KLIK HIER!

KVK

OKTOBER 2021

WEGWIJZER CYBER-SECURITY

6 tips Wat kun je doen tegen ransomware?

Hoe cyberveilig ben jij? Doe de quiz

Onderbroek op slot! En 4 andere bizarre hacks bij bedrijven

10 experts delen hun grootste blunders én gouden beveiligingstips

---

SLUIT JE AAN BIJ ONS CYBERNETWERK OP LINKEDIN

INCLUSIEF HANDIGE VEILIG ONLINE CHECKLIST

UITGELICHT

Geen ver-van-mijn-bed-show

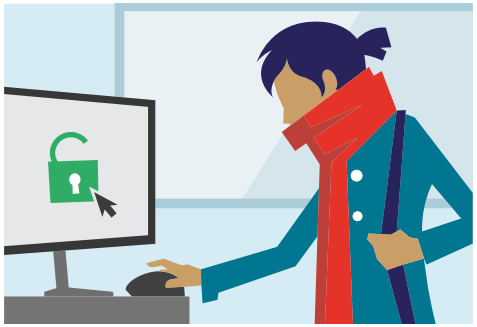
Informatiebeveiliging moet in 2021 bij elke onderneming onderdeel worden van de bedrijfsvoering. Jack van Diepen is het daar hartgrondig mee eens sinds zijn onderneming digitaal werd gegijzeld.

Ga naar artikel >

Cyberexperts aan het woord

We vroegen 10 experts naar hun grootste blunder, gouden tip en kijk op de securitytrends die zij signaleren. Voorkom met hun inzichten beveiligingsblunders in je eigen bedrijf.

Ga naar artikel >



Quiz: Hoe cyberveilig ben jij?

Bekijk hoe jij omgaat met deze situaties en ontdek hoe cyberveilig je bent.

Ga naar artikel >

Inhoud

Hoe vervelend ik het ook vind: cybercriminaliteit is aan de orde van de dag. Jaarlijks krijgt 1 op de 5 ondernemers – groot en klein – hiermee te maken. Jezelf daartegen beschermen is dus geen luxe, maar een must.

Voorwoord

WEERBAAR TEGEN CYBERCRIME

Nederlandse bedrijven krijgen per week gemiddeld 294 cyberaanvallen te verduren. De meeste aanvallen worden gelukkig afgeslagen, maar een 'geslaagde' aanval kost een getroffen bedrijf al gauw 67.000 euro! Jezelf hiertegen beter beschermen bespaart je dus een hoop geld en kopzorgen.

KVK doet er alles aan om ondernemers veilig zaken te laten doen. Dat betekent ook dat we je graag ondersteunen in het digitaal veiliger maken van jouw onderneming. Daarmee voorkom je mogelijk een hoop ellende en dat is in veel gevallen ook een stuk goedkoper en makkelijker dan achteraf repareren.

En weet dat je met een paar simpele maatregelen hackers vaak al buiten de deur houdt. Daarom ook dit magazine. Hier lees je tips en adviezen van experts. Daarmee maak je in principe in één uur je bedrijf al weerbaarder tegen cybercrime. Ook vertelt ondernemer Jack van Diepen hoe hij omging met de digitale gijzeling van zijn loonbedrijf. Betaal je bijvoorbeeld losgeld of niet?

Ik verwacht dat je na het lezen van dit magazine beter voorbereid bent op digitale bedreigingen. Want je moet er niet aan denken dat een hacker ook jouw zaak op slot zet. Laten we er samen voor zorgen dat cyberveiligheid straks net zo vanzelfsprekend is als een goed slot op je winkel of kantoorpand.

Greet Prins
Voorzitter Raad van Bestuur KVK

6 tips WAT KUN JE DOEN TEGEN RANSOMWARE?

Er gaat geen week voorbij zonder nieuws over ransomware-aanvallen. Ook als klein bedrijf ben je kwetsbaar voor zo'n aanval. Goed nieuws: je kunt actie ondernemen om jezelf te beschermen.

Bad Rabbit, Spider, GoldenEye: ze klinken als spannende actiefilms, maar het zijn gevaarlijke softwareprogramma's, bedoeld om geld van bedrijven te stelen. We hebben het over ransomware. Goed nieuws: volgens het Britse securitybedrijf Sophos zijn in januari en februari 2021 minder organisaties aangevallen met ransomware dan een jaar eerder: 37% in plaats van 51%. Slecht nieuws: de financiële schade door een ransomware-aanval verdubbelde wereldwijd. Gemiddeld is de schade door 1 aanval zo'n 1,5 miljoen euro.

Wat is ransomware?

Ransomware is schadelijke software, of malware, die computers en bestanden gijzelt. Vandaar de Nederlandse naam 'gijzelsoftware'. Criminelen blokkeren of versleutelen je computers, bestanden, soms zelfs hele netwerken en geven die pas weer vrij als je losgeld betaalt. Volgens experts is dubbele versleuteling in opkomst: de ransomware versleutelt je data dan niet 1 keer, maar 2 keer. Voor beide sleutels moet je betalen.

Bestanden gegijzeld

Een aanval kan op meerdere manieren verlopen. Via links, via bijlages in e-mail, advertenties, maar ook via gerichte aanvallen op servers proberen criminelen de software een systeem binnen te loodsen. Is de ransomware eenmaal binnen, dan kan het zichzelf verspreiden. De software blokkeert dan de toegang tot je computer of netwerk, of versleutelt bestanden. In een pop-up eisen de criminelen achter de aanval betaling, vaak in bitcoin of een andere cryptovaluta.

Wat kun je doen bij een ransomware aanval?

Wat moet je doen als je bent aangevallen? Neem natuurlijk contact met je IT-beheerder, als je die hebt. En verder kun je het volgende doen:

Onderzoek om welke ransomware het gaat

Van oudere software is soms de decryptiesleutel bekend, waarmee je bestanden weer kunt worden ontsleutelen. Op nomoreransom.org, een internationaal samenwerkingsverband tussen beveiligingsbedrijven en politie, kun je dat controleren. Ransomware verwijderen is een vak apart, dus het is slim om daarbij hulp in te roepen van een expert.

Betaal geen losgeld

Dat is natuurlijk makkelijk gezegd en er zijn bedrijven die geen andere optie hebben. In januari en februari 2021 betaalde 32% van organisaties wereldwijd losgeld na een aanval met kwaadaardige software. Vaak is het trouwens een verzekeraar die het losgeld betaalt. Maar alleen als er iets te halen valt, blijft deze vorm van criminaliteit bestaan. De Nederlandse politie adviseert dan ook bij ransomware: betaal niet. Doe wel aangifte. En meld de aanval ook bij de Fraudehelpdesk.

Zorg voor goede antivirusprogramma's

Het is een open deur, maar alleen met goede virusscanners die ook ransomware herkennen, ben je goed beschermd. Van de Nederlandse bedrijven die begin 2021 werden aangevallen, wist bijna een kwart de aanval te verijdelen voordat er bestanden waren versleuteld.

Bad Rabbit en GoldenEye klinken als spannende actiefilms, maar het zijn gevaarlijke softwareprogramma's.

Beveiliging tegen ransomware

Het is natuurlijk beter om cybercriminelen een stap voor te blijven. Dit kun jij als ondernemer doen tegen gijzelsoftware.

Investeer in back-ups

Een back-up, vooral als je die op een externe plek bewaart, is een goede beveiliging. Want zo hoef je niet eens te overwegen om losgeld te betalen voor je gegevens. Uit het eerder genoemde onderzoek van Sophos bleek dat wereldwijd 57% van aangevallen organisaties hun data uiteindelijk terugkregen via hun eigen back-ups.

Update je software

Cybercriminelen gebruiken zwakke plekken in software om je systeem met ransomware binnen te dringen. Zorg dat je kwetsbaarheden op tijd repareert en update dus altijd de software die je gebruikt.

Blijf opletten!

Experts waarschuwen: mensen zijn een zwakke schakel in de beveiliging van data. Op een link is zo geklikt, een bijlage is zo geopend: wees daar dus voorzichtig mee. Wantrouw mails van onbekenden, en zorg ook dat eventuele medewerkers geen privémail ontvangen via het zakelijke mailadres.

Je staat er niet alleen voor

- De Fraudehelpdesk kan je bij een aanval adviseren en eventueel doorverwijzen.
- Het Digital Trust Center (DTC), opgericht door het ministerie van Economische Zaken en Klimaat, geeft je nadere uitleg over wat je kan doen als je computer-systeem door software gegijzeld is.
- Het Nationaal Cyber Security Center (NCSC), opgericht door het ministerie van Justitie en Veiligheid, bestrijdt cybercrime in Nederland. Het NCSC publiceert regelmatig over het voorkomen van cybercrime.

Wereldwijd betaalde 32% van organisaties losgeld na een aanval met ransomware.

Ransomware in cijfers

Het Britse securitybedrijf Sophos doet elk jaar een groot onderzoek naar ransomware. 150 Nederlandse bedrijven en organisaties deden mee aan het onderzoek. Dit zijn opvallende resultaten uit het onderzoek van 2021.

- 32% van de 150 Nederlandse organisaties die meededen aan het onderzoek zijn in 2021 aangevallen met ransomware. Dit percentage ligt dichtbij het wereldwijde gemiddelde van 37%. Bedrijven in retail worden het vaakst getroffen.
- Het land met de meeste ransomware-aanvallen is India. 68% van Indiase bedrijven meldde een aanval met ransomware, voornamelijk door Indiase cybercriminelen. Het land met de minste aanvallen is Polen, waar 13% van de organisaties werd aangevallen.
- Het gemiddelde bedrag dat Nederlandse organisaties volgens dit onderzoek aan ransomware kwijt zijn, is hoger dan het wereldwijde gemiddelde. De 48 Nederlandse organisaties die een aanval meldden, betaalden in 2021 gemiddeld 2,3 miljoen euro aan kosten per bedrijf.

20.000 FLOPPY'S: HET BIZARRE ONTSTAAN VAN RANSOMWARE

Het is 1989 en de hele wereld is in de ban van het nieuwe AIDS-virus. De Amerikaanse bioloog Joseph Popp, afgestudeerd aan de universiteit Harvard, doet onderzoek naar de mysterieuze ziekte. In december 1989 verstuurt hij 20.000 floppy-disks naar wetenschappers in 90 landen. Een gigantische logistieke klus. Op de floppy's: een interactieve enquête om te bepalen of mensen aan AIDS lijden.

Scherm op rood

Maar de enquête is hartstikke nep. Wie de floppy in de computer stopt en de inhoud downloadt, infecteert ongemerkt zijn computer. Na de 90ste keer opstarten worden alle bestanden versleuteld, en verschijnt in het rood de boodschap: "Beste klant, het is tijd om uw softwarelicentie te betalen." Afzender: PC CYBORG CORPORATION. Alleen wie een cheque van 189 dollar verstuurt naar een postbus in Panama, krijgt de sleutel tot de vergrendelde bestanden. De bioloog Popp verspreidde zo de allereerste ransomware.

Condooms en krulspelden

Gelukkig bleek Popp niet zo'n goede hacker. Securityexperts komen er snel achter dat de versleuteling van zijn ransomware makkelijk te kraken is. De FBI arresteert Popp een paar weken later en hij verschijnt voor Britse rechter wegens chantage. De rechtszaak verloopt niet bepaald soepel. Nadat Popp condooms op zijn neus zet en krulspelden in zijn baard doet om gevaarlijke straling af te weren, verklaart de rechter hem in 1991 ontoerekeningsvatbaar.

Vlindertuin

Joseph Popp wordt dus nooit berecht. Hij vertrekt naar oostelijk Afrika om bavianen te onderzoeken, en opent later in New York een vlindertuin. Toch blijft hij vooral bekend als het brein achter de allereerste ransomware-aanval ter wereld. 30 jaar later plukken cybercriminelen wereldwijd de vruchten van zijn 'onderzoek'. Anno 2021 houdt ransomware bedrijven wereldwijd in zijn greep.

HOE HERKEN JE PHISHING-MAILS?

Ransomware komt niet zomaar op je netwerk. Vaak gebruiken cybercriminelen phishing om toegang tot je netwerk te krijgen en de malware te verspreiden. Hoe herken je zo'n phishingmail?

Je hebt er vast wel eens een gekregen: een phishingbericht. Een nepbericht via e-mail, sms of WhatsApp dat van een kennis of betrouwbare partij lijkt te komen, maar waar iets mee aan de hand is. Als je op het linkje klikt, geef je criminelen onbedoeld toegang tot je systeem, of tot persoonlijke informatie.

Het is vaak lastig om het verschil te zien tussen een valse en echte e-mail. Je herkent een phishingmail aan de volgende kenmerken:

> Wees alert op phishing (KVK.nl)

CHECKLIST VEILIG ONLINE

Om veilig online te ondernemen moet je tijd investeren in je cyberveiligheid. Maar waar begin je? In deze checklist staat wat je minimaal zou moeten doen om cybercriminelen zoveel mogelijk buiten de deur te houden. Hoeveel punten kun jij al afvinken?

1. Gebruik veilige wachtwoorden en/of een wachtwoordmanager.
2. Gebruik een veilige internetverbinding.
3. Wees alert op phishing-mails en -telefoontjes.
4. Voer software-updates uit.
5. Deel gevoelige gegevens versleuteld.
6. Pas waar mogelijk tweestapsverificatie toe.
7. Gebruik antivirussoftware.
8. Maak back-ups en test deze.
9. Kies kritisch welke software je downloadt.
10. Kom je er zelf niet uit? Vraag hulp aan je IT-dienstverlener of een cyberveiligheidsexpert.

CYBERCRIMINALITEIT IS GEEN VER-VAN-MIJN-BED-SHOW

Internetcriminelen worden steeds slimmer. Informatiebeveiliging moet daarom bij elke onderneming onderdeel worden van de bedrijfsvoering, zeggen beveiligingsexperts. Jack van Diepen van Loonbedrijf Van Diepen is het daar hartgrondig mee eens sinds zijn onderneming digitaal werd gegijzeld.

Cybercriminaliteit, gijzelsoftware: iedereen heeft er wel eens van gehoord. Maar vooral kleinere ondernemers denken dat het hen niet zal overkomen. Volgens beveiligingsexperts is dat een misverstand. Internetcriminelen weten vaak niet eens met wat voor bedrijf ze te maken hebben. Ze kijken vooral hoe makkelijk ze ergens kunnen binnenkomen. En dan is losgeld vragen de volgende stap.

Niets werkte

“Misschien is de stroom er even af geweest”, dacht Jack van Diepen toen hij vorig jaar de hoofdpoort van zijn bedrijfsterrein niet kon openen. Die poort (en alle buitendeuren van zijn pand) werkt met sleutel-tags die via wifi-verbinding maken met de bedrijfscomputer. En geen enkele reageerde. Toen kwamen de telefoontjes van zijn werknemers. “Verschillende mannen waren al met machines op pad en hadden storingen. Bij de ene werkte de gps niet meer, bij een ander deed het egalisatieprogramma het niet. Alle tractoren, kranen en andere machines werken met data en alles wat ze doen, wordt geregistreerd. Al die data bewaren we in de cloud en niets werkte meer.”

Worm losgelaten

Van Diepen belde direct zijn ICT-leverancier, die hem adviseerde alles uit te schakelen en de verbindingen met internet te verbreken. “Ze kwamen meteen langs en binnen een paar uur kreeg ik de mededeling dat het foute boel was.” Internetcriminelen waren ’s nachts 5 keer in zijn cloud geweest en hadden daar een ‘worm’ achtergelaten die alle gegevens was gaan versleutelen. Tegen de tijd dat Van Diepen er iets van merkte, was het hele systeem al aangetast.

Bitcoins

Al snel na het ontdekken van de inbraak kreeg Van Diepen een verzoek om losgeld te betalen. Daarna zou hij zijn bestanden weer in kunnen. “Ik moest 3.800 euro aan bitcoins kopen en overmaken”, vertelt hij. “Mijn ICT-leverancier raadde het af en ik zag het zelf ook niet zitten. Ik ben eens bij een cyber-evenement geweest en hoorde daar iemand spreken die hetzelfde was overkomen. Die had flink betaald maar uiteindelijk toch niet alles teruggekregen. Ik wilde er ook niet aan meewerken, dat gaat tegen mijn principes in. Bovendien had ik geen vertrouwen dat het goed zou komen. Want ja, het blijven toch criminelen.” Van Diepen heeft wel aangifte gedaan bij de politie.

Zonder moraal

2 medewerkers van zijn ICT-leverancier zijn 2 weken bezig geweest om alles terug te sleutelen. Ook ’s nachts bleven er programma’s draaien om gegevens terug te vinden.

“Wat valt er nou te halen bij een loon-bedrijf? Maar daar gaat het niet om, ze proberen het gewoon.”

“Uiteindelijk hebben we 85% teruggekregen, daar kan ik mee leven. Achteraf had ik wel eens een moment dat ik dacht: als ik had betaald, was ik er misschien in één keer mee klaar geweest. Het hele proces heeft me een hoop ellende gebracht en meer gekost dan het afpersbedrag. Zo moest ik bijvoorbeeld een egalisatieprogramma opnieuw aanschaffen. Gelukkig tegen een gereduceerde prijs, dat was heel aardig, maar het was nog een flinke uitgave.” Toch heeft Van Diepen er geen spijt van. “Als je losgeld betaalt, stap je in een wereld zonder moraal. Daar doe ik niet aan mee.”

Slimmer en beter

Hoe de criminelen zijn systeem zijn binnengekomen, is Van Diepen niet helemaal duidelijk geworden. “De beveiliging was niet op orde, dat blijkt. Ik had dat overgelaten aan mijn ICT-leverancier. Ik dacht dat alle poorten dicht genoeg zaten, maar die internetcriminelen worden steeds slimmer en beter. En je wilt je systeem ook niet te ingewikkeld maken, want dat maakt het lastig werken. Het is steeds een afweging.”

Inmiddels is zijn systeem een stuk veiliger, vertelt hij. “We hebben beeldschermbeveiliging. Dus als ik achter mijn computer wegloop, schakelt die zich na 2 minuten uit. Ook zitten er sloten op de deuren in het kantoor, dus je loopt niet zomaar binnen om iets te doen. Iedere maand wordt de beveiliging geüpdatet en mijn ICT-leverancier kijkt dagelijks of er een poging is gedaan om binnen te komen.”

Ver van mijn bed

Van Diepen heeft er van geleerd. “Voorheen dacht ik altijd dat cybercriminaliteit een ver-van-mijn-bed-show was. Wat valt er nou te halen bij een loonbedrijf? Ik kan niet zomaar grote sommen geld contant maken of zoiets. Maar daar gaat het niet om. Ze proberen het gewoon. Ik zorg er nu wel voor dat de beveiliging op orde blijft.” Van Diepen adviseert ondernemers er rekening mee te houden dat het iedereen kan overkomen: “Neem dat standaard mee als kostenplaatje in je bedrijfsvoering.”

En hij waarschuwt ondernemers over thuiswerken. “Overal maar kunnen inloggen is fantastisch, maar pas op voor lekken. Via de wifi verspreidt die software zo van de één naar de ander.” Wat betreft beveiliging doet Van Diepen alleen zaken met professionele bedrijven. “Met een pand en een brievenbus. Ook je beveiligingscamera’s en de digitale sloten op de deur werken via wifi. Als daar dan iets misgaat, heb je een aanspreekpunt Iemand die de ernst van de situatie snapt en die het voor je oplost.”

Rooskleurig

Inmiddels is de rust weergekeerd en ziet Van Diepen de toekomst rooskleurig in. “De opvolging in ons bedrijf is in gang gezet, met mijn zoon en de zoon van mijn broer. En onze machines gaan steeds meer met data werken, zeker nu de landbouw aan steeds meer regeltjes moet voldoen. Voor een enkele boer zal dat lastig zijn, maar als professioneel bedrijf kunnen wij daar goed op anticiperen. Dus ik zie het positief in.”

> “Als je losgeld betaalt, stap je in een wereld zonder moraal. Daar doe ik niet aan mee.”

Jack van Diepen
Mede-eigenaar Loonbedrijf Van Diepen

Loonbedrijf J.S. Van Diepen werd in 1965 opgericht door de vader van Jack. Hij begon ooit bij een collega-loonbedrijf op de tractor maar werkt sinds 1982 in het bedrijf. In de loop van de tijd zijn het machinepark en het personeelsbestand fors uitgebreid.

Je zaak ook online beveiligen?

Check onze tips tijdens de KVK Live Adviesdagen

Meld je aan voor de workshops via KVK.nl/adviesdagen

met onder andere:

- Veilig online ondernemen, waar begin je?
- Hoe overleef je een cyberaanval?

KVK LIVE ADVIESDAGEN

Online ondernemen

CYBERCRIME IN HET MKB: VEEL SLACHTOFFERS, WEINIG MAATREGELEN

Meer dan de helft van het bedrijfsleven doet geen aangifte van cybercrime. En bedrijven nemen onvoldoende maatregelen om zich te beschermen tegen digitale fraude. Dat zijn de belangrijkste uitkomsten van het Cybersecurity onderzoek Veilig Online 2021 dat I&O Research uitvoerde in opdracht van het ministerie van Economische Zaken en Klimaat (EZK).

Cybercriminaliteit is een plaag voor bedrijven. Bijna dagelijks ontvangen ondernemers nepmails en links naar nepwebsites. Ze hebben te maken met DDoS-aanvallen waarbij cybercriminelen een bedrijfswebsite of webshop platleggen. Daarnaast gebruiken criminelen ransomware om je computers, bestanden of netwerk te blokkeren of versleutelen. Ze geven die pas weer vrij als je betaalt. Ook kan een fraudeur op social media doen alsof hij voor je bedrijf werkt en zo je klanten misleiden, een vorm van zakelijke identiteitsfraude.

Deze gegevens komen uit het Cybersecurity onderzoek Veilig Online 2021, deelrapport bedrijfsleven. Dit deelrapport behandelt de resultaten van medewerkers en ICT-verantwoordelijken in het bedrijfsleven. Medewerkers worden in het rapport uitgesplitst naar klein mkb, groot mkb en grootbedrijf. Ook is er uitsplitsing naar medewerkers werkzaam in de vitale infrastructuur en niet-vitale infrastructuur. In de duiding wordt ingezoomd op de resultaten van het mkb.
Het volledige onderzoeksrapport vind je op de website van Alert online.

- *Klein mkb: 1 - 9 werknemers*
- *Groot mkb: 10 - 199 werknemers*
- *Grootbedrijf: 200+ werknemers*
- *Vitale infrastructuur: producten, diensten en onderliggende processen die van essentieel belang zijn voor het dagelijkse leven van de meeste mensen in Nederland, zoals toegang tot drinkwater, elektriciteit, internet en betalingsverkeer.*

Vormen van cybercrime

Het ministerie van EZK onderzocht welke vormen van cybercriminaliteit het meest voorkomen in het bedrijfsleven. De phishingmail staat met stip op 1. Ruim een kwart van de medewerkers binnen het klein en groot mkb heeft in de afgelopen 12 maanden valse e-mails ontvangen. Binnen het grootbedrijf ligt dit percentage nog iets hoger. Op plek 2 staat acquisitiefraude. Bij deze vorm van fraude benaderen onbetrouwbare advertentiebureaus je telefonisch of via e-mail voor het plaatsen van advertenties in tijdschriften, bedrijfsgidsen of op websites. Het zijn advertenties waar je voor betaalt maar die niet of nauwelijks geplaatst worden. Van de medewerkers werkzaam binnen het klein mkb heeft 13% het afgelopen jaar te maken gehad met acquisitiefraude. 3% van de bedrijven werd het afgelopen jaar slachtoffer van ransomware.

Sluit je aan bij ons Cybernetwerk op LinkedIn

Heeft u in de afgelopen 12 maanden zelf weleens te maken gehad met een van de onderstaande voorvallen in uw werksituatie?	ICT	Medewerkers				
	Totaal n=525	Totaal n=1.066	Klein mkb n=103	Groot mkb n=359	Groot-bedrijf n=604	Vitaal n=159
Phishingmail ontvangen	51%	26%	26%	25%	29%	27%
Acquisitiefraude	28%	10%	13%	10%	7%	7%
Benaderd op social media met een vraag om een onbekende link aan te klikken	21%	8%	6%	8%	9%	14%
Benaderd met een onechte uitnodiging op sociale media voor zakelijk gebruik	22%	7%	5%	7%	8%	7%
Een foute link ook daadwerkelijk aangeklikt	6%	3%	3%	4%	3%	2%
Website werkte tijdelijk niet (bijv. door DDoS-aanval)	6%	3%	1%	3%	4%	4%
Computer werkte tijdelijk niet door malware	3%	3%	1%	3%	3%	5%
Ransomware	3%	3%	2%	3%	4%	5%
Malware verspreid door downloaden geïnfecteerde software/ bestanden	5%	2%	2%	2%	3%	3%
Bestanden geopend/gegevens ingevuld n.a.v. een phishingbericht	4%	2%	0%	2%	1%	0%
Benaderd voor WhatsAppfraude	4%	2%	2%	2%	3%	6%
Identiteitsdiefstal	3%	2%	1%	3%	1%	4%
Iemand logde zonder toestemming bij een apparaat in	1%	2%	2%	3%	2%	3%
Iemand logde zonder toestemming bij een account in	3%	1%	0%	2%	1%	2%

Melden cybercriminaliteit

Opvallend is dat de helft van de medewerkers binnen het bedrijfsleven geen melding doet van cybercrime. Circa een derde meldt incidenten bij de eigen ICT-afdeling. 9% meldt de cybercriminaliteit bij de Fraudehelpdesk, 4% doet aangifte en 3% maakt een melding bij de politie. Toch is aangifte doen een belangrijke stap in het bestrijden van cybercrime. Door aangifte te doen laat je de politie weten dat je slachtoffer bent van een misdrijf. Die kan dan de situatie in de gaten houden, een onderzoek starten naar het strafbare feit en mogelijk de dader opsporen. Daarnaast heb je meer kans op schadevergoeding als je aangifte doet.

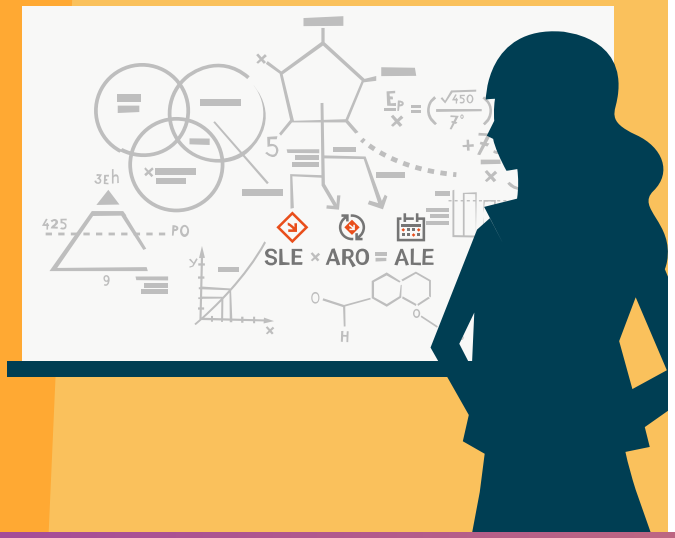
Voorkomen cybercrime

Ook voor cybercriminaliteit geldt: voorkomen is beter dan genezen. Aan medewerkers is gevraagd welke maatregelen er in hun bedrijf zijn genomen om digitaal veilig te ondernemen. Bijna een kwart (23%) geeft aan dat er geen maatregelen zijn genomen in hun bedrijf. Als er wel acties zijn genomen, dan lopen die sterk uiteen. De meest voorkomende maatregel is dat medewerkers zelf geen software kunnen installeren maar dat alleen de systeembeheerder van het bedrijf dit kan. Ook maken veel bedrijven afspraken over het gebruik van websites en/of e-mail. Denk hierbij aan het herkennen van valse websiteadressen en het alert zijn op phishingmails. Een derde (33%) van de medewerkers in het klein mkb weet niet of de werkgever actie heeft genomen rondom digitale veiligheid.

Welke acties zijn er binnen uw bedrijf/ organisatie ondernomen ten behoeve van online veilig gedrag?	ICT	Medewerkers				
	Totaal n=525	Totaal n=1.066	Klein mkb n=103	Groot mkb n=359	Groot-bedrijf n=604	Vitaal n=159
Alleen systeembeheerders kunnen software installeren	46%	41%	22%	40%	54%	50%
Afspraken over het gebruik van websites en/of e-mail	50%	37%	16%	35%	53%	52%
Afspraken over het versturen/uitwisselen van bestanden	43%	32%	16%	29%	47%	47%
Afspraken over hoe je veilig online thuiswerkt	41%	31%	13%	28%	48%	47%
Afspraken over het versturen/uitwisselen van persoonsgegevens	49%	30%	19%	26%	46%	48%
Afspraken over gebruik zakelijke smartphones, laptops en/of tablets	42%	29%	8%	26%	49%	27%
Afspraken over gebruikmaken opslagmedia als usb-sticks of externe harde schijven	35%	27%	9%	25%	41%	45%
Afspraken over gebruik van sociale media	34%	23%	10%	19%	39%	41%
Toegang geblokkeerd tot bepaalde websites of sociale media	25%	22%	8%	18%	42%	38%
Toegang geblokkeerd tot bepaalde verzendplatforms (zoals WeTransfer)	13%	11%	5%	8%	24%	22%
Het gebruik van USB-sticks in onze organisatie is onmogelijk gemaakt	9%	10%	5%	9%	18%	17%
Geen enkele actie ten behoeve van veilig online gedrag	8%	8%	23%	7%	2%	4%
Weet ik niet	8%	27%	33%	30%	20%	22%

Blunders en tips

10 CYBER-EXPERTS AAN HET WOORD



We vroegen 10 experts naar hun grootste blunder, gouden tip en kijk op de securitytrends die zij signaleren. Voorkom met hun inzichten beveiligingsblunders in je eigen bedrijf.

1. Tanya Wijngaarde, woordvoerder bij Fraudehelpdesk

Wat is je gouden tip voor ondernemers?

"Iedereen is interessant voor criminelen. Vooral kleine ondernemers denken vaak dat zij geen interessant doelwit zijn omdat er in hun bedrijf niet veel te halen is wat voor anderen aantrekkelijk kan zijn. Dat is een misvatting: alle ondernemers zijn een potentieel doelwit. Dat geldt ook als je alleen kippenvoer verkoopt of zzp'er bent. Maak daarom in elk geval regelmatig van al je gegevens een back-up op een externe harde schijf. Als je dan wordt getroffen door gijzelsoftware, een eng virus of wat dan ook, ben je niet meteen alles kwijt en hoef je ook geen criminelen te betalen."

Welke securitytrend vind jij dit jaar het opvallendst?

"Wat bij de Fraudehelpdesk het meest opvalt is dat oplichters over steeds meer informatie beschikken voordat ze hun grote slag slaan. Ze ontfutselen bijvoorbeeld eerst de inloggegevens van je bankaccount via een phishinglink en bellen je daarna op als 'bankmedewerker' die inderdaad van alles weet over je recente transacties. Met al die persoonlijke informatie komen oplichters betrouwbaar en overtuigend over. Mensen geven dan sneller hun gevoelige informatie weg."

2. Henk van Ee, docent en onderzoeker bij Information Security Expert Saxion Hogeschool

Wat is je grootste security blunder?

"Ik had een awareness training georganiseerd bij een security consultancy bedrijf en binnen no time hadden de deelnemers de tablet die ik bij me had met een wachtwoord-sterktemeter erop gehackt. Het was een oud apparaat, dus extra belangrijk om security updates te draaien. Wat een plezier hadden de ethisch hackers toen ze me daarop wezen. Tja, en gelijk hadden ze!"

Wat is je gouden tip voor ondernemers?

"Voel je vooral niet dom als het aankomt op cybersecurity. Veel mensen worstelen met de zogenaamde eenvoudige maatregelen. Veel voorlichtingscampagnes geven altijd zogenaamd 'makkelijke tips' om 'snel en in een handomdraai' veiliger te zijn. Maar het installeren van een wachtwoord-manager is voor een gemiddelde ondernemer helemaal niet makkelijk. Laat een mbo ICT-student eens stage lopen binnen je organisatie om je te helpen met dit soort maat-regelen."

“Ooit gebruikte ik overal hetzelfde wachtwoord voor”

3. Joris den Bruinen, directeur-bestuurder van stichting The Hague Security Delta

Wat is je grootste securityblunder?

“Ik had mijn laptop niet afgesloten en ben even van mijn werkplek gegaan. Op dat moment hadden wij een stagiair die bezig was met cyber awareness bij ons intern en zij heeft vanuit mijn naam een mailtje gestuurd naar hele kantoor waarin stond dat ik de dag erna zou trakteren op taart. Cleandesk, vernietigen van papier met gevoelige gegevens, de computer en laptop afsluiten en foute mailtjes met phisinglinkjes herkennen hoort allemaal ook bij data-beveiliging. Vanaf dat moment geef ik het goede voorbeeld in mijn eigen gedrag.”

Welke securitytrend vind jij dit jaar het opvallendst?

“De hoeveelheid aan ransomware-aanvallen, waarbij de bestanden versleuteld en tegen betaling vrijgegeven worden door de cybercriminelen. En dat dit willekeurig gebeurt bij degene die z’n digitale beveiliging niet op orde heeft. Het treft daarmee ook veel mkb’ers.”

4. Petra Oldengarm, directeur bij Cyberveilig Nederland

Wat is je grootste securityblunder?

“Ik heb wel eens een mailtje aan naar de verkeerde persoon gestuurd. Het algoritme van m’n e-mailprogramma ‘hielp’ me, door de naam van een ontvanger voor te stellen. Gelukkig stond er niets vertrouwelijks in, maar het was toch wel ongemakkelijk. Als ik nu een gevoelige mail stuur, controleer ik extra goed of ik de juiste geadresseerde heb ingevuld.”

Wat is je gouden tip voor ondernemers?

“Een redelijk simpele tip voor zelfstandigen of mkb’ers: versleutel de harde schijf van je laptop. Dat kan tijdens het installeren, maar ook achteraf. Het is een kwestie van een vinkje zetten en een ingewikkeld wachtwoord kiezen. Op die manier ligt je data niet op straat als iemand je laptop steelt en de harde schijf eruit haalt. Het wachtwoord moet je natuurlijk niet vergeten, daarvoor gebruik je een wachtwoordmanager.”

5. Henk Schippers, digitaal specialist bij Schippers IT

Wat is je grootste securityblunder?

“Dat ik ooit overal steeds hetzelfde wachtwoord gebruikte. Tegenwoordig gebruik ik een zogeheten keypass met voor iedere site een ander wachtwoord.”

Wat is je gouden tip voor ondernemers?

“Laat je online veiligheid regelmatig checken door andere bedrijven dan de eigen IT-afdeling.”

6. Dim Gerssen, manager bij securitybedrijf Surelock

Wat is je grootste securityblunder?

“Ik heb het geluk dat mij nog nooit iets ‘ergs’ is overkomen op digitaal gebied. Wel moet ik zeggen, met de kennis van nu, dat mijn wachtwoorden uit het verleden niet zo heel goed waren. Ik gebruikte eigenlijk overal hetzelfde zwakke wachtwoord. Gelukkig heeft dat geen grote gevolgen gehad.”

Wat is je gouden tip voor ondernemers?

“Vergeet je medewerkers niet. Medewerkers vormen een essentieel onderdeel van je beveiliging. Technisch gezien kun je een hoop dicht timmeren, maar als een medewerker gephisht wordt of een malafide USB-stick in een computer steekt, kan het alsnog fout aflopen.”

7. Jan Los, eigenaar van Aurio ICT

Wat is je gouden tip voor ondernemers?

"Neem alle meldingen die je over veiligheid krijgt serieus totdat het tegendeel is bewezen. Ik kom regelmatig data-lekken of kwetsbare systemen tegen online. Als ik mensen daarvoor waarschuw, krijg ik vaak geen reactie. Maar als je niks doet met een waarschuwing, blijft de data beschikbaar of het systeem kwetsbaar."

Welke securitytrend vind jij dit jaar het opvallendst?

"Eentonig waarschijnlijk: de explosie van ransomware. Aan de ene kant verbaast het me niet, want het is voor criminelen een geweldig verdienmodel. Maar het wordt nu echt een plaag voor het mkb. Ondernemers hebben zwaardere maatregelen nodig terwijl ze daar niet aan toe zijn of geen geld aan uit willen geven. En helaas: 'We doen alles in de cloud' is geen Haarlemmerolie."

8. Sanne Maasakkers, ethisch hacker

Wat is je gouden tip voor ondernemers?

"Je kunt nooit 100% voorkomen dat je gehackt wordt, dus bedenk ook eens wat je moet doen als het mis gaat. Je doet eens per jaar een brandoefening, maar waarom geen digitale brandoefening? Loop stap voor stap zo'n situatie door en bedenk welke acties je gaat ondernemen. Zo sta je minder voor verrassingen wanneer er echt iets gebeurt."

Welke securitytrend vind jij dit jaar het opvallendst?

"Eigenlijk sta je bijna nergens meer van te kijken tegenwoordig. Iets wat we het afgelopen jaar veel in het nieuws hebben gezien is misbruik van kwetsbaarheden in producten van Microsoft of supply-chain attacks via Kaseya. Hierdoor zou je bijna denken dat aanvallers vrij spel hebben, maar bedenk dat cybersecurityspecialisten ook heel veel aanvallen wél voorkomen en tegenhouden."

9. Jaap Schouten, Digitaal forensisch specialist bij Praetorian-IT

Wat is je gouden tip voor ondernemers?

"Denk niet dat je nooit het slachtoffer kan worden van cybercrime en dat Cyber Awareness een eenmalig ding is."

Welke securitytrend vind jij dit jaar het opvallendst?

"Phishing vind ik dit jaar het opvallendst. Ook dit jaar is tot op heden thuiswerken een norm waar cybercriminelen op een sluwe en vaak geraffineerde manier gebruik van maken in de vorm van phishing."

10. Gina Doekhie, cybersecurityspecialist bij de politie

Wat is je grootste securityblunder?

"Tijdens een onderzoek waarbij iemand dacht dat de muis van een laptop bewoog zonder dat diegene de muis aanraakte, installeerde ik software waarmee je muisbewegingen registreert. Maar in de software zat malware en toen stond de security officer binnen een paar minuten naast mij. Gelukkig kon ik het incident gelijk oplossen."

Welke securitytrend vind jij dit jaar het opvallendst?

"Ik denk de toename van flubot malware. Dat is malware op een telefoon. Voorheen was het nog niet heel veel voorkomend. Dit betekent dat we ook veel bewuster moeten omgaan met security op je telefoon! Ik denk dat die trend wel door gaat zetten."

ZO BESCHERM JE JE TEGEN SOCIAL ENGINEERING

Bij cybercrime denk je misschien snel aan een hacker achter een computerscherm met programmeercodes. Toch is de werkelijkheid vaak minder hightech. Veel aanvallen beginnen bij menselijke misleiding, ofwel ‘social engineering’.

Bij social engineering maken internetcriminelen misbruik van menselijke eigenschappen zoals angst, hebzucht, nieuwsgierigheid, vertrouwen en onwetendheid. Zo verleiden oplichters je bijvoorbeeld om persoonlijke of bedrijfsgevoelige gegevens te delen voor het zogenaamd deblokkeren van een account. Welke soorten social engineering zijn er, en hoe bescherm je je ertegen?

Fysieke social engineering

Er zijn 2 soorten social engineering: fysieke en digitale. Bij fysieke social engineering vindt de misleiding op locatie plaats. Het doel van de crimineel of hacker is om belangrijke informatie te stelen, die hij op een later moment gebruikt om een digitale aanval te plegen. De belangrijkste vormen van fysieke social engineering zijn:

Afval doorzoeken

Criminelen doorzoeken je afval op jacht naar bedrijfsgegevens, zoals brieven of gekopieerde documenten. Deze techniek wordt ook wel ‘dumpster diving’ genoemd. De gegevens gebruiken ze bijvoorbeeld om geloofwaardig over te komen wanneer ze telefonisch contact met je opnemen.

Vernietig je informatie zorgvuldig

Wees je bewust van welke informatie je weggooit en hoe je dat doet. Zelfs onschuldig lijkende informatie zoals een bellijst of functieomschrijving kan voor een crimineel nuttig zijn bij een gerichte aanval. Maak gebruik van een papierversnipperaar of een container met een slot.

Besmette USB-stick
Het is verleidelijk om een gevonden USB-stick in je computer te steken. Het is niet verstandig maar toch gebeurt het. Je wilt waarschijnlijk weten wat erop staat. Een hacker gebruikt deze nieuwsgierigheid. Hij laat expres USB-sticks rondslingeren met daarop schadelijke software. Deze software start zodra jij de USB-stick in je computer steekt en installeert bijvoorbeeld automatisch malware. Hiermee krijgt de crimineel toegang tot je interne computersystemen of 'gijzelt' je netwerk met ransomware.

Beveilig je apparaten en maak back-ups
Beveilig je apparaten en computernetwerk met antivirussoftware. Maak regelmatig back-ups van je computerbestanden en houd je software up-to-date.

Impersonatie
Bij impersonatie doen criminelen zich voor als een vertrouwde partij om je te misleiden. De crimineel doet bijvoorbeeld alsof hij een klusjesman is en meldt zich bij de receptie voor een reparatie. Of hij komt langs als servicemonteur voor onderhoud aan je wifi-netwerk. Eenmaal binnen zit deze 'monteur' achter een computer in je bedrijf en heeft hij toegang tot gevoelige bedrijfsgegevens.

Registreer bezoekersgegevens
Laat bezoekers nooit zomaar je pand binnen. Registreer de bezoekersgegevens en vraag altijd om een identiteitsbewijs.

Meekijken
Je bent onderweg en werkt op je laptop, bijvoorbeeld in de trein. Nietsvermoedend typ je een wachtwoord in of werk je aan een stuk met gevoelige informatie. Houd er rekening mee dat een crimineel eenvoudig over je schouder kan meekijken. Hij kan de informatie die hij ziet later gebruiken voor het hacken van je computersysteem. Deze vorm van social engineering wordt ook wel 'shoulder surfing' genoemd

Gebruik een screenprotector
Gebruik een screenprotector op je laptop en telefoon. Dit is een speciale laag plastic of glas op je scherm die ervoor zorgt dat anderen niet kunnen meekijken.

Digitale social engineering

Bij digitale social engineering vindt de misleiding digitaal plaats. Bijvoorbeeld via internet en telefonie. Hiervoor maakt de cybercrimineel onder andere gebruik van op locatie of social media gestolen informatie.

Social media
Via social media zijn persoonlijke gegevens van een slachtoffer te achterhalen. Criminelen gebruiken bijvoorbeeld LinkedIn als bron om je vervolgens met behulp van die informatie op te lichten. Bijvoorbeeld door het sturen van phishingberichten.

Blijf kritisch
Denk goed na over welke informatie je deelt op social media. Beveilig je account met sterke wachtwoorden en blijf kritisch op berichten die je ontvangt. Accepteer bijvoorbeeld niet zomaar een uitnodiging van een onbekend persoon.

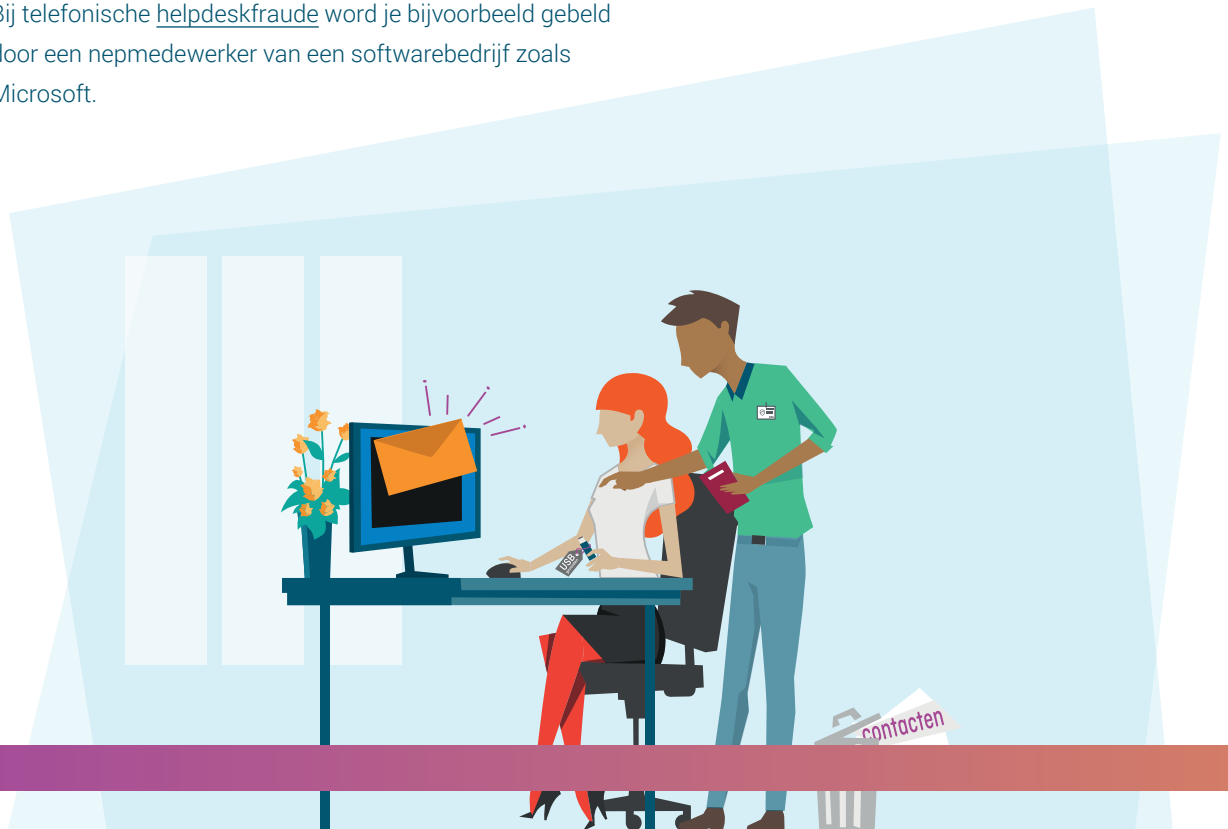
Phishing
Phishing is een vorm van digitale oplichting. Fraudeurs misleiden je met gerichte valse e-mails. De e-mails lijken op berichten van bekende, en vaak betrouwbare, organisaties. Zoals overheidsinstellingen en banken. Zo proberen de criminelen jouw inloggegevens, creditcardinformatie, pincode of andere persoonlijke informatie te achterhalen. Naast e-mail gebruiken criminelen ook sms en WhatsApp voor phishing.

"Veel cyberaanvallen beginnen bij menselijke misleiding, ofwel social engineering"

Klik voorzichtig
Klik nooit zomaar op links of bijlagen in een e-mail die je niet vertrouwt. Links of bijlagen in valse e-mails kunnen ervoor zorgen dat er schadelijke software op je computer wordt geïnstalleerd.

Telefoonfraude en CEO-fraude
Bij telefoonfraude word je opgelicht via een telefoongesprek met bijvoorbeeld een zogenaamde helpdesk of bank.

Even wat software installeren
Bij telefonische helpdeskfraude word je bijvoorbeeld gebeld door een nepmedewerker van een softwarebedrijf zoals Microsoft.



Hij geeft aan dat er een probleem is met jouw software en dat dit gevaar oplevert. Hij wil dit graag direct oplossen en vraagt je om even wat software te installeren. Het blijkt dan te gaan om schadelijke software waarmee criminelen toegang krijgen tot je computersysteem.

Snel geld overmaken
Een oplichter kan zich aan de telefoon ook voordoen als een medewerker van je bank. Hij overtuigt je ervan dat je bankrekening is gehackt omdat hij verdachte betalingen ziet.

Hij legt uit dat je geld kunt overmaken naar een 'veilige rekening' of een 'kluisrekening'. Zulke rekeningen bestaan niet, in werkelijkheid is het de rekening van de oplichter zelf. Hij biedt aan je te helpen bij het overboeken. Zo komt je geld op de rekening van de oplichter terecht.

CEO-fraude
Bij CEO-fraude krijgt een medewerker de opdracht om een geldbedrag over te maken naar een bepaalde rekening. De opdracht lijkt van de directie afkomstig te zijn. Het verzoek komt echter niet van de directie, maar van een cybercrimineel die zichzelf als leidinggevende voordoet. Het geld gaat dan ook naar de bankrekening van deze fraudeur.

Bij CEO-fraude maken cybercriminelen vaak gebruik van e-mailspoofing. Dit is een techniek waarmee je een e-mail uit naam van iemand anders verzendt. In het geval van CEO-fraude lijkt een e-mailbericht afkomstig van de directeur. Doordat de medewerker het e-mailadres van zijn werkgever ziet, is hij eerder geneigd om op het verzoek in te gaan.

Laat je niet onder druk zetten
Vertrouw niet iedereen zomaar en laat je niet onder druk zetten. Aanvallers maken gebruik van urgentie en proberen je hiermee onder tijdsdruk te zetten. Trap hier niet in, blijf rustig nadenken en neem geen overhaaste beslissingen.

QUIZ

HOE CYBER-VEILIG BEN JIJ?

Bekijk hoe jij omgaat met deze situaties en ontdek hoe cyberveilig je bent.

1. Je zit in de trein, onderweg naar een zakelijke afspraak, wanneer je je realiseert dat je bent vergeten een belangrijk document naar een andere klant te sturen. Wat doe je?

- A. Je pakt je laptop erbij en maakt verbinding met de wifi van de trein om het document alsnog te versturen.
- B. Je doet niets en verstuurt het document pas als je weer op je werkplek/kantoor met internet verbonden bent.
- C. Je maakt een hotspot van je mobiele telefoon en gebruikt die verbinding op je laptop om het document te versturen.

2. Eenmaal aangekomen op je eindbestemming loop je naar de koffiezaak, waar je wacht op je afspraak. Het is vrij druk, maar je vindt een plekje aan een gemeenschappelijke tafel. Je werkt achter je laptop en besluit een kopje koffie te halen. Wat doe je?

- A. Je logt uit en laat je laptop op de tafel, zodat je plekje niet wordt ingepikt als je koffie haalt.
- B. Je neemt je laptop mee om koffie te halen.
- C. Je logt uit en vraagt de persoon naast je of zij even op je laptop kan letten als jij koffie haalt.

3. Je wordt gebeld door een onbekend nummer. Het is een medewerker van je bank. Criminelen halen je rekening leeg! Snelle actie is vereist om te voorkomen dat je al je geld kwijtraakt. De medewerker vraagt ter verificatie om je wachtwoord zodat hij je account direct kan blokkeren.

- A. Je geeft je wachtwoord, want je hebt geen tijd te verliezen.
- B. Je hangt direct op. Een échte bankmedewerker vraag nooit naar je wachtwoord, toch?
- C. Je checkt of de medewerker geen oplichter is door te vragen of hij jouw naam, geboortedatum en rekeningnummer kan opnoemen. Wanneer hij dit foutloos kan, geef je het wachtwoord.

4. In je ooghoek zie je je afspraak arriveren. Er komt nét een mailtje binnen van een onbekende afzender. Het is waarschijnlijk een potentiële nieuwe klant.

- A. Fijn! Een nieuwe klant, je opent de mail en klikt op het webadres dat de afzender in de mail heeft gezet om te kijken of het wat voor je is.
- B. Je laat de mail staan, na je afspraak kun je deze in alle rust bekijken.
- C. Je hebt eigenlijk geen tijd maar opent snel de mail om even te kijken of het belangrijk is voor je bedrijf.

5. Je afspraak verloopt soepel. Jullie besluiten samen te werken. Hiervoor moeten jullie zeer vertrouwelijke bestanden met elkaar delen. Hoe doe je dit?

- A. De persoon met wie je de afspraak hebt, biedt zijn USB-stick aan. Hiermee kunnen jullie met gemak de bestanden uitwisselen.
- B. Jullie versturen de bestanden versleuteld, en delen de toegangscode alleen mondeling met elkaar.
- C. Jullie sturen elkaar de bestanden via een online verzendplatform.

6. Aan het eind van de dag ben je weer op je werkplek/kantoor en rond je wat laatste zaken af. Je staat op het punt om uit te loggen als je een melding van je laptop krijgt: je moet updates draaien. Dit zal zo'n 5 minuten duren.

- A. Je klikt de melding weg want het komt nu niet uit. Dit doe je altijd tot de melding komt op een geschikt moment en je de updates rustig kunt draaien.
- B. Je draait direct de update, want met een oude software-versie loop je een groter risico om gehackt te worden.
- C. Je sluit de laptop af en neemt je voor de update morgenochtend te draaien zodra je weer aan het werk gaat.

Check je score.

Heb je de meeste A's? Ai, je cyberveiligheid is waarschijnlijk niet zo goed op orde. Als ondernemer ben je steeds afhankelijker van online tools om zaken te kunnen doen. Daarmee word ook je bedrijf kwetsbaarder voor cyberaanvallen. Vind je cyberveiligheid ingewikkeld en weet je niet waar je moet beginnen? Gebruik de checklist op pagina 9.

Heb je de meeste C's? Cyberveiligheid heeft voor jou misschien geen grote prioriteit. Maar wist je dat 1 op de 5 mkb'ers slachtoffer wordt van cybercriminelen? En dit aantal blijft maar stijgen. Houd criminelen buiten de deur door jezelf online veilig te gedragen. Op pagina 17 krijg je tips van cyberexperts.

Heb je de meeste B's? Jij weet dat cyberveiligheid tijd (en soms ook geld) kost en kiest ervoor dat te investeren. Heel goed. Blijf op de hoogte van relevante ontwikkelingen op het gebied van veilig online ondernemen en word lid van het Cybernetwerk Ondernemend Nederland. Daar stel je al je cybervragen direct aan specialisten.

ONDERBROEK OP SLOT!
EN 4 ANDERE BIZARRE HACKS BIJ BEDRIJVEN

Inbreken via een aquarium of losgeld eisen met een kassabon: cybercriminelen zijn behoorlijk creatief. Dit zijn 5 gekke hacks bij bedrijven van de afgelopen jaren. En we trekken er lessen uit. Bijvoorbeeld: maak goede back-ups.

In films hacken criminelen met 1 druk op de knop een kerncentrale. In het echte leven is dat moeilijker. Maar toch, deze 5 waargebeurde hacks bij bedrijven zouden zo in een film kunnen. Je steekt er ook iets van op. Met goede cybersecurity voorkom je schade aan je bedrijf door cybercrime.

1

Onder de gordel

Een metalen onderbroek met een digitaal slot erop: 40.000 van dit soort slimme kuisheidsgordels verkocht het Chinese bedrijf Qiui wereldwijd. Goede zaken dus. Tot oktober 2020, toen een securitybedrijf een kwetsbaarheid in de beveiliging ontdekte. Hackers zouden de gordel, die via een app bediend wordt, op afstand op slot kunnen zetten. De enige manier om dan je edele delen te bevrijden: een betonschaar. Het gat in de beveiliging kwam naar buiten en het bedrijf leed enorme reputatieschade.

Wijze les:

Is het succes van je onderneming sterk afhankelijk van digitale technologie? Zorg dan dat je de veiligheid regelmatig goed test. Begin bijvoorbeeld met een cyberscan, of laat een pentest uitvoeren.

2 Dag Sinterklaasje

5 december is een perfecte dag om mensen te misleiden. Dat ontdekte securityexpert Matthieu Paques, nu senior manager Cybersecurity bij KMPG. Tijdens een oefening verkleedden hij en een collega zich als Sint en Piet. In hun jutezak hadden ze niet alleen pepernoten, maar ook spionageapparatuur.

De goedheiligman en Paques, in de rol van Piet, meldden zich bij de receptie van een datacenter en deelden pepernoten en een chocoladeletter uit. “Al snel stonden we binnen. En dat terwijl een datacenter behoorlijk goed beveiligd is”, vertelt Paques. Hij had als securitytester toestemming voor deze oefening, maar een crimineel kan zo’n truc natuurlijk ook bedenken.

Wijze les:
Wees altijd op je hoede, vertrouw zelfs Sinterklaas niet. Criminelen gebruiken social engineering om je vertrouwen te winnen en je op te lichten. Controleer altijd of iemand is wie hij zegt dat hij is.

3 Vis in het water

In 2017 kocht een casino in de Verenigde Staten een nieuw aquarium met slimme sensors die de temperatuur van het water in de gaten hielden. Die sensors waren verbonden met een pc. Maar de internetverbinding tussen het aquarium en de pc was slecht beveiligd. Cybercriminelen drongen via die verbinding het computernetwerk binnen. Zo stalen ze 10 gigabyte aan data van het casino via het aquarium. De hack werd snel ontdekt, dus geen miljoenenbuit voor deze dieven.

Wijze les:
Let op de beveiliging van je slimme apparaten. Vervang altijd de standaardwachtwoorden van dit soort ‘IoT-apparaten’ met sterke wachtwoorden.

4 Bonnetje erbij?

Stel je voor: je supermarkt staat vol klanten, en dan slaan de printers van alle kassa’s ineens op hol. Het gebeurde in november 2020 bij tientallen supermarkten in Chili en Argentinië. Op de bonnetjes stond deze boodschap: “Je netwerk is aangevallen, je computers en servers zijn op slot gezet!” Cybercriminelen hadden data van het moederbedrijf gegijzeld met ransomware. Ze eisten miljoenen dollars losgeld, via de kassabonnetjes. Het is onbekend of het bedrijf betaald heeft.

Wijze les:
Bescherm je bedrijf tegen ransomware: installeer antivirussoftware en maak regelmatig back-ups. Zo beperk je de schade bij een cyberaanval.

5 Handen thuis

In 2018 installeerde een luxe warenhuis in de VS 10 vingerafdruksloten op de magazijnen. Een cybercrimineel hackte dat slotsysteem en uploadde zijn eigen vingerafdruk. Op die manier wilde hij later bij het magazijn eenvoudig zijn vinger scannen en naar binnen wandelen. Helaas voor hem: een securitybedrijf ontdekte zijn hack binnen een paar minuten. Bewijzen dat hij de dader was bleek simpel: zijn vingerafdruk had hij immers zelf geleverd.

Wijze les:
Beveilig biometrische gegevens zoals vingerafdrukken en gezichtsherkenning streng. Dat ben je volgens de privacywet AVG verplicht.

Sluit je aan!

Heb je nog vragen over de online veiligheid van je bedrijf? Wil je weten hoe andere ondernemers omgaan met cybercrime? Of heb je een technische cybersecurityvraag? Voor antwoorden en inspiratie kun je ook op LinkedIn terecht. In de besloten groep Cybernetwerk Ondernemend Nederland zitten allerlei cybersecurityexperts die je graag adviseren of op weg helpen. Sluit je aan bij het netwerk via deze link: Cybernetwerk Ondernemend Nederland | Groepen | LinkedIn

Ontdek meer

Beveilig je onderneming met behulp van de artikelen en video's op KVK.nl/cyber.

Colofon

KLIK HIER! is een uitgave van Kamer van Koophandel®, Utrecht, oktober 2021

Contact

Vragen of opmerkingen over de inhoud van dit magazine? Mail naar kvk.cyber@kvk.nl

Cybernetwerk Ondernemend Nederland