REDPAPER

Avantage
MAKES IT SIMPLE

zo'n hack... dat zal mij toch niet gebeuren?

Dan moet je wel zeker weten dat jouw organisatie goed is beschermd tegen online dreigingen.

De coronacrisis heeft een enorme impact gehad op de manier waarop we met elkaar samenwerken. Het kantoor als vaste werkplek heeft waar mogelijk plaats gemaakt voor thuiswerkplekken. In de toekomst zal de verhouding tussen werken op kantoor en thuiswerken ongetwijfeld meer in evenwicht komen, maar 'hybride samenwerken' (door kantoor- met thuiswerkers) is gegarandeerd een blijvertje. Al was het alleen maar omdat een aanzienlijke meerderheid van de huidige thuiswerkers heeft aangegeven na versoepeling van de coronamaatregelen één à twee dagen per week thuis te willen blijven werken. Dat vraagt niet alleen om investeringen in voorzieningen die Het Nieuwe Samenwerken optimaal faciliteren. Het vraagt ook om het reserveren van budgetten voor cybersecurity.

Veel organisaties zijn zich overigens bewust van de noodzaak om de digitale weerbaarheid te verhogen. De uitdaging is alleen om cybersecurity zodanig in te richten dat er aan drie elementaire voorwaarden wordt voldaan. Het is niet voldoende om alleen de technologische voorzieningen op orde te brengen. Ook in de bedrijfsprocessen en de manier van werken moet cybersecurity worden verankerd. Daarnaast moeten medewerkers zich bewust zijn van het belang van 'veilig werken'. Je kunt alles nog zo goed geregeld hebben; wanneer iemand op de verkeerde knop drukt, kan dat verstrekkende financiële gevolgen hebben. En dan praten we nog niet over de secundaire schade die daarbij ontstaat. Want wie wil zakendoen met een digitaal onveilige organisatie? Juist.

Wat ga je lezen?

In dit redpaper nemen we je eerst mee langs de dreigingen waartegen je jouw organisatie moet wapenen. We gaan het ook hebben over het veranderende aanvalslandschap en de noodzaak om cybersecurity een vaste plek op de directieagenda te geven, waarbij we meteen aangeven hoe je dat voor elkaar krijgt. Vervolgens leggen we uit met welke aanpak je cybersecurity in jouw organisatie naar een hoger niveau kunt tillen en bespreken we de middelen die je daarbij kunt gebruiken. Tot slot geven we je mee hoe je jouw kennis over cybersecurity op peil kunt houden. Daarmee hopen we te bereiken dat jouw organisatie niet onnodig slachtoffer wordt van cybercriminaliteit.

Cybersecurity: trends in cijfers

Laten we maar eens beginnen met een aantal cijfers die aangeven in hoeverre cybersecurity op het netvlies van organisaties staat. Recente cijfers laten zien dat slechts 13% van de MKB-bedrijven de cybersecurity op orde heeft. Anders gezegd: 7 van de 8 MKB-bedrijven hebben cybersecurity niet op orde. Daar is overigens wel een verklaring voor te vinden. Maar liefst 67% van diezelfde MKB-bedrijven denkt namelijk geen interessant doelwit te zijn voor cybercriminelen.

67%

van de MKB-bedrijven denkt geen doelwit te zijn

Gemiddelde security incident bedraagt

€ 80.000

Dat is bijzonder, als je bedenkt dat bijna de helft van alle cyberaanvallen is gericht op het midden- en kleinbedrijf. Tegelijk zegt 64% van de MKB'ers wel degelijk behoefte te hebben aan een partner die hen op het gebied van cybersecurity ondersteunt. Het gegeven dat de gemiddelde financiële schade per digitaal veiligheidsincident net iets minder dan 80.000 euro bedraagt, heeft daar mogelijk iets mee te maken.

Ransomware

Maar wat zijn dan de cyberdreigingen waartegen je jouw organisatie moet wapenen? Een ´goed´ voorbeeld is ransomware, een hackersinstrument om een IT-omgeving te gijzelen en losgeld te eisen van de getroffen organisatie. Wanneer het losgeld is betaald, worden de IT-systemen in de IT-omgeving doorgaans weer vrijgegeven. Het komt echter ook voor dat losgeld wordt geëist om te voorkomen dat de data van een organisatie op straat komt te liggen. Tegenwoordig ben je als organisatie dus niet (meer) veilig met alleen een goede back-up, die je als tegenactie terug kunt zetten na het encrypten van je data.

Universiteit van Maastricht

Een aansprekend geval was de hack van de IT-omgeving van de Universiteit van Maastricht in 2019. Medio oktober verzonden hackers phishing mails naar medewerkers van de universiteit. Slechts enkele medewerkers klikten op een link in die mails, maar dat was genoeg om het onheil binnen te halen. Op die manier werd een virus geïnstalleerd op de (maar liefst 1650) universiteitsservers, waarvan er 5 of 6 op iets verouderde software draaiden. Dat was echter ruim voldoende voor de hackers om toegang tot de IT-omgeving te krijgen.

Verkenning

Op 20 november hadden de cybercriminelen de volledige controle over het netwerk. Daarna zijn ze voornamelijk bezig geweest met verkenningswerk. Door alle servers in kaart te brengen konden de hackers de ransomware optimaal uitrollen. Daarnaast hebben ze de back-up mogelijkheden van de universiteit bestudeerd. Uiteindelijk was het idee om het onmogelijk te maken voor

de universiteit om terug te vallen op een back-up. De hackers namen rustig hun tijd en konden onopgemerkt van binnenuit hun plan beramen. Op de universiteit had niemand iets in de gaten. Op zich niet vreemd, want het duurt gemiddeld bijna 200 dagen voordat een hacker wordt ontdekt.

De aanval

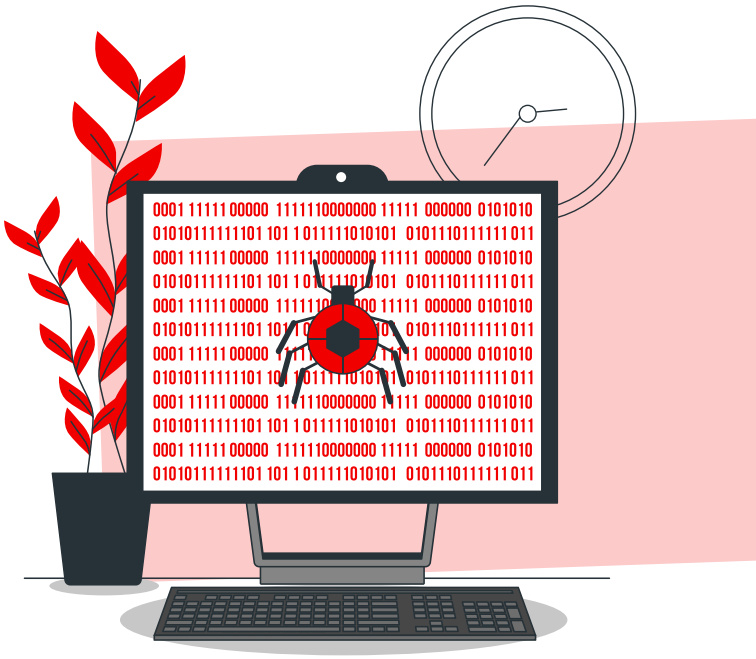
Op 24 december kwam de Universiteit van Maastricht naar buiten met het bericht dat het instituut slachtoffer van een cyberaanval was geworden. Na een lang proces van verkenning en planning hadden de hackers dus toegeslagen. Daarbij maakten ze gebruik van Clop-ransomware, die zich met name op volledige computernetwerken richt. Helaas is daar nog geen publieke decryptor (het ongedaan maken van de versleuteling) voor beschikbaar. Zodra de Clop-ransomware actief is, versleutelt het zoveel mogelijk bestanden en voegt het de .clop extensie toe. Zo weet het slachtoffer dat het bestand geraakt is.

Kostenpost

Daarnaast wordt een read-me bestand op het netwerk geplaatst. Hierin staan gegevens van de hackers om overeenstemming te krijgen over betaling. De datum, vlak voor de kerstdagen, was geen toeval. Doordat de aanval rondom de feestdagen werd ingezet, was bij het slachtoffer niet de juiste expertise aanwezig om snel tot een oplossing te komen. De Universiteit van Maastricht kwam voor de keus te staan om te betalen of de IT-omgeving minstens een maand te sluiten om de problemen op te lossen. De schade zou immens zijn omdat veel studenten dan niet zouden kunnen afstuderen. De kosten waren uiteindelijk 30 bitcoins. Tegen de koers van 30 december 2019 was dat omgerekend zo'n 197.000 euro. Al met al een hele hoge kostenpost.

Malware

Ransomware is in wezen een familielid van malware; alle mogelijke software die gebruikt wordt om computersystemen te verstoren, data te vernietigen, virussen te verspreiden, persoonsgevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen, waartoe ook thuisnetwerken worden gerekend. Door de toename van het thuiswerken als direct gevolg van de coronapandemie is malware stevig in opkomst.



Microsoft 365

Een van de manieren waarop cybercriminelen de kans krijgen om malware op een device of in een netwerk te installeren, is door gebruik te maken van de 'achterdeurtjes' in Microsoft 365-applicaties. Dat wil niet zeggen dat het Microsoft 365-pakket onveilig is; het tegendeel is eerder het geval. Maar hackers kunnen wel via Microsoft binnendringen door gelekte of standaard wachtwoorden te misbruiken. Dat kun je ze overigens nagenoeg onmogelijk maken door multifactor authenticatie (MFA) te gebruiken bij het inloggen op je Microsoft-account. Tegen phishing helpt dat helaas niet. Onachtzame medewerkers die op een 'foute link' in een mailbericht klikken, zijn nog te vaak een eenvoudige prooi voor cybercriminelen.

Spear phishing

Phishing wordt weleens vergeleken met 'schieten met hagel'. De cybercrimineel stuurt dan hetzelfde nepbericht naar zo veel mogelijk adressen in de hoop dat een aantal ontvangers zich laat verleiden om op de foute link te klikken. Bij spear phishing wordt niet met hagel geschoten, maar gebruikt de aanvaller een scherpschuttersgeweer om een specifiek persoon of een bepaalde afdeling op de korrel te nemen. Een spraakmakend voorbeeld daarvan is de aanval op bioscoopketen Pathé, in 2018.

Overname in Dubai

Op 8 maart van dat jaar ontvangen de CEO en de CFO een mailbericht, waarin de afzender zich voordoet als de bestuurder van het Franse hoofdkantoor van Pathé. Er moet snel geld worden overgemaakt (ruim 800.000 euro) voor de overname van een bedrijf in Dubai. Dat nieuws mag alleen nog niet aan de grote klok worden gehangen. Daarom wordt in de mail dringend verzocht om geheimhouding. Daarnaast wordt aangekondigd dat het betreffende bedrag na het rondkomen van de overeenkomst wordt teruggestort.

Rechtsgeldig

Beide directieleden twijfelen aan de gang van zaken, maar besluiten om de hiërarchie te respecteren en akkoord te gaan wanneer een formele bevestiging van de overname wordt ontvangen. De papieren worden naar hen gemaild, voorzien van de juiste handtekeningen namens Pathé, die wel worden vergeleken met handtekeningen op eerdere documenten. Daar mankeert echter niets aan. Gerustgesteld door de ogenschijnlijk betrouwbare bevestiging wordt het bedrag naar het opgegeven rekeningnummer overgemaakt.

Cashpool

Een kleine week later volgt een tweede factuur van meer dan 2,5 miljoen euro. De algemeen directeur dringt per mail bij het hoofdkantoor aan op telefonisch contact, vanwege de precaire financiële positie, maar dat wordt afgewimpeld. Om de relatie met het hoofdkantoor niet op het spel te zetten, wordt besloten om de factuur te voldoen en dat geldt ook voor twee volgende rekeningen die per mail worden ontvangen. Daarvoor moet geld worden geleend uit de cashpool van het Franse hoofdkantoor. Dat fonds wordt vaker gebruikt bij omvangrijke financiële transacties, dus dat wekt niet direct argwaan.

19.244.304 euro

Op 22 maart vragen de cybercriminelen om een aanvullend budget voor ‘communication and development’. Deze keer gaat het om een bedrag van 5,8 miljoen euro en ook die transactie verloopt, met steun van het nietsvermoedende hoofdkantoor, probleemloos. Een paar dagen later ploft het volgende verzoek om miljoenen over te maken in de mailbox van de directie. Weer biedt de cashpool uitkomst. Intussen is op die manier ruim 19 miljoen euro van eigenaar gewisseld. En dan gaan de alarmsirenes bij het Franse hoofdkantoor wel af. De fraude komt aan het licht, maar het geld is niet meer te achterhalen en de directie van Pathé Nederland moet het veld ruimen, hoewel dat bij de CFO niet zonder slag of stoot gaat. Uiteindelijk moet er een rechtszaak aan te pas komen om het ontslag af te wikkelen.

Wie zijn die hackers?

Bij phishing is het niet altijd eenvoudig om in de gaten te hebben dat het om phishing gaat. Een luttel moment van onoplettendheid kan enorme gevolgen hebben. En als hackers al in je netwerk zijn binnengedrongen, is het helemaal een geweldige opgave om echt van namaak te onderscheiden, bijvoorbeeld wanneer hackers een e-mailaccount van een directeur of manager hebben overgenomen. Het is dan ook van het groot belang om ongewenste toegang tot je IT-omgeving te voorkomen. Maar tegen wie bescherm je je nu eigenlijk?

Financieel gewin

Met digitale beveiligingsmaatregelen probeer je hackers buiten de deur te houden. De meeste hackers zijn doorgaans ‘black hats’ die, net als andere criminelen, uit zijn op financieel gewin. Ze hoeven niet eens zelf de technische kennis te hebben om succesvol te hacken. Op het Dark Web kun je voor relatief weinig geld

Hackers: wie, wat en waarom?

Hackers heb je in alle soorten en maten en ook nog eens met verschillende motieven die niet allemaal met geld te maken hebben. In deel 1 van ‘Hack van de dam’, onze podcastserie over cybersecurity, vertellen we er meer over.

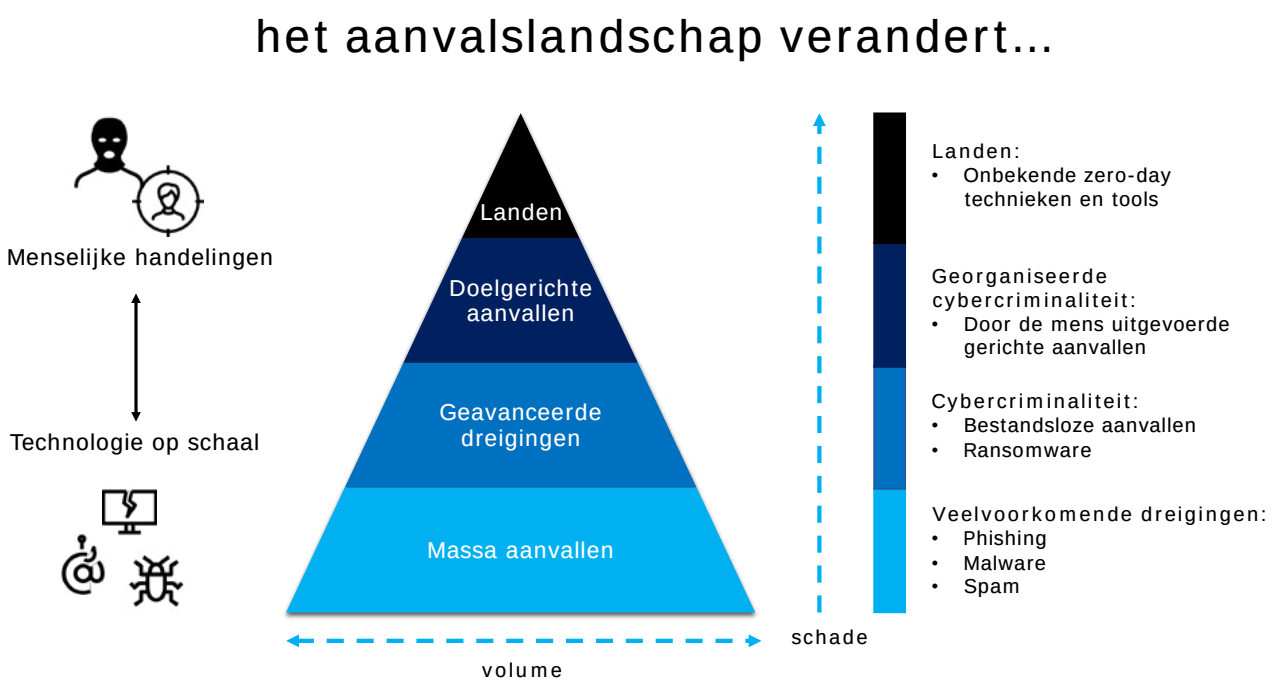
kant-en-klare hackpakketten kopen die door slimme techneuten in elkaar zijn gezet. Dat daarmee anderen geschaad worden, is voor de hackers niet van belang; zij liggen daar geen moment wakker van. Zolang de kassa rinkelt, vinden ze het allemaal prima.

Andere motieven

Toch komt het ook voor dat hackers geen financiële motieven hebben. Zo zijn er 'scriptkiddies' die vooral willen uitproberen hoe ver hun kennis reikt en hoe ze beveiligingsmaatregelen kunnen omzeilen. Verder onderkennen we 'hacktivisten', een groep of protestbeweging die het niet eens is met het beleid van een organisatie en daarom het netwerk van die organisatie platlegt. Dan is er in feite sprake van digitale chantage, maar het kan ook gaan om exposure, waar het bij activisme vaak om draait, en zelfs vanuit een overheid worden gedaan (State Sponsored). En je hebt ook nog ethische hackers (white hats) die de digitale beveiliging met medeweten van een organisatie testen om zwakke plekken op te sporen zodat problemen voortijdig opgelost kunnen worden.

Veranderend aanvalslandschap

De aanvallen op de Universiteit van Maastricht en Pathé illustreren het veranderende aanvalslandschap. In eerste instantie voerden hackers vooral aanvallen uit door massaal phishing-netten uit te gooien, netwerken met malware te besmetten of simpelweg spam te verspreiden. Daartegen is het relatief eenvoudig om beschermende maatregelen te nemen. Denk aan antispam, antivirus en antimalware oplossingen.



Endpoint Detection & Response

Om je tegen geavanceerde dreigingen en doelgerichte aanvallen te beschermen, waarbij hackers proberen je IT-systeem binnen te dringen en door verkenning vast te stellen waar je het meest kwetsbaar bent, moet je het gaan zoeken in oplossingen als Endpoint Detection & Response. Zeker in deze tijd waarin thuiswerken een geweldige vlucht heeft genomen, is het belangrijk om de thuiswerkplekken te monitoren om te voorkomen dat die voor hackers een toegangspunt tot de IT-omgeving van de organisatie worden. Met EDR worden alle werkplekken en servers binnen een IT-omgeving voortdurend gemonitord om digitale bedreigingen in de kiem te kunnen smoren. Afwijkende en onverwachte activiteiten worden direct in kaart gebracht en potentiële dreigingen worden vervolgens meteen geneutraliseerd. Dat verhoogt niet alleen de veiligheid, maar maakt het IT-beheer ook nog eens beduidend eenvoudiger.

Identiteitsfraude Preventie

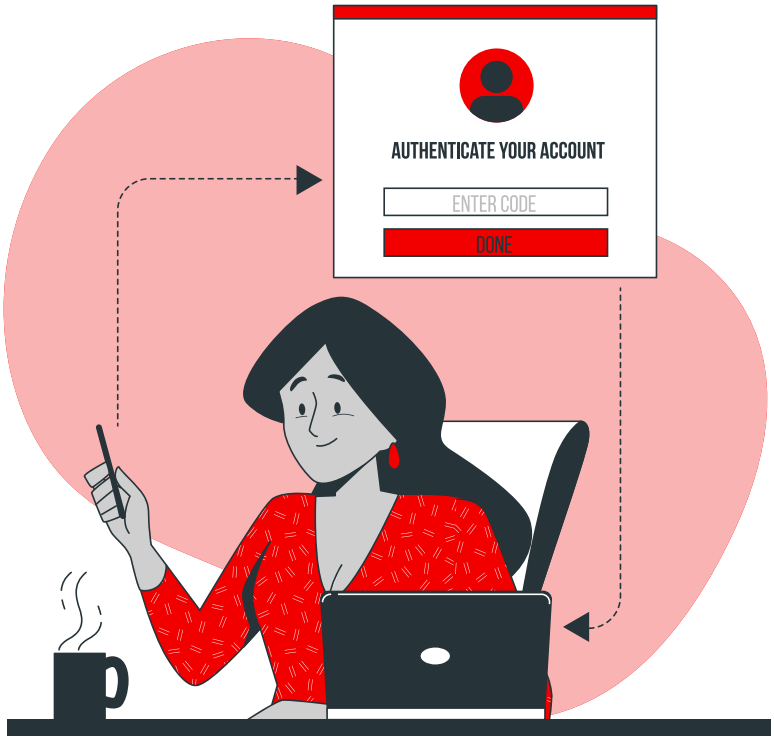
Om te voorkomen dat persoonlijke en/of privacygevoelige gegevens van medewerkers door hackers worden misbruikt, is Identiteitsfraude Preventie een goed idee. Dan wordt mogelijk onrechtmatig gebruik van dergelijke gegevens direct gedetecteerd en kan bij misbruik meteen actie worden ondernomen. Een bijkomend voordeel is dat deze oplossing ook nog eens bijdraagt aan het creëren van veiligheidsbewustzijn bij medewerkers op kantoor en thuiswerkers.

Op de agenda van de directie

We gaan er van uit dat je intussen overtuigd bent dat jouw organisatie iets moet doen om de digitale weerbaarheid te verhogen. Als je IT-manager bent, hoeven we dat vast niet te benadrukken. Dan weet je als geen ander dat cybersecurity van groot belang is om de continuïteit van de bedrijfsprocessen te verzekeren. Alleen is digitale veiligheid niet alleen voorbehouden aan de IT-afdeling. Wanneer de overige medewerkers in de organisatie zich daar niet voor inspannen, ben je een roepende in de woestijn en loop je het risico dat jouw vraag om aandacht voor dit onderwerp een hoog ‘Peter en de wolf’ gehalte krijgt. Dus: hoe krijg je het voor elkaar om de mensen die daar iets over te zeggen hebben over de streep te trekken? Dan is het eerst zaak om cybersecurity op de agenda van de directie te krijgen.

Veiligheidsbewustzijn

Ook Nederland ICT vindt overigens dat cybersecurity op directieniveau blijvende aandacht behoeft. Volgens de IT-brancheverenigingmaken organisaties idealiter minimaal 10 procent van hun IT-budget voor digitale veiligheid vrij. Daarnaast moeten directies zich meer bewust zijn van het belang van een goede aanpak. “Binnen de top van bedrijven moet de kennis van security echt omhoog”, stelt Nederland ICT. Daar komt bij dat het topmanagement van bedrijven in verreweg de meeste gevallen niet onderkent dat de verantwoordelijkheid voor goede beveiliging bij de directie ligt, en niet bij de IT-afdeling. Bovendien wordt de potentiële schade van een digitale aanval regelmatig onderschat. Dat leidt tot de logische conclusie dat eerst het veiligheidsbewustzijn op directieniveau moet worden verhoogd. Pas dan kunnen investeringen in IT-veiligheidsmaatregelen worden gedaan.



Belevingswereld

Daarbij is de uitdaging om de inzichten op het gebied van cybersecurity te vertalen naar de belevingswereld van de directie en/of het bestuur van een jouw organisatie. Dus niet: ‘We gaan een innovatie implementeren en die moet wel veilig gebruikt kunnen worden…’, maar ‘We gaan innoveren, uitstekend! Maar als we die niet gebruiksveilig implementeren, zijn we kwetsbaar voor cyberaanvallen. De gemiddelde schade bij een cyberaanval bedraagt in het MKB bijna 80.000 euro, buiten de indruk die we op onze klanten maken wanneer bekend wordt dat we door een cyberaanval zijn getroffen. Willen we dat risico lopen?’ Grote kans dat je daarmee meer indruk maakt dan wanneer je cybersecurity alleen uit technisch oogpunt benadert.

Preventie

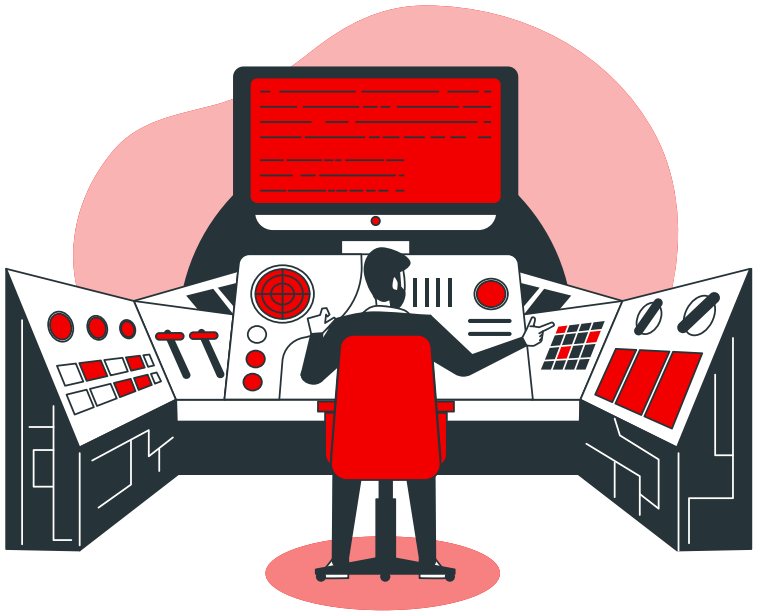
Een extra argument om cybersecurity in de schijnwerpers te zetten, is de institutionalisering van het thuiswerken. Buiten de traditionele kantooromgeving, waar het netwerk vanzelfsprekend optimaal is beveiligd, liggen digitale gevaren in thuiswerksituaties volop op de loer. Applicaties en diensten worden afgenomen uit de cloud en medewerkers kunnen overal werken. Om bedrijfsprocessen toch veilig te laten verlopen, is investeren in een veilige IT-omgeving - inclusief het vaststellen van protocollen om toegang tot die omgeving te krijgen - uit het oogpunt van preventie absoluut noodzakelijk.

Security Advisory Center

Doordat de cyberdreigingen toenemen - en steeds doelgerichter worden - groeit de behoefte aan gespecialiseerde kennis om de cyberveiligheid te verhogen. Vaak is dat kennis die niet binnen de eigen organisatie aanwezig is. En cybercriminaliteit is helaas nooit volledig te voorkomen, maar je kunt het risico om er slachtoffer van te worden wel aanmerkelijk verkleinen. Om daar concreet aan bij te dragen, hebben wij binnen onze eigen organisatie het Security Advisory Center opgericht.

Bijzondere status

Ons Security Advisory Center heeft een bijzondere status binnen Avantage. Het SAC is een zelfstandige afdeling en staat los van de operationele afdelingen. Daardoor zijn onze ervaren securityspecialisten in staat om onze klanten onafhankelijk te adviseren op het gebied van cyberweerbaarheid en veiligheid. De dienstverlening is gericht op het analyseren van cyberdreigingen tot en met het uitvoeren van complete cybersecurity assessments. Steeds met het doel om de klant het juiste securityadvies te geven, passend bij de specifieke bedrijfsactiviteiten en ook om ons klantenteam te adviseren met adequate maatregelen om dreigingen te neutraliseren.



Continu proces

Nu wil je als organisatie niet alleen vandaag digitaal veilig zijn, maar ook in de toekomst. Daarom ontwikkelt het SAC gestandaardiseerde security solutions. Dit zijn pasklare oplossingen voor de meest voorkomende uitdagingen op het gebied van cybersecurity. Het voordeel van onze ‘standaardoplossingen’ is dat deze snel en eenvoudig geïmplementeerd kunnen worden. Door de oplossingen slim te combineren, krijg je exact de mate van cybersecurity die past bij jouw organisatie. Omdat wij ervoor zorgen dat de oplossingen up-to-date zijn, heb je er in de praktijk geen omkijken naar.

Veiliger werken

Naast aandacht voor IT-oplossingen, is het minstens zo belangrijk om het security bewustzijn binnen jouw organisatie te verhogen. Aan de ene kant door medewerkers bij te brengen hoe ze digitale gevaren beter kunnen onderkennen; aan de andere kant door werkwijzes om veiliger te werken te introduceren. We kunnen bijvoorbeeld scannen op gestolen ‘credentials’ (inlogcombinaties en gevoelige persoonlijke informatie); security bewustwording campagnes lanceren om identiteitsfraude te voorkomen; een veilige back-up van bedrijfsdata in de cloud aanbieden; monitoren van ongewenst gedrag op werkplekken en servers; scannen op kwetsbaarheden in de IT-omgeving; beschermen tegen virussen/malware en de werkplekken periodiek updaten om de beveiliging op peil te houden. We bieden dus een compleet pakket om de digitale weerbaarheid van jouw organisatie te verhogen en veiliger te werken.

CIS raamwerk

Ons Security Advisory Center bouwt oplossingen op het fundament van het CIS-raamwerk. CIS is een internationaal erkende standaard van securitymaatregelen, opgesteld door het Center for Internet Security (CIS). De grondslag van het CIS-raamwerk is dat de cybersecurity van een organisatie in belangrijke mate op orde is - en risico's zijn geminimaliseerd - wanneer de betreffende maatregelen volledig zijn geïmplementeerd.
Het raamwerk zelf bestaat uit verschillende securityelementen (controls), die stuk voor stuk zijn onderverdeeld in meerdere gerelateerde subcontrols.

Gefaseerde invoering

De controls hebben te maken met verschillende aspecten van cyberveiligheid. Allereerst zal aan de basiseisen moeten worden voldaan. Daarmee is een belangrijke stap op weg naar cybervolwassenheid gezet. Op het fundament van de basishygiëne kunnen vervolgens diverse securitybouwstenen worden geplaatst om de cyberveiligheid te optimaliseren. Daarnaast gaat het CIS-raamwerk in op een aantal organisatorische aspecten van cybersecurity. Hoe uitgebreid alle CIS-elementen in beschouwing worden genomen, hangt af van de omvang, complexiteit en privacygevoeligheid van de organisatie. Uit het oogpunt van zorgvuldigheid worden de voorkomende maatregelen doorgaans gefaseerd ingevoerd.

CIS Controls

01 Inventory and Control of Enterprise Assets	02 Inventory and Control of Software Assets	03 Data Protection
04 Secure Configuration of Enterprise Assets and Software	05 Account Management	06 Access Control Management
07 Continuous Vulnerability Management	08 Audit Log Management	09 Email and Web Browser Protection
10 Malware Defenses	11 Data Recovery	12 Network Infrastructure
13 Network Monitoring and Defense	14 Security Awareness and Skills Training	15 Service Provider Management
16 Applications Software Security	17 Incident Response Management	18 Penetration Testing

Steeds veiliger in vier stappen

#1. Weten wat je hebt

Als je niet weet wat je hebt, kun je het ook niet beveiligen. Je zult dus eerst moeten inventariseren welke elementen deel uitmaken van jouw IT-omgeving voordat je kunt bepalen welke risico's er zijn. Deze eerste stap is essentieel voor het vervolg om de digitale beveiliging naar een zo hoog mogelijk niveau te tillen.

#2. Voorkomen van schade

Wanneer je eenmaal in kaart hebt gebracht welke potentiële kwetsbaarheden er zijn, is het zaak om vast te stellen hoe we kunnen voorkomen dat die 'zwakke plekken' tot schade voor jouw organisatie leiden. Daarbij nemen we niet alleen IT-oplossingen in beschouwing, maar zoeken we ook naar mogelijkheden om cybersecurity in de werkwijze van jouw organisatie te verankeren. Bovendien nemen we ook het online gedrag van jouw medewerkers in onze overwegingen mee. Het ontwikkelen en verhogen van veiligheidsbewustzijn binnen jouw organisatie is een belangrijke randvoorwaarde om de digitale weerbaarheid te versterken.

#3. Signaleren en neutraliseren

Als je een adequaat pakket met beveiligingsmaatregelen hebt samengesteld, is dat eigenlijk nog maar het begin van duurzame cybersecurity. Je zult voortdurend in de gaten moeten houden of zich toch veiligheidsincidenten voordoen, bijvoorbeeld door onachtzaamheid van medewerkers, niet tijdig updaten van beveiligingstools of door aanpassingen in jouw IT-omgeving. Daarvoor zijn geautomatiseerde oplossingen beschikbaar, die bij signalering van incidenten direct aanzetten tot het nemen van acties.

#4. Reageren en bijsturen

Tot slot is het van belang om het securitybeleid regelmatig te toetsen aan de realiteit. Voldoen alle maateregelen nog? Zijn er zaken die moeten worden aangepast? Door het securitybeleid stelselmatig te actualiseren, blijf je in elk geval bij de les en voorkom je onnodige risico's.

> *'De eerste stap is essentieel voor het vervolg om de digitale beveiliging naar een zo hoog mogelijk niveau te tillen.'*

Cybersecurity Technical Scan

‘Wat zijn voor mijn organisatie de belangrijkste risico’s als gevolg van cyberdreigingen?’ ‘En waarin moeten wij investeren om als organisatie veiliger te worden?’ Om daar antwoord op te kunnen geven, zetten we in eerste instantie onze Cybersecurity Technical Scan in. Daarmee brengen we het basisniveau van de cyberveiligheid van jouw organisatie in kaart. Dat doen we door op 5 hoofdpunten te inventariseren in hoeverre technische maatregelen in jouw IT-omgeving zijn geïmplementeerd en vast te stellen wat de impact daarvan is, waarna we onze bevindingen met jou delen.

Identeiteit en toegang

We kijken onder meer naar het wachtwoordbeleid in jouw organisatie en we checken ook of er sprake is van ‘slapende accounts’ in jouw IT-omgeving. Daarnaast willen we graag weten of je multifactor authenticatie (MFA) gebruikt. Bovendien stellen we vast of wachtwoorden van medewerkers onbedoeld ‘gelekt’ zijn en wat de kwaliteit van de gebruikte wachtwoorden is.

E-mail security

Hoe zit het met antispam en aanvullende e-mail securityoplossingen? Is de verzender van een inkomend e-mailbericht wel gerechtigd om dat bericht namens de vermelde afzender te verzenden? We hebben geautomatiseerde tools om dat vast te stellen en zetten die daar dan ook volop voor in.

Werkplekken en servers

Natuurlijk kijken we ook of de antivirus oplossing goed functioneert en of je beschermd bent tegen malware. En we controleren hoe het staat met het patchmanagement (ook van ‘third party apps’), de ondersteuning van het besturingssystemen en de versleuteling van mobiele devices die op Microsoft Windows draaien.

Externe toegang

Medewerkers die vanuit huis of onderweg werken, moeten veilig verbinding kunnen maken met jouw IT-omgeving én over een veilige internetverbinding beschikken. Dat moeten we dus zeker weten. We stellen ook meteen vast of er andere externe kwetsbaarheden zijn.

Back-up and recovery

Zijn er gegevens in jouw organisatie waarvoor bewaarplicht geldt? Zijn de data in de back-up versleuteld en hoe snel kunnen de gegevens worden teruggezet? Ook dat checken we nauwkeurig.

Rapportage

Op basis van onze constateringen ontvang je een scanrapport, inclusief een advies met oplossingen voor punten die aandacht behoeven. Het advies wordt met jou besproken, zodat we samen kunnen kiezen voor maatregelen die passen bij jullie organisatie en ambitie om de cyberveiligheid te verhogen.

Cybersecurity Assessment

De meest nauwkeurige manier om het niveau van cybersecurity in jouw organisatie vast te stellen, is aan de hand van een Cybersecurity Assessment. Het al eerdergenoemde CIS-raamwerk is de perfecte manier om de cybersecurity volwassenheid van jouw organisatie gestructureerd te meten en van daaruit een concreet actieplan te creëren om de cyberveiligheid van de organisatie te optimaliseren. Daarvoor gebruiken we een vijfstappenplan.

Identeiteit en toegang

De eerste stap is een ‘scoping’ workshop waarin we jouw verwachtingen van het assessment doorspreken en samen bepalen welke subcontrols relevant zijn voor het assessment.

E-mail security

Als tweede gaan we voor die subcontrols informatie verzamelen, die we bij jou verifiëren voordat we de volgende stap zetten.

Werkplekken en servers

De tijdens eerdere stappen verkregen informatie analyseren we met behulp van een assessment tool. Daaruit komt een score tevoorschijn die de mate van volwassenheid van het cybersecurityniveau binnen jouw organisatie weergeeft. Daarbij wordt ook de informatie geïnterpreteerd, worden risico’s in kaart gebracht en conclusies getrokken.

Externe toegang

Aansluitend stellen we een adviesrapport voor je op, waarin we concrete aanbevelingen doen om de cyberveiligheid in jouw organisatie te optimaliseren.

Back-up and recovery

Tenslotte worden de uitkomsten en het advies van het assessment aan jou (en eventuele andere belanghebbenden) gepresenteerd.

Helder securitybeleid

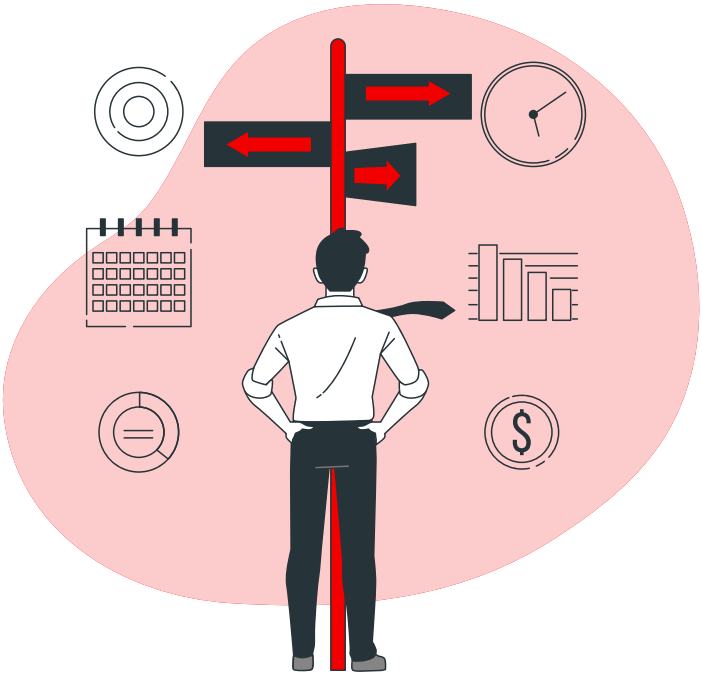
Voordat je aan de slag gaat met het verhogen van de digitale veiligheid in jouw organisatie, moet je beseffen dat cybersecurity geen ‘feestje van IT’ is. Het is noodzakelijk om securitydoelstellingen te vertalen naar securitybeleid dat door de directie wordt vastgesteld en door de gehele organisatie wordt gedragen. Helder securitybeleid maakt het bovendien eenvoudiger om nieuwe medewerkers tijdens het onboarding traject duidelijk te maken welk belang jouw organisatie aan digitale veiligheid hecht. Daardoor wordt het voor de volledige organisatie steeds duidelijker dat digitale veiligheid geen exclusieve IT-aangelegenheid is, maar iedereen aangaat en dat elke medewerker daar zijn of haar steentje aan kan - en zelfs móet - bijdragen. HR kan dat proces uitstekend borgen in de organisatie.

Welke middelen kies je?

De afbeelding van het CIS-raamwerk (op pagina 9) toont de controls die gebruikt worden om de mate van digitale veiligheid in een organisatie vast te stellen. Hieronder kun je zien in welke fase van cybersecurity diverse controls kunnen worden ingezet. Daar lichten we er een aantal van uit. Eerder hebben we al Endpoint Detection & Response en Identiteitsfraude Preventie aangestipt. Nu gaan we kort in op continue scanning van de IT-omgeving, extra beveiliging bij aanmelden en het veilig houden van werkplekken.

Vulnerability Scanning

Om een goed vervolg te geven aan een Cybersecurity Assessment, is Vulnerability Scanning zeker het overwegen waard. De IT-omgeving van jouw organisatie moet namelijk altijd veilig toegankelijk zijn voor thuiswerkers. Het is dus belangrijk om potentiële kwetsbaarheden in jouw IT-omgeving proactief op te sporen, zodat er geen data verloren gaan of in verkeerde handen komen. Daarom is het verstandig om jouw IT-omgeving continu (extern) te laten scannen op kwetsbaarheden en op de hoogte gehouden te worden van de resultaten. Met Vulnerability Scanning heb je er geen omkijken naar.



MultiFactor Authenticatie (MFA)

Als organisatie wil je natuurlijk wel zeker weten dat degene die zich bij jouw netwerk aanmeldt ook écht de persoon is die hij of zij claimt te zijn. Dat kun je borgen via MultiFactor Authenticatie (MFA). Dat gaat een stap verder dan aanmelden met een gebruikersnaam en een wachtwoord. In feite creëer je met MFA een extra beveiligingslaag, waardoor het voor kwaadwillenden nóg moeilijker wordt om jouw digitale omgeving binnen te dringen. Wij kunnen je adviseren welke specifieke MFA-oplossing het meest geschikt is voor (de situatie in) jouw organisatie.

Security & Update Management

Het updaten van (beveiligings)software is essentieel voor een veilige online werkomgeving. Om digitaal veilig vanuit huis of onderweg te kunnen werken, is het belangrijk dat de meest recente software- en beveiligingsupdates op een pc of laptop zijn geïnstalleerd. Updates zorgen er namelijk voor dat beveiligingslekken worden gedicht. Wanneer dat niet het geval is, wordt een online werkplek een eenvoudige prooi voor hackers. Door de updates uit te voeren, geef je hen weinig kans om online toegang te krijgen tot een werkplek. Daarnaast is een up-to-date antivirusprogramma van het hoogste belang om digitale aanvallen te voorkomen. Met Security & Update Management wordt dat automatisch verzekerd.

Security Awareness

Ook al werken jouw medewerkers in een veilige IT-omgeving, het blijven mensen. Wanneer ze niet weten welke cybergevaren er zijn, kun je dus ook niet van ze verlangen dat ze alert op bedreigingen reageren. Dan maken ze fouten uit onwetendheid. Daarbij komt ook nog eens dat cybersecurity voor veel mensen een ver-van-mijn-bed-show is. Het wordt zelden in verband gebracht met iets waar ze zelf iets aan kunnen doen. Toch is dat wel degelijk het geval. Op het niveau van IT-gebruikers kun je als directie en management een paar eenvoudige stappen zetten om de security awareness in jouw organisatie te verhogen. Met een gedegen programma is dat niet eens zo ingewikkeld. In het kort komt het plan van aanpak neer op testen, blijven testen, kennis aanbieden en het ‘leuk’ houden.

Uit de praktijk

Bij een van onze klanten is security awareness inmiddels uitgegroeid tot een bedrijfsproces, waarin phishingtesten, e-learning en gamification zijn geïntegreerd. Wanneer je een nepmail zelf verstuurt, kun je meten hoeveel medewerkers in jouw organisatie zich laten verleiden om op de ingevoegde link te klikken en welke onderwerpen daarbij populair zijn. Op een e-learning platform kun je korte video's plaatsen waarin één aspect van cybersecurity wordt behandeld. Denk aan het maken van sterke wachtwoorden, veilige opslag (en veilig delen) van gegevens of een betrouwbare internetverbinding. Zo zijn er veel meer securitythema's die je op een gebruikersvriendelijke manier tot leven kunt laten komen. En je kunt spelelementen aan het proces toevoegen, zoals een cybersecurity quiz waarin verschillende vragen over digitale gevaren worden gesteld. Zo wordt cybersecurity geen zwaar onderwerp, maar eerder iets om samen te doen en dat is ook nog eens goed voor de teamgeest. Maar het belangrijkste is om cybersecurity een vaste plek in jouw organisatie te geven. Tenslotte gaat digitale veiligheid iedereen aan.

Optelsom van IT, werkwijze en gedrag

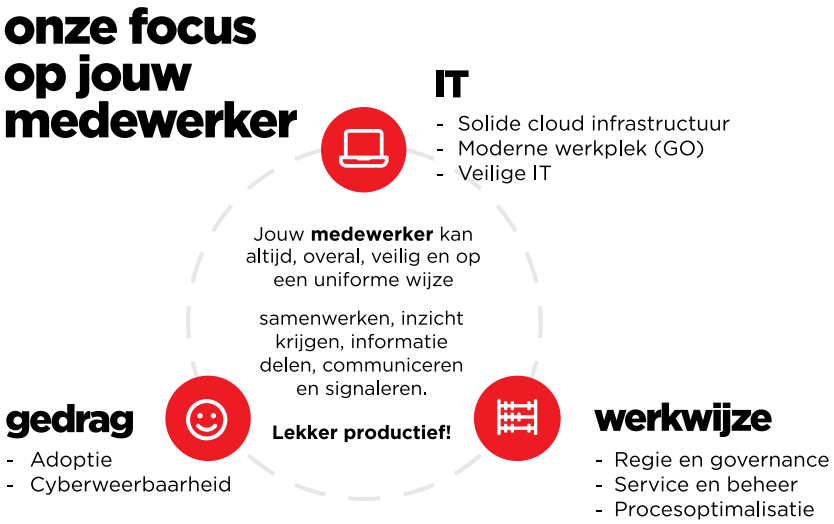
Cybersecurity is veel meer dan een veilige pc of laptop en een veilige internetverbinding. Digitale veiligheid heeft ook te maken met de manier waarop gewerkt wordt en het veiligheidsbewustzijn van medewerkers. Je moet niet alleen je technische voorzieningen op orde hebben, maar ook bedrijfsprocessen en -procedures digitaal veilig inrichten én je medewerkers doordringen van het belang van veilig werken. Door hen goed voor te lichten over de gevaren, de werkwijze efficiënt af te stemmen op je bedrijfsvoering en je IT-omgeving daarop in te richten, bereik je het maximale resultaat.

Hack van de dam

In onze podcastserie 'Hack van de dam' draait alles om het verhogen van de digitale weerbaarheid en veiligheid van organisaties. Die thema's belichten we vanuit meerdere perspectieven (logischerwijze IT, werkwijze en gedrag), waarbij ons doel is om te informeren, te inspireren en het security bewustzijn te verhogen. Ben je benieuwd naar de podcast? Je vindt de afleveringen hier.

Over Avantage

Wij geloven dat IT altijd en overal voor jou moet werken. Daarbij maakt het niet uit op welke van de laatste woorden je de klemtoon legt. **IT móet gewoon voor jou wérken. Bovendien moet IT vóór jóu werken.** Dat is precies het vakgebied waar wij al meer dan 30 jaar verstand van hebben. Met onze praktische klantervaringen en ons uitgebreide dienstenpakket combineren wij de werkwijze in jouw organisatie en het digitaal gedrag van jouw medewerkers met onze IT om 'de mensen die het moeten doen' productiever (samen) te laten werken. Daarbij bestaat de basis uit een solide infrastructuur, een veilige IT-omgeving, efficiënt beheer, klantgerichte ondersteuning en hulp bij de adoptie van innovaties. Dat komt allemaal samen in ons online platform GO, waar iedereen vanuit de eigen rol direct beschikt over alle informatie en middelen die nodig zijn om de productiviteit in jouw organisatie te verhogen en jouw klanten nóg beter te bedienen.



SINDS 1990

1354 KLANTEN

202 COLLEGA'S

EEN 8 GEMIDDELD

32 MILJOEN PER JAAR

152.000 WERKPLEKKEN

Wil je de cybersecurity-aanpak van jouw organisatie naar een hoger niveau tillen? Neem dan contact op met Vincent Quast en maak een afspraak voor een kosteloze sessie om je te inspireren op het gebied van cybersecurity.

vincent.q@avantage.nl

06 22 99 98 85

Call/chat via Microsoft Teams