Crowe

ACA IT-Solutions, onderdeel van Crowe

Whitepaper:

De financiële risico's van cybercrime

Hackers richten zich nu ook op het mkb.
Extra cyberbeveiliging is hard nodig.

ACA IT-Solutions, onderdeel van Crowe

De financiële risico’s van cybercrime

1. Inleiding cybersecurity

Hoe kan ik de kwetsbare punten binnen mijn organisatie verkleinen?

Als finance manager of directeur kun je denken dat jouw organisatie niet interessant is voor hackers, maar niets is minder waar. Hierdoor is het niet meer de vraag of je aangevallen wordt, maar wanneer. Door scanning en automatisering van aanvallen zijn de mogelijkheden voor kwaadwillenden enorm vergroot. Het vinden en binnenkomen van kwetsbare ICT-omgevingen is vele malen eenvoudiger geworden dan voorheen. Het is daarom zaak het aantal kwetsbaarheden zo klein mogelijk te houden.

De aanvalsmethodieken van hackers zijn geëvolueerd. Ze focussen zich al lang niet meer alleen op een specifiek bedrijf om daar binnen te komen. Doordat er veel aandacht is voor ICT-beveiliging bij grotere organisaties, richten hackers zich nu op het mkb. Dat constateerde de Cyber Security Raad (CSR) ook, zoals zij in een rapport stelden dat er meer moet worden geïnvesteerd in cybersecurity. Het kabinet heeft hiervoor 380 miljoen euro begroot. Het CSR vindt ook dat de vitale sector beter beschermd moet worden en dat het Nederlandse mkb alerter moet zijn op cybercrime.

> *De werkwijze van cybercriminelen verandert. Er worden nieuwe technieken gehanteerd door hackers en daar moet je als Nederlands bedrijf maatregelen voor treffen op verschillende vlakken, enerzijds preventief om hackers buiten de deur te houden en anderzijds correctief om schade tot het minimum te beperken. Daar wordt het overgrote deel van de aanvallen mee voorkomen. Een Fort Knox bouwen is een utopie en daarom is het belangrijk om ook een ‘calamiteitenplan’ te hebben. Door ook daar de juiste maatregelen te treffen, kan schade aanzienlijk worden beperkt en daarmee de continuïteit van de organisatie worden gewaarborgd. De continuïteit, dat is the big picture die de directie en het management in het vizier moeten hebben en houden.*

Geert Rademakers, directeur van ACA IT-Solutions

2. Wat zijn de actuele bedreigingen?

Organisaties zijn digitaler dan ooit en het aantal kwetsbaarheden neemt toe door de volgende oorzaken, die hier nader worden toegelicht:

1. Afhankelijkheid van ICT is toegenomen.
2. De complexiteit van de ICT-omgeving wordt alsmaar groter.
3. Ontwikkelaars van bedrijfssoftware hebben niet altijd voldoende verstand van beveiliging.
4. Behoefte aan gegevensuitwisseling tussen applicaties zorgt voor een gebrek aan overzicht en onduidelijkheid over waar data zijn opgeslagen.
5. Het gebruik van generieke wachtwoorden en te eenvoudige inlogmethodes.
6. Toenemende handel van gebruikersnamen en wachtwoorden op de digitale zwarte markt (darkweb).
7. Op afstand werken (o.a. thuiswerkers) zorgt voor toenemende complexiteit van cybersecurity.
8. Cybercriminelen maken steeds sneller misbruik van ontstane kwetsbaarheden bij softwareleveranciers.
9. De rechtenstructuur binnen een organisatie is vaak niet actueel en/of onduidelijk.

1. Afhankelijkheid van ICT is toegenomen

Data zijn 24 uur, 7 dagen in de week beschikbaar. Dat is de behoefte van de werkwijze van de medewerker, maar tegelijkertijd stuwt het ook de afhankelijkheid van ICT. Dit vraagt om een inventarisatie van het ICT-landschap. Wie is waarvoor verantwoordelijk? Wie kan bij welke data? En waar zijn welke data opgeslagen? Dat gaat verder dan het eigen landschap, maar gaat ook over de gehele keten. Cybercriminelen maken namelijk steeds vaker gebruik van bedrijven in je keten om via die weg bij jouw organisatie binnen te komen. Zo kan een hack bij bijvoorbeeld een leverancier of klant een risico vormen voor jouw organisatie. Een inventarisatie van jouw kritische bedrijfsprocessen in relatie tot jouw ICT-landschap moet dan ook klanten, leveranciers en medewerkers als elementen bevatten. Betrek daar ook jouw ICT-partner(s) bij.

> *Cybercriminelen maken steeds vaker gebruik van bedrijven in je keten om via die weg bij jouw organisatie binnen te komen.*

2. De complexiteit van de ICT-omgeving wordt alsmaar groter

Omdat veel bedrijven bezig zijn met een digitale transformatie hebben lekken, zoals recentelijk bij Microsoft Exchange, meteen een grote impact. Die digitale transformatie is een reis van ‘verantwoordelijk voor ICT’ naar ‘afhankelijk van ICT’. Dat merken financieel eindverantwoordelijken ook. Vroeger was de ICT-infrastructuur behapbaar, klein en afsluitbaar. Tegenwoordig is er meestal sprake van een combinatie van cloud, Software-as-a-Service (SaaS) en eventueel ook nog servers op de eigen locatie. De digitale transformatie bevordert het gebruiksgemak, maar maakt organisaties dus ook extra kwetsbaar, omdat het aanvalsvlak is vergroot.

3. Ontwikkelaars van bedrijfssoftware hebben niet altijd voldoende verstand van beveiliging

De kwalificaties die je als organisatie stelt aan een ICT-leverancier kun je onderbrengen in contractmanagement. Daar probeer je zo goed mogelijk te doorgronden hoe goed een leverancier met jouw data en processen omgaat. Speciale aandacht vragen we daarbij voor de applicaties die er binnen jouw organisatie worden gebruikt.

Applicatieleveranciers zijn de laatste jaren en masse overgestapt naar de cloud. Maar een applicatie ontwikkelen is compleet iets anders dan het beschikbaar houden van een (cloud)dienst of het beveiligen van data. Met de overgang naar de cloud stappen ze een (voor hen) onbekende wereld binnen van beschikbaarheid en beveiligingsaspecten. Soms wordt dat ingevuld met bestaande software die direct aan het internet verbonden wordt. Dat resulteert in software die niet per definitie geschikt is om als cloudapplicatie beschikbaar te stellen.

4. Behoefte aan gegevensuitwisseling tussen applicaties zorgt voor een gebrek aan overzicht en onduidelijkheid over waar data zijn opgeslagen.
Veel organisaties knopen systemen middels API's aan elkaar. Daardoor is vaak niet meer in beeld welke applicaties met elkaar 'praten' en waar welke data blijft. Kortom, een continuproces van inventarisatie van de ICT-systemen is welhaast een must om te doorgronden hoe het ICT-landschap in elkaar zit. Het is een eerste stap naar bewuste keuzes voor systemen en applicaties en de bijbehorende beveiliging. Ook voor de privacy wetgeving (GDPR) is dit een belangrijk punt van aandacht.

> *Vaak is niet meer in beeld welke applicaties met elkaar 'praten' en waar welke data blijft.*

5. Het gebruik van generieke wachtwoorden en te eenvoudige inlogmethodes
Een ander pijnpunt is de inzet van gebruikersnamen en wachtwoorden. Een ambtenaar van de gemeente Hof Van Twente heette hackers in december 2020 wel erg letterlijk welkom, door een wachtwoord aan te passen naar Welkom2020. Hierdoor is een mogelijkheid ontstaan om de gehele omgeving van de organisatie over te nemen, simpelweg doordat cybercriminelen geautomatiseerd het wachtwoord konden raden.

Arwi van der Sluijs, directeur en onderzoeker Nederlands Forensisch Incident Respons, in dagblad Tubantia:
"29 oktober 2019 is door een aanpassing van de firewall een bepaalde server via het internet toegankelijk geworden, waardoor er op afstand kon worden gewerkt. Er volgden miljoenen aanvallen, waarbij allerlei combinaties van gebruikersnamen en wachtwoorden vergeefs werden geprobeerd. Kennelijk gaf het wachtwoord toen genoeg bescherming. Op 15 oktober 2020 werd het wachtwoord van het testadmin-account veranderd in Welkom2020. Toen werd zeer waarschijnlijk het wachtwoord geraden tijdens een nieuwe geautomatiseerde cyberaanval. Het testadmin-account had de hoogste rechten binnen het netwerk van de gemeente. Mede hierdoor konden de aanvallers zich direct vrij binnen het netwerk bewegen en malicieuze handelingen uitvoeren. Het is een raadsel waarom het wachtwoord zo is veranderd. Soms kan het nodig zijn iemand anders toegang te geven, maar doe het dan onder de juiste voorwaarden."

Even later vertelt hij tegen Tubantia: "Of het nu van een gemeente of een bedrijf is, elk netwerk heeft ermee te maken dat poorten van een firewall dag en nacht worden gescand door hackers, maar soms ook door heel legitieme diensten. Dat wil je niet eens allemaal monitoren, zoveel informatie is dat. Maar je wilt in die firewall wel allerlei zaken monitoren, want je wilt weten welke poorten er openstaan en hoe de verdediging daarachter is ingericht. En mocht er dan sprake zijn van een doorbraak in jouw netwerk, wil je dat kunnen zien. Vergelijk het met een inbraakalarm. Monitoring was echter niet voorhanden."

Cybersecurity is dus niet alleen een kwestie van het ICT-landschap overzien. Aan de andere kant zitten gebruikers van de software. Wat je vaak ziet, met name in het mkb, is dat software in de cloud een enkelvoudige inlogmethode kent, dus alleen gebruikersnaam en wachtwoord. Dit is van oudsher zo ingericht in veel applicaties en dient het gebruikersgemak. Daarbij zijn vaak de inloggegevens ook nog opgeslagen in de browser van de betreffende gebruiker. Deze werkwijze is niet meer toereikend met het oog op cyberveiligheid, zeker niet voor applicaties die essentieel zijn voor de bedrijfsvoering en/of (privacy)gevoelige data verwerken en opslaan.

6. Toenemende handel van gebruikersnamen en wachtwoorden op de digitale zwarte markt (darkweb)
Op digitale zwarte markten, het darkweb, worden inloggegevens massaal verhandeld. Deze data wordt buitgemaakt bij datadiefstallen bij veelal grote organisaties. Denk aan online platformen (zoals Microsoft), social media (LinkedIn, Facebook), gemeentes en webshops. Daar worden gebruikersnamen en wachtwoorden vergaard. Dat zijn voor hackers waardevolle gegevens. Met de vergaarde wachtwoorden wordt bijvoorbeeld geprobeerd om op andere applicaties van dezelfde gebruiker in te loggen. Een hacker weet namelijk dat nog altijd veel mensen hetzelfde wachtwoord gebruiken voor meerdere applicaties of doeleinden.

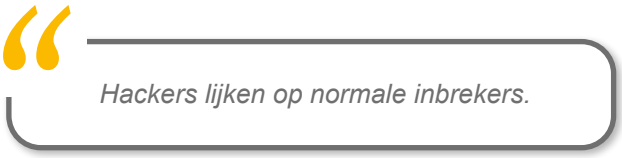
De voorbeelden die de media halen zijn er in overvloed en vaak ligt dit eraan ten grondslag: de basis is vaak nog niet goed. We praten hier niet over Fort Knox, maar echt over basisprincipes. Een gebruikersnaam en wachtwoord zou vergezeld moeten gaan met two-factor authentication. Naast jouw wachtwoord gebruik je dan een tweede middel om je te identificeren. Denk aan een code die via een app gegenereerd wordt, zoals een authenticator of een fysieke token die continu nieuwe codes genereert. Een kwaadwillende kan daardoor niets met alleen gebruikersnaam en wachtwoord als hij deze in handen heeft gekregen. Men heeft immers geen inzicht in de additionele authenticatiecode.

> *Een gebruikersnaam en wachtwoord moeten vergezeld gaan met two-factor authentication.*

7. Op afstand werken (o.a. thuiswerkers) zorgt voor toenemende complexiteit van cybersecurity
Toen het coronavirus Nederland bereikte, moesten organisaties onder druk snel het thuiswerken mogelijk maken. Daarbij lag de prioriteit minder op cybersecurity. Nu is het de tijd om terug te kijken wat er is gedaan en het netjes te gaan verzorgen ‘volgens de spelregels’ zoals met behulp van een IT risico normenkader.

Onderzoek van het Kennisinstituut voor Mobiliteitsbeleid, een onderdeel van het ministerie van Infrastructuur en Waterstaat wijst uit dat in januari 2021 maar liefst 48 procent van de werkende Nederlanders een deel van de week thuiswerkte. 45 procent van de thuiswerkers wil na de coronacrisis meer thuiswerken dan ze voor de coronacrisis deden. Dat laatste blijkt dan weer uit onafhankelijk onderzoek van Ruigrok NetPanel. Oftewel: thuiswerken is here to stay. Maar waar er wel controle is over de ICT-activiteiten binnen de organisatie, heb je dat niet buiten jouw organisatie. Via die weg is het dan ook makkelijker voor kwaadwillenden om aan jouw bedrijfsgegevens te komen.

8. Cybercriminelen maken steeds sneller misbruik van ontstane kwetsbaarheden bij softwareleveranciers
Doordat grote organisaties verder zijn in het anticiperen op cybercriminaliteit, kost het voor digitale criminelen veel meer moeite, waardoor ze er simpelweg vaak niet aan beginnen. Wat dat betreft lijken hackers op normale inbrekers. Kost het te veel moeite om in te breken, dan gaan ze een deur verder. Die deur verder is tegenwoordig het mkb, waar de sloten op de deur nog verbetering behoeven of waar zelfs deuren wagenwijd openstaan. Patchmanagement staat daarbij op nummer één als open deur. Updates moeten zo spoedig mogelijk worden doorgevoerd.



Wat velen namelijk niet weten is dat het overgrote deel van de updates die ontwikkelaars uitbrengen niet gaan over de functionaliteit van de software, maar over de beveiliging daarvan. Het is dus zaak je updates zo snel mogelijk te doen. Tussen de ontdekking van de kwetsbaarheid door de software leverancier en de daadwerkelijke installatie door jouw organisatie bestaat een inbraakkans die wordt aangegrepen door hackers. Zeker nadat de softwareontwikkelaar de update wereldkundig heeft gemaakt. Want als je het weet, dan weet de hacker het ook. Dan gaan ‘de scanners’ aan en gaan hackers op zoek naar bedrijven die deze software in huis hebben en nog op de oude (lees: kwetsbare) versie draaien.

9. De rechtenstructuur binnen een organisatie is vaak niet actueel en/of niet duidelijk
We pleiten dan ook voor een betere rechtenstructuur. Of die systemen nu op locatie of in de cloud zijn, dat maakt daarvoor niet uit. Jouw ICT-management is verantwoordelijk voor het toedelen en ontzeggen van de toegang tot systemen en het rechtenniveau. Het gekke is dat die verantwoordelijkheid met de snelle opkomst van cloud vaak rücksichtslos de nek om is gedraaid, terwijl systemen voor identity en access management een must zijn. SaaS-applicaties moeten niet zomaar toegankelijk zijn zonder dat de IT-beheersorganisatie er over waakt. Die beheersorganisatie pakt hire and fire policy’s op en de vraag wie toegangsrechten heeft en op welk niveau. In dat centrale platform geef je de regels vorm. Dat beleid is gekoppeld aan de functie die HR je heeft toegewezen. Data buiten die bandbreedte van wat je mag, worden automatisch door het systeem opgemerkt. Dat kan als verdacht worden bestempeld.

3. Wat kan je doen om jouw organisatie veiliger te maken?

Cybersecurity in 5 stappen

1. Zet cybersecurity hoog op de agenda

IT-beveiliging is een keiharde must. Dat begint bij de beleidsbepalers, want daar worden de lijnen uitgezet en de kaders bepaald die door de IT-afdeling (samen met IT-partners) worden gerealiseerd en dag in dag uit door de medewerkers worden gebruikt. Een dag zonder ICT is niet denkbaar. In één klap alle data (klantgegevens, orders, financiële gegevens, informatie over lopende projecten etc.) kwijt zijn is een nachtmerrie. Langdurig geen toegang hebben tot het bedrijfsnetwerk en alle applicaties zet de continuïteit van de organisatie op het spel. Met dit in het achterhoofd dient cybersecurity de juiste prioriteit mee te krijgen, binnen alle lagen van de organisatie.

> *Digitale beveiliging is niet alleen meer een IT-feestje.*

2. Doe een cyberrisicoanalyse

Hoe is de huidige staat van jouw IT-beveiliging? Welke risico's loopt jouw organisatie en in welke mate? En welke tegenmaatregelen zou je dan moeten nemen en met welke priorisering? Dit zijn de vragen die typisch horen bij risicomanagement en die je ook kunt toepassen op cybersecurity. Voer een nulmeting uit: hoe is de techniek, hoe zijn de processen en hoe is de bewustwording van alle medewerkers? Dit geeft een helder beeld van de huidige situatie en een vertrekpunt voor het dichten van de kwetsbaarheden.

3. Zorg dat je weet dat je data ergens veilig staat

Met talloze gebruikte applicaties, soms zelfs buiten de organisatie om, is het de vraag waar al die data terechtkomt. Met veel kantoren en nog meer medewerkers die niet per se op kantoor achter een pc zitten, moet er wel duidelijkheid zijn over de te gebruiken applicaties in de cloud en waar dan de gegevens zijn opgeslagen. Dat begint bij dataclassificatie. Op basis daarvan kan worden bekeken waar de prioriteiten liggen en welke applicaties extra beveiligd moeten worden. Dit wordt gedaan in een Business Continuity Plan (BCP), waarmee de organisatie haar eisen en verwachtingen omtrent het opslaan, beveiligen en herstellen van data bepaalt. Dit is een belangrijke, preventieve maatregel om jouw organisatie te beschermen tegen cyberaanvallen. Mocht een hacker jouw data weten te versleutelen (cryptolocker, ransomware) dan kun je op die manier aanspraak maken op een veilige kopie van jouw data. Dit helpt je om de bedrijfscontinuïteit van jouw organisatie te waarborgen.

4. Maak medewerkers bewust van de risico's

Het (IT-)beleid, de procedures en de technische beveiligingsmaatregelen kunnen nog zo goed zijn, als de mens er niet naar handelt (of niet weet hoe) dan wordt de strijd tegen cybercriminaliteit zeer zwaar. Daarom is het belangrijk om de medewerkers, geen functie of afdeling uitgezonderd, te betrekken en bewust te maken van hun rol. De beste methode is de inzet van een security awareness programma, toegespitst op jouw organisatie. Dat bestaat vaak uit het opstellen, communiceren en monitoren van procedures, bewustwordingstrainingen, gedrag en alertheid van medewerkers te verbeteren en periodieke metingen (en bijsturing).

> *Het is belangrijk om de medewerkers, geen functie of afdeling uitgezonderd, te betrekken en bewust te maken van hun rol.*

5. Behoud focus

Cybersecurity is niet alleen een IT-vraagstuk, maar zeer zeker ook een bredere organisatorische uitdaging. Het onderwerp moet dan ook continu de aandacht krijgen, ook omdat cybercriminelen telkens nieuwe technieken verzinnen. Het is daarom de kunst op dit onderwerp de focus te behouden. Dit doe je als organisatie namelijk niet alleen om aan wet- en regelgeving zoals de Algemene Verordening Gegevensbescherming (AVG) te voldoen, maar breder om jouw medewerkers verantwoordelijk te laten zijn voor hun data. In essentie zijn het veelal gegevens van klanten, collega's of derde partijen die je niet op straat wil laten zwerven.

4. Visie: Beleid, techniek & mens

Voor jou, directie of financieel verantwoordelijke, staat de continuïteit van de organisatie centraal. Die mag niet in het geding zijn. Cybercriminelen kennen deze zorgen en leggen de vinger graag op de zere plek, want dan gaat de portemonnee open. Het doelwit: de kroonjuwelen van jouw organisatie. Anders gezegd: het bedrijfsnetwerk, de applicaties en de data. Hierin zit de waarde van een organisatie. Door een gedegen samenspel tussen de pijlers beleid, techniek en mens bescherm je de kroonjuwelen van jouw organisatie en daarmee het voortbestaan van jouw bedrijf.

> *Door een gedegen samenspel tussen de pijlers beleid, techniek en mens bescherm je de kroonjuwelen van jouw organisatie.*

Financials zien meeste investeringen in informatiebeveiliging

Eerder namen 325 financiële professionals deel aan onderzoek van Executive Finance en Controllers Magazine naar de invloed van technologische ontwikkelingen op de financiële functie in 2020. Informatiebeveiliging blijft met 35 procent stevig op de eerste plaats staan waar het gaat om nieuwe technologische ontwikkelingen waar de finance professional zich mee geconfronteerd ziet. Organisaties investeren er ook het meest in. 32 procent investeert het meeste in informatiebeveiliging, gevolgd door ERP met 29 procent en cloud computing met 27 procent.

Het Jericho-principe

Wie werk wil maken van cybersecurity moet uitgaan van het Jericho-principe. Het uitgangspunt daarvan is dat informatie beveiligd moet worden op het niveau van de gegevenselementen zelf. Jericho gaat uit van beveiligingsmaatregelen zoals encryptie/versleuteling, inherent veilige computerprotocollen, inherent veilige computersystemen en authenticatie op gegevensniveau. De naam Jericho is afgeleid van de vernietiging van de stad Jericho zoals die in het Oude Testament van de Bijbel is verwoord. Jericho was een met muren versterkte stad, die desondanks ten prooi viel aan de aanvallers. Wie aanvallers wil afweren, zal dus extra zijn kroonjuwelen moeten beschermen en niet alleen een muur op moeten werpen. Dat alleen werkt niet, zeker nu het aanvalsvlak groter en groter is geworden.

Open source intelligence

Een ander belangrijk punt van aandacht is open source intelligence (OSINT). Inlichtingendiensten van de overheid gebruiken OSINT vaak als methode om informatie via openbare bronnen te verzamelen. Dit hoeft niet altijd in de vorm van geschreven tekst te zijn. Ook (digitale) foto's, video- en audiofragmenten kunnen, als je die op de juiste manier analyseert, cruciale inlichtingen bevatten. Die kan je organisatie gebruiken voor het effectief bestrijden van criminele activiteiten. Vooral als het gaat om inzicht te geven in de cyberrisico's van jouw bedrijf, kan OSINT behoorlijk waardevol zijn. Door OSINT te gebruiken kan je meer informatie verzamelen over cyberdreigingen, datalekken en kan je informatie verzamelen over jouw bedrijf. Als je deze kan vinden, kan deze ook gemakkelijk toegankelijk zijn voor cybercriminelen. Het verzamelen van OSINT is een mooie manier om te begrijpen welke informatie potentiële aanvallers hebben. Als je weet welke informatie uit openbare bronnen over jouw bedrijf kan worden verzameld, helpt dit je beveiligingsteam om betere verdedigingsstrategieën te ontwikkelen.

> *Informatie uit openbare bronnen over jouw bedrijf helpen je beveiligingsteam om betere verdedigingsstrategieën te ontwikkelen.*

ACA IT-Solutions, onderdeel van Crowe

Traditionele gedachte over bedrijfscontinuïteit

Als een hacker specifiek een onderneming uitkiest, dan kan dat zware gevolgen hebben. Een onderneming waarbij dat onlangs gebeurde, had zijn back-ups gedaan. Maar je ziet daar een traditionele gedachte over bedrijfscontinuïteit terugkomen. Back-ups worden gemaakt voor het geval er waterschade of brand is. ‘Als ik back-ups maak, zal het wel goed zijn’, is de gedachte. Maar als het goede hackers zijn, nemen ze de tijd om uit te zoeken hoe de lijnen lopen. In dit geval werden zowel de data in de primaire systemen als de back-up in de cloud gecompromitteerd. Dat maakte dit bedrijf vleugellam en dit resulteerde in een digitale gijzeling. Het bleek volgens de politie een gerenommeerde hackersfamilie. Het is van de gekke, maar ze stonden te boek bij de politie als betrouwbaar: wie betaalde kreeg over het algemeen zijn data wel weer terug. Dat is verre van vanzelfsprekend. De getroffen onderneming (45 medewerkers, 30 miljoen euro omzet) kreeg het advies om 40.000 euro losgeld te betalen. Een grote gok zonder garanties. Een goede back-up oplossing had dit kunnen voorkomen.

Bedrijfscontinuïteit op bordje financieel eindverantwoordelijke

Met de digitale transformatie in het achterhoofd, is cybersecurity ook een primaire verantwoordelijkheid van de financieel verantwoordelijke oftewel de CFO. Het bedrijf wordt digitaler dan ooit en bedrijfscontinuïteit en risicomanagement liggen duidelijk op het bordje van de Chief Financial Officer. Hij of zij zit vaak met zijn accountant aan tafel. Als de vennootschap ophoudt te bestaan (door een besluit om te stoppen of doordat de vennootschap niet meer in staat is aan haar verplichtingen te voldoen), is duurzame voortzetting niet meer mogelijk en treedt dus discontinuïteit op. Dat kan ook via een cyberaanval het geval zijn. Het is tegenwoordig zelfs één van de grootste risico’s.

ACA IT-Solutions, onderdeel van Crowe

Techniek, mens en organisatie

Cyberrisico's voorkomen is dus een enorme uitdaging. De term cybersecurity omvat alle maatregelen – beleid, techniek, mens - om illegale digitale activiteiten tegen te gaan, te signaleren en om de schade ervan tot het minimum te beperken. Om de organisatie te wapenen tegen cybercriminelen zijn technische beveiligingsmiddelen alleen niet genoeg. Cybersecurity is een doordacht bouwwerk van beleid, techniek en mens.

> *Om de organisatie te wapenen tegen cybercriminelen zijn technische beveiligingsmiddelen alleen niet genoeg.*

Ieder deel moet voldoende en passende aandacht krijgen om te zorgen dat jouw cybersecurity als geheel solide blijft. Traditioneel zijn het de pilaren techniek en beleid die de meeste aandacht krijgen. Het management stelt beleid en procedures op. De IT-afdeling zet bijvoorbeeld technische maatregelen in (zoals firewalls en antivirussoftware) en richt processen in die de kans op beveiligingslekken verkleinen. Maar vaak blijkt, hoe clichématig ook, de mens uiteindelijk de zwakste schakel. Bewustzijn ten aanzien van de risico's en de mogelijke gevolgen én het vermogen naar dat bewustzijn te handelen zijn net zo belangrijk als technologische beveiligingsmiddelen. Het is van groot belang dat de medewerkers zich veilig gedragen, verdachte omstandigheden herkennen en de juiste vervolgstappen nemen. De pijlers beleid, techniek en mens vormen samen de sleutel tot succes, of beter gezegd: het slot op de deur.

Niet alles is te beveiligen. Bovendien is dat vaak ook te kostbaar. Des te belangrijker is het om een goede afweging te maken met een gedegen risicoanalyse als vaak gekozen startpunt. Dat moet CFO's met risicomanagement en ICT in de portefeuille aanspreken. Zij zijn het die als geen ander zich dit onderwerp eigen kunnen maken en hierin weloverwogen keuzes maken.

Advies & ondersteuning

Bij ACA IT-Solutions, onderdeel van Crowe, draait alles om de drie-eenheid Beleid, Techniek en Mens. Elk vraagstuk is een samenspel van deze elementen. Dat leidt tot innovatieve IT-bedrijfsoplossingen, waarbij continuïteit, beschikbaarheid en veiligheid essentieel zijn. Daarmee bereiken onze klanten een onderscheidend resultaat.

Contact

Wil je meer informatie of een afspraak maken? Neem dan contact met ons op via onderstaande contactgegevens.

Adresgegevens

ACA IT-Solutions, onderdeel van Crowe
Beukenlaan 40-50
5651 CD Eindhoven

Contactgegevens

040 - 8 800 100
info@aca-it.nl
www.aca-it.nl