ABN·AMRO

De belangrijkste cybersecurity-bedreigingen

En wat u er tegen kunt doen

Introductie

In het door internet gedomineerde tijdperk komt cybercriminaliteit steeds vaker voor. Het is voor bedrijven van belang om zich hiertegen te beschermen. Cybersecurity biedt hierbij een uitkomst: het zorgt voor het beschermen van ICT-componenten tegen verstoring of schadelijke aanvallen. Onder ICT vallen onder andere computers, servers en netwerken. Cybersecurity zorgt er voor dat de kans minder groot is dat betrouwbare en vertrouwelijke informatie wordt gestolen of doorverkocht aan cybercriminelen.

Er bestaan meerdere soorten cyberbedreigingen, ook wel *cyber threats* genoemd. Wij zullen verder inzoomen op de 10 meest voorkomende cyberbedreigingen, waarmee midden-- en kleinbedrijven kunnen worden geconfronteerd: phishing, wachtwoord-hergebruik, malware et cetera. De gevolgen van deze bedreigingen komen aan bod, met aanbevelingen tot het beschermen tegen deze bedreigingen.

Phishing

Beschrijving

Phishing kan gezien worden als digitale oplichting. Dit kan op verschillende manieren:

- Via links in e-mails. Cybercriminelen kunnen proberen om login-gegevens te verkrijgen of computers te infecteren. Login-gegevens kunnen worden verkregen door het sturen van een e-mail met een link. Als op de link wordt geklikt, wordt de persoon naar een nagemaakte website gestuurd. Daar wordt gevraagd om in te loggen. Het gevolg is dat cybercriminelen login-gegevens verkrijgen.
- Via bijlagen in e-mails. Infecteren van de computer kan door een kwaadaardige bijlage in een e-mail. Wanneer de bijlage wordt geopend, wordt de malware automatisch (ongezien) gedownload. Hierdoor kunnen cybercriminelen toegang krijgen tot het bedrijfsnetwerk.
- Phishing via SMS wordt ook wel SMishing genoemd. Bij SMishing wordt er een tekstbericht gestuurd naar een ondernemer. Het lijkt er dan op dat dit bericht wordt verstuurd door een ander bedrijf. Er wordt gevraagd naar persoonlijke of financiële gegevens zoals een rekeningnummer. Wanneer deze gegevens worden verstrekt kunnen cybercriminelen daar misbruik van maken.

Gevolgen

Phishing kan er voor zorgen dat de cybercriminelen toegang krijgen tot computers om (vertrouwelijke) informatie te verkrijgen. Dit kan bijvoorbeeld ten behoeve van afpersing of om informatie door te verkopen aan andere cybercriminelen. Informatie kan direct worden ontvreemd bij toegang tot het netwerk, maar cybercriminelen kunnen zich ook een tijd ‘schuilhouden’ in het netwerk om later toe te slaan.

Aanbevelingen

Onderstaande aanbevelingen verkleinen de kans op infectie:

- Zorg ervoor dat uw bedrijf een goede antivirusscanner en spamfilter heeft, zodat valse e-mails bij detectie worden geblokkeerd.
- Zorg voor awareness bij medewerkers door middel van (online) trainingen.
- Controleer de afzender van e-mails. Weet van wie de e-mail afkomstig is voordat de mail wordt geopend. En controleer of de inhoud van de e-mail past bij de afzender.
- Zorg dat er een meldpunt is dat u kunt benaderen als er (mogelijk) sprake is van phishing, zodat er zo snel mogelijk maatregelen kunnen worden getroffen. Een meldpunt kan een ICT-team of leverancier zijn.

Wachtwoord hergebruik

Beschrijving

Het hergebruiken van hetzelfde wachtwoord voor verschillende systemen, is een grote bedreiging voor bedrijven. Wanneer een cybercrimineel, bijvoorbeeld door phishing, het wachtwoord heeft verkregen, kan de crimineel in elk systeem komen waar hetzelfde wachtwoord wordt gebruikt.

Gevolgen

Wanneer hetzelfde wachtwoord voor alle systemen en/of netwerken wordt gebruikt en de cybercrimineel heeft dit wachtwoord verkregen, dan kan in alle systemen en/of netwerken worden ingelogd waar hetzelfde wachtwoord wordt gebruikt. Dit betekent dat de crimineel de controle in handen heeft en toegang heeft tot alle vertrouwelijke informatie van het bedrijf.

Aanbevelingen

- Zorg dat elke login een ander wachtwoord heeft. Maak gebruik van een complex password, gebruik hiervoor hoofdletters, cypers en leestekens.
- Maak gebruik van een password-manager. Hier kunnen alle gebruikersnamen en wachtwoorden worden opgeslagen. Dit voorkomt dat u veel wachtwoorden moet onthouden. Tevens maakt een password-manager het mogelijk om lastigere, langere wachtwoorden te maken.

Business Email Compromise

Beschrijving

In Business Email Compromise (BEC) richten cybercriminelen zich op belangrijke personen binnen een bedrijf. Bijvoorbeeld een CEO, CFO of medewerkers van een financiële afdeling. Naar deze personen is vooraf grondig onderzoek gedaan, omdat het bedrijf zorgvuldig als slachtoffer is uitgekozen. De cybercriminelen vervalsen het emailadres van de gekozen persoon door bijvoorbeeld één letter toe te voegen. Dit is vaak niet (direct) zichtbaar voor het slachtoffer. Via het vervalste mailadres proberen de criminelen vervolgens de medewerker te misleiden om geld over te maken. Vaak wordt er in de email gesproken van een spoedoverboeking, waardoor het slachtoffer geen tijd wil verliezen en het geld gelijk overmaakt.

Gevolgen

Het gevolg van BEC is een groot financieel verlies voor een bedrijf. Het overgemaakte bedrag is vaak lastig terug te halen, omdat de persoon een 'legitieme' transactie heeft uitgevoerd. Een ander mogelijk gevolg van BEC is eventuele reputatieschade.

Aanbevelingen

- Zorg voor een goed email detectiesysteem dat phishing als fake e-mails blokkeert.
- Zorg voor een goed detectiesysteem dat e-mails die niet op de whitelist staan, snel detecteert.
- Creëer detectieregels voor het monitoringssysteem waarmee spoofed e-mails kunnen worden gedetecteerd en medewerkers kunnen worden gealarmeerd.
- Controleer regelmatig tegengehouden e-mails. Wanneer hier een e-mail tussen zit die lijkt op die van de CEO, of medewerker, zet het domein of de afzender dan op een blacklist.

Insider-dreiging

Beschrijving

Insiders zijn personen binnen een bedrijf met toegang tot netwerkinformatie van het bedrijf. Insiders behoren tot de grootste bedreigingen voor bedrijven omdat zij vaak deel uitmaken van een incrowd. Insider-dreigingen kunnen de vorm aannemen van sabotage, fraude, diefstal van activa, verstoring, spionage of het stelen van intellectuele eigendommen. Een insider-dreiging kan plaatsvinden door een ontevreden medewerker, een externe contractant of iemand met directe toegang tot het gebouw of de host-werkstations van een bedrijf.

Gevolgen

De gevolgen van een insider-attack kunnen groot zijn. Omdat het gaat over een interne medewerker of groep waarvan het bedrijf geen bedreiging verwacht en zich daarom minder gemakkelijk kan beveiligen.

Aanbevelingen

- Geef medewerkers alleen toegang tot bestanden en data die nodig zijn voor hun werk. Toegang tot andere gegevens dient te worden geblokkeerd en/of zo veel mogelijk beperkt.
- Zorg dat medewerkers belangrijke documenten alleen kunnen lezen en niet kunnen aanpassen. Er kunnen bijvoorbeeld regels worden gecreëerd over wie toestemming heeft om documenten te kunnen wijzigen.
- Bewaar auditlogs van systemen, zodat altijd gecontroleerd kan worden wie welk bestand heeft ingezien en aangepast.

Malware

Beschrijving

Malware is een afkorting voor *malicious software* en is ontworpen om malafide activiteiten uit te voeren. Er zijn twee typen vaak voorkomende malware.

1. Frequent voorkomende malware is ransomware. Bij ransomware worden bestanden in de computer versleuteld zodat deze niet meer gebruikt kunnen worden door de gebruiker. Deze bestanden kunnen alleen worden ontsleuteld door geld over te maken naar de criminelen. Vaak staan betaalinstructies in een tekstbestand, dat tussen de documenten wordt achtergelaten. Wanneer het geld is ontvangen, worden de documenten mogelijk vrij gegeven voor gebruik of krijgt men de decryptiesleutel om de bestanden te ontsleutelen.
2. Spyware is een andere vorm van malware. Spyware verzamelt gegevens van een computer (of ander apparaat) en stuurt deze door naar cybercriminelen. Dit is niet zichtbaar voor het slachtoffer. Het gaat hierbij voornamelijk om vertrouwelijke gegevens zoals gebruikersnamen, wachtwoorden en betaalgegevens.

Gevolgen

Naast het lekken van vertrouwelijke gegevens, kunnen door malware onverklaarbare foutmeldingen op de computer of in het systeem voorkomen. De computer wordt traag en kan crashen of oververhitten.

Aanbevelingen

- Download alleen bestanden van een betrouwbare website of e-mail afzender.
- Controleer of de e-mail daadwerkelijk door de afzender is verstuurd.
- Zorg voor een goede antivirusscanner.

Kwetsbaarhedenexploitatie

Beschrijving

ICT-componenten en software/applicaties zijn kwetsbaar als deze niet up-to-date zijn. Het is van groot belang dat alle systemen worden voorzien van de nieuwste software en beveiligingspatches.

Gevolgen

Wanneer systemen niet goed beveiligd zijn, lopen deze grote kans gebruikt te worden door cybercriminelen om in het netwerk van het bedrijf te komen of om informatie buit te maken.

Aanbevelingen

- Zorg voor een goede kwetsbaarheidsscanner. Deze software scant de computersystemen en netwerk componenten op kwetsbaarheden, zoals verouderde software/firmware en misconfiguratie.
- Zorg dat de software/firmware van uw apparaten zoveel mogelijk up-to-date is.
- Maak iemand verantwoordelijk voor het controleren en identificeren van nieuwe kwetsbaarheden en het erop toezien dat deze worden verholpen.

Kwetsbaarheden in Cloud-services

Beschrijving

Het wordt tegenwoordig steeds populairder om data op te slaan in de Cloud. Gegevens in de Cloud kunnen ten alle tijden worden opgevraagd en bewerkt. De Cloud-serviceprovider is verantwoordelijk voor het onderhoud van apparatuur, beschikbaarheid van de opgeslagen gegevens en bescherming van gegevens wanneer deze worden verplaatst tussen locaties van serviceproviders. Wanneer de gegevens niet goed beschermd zijn, kunnen cybercriminelen 'inbreken' in de Cloud en gegevens stelen. Het risico van de Cloud is dat gegevensbescherming niet in eigen handen is.

Gevolgen

Als gegevens uit de Cloud worden gestolen, kunnen de gevolgen voor een bedrijf groot zijn. Gegevens kunnen worden verkocht of openbaar gemaakt worden.

Aanbevelingen

- Zorg voor een betrouwbare provider die de Cloud goed beveiligt en deze up-to-date houdt.
- Maak duidelijke Service Level Agreement-overeenkomst over beschikbaarheid, betrouwbaarheid en integriteit van data.
- Zorg dat duidelijk is waar incidenten direct kunnen worden gemeld en verholpen.
- Zorg ervoor dat uw Cloud-provider beoordeeld is door onafhankelijke partijen.

(D)DoS aanval

Beschrijving

(Distributed) Denial of Service, ook wel (gedistribueerde) netwerkaanvallen, richten zich op de capaciteitlimiet op netwerkbronnen van een bedrijf. Denk hierbij aan de infrastructuur die de website van een bedrijf faciliteert. Bij een (D)DoS aanval wordt zoveel verkeer naar de aangevallen website/applicatie verstuurd, dat deze niet meer (goed) kan functioneren en onbruikbaar kan worden.

Gevolgen

De website/applicatie van het bedrijf kan onbereikbaar raken, waardoor klanten de diensten van het bedrijf niet meer kunnen raadplegen. Dit kan een financieel verlies van het bedrijf betekenen.

Aanbevelingen

- Zorg voor een Web Application Firewall voor de webservers van de website.
- Zorg voor netwerksegmentatie, zodat computers niet met elkaar kunnen ‘praten’. Dit maakt de kans op een succesvolle (D)DoS aanval kleiner.
- Gebruik (D)DoS beschermingsservices van gerenommeerde leveranciers.
- Zorg dat uw website en medewerkersnetwerk gescheiden zijn.

Supply Chain-dreiging

Beschrijving

Een supply chain-aanval vindt plaats wanneer iemand het systeem van een bedrijf infiltreert via een externe partner of provider met toegang tot systemen en gegevens. Doordat de externe partner of provider wordt gezien als betrouwbaar, kunnen cybercriminelen hierdoor makkelijk toegang krijgen tot informatie. Het detectiesysteem zal interacties beschouwen als normaal verkeer, zolang de aanvaller geen vreemd verkeer genereert.

Gevolgen

Criminelen kunnen via een derde partij informatie buitmaken, niet alleen van het bedrijf maar ook van anderen die zijn aangesloten bij deze partij.

Aanbevelingen

- Onderzoek de veiligheid en betrouwbaarheid van de derde partij.
- Maak een duidelijke SLA-overeenkomst over CIA (vertrouwelijkheid, integriteit en beschikbaarheid) en de gevolgen daarvan.

Dreiging van derde partijen

Beschrijving

In tegenstelling tot supply chain-dreiging, waarbij criminelen via leveranciers/derde partijen de organisatie binnendringen, zijn bij derde partijen-bedreigingen juist de derde partijen zélf die misbruik maken van hun relatie met het bedrijf. Zwakke beveiliging bij gecontracteerde derde partijen of op externe locaties kan uitgebuit worden om niet-geautoriseerde toegang tot systemen en dus ook vertrouwelijke informatie te krijgen.

Gevolgen

Vertrouwelijke informatie kan worden gestolen en worden gebruikt voor afpersing of verkoop aan andere cybercriminelen.

Aanbevelingen

- Maak alleen gebruik van vertrouwde partijen.
- Maak een duidelijke SLA-overeenkomst over CIA (vertrouwelijkheid, integriteit en beschikbaarheid) en de gevolgen daarvan.
- Beoordeel de beveiligingsaudits van derden.
- Vraag bewijs van certificaten aan.