KVK

OKTOBER 2022

KLIK HIER!

WEGWIJZER CYBER-SECURITY

SLUIT JE AAN BIJ ONS
CYBERNETWERKOPLINKEDIN

Sluit je aan!

Heb je 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: 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®
in samenwerking met het Digital Trust Center.
Utrecht, oktober 2022

Contact

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

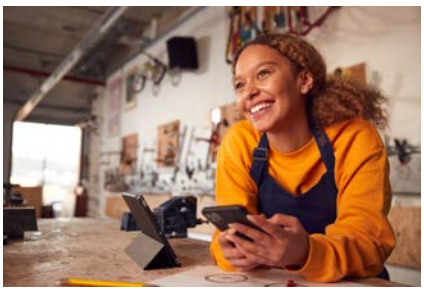
KVK

digital trust center.

Inhoudsopgave

Paniek om een virus!

Een virusje op de laptop: we halen er nu onze schouders over op. Maar zo'n 30 jaar geleden was er voor het eerst grote paniek over een computervirus bij Nederlandse bedrijven. Wat was dat voor virus? En hoe liep het af? **p. 10**



Bescherm je bedrijf met deze 7 maatregelen

Iedere onderneming is anders. Toch is er een aantal veiligheidspunten waar vrijwel iedere ondernemer aan moet denken. Hoe cyberweerbaar is jouw bedrijf? Het Digital Trust Center zet zeven maatregelen op een rij waar je direct mee aan de slag kunt. **p. 18**

"We hadden geen beleid" Wat Joost Fromberg leerde van een hack

Met de digitale veiligheid van zijn bedrijf was Joost Fromberg, eigenaar van online marketingbureau ODIV, niet bezig. Totdat zijn bedrijf gehackt werd en hij zich maandenlang moest bezighouden met de gevolgen. Wat was de impact en wat heeft hij ervan geleerd? **p. 30**

Wachtwoord Do's & Don'ts

Een ijzersterk wachtwoord, hoe lang moet dat zijn? Wat kun je wel gebruiken en wat juist niet? En hoe vaak moet je een wachtwoord veranderen? Met deze do's & don'ts maak je het voor cybercriminelen zo lastig mogelijk om je wachtwoorden te kraken. **p. 34**

En verder

Samen werken aan cyberveiligheid

Voorwoord

Nederland behoort op digitaliseringsgebied tot de absolute wereldtop. Onze digitale infrastructuur vormt de internationale maatstaf en ook onze samenleving loopt ver voorop in haar digitalisering. Dat merken we aan onze slimme apparaten thuis, aan hoe we werken, hoe we winkelen en hoe we ondernemen.

Ik hoop dat u de kansen die digitalisering voor uw bedrijf en dagelijks leven biedt weet te benutten. Daar helpen we u ook graag bij met initiatieven als Mijn Digitale Zaak, waar de retail-mkb'er op maat een digitaliseringaanbod kan vinden en subsidie kan aanvragen.

Maar ons enthousiasme voor de kansen van digitalisering kan niet zonder aandacht voor onze cyberveiligheid. Dat geldt des te meer voor het door ons gekoesterde mkb, waar kwaadwillenden hun oog vaak op laten vallen. Een op de vijf medewerkers blijkt nog te reageren op een phishingmail. En al ruim 3.000 keer heeft het Digital Trust Center sinds juni 2021 individuele bedrijven voor een ernstige bedrijfsspecifieke digitale dreiging of kwetsbaarheid gewaarschuwd.

Ik gun u een veilige digitale omgeving om zaken te doen. Dat vraagt om oplettendheid en een sterke samenwerking tussen overheden, instanties en bedrijfsleven. Alertheid en het vergroten van onze cyberweerbaarheid zijn daarbij de speerpunten.

Laat u daarbij helpen door de experts van het Digital Trust Center en KVK. Hun samenwerking levert u de middelen waarmee u kunt bouwen aan uw cyberweerbaarheid.

In dit magazine vindt u inspiratie en tips die u als ondernemer een stap verder helpen om uw bedrijf digitaal veiliger te maken. Lees bijvoorbeeld het verhaal van ondernemer Henny de Haas, die zelf slachtoffer werd van een cyberaanval. Of ontdek hoe u een sterk wachtwoord maakt.

Zet de volgende stap in uw digitale weerbaarheid.

Ik wens u veel leesplezier en inspiratie toe!

M.A.M. Adriaansens
Minister van Economische Zaken & Klimaat

Micky Adriaansens
Minister van Economische Zaken & Klimaat

"We helpen u graag met initiatieven als Mijn Digitale Zaak, waar u op maat een digitaliseringaanbod vindt en subsidie kunt aanvragen."

JE HALVE OMZET KWIJT AAN OPLICHTERS

DIT IS BEC-FRAUDE

Het is geen woord dat je elke dag hoort: BEC-fraude. Maar volgens het Openbaar Ministerie groeit BEC-fraude enorm. Deze oplichting via e-mail kan je veel geld kosten, óók als je een klein bedrijf hebt. Twee experts beantwoorden vier vragen over BEC-fraude.

Het begon als een normale zakendeal. Begin 2021 maakte een bedrijf uit Leimuiden afspraken met een Europese leverancier. Na wat mailverkeer plaatste het bedrijf een bestelling, ontving twee facturen voor in totaal 80.000 euro en maakte het geld over. In mei 2021 vroeg de leverancier: "Waar blijft de betaling?" Wat bleek: het Leimuidense bedrijf had het geld niet betaald aan de echte leverancier, maar aan criminelen. De oplichters kregen dat voor elkaar met BEC-fraude.

1. Wat is BEC-fraude?

"BEC staat voor Business E-mail Compromise", vertelt Koen Hermans. Hij werkt als aanklager voor het Openbaar Ministerie en ziet elke week voorbeelden van BEC-fraude. "Criminelen gebruiken je zakelijke e-mailverkeer om je op te lichten." Er zijn verschillende vormen van BEC-fraude, maar twee elementen komen bijna altijd terug: criminelen gebruiken e-mail en ze doen zich voor als iemand anders.

Factuurfraude

Een andere vorm van BEC-fraude is factuurfraude. Hermans legt uit: "Je krijgt een factuur die je verwacht, maar op de factuur is het rekeningnummer aangepast. Het geld dat je overmaakt gaat niet naar je leverancier, maar naar de crimineel. Soms schrijven de criminelen in de mail dat het bedrijf waar je vaker zaken mee doet een nieuw rekeningnummer heeft. Ze vragen je dan of je het rekeningnummer in je boekhoudsysteem wilt aanpassen."

"Er zijn verschillende vormen van BEC-fraude, maar twee elementen komen bijna altijd terug"

CEO-fraude

Een bekende vorm van BEC-fraude heet ook wel CEO-fraude. "Daarbij krijgt een medewerker een e-mail van 'de baas', met de vraag om een geldbedrag over te maken. Uiteindelijk blijkt 'de baas' een crimineel die het geld wegsluist. Een bekend voorbeeld is de Pathé-zaak in 2018. In die zaak maakte de bioscoopketen zonder het zelf door te hebben in totaal 19 miljoen euro over aan criminelen." Begin 2022 ging een Rotterdams staalbedrijf voor ruim 11 miljoen euro het schip in door CEO-fraude.

Spoofing

Hoe krijgen criminelen het voor elkaar dat jij denkt dat de mail van je leverancier komt? "Het kan zijn dat het mailadres gespooft is, of overgenomen", legt Hermans uit. "Dan zie je niet aan het mailadres dat de mail eigenlijk van iemand anders komt. Maar we zien ook veel 'typosquatting'. Daarbij wijzigt de oplichter één letter of cijfer in het mailadres. Niemand let daarop." Is het echte adres info@kvk.nl, dan gebruikt de crimineel misschien info@kvk.nu. Of zelfs @kvk.nl, waarbij de laatste letter van het mailadres een hoofdletter 'i' is.

2. Raakt BEC-fraude kleine bedrijven?

Volgens Hermans is BEC-fraude ook een gevaar voor kleinere bedrijven en stichtingen. “Een aangifte die ik heb gezien, was van een bedrijf dat jaarlijks zo’n twee ton aan omzet binnenkreeg. Het werd voor een ton opgelicht. Dus ja: BEC-fraude overkomt ook bedrijven die geen miljoenenomzet hebben.”
In april 2021 kreeg de penningmeester van een Zoetermeerse sportvereniging via e-mail een betaalverzoek van de voorzitter: of hij 3.500 euro wilde overmaken. Toen de penningmeester even belde, bleek dat de voorzitter die mail nooit verzonden had. “Op het moment dat je denkt ‘dit is vreemd’: pak de telefoon en bel de afzender”, adviseert Hermans.

Schade

De schade door BEC-fraude in Nederland is lastig in te schatten, zegt Bert Feskens, securityexpert bij Security Delta HSD. “Weinig bedrijven doen aangifte van cybercrime, omdat ze bang zijn voor reputatie-schade of zich schamen. Dus we hebben te maken met onderrapportage. Maar volgens de Amerikaanse veiligheidsdienst FBI neemt deze vorm van fraude enorm toe. In 2021 was de gerapporteerde schade in de VS door BEC-fraude bijna 2,4 miljard dollar.”

3. Hoe voorkom je BEC-fraude?

Feskens en Hermans geven vier tips waarmee je BEC-fraude helpt voorkomen:

1. Zorg voor technische drempels. Stel bijvoorbeeld je boekhoudsysteem zo in, dat het lastig is om een rekeningnummer te wijzigen. Zorg ook dat de beveiliging van je e-mailverkeer op orde is, zodat criminelen moeilijker je e-mailadres kunnen misbruiken.
2. Gebruik het vier-ogenprincipe. Laat altijd meerdere medewerkers meekijken met het betalen van facturen boven een bepaald bedrag. Zie je iets vreemds? Neem dan telefonisch contact op met de leverancier om de factuur te checken. Doe dat niet per e-mail, want het kan zijn dat criminelen je mailserver hebben gehackt en je mail onderscheppen.
3. Creëer een open bedrijfscultuur. Als medewerkers niet bang zijn om jou vragen te stellen of feedback te geven, zullen ze een verdachte situatie eerder melden. Een open houding richting je medewerkers kan BEC-fraude dus voorkomen.
4. Let extra op in vakantietijd. Criminelen slaan vaak hun slag als de bezetting laag is, bijvoorbeeld tijdens het weekend of in de vakantie.

4. Wat moet ik doen als ik slachtoffer ben?

Kom je erachter dat je bent opgelicht via BEC-fraude? Hermans adviseert dan deze vier acties:

1. Bel direct je bank. “Kijk of zij het geld terug kunnen boeken. Vaak is dat niet mogelijk, omdat criminelen het geld meestal snel naar een andere rekening verplaatsen.”
2. Neem contact op met je IT-beheerder, als je die hebt. “Het kan namelijk zijn dat je mailserver is gehackt, dus het is goed als een specialist met je meekijkt.”
3. Doe aangifte bij de politie. “De politie en het OM kunnen pas stappen zetten als ze informatie krijgen. Op het moment dat je het niet meldt of geen aangifte doet, kunnen ze niks tegen de criminelen doen.”
4. Meld de fraude bij de Fraudehelpdesk. Zij waarschuwen andere ondernemers.
5. Meld de oplichting ook via de website Bec-Off bij Onderzoeksinstituut TNO. Dit helpt hen bij het onderzoek naar manieren om BEC-fraude te voorkomen.

In 2020 hackten criminelen de e-mail van een Haarlems softwarebedrijf. Tientallen klanten ontvingen valse facturen. Het hele verhaal lees je op de website van het Digital Trust Center (DTC).

PANIEK OM EEN **VIRUS!**

Een virusje op de laptop: we halen er nu onze schouders over op. Maar zo'n 30 jaar geleden was er voor het eerst grote paniek over een computervirus bij Nederlandse bedrijven. Een nieuw virus zou massaal data gaan wissen, met dramatische gevolgen. "Er gaan mensen uit het raam springen", waarschuwden computerexperts zelfs. Wat was dat voor virus? En hoe liep het af?

1988
Januari

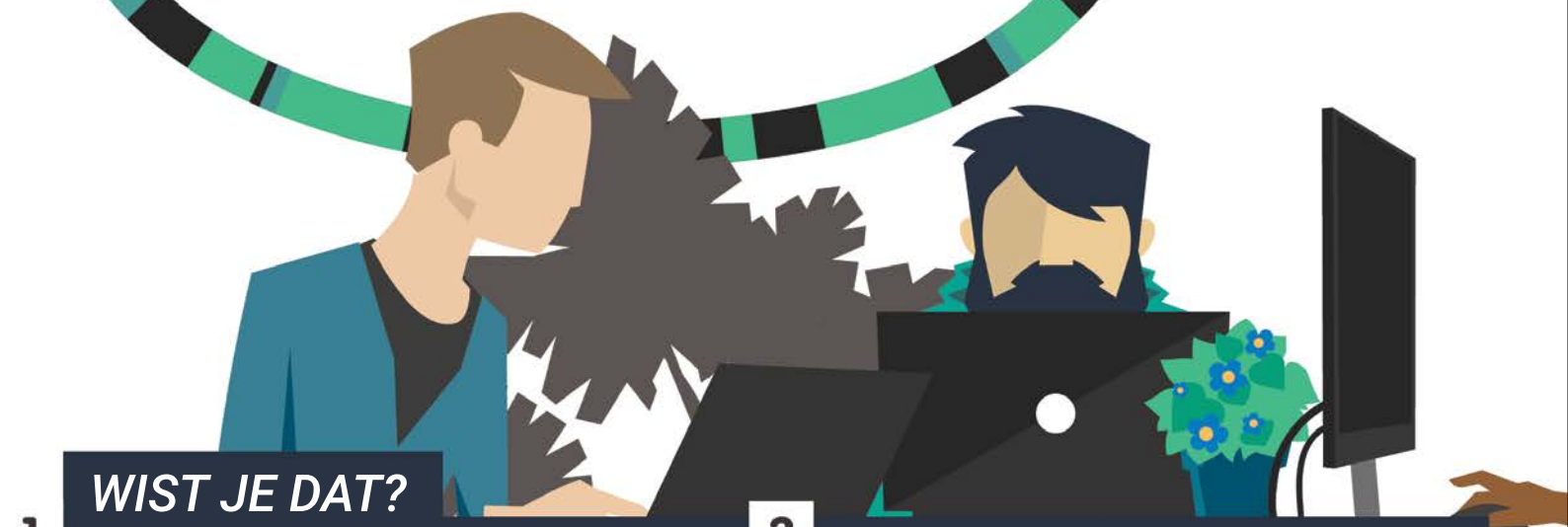
Virus ontdekt in Israël

Computerdeskundigen in Israël ontdekken begin 1988 een nieuw 'elektronisch computervirus'. Niemand weet wat dat is, daarom leggen de kranten het uit: "De term 'virus' is vaktaal voor een reeks commando's die uit zichzelf starten. Het kan alle gegevens die op de computer staan onherstelbaar vernietigen."

1989
Januari

Chaos in Engeland

Het virus dat in Israël ontdekt is, duikt begin 1989 op in Engeland. "Computervirus ontwaakte op vrijdag de 13de", schrijft het Nieuwsblad van het Noorden. Bij een aantal Britse bedrijven vernietigt het virus programma's en data. Dat zorgt volgens de krant voor 'chaotische taferelen'.



WIST JE DAT?

1 Een van de eerste computervirussen heette Ping Pong. Als je computer besmet was, zag je op je scherm een balletje naar alle kanten stuiteren. Het werd in 1988 ontdekt.

2 Rond 1988 waren er ongeveer 45 bekende computervirussen. In 2021 werden er zo'n 23,7 miljoen nieuwe malwaresamples ontdekt, ongeveer 65.000 per dag.

1989
September

Nederland, pas op!

Het Israëlische virus krijgt drie namen: 'vrijdag-de-dertiende-virus', 'computervirus Jeruzalem' en 'PLO-virus', omdat er misschien Palestijnse hackers achter zitten. Via floppy's en gedeelde servers verspreidt het virus zich ook in Nederland. Experts waarschuwen in Nederlandse kranten: Pas op! Op vrijdag 13 oktober 1989 zal het virus ook hier actief worden.

1989
10 oktober

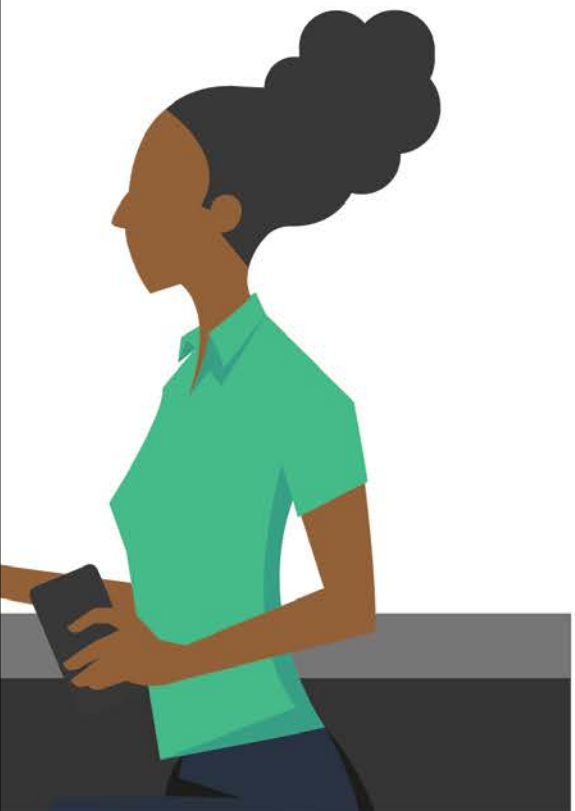
De spanning stijgt...

Nederlandse computergebruikers krijgen begin oktober de bibbers, schrijft de krant Het Vrije Volk: "In de computerwereld stijgt de spanning nu blijkt dat het computervirus Jeruzalem zich in grote omvang heeft verspreid. Het aantal computergebruikers dat gedupeerd dreigt te worden door dit virus loopt in de tienduizenden." Politie en verzekeraars maken zich op voor een computerramp.

1989
14 oktober

Hoe loopt het af?

Het loopt af met een grote sisser. Volgens de Telegraaf zijn tussen de vijf en tien Nederlandse bedrijven getroffen. Achteraf lijkt alle paniek volgens de krant 'een storm in een glas water'. Dat heeft een voordeel, schrijft Het Vrije Volk: "Tienduizenden argeloze computergebruikers zullen in het vervolg veel zorgvuldiger omgaan met hun apparatuur."



Hebben we ervan geleerd?

Ben jij goed beschermd tegen virussen en andere vormen van cybercrime? Ontdek op kvk.nl/cyber hoe je digitaal veilig werkt en blijf op de hoogte van actuele cyberdreigingen.

HOPPENBROUWERS TECHNIEK ZIET CYBERAANVAL ALS UITDAGING

Vrijdagavond lag het hele bedrijf plat en maandagochtend ging iedereen weer min of meer normaal aan het werk. Hoppenbrouwers Techniek werd in 2021 slachtoffer van een cyberaanval en werkte een weekend lang met man en macht om de gevolgen zo klein mogelijk te houden. Eigenaar Henny de Haas is er opmerkelijk positief uitgekomen. “Ik voel me erdoor gesterkt.”

De cyberaanval werd ontdekt toen een medewerker op 2 juli 2021 rond half zeven ‘s avonds de helpdesk belde. Hij kwam niet meer in zijn laptop. Al snel bleek dat de helpdesk zelf ook problemen had. “Toen was de conclusie: we zijn waarschijnlijk gehackt”, vertelt Henny de Haas. Hoppenbrouwers Techniek was slachtoffer van een wereldwijde cyberaanval. “De malware is binnengekomen via een update van onze Kaseya-software, waarmee we eindpunten en systemen kunnen beheren op afstand. Iedereen die deze software gebruikt en de update had geïnstalleerd werd erdoor geraakt.”

Een raampje vinden

En dat terwijl De Haas dacht dat hij zich goed had gewapend tegen cyberaanvallen. “We waren al een jaar of vier verzekerd tegen schade door hackers. Onze beveiliging was gecertificeerd, we gebruiken dubbele authenticatie bij inloggen en onze computers worden goed in de gaten gehouden. Medewerkers moeten bij indiensttreding een examen afleggen over alle regels rond wifi, wachtwoorden, enzovoort. Dus het bewustzijn onder de medewerkers is vrij hoog. Maar die hackers hoeven maar ergens een raampje te vinden en ze zijn binnen.”

Alles kon besmet zijn

Na de melding op vrijdagavond nam de ICT-afdeling contact op met een gespecialiseerd beveiligingsbedrijf. “Zij zijn begonnen met inventariseren en een plan van aanpak te maken voor het komende weekend.” Toen De Haas zelf was gealarmeerd, begreep hij al snel dat het niet alleen om de servers ging. “Van de laptops tot de beveiliging van de gebouwen zelf, alles kon besmet zijn. Naast de ICT-afdeling hebben heel veel andere medewerkers ICT-kennis, dus hebben we teams gemaakt die allemaal een deel van de systemen voor hun rekening namen. Iedereen die dacht dat hij iets kon bijdragen, mocht meedenken.”

Webinars voor personeel

Op zaterdag was in elke Hoppenbrouwers-vestiging een team van medewerkers bezig met computers nakijken, bouw- en installatieprojecten nalopen, monteurs bellen. “Zaterdagmiddag hadden we 80 procent van de problemen al opgelost. Zaterdagavond konden we een back-up terugzetten en werd de server langzaam maar zeker opgeschoond. Zondagavond kon ik weer inloggen en op maandag konden we weer aan de slag.” Tussendoor werden

“Achteraf denk ik dat we een protocol hadden moeten hebben en dat testen. Je doet toch ook brandoefeningen?”

het personeel en de buitenwereld op de hoogte gehouden. “Met behulp van de afdeling communicatie heb ik twee webinars gehouden, waarin ik alle stappen die we namen voor het personeel heb toegelicht. Op een speciale website konden medewerkers constant updates lezen. En ik heb nog vijf radiozenders en een aantal tv-zenders te woord gestaan.”

Vraag om losgeld

Na het weekend werd het werk weer opgepakt. “We hebben nog wat klanten gebeld, omdat enkele facturen uit ons systeem waren verdwenen, maar afgezien daarvan viel de schade erg mee. De ICT-afdeling en de beveiligingsspecialisten zijn wel nog ruim een week bezig geweest om de laatste dingen na te lopen en op te schonen.” En ja, dan was er natuurlijk nog de vraag om losgeld. “Dit was een wereldwijde aanval op meer dan duizend bedrijven en de hackers eisten zeventig miljoen aan losgeld. Hadden we met een collectezakje moeten rondgaan? We zijn er niet op ingegaan en hebben niet betaald. We waren al druk genoeg met het dichten van de gaten.”

Protocollen oefenen

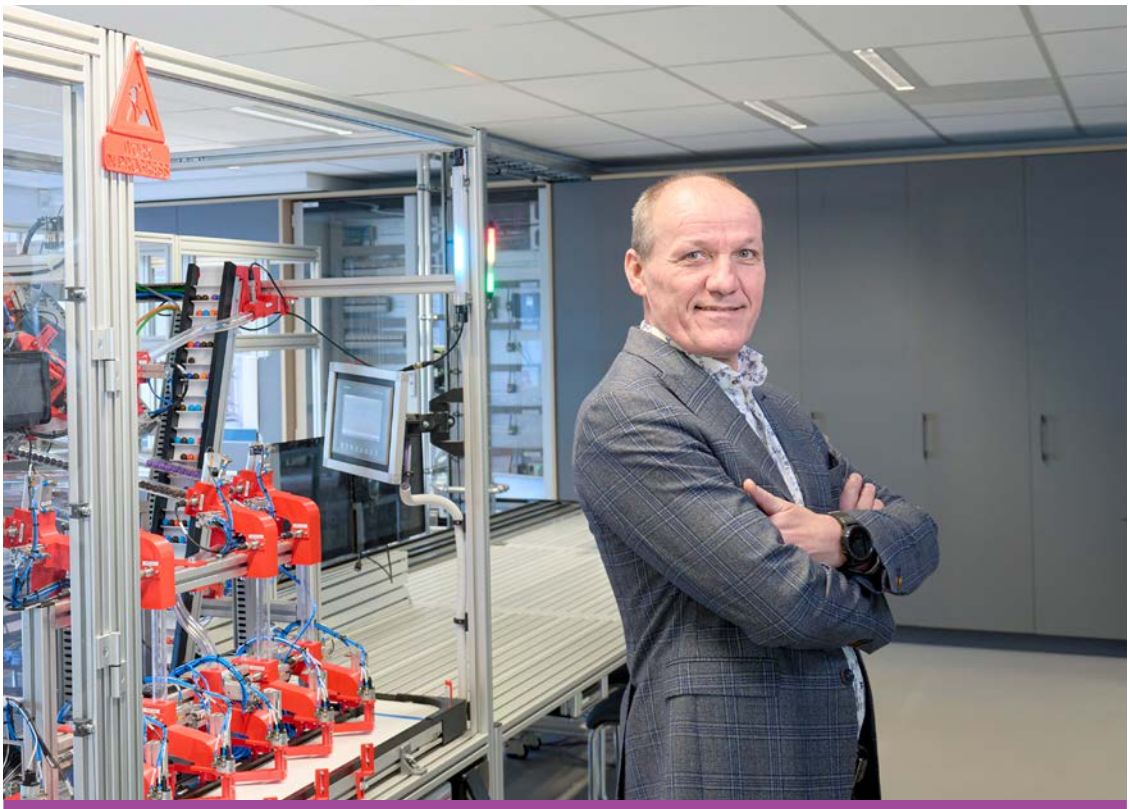
Terugkijkend is De Haas verbaasd over hoe zijn bedrijf zo snel tot actie overging. “We hadden geen plan vooraf wat we zouden doen in een dergelijk geval. Maar ik had ook niet van tevoren kunnen bedenken dat we tijdens dat weekend zo snel een effectieve aanpak zouden ontwikkelen. Achteraf denk ik dat we een protocol hadden moeten hebben en dat ook hadden moeten testen. Dat doet niemand, maar eigenlijk is dat gek. Je doet toch ook brandoefeningen?”

Cohesie binnen het bedrijf

Op de vraag wat De Haas hiervan heeft geleerd, komt een verrassend antwoord: “Het klinkt misschien gek, maar ik had het niet willen missen. Dit gun je niemand, maar ik heb er veel van geleerd. Binnen ons bedrijf werken we in zelfsturende teams en ligt de verantwoordelijkheid laag in de organisatie, dus medewerkers zijn gewend om mee te denken. Door al die mensen in een crisis bij elkaar te brengen, organiseer je zoveel denkkracht, dan komt de oplossing vanzelf. Ik vond de cohesie die in het bedrijf ontstond heel ontroerend.” Daarnaast is het bewustzijn nog scherper geworden dan voorheen. “Want de kans dat we nog eens worden gehackt, is net zo groot als dat ieder ander wordt geraakt. Natuurlijk houden we de systemen nog beter in de gaten, hebben we software die vreemde activiteiten op het netwerk signaleert en hebben we eigen cyberspecialisten. Maar als hackers echt op zoek gaan, vinden ze altijd wel een zwak punt. Alleen, net als bij inbrekers, degene met het beste slot lopen ze misschien voorbij.”

Cyberaanval als uitdaging

De tegenslag heeft De Haas in elk geval niet bij de pakken doen neerzitten. Het bedrijf heeft een ambitieuze toekomstvisie voor 2030 en die wordt volgens plan uitgevoerd, zegt De Haas. “We denken onze omzet te verdrievoudigen en het aantal vestigingen te verdubbelen, zodat we echt landelijke dekking krijgen. Tegen die tijd hebben we 5.000 medewerkers in dienst, zijn we 100 procent CO_2-neutraal en circulair ingericht en gaan we voor een excellente klantbeleving. Die cyberaanval zie ik als een uitdaging en ik voel me erdoor gesterkt.”



Henny de Haas

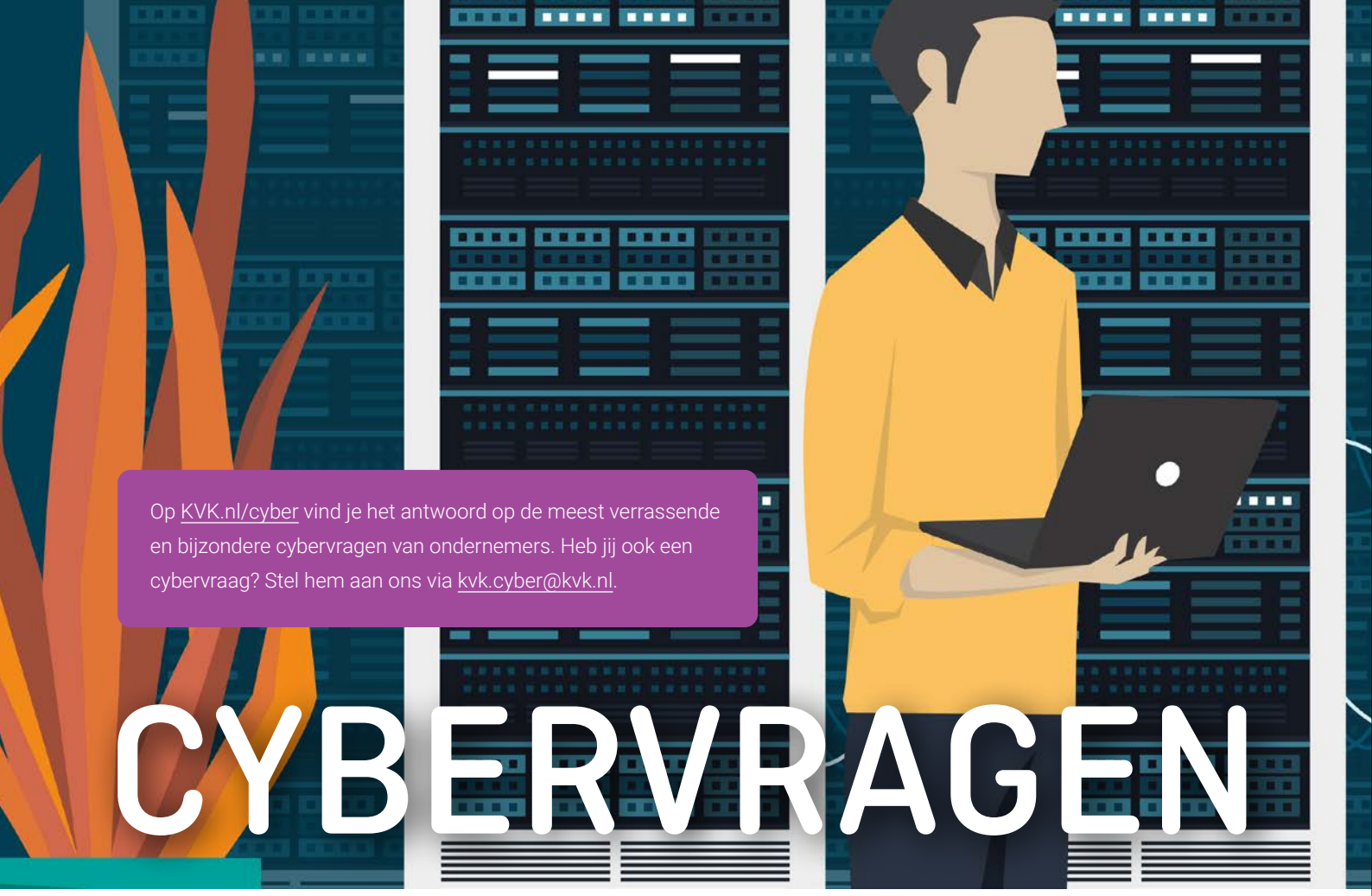
Directeur-eigenaar van Hoppenbrouwers Techniek

Sinds hij als boerenzoon besloot dat hij meer wilde dan koeien melken, maakte hij stapsgewijs zijn dromen waar: van elektricien werd hij uiteindelijk directeur (2002) en eigenaar (2013) bij Hoppenbrouwers.

“Ik vond de cohesie die in het bedrijf ontstond heel ontroerend.”

- Hoppenbrouwer Techniek
- Totale schade door cyberaanval: 500.000 euro (deels gedekt door de verzekering)
- 1.600 werknemers

Tip: “Laat niet alles over aan ICT-specialisten, maar verdiep je zelf ook in computers en veiligheid. De hele wereld hangt van ICT aan elkaar en je moet weten hoe kwetsbaar je bent. Doordat zoveel van onze medewerkers wat computerkennis hebben, konden we de taken verdelen en alles tegelijk aanpakken. Daardoor konden we snel weer aan het werk.”



Op KVK.nl/cyber vind je het antwoord op de meest verrassende en bijzondere cybervragen van ondernemers. Heb jij ook een cybervraag? Stel hem aan ons via kvk.cyber@kvk.nl.

CYBERVRAGEN

Help, ik ben mijn laptop kwijt. Wat moet ik doen?

Stel: je komt terug van een zakenreis. Op het vliegveld kom je erachter dat je laptop kwijt is, mét alle gegevens van je klanten. Een datalek dus. Maria Genova, expert op het gebied van online privacy, vertelt wat je moet doen.

Meld het datalek bij Autoriteit Persoonsgegevens

Bij klantgegevens gaat het om privacygevoelige informatie. "Volgens de privacywet AVG moet je in zo'n geval een melding maken bij de Autoriteit Persoonsgegevens. Doe je dat niet, dan kun je een boete krijgen die kan oplopen tot maximaal 820.000 euro.

Voor klanten kan een datalek vervelende gevolgen hebben. Informeer je klanten daarom altijd over het datalek en waarschuw ze voor de risico's. Oplichters sturen hen mogelijk phishingmails of plegen neptelefoontjes en kunnen vervolgens met de juiste gegevens bankrekeningen volledig leegplundeΔren", vertelt Genova. "Het beste is natuurlijk een datalek voorkomen. Dus beveilig je laptop met een sterk wachtwoord en versleutel je harde schijf."

Stel je cybervraag via kvk.cyber@kvk.nl.

> “Informeer je klanten altijd over het datalek en waarschuw ze voor de risico’s”

Waarom moet je niet zomaar je paspoort laten kopiëren?

Je staat aan de balie van een Spaans hotel, of je huurt een schuurmachine om je kantoorvloer eens op te frissen. Dan komt de vraag: mag ik uw identiteitsbewijs even kopiëren? Dat is niet zonder gevaar.

“Dat komt doordat we in Nederland werken met het BSN-nummer”, zegt Frans van Berkel van het bedrijf PassProtect. “Bij je geboorte krijg je een uniek BSN-nummer. Dat is de sleutel tot je identiteit. Als een kwaadwillende dat nummer in handen krijgt, kan hij op jouw naam een abonnement of een lening afsluiten, of zelfs een pand huren voor een wietplantage.” Frauderen met je identiteit dus.

Zo bescherm je je gegevens

- **Weiger een kopie.**
  Volgens de privacywet AVG mag niet zomaar iedereen een kopie van je paspoort eisen. Alleen organisaties die dat wettelijk verplicht zijn mogen dat, zoals banken, verzekeraars of overheids-instanties.
- **Maak gevoelige gegevens onleesbaar.**
  Bijvoorbeeld met de app KopieID van de overheid. Er bestaan ook verschillende fysieke methodes. Zo ontwikkelde PassProtect een afneembare folie die je over je paspoort, rijbewijs of ID-kaart plakt. Als iemand dan een kopie van je paspoort in handen krijgt, zijn je foto en BSN-nummer niet geheel zichtbaar. Ook de ANWB biedt zo’n product aan.

BESCHERM JE BEDRIJF MET DEZE 7 MAATREGELEN

Iedere onderneming is anders. En er zijn verschillende manieren om cyberveilig te werken. Toch is er een aantal veiligheidspunten waar vrijwel iedere ondernemer aan moet denken. Hoe cyberweerbaar is jouw bedrijf? Het Digital Trust Center, onderdeel van het ministerie van Economische Zaken en Klimaat, zet zeven maatregelen op een rij waar je direct mee aan de slag kunt.

1 Maak een back-up

Beperk de schade van een cyberincident met een goede back-up. Zorg voor één of meerdere kopieën van je bedrijfsdata. Bewaar minimaal één zo'n back-up op een andere locatie. Heb je een IT-dienstverlener die dit voor je regelt? Vraag dan om periodieke rapportage. Zo zie je wat en hoe er geback-upt wordt.

2 Gebruik multifactorauthenticatie

Multifactorauthenticatie is een van de belangrijkste maatregelen waarmee je voorkomt dat een onbevoegde toegang krijgt tot je account. Het werkt als een extra slot op je account. Om in te loggen heb je dan niet alleen je wachtwoord nodig, maar bijvoorbeeld ook je vingerafdruk of een code die je via sms of een app ontvangt. Schakel dit in ieder geval in op je zakelijke e-mailaccount en je belangrijkste bedrijfsapplicaties.

3 Zet automatische updates aan

Software-updates bevatten naast verbeteringen voor de gebruiker vaak ook beveiligingsupdates. Hackers zoeken actief naar kwetsbaarheden in verouderde software. Wacht daarom niet met updaten van je software en zet bij voorkeur automatisch updaten aan. Denk hierbij niet alleen aan je computer of smartphone, maar bijvoorbeeld ook aan je tablet, printer of router.

4 Gebruik antivirussoftware

Installeer een antivirusprogramma en zorg dat deze software up-to-date blijft. Doe dit op alle computers en servers binnen je bedrijf. Op deze manier detecteer en verwijder je digitale bedreigingen.

Het gebruik van een antivirusprogramma beschermt ook indirect de apparaten van je klanten en bijvoorbeeld toeleveranciers. Veel virussen maken namelijk gebruik van een e-mailprogramma om zichzelf te verspreiden. Met antivirussoftware bescherm je dus jezelf én anderen.

5 Controleer je e-mail beveiligingsstandaarden

Via internet.nl controleer je de beveiliging van je e-mailadres. Je vindt er of je domeinnaam, het gedeelte achter de '@', beveiligingsstandaarden gebruikt en welke dat zijn. Gebruikt je domeinnaam geen beveiligingsstandaarden? Bespreek dan met een IT-dienstverlener hoe je dit kunt verbeteren. Goede e-mail beveiligingstandaarden zorgen ervoor dat cybercriminelen je identiteit niet kunnen misbruiken om spam zoals phishing te versturen.

6 Herken phishing

Phishing is een groot gevaar voor iedere onderneming. Maak je medewerkers alert en zorg dat ze phishing herkennen. Oefenen kan hierbij helpen. Deel bijvoorbeeld de online phishing quiz of phishingbingo op digitaltrustcenter.nl of start een phishingtest in samenwerking met een IT-dienstleverancier.

TIP

Controleer het e-mailadres van de afzender. Dat doe je zo:

- Kijk goed naar de domeinnaam waarvan je de e-mail hebt ontvangen.
- Controleer of de domeinnaam overeenkomt met het websiteadres.
- Het verschil zit soms in een klein detail. Zie jij het verschil tussen mail@31008mailers.nl en mail@3I008mailers.nl?

7 Maak een offline bellijst

Zorg dat contactgegevens van belangrijke partners uitgeprint klaarliggen in het geval van een cyberincident. Denk hierbij aan een IT-dienstverlener, softwareleverancier en een cybersecurity bedrijf dat je verder helpt bij problemen. Een voorbeeld van zo'n bellijst vind je op digitaltrustcenter.nl.

Aan de slag met de cyberweerbaarheid van je bedrijf

Speciaal voor ondernemers die weinig ervaring hebben met cybersecurity, ontwikkelde het DTC de CyberVeilig Check voor zzp en mkb. Binnen vijf minuten weet je hoe je start met de digitale beveiliging van je bedrijf. Download je eigen actielijst en ga direct aan de slag met de praktische instructies en tips.

KIJK, MIJN WEBSHOP DEUGT!

Heb je je wel eens afgevraagd hoe betrouwbaar je website of webshop overkomt op mogelijke klanten? Als je niet betrouwbaar lijkt, zullen weinig klanten zaken met je willen doen. Neem daarom jouw website eens goed onder de loep. Kom je betrouwbaar genoeg over?

Klanten zijn op hun hoede, omdat oplichters zich online voordoen als eerlijke ondernemers. Er zijn verschillende manieren waarop je je webshop voor klanten betrouwbaar maakt.

Keurmerken

Met een keurmerk laat je direct aan je klanten zien dat je voldoet aan wet- en regelgeving en een veilige betaalomgeving biedt. Er zijn verschillende gecertificeerde keurmerken. Gerard Spierenburg, woordvoerder van de Consumentenbond geeft advies: "Wij raden consumenten vooral Thuiswinkel Waarborg of Webshop Keurmerk aan, omdat deze keurmerken algemene voorwaarden hanteren die met ons zijn afgesproken. Ook zijn deze ondernemers aangesloten bij de onafhankelijke Geschillencommissie die helpt bij eventuele conflicten tussen webshop en consument. Zo'n commissie is voor veel klanten een hele geruststelling."

Nog effectiever

Je denkt nu misschien: een keurmerk, dat is het belangrijkste. Maar volgens Michiel Henneke van Stichting Internet Domeinregistratie Nederland (SIDN) letten consumenten ook op andere zaken. Henneke deed daar onderzoek naar. "Wij stelden bijna 4.000 consumenten de vraag: waar let je op als je wilt weten of een website betrouwbaar is? Keurmerken kwamen op de derde plaats (51%), onder reviews van andere consumenten (66%) en veilige betaalmogelijkheden (60%)."

Reviews

Beoordelingen van andere consumenten, oftewel reviews, zijn volgens het onderzoek van SIDN de meest invloedrijke factor. Zorg ervoor dat reviews goed zichtbaar zijn op je site, zodat je klant deze gelijk kan zien. "Het scheelt een klant zelf zoeken als je ze prominent op je site zet. Zo blijven je klanten in

Een goede webshop toont alles in één oogopslag en laat de klant niet zoeken naar keurmerken, reviews en betaalmogelijkheden.

jouw online omgeving en wijken ze niet uit naar bijvoorbeeld Google om daar reviews te lezen", legt Henneke uit.

iDEAL

Dat de betaalmogelijkheid belangrijk is voor het vertrouwen van de klant is volgens Henneke opvallend. "Het is dus verstandig om kritisch te kijken naar je betaalmogelijkheden. iDEAL is ook een soort keurmerk geworden. Klanten weten dat iDEAL goed controleert welke partijen hun dienst aanbieden."

Design en domeinnaam

Als het gaat om betrouwbaar overkomen op klanten, moet je het design en de domeinnaam van je site niet onderschatten, vindt Henneke. "Te gek als je

"Tegenwoordig zie je dat veel webshops logo's van reviewsites zoals Trustpilot en Klantenvertellen delen. Dat zijn niet echt keurmerken, maar in de beleving van de klant is het vergelijkbaar. Of zelfs beter, want alleen al een logo van een betrouwbare reviewsite geeft klanten vertrouwen."

een mooi keurmerk hebt, maar als je dat vervolgens nauwelijks kunt zien omdat het dezelfde kleur heeft als je website, heb je er weinig aan. Een goede webshop toont alles in één oogopslag en laat de klant niet zoeken naar keurmerken, reviews en betaalmogelijkheden", tipt Henneke.

Een domeinnaam die eindigt op .nl wekt volgens Henneke het meeste vertrouwen bij Nederlandse consumenten. "Als je ook in het buitenland wilt verkopen, bijvoorbeeld in België, kan het de moeite waard zijn om .be te kopen als domeinnaam. Zo heb je sneller het vertrouwen van je Belgische klanten."

Vertrouwen

Je wil niet dat klanten vroegtijdig afhaken omdat ze de boel niet vertrouwen. Dat is waar het volgens Henneke uiteindelijk op neerkomt. "De concurrentie online is vaak moordend, je moet je onderscheiden. Dus als je een mooi bedrijf hebt, laat dat gelijk aan je klanten zien. Investeer in de transparantie van je bedrijf, daar pluk jij de vruchten van."

Laat je niet hacken: drie simpele tips voor een veilige webshop

Wat kun je doen om je webshop veiliger te maken? Marc van Vliet, securityadviseur bij Perfect Day geeft drie tips om je webshop te beschermen tegen digitale dreigingen. Hij werkte jarenlang in de e-commerce en kent de online gevaren vanuit de praktijk.

1. Check welke gegevens je van klanten hebt. "Veel ondernemers hebben niet in de gaten hoeveel klantgegevens ze eigenlijk hebben, of waar ze die opslaan. Pas als je dat weet, weet je waar je moet beginnen met beveiliging. En vraag niet te veel gegevens van je klanten. Je hebt geen geboortedatum nodig om een muismat te verzenden." Klantgegevens die je niet hebt, hoef je ook niet te beveiligen.
2. "Geef je medewerkers individuele gebruikersaccounts, met unieke wachtwoorden." Bij een gedeeld account en gedeeld wachtwoord is de kans groter dat een kwaadwillende of slordige medewerker schade aanricht.
3. "Beveilig je contactformulier met een captcha, dat is een test waarmee een klant bewijst dat die geen robot is." Je kunt meer spam en phishingmails verwachten als je je contactformulier niet goed beveiligt. Als je minder van die phishingmails krijgt, zul je waarschijnlijk minder snel op een besmette link klikken.

CYBERSECURITY QUIZ
TEST JE KENNIS

Weet jij hoe je een zwak wachtwoord beveiligt? Ooit gehoord van hackers met gekleurde hoedjes? En kun je een datalek signaleren? Test je kennis en vergroot je cyberweerbaarheid. De letters bij de juiste antwoorden vormen uiteindelijk een zin.

1 Schadelijke software waarmee een cybercrimineel je digitale bestanden op slot zet en je afperst, noem je?

- C. Blackmailware
- K. Ransomware
- W. Spyware

2 Niet alle hackers zijn criminelen. Ethisch hackers sporen veiligheidslekken bij bedrijven op en melden deze bij hen. Wat is een ander woord voor ethisch hacker?

- L. White hat hacker
- Y. Green hat hacker
- A. Black hat hacker

3 Bij deze cyberaanval sturen criminelen in één keer zo veel verkeer naar computers, netwerken en servers, dat die overbelast raken. Websites en netwerken worden hierdoor heel traag of zelfs geheel onbereikbaar. Heel onhandig als je bijvoorbeeld een webshop hebt.

- C. Brute Force aanval
- I. DDoS-aanval
- B. Spoofing

4 Bij een hacker denk je misschien aan iemand achter een computerscherm. Maar sommige aanvallen beginnen bij offline misleiding. Bijvoorbeeld wanneer een crimineel je bedrijfspand binnenkomt door zich voor te doen als iemand anders. Of je wordt gebeld door iemand die informatie zoals je wachtwoord probeert te ontfutselen. Hoe noem je dit soort misleiding?

- O. Fysieke intimidatie
- R. Offline virus
- K. Social engineering

5 Openbare wifi-netwerken zoals in de trein of op een vliegveld zijn onveilig. Zodra je inlogt op zo'n wifi-netwerk, kan een hacker toegang krijgen tot je apparaat. Op welke manier kun je veiliger gebruikmaken van openbare netwerken?

- H. Door het gebruik van een VPN. Daarmee ben je anoniemer op het internet.
- E. Door het gebruik van een firewall die aanvallen tegenhoudt.
- T. Door het gebruik van blacklisting. Daarmee maak je je apparaat onzichtbaar voor hackers.

6 Cyberspecialisten noemen dit de zwakste schakel in cybersecurity.

- V. Zwakke wachtwoorden
- I. Mensen
- P. Slechte antivirussoftware

7 Wat is de beste manier om een zwak wachtwoord zoals 'hallo123' beter te beveiligen?

- L. Sla het wachtwoord op in een wachtwoordmanager.
- U. Gebruik het voor maar 1 account en deel het met niemand.
- E. Zet tweestapsverificatie aan.

8 In welk geval is er sprake van een datalek?

- N. Je hebt al een jaar geen back-up gemaakt.
- M. Je schakelt je laptop uit voordat een software-update is afgerond.
- R. Je stuurt een vertrouwelijke e-mail naar de verkeerde persoon.

Vul hier de letters van je antwoorden in.

								!

Antwoord

Het antwoord vind je achterin dit magazine op p. 35.

SLUIT JE AAN BIJ DE DTC COMMUNITY

Het Digital Trust Center heeft een vertrouwde online community waar kennis, informatie en ervaringen rondom cyberveiligheid gedeeld worden. De DTC Community is voor Nederlandse ondernemers en IT-specialisten.

Meld je aan en blijf op de hoogte van ernstige beveiligingslekken. Door je aan te sluiten bij deze community vergroot je de digitale weerbaarheid van je organisatie en draag je bij aan een veiliger ondernemersklimaat in Nederland.

Zien we je binnenkort bij de DTC Community? Ga naar digitaltrustcenter.nl/community.

Wat te doen bij een cyberincident?

doorloop deze stappen als je te maken hebt met een cyberincident

1. **Blijf kalm**

2. **Bel je ICT helpdesk**

3. **Bespreek**
   a. of je internetverbinding wel of niet beschikbaar blijft
   b. of je systemen aan- of juist uitgezet moeten worden

4. **Inventariseer wat er nog werkt**

5. **Leg direct alle acties en activiteiten vast in een logboek**

BIJNA GEHACKT!

WAT ER GEBEURDE TOEN IK EEN PHISHINGTEST DEED

Dikke kans dat je er laatst een hebt gekregen: een raar mailtje van een onbekende, of een sms over een levering terwijl je niks hebt besteld. Phishing hoort erbij. Maar herken je elk verdacht bericht? Ik deed een phishingtest en kwam erachter dat sommige phishingmails echt overtuigend zijn.

Liesbeth Sparks
Content creator bij KVK

Wat er vroeger allemaal misging, weet ik als historicus heel goed. Maar ook in de 21ste eeuw zijn we onveilig. Ik onderzoek in deze serie risico's van nu. Hoe beschermen we onze bedrijven tegen cybercrime? Daarover praat ik met experts.

Soms vraag ik me af of iemand er ooit in trapt, in zo'n e-mail van ene 'dr mike paul'. Vanuit Burkina Faso vraagt hij om persoonlijke gegevens. In ruil voor tien miljoen dollar. Dacht het niet, vriend. Die mail gaat direct in de prullenbak. Maar ook al herken je sommige phishing makkelijk, het blijft een groot probleem. "Wereldwijd begint zo'n 90% van alle datalekken met een phishingbericht", zegt security-expert Dim Gerssen. Tijd om eens te testen hoe cybercriminelen te werk gaan. Trap ik in een écht goede phishingmail?

Maart - Nep-phishing

"Dat is dan afgesproken", zegt Gerssen aan de telefoon. Securitybedrijf Surelock zal mij en twee van mijn collega's de komende tijd phishingmails sturen. Of eigenlijk: nep-phishingmails. Het security-bedrijf traint ondernemers en hun medewerkers met zogenoemde phishingsimulaties. Als ik op een 'verdachte' link klik in zo'n nepmail, kom ik niet uit bij schadelijke software, maar bij de melding: 'Je bent gephisht!' Hopelijk trap ik er niet in …

April - Alles verdacht

Na het gesprek met Gerssen zie ik overal hackers. Ieder mailtje met een onbekende afzender bekijk ik drie keer. Een paar mails gooi ik gelijk weg. Ik ben niet de enige van mijn team die niks meer vertrouwt. "Ik ben helemaal para", lacht collega Hajar.

Maar het duurt wel lang, dit experiment. Als ik na een paar weken geen écht verdachte mails heb gekregen, let ik niet meer zo goed op. "Dat is heel normaal", zegt Gerssen. "Aan het begin van een simulatie ben je er constant mee bezig. Maar na verloop van tijd verslapt je aandacht. Duitse wetenschappers zagen een half jaar na een simulatie een verval in de scherpte bij proefpersonen." En van even niet opletten profiteren cybercriminelen. Volgens de Nederlandse Vereniging van Banken (NVB) was de schade door online oplichting in Nederland in 2021 maar liefst 62,5 miljoen euro.

September - De test

'Ping'. Ik zit op kantoor, een bekertje koffie naast me. Hee, een mail van Hajar. Wat gek, ik verwacht geen nieuws over ons project. En is dat nou een linkje naar een pdf? Ik ga er met m'n muis naartoe, maar blijf toch even hangen. Dit klopt niet. "Hajar", zeg ik. Handig dat ze tegenover me zit. "Heb jij me nou net een mailtje gestuurd?" Ze kijkt me vragend aan. "Huh? Nee."

De schrik zit erin. Ik overleg met mijn teamgenoten. Twee anderen hebben de mail van 'Hajar' ook gekregen. We maken een melding bij IT. Ik pieker me suf: wie zit hierachter? Pas na een half uur bedenk ik: is dit niet die phishingtest? Ik veeg het zweet van m'n voorhoofd terwijl ik Gerssen bel. Intussen onderzoekt onze securityafdeling de mail. Op het scherm lezen ze: 'Je bent gephisht!' Dat was op het nippertje.

LinkedIn

Als ik Gerssen aan de lijn krijg, heb ik wel een paar vragen. Hoe wist hij bijvoorbeeld dat Hajar en ik veel samenwerken? "Via LinkedIn", vertelt hij. Inderdaad, wij reageren vaak op elkaars berichten. Had ik dit kunnen voorkomen? "Nee, eigenlijk niet", zegt Gerssen. "Er is altijd iets bekend over een bedrijf: via social media, nieuwspagina's, of in dit geval medewerkers die berichten plaatsen bij anderen." Je moet dus zeker voorzichtig zijn met wat je deelt, maar nóg belangrijker is dat je herkent dat er iets niet klopt als je een phishingmail ontvangt.

Onderbuik

Ik werk zoveel samen met mijn collega Hajar, dat ik haar mails als geen ander ken. Dit bericht 'klonk' niet als Hajar: daarom klikte ik niet op de link. "Dat onderbuikgevoel is de basis", zegt Gerssen. "Ik kan wel zeggen: 'controleer altijd het e-mailadres van de afzender', maar daar let je waarschijnlijk niet direct op. Voel je dat er iets niet klopt? Dat is het moment om de mail grondig te controleren. Dus bij twijfel: niet klikken, maar stoppen."

Wat je kunt doen:

- Check de afzender. Is het een rare of onbekende afzender, of een gekke variant op een officieel mailadres, gooi de mail dan weg. Of laat 'm controleren door je IT-beheerder.
- Controleer het linkje of de bijlage. Als je de cursor boven het linkje houdt, kun je zien waar deze naartoe leidt. Of google de bedrijfsnaam in de link.
- Bel of mail met de afzender. Antwoord niet op het mailtje dat je hebt gekregen, maar zoek contactgegevens op via een officiële website of je eigen contactenlijst.
- Vergelijk de mail met de voorbeeldphishingmails op Fraudeheldesk.nl.

Moeite

'Gaat een crimineel écht zoveel informatie verzamelen over mij voor één mailtje?', vraag ik me af. "Bij een klein bedrijf met tien medewerkers is dat risico inderdaad niet zo groot. Maar bij een groter bedrijf gebeurt dat zeker", antwoordt Gerssen.

Criminelen vallen kleine bedrijven aan door te schieten met hagel. Ze kopen e-maillijsten op, bijvoorbeeld op het darkweb. Alle adressen op die lijsten sturen ze phishingmails. "Als jouw zakelijke e-mailadres op zo'n lijst staat, is de kans dus groot dat je een phishingmail krijgt." En als het bij de eerste niet lukt, proberen ze het gewoon nog een keer. En nog een keer.

Oktober – Opletten

Het heeft indruk op me gemaakt, deze test. Ik dacht: kom maar op met die nep-phishingmail. Maar ik trapte er echt bijna in. Hoe zinvol zo'n simulatie is op de lange termijn, daar zijn experts het niet over eens. Het lijkt erop dat alleen een nepmail ontvangen niet genoeg is: ondernemers en medewerkers hebben meer kennis en informatie nodig om phishing te herkennen. Speciale trainingen zouden daarbij kunnen helpen. Hoe dan ook, ik ben de komende tijd in ieder geval extra voorzichtig.

ZO HERKEN JE EEN PHISHINGMAIL

‘WE HADDEN GEEN BELEID’

WAT ONDERNEMER JOOST FROMBERG LEERDE VAN EEN HACK

Met de digitale veiligheid van zijn bedrijf was Joost Fromberg, eigenaar van online marketingbureau ODIV, niet bezig. Liever hielp hij klanten met het bouwen en optimaliseren van websites, social media, e-mailmarketing en analyseren van data. Totdat zijn bedrijf vorig jaar zomer gehackt werd en hij zich maandenlang moest bezighouden met de gevolgen hiervan. Wat gebeurde er precies, wat was de impact en wat heeft hij ervan geleerd?

Je bent gehackt. Hoe is dat gegaan?

"Het begon vrij onschuldig. Een collega zei: 'Hé, er zit iemand iets met mijn mail te doen. Ik krijg een bericht dat iemand in mijn privémail zit en ik kan er zelf niet meer in.' Het wachtwoord en de tweefactor-authenticatie werkten niet meer. Hij kon nergens meer bij. Ook ons Facebook Business Manager account bleek geblokkeerd. Wij gebruiken deze tool om advertenties van klanten op Facebook en Instagram te tonen. Aan deze tool was de privémail van onze collega gekoppeld. We hebben in Facebook Business Manager zo'n 130 advertentieaccounts van onze klanten mét hun creditcardgegevens staan. Op dat moment zien we dat er mailtjes binnenkomen en dat gaat maar door. We kunnen zelf niet meer bij de gegevens maar we zien dat er advertenties worden geplaatst met een budget van 5.000 euro per dag. Flinke paniek. We zijn gehackt."

Kip zonder kop

"Wat moeten we doen? De eerste dag liepen we rond als een kip zonder kop. We hadden nog nooit een hack meegemaakt en ook geen beleid hiervoor. Een stappenplan wat je in zo'n situatie moet doen, hadden we niet. Mijn collega's en ik sloten ons op in een ruimte en probeerden inzichtelijk te maken welke accounts gehackt waren. Die klanten hebben we gebeld en gevraagd onmiddellijk hun creditcard te blokkeren of de betaalmethode te verwijderen. Facebook schrijft meerdere keren per dag geld af, iedere keer een paar honderd euro. Dus als je er snel bij bent, is de schade te overzien."

Vermoeiend proces

"Het kostte veel tijd om alle klanten te bellen. Ook klanten waar we al langere tijd niet meer actief waren, moesten we benaderen. Gelukkig bleef de financiële impact beperkt. Toen kwam de vraag: hoe zorgen we ervoor dat we weer verder kunnen met onze advertentieaccounts op Facebook? Hier waren de historie en data van de klanten aan gekoppeld en deze wilden we graag bewaren. Het contact met Facebook was een drama. Iedere keer kregen we weer een nieuwe klantenservicemedewerker die er niets van snapte. We werden telkens doorverwezen en er was echt nul hulp. Een vermoeiend proces."

Wat was de impact van de hack?

"De impact voor ons bedrijf was enorm. Het oplossen van de hack heeft ons zo'n zes maanden gekost. De eerste tijd zijn we vooral bezig geweest met het informeren van klanten en het vastleggen daarvan. Dit had ik achteraf gezien anders moeten doen. Door niet zo strikt bij te houden welke klant we al geïnformeerd hadden en welke niet, zijn we er lang mee bezig geweest. Door beter te loggen hadden we dossiers kunnen afstrepen. Het bleef een beetje chaos. Maar goed, we wisten ook niet hoelang het afhandelen van de hack zou duren."

Fouten toegeven

"Naar klanten toe zijn we altijd transparant geweest. Als je al een tijd met elkaar samenwerkt, je fout toegeeft en samen wilt werken aan een oplossing, kun je rekenen op veel begrip. Een klant zei: voor mij is het een klein beetje vervelend, maar voor jullie, met 130 klanten, is het nog veel vervelender. We hebben dan ook geen klanten verloren door de hack. Verder hebben we de politie erbij betrokken omdat er sprake was van identiteitsfraude. Maar leg maar eens aan de eerste de beste agent uit hoe bij ons Facebook, de advertentieaccounts en e-mail samenwerken. De aangifte leverde niets op. We hebben echt geluk gehad dat onze klanten uiteindelijk niet financieel zijn gedupeerd. Facebook heeft ervoor gezorgd dat het geld teruggestort werd. Maar cyberveiligheid is duidelijk een industrie die in de kinderschoenen staat. Je staat er helemaal alleen voor."

Wat heb je ervan geleerd?

"Mijn bedrijf ODIV bestaat zes jaar. Tot de hack waren we niet bezig met onze digitale veiligheid. Nadat de hack opgelost was, zijn we flink aan de slag gegaan met onze beveiliging. We hebben eerst een aantal praktische zaken geregeld. Zo hebben we een wachtwoordmanager ingesteld voor alle collega's, met gratis accounts voor familie en vrienden zodat het belang van veilige wachtwoorden ook in de privésfeer doordringt."

Ervaring delen

"Daarna kwam de vraag: wat is onze rol richting klanten? We willen niet dat klanten in dezelfde situatie komen als wij. De cyberveiligheid is bij mkb-ondernemingen vaak niet op orde. Ook is de informatievoorziening matig. Er is nog geen stappenplan met preventie- of escalatiebeleid. Daarom hebben wij onze bevindingen en ervaringen samengevat en vastgelegd in een whitepaper. In deze whitepaper, een rapport dat een probleem weergeeft en zorgt voor een oplossing, staan twee vragen centraal: 'Hoe zorg je ervoor dat je niet gehackt wordt?' en 'Wat doe je als je wél gehackt wordt?' Als we merken dat klanten slecht omgaan met wachtwoorden of data doorsturen op een onveilige manier, dan gaan we met ze in gesprek. We kijken nu of we binnenkort kunnen starten met ontbijtsessies of lunch&learn-sessies. De insteek hiervan is: dit is wat ons is overkomen, hier moeten jullie rekening mee houden en dit kunnen jullie eraan

"Als je al een tijd met elkaar samenwerkt, je fout toegeeft en samen wilt werken aan een oplossing, kun je rekenen op veel begrip"

“We hebben de hack omgezet in iets positiefs en delen onze ervaring en kennis graag met andere ondernemers”

doen. We willen zoveel mogelijk bedrijven bewust maken van digitale veiligheid en een stappenplan bieden voor noodsituaties. Wat ons is overkomen, hopen we niet meer mee te maken. We hebben het omgezet in iets positiefs en delen onze ervaring en kennis graag met andere ondernemers. Digitale veiligheid is een belangrijk onderdeel van ons bedrijf geworden.”

Tips van Joost Fromberg

- Koppel je privémailadressen los van je zakelijke accounts.
- Wees voorbereid op een mogelijke hack en maak een stappenplan.
- Denk niet dat het jou niet overkomt: het gaat niet om hoe groot je bedrijf is maar hoe makkelijk je te hacken bent.

Wachtwoord

Tips voor een sterk wachtwoord

★★★★_

& Do's Don'ts

Do's

ABCDEF
GHIJKL

Gebruik lange wachtwoorden of wachtzinnen, bij voorkeur meer dan **12 karakters**.

hB!a@01

Gebruik **kleine letters, hoofdletters, cijfers en speciale tekens.**

Kies voor onzinnige combinaties die **alleen voor jou logisch zijn**.

(O)dernemen
(I)s
(L)euk

Gebruik een **acroniem**, neem alleen de eerste letters van een zin en voeg deze samen.

D30dorant

Vervang één of meer letters door **een cijfer**.

Don'ts

dupliceer
dupliceer
dupliceer

Wachtwoorden herhalen voor meerdere accounts.

Kaarshouder231!

Hoofdletters op een **voorspelbare plek** plaatsen.

1234567890

Voor de hand liggende woorden of reeksen gebruiken.

30_12_92@1!

Persoonlijke informatie zoals je geboortedatum, adres of de naam van een familielid gebruiken.

Je wachtwoord **nooit veranderen**, doe dit minimaal één keer per jaar.

Het antwoord van de quiz op p. 23 = KLIK HIER!


KVK