnamro.nl/nl/zakelijk/insights/cybersecurity/de-verschillende-vormen-van-business-email-compromise

DDoS
Een DDoS-aanval is een poging om de continuïteit van online diensten te ondermijnen door het verkeer van een server, online service of netwerk te verstoren. Kijk voor meer informatie op: abnamro.nl/nl/zakelijk/insights/cybersecurity/ddos-aanval

Deepfake-technologie
Deepfake-technologie verwijst naar realistische, maar niet echte, visuele, audio- of tekstuele content die is geproduceerd met behulp van Artificiële Intelligentie (AI). Kijk voor meer informatie op: abnamro.nl/nl/zakelijk/insights/cybersecurity/deepfake-technologie

Exploitatie van kwetsbaarheden
Kwetsbaarheden in de software kunnen het gevolg zijn van onjuiste beveiligingsconfiguraties en/of programmeerfouten. Als ze niet worden aangepakt, kunnen deze kwetsbaarheden beveiligingslekken creëren. Kijk voor meer informatie op: abnamro.nl/nl/zakelijk/insights/cybersecurity/exploitatie-van-kwetsbaarheden-in-software

Ransomware
Ransomware (gijzelsoftware) is kwaadaardige software die de toegang tot een computer of mobiel apparaat blokkeert en/of bestanden versleutelt. Kijk voor meer informatie op: abnamro.nl/nl/zakelijk/insights/cybersecurity/ransomware-hoe-werkt-het-en-wat-kunt-u-ertegen-doen

Supply-chainaanval
Een supply-chainaanval betekent dat een bedrijf wordt aangevallen via een ander bedrijf in de keten. Kijk voor meer informatie op: abnamro.nl/nl/zakelijk/insights/cybersecurity/supply-chain-aanval

Webskimming
Webskimming is een vorm van cybercrime waarbij hackers schadelijke code in een online winkel plaatsen waardoor zij betaalinformatie zoals creditcardgegevens kunnen stelen. Kijk voor meer informatie op: abnamro.nl/nl/zakelijk/insights/cybersecurity/web-skimming

Bijlage 2
Uitleg termen

DDoS

Distributed Denial-of-Service-aanvallen (DDoS-aanvallen) zijn pogingen om een computer, computernetwerk of dienst onbereikbaar te maken voor gebruikers. Typerend is dat meerdere computers tegelijk de aanval uitvoeren op een doelwit. Voor DDoS wordt vaak een programma gebruikt waarmee dat automatisch gebeurt (een botnet), maar het kan ook gaan om meerdere personen die hun acties coördineren. Zoiets gebeurt bijvoorbeeld bij aanvallen van de zogeheten Anonymous-beweging. Vaak zijn de doelen prominente websites of diensten.

Een veel voorkomende vorm van een DDoS-aanval is het doelbewust overbelasten van het systeem met externe communicatieverzoeken. Daardoor kan het systeem niet reageren op legitieme verzoeken of het wordt daardoor zo traag dat het niet meer effectief te gebruiken is. Dit soort aanvallen leidt doorgaans tot overbelasting van de server.

Keylogger

Een keylogger is een type surveillance software, dat de mogelijkheid biedt om elke toetsaanslag die de gebruiker doet, vast te leggen in een logbestand. Een keylogger kan zo alle wachtwoorden en e-mails die de gebruiker intikt via het toetsenbord vastleggen. Het logbestand dat met de keylogger is gemaakt, kan daarna worden verstuurd.

Macro-virus

Veel voorkomende toepassingen zoals Microsoft Outlook en Microsoft Word staan toe dat macro's worden geïntegreerd in documenten of e-mails. Deze macro's (programma's) worden automatisch uitgevoerd zodra het document wordt geopend. Een macro-virus (ook wel documentvirus genoemd) is een virus dat in een macro-taal is geschreven. Het infecteert de computer van de gebruiker zodra het bestand zich opent. Dit is een van de redenen waarom het gevaarlijk is om onverwachte bijlagen in een e-mail te openen.

Malware

Malware is een samentrekking van het Engelse malicious software (kwaadaardige software). Malware wordt gebruikt om computersystemen te verstoren en te beschadigen, maar kan ook gevoelige informatie verzamelen of toegang proberen te krijgen tot computersystemen.

Phishing

Phishing is een vorm van internetfraude waarbij criminelen via e-mail proberen om vertrouwelijke informatie in handen te krijgen, zoals gebruikersnamen, wachtwoorden en creditcardgegevens. Maar phishing kan ook tot andere schade leiden. Criminelen proberen vaak om – onder valse voorwendselen – mensen te verleiden op een link te klikken. Die link leidt naar een valse website die sprekend lijkt op de legitieme website. Criminelen sturen bijvoorbeeld e-mails die zo op het oog afkomstig zijn van populaire sociale websites, banken, creditcardbedrijven of IT-bedrijven. Vaak wordt mensen gevraagd om bepaalde informatie in te voeren die dan later kan worden misbruikt. Ook kunnen mensen worden verleid om bijlages te openen, waardoor schadelijke software wordt geïnstalleerd.

Phishing is een voortdurende bedreiging en door sociale media als Facebook, LinkedIn en Twitter is het risico nog groter geworden. Hackers maken een kloon van een website en verleiden slachtoffers om persoonlijke gegevens in te voeren. Zij profiteren van het vertrouwen dat de gebruiker heeft in deze bedrijven en het gegeven dat veel gebruikers niet in staat zijn om te beoordelen of de site echt is of niet.

Spyware

Spyware is elke vorm van technologie die helpt bij het verzamelen van informatie over een persoon of organisatie zonder hun medeweten. Spyware (ook wel Spybot of trackingsoftware genoemd) is software die op iemands computer wordt gezet om in het geheim informatie te verzamelen over de gebruiker. Die informatie wordt vervolgens doorgegeven aan adverteerders of andere belanghebbenden. Spyware komt op een computer via een softwarevirus of via het installeren van een nieuw programma.

Trojan

Een Trojan is malware dat zich voordoet als een legitiem programma. Het programma kan een legitieme functie hebben, maar heeft bijbedoelingen. Trojans kunnen gegevens verwijderen, de beveiliging uitschakelen of een computer infecteren. Trojans worden over het algemeen verspreid via phishing, maar een Trojan kan ook meekomen via een bestand bij een download. Veel moderne Trojans fungeren als een achterdeur waardoor een onbevoegde toegang kan krijgen tot de computer.

Virus

Een computervirus hecht zich aan een programma of bestand zodat het zich kan verspreiden van de ene naar de andere computer. Een virus kan behalve computerprogramma's ook databestanden en zelfs het opstartdeel van de harde schijf (bootsector) infecteren. Een virus vernietigt vaak gegevens of zoekt naar zaken als wachtwoorden, creditcardnummers en andere gevoelige gegevens. Bijna alle virussen zijn gekoppeld aan een uitvoerbaar bestand (herkenbaar aan de extensie .exe).

Dat betekent dat een virus op uw computer de computer niet kan besmetten, tenzij het programma wordt uitgevoerd. Het is dus belangrijk om te weten dat een virus alleen kan worden verspreid door menselijk handelen. Bijvoorbeeld door het uitvoeren van een geïnfecteerd programma. Mensen dragen zo dus onbewust bij aan de verspreiding van een computervirus door het delen van de geïnfecteerde bestanden of het versturen van e-mails met een virus als bijlage.

Worm

Een computerworm is een losstaand computerprogramma dat zichzelf repliceert om zich te verspreiden naar andere computers. Vaak verspreidt het zich via het computernetwerk door gebruik te maken van zwakke plekken in de beveiliging. In tegenstelling tot een computervirus heeft een worm geen ander programma nodig om zich aan te hechten. Wormen veroorzaken bijna altijd enige schade aan het netwerk, terwijl virussen bijna altijd bestanden op een computer wijzigen of onbruikbaar maken. Wormen komen vaak via e-mail binnen en sturen een kopie van zichzelf naar alle e-mailadressen in het adresboek, vermomd als bericht van de gebruiker. Wormen worden vaak gebruikt om virussen te verspreiden

Bijlage 3
Nuttige online documentatie

ABN AMRO: Veilig zakendoen
abnamro.nl/nl/zakelijk/insights/cybersecurity/index

ABN AMRO: Cyber Trends Rapport 2024
abnamro.nl/nl/zakelijk/insights/sectoren-en-trends/technologie/cyberaanval-schudt-ondernemer-lang-niet-altijd-wakker

ABN AMRO: Praktijkgids NIS2
doorpakken.abnamro.nl/hulpmiddelen-en-diensten/veilig-ondernemen/nis2/download-nis2-praktijkgids/

Digital Trust Center: Incident response plan
digitaltrustcenter.nl/incident-response-plan

Nationaal Cyber Security Centrum
ncsc.nl

KVK: Werk jij digitaal veilig? Controleer het met de checklist
kvk.nl/veilig-zakendoen/werk-jij-digitaal-veilig-controleer-het-met-de-checklist/

Samen Digitaal Veilig: Alles over NIS2 voor de MKB
samendigitaalveilig.nl

ABN·AMRO