axians

E-BOOK

De ultieme gids met 33 cyber security termen die je moet kennen

Axians
Rivium Boulevard 41
2909 LK Capelle aan den IJssel
Tel: +31 88 988 96 00
axians.nl/cybersquad

The best of ICT with a human touch

VINCI ENERGIES

Begrippenlijst

Van CASB tot SOC en Zero Trust

Zie jij door alle afkortingen het (security) landschap nog? Het lijkt alsof er dagelijks nieuwe cyber security-termen bijkomen. Naarmate het aantal toeneemt, groeit ook de verwarring over de betekenis van deze afkortingen en begrippen. Om je te helpen het overzicht te behouden en te bepalen welke security-maatregelen voor jouw organisatie interessant zijn, hebben we deze gids gemaakt. Een leidraad, met als uitgangspunt het NIST cyber security framework, waarbij de begrippen zijn gekoppeld aan één van de vijf pijlers of aansluiten op de wet- en regelgeving.

"Aan de hand van het NIST framework helpen we organisaties bij het bouwen van een sterke security-architectuur."

NIST Framework

Het NIST Cyber Security Framework is ontwikkeld door het National Institute of Standards and Technology. Sinds 1972 voert dit instituut cyber security-onderzoek uit en ontwikkelt het richtlijnen voor cyberbeveiliging. Het framework is gebaseerd op bestaande normen, richtlijnen en practices en is voor organisaties om cyberrisico's te beheren en verminderen. Daarnaast bevordert het de communicatie over risico- en cyberbeheer tussen zowel interne als externe belanghebbenden. Aan de hand van het NIST framework helpen we organisaties bij het bouwen van een sterke security-architectuur. De pijlers – identify, protect, detect, respond, recover – en bijbehorende begrippen lichten we in dit e-book toe.

Identify

Systemen, mensen, data en processen zijn kwetsbaar voor cyberaanvallen en datalekken. De eerste stap in het voorkomen daarvan is begrijpen wat je kroonjuwelen, huidige processen en risico's zijn. Welke software en welke fysieke componenten ondersteunen welke processen? Wat is de waarde van die processen en wat zijn de specifieke risico's? Dit geeft je de focus om te bouwen aan een solide security-strategie.

Security maturity

Om te weten waar je moet beginnen en waar de prioriteiten liggen, kijk je eerst naar hoe volwassen je security is: de security maturity. Is jouw organisatie in de veranderende omgeving nog veilig? Zijn je tools, mensen en processen klaar voor onbekende dreigingen? Hiervoor zijn verschillende frameworks beschikbaar die je op een gestructureerde manier helpen om grip te krijgen op jouw security.

CIS18

De CIS18 scan, afkomstig van het Center for Internet Security, brengt de volwassenheid van jouw IT-omgeving in kaart aan de hand van zogenoemde 'controls'. Het is een volledige audit op alle aspecten van security: software, mensen en proces. Je start met een nulmeting waarmee je zicht krijgt op wat het verschil is tussen het huidige en het gewenste security-niveau. Na deze audit weet je dus precies hoe volwassen je security is en met welke aandachtspunten je als eerste aan de slag kan. Dit vormt de basis voor je roadmap; een verbeterplan waarin je vastlegt aan de hand van welke acties je binnen welke tijd het gewenste doel wil gaan halen.

Indien je in verband met compliance redenen ook te maken hebt met bijvoorbeeld ISO27001, OASP of MITRE ATT&CK, dan biedt CIS18 hier bovendien vertalingen naar.

"Systemen, mensen, data en processen zijn kwetsbaar voor cyberaanvallen en datalekken. De eerste stap in het voorkomen daarvan is begrijpen wat je kroonjuwelen, huidige processen en risico's zijn."

MITRE ATT&CK

Het MITRE ATT&CK is een kennisbank waarin onder andere de tactieken en technieken die cyberaanvallers gebruiken, worden vastgelegd. Gebaseerd op observaties uit de echte wereld. Bijvoorbeeld threat hunters en redteams gebruiken deze kennisbank om aanvallen te classificeren, doelen te identificeren en het risico van een organisatie te beoordelen. Op basis van dit overzicht kunnen vendoren bovendien aangeven tegen welke dreigingen een oplossing bescherming kan bieden. Wat vervolgens handvaten biedt om te bepalen welke oplossingen het beste aansluiten bij de wensen van jouw organisatie.

Vulnerability scan

In de aanwezige systemen en applicaties van de organisatie kunnen zich kwetsbaarheden (vulnerabilities) bevinden. Kwetsbaarheden kunnen ertoe leiden dat een aanvaller ongezien jouw infrastructuur binnenkomt. Het is dus van belang dat je actief een overzicht bijhoudt van de gebruikte systemen en applicaties en dit vervolgens vergelijkt met de nieuwe CVE's (Common Vulnerabilities and Exposures) die dagelijks uitkomen. Een vulnerability scan is niet een oplossing die je eenmalig of periodiek uitvoert. Het identificeren van de risico's en kwetsbaarheden moet je constant uitvoeren, zie ook Vulnerability management.

CVE
Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures is een lijst met informatie over bekende kwetsbaarheden in software. Het doel hiervan is het identificeren, definiëren en vastleggen van openbaar gemaakte cyber security-kwetsbaarheden, zodat organisaties die de software gebruiken de juiste acties kunnen ondernemen.

Vulnerability management

Met vulnerability management heb je altijd een actueel overzicht van alle kwetsbaarheden in de systemen en applicaties die in je landschap draaien. Hierdoor kun je sneller en adequater reageren op veiligheidsdreigingen. Dit kan aan de hand van advies en rapportages op maat, waardoor je altijd op de hoogte bent van wat je moet patchen, welke patches beschikbaar zijn en welke kwetsbaarheden prioriteit moeten krijgen.

Pentest / penetratietest

Met een pentest / penetratietest worden 'real-life' aanvallen nagebootst om methoden te identificeren voor het omzeilen van de beveiligingsfuncties van een applicatie, systeem of netwerk. Met behulp van tools en technieken die aanvallers normaal gebruiken, wordt een aanval geïnitieerd op echte systemen en gegevens. Het doel van de meeste tests is zicht krijgen op combinaties van kwetsbaarheden op een of meerdere systemen, die aanvallers kunnen gebruiken om meer toegang te krijgen dan via een enkele kwetsbaarheid. Daarnaast kan je een pentest bijvoorbeeld gebruiken om te bepalen in welke mate het systeem aanvallen verdraagt en welke aanvullende maatregelen de organisatie moet nemen om het systeem te versterken.

De drie categorieën die je hierin kan onderscheiden zijn:

- Black-box | Hiermee simuleer je echte hacks, het testteam krijgt geen informatie over de IT-infrastructuur.
- Grey-box | Hierbij krijgt het testteam een gebruikersaccount van een standaard medewerker / klant.
- White-box | Hiermee controleer je of netwerksystemen correct zijn geconfigureerd. Het testteam krijgt inzicht in de beheerdersrechten en toegang tot configuratiebestanden.

CMDB
Configuration Management Database

In de Configuration Management Database (CMDB) staat de informatie over de componenten waaruit je IT-infrastructuur bestaat. Deze componenten worden vaak CI's, oftewel configureerbare items, genoemd. In de CMDB staan ook de kenmerken van de CI's, zoals het serienummer, het hardware ID, de onderhoudscontracten en eventuele licenties, en de onderlinge relaties.

Protect

Het actief beschermen van je data, apps en infrastructuur is nodig om problemen te voorkomen. Maar waar begin je? Je hebt veel data en die data reizen iedere seconde van de dag door een complex landschap van applicaties, devices en hybride infrastructuren. In zo'n omgeving, die bovendien snel verandert, is het lastig om te bepalen welke actie de meeste impact heeft en prioriteiten te stellen. Je netwerk en applicatielandschap beperken zich namelijk steeds minder tot je eigen infrastructuur. Steeds meer functionaliteiten en data bevinden zich in public clouds en SaaS-applicaties. Bovendien werken we al lang niet meer iedere dag op kantoor.

SASE

Secure Access Service Edge

Secure Access Service Edge (SASE) is niet een product, maar meer een concept bestaande uit enerzijds een combinatie van uitgebreide connectivity-technieken (zoals SD-WAN) en anderzijds een set aan beveiligingsfuncties (gefocust op cloud security). Het is een nieuwe manier om netwerk en beveiliging te implementeren met als doel de dynamische, veilige toegangsbehoeften van organisaties te ondersteunen. Tegenwoordig – met de komst van de cloud – zijn namelijk gebruikers, apparaten en de netwerkmogelijkheden waartoe ze veilig toegang nodig hebben, overal. Ook de beveiligde toegangsdiensten moeten daarom overal aanwezig zijn. Gartner introduceerde dit concept in 'The future of network security is in the cloud' in 2019.

De identiteit van de gebruiker, het apparaat of de service is bij SASE een van de belangrijkste onderdelen waarmee je rekening houdt in het toegepaste beleid. Andere relevante bronnen zijn de locatie van de identiteit, het tijdstip, de risico- / vertrouwensbeoordeling van het apparaat waar de gebruiker toegang toe heeft en de gevoeligheid van de gegevens waar de gebruiker toegang toe wil. Het enterprise datacenter is dus niet meer het centrum van de architectuur. Het is slechts een van de vele op internet gebaseerde services waartoe gebruikers en apparaten toegang moeten hebben.

De kerncomponenten van SASE zijn SD-WAN (netwerk), SWG, CASB, ZTNA en FWaaS (security). De security-componenten worden hieronder verder toegelicht.

SSE

Security Service Edge

Eind 2021 introduceerde Gartner een nieuw concept genaamd 'Security Service Edge' (SSE). Dit beschrijft alleen het Security as a Service gedeelte van SASE en laat het Network as a Service deel buiten beschouwing.

DNS security

Wanneer je een website opent, wordt het Domain Name System (DNS) gebruikt om de naam van de site te vertalen in een IP-adres. De functie van DNS is cruciaal en dus kwetsbaar, waardoor dit een populair doelwit is voor hackers. DNS security biedt beveiligingsopties om DNS aanvragen en antwoorden te beschermen.

SWG

Secure Web Gateway

Een Secure Web Gateway (SWG) beschermt gebruikers tegen web-gebaseerde bedreigingen. In plaats van rechtstreeks verbinding te maken met een website krijgt een gebruiker toegang tot de SWG. Deze is vervolgens verantwoordelijk voor het verbinden van de gebruiker met de gewenste website en het uitvoeren van functies, zoals URL-filtering, web-zichtbaarheid, inspectie van schadelijke inhoud, web-toegangscontroles en andere beveiligingsmaatregelen.

"Het actief beschermen van je data, apps en infrastructuur is nodig om problemen te voorkomen."

SWG's vormen een belangrijk onderdeel van een uitgebreide SSE-strategie. Hiermee bied je namelijk gebruikers veilige internettoegang wanneer ze geen verbinding hebben met de zakelijke VPN. Bovendien kan je de toegang tot ongepaste websites of inhoud blokkeren op basis van acceptabel gebruiksbeleid, beveiligingsbeleid afdwingen om internettoegang veiliger te maken en helpen gegevens te beschermen tegen ongeoorloofde overdracht.

CASB

Cloud Access Security Broker

Cloud Access Security Brokers (CASB's) helpen organisaties te ontdekken waar hun gegevens zich bevinden in de Software as a Service (SaaS)-applicaties. Ook geven ze aan of deze gegevens in beweging zijn in cloud-omgevingen, on-premise datacenters of toegankelijk zijn voor mobiele werknemers. Een CASB dwingt ook het beveiligings-, governance- en nalevingsbeleid van een organisatie af. Geautoriseerde gebruikers hebben hierdoor toegang tot cloud-resources en ze kunnen deze gebruiken. Terwijl organisaties tegelijkertijd hun gegevens op meerdere locaties effectief en consistent kunnen beschermen.

Zero Trust

Zero trust is een principe dat is ontwikkeld met als basisgedachte 'never trust, always verify'. Je vertrouwt niet op het bestaan van een 'veilig intern netwerk'. Elke gebruiker die of elk apparaat en IP-adres dat toegang wil, vormt een bedreiging totdat tegendeel is bewezen. Je kan dit principe als organisatie implementeren aan de hand van een strikte toegangscontrole en door alles te verifiëren dat verbinding probeert te maken met het netwerk van de organisatie.

ZTNA

Zero Trust Network Access

Zero Trust Network Access (ZTNA) is een categorie technologieën die veilige, externe toegang biedt tot applicaties en services op basis van gedefinieerd toegangscontrolebeleid. In tegenstelling tot virtuele privénetwerken (VPN's), die volledige toegang tot een LAN verlenen, weigeren ZTNA-oplossingen standaard en bieden ze alleen de toegang tot services die je expliciet aan de gebruiker verleent.

FWaaS

Firewall as a Service

Met FWaaS (Firewall as a Service) kunnen firewalls worden geleverd als onderdeel van de cloud-infrastructuur van een organisatie om cloud-gebaseerde gegevens en applicaties te beschermen.

Een SSE-strategie maakt gebruik van FWaaS-mogelijkheden, zodat je verkeer uit meerdere bronnen kan verzamelen. Of het nu gaat om on-site datacenters, filialen, mobiele gebruikers of cloud-infrastructuur. Het zorgt ook voor een consistente toepassing en handhaving van het beveiligingsbeleid op alle locaties en gebruikers, terwijl je volledige zichtbaarheid hebt op het netwerk zonder fysieke apparaten te implementeren.

DDoS

Distributed Denial of Service

Met een DDoS-aanval sturen cybercriminelen gigantische hoeveelheden data naar een server om de omgeving te overbelasten. Met als doel deze onbereikbaar te maken. De aanvallen van vandaag zijn geëvolueerd en omvatten nu DDoS-toolkits, bewapende IoT-apparaten, online DDoS-services en meer. Gevestigde oplossingen, die afhankelijk zijn van ineffectieve, op handtekeningen gebaseerde IPS of alleen beperking van de verkeerssnelheid, zijn niet langer toereikend.

"Met een Identity and Access Management (IAM) -oplossing kunnen IT-beheerders de digitale identiteiten en gerelateerde toegangsrechten van gebruikers veilig en effectief beheren."

IAM

Identity and Access Management

Met een Identity and Access Management (IAM) -oplossing kunnen IT-beheerders de digitale identiteiten en gerelateerde toegangsrechten van gebruikers veilig en effectief beheren. Ze kunnen gebruikersrollen instellen en aanpassen, gebruikersactiviteit traceren en rapporteren, en bedrijfsbeleid en beleid voor de naleving van richtlijnen afdwingen om de data security en privacy te waarborgen.

PAM

Privileged Account/ Access Management

In PAM staat de P voor Privileged en de M voor Management. Waar de A voor staat, zijn de meningen over verdeeld. Dit kan zijn Account, of Access. Beide betekenissen kloppen, en zijn logisch. Want met PAM:

- ken je 'hoog risico' rechten toe op het moment dat deze voor een bepaalde taak noodzakelijk zijn en trek je ze weer in zodra deze is uitgevoerd.
- leg je de reden van deze uitgifte vast. Hierdoor kan je achteraf inzien waarom de rechten zijn toegekend en wie het heeft geautoriseerd.
- leg je de transacties vast die je hebt uitgevoerd, zodat je achteraf kan inzien wie wat wanneer heeft gedaan.

NAC

Network Access Control

Met Network Access Control (NAC) -oplossingen zorg je voor gecontroleerde toegang tot het netwerk. De voornaamste functionaliteit is 'AAA', oftewel Authenticatie, Autorisatie en Accounting. Deze drie factoren vormen de basis voor het verlenen van netwerktoegang.

Detect

Alleen wanneer je ziet wat er gebeurt in je IT-landschap en iedere potentiële dreiging in beeld hebt, weet je wat jouw organisatie moet doen om systemen, apps en data veilig te houden. Ondanks de juiste preventie is de kans groot dat een cybercrimineel de ingang naar je systemen vindt. Maar wanneer de detectie tijdig plaatsvindt, kan je de kans op schade minimaliseren.

SIEM

Security Information and Event Management

Met een SIEM wordt log-informatie gecorreleerd en geanalyseerd. Welke correlaties en log-informatie een alarm genereren, is gebaseerd op vooraf gedefinieerde 'use-cases'. Voorbeelden van veelvoorkomende use-cases behoren tot categorieën als identiteit en toegang, account-gebruik, bewaken belangrijke servers en netwerkverkeer. Wanneer bijvoorbeeld vanaf verschillende devices tegelijk honderden inlogpogingen worden gedaan, dan is er meer aan de hand. Op dat moment wordt er een alarm gegenereerd. De security-specialist kan deze alarmen monitoren en erop reageren zoals vooraf is vastgelegd in bijvoorbeeld een Incident Response plan (zie Respond).

EDR

Endpoint Detection and Response

Met een Endpoint Detection and Response (EDR) -oplossing kan een organisatie endpoints controleren op verdacht gedrag. Elke afzonderlijke activiteit en gebeurtenis wordt vastgelegd. Om context te bieden en geavanceerde dreigingen te signaleren wordt deze informatie gecorreleerd. En doordat een EDR-agent op de endpoint zelf wordt geïnstalleerd kan deze bijvoorbeeld precies aangeven of een virus is binnengekomen via een macro in MS Word of via de bijlage van een e-mail. EDR kan bovendien geautomatiseerde responsactiviteiten uitvoeren, zoals het bijna realtime isoleren van een geïnfecteerd endpoint en het voorziet je van de context die van belang is om verder onderzoek te kunnen doen naar het voorgevallen event.

"Wanneer de detectie tijdig plaatsvindt, kan je de kans op schade minimaliseren."

NDR

Network Detection and Response

Om het daadwerkelijke verkeer binnen je netwerk te monitoren, bestaat de Network Detection and Response (NDR) -oplossing. Hiermee krijg je zicht op het verkeer dat werkelijk actief is. Zo heb je ook het verkeer in beeld dat van en naar endpoints gaat waarop geen EDR-agent geïnstalleerd kan worden, zoals IoT-devices of OT-machines. NDR houdt naast het verkeer in en uit het netwerk, oftewel Noord-Zuid verkeer, ook de zijwaartse Oost-West stromen binnen het interne netwerk in de gaten. Dit maakt het mogelijk om server-naar-server communicatie te monitoren. Of het nu een fysiek datacenter is of een locatie in de cloud, iedere verandering in het gedrag van dit verkeer wordt door NDR tijdig gedetecteerd.

XDR

Extended Detection and Response

XDR is een afkorting die de laatste tijd in de cyberwereld vaak voorbij komt. Waar de afkorting voor staat zijn we het allemaal wel over eens: Extended Detection and Response. Maar de invulling van XDR (en met name de definitie van Extended) wordt door verschillende fabrikanten en dienstverleners breed geïnterpreteerd. Wij zien het als een uitbreiding op bestaande EDR- en NDR-oplossingen, waarbij Extended staat voor de integraties die geautomatiseerde respons faciliteren/realiseren en ook vooral de samenwerking vormen tussen de EDR en NDR.

SOC

Security Operations Center

Het kunnen detecteren van afwijkend gedrag is één. Het is echter alleen effectief wanneer je de meldingen die hieruit voortkomen ook daadwerkelijk monitort. In het Security Operations Center (SOC) houdt een toegewijd team van cyber security-specialisten de situatie in je IT-infrastructuur nauwlettend in de gaten. Van de gemonitorde omgeving verzamelen de experts informatie met betrekking tot security-incidenten. Deze informatie analyseren ze vervolgens op dreigingen, verdacht gedrag en risico's. Indien nodig komt het SOC vervolgens met een passend mitigatie-advies en wordt de detectie uiteraard gerapporteerd. Is er daadwerkelijk sprake van een beveiligingsincident, dan kan dit team snel en adequaat reageren, en een onderzoek initiëren naar hoe dit heeft kunnen plaatsvinden.

CDC

Cyber Defense Center

Zie omschrijving bij 'SOC'.

Circle of Visibility

Het naast elkaar gebruiken van EDR, NDR en SIEM noemen we de Circle of Visibility. Elke oplossing heeft zijn eigen kracht, maar wanneer je ze naast elkaar gebruikt, dan versterken ze elkaar. Je bouwt hiermee een 'circle of visibility' rondom je IT-infrastructuur. Wanneer je afwijkend gedrag middels logbestanden, endpoints en het netwerk kan analyseren, verklein je de kans aanzienlijk dat een cybercrimineel ongezien zijn doel kan bereiken. Gartner noemt dit ook wel de 'Visibility Triad'.

Threat hunting

Naast het wachten op een detectie, kan je ook proactief en systematisch zoeken naar signalen van potentiële dreigingen binnen het netwerk of de systemen van een organisatie. Oftewel threat hunting. Dit kan door middel van handmatige en geautomatiseerde technieken. Denk bijvoorbeeld aan het analyseren van loggegevens, het gebruiken van feeds met informatie over dreigingen en het uitvoeren van netwerkscans. Met als doel potentiële dreigingen in een vroeg stadium detecteren en hierop reageren om zo de kans dat je getroffen wordt door een cyberaanval te minimaliseren.

Respond

Snel reageren op signalen maakt het verschil als het gaat om cyberdreigingen. Dat begint met goede planning. Processen moeten worden ingericht, procedures moeten klaarliggen en medewerkers moeten voldoende getraind zijn. Zodat ze de juiste beslissingen nemen en een cyberdreiging of datalek in een vroeg stadium kunnen stoppen. Hierbij hoort ook de communicatie met alle stakholders, intern en extern, en goede informatievoorziening is essentieel.

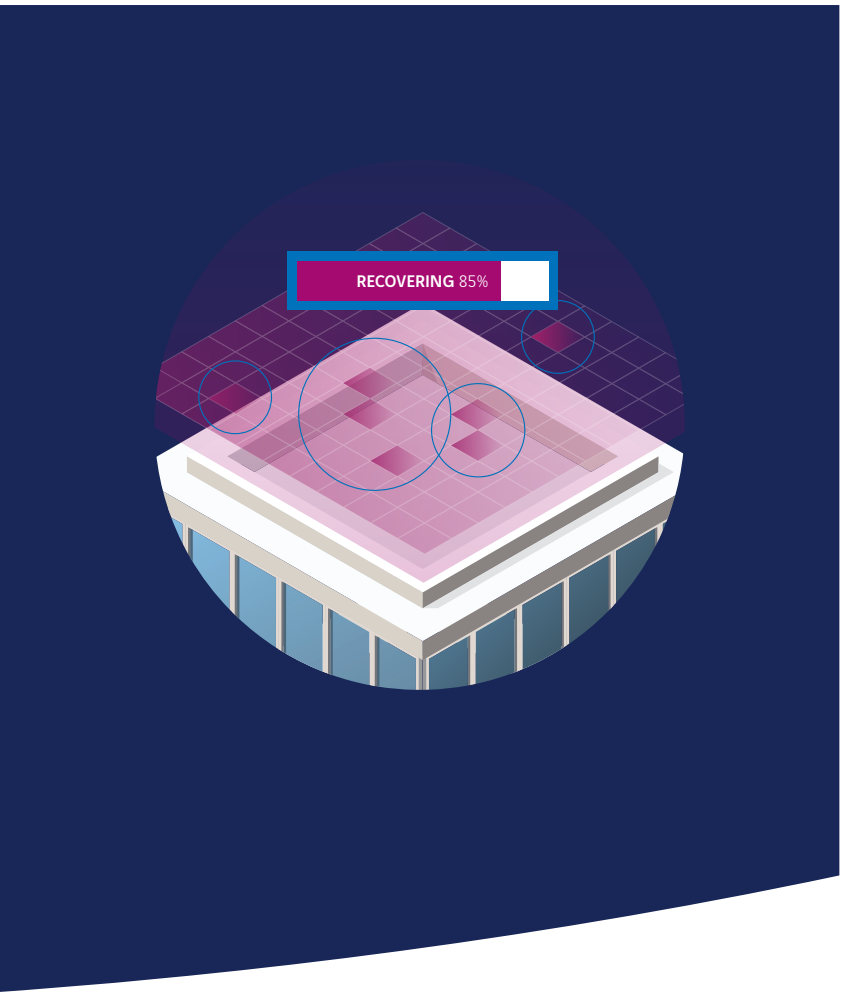
Incident Response Plan

Het proces dat gevolgd moet worden in het geval van een datalek of cyberaanval, inclusief de manier waarop de organisatie omgaat met de gevolgen van het lek of de aanval leg je vast in het Incident Response Plan.

Als je de juiste kennis en tooling hebt, kun je makkelijk de verbinding met geïdentificeerde, kwaadaardige IP-adressen blokkeren. Op basis van een database met threat signatures kun je, geholpen door machine learning-algoritmen, mogelijke aanvallen zelfs volautomatisch blokkeren. Maar het succes van dit soort systemen hangt wel af van de kwaliteit van de implementatie. Er is geen plug and play-oplossing voor security response op complexe landschappen. Kennis en ervaring blijft altijd nodig.

Recover

Indien je organisatie toch te maken krijgt met een security-incident of cyberaanval, wil je dat de schade beperkt blijft. Het verlies van onvervangbare en kritische informatie, zoals intellectueel eigendom, financiële transacties of patiënt-, student-, of klantgegevens leidt tot ernstige reputatie-, financiële of immateriële schade. Hoe zorg je dat dataverlies, ransomware of een systeemcrash zo min mogelijk invloed hebben op de continuïteit van je business? Met disaster recovery en een goede back-upstrategie zorg je ervoor dat je in control bent, ook na een incident.



Back-up

Met een back-up maak je een kopie van je gegevens, zodat je deze kan terugzetten wanneer bijvoorbeeld data wordt versleuteld door ransomware. Een incident is namelijk nooit 100% uit te sluiten. Een goede back-upstrategie is dus essentieel. Dit begint bij het maken van een plan waarin staat wanneer back-ups worden gemaakt en waar ze worden bewaard.

Bedenk ook hoe je omgaat met gevoelige systemen. Daar moet je misschien wel dagelijks of nog vaker een back-up van maken. Door kritische back-ups zo op te slaan dat ze vanuit het bronsysteem niet te traceren zijn, zijn ze niet te benaderen met normale authenticatie of beheeraccounts. Hierdoor kan de hacker, zelfs wanneer hij zich beheerrechten heeft toegeëigend, de data niet beschadigen. En vergeet de cloudapplicaties niet in het plan. Test bovendien de back-ups door deze regelmatig terug te zetten, zorg ervoor dat ze versleuteld zijn en bepaal wie er toegangsrechten moet krijgen.

Disaster recovery

Hoe reageer je op het moment dat er een cyberincident heeft plaatsgevonden? In een disaster recovery plan leg je vast in welke situatie wie wat moet doen. Hierdoor kan je de schadelijke impact op je bedrijfsvoering beperken. Daarnaast is het belangrijk om je disaster recovery plan te testen. Zo weet je zeker dat je na een hack of ander incident snel weer aan het werk kunt.

Wet- en regelgeving

"Tijdens de invoer van AVG zag je al dat organisaties en consumenten bewuster werden van de consequenties van het gebruik van persoonlijke data."

NIS 2

Sinds 2018 werken we in Europa met de NIS 1 (Network & Information Security) richtlijn voor essentiële bedrijven zoals water- en telecombedrijven. Met de komst van NIS 2 worden hogere cyber security-eisen geïntroduceerd en bovendien gelden deze voor veel meer bedrijven. Denk hierbij aan de gehele gezondheidszorg, regionale en lokale overheden, bare metal datacenters en ondernemingen die essentiële diensten leveren. Ben je een klein bedrijf (minder dan 250 medewerkers) en verleen je geen essentiële of belangrijke dienst? Dan hoef je in principe niet te voldoen aan de NIS 2. Maar ook hierop zijn uitzonderingen. Zo worden bijvoorbeeld verbonden organisaties bij elkaar opgeteld. Bovendien komt er meer aandacht voor ketenbeheer. Wanneer je samenwerkt met een essentieel bedrijf word je door NIS 2 gedwongen om aan je leveranciers in de keten eisen te stellen.

We zetten 3 tips voor een goede naleving van NIS 2 op een rijtje:

- **Weet wie je leveranciers zijn**
  Weet wat ze leveren en onder welke condities. Inventariseer welke afspraken je met ze hebt gemaakt over cyber security van hun producten en/of diensten. Voldoen ze aan de eisen van NIS 2? Zo niet, ga hier dan met hen over in gesprek en maak het in orde.

- **Beleid**
  Definieer je beleid en zorg voor een juridisch kader om intern toezicht te houden op gebruikers en beheerders. Zorg dat ze verantwoord te werk gaan (bijvoorbeeld door een 2-factor authenticatie) en kies een normenkader dat bij je past. Er zijn al goed doordachte kaders beschikbaar die je zelf kunt aanvullen, zodat ze aansluiten bij jouw organisatie.

- **Bewustwording**
  Tijdens de invoer van AVG zag je al dat organisaties en consumenten bewuster werden van de consequenties van het gebruik van persoonlijke data. Dit wordt bij de NIS 2 steeds belangrijker.

Guido Eschbach
Client Manager Security
+31 6 5362 9465
guido.eschbach@axians.com

Get in touch

Dit waren de 33 cyber security termen en de bijbehorende toelichting. Hopelijk heeft het overzicht bijgedragen in het bepalen van welke security-maatregelen voor jouw organisatie interessant zijn. Wil je weten waar je als organisatie het beste kan starten? We helpen je graag.

The best of ICT with a human touch

axians

Rivium Boulevard 41
2909 LK Capelle aan den IJssel
Tel: +31 88 988 96 00
axians.nl/cybersquad