Copaco | **Cloud Value Academy**

Thema: **Security**

e-book met de belangrijkste ins en outs over **Security**

Copaco Cloud Value Academy (CCVA)
e-book met de belangrijkste ins en outs over Security.

CCVA niveau: Essentials

Inhoudsopgave

Waterdichte security is cruciaal om als bedrijf te kunnen blijven functioneren: hiermee zorg je dat iedereen zijn werk op een efficiënte, betrouwbare en veilige manier kan blijven doen (continuïteit) en dat alle medewerkers daarbij voldoen aan de regels, zoals de privacywetgeving AVG (compliancy).

Waarom is security zo belangrijk?

Zonder security kan een organisatie niet functioneren. Organisaties die een securitytotaaloplossing gebruiken die perfect past bij hun processen, systemen en mensen profiteren van:

Continuïteit

Met de juiste securityoplossing is jouw klant gegarandeerd van een beschermde IT-omgeving. Met hardware en software waaraan geen gebruiksrisico's kleven en doen wat ze moeten doen. Het voorkomt onder andere dat cybercriminelen toegang hebben tot systemen en daar gegevens stelen, de systemen platleggen of data gijzelen. Dat kan leiden tot flinke kosten en reputatieschade. Op deze manier is security een voorwaarde voor bedrijfscontinuïteit.

Compliancy

Security zorgt voor compliancy: het leidt ertoe dat medewerkers met (privacygevoelige) bedrijfsinformatie omgaan zoals de wet dat voorschrijft. Ongeacht in welke vorm en op welk device deze informatie gebruikt wordt. Of het nou gaat om e-mail, dossiers in de cloud of apps op smartphones – de security zorgt ervoor dat jouw klant compliant is met de wet- en regelgeving, zoals de privacywet AVG. Zo voorkomt een securityoplossing dat jouw klant een boete krijgt voor het onzorgvuldig omgaan met privacygevoelige gegevens. Dit bedrag kan oplopen tot 20 miljoen euro of 4 procent van de wereldwijde omzet.

Compliance wordt verondersteld het minimale veiligheidsniveau te verhogen, maar het resulteert er vooral in dat we doen wat er van ons geëist wordt en niets meer. Het is daarom aan te raden dat niet de gehele risico-strategie is gebaseerd op compliance.

IT-onderwerpen die onlosmakelijk verbonden zijn met security

Connectivity

Meer en meer organisaties verbinden een toenemend aantal systemen met internet en we gebruiken tegenwoordig meer devices dan alleen een pc. IT-omgevingen bestaan uit uiteenlopende devices voor eindgebruikers, zoals smartphones, tablets, laptops en pc's. Op al deze apparaten gebruiken we veel verschillende applicaties, waarvan sommige op het device en andere op lokale servers of in de cloud draaien. Dit complete netwerk, met alle applicaties en hun data, op verschillende devices en opslagmedia, moet waterdicht beveiligt zijn. Een behoorlijke uitdaging, want de verbindingsmogelijkheden nemen ook verder toe. Zo komen er in een gemiddeld bedrijfsnetwerk steeds nieuwe onderdelen bij die allemaal onderling verbonden zijn. Bijvoorbeeld uiteenlopende verbindingen (waaronder draadloos), slimme hardware, applicaties en hybride IT-omgevingen. Door de toenemende connectiviteit en het groeiende aantal hybride omgevingen versnippert het IT-beheer. Dat komt doordat applicaties en data op verschillende plekken in diverse versies opgeslagen zijn. Dat alles vraagt om steeds betere en completere security.

Infrastructure

De cloud wordt steeds populairder. Dat leidt tot de opkomst van Infrastructure-as-a-Service (IaaS) en bijbehorende as-a-service-modellen, zoals Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS) en Database-as-a-Service (DBaaS). Al deze diensten hebben in de basis dezelfde voordelen: flexibel op- en afschalen, geen aanschafkosten voor hardware en licenties, gegarandeerde prestaties en pay-per-use. De opkomst van as-a-service-modellen brengt risico's voor de infrastructuur met zich mee... en vereist goede security. Hiermee weet je als organisatie zeker dat de infrastructuur continu goed in de gaten wordt gehouden. Zo neemt infrastructuurbeveiliging de IT-afdeling werk uit handen en kunnen de systeembeheerders 's avonds met een gerust hart gaan slapen.

Back-up & Disaster Recovery

Back-up en disaster recovery wordt steeds belangrijker. Dat komt in de eerste plaats doordat IT-systemen meer en meer verbonden zijn met de buitenwereld, via bijvoorbeeld de cloud en het Internet of Things (IoT). In de tweede plaats moeten medewerkers via hun laptops en mobiele telefoons toegang hebben tot bedrijfssystemen. En in de derde plaats werken veel organisaties met digitale, online bestelsystemen voor klanten en leveranciers. Al die verbindingen tussen bedrijfssystemen en de buitenwereld brengen risico's met zich mee. Gaat er iets fout, dan moeten systemen in de lucht blijven en medewerkers kunnen doorwerken. Daarom is het heel belangrijk dat bedrijfsgegevens voortdurend beschermd worden en op een veilige locatie (redundant, ofwel dubbel) opgeslagen worden. Dan kan jouw klant in een noodgeval zijn systemen snel weer opstarten en is zijn business in no-time weer up and running.

Workspace

Onder workspace wordt de moderne, digitale werkplek verstaan. Met applicaties en data in de cloud, die via internet op elk device beschikbaar zijn. Deze workspace vraagt om een uitgebreide, efficiënte - en vooral veilige - IT-omgeving, waar applicaties en data altijd beschikbaar zijn voor geautoriseerde medewerkers. Uitstekende beveiliging is dus essentieel om de workspace perfect te laten functioneren en bedrijfscontinuïteit te garanderen.

Recente ontwikkelingen op securitygebied

Bedreigingen worden innovatiever

Nieuwe securitybedreigingen volgen elkaar in hoog tempo op, waarbij de ene nog slinkser te werk gaat dan de andere. In 2017 ontdekten verschillende securityleveranciers samen elke dag gemiddeld 323.000 nieuwe dreigingen! Een paar voorbeelden van relatief nieuwe vormen van cyberaanvallen:

- Ransomware. Een cybercrimineel gijzelt bestanden door deze te versleutelen of (een deel van) de IT-omgeving door deze onbereikbaar te maken. Pas als je losgeld (ransom) betaalt, kan je de bestanden of IT-omgeving weer gebruiken
- CEO Fraude. Een crimineel doet zich voor als een hooggeplaatst persoon binnen een bedrijf en vraagt een medewerker een bedrag over te maken, voor zogenaamde zakelijke (dringende) doeleinden.
- Social Engineering. Criminelen maken misbruik van onze menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen, hebzucht, angst en onwetendheid. Zo proberen zij vertrouwelijke informatie los te krijgen of het slachtoffer een bepaalde handeling te laten verrichten.
- IoT hacks. Steeds meer apparaten in het bedrijf en de woonomgeving gaan zelfstandig communiceren via IoT. Denk hierbij aan webcams, slimme thermostaten, routers en opslagapparaten in je netwerk. De wildgroei binnen IoT maakt deze apparatuur tot een interessant doelwit, vooral omdat de beveiliging doorgaans niet op orde is.

Cybercrime-as-a-Service (CaaS)

CaaS wordt steeds professioneler. Zo kunnen cybercriminelen tegenwoordig de software die ze nodig hebben voor hun digitale inbraken eenvoudig bestellen op online markplaatsen zoals op het dark web. Je hoeft als hacker dus niet meer te weten hoe je een digitale aanval uitvoert, je moet er alleen voor kunnen betalen. Vervolgens wordt er een hacking service op maat geleverd. CaaS komt steeds vaker voor. Achter veel bedreigingen zit tegenwoordig een uitgebreide CaaS-infrastructuur. Daarmee kunnen criminelen razendsnel en op wereldwijde schaal te werk gaan. De komende jaren zullen we steeds meer van deze cyberaanvallen tegenkomen, want de vraag naar en het aanbod van CaaS blijft groeien.

Mobiel werken

Meer en meer werknemers werken flexibel en mobiel: ze gebruiken applicaties via steeds meer verschillende apparaten zoals laptops, tablets en mobiele telefoons. Helaas zien we dat deze apparaten vaak buiten de organisatie niet tot nauwelijks beveiligd zijn. Of het nu gaat om Bring Your Own Device (BYOD), Choose Your Own Device (CYOD) of Company-issued, Personally-enabled (COPE).
Wat kun je hieraan doen? In de eerste plaats kunnen organisaties de awareness onder medewerkers vergroten, zodat ze zich bewust worden van de gevaren van onbeveiligde devices. Ten tweede moeten organisaties zo veilig mogelijke voorzieningen treffen. Denk daarbij aan een beveiligd netwerk (VPN) 'Multifactor Authentication', encrypten (versleutelen) van gegevens op mobiele devices, het blokkeren van bepaalde applicaties buiten het bedrijfsnetwerk en de mogelijkheid om het synchroniseren van bestanden uit te zetten. Ten derde zijn duidelijke regels belangrijk. Bijvoorbeeld bedrijfsregels voor geheimhoudingsplicht, het melden van beveiligingsincidenten en een gedragscode voor internet en e-mail.

Algemene Verordening Gegevensbescherming (AVG)

Sinds 25 mei 2018 is de AVG officieel van kracht. Deze Europese wet maakt het voor organisaties nóg belangrijker om hun organisatorisch, juridisch en technologische beleid duidelijk op papier te zetten, in te richten en hun medewerkers daarvan op de hoogte te brengen. Dit beleid moet gericht zijn op het beveiligen van alle eindpunten, zodat privacygevoelige informatie overal veilig is.

Internet-of-Things (IoT)

IoT opent een wereld aan mogelijkheden voor hackers. Zo kunnen ze via met internet verbonden apparaten zoals thermostaten, beveiligingscircuits of printers inbreken op een bedrijfsnetwerk of (persoons)gegevens stelen. Vooral bij consumentenapparaten is security vaak een ondergeschoven kindje. Deze apparaten moeten namelijk zo goedkoop mogelijk zijn, waardoor producenten bezuinigen op de security. Beveiliging van deze intelligente objecten is dus nog belangrijker dan ooit te voren. Het is daarom noodzakelijk dat organisaties weten welke apparaten bij hen op het netwerk zijn aangesloten en tijdige controles uitvoeren om te voorkomen dat een cybercrimineel de besturing van het hele bedrijf overneemt.

Data analytics, Artificial Intelligence (AI) en Machine Learning

Applicaties worden slimmer doordat ze uitgerust zijn met data analytics-, Artificial Intelligence- (AI) of Machine Learning-functionaliteit. Hierbij wordt op grote schaal data uitgewisseld tussen verschillende gekoppelde bronnen. Het is vaak lastig gegevensbronnen te koppelen. Security wordt hierbij als een hindernis of vertragende factor ervaren, want per databron moet een datarisicoanalyse uitgevoerd worden. Het begrijpen waar de data heen vloeit en weer opgeslagen wordt, is van belang voor de beveiliging ervan.

Identity & Access Management (IAM)

Een nieuwe werknemer wil het liefst op zijn eerste dag al toegang hebben tot alle nodige bedrijfsystemen. Tenminste, de systemen waarvoor hij geautoriseerd is – dus die hij mag gebruiken. Deze toegang wordt steeds vaker geautomatiseerd geregeld via IAM. Een goed teken, want voorheen gingen organisaties daar vaak slordig mee om, om het tempo er in te houden. Zo werden toestemmingsformulieren voor bepaalde applicaties niet volledig ingevuld of werden de autorisatie-instellingen van een andere medewerker gekopieerd. Daardoor kregen medewerkers soms toegang tot gegevens waarvoor ze eigenlijk niet geautoriseerd waren, met alle risico's van dien.

Staten bemoeien zich met datahuishouding

Oorlogen spelen zich vandaag de dag ook in cyberspace af. Daardoor zullen regeringen zich vaker gaan bemoeien met de security van de organisatie en bedrijven in hun land. Bijvoorbeeld met nieuwe wetgeving of door organisaties te verplichten gegevens doorzoekbaar te maken voor opsporingsdiensten.

Het delen van securityinformatie

Securitybedreigingen worden steeds innovatiever en groeien in aantal. Door informatie over deze bedreigingen te delen, kunnen organisaties hun collega's helpen deze bedreigingen buiten de deur te houden. Dit delen van securityinformatie en -analyses zal op steeds grotere schaal en sneller gebeuren – soms zelfs real-time.

Teveel vertrouwen in de bedrijfssecurity

Medewerkers zijn op hun werk vaak lakser als het gaat om security dan thuis. Ze vertrouwen er – soms onterecht – op dat hun werkgever de beveiliging wel goed geregeld heeft. Om een voorbeeld te geven: thuis maken Nederlanders van 60 procent van hun bestanden een back-up. Op het werk is dit slechts 29 procent. Waarom? 48 procent van de werkenden gaat er vanuit dat de IT-afdeling dit wel regelt[1]. Door awareness te creëren kunnen organisaties de bijkomende beveiligingsrisico's voorkomen. Dus jouw klanten doen er goed aan hun medewerkers bewust te maken van hun gevaarlijke gedrag en ze te wijzen op de risico's.

[1]https://www.bit.nl/uploads/images/PDF-Files/bit-onderzoeksrapport-2016.pdf, pag 6

Mogelijke gevolgen van security issues

Bij de gevolgen van securityproblemen draait het om drie aspecten: beschikbaarheid, integriteit en vertrouwelijkheid (BIV).

Beschikbaarheid

Door een cyberaanval kunnen servers niet beschikbaar zijn, waardoor jouw klant niet bij zijn applicaties of data kan. Dat betekent geen business-as-usual meer, want medewerkers zijn voor hun dagelijkse werkzaamheden afhankelijk van deze gegevens en applicaties. Het bedrijf ligt grotendeels stil, wat een grote impact heeft op de reputatie en omzet.

Integriteit

Heeft een ongeautoriseerde medewerker toegang tot (gevoelige) bedrijfsinformatie? Dan kan een cybercrimineel deze data op een sluwe manier ontfutselen en manipuleren. Met een goede beveiliging heeft een organisatie dat op tijd door. Het komt, helaas, ook vaak voor dat een organisatie hier pas laat achter komt. Het gevolg? Data is onvolledig of zelfs onbruikbaar, waardoor de business bij jouw klant stil komt te liggen.

Vertrouwelijkheid

Vertrouwelijke bedrijfsinformatie mag niet in verkeerde handen vallen. Via een ongeautoriseerde medewerker kunnen gegevens misbruikt worden en uitlekken. Door encryptie en toegangsbeveiliging te gebruiken, kan jouw klant dit voorkomen.

De directe gevolgen van een securityprobleem

Over het algemeen leiden security issues tot dataverlies en onbruikbare systemen. Enkele voorbeelden van dergelijke directe gevolgen:

a. Ransomware gijzelt bepaalde gegevens of servers, waardoor medewerkers hier geen gebruik (meer) van kunnen maken.

b. Medewerkers kunnen niet meer inloggen in systemen omdat deze besmet of onbereikbaar zijn.

c. Personeel heeft wel toegang tot gegevens, maar deze zijn corrupt – en dus niet bruikbaar waardoor bijvoorbeeld:

- Bestellingen van klanten niet meer verwerkt worden.
- Productielijnen en machines tot stilstand komen.
- Arbeidsuren niet meer in rekening gebracht worden.
- Voorraadbeheer niet meer bijgehouden wordt.
- De communicatie met klanten verstoord is.

De indirecte gevolgen van een securityprobleem

Onder het overzicht met directe oorzaken heb je gelezen wat de technische gevolgen zijn van onvoldoende IT-beveiliging. Deze gevolgen kunnen op hun beurt leiden tot grotere businessgevolgen zoals:

d. Boetes – bijvoorbeeld omdat een organisatie niet voldoet aan de AVG-privacywetgeving.

e. Tijdverlies door dataverlies – bestanden die verloren zijn gegaan en opnieuw opgesteld moeten worden.

f. Reputatieschade – systemen werken niet waardoor een bedrijf bepaalde diensten of producten niet kan leveren.

g. Gedemotiveerd personeel – medewerkers moeten werk opnieuw doen omdat bestanden verloren zijn gegaan.

h. Verlies van concurrentiepositie – klanten of leveranciers stappen over naar de concurrent.

i. Minder omzet – doordat diensten niet geleverd kunnen worden en klanten kiezen voor concurrenten.

j. Minder productiviteit – systemen functioneren niet waardoor personeel ook niet kan werken.

k. Juridische aansprakelijkheid – een klant of leverancier kan een organisatie aansprakelijk stellen voor niet nagekomen afspraken.

De voordelen van adequate securityvoorzieningen

Met de juiste securityvoorzieningen voorkom je alle bovengenoemde problemen. Maar er zijn meer voordelen bij een goed securitybeleid. Zo verkort je de detectietijd: bedreigingen worden eerder gedetecteerd. Dat stelt je in staat deze direct aan te pakken in plaats van achter de feiten aan te lopen. Vroeger werden de securityproblemen achteraf opgelost, nu kun je die in de kiem smoren en in het beste geval zelfs voorkomen. Daardoor is een organisatie niet langer reactief, maar proactief wanneer het aankomt op security. Vindt er dan toch een security issue plaats? Dan ligt er een correctief plan klaar – een protocol dat direct in werking treedt en aan de hand van een stapsgewijs plan van aanpak de gevolgen zoveel mogelijk beperkt en de ICT omgeving hersteld en beschikbaar maakt.

De voordelen van adequate securitybeleid en -voorzieningen nog even op een rijtje:

- Voorkomen van security breaches
- Kortere detectietijd
- Mogelijkheid om proactief met securityprobleem om te gaan
- Aanwezigheid van een correctief en herstel plan

Belangrijke kernbegrippen

Welke securitytermen moet je als partner kennen? De belangrijkste termen op een rijtje:

- **Malware**: elke software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen. Het woord is een samentrekking van het Engelse malicious software.
- **Ransomware**: Een verzamelnaam voor malware die een computer, server en/of gegevens blokkeert. De gebruiker moet betalen om de computer, server of data weer te 'bevrijden'. Oudere, minder vaak voorkomende, varianten van ransomware blokkeren alleen de internetbrowser of het opstarten van de computer.
- **Cryptoware**: is een vorm van ransomware die bestanden gijzelt door ze te versleutelen. Dit houdt in dat je bestanden niet meer kunt openen. Er wordt betaling geëist in de digitale munteenheid Bitcoin. Betaal je niet binnen de tijdslimiet, dan wordt het geëiste bedrag steeds hoger. Besmetting verloopt via kwaadaardige bestanden (meestal in e-mailbijlages) of via een lek op de pc door niet-bijgewerkte software. De versleuteling is meestal niet zonder de sleutel ongedaan te maken. Cryptoware kan ook bestanden besmetten op aangesloten externe harde schijven of netwerkopslag die in Windows Verkenner een schijfletter heeft (zoals E:, F:, G:). Bewaar een back-up daarom altijd gescheiden van de pc.
- **Spyware**: software die het gebruikersgedrag op een computer bijhoudt. Spyware dient vaak een ander doel, namelijk het aftappen van gegevens. Meestal wordt deze informatie gebruikt voor reclamedoeleinden.
- **Internet of Things (IoT)**: apparaten die onderling via het internet verbonden zijn en data uitwisselen. Denk aan de slimme thermostaat, voertuigvolgsysteem of camerabeveiliging op een bedrijventerrein.
- **Artificial Intelligence (AI)**: ofwel kunstmatige intelligentie, dus alle intelligentie die niet biologisch is. Bij AI leren machines acties en beslissingen van mensen te kopiëren. Ze redeneren logisch, begrijpen taal en leren van fouten.
- **Machine learning**: een vorm van AI waarbij systemen leren om een taak beter uit te voeren op basis van eerdere acties en de gegevens daarover. Machine Learning maakt daarbij gebruik van complexe algoritmes.
- **Social Engineering**: het misbruik maken van menselijke eigenschappen als nieuwsgierigheid, vertrouwen en hebzucht. Het doel? Achter vertrouwelijke informatie komen of het slachtoffer een bepaalde handeling laten verrichten.
- **Multi-Factor Authenticatie (MFA):** een authenticatiemethode waarbij meerdere bronnen ingezet worden om de identiteit vast te stellen. Twee van de drie mogelijke bronnen moeten kloppen om de authenticatie te laten slagen. Bijvoorbeeld iets dat de gebruiker weet (zoals een pincode of gebruikersnaam) en iets fysieks dat de gebruiker heeft, zoals een keycard of een token, of iets dat de gebruiker is, zoals een vingerafdruk, een gezichtsscan of stemherkenning. Als twee van de drie bronnen gebruikt worden voor authenticatie, is een identiteit doorgaans goed beschermd tegen hackers. De beste MFA is dus gebaseerd op tenminste twee van de volgende kenmerken:
  › iets dat je weet
  › iets dat je hebt
  › iets dat je bent

Je hebt nu geleerd...

- Dat goede security vooral belangrijk is voor de continuïteit en compliancy bij jouw klant.
- Dat security onlosmakelijk verbonden is met de thema's Infrastructure, Connectivity & Networking, Back-up & Recovery en Workspace.
- Wat de meest actuele ontwikkelingen zijn op securitygebied en wat deze in grote lijnen inhouden.
- Wat mogelijke directe en indirecte (business)gevolgen zijn van security issues.
- Wat de belangrijkste securitybegrippen zijn en wat deze termen betekenen.