HOFFMANN TIPS

voor bedrijfsleven en publieke sector

Special | Cybersecurity & Risk management

Niet óf, maar wánneer. Bent u goed voorbereid?

- *Een hackdemo waar je mond van openvalt*
- *Europese wetgeving cybersecurity: NIS2*
- *Klantverhaal: Rekenkamercommissie (Jeroen van Oort)*
- *Praktijkcasus: Onze mystery guests testen de fysiek beveiliging*
- *Phishing via Teams succesvol*
- *Hoffmann@DEF CON Las Vegas*

Hoffmann

Column

Niet óf, maar wánneer. Bent u goed voorbereid?

Brandblussers worden elk jaar verplicht gecontroleerd binnen uw organisatie. Rookmelders worden geregeld getest. En de bhv'ers gaan elk jaar op herhaaltraining voor up-to-date kennis. Het zijn voorbeelden van concrete en zichtbare manieren waarop u uw organisatie beschermt. Veel minder zichtbaar en een stuk abstracter is cybersecurity binnen uw organisatie.

Nieuwe Europese richtlijn vanaf 2024
Een concrete ontwikkeling die zorgt voor zichtbaarheid en aandacht, is de richtlijn Network and Information Security (NIS2). Deze Europese richtlijn gaat vanaf 2024 gelden en is veel minder vrijblijvend. Een grote verandering ten opzichte van de eerste NIS-richtlijn is de bredere groep van sectoren waarvoor de richtlijn geldt. Een ander verschil is dat niet alleen naar de eigen organisatie gekeken wordt, maar ook naar de keten. Kwetsbaarheden bij een samenwerkingspartner of leverancier kunnen uiteindelijk ook impact hebben op uw eigen bedrijfsvoering. Daar zijn helaas legio voorbeelden van te noemen. Vanuit Hoffmann juichen we deze integrale blik op cyberveiligheid dan ook toe.

Niet of, maar wanneer
In deze tijd waarin personen, spullen en netwerken steeds meer (online) met elkaar verbonden zijn, is cyberveiligheid essentieel. Ransomware is een bedreiging voor elke organisatie. Ik zeg vaak: het is niet de vraag óf uw organisatie geraakt wordt, maar wánneer. Misschien geen leuke uitspraak, wel realistisch. Wist u bijvoorbeeld dat het risico van een cyberaanval op uw organisatie 1 op 5 is, terwijl het risico op een fysieke inbraak vele malen kleiner is met 1 op 250? U kunt niet voorkomen dat uw organisatie wordt aangevallen, maar u kunt u wel goed voorbereiden.

Investeer in preventie
Gelukkig zien we dat organisaties zich steeds bewuster worden van de cyberrisico's voor hun bedrijfsvoering én hun partners, leveranciers en serviceproviders. Uit onderzoek in opdracht van het Ministerie van Economische Zaken blijkt dat de kosten van een cyberincident ongeveer 300.000 euro zijn. Dit weegt niet op tegen de investering in maatregelen om de cyberweerbaarheid van uw organisatie te verhogen. Het reserveren van budget voor het in kaart brengen van cyberrisico's en het nemen van adequate maatregelen is dan ook geen overbodige luxe.

Tijd voor actie
Wees goed voorbereid op wat er kan gebeuren! Op allerlei verschillende manieren helpen wij organisaties om bewustzijn te creëren rondom cyberveiligheid. Met deze special van de Hoffmann Tips kunt u inspiratie en kennis opdoen. Op het gebied van menselijk gedrag, de techniek en de organisatie. En twijfel niet: bij vragen staan onze pentesters, gedragswetenschappers en risicospecialisten klaar om u verder op weg te helpen.

Ik wens u veel leesplezier!
Johan van Slooten

Director Cybersecurity & Risk management

Een hackdemo waar je mond van openvalt

Op het jaarlijkse partnerevent van een van onze samenwerkingspartners gaven wij deze zomer een presentatie met een live hackdemo. Ongeveer 100 mkb'ers kijken met grote ogen naar een van onze ervaren pentesters. Hij laat live zien hoe hacken werkt en welke fases daarbij doorlopen worden. Op een splitscreen zien de mkb'ers wat de hacker ziet en doet én wat het fictieve slachtoffer in zijn scherm ziet.

De eerste stap: de klik op een verkeerde link
Op een verkeerde link klikken kan iedereen overkomen. Het gaat erom hoe je er vervolgens mee omgaat. Had je door dat het niet helemaal deugde? En wat gebeurt er eigenlijk achter de schermen als je op een linkje klikt? De deelnemers in de zaal zien wat het nut is van Multi-Factor Authenticatie (MFA), maar ook dat het niet de heilige graal is. Onze pentester heeft namelijk mogelijkheden om de MFA te omzeilen. En dan zijn inloggegevens makkelijk af te vangen. Hij heeft een voet tussen de deur.

De tweede stap: het lokale systeem binnenkomen
Lukt het de hacker vervolgens om de deur open te zetten? Onze pentester laat zien hoe hij een bijlage met schadelijke code verstuurt naar ons fictieve slachtoffer. Het publiek krijgt ook te zien hoe betrouwbaar de e-mail eruitziet. En hoe verleidelijk het is om geen aandacht te besteden aan een bijlage die niet goed opent. Door de poging om de bijlage te openen heeft de hacker echter zijn doel al bereikt: de schadelijke code is op het lokale systeem geïnstalleerd en geeft de hacker toegang.

De derde stap: het lokale systeem benutten
De hacker is het lokale systeem van het slachtoffer binnengedrongen. We laten zien hoe de hacker zichzelf meer rechten geeft, zodat hij 'eigenaar' wordt van het lokale systeem. Dit betekent dat hij documenten kan aanpassen of verwijderen. Om te demonstreren wat er met meer rechten mogelijk is, maken we ongemerkt een foto van het publiek in de zaal. Eenmaal eigenaar van het systeem kun je namelijk ook de webcam bedienen.

De vierde stap: het organisatiesysteem binnenkomen
Zou het ook lukken om vanuit het lokale systeem de sprong te maken naar het organisatiesysteem? Zodra een hacker zich door het organisatiesysteem kan bewegen én zichzelf meer rechten kan geven, kan hij alles op slot zetten. Een ransomware-aanval dus.

Urgentie en bewustzijn als resultaat
Met onze hackdemo laten we zien wat er kan gebeuren: van de eerste klik op een link tot een aanval met ransomware. In 20 minuten doorlopen we een heel scenario met het publiek. Natuurlijk kunnen we niet alles laten zien, maar de bewustwording is op gang geholpen. Vooral de concrete casus en voorbeelden werken goed, merken we. Na afloop zijn er diverse deelnemers die het gesprek met ons aanknopen over hoe om te gaan met dit soort risico's. En dat is juist het gesprek dat we op gang willen brengen.

Presentatie met een confronterend intermezzo

Doordat we in de hackdemo heel concreet laten zien wat er gebeurt, zit iedereen aandachtig te luisteren. Het wordt een beetje onrustig in de zaal zodra we tijdens een kort intermezzo een socialmedia-profiel laten zien. Dit profiel komt sommigen namelijk behoorlijk bekend voor. En dat kan kloppen, want in de voorafgaande week hadden wij ongeveer de helft van de deelnemers benaderd vanaf dit account. Het overgrote deel ging hierop in. En met een aantal voerden we zelfs een digitaal gesprek. Het hele profiel hadden we opgebouwd met AI: een AI-foto en een hele geschiedenis die gegenereerd was met AI. Het is een extra concreet voorbeeld dat het publiek laat zien hoe snel vertrouwen online op te bouwen is. Later horen we reacties terug van "Ik heb er geen moment bij stilgestaan dat een socialmedia-profiel een bedreiging kan zijn," tot "Ik heb de connectie gelijk verwijderd!"

Nulmeting informatiebeveiliging

Zoals u wellicht weet, levert Hoffmann verschillende diensten met als centrale thema risicobeheersing. Zo screenen wij nieuw personeel, voeren we social engineeringtesten uit, doen we fraude- en integriteitsonderzoek en organiseren we crisismanagementtrainingen. Binnen het domein Cybersecurity ontvangen wij regelmatig van organisaties het verzoek om een nulmeting informatiebeveiliging uit te voeren. In dit artikel lichten wij toe wat een dergelijke nulmeting inhoudt en waarom dit waarde toevoegt.

Integrale benadering nulmeting informatiebeveiliging
De dienstverlening van Hoffmann heeft tot doel om incidenten binnen organisaties te voorkomen, maar ook om de impact ervan te minimaliseren wanneer ze zich onverhoopt toch voordoen. Preventieve trajecten benaderen wij vanuit een perspectief waarbij het risico centraal staat. Een vraag vanuit een organisatie zou dus kunnen zijn wat haar grootste risico's zijn op het gebied van informatiebeveiliging.

Om deze risico's goed en volledig in kaart te kunnen brengen, is het van belang om zowel het informatiebeveiligingsniveau van de 'mens' (gedrag), als de 'techniek' (ICT) en de 'organisatie' (processen) te onderzoeken. Het gedrag van uw medewerkers (de 'mens') kunnen wij testen met diverse social engineeringstesten. Denk hierbij bijvoorbeeld aan e-mailphishing, voicephising en fysieke inlooptesten (mystery guest visits). Het segment 'techniek' kunnen wij testen met penetratietesten, waarbij wij testen of uw netwerk of applicaties kwetsbaar zijn voor gerichte aanvallen van hackers en andere kwaadwillenden. En hoewel over de segmenten 'mens' en 'techniek' genoeg te vertellen valt, leggen wij in het vervolg van dit artikel de nadruk op het segment 'organisatie'. Wat houdt dit precies in en hoe pakt Hoffmann dit aan?

De organisatie
Binnen het segment 'organisatie' maken wij, op het vlak van informatiebeveiliging, een inschatting van het huidige volwassenheidsniveau van uw organisatie. Dit doen wij met behulp van het zogenoemde 'volwassenheidsmodel informatiebeveiliging' en de wereldwijd erkende norm voor informatiebeveiliging, de ISO27001.

Volwassenheidsmodel informatiebeveiliging
Het volwassenheidsmodel informatiebeveiliging biedt handvatten om de informatiebeveiliging binnen de organisatie op orde te brengen. Zo geeft het inzicht in het volwassenheidsniveau van uw organisatie en geeft het richting aan de stappen die u nog moet ondernemen om de informatiebeveiliging (verder) te optimaliseren. Het model bestaat uit verschillende volwassenheidsniveaus. Wanneer organisaties zich op niveau 1 (initieel), 2 (herhaalbaar) of 3 (gedefinieerd) bevinden, richten zij hun aanpak vooral op de inrichting van informatiebeveiliging en het beleggen van de verantwoordelijkheden. Wanneer zij zich op niveau 4 (beheersen) of 5 (optimaliseren) bevinden, richten zij zich met name op het realiseren van een continu verbeterproces en een informatieveilige cultuur, zie het Maturity Model hieronder.

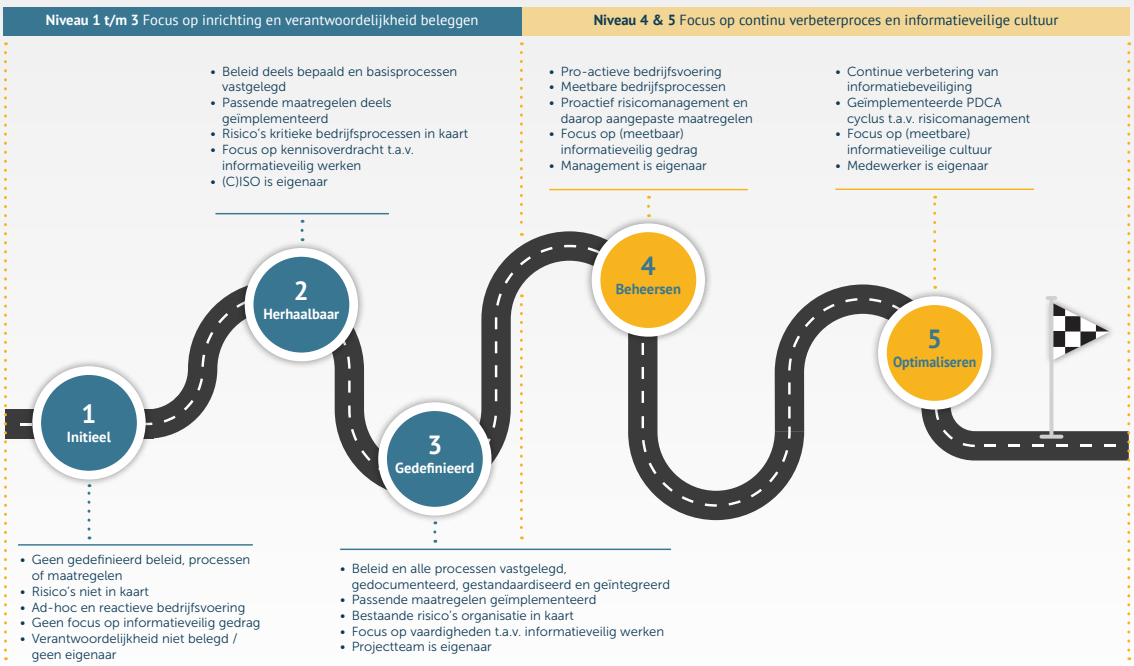
Kort samengevat, houdt bovenstaande in dat organisaties op niveau 1 niet beschikken over een pro-actieve aanpak of informatiebeveiligingsbeleid. Terwijl bij organisaties op niveau 5 informatiebeveiliging volledig geïntegreerd is in de bedrijfsvoering en sprake is van continue verbetering. Uit onze eigen onderzoeken blijkt dat de meeste organisaties niveau 2 of 3 behalen bij een nulmeting.

ISO27001
De ISO27001 is een wereldwijd erkende norm op het gebied van informatiebeveiliging. Voor de nulmeting op het segment 'organisatie' maakt Hoffmann gebruik van ISO27002, die met beheersingsmaatregelen een verdieping geeft op ISO27001. Dit kader kan worden gezien als een 'best practice' en bevat een uitgebreide set van beveiligingsmaatregelen om risico's met betrekking tot beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te identificeren en op een juiste wijze op te volgen.

Bij de uitvoering van een nulmeting beoordelen de professionals van Hoffmann de opzet en het bestaan van maatregelen binnen de organisatie. Onder 'opzet' wordt verstaan of het beleid, de processen en de procedures van informatiebeveiliging zijn beschreven. Onder 'bestaan' wordt verstaan of het beleid, de processen en de procedures ook in de praktijk worden toegepast. Bij deze nulmeting maken wij gebruik van diverse onderzoeksmethoden, zoals documentenanalyse, observatie en interviews met relevante functionarissen. Voorafgaand aan de uitvoering stemmen de consultants met de opdrachtgevers af welke medewerkers voor welke onderwerp worden bevraagd. Op basis van de verkregen inzichten worden vervolgens per thema de sterke punten en de verbeterpunten van uw organisatie op het gebied van informatiebeveiliging geformuleerd.

Tot slot vertalen wij de verkregen inzichten in een volwassenheidsscore per thema en een algemene volwassenheidsscore. Deze scores bieden aanknopingspunten om te bepalen welke thema's aandacht behoeven om het niveau van informatiebeveiliging binnen de organisatie naar een volgend niveau te tillen. Zo heeft u niet alleen inzicht in het huidige niveau, maar weet u ook op welke wijze u verbeteringen kan doorvoeren. En vanzelfsprekend adviseert en ondersteunt Hoffmann u daar graag bij.

Maturity Model Information security



Ransomware: **zet aanvallers op tijd buiten**

Via onze Tips, de website en andere kanalen hebben wij u regelmatig gewaarschuwd voor een aanval met ransomware. In deze artikelen gaven we u tips om te voorkomen dat hackers uw vitale systemen kunnen binnendringen. Uiteraard is het belangrijk dat u deze tips ter harte neemt. Maar helaas is het tegenwoordig ook zo dat het niet meer de vraag is of u wordt gehackt, maar wanneer. En dan kunt u maar beter goed voorbereid zijn.

Maar eerst nog even dit: hoe werkt ransomware ook alweer?
Bij een aanval met ransomware verschaffen hackers zich toegang tot het netwerk van uw organisatie. Met een phishing e-mail bijvoorbeeld, of door gebruik te maken van kwetsbaarheden in de software. Na het versleutelen van uw gegevens ontvangt u een melding dat u pas weer toegang tot die gegevens krijgt nadat u losgeld heeft betaald. Hackers gaan daarbij steeds professioneler te werk. Zo nemen ze vaak een aantal weken tot zelfs maanden de tijd om rond te kijken op uw systemen en de aanval zorgvuldig voor te bereiden.

Workshop Forensic Readiness
Eén van de manieren om u voorbereiden op een aanval is de workshop Forensic Readiness. Na afloop van deze workshop krijgt u antwoord op de vraag of bij een incident de juiste digitale informatie voorhanden is en blijft om een forensisch onderzoek uit te kunnen voeren. Wordt belangrijke informatie uit de systemen bijvoorbeeld bewaard zodat bij een incident de oorzaak kan worden achterhaald?

Kwetsbaarhedenscan
Een andere manier om direct zicht te krijgen op een mogelijk risico is de inzet van een periodieke kwetsbaarhedenscan. Deze scan geeft inzicht in de aanwezige technische risico's en kwetsbaarheden en de te nemen maatregelen om de eventueel geconstateerde risico's te kunnen ondervangen.

Logging, detectie en monitoring
Hackers gebruiken vaak dezelfde modus operandi. Als uw organisatie de logging op orde heeft, is die modus operandi in een vroegtijdig stadium te herkennen. Hoe? Door logdata te controleren en te analyseren. Dit kan als u vermoedt dat er hackers op het netwerk aanwezig zijn, maar ook periodiek.

E-mail phishing
Om de mate van bewustwording van uw medewerkers vast te stellen, is het ook mogelijk deze in de praktijk te testen. Met een e-mail aan een grote groep medewerkers wordt dan geprobeerd om informatie van uw medewerkers en/of uw organisatie te bemachtigen.

Vermoedt u dat er hackers binnen zijn?
Heeft u signalen dat er hackers op uw netwerk aanwezig zijn? Bijvoorbeeld omdat uw systemen traag zijn of afwijkend gedrag vertonen? Of er mails worden verstuurd uit uw naam zonder dat u ze heeft opgesteld? Of wilt u uw logdata periodiek laten controleren en analyseren? Dan zijn onze forensisch onderzoekers u graag van dienst.

Een nieuwe Europese richtlijn voor cybersecurity – NIS2

Om de digitale weerbaarheid van organisaties te verbeteren heeft de Europese Unie in oktober 2022 een nieuwe richtlijn voor cybersecurity aangenomen, de zogenoemde 'NIS2'. Met deze richtlijn wil de Europese Unie dat organisaties aan strengere beveiligings- en rapportagevereisten gaan voldoen. Dit is niet alleen in het belang van die organisaties zelf, maar ook in het belang van hun klanten. Tegelijkertijd is het belangrijk om realistisch te blijven. Want het is niet de vraag óf u het slachtoffer wordt van een cyberaanval, maar wanneer. Ook als u voldoet aan de NIS2-richtlijn is niet gegarandeerd dat uw organisatie nooit het slachtoffer wordt van cybercriminaliteit. Wel helpt de NIS2-richtlijn bij het realiseren van een betere bescherming en een betere respons op eventuele cyberincidenten.

In dit artikel geeft Hoffmann antwoord op de volgende vragen: Wat is NIS2? Valt uw organisatie onder NIS2? Welke impact heeft NIS2? En wat moet u doen om te voldoen aan NIS2?

Wat is NIS2?
De afkorting NIS staat voor Network and Information Systems. NIS2 is een uitbreiding van NIS1. Zo is NIS2 bijvoorbeeld van toepassing op meer organisaties, inclusief hun partners, leveranciers en serviceproviders. Daarnaast is in NIS2 de verantwoordelijkheid voor het beheersen van cybersecurity risico's nadrukkelijk bij het management belegd. Verder zijn de beheersings-maatregelen strenger en gelden er voor incidenten meldingsvereisten. Tot slot zijn de sancties op het niet voldoen aan de regels aangescherpt. Organisaties riskeren onder NIS2 een boete van maximaal 10 miljoen euro of 2% van de totale wereldwijde jaaromzet. Uiterlijk op 17 oktober 2024 moet Nederland de NIS2-richtlijn hebben omgezet in nationale wetgeving.

Valt uw organisatie onder NIS2?
Of uw organisatie onder NIS2 valt hangt af van de sector waarin u actief bent en de omvang van de organisatie. Kort samengevat vallen alle sectoren die van groot belang zijn voor een land onder de reikwijdte van NIS2. Denk aan de gezondheidszorg, overheidsdiensten, energie en drinkwater, maar ook ruimtevaart. Daarnaast worden individuele organisaties gekenmerkt als essentieel of belangrijk. Voor het bepalen van de juiste classificatie is de omvang van uw organisatie in medewerkers, jaaromzet en balanstotaal van belang. Een juiste classificatie als 'essentieel' of 'belangrijk' is van belang omdat deze organisaties met strenger toezicht en handhaving te maken krijgen. Wacht daarom niet te lang met het vaststellen van de classificatie die op uw organisatie van toepassing is.

Welke impact heeft NIS2?
Zoals aangegeven wordt als gevolg van de NIS2-richtlijn de verantwoordelijkheid voor het beheersen van cybersecurity risico's nadrukkelijk bij het management van een organisatie belegd. Van het management wordt actieve betrokkenheid verwacht bij het beheersen van cybersecurity risico's en het selecteren en implementeren van passende beheersingsmaatregelen. Het niet naleven van de NIS2-richtlijn kan zelfs leiden tot persoonlijke aansprakelijkheid. Een ander belangrijk thema zijn de beheersingsmaatregelen. Als basis voor de te nemen maatregelen is het nodig een risicoanalyse uit te voeren. Vanuit de beroepsorganisatie van IT-auditors (NOREA) is een handreiking opgesteld op basis waarvan u inzicht krijgt in de aanwezige cyberrisico's bij uw organisatie. Daarnaast heeft het Centre for Cyber Security Belgium een cyber fundamentals framework ontwikkeld. In dit raamwerk zijn diverse internationale normen en standaarden verwerkt, waaronder de ISO27001 als norm voor informatiebeveiliging. Een derde thema is de rapportageplicht bij incidenten. Naast de meldplicht van een datalek bij de Autoriteit Persoonsgegevens hebben organisaties straks op basis van NIS2 ook een verplichting om over significante incidenten te rapporteren.

Wat moet u doen in voorbereiding op NIS2?
De allereerste actie voor uw organisatie is om te onderzoeken en vast te stellen in hoeverre NIS2 op uw organisatie van toepassing is. In voorbereiding op de daadwerkelijke vertaling van NIS2 naar nationale wetgeving is het verder verstandig om tijdig een eerste nulmeting uit te voeren, met als doel om de risico's in kaart te brengen en het huidige beveiligingsniveau van uw organisatie vast te stellen. Een hulpmiddel hierbij is het uitvoeren van een pentest. Met een pentest wordt de beveiliging van uw netwerk en applicaties door een ethical hacker getest. Tegelijkertijd kan deze nulmeting de basis vormen voor eventuele vervolgacties. Door het tijdig uitvoeren van deze acties wordt uw organisatie niet onnodig verrast en voldoet uw organisatie per 17 oktober 2024 aan de wet.

Jeroen van Oort en Mo Ballari vertellen over de geslaagde samenwerking tussen Hoffmann en de Rekenkamercommissie

In het begin van deze Tips heeft u kunnen lezen over de zogenaamde 'nulmeting informatiebeveiliging'. De Rekenkamercommissie van de gemeenten Opmeer en Medemblik is één van de organisaties die Hoffmann de opdracht heeft gegeven voor een soortgelijk onderzoek bij de gemeente Opmeer en Medemblik. In deze casus vertellen Jeroen van Oort, voorzitter van de Rekenkamercommissie, en Mo Ballari, senior consultant Cybersecurity & Risk management bij Hoffmann, daar meer over.

Aanleiding

Jeroen: "De directe aanleiding voor dit onderzoek, dat in het voorjaar van 2022 in gang is gezet, was een aantal hacks bij grote organisaties. We zagen in de media dat die hacks veel impact hadden en de betreffende organisaties weken hadden stilgelegen, met alle schade van dien. Daarnaast had een aantal andere rekenkamers ook al een onderzoek laten doen."

"Informatieveiligheid zou binnen gemeenten een enorm belangrijk onderwerp moeten zijn," vervolgt hij. "Zij verwerken, gebruiken en verstrekken veel privacygevoelige informatie. Denk maar eens aan rijbewijzen, paspoorten en gegevens over uitkeringen. Informatie die enorm belangrijk is voor het functioneren van een overheid, maar die dus ook goed beveiligd moet worden. Bestuurlijk gezien is daar nog niet in elke gemeente voldoende aandacht voor. Ook worden er nog niet altijd voldoende financiën voor vrijgemaakt. Terwijl de financiële consequenties bij een geslaagd hack vaak vele malen groter zijn."

Tijd voor een onderzoek dus. Via een aanbesteding koos de Rekenkamercommissie voor de aanpak van Hoffmann.

> *'Informatieveiligheid zou binnen gemeenten een enorm belangrijk onderwerp moeten zijn'*
>
> *Jeroen van Oort*

Mo: "Een onderzoek naar informatieveiligheid is altijd maatwerk, maar richt zich in ieder geval op de pijlers mens, techniek en organisatie. Bij de gemeenten Opmeer en Medemblik hebben wij ons binnen die pijlers enerzijds gericht op wat wij 'opzet' noemen: de aanwezigheid van beleidsstukken en kaders over informatiebeveiliging. Anderzijds hebben we gekeken naar 'bestaan en werking', waarbij we hebben onderzocht hoe de uitwerking van dat beleid in de praktijk was. Daarvoor hebben we niet alleen gekeken naar het beleid en gesprekken met stakeholders gevoerd, maar hebben we ook onze ethical hackers ingezet. En uiteraard hebben we ook inlooptests uitgevoerd, waarbij we als 'mystery guests' hebben getracht om fysieke lokaties binnen te dringen."

Samenwerking

Uit het onderzoek dat Hoffmann uitvoerde, is een aantal kwetsbaarheden gekomen. "Die zijn ook gepubliceerd, dat is geen geheim," aldus Mo. "Eigenlijk treffen we bij ieder onderzoek wel kwetsbaarheden aan. Maar wat ik zo fijn vond aan de samenwerking met deze Rekenkamer, is dat we vooraf hadden afgesproken dat we bij zwaarwegende bevindingen die om een urgente oplossing vroegen direct contact zouden leggen. En dus niet pas bij publicatie van het rapport. In de praktijk bleken die bevindingen er ook te zijn. De Rekenkamercommissie is toen razendsnel bij elkaar gekomen en door ons bijgepraat, waarna ze ook direct toestemming gaf om met de CISO's [Chief Information Security Officer; red.] van de gemeenten naar oplossingen te zoeken. Daardoor werden er nog tijdens het onderzoek grote slagen in de beveiliging gemaakt."
"Dat klopt inderdaad," beaamt Jeroen. "Er is razendsnel een aantal stappen gezet. Helaas heeft het bestuurlijk gezien nog best een tijdje geduurd totdat er budget werd vrijgemaakt om ook de andere stappen te zetten. Publicatie van het rapport heeft in die zin wel bijgedragen aan het gevoel van urgentie."

Op de vraag wat Jeroen prettig vond aan de samenwerking met Hoffmann, antwoordt hij: "Met uitzondering van de CISO's, die technisch natuurlijk wel een aardig woordje meepraten, zijn de meeste gemeentebestuurders, zoals burgemeesters, wethouders en raadsleden, leken op het gebied van informatiebeveiliging. Terwijl ze toch er toch verantwoordelijk voor zijn. In hele heldere bewoordingen weet Hoffmann duidelijk te maken wat er technisch aan de hand is en wat daarvan de gevolgen – zowel voor de bedrijfsvoering van de gemeenten als maatschappelijk – zouden kunnen zijn. In die vertaalslag is Hoffmann heel goed. Daarnaast is de kwaliteit van het onderzoek gewoon goed. Het is wat je van een dienstverlener verwacht, maar het is wel prettig als dat ook uitkomt."

> *Vanuit Hoffmann hebben we de rol van de Rekenkamercommissie enorm gewaardeerd*
>
> *Mo Ballari*

"Als ik daar nog iets aan mag toevoegen," vervolgt Mo. "Vanuit Hoffmann hebben we de rol van de Rekenkamercommissie enorm gewaardeerd. Bij een dergelijk onderzoek is de Rekenkamer de opdrachtgever, de gemeente de onderzochte partij en het college van B&W verantwoordelijk. Dat kan een spanningsveld en soms ook weerstand opleveren. Maar in deze casus heeft de Rekenkamercommissie daar een goede rol in gespeeld, door een gezamenlijke startbijeenkomst te organiseren en uit te leggen wat er ging gebeuren. Daardoor zat iedereen op één lijn. Dat werkte heel plezierig."

Mo Ballari en Jeroen van Oort (v.l.n.r.)

Business *not as usual*

U zult het vast herkennen, de verplichte wekelijkse teamvergaderingen waarin doorgaans wordt gesproken over dagelijkse werkzaamheden en nieuwe ontwikkelingen. We noemen deze situatie ook wel 'business as usual'. Maar wat doet u als de continuïteit van uw organisatie ernstig in gevaar komt? Over crisismanagement nadenken gebeurt vaak pas op het moment dat een crisis zich aandient. De vraag is of we ons dit reactief handelen eigenlijk wel kunnen veroorloven. In dit artikel vertellen we over 'business not as usual' en wat u kunt doen om uw organisatie voor te bereiden op een crisis.

Crisissen kennen vele vormen. Denk hierbij aan natuurinvloeden zoals klimaat- en natuurrampen, maar ook aan een personeelscrisis, onbeschikbaarheid van gebouwen en leveranciers of cyberaanvallen bij uzelf of een belangrijke leverancier. Deze crisissen hebben één ding gemeen: zij zorgen voor een ernstige verstoring van de bedrijfscontinuïteit. Organisaties lopen hierdoor niet alleen risico op financieel-economische schade, maar ook op reputatieschade.

Geen woorden, maar daden

Nu dwingt wetgeving steeds meer organisaties om aan de slag te gaan met een crisisplan. Voorbeelden hiervan zijn artikel 16 van de Wet veiligheidsregio's en de Wet herstel en afwikkeling van verzekeraars. De verplichte aanwezigheid van een crisisplan is dan ook van toepassing op verschillende bedrijfstakken en overheidsorganen. Een mogelijk gevolg van deze verplichting is dat organisaties het gaan beschouwen als een hygiënefactor, een 'tick in the box', waarbij de kwaliteit en effectiviteit van het plan ondergeschikt is.

Om de effectiviteit van een crisisplan te verhogen is het belangrijk dat het belang hiervan wordt uitgedragen door het hoger management, de plannen periodiek geëvalueerd worden en nóg belangrijker: er regelmatig geoefend wordt met het plan. Want hoewel preventieve maatregelen kunnen bijdragen aan het voorkomen van een crisissituatie, blijft de realiteit dat een crisis elke organisatie kan raken. Ook uw organisatie. Ook wanneer er sprake is van 'business not as usual' moet u krachtige repressieve maatregelen kunnen treffen om het incident en de gevolgen hiervan te managen. De focus moet daarbij liggen op het beperken van de schade en het zo snel als mogelijk terugkeren naar 'business as usual'. Het is daarom belangrijk om u op een crisis voor te bereiden. Dat doet u met een crisisoefening.

Oefening baart kunst

Het doel van een crisisoefening is tweeledig. Enerzijds is het doel om het bestaande crisisplan te testen op inhoud en effectiviteit. Anderzijds is het doel om het crisisteam voor te bereiden op het daadwerkelijk managen van een crisis. Na een training zijn deelnemers onder meer in staat om zowel de eigen taken als de taken en verantwoordelijkheden van de andere leden binnen het crisisteam te benoemen. Daarnaast weet het crisisteam na de training de crisisplannen toe te passen, een crisisvergadering effectief te laten verlopen, samen te werken met een helder gezamenlijk doel en op adequate wijze te reageren op (social) mediaberichten.

Uit onze ervaring weten wij dat crisismanagement maatwerk is en contextafhankelijk. De crisistrainers van Hoffmann verdiepen zich daarom in de organisatiestructuur en lezen zich in over taken en verantwoordelijkheden binnen en tussen de teams, de bestaande crisis- en crisiscommunicatieplannen en de bedrijfscontinuïteitsplannen. Op basis van deze achtergrondinformatie en na overleg met de opdrachtgever, ontwikkelen wij een scenario. Om een strakke organisatie van de oefening te borgen, werken wij het scenario en de crisisoefening uit in een gedetailleerd draaiboek.

De crisisoefening is verdeeld in een theoretische introductie en een tabletop-oefening. De trainers van Hoffmann nemen de deelnemers van uw organisatie stap voor stap mee door de theorie en het crisisscenario; van alarmering, opschaling en respons tot nazorg. Op deze manier wordt het crisisteam door het hele traject van een crisis begeleid waarbij zij, onder begeleiding van de trainers, oefenen met rollen en verantwoordelijkheden zoals beschreven in het crisisplan. Na afloop van de oefening wordt er met het crisisteam geëvalueerd om samen stil te staan bij de sterke- en de verbeterpunten. Een eindrapportage beschrijft alle waarnemingen en actie en leerpunten. Een waardevol document voor een herevaluatie van het crisisplan. Iets wat vervolgens natuurlijk weer in de praktijk geoefend kan worden!

Lukt het een kwaadwillende om binnen te komen?

Tegenwoordig zijn er verschillende bedrijven die maatschappelijk onder een vergrootglas liggen. Dat maakt hen een interessant doelwit voor hackers en activisten. Zo ook het internationale bedrijf met vestigingen in meerdere landen dat ons inschakelt voor een onderzoek. Twee collega's gaan op pad om te kijken of de fysieke beveiliging van de vestiging in een Afrikaans land op orde is.

Scenario's en verkenning
Eerst bespreken we met de opdrachtgever de scenario's die we op locatie gaan gebruiken. Eenmaal in het Afrikaanse land verkennen onze inloopexperts eerst de omgeving. De vestiging staat op een campus met andere bedrijven waaronder een golfclub en een sportschool. In hetzelfde pand zit een bedrijf dat vergader- en kantoorruimtes verhuurt. Dat biedt mogelijkheden.

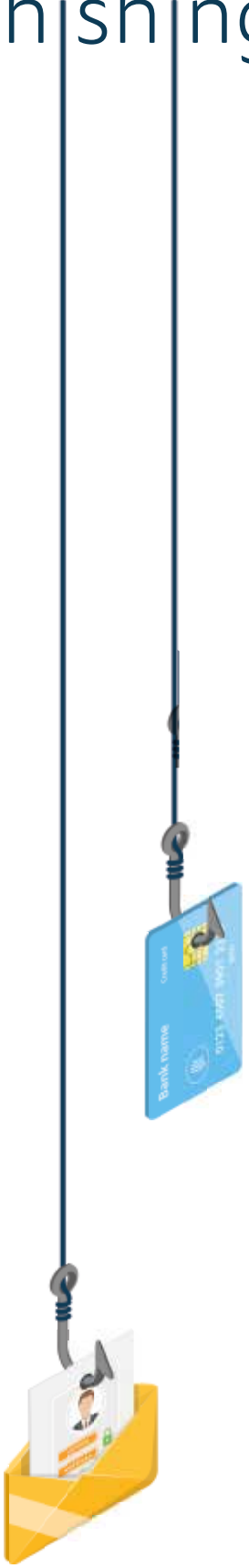
Met de taxi de campus op
Op dag 1 gaan onze onderzoekers met een taxi op weg naar de campus. De eerste hindernis, de beveiliging van de campus, is makkelijk te nemen. Zonder controle of vragen mag de taxi verder het terrein op rijden. De tweede hindernis is binnenkomen in het pand. Ze wandelen een aantal rondjes over het terrein. Een van de onderzoekers gaat in de parkeergarage van het pand polshoogte nemen. Daar ziet ze allerlei oude computers en andere hardware die achter simpele bouwhekken word bewaard. Overdag staat er slechts één bewaker bij. Snel maakt ze een foto van deze bevinding.

Naar binnen door tailgating
Vervolgens kan ze bij een schoonmaker in de lift stappen. Deze schoonmaker heeft een toegangspas voor de lift (tailgating). Zo komt ze in de hal van de vestiging terecht. De schoonmaker gaat een volgende, beveiligde ruimte binnen. Op de vraag wat ze komt doen, heeft onze onderzoeker natuurlijk een mooi verhaal klaar. Iets over een verloren oorbel na de vergadering van vorige week. Ze mag doorlopen naar de balie. Daar zit echter de hoofdbeveiliger van de vestiging. En die werkt helemaal volgens protocol: "Er is niets gevonden. En ik mag u ook niet naar binnen laten." Die dag testen onze collega's nog een aantal andere scenario's om onbevoegd binnen te dringen.

Dichtbij genoeg komen
Voor dag 2 hebben onze collega's een vergaderzaal gehuurd bij het bedrijf in hetzelfde pand. Opvallend is dat ze niet vooraf hoeven te betalen en ook geen legitimatie hoeven te laten zien. En wat blijkt? Als huurders kunnen zij gebruikmaken van dezelfde toiletruimtes als de medewerkers van onze opdrachtgever. En er zit maar een dun wandje tussen de vergaderruimte en de ruimtes van onze klant. Wat als een groep van 30 kwaadwillenden deze ruimte zou huren? Ze kunnen dichtbij genoeg komen om herrie te gaan schoppen.

Terugkoppeling van onze bevindingen
De opdrachtgever is onder de indruk van de bevindingen van onze inlooptests. Het doordringen van de buitenste schil (de campus) was echt té gemakkelijk. Daarnaast is het vooral een eye-opener dat er kwetsbaarheden ontstaan doordat de opdrachtgever het pand deelt met een ander bedrijf. En ook de opslag van de oude computers die mogelijk data zouden kunnen bevatten in de parkeergarage hadden ze niet eerder als een kwetsbaarheid gezien. Zo leverde de reis een hoop inzichten op waar onze opdrachtgever nu de juiste maatregelen voor in kan zetten. Iets wat zeker zo blijft, is het werken volgens het protocol. De hoofdbeveiliger van de vestiging verdient hiervoor absoluut een compliment.

Phishing - *Meten is weten*

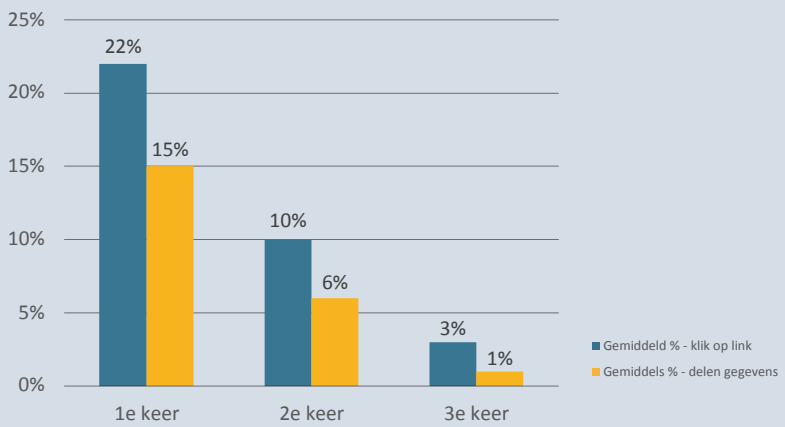


U heeft het vast vaker gehoord: binnen informatiebeveiliging is het gedrag van de mens vaak bepalend. Om uw medewerkers te misleiden gebruiken criminelen dan ook verschillende psychologische gedragstechnieken, bekend onder de term social engineering, een methode die in de praktijk meestal goed werkt. Dit komt doordat (cyber)criminelen inspelen op nieuwsgierigheid, behulpzaamheid of het vertrouwen dat mensen in elkaar hebben. Effectieve bescherming tegen social engineering vereist bewustwording, training en beveiligingsmaatregelen om medewerkers te helpen deze vorm van misleiding te herkennen en te voorkomen.

Door middel van social engineering kan een kwaadwillende toegang krijgen tot informatie als wachtwoorden, persoonlijke gegevens of gevoelige bedrijfsinformatie. Naast reputatieschade kan dit leiden tot een financieel verlies of verlies aan vertrouwelijke gegevens.

Een van de diensten die Hoffmann aanbiedt uit haar social engineering pakket is phishing. Phishing kan plaatsvinden in de vorm van een e-mail of direct 1-op-1 contact via de telefoon. Hoffmann heeft inmiddels jarenlange ervaring met het uitvoeren van verschillende phishing acties. Op basis van een eigen onderzoek naar het effect van deze acties kunnen we vaststellen dat herhaalde acties bijdragen aan verankering en verhoging van digitaal veiligheidsbewustzijn. Ons onderzoek laat zien dat over een periode van vier jaar het aantal personen dat op een link klinkt of gegevens zoals gebruikersnaam en wachtwoord verstrekt, na drie herhalingen spectaculair afneemt. De kracht van herhaling!

Resultaat phishing campagnes Hoffmann 2019 - 2023



In onze aanpak proberen we onze methode zo goed mogelijk af te stemmen op de situatie van de klant. Zo hebben we recent voor het eerst een phishing uitgevoerd via Teams, aangezien de medewerkers van deze organisatie veelvuldig contact met elkaar hebben via Teams. Uit voorlopige resultaten blijkt dat deze manier van phishing zeer succesvol is. Ruim 30% van de medewerkers die wij voor de eerste keer benaderden verstrekte zijn of haar gebruikersnaam en wachtwoord.

Met het uitvoeren van sociaal engineering activiteiten krijgt u dus meer inzicht in de mate waarin uw organisatie is beschermd. Ook krijgt u inzicht in de mate waarin uw medewerkers zich bewust zijn van de aanwezige risico's. Tegelijkertijd traint u met het uitvoeren van de activiteiten uw medewerkers en creëert u hierdoor bewustwording.

Specialist aan het woord: ***Isa***

Na haar master Forensische Criminologie werkte Isa eerst als Know Your Customer analist bij een bank. Op zoek naar meer afwisseling ging ze voor een baan als onderzoeker bij Hoffmann. Op de vraag of ze ook als Consultant Cybersecurity & Risk management aan de slag wilde, antwoordde ze bevestigend. Maar wat doe je dan eigenlijk precies? We vroegen het haar.

"Mijn werk bij Hoffmann is heel gevarieerd," trapt Isa enthousiast af. "Zo houd ik mij binnen onze preventieve tak onder meer bezig met risicoanalyses op het gebied van fysieke beveiliging en, sinds kort, fraude. Daarvoor voeren we analyses uit van documenten, maar gaan we ook fysiek langs bij organisaties, om zo te achterhalen waar de organisatie kwetsbaar is en welke aanvullende beheersmaatregelen moeten worden genomen."

Ook geeft Isa samen met haar collega's crisistrainingen en neemt zij deel aan Red Teaming oefeningen, waar zij vaak de voice phishing en inlooptests voor haar rekening neemt. Isa:"Dat zijn altijd hele leuke oefeningen. Maar als het lukt om ergens binnen te komen voelt dat soms ook wel dubbel. Rationeel weet je dat je iets goeds doet omdat je een kwetsbaarheid blootlegt, maar gevoelsmatig wringt het wel eens. Je kan mensen ook een rotgevoel geven omdat je misbruik maakt van hun behulpzaamheid. Zo ben ik, toen ik net terug was van zwangerschapsverlof, wel eens een beveiligde zone van een organisatie binnengekomen door tegen de receptioniste te zeggen dat ik moest kolven. Dit was voor ons echt de enige manier om binnen te komen, omdat dit bedrijf de procedures verder heel strikt volgde. Na afloop bekruipt je dan wel eens een gevoel van 'Ben ik niet te ver gegaan?'. Maar aan de andere kant, iemand die echt kwaad wil kan ook heel ver gaan."

Over de crisistrainingen die op pagina 10 worden uitgelegd zegt Isa: "Op dit moment geven we veel crisistrainingen die gericht zijn op ransomware aanvallen. Een actueel thema natuurlijk, en een scenario waar veel organisaties zich op willen voorbereiden. Wij maken tijdens deze training gebruik van verschillende scenario's, die we gedurende de training aanpassen zodat het team steeds weer wordt gedwongen om over nieuwe dingen na te denken. Wat we daarbij vaak zien is dat de dynamiek en rolverdeling binnen een team tijdens zo'n oefening anders is dan van tevoren gedacht. Zo nemen bijvoorbeeld andere personen dan de voorzitter de leiding. En ook de meest ervaren teamleden lopen altijd tegen nieuwe leer- en actiepunten aan. Dat is leuk om te zien, zo'n training zet iedereen weer even op scherp."

Heeft Isa geen spijt van de keuze die zij aan het begin heeft gemaakt? "Nee zeker niet. Mijn werk is heel afwisselend, en dat is ook wel wat ik nodig heb. Je bent hier nooit uitgeleerd en krijgt alle vrijheid om nieuwe dingen uit te proberen. Je hoeft je letterlijk nooit te vervelen.

Uit de oude doos

Kamerkrant — Automatisering — juni 1997 — 7

Fraude met computers neemt snel toe

De ontwikkeling in de automatisering raast maar door. Computergebruikers zijn elke dag weer meer te kunnen en sneller te werken. Maar zijn ze ook minder fraude-gevoelig? Neel Fraude in Nederland, waarvoor computercriminaliteit, loopt volgens schattingen in de miljarden. Vooral het bedrijfsleven is vaak het slachtoffer. Hoe herken je het en wat kun je er tegen doen?

Computercriminaliteit oftwel het plegen van fraude met een elektronisch hulpmiddel komt vaker voor dan menig ondernemer denkt. Beweert G. Hoffmann jr., directeur van Bedrijfsrecherche Hoffmann uit Amsterdam. 'Als ondernemers denken dat het hen niet zal overkomen, is de fraude in hun bedrijf een stap dichterbij gekomen.'

Landelijke cijfers omtrent de exacte omvang van computercriminaliteit bestaan niet. Toch blijkt het geen twijfel dat juist deze vorm van fraude de laatste jaren behoorlijk de kop is opgestoken. 'Ons bedrijf floreert als nooit tevoren, waarmee ik maar wil zeggen dat het aantal delicten in deze vorm snel toeneemt en het vaak om flinke bedragen gaat,' aldus Hoffmann. 'Slechts in een enkel geval draait het om hoogstaande technologische handelingen; meestal echter wordt de computer als modern hulpmiddel misbruikt, zoals vroeger het knoboek werd vervalst.'

Voorbeelden

Hoffmann onderscheidt bij de fraude-identificatie vier categorieën: goederen, geld, tijd en gegevens. 'De computerkassa in de detailhandel is wat betreft geld, nog steeds het meest aangrijpende voorbeeld. Zeker de vanuit-huis-die geen mutaties voorhouden en bijvoorbeeld de subtotalen niet registreren zijn fraude-gevoelig. Meestal adviseer ik een andere kassa te nemen of een niet-manipuleerbaar computerprogramma aan te schaffen. Duizelbe doe ik bij andere "klassieke" voorbeelden van geldfraude, zoals het prodiscreten of verzenden van facturen, maar het in de computerboekhouding doen verwijderen ervan.

Fraude waarbij goederen "zoekraken" is volgens Hoffmann ook een hot item. 'Vaak zijn er meerdere personen bij betrokken, zoals de verkoop-binnendienstmedewerker en een chauffeur. De eerstgenoemde voert een pakbon in, het magazijn verwerkt deze en de chauffeur levert af. De laatste ontvangt het bedrag cash, terwijl de binnendienstmedewerker de pakbon uit de administratie haalt.' 'Als de fraudeur solo werkt, heeft hij een duidelijke voorkeur voor klein spul met een hoge waarde. Vooral laptops en computerchips staan daarom hoog genoteerd op de lijst van verzinsie goederen.'

Ook declaraties waarbij gefraudeerd is met het in werkelijkheid gemaakte aantal uren ziet Hoffmann geregeld aan zich voorbijkomen. Evenals het "leveren" van bedrijfsgegevens aan de concurrent. Omdat steeds meer bedrijven werken met netwerksystemen, worden bedrijfsgeheimen voor teveel personeelsleden toegankelijk. De mogelijkheid om marketingplannen door te lekken of relatiebestanden te verkopen, is bijzonder eenvoudig geworden.'

Voorkomen

Om fraude met dit elektronische hulpmiddel te voorkomen, hanteert Hoffmann een vier-stappen model. 'Allereerst moet de ondernemer zich realiseren dat dit fenomeen bestaat en dat het hem ook kan treffen. Vervolgens doet hij er verstandig aan de diverse automatiseringssystemen in de onderneming door de ogen van een fraudeur te bekijken. Stap 3 is het niet langer meer blindelings vertrouwen van eigen personeel. Uit cijfers van onze fraude-onderzoeken blijkt dat 80% van de bedrijfsfraudeurs is aangenomen zonder dat er ooit kennis is ingewonnen over de betreffende medewerkers. Ook tonen gegevens aan dat in 47% van de gevallen de fraudeur tot de "sleuteldragers" behoorde. Kortom; ondernemers moeten eerst een zorgvuldige afweging maken, alvorens medewerkers op fraude-gevoelige plekken te plaatsen of in aanraking te laten komen met fraude-gevoelige apparatuur.'

De laatste stap in het voorkomen van bedrijfsfraude met computers is het realiseren van controle en toezicht. Hoffmann: 'Controleer daarom regelmatig alle computerdata. Nog verstandiger is reeds bij de aanschaf van nieuwe programmatuur de manipuleerbaarheid ervan mee te laten wegen bij de keuze voor het pakket. Want ook bij bedrijfsfraude is voorkomen beter dan genezen.'

Millennium en Euro kosten handen vol tijd en geld

Oplangs heeft de branche-organisatie van automatiseringsbedrijven de regering een brandbrief verstuurd. De opstellers maken hierin melding van een schrikbarend tekort aan computerprogrammeurs: een groep professionals die met het oog op het jaar 2000 én met het oog op de invoering van de Euro voor veel (MKB)bedrijven als reddende engel moeten gaan fungeren.

'Slechts een enkeling realiseert zich dat de verandering van 1999 in 2000 meer is dan het vervangen van de wijzers,' zegt M.Hendriks, organisatie-adviseur bij CMG (Computer Management Groupe). Hendriks legt uit: 'Vroeger waren computers duur. Daarom bespaarde men op capaciteit voor gebeurtenisopslag en werd er vaak in 2-digits gepro-grammeerd: computers lezen dan geen 1996, maar 66. Geen probleem dacht men, want de programmatuur zou snel evolueren. Maar tussentijds is lang niet alle programmatuur vervangen. Daarom zal menig computer 1 januari 2000 lezen als 1 januari 1900. Met alle gevolgen van dien.'

Vreug of laat krijgt ieder bedrijf volgens Hendriks met het probleem van de verandering van het millennium te maken. 'Als je een lease-maatschappij hebt en je hebt onlangs auto's geleverd met een contract voor 36 maanden, dan zal de computer deze auto's binnenkort al gaan terugroepen, omdat bij in plaats van 2000, namelijk 1900 "leest" en aangezien dat jaartal al eeuwen tijd achter ons ligt...'

Gewaarschuwd

Vooral bedrijven die met ontvangrijke netwerken opereren, worden door het jaar 2000 gecondroneerd met tijd-, en geldrovende operaties. Maar ook het MKB is gewaarschuwd. 'Zolang het om een kleine arbeidsmarkt gaat die met één PC werkt, is het leed waarschijnlijk snel te overzien. In dat geval, doet de ondernemer er verstandig aan eerst te kijken of bij de systeemdatum van zijn computer eigenlijk wel gebruikt. Gebruikt bij deze automatische tijd wel, bijvoorbeeld bij correspondentie, dan adviseer ik hem de systeemdatum van zijn computer, bij wijze van test, nu al op 31-12-1999 te zetten en af te wachten wat er gaat gebeuren. Geeft de computer vervolgens in-derdaad "1900" aan, dan is een telefoontje naar de leverancier van het softwarepakket de volgende stap. Deze kan je aanspreken voor een vervangend, millennium-bestendig, pakket. Ten minste als je beschikt over moderne software waarvoor een millennium-bestendige versie wordt gemaakt. Want laat één ding duidelijk zijn: lang niet alle programmatuur krijgt een 2000-versie!'

Hendriks vreest, op basis van bovenstaand verhaal, dat het volgende millennium ondernemers tijd en geld gaat kosten. 'De mate waarin hangt af van de omvang en de complexiteit van de automatisering én van de soft- en hardware, waarover de ondernemer beschikt. Bovendien mag het duidelijk zijn dat indien de organisatie over een deskundige beschikt, de kosten minder ontvangrijk zullen zijn, dan als die persoon er niet is.'

Euro

Indien een ondernemingen besluit externe hulp in te roepen, adviseert Hendriks meteen de invoering van de Euro in de automatisering mee te nemen. Deze staat gepland op 1 januari 1999, maar zal niet eerder verplicht worden gesteld dan het jaar 2002.

'Gelukkig is de invoering van de Euro, in tegenstelling tot de aanpassing van het jaar 2000, een minder defensieve klus. Maar ook bij de Euro geldt dat de mate waarin de ondernemer is geautomatiseerd uiteindelijk bepaalt hoeveel tijd en geld hij hieraan kwijt is. Aan de andere kant zal een ondernemer die handel drijft met het buitenland eerder voorzieningen moeten treffen dan een kleine zelfstandige die louter zaken doet in eigen land. Er zijn eenkomen kan echter niet, want iedere ondernemer factureert en werkt derhalve met geld. Daarom adviseer ik nu actie te ondernemen, vooraf het dreigende tekort aan gekwalificeerd personeel menig ondernemer in het jaar 2000, en waarschijnlijk al daarvoor, van laat kopen.

Computer- en informatiebeveiliging in apart paviljoen op Security '97

Steeds meer bedrijven wisselen digitaal informatie met elkaar uit. Ook het aantal internet-gebruikers heeft een hoge vlucht genomen. Wie zijn computer 'open stelt' voor anderen moet zorgen voor een goede beveiliging.

Tijdens de internationale beveiligingsbeurs 'Security '97', die van 30 september tot en met 3 oktober in de Jaarbeurs in Utrecht wordt gehouden, is een apart themapaviljoen ingericht over computer- en informatiebeveiliging. De bedrijven die er acte de présence geven zijn onder meer aanbieders van anti-virus producten, van vervangende computerfaciliteiten ('computer-uitwijk'), beveiligde netwerken en bedrijven die adviezen over computerbeveiliging.

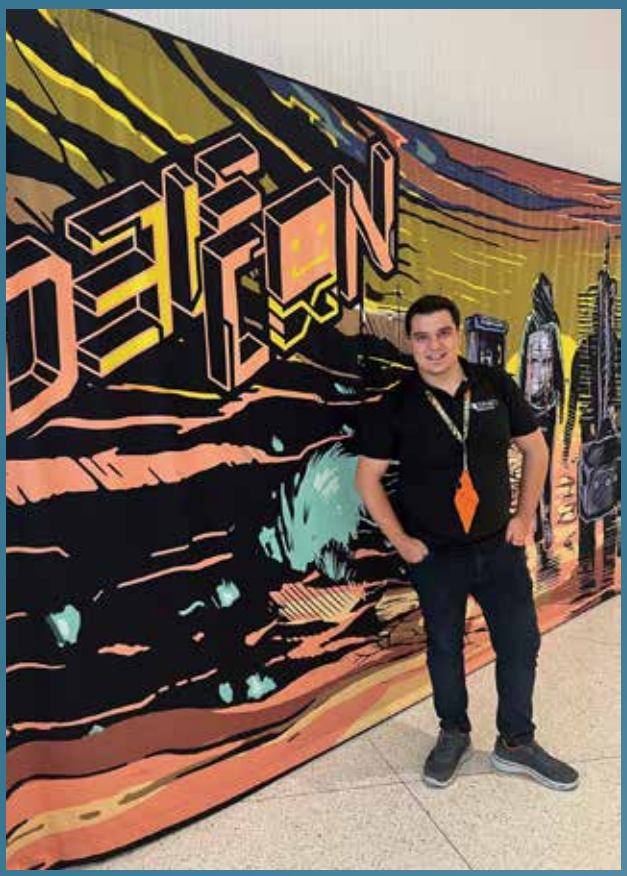
Dit krantenartikel is gepubliceerd in de 'kamerkrant' in juni 1997.

26 jaar geleden stond dit artikel in de krant. Onze toenmalige directeur Gert Hoffmann jr. in het artikel: "Als ondernemers denken dat het hen niet zal overkomen, is de fraude in hun bedrijf een stap dichterbij gekomen." Bijzonder dat die boodschap nog steeds zo actueel is, kijk maar naar de titel van deze Hoffmann Tips. De adviezen die we tegenwoordig aan onze klanten geven zijn uiteraard mee gegroeid in al die jaren. Daar staat deze Hoffmann Tips vol mee.

Hoffmann presenteert wederom op hackers-conferentie DEF CON in Las Vegas

Vorig jaar stond onze collega Utku Yildirim voor de eerste keer als spreker op 's werelds grootste hackers-conferentie DEF CON. En ook deze zomer schitterde hij op dit podium van alweer de 31e editie van het evenement. Het evenement bestaat uit lezingen, workshops, ontmoetingen en wedstrijden. De bezoekers en sprekers komen vanuit de hele wereld en het congres is naar verwachting door meer dan 5.000 geïnteresseerden bezocht.

Presentatie over de gevaren van 5G
Utku gaf in zijn presentatie een technisch overzicht van, hoe het op dit moment veelgebruikte en meest veilige telecommunicatieprotocol 5G, kan worden gedowngrade naar het minder veilige en meest kwetsbare 2G-protocol, waarna sms-berichten kunnen worden gestolen. En dat is een risico, want veel banken en overheidsinstanties versturen via sms gevoelige informatie naar gebruikers, zoals tweefactorauthenticatiecodes. Door deze potentiële beveiligingsproblemen uit te lichten in scenario's waarin bijvoorbeeld gevoelige gegevens en/of identiteitsinformatie in een sms-bericht worden gedeeld, wilde Utku het bewustzijn vergroten en beschermingsmethoden tegen dergelijke cyberaanvallen delen.



Over Utku
"Ik werk als ethical hacker en red teamer bij Hoffmann. Ik houd mij bezig met penetratietesten. Daarnaast heb ik ervaring op veel gebieden van cyberbeveiliging, waaronder Incident Response, Digital Forensics en Network Forensics. Ik zie cybersecurity niet alleen als een beroep, maar ook als een manier van leven. Ik ga graag uitdagingen aan in alle aspecten van mijn leven met behulp van de ervaring die ik heb opgedaan op het gebied van cybersecurity. Mijn onderzoek en ervaringen deel ik graag met andere cybersecurity-enthousiastelingen op internationale conferenties, waaronder dus twee keer op rij op DEF CON. In de toekomst blijf ik op (inter)-nationale conferenties werken aan het vergroten van de nationale en internationale erkenning van de positie en innovatieve methoden van Hoffmann. Als cybersecurity-onderzoeker is het een van mijn doelen om de potentiële positieve resultaten van mijn werk op huidige en opkomende gebieden zoals AI, cloudbeveiliging en autohacking te delen."

PS: wist u al dat Utku een van de Hoffmannspecialisten is die bij klanten een live hackdemo kan geven, zoals op pagina 3 staat beschreven van deze Hoffmann Tips?

Hoffmann

Vertrouwen is goed,

Hoffmann is beter

Over Hoffmann
Uw veiligheid, daar maken we ons sterk voor, al meer dan 60 jaar. Oplossingsgericht als het moet, dankzij onze doorgewinterde onderzoekers en adviseurs. Integer, objectief en altijd snel beschikbaar.

Fraude & Integriteit:
Fraude, diefstal, corruptie, sabotage; niemand wil dat, maar het gebeurt. In die gevallen rekent u direct op ons. Met ruim 60 jaar ervaring, onderzoeken we discreet en objectief wat er is gebeurd en proberen we de schade te beperken.

Grensoverschrijdend gedrag:
Onderzoek naar grensoverschrijdend gedrag op de werkvloer komt steeds vaker voor omdat melders durven op te staan. Met de mens als slachtoffer is een andere aanpak nodig en zo werken wij o.a. met psychologen tijdens het feitenonderzoek.

Cybersecurity:
Het is tegenwoordig niet meer de vraag of uw organisatie wordt gehackt maar wanneer. Onze experts helpen u om uw ICT-systemen te beschermen en uw medewerkers blijvend weerbaar te maken tegen een cyberaanval.

Risk management:
Hoffmann helpt bij inzicht verkrijgen in dreigingen en risico's, het advies over passende maatregelen en het testen ervan. U bent voorbereid op incidenten zoals fraude, bedreigingen en overige crisissituaties die uw kritieke processen verstoren.

Bezoekadres: Luidsprekerstraat 10, 1322 AX ALMERE
Postadres: Postbus 60090, 1320 AB ALMERE
Telefoon: 088 - 298 6600
info@hoffmann.nl - www.hoffmann.nl