10 tips voor een digitaal veiliger bedrijf

Whitepaper cybersecurity

kamer van koophandel

Colofon

Kamer van Koophandel, mei 2018

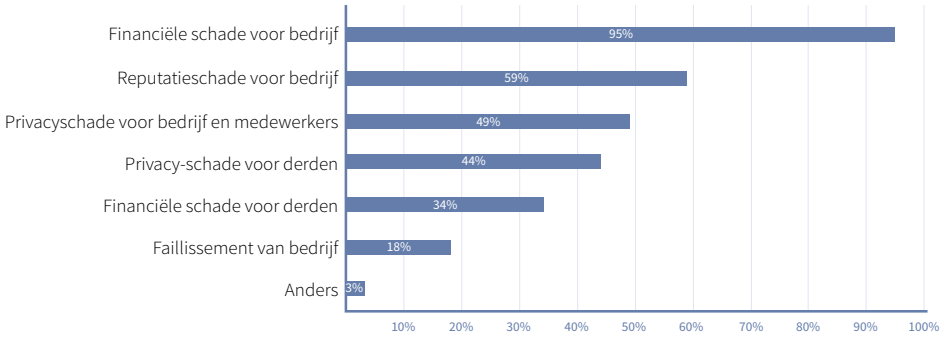
Inleiding

“De mail zag er uit alsof deze door een van mijn relaties was gestuurd en voor ik het wist had ik de bijlage geopend. Tegen de tijd dat ik doorhad dat ik hiermee schadelijke software toegang had gegeven tot mijn online bedrijfsomgeving was het al te laat. Het heeft me vijf dagen gekost om van die zwarte lijst af te komen. De inkomstenderving was funest voor mijn omzet dat kwartaal.”

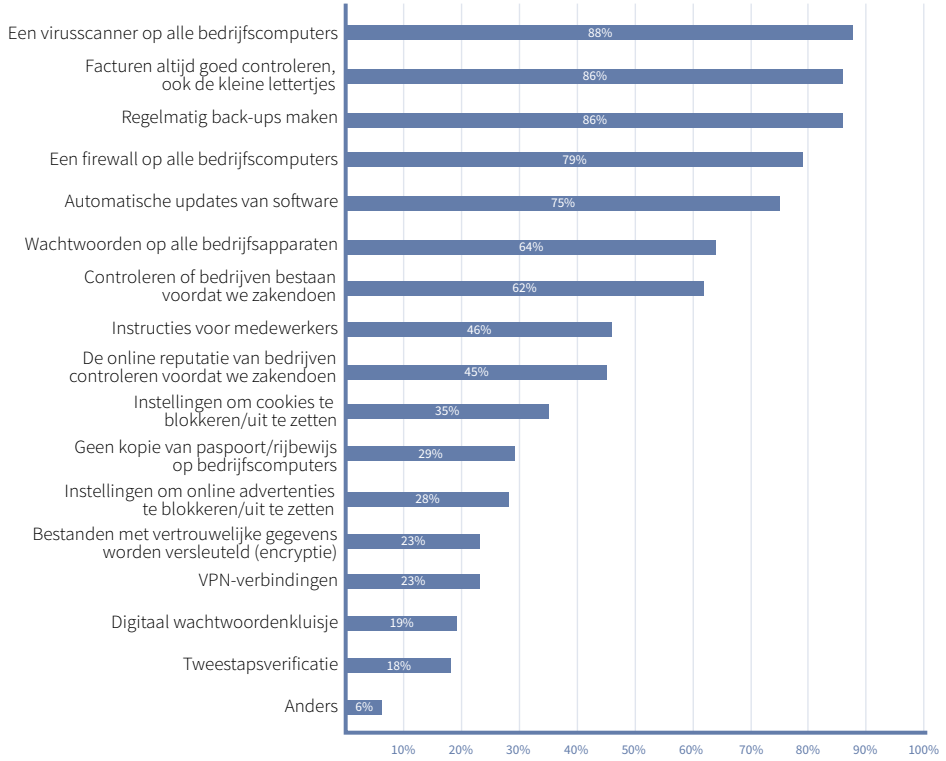
De wereld digitaliseert in een hoog tempo. Steeds meer ondernemers zijn met hun website, e-mailverkeer en online betalingen in grote mate afhankelijk van ict. Maar op het gebied van preventie tegen digitale fraude valt er bij freelancers en het midden- en kleinbedrijf (mkb) nog veel te winnen. Zo blijkt uit recent onderzoek van de Kamer van Koophandel (KvK) dat 39% van de mkb’ers in het afgelopen jaar te maken had met vormen van digitale fraude.

Om deze gaten in de digitale beveiliging te voorkomen, geven wij u 10 tips voor een digitaal veiliger bedrijf. Deze tips zijn voor elke ondernemer eenvoudig toepasbaar.

Welke mogelijke gevolgen ziet u in het geval van digitale fraude?
Meerdere antwoorden mogelijk.



Welke van de onderstaande maatregelen heeft u getroffen om digitale fraude te voorkomen?
Meerdere antwoorden mogelijk.



Het belang van cybersecurity

Het gevaar van cyberaanvallen als DDoS, ransomware en phishing ligt voor iedere onderneming op de loer. Toch zijn er nog veel ondernemers die zich onvoldoende beschermen tegen cybercrime. Deels uit onwetendheid en deels omdat het simpelweg niet in hun systeem zit. Dat terwijl de impact van een cyberaanval erg groot kan zijn.

Gelukkig kunt u ook als kleine ondernemer met simpele stappen hier iets tegen doen zodat de risico's beperkt blijven. Op die manier creëert u als ondernemer de juiste digitale randvoorwaarden om veilig zaken te doen en de continuïteit van uw bedrijf veilig te stellen.

We bezitten steeds meer 'smart' apparaten. Niet alleen onze televisie en telefoon staan straks in verbinding met internet, maar ook bijvoorbeeld onze auto en de koelkast. In al deze ontwerpen wordt gekeken naar het gemak van de mens, maar de dief wordt in het ontwerpproces vergeten. Tref dus zelf maatregelen. Zo voorkomt een ijzeren doosje bijvoorbeeld dat uw autosleutel wordt uitgelezen. Neem altijd het zekere voor het onzekere.

Financiële consequenties

Cybercriminelen zijn in veel gevallen uit op financieel gewin. Door bijvoorbeeld systemen of data te gijzelen, wordt een ondernemer gedwongen een geldsom te betalen aan de hacker. Maar een aanval heeft veelal een grotere financiële impact op een bedrijf dan alleen die directe kosten. Denk bijvoorbeeld aan de kosten voor het vervangen van aangetaste IT-infrastructuur of de tijd dat een bedrijf niet operationeel kan zijn. Bovendien levert cybercriminaliteit ook schade op aan de reputatie van een bedrijf, wat de omzet van het bedrijf op termijn negatief beïnvloedt. Zo kan de schade oplopen tot flinke bedragen.

Veilige keten

Door uw bedrijf digitaal te beveiligen, verkleint u niet alleen deze risico's op (financiële) schade, het is ook een manier om zakelijke kansen te creëren. Er zijn vandaag de dag steeds meer grote organisaties die alleen willen samenwerken met partners die hun beveiliging op orde hebben. Ook daarom is het van belang om bewust met cybersecurity bezig te zijn, zodat u deel uitmaakt van een veilige keten.

> "Besteed 10 procent van het ICT-budget aan cybersecurity."

Voorbeelden cybercrime

Cybercrime is feitelijk niets anders dan een moderne manier van inbreken. Zo zullen er altijd inbrekers zijn die alle deuren langsgaan om te kijken of er één open is. Met deze sleepnetmethode loopt iedereen kans om slachtoffer te worden. Ook is er een groep hackers die steeds slimmer te werk gaat. Zij maken gebruik van de nieuwste technieken en nemen de tijd om hun hack voor te bereiden. Bij deze hackers is niet de techniek meer de uitdaging, maar wel hoe hij met cybercrime zijn geld verdient en uit handen van politie en justitie blijft. Met de opkomst van cryptocurrency, zoals de bitcoin, wordt het makkelijker om gestolen geld wit te wassen en om onder de radar te blijven. Zo eisen criminelen tegenwoordig vaak losgeld in bitcoins van bedrijven nadat ze met ransomware data hebben gegijzeld.

U laat digitaal allerlei sporen achter, waar cybercriminelen gebruik van maken. Zo kan een hacker informatie verzamelen door het bestuderen van iemands gedrag en interesses op social media. Deelt u op LinkedIn regelmatig kennis over cryptocurrency, dan is de kans groot dat u zelf ook een e-wallet bezit.

Zzp'ers en mkb'ers moeten vooral oppassen voor malware en phishing. Maar ook het gebruik en misbruik van persoonsgegevens (datalekken) wordt een steeds belangrijker aspect van cybersecurity. Een andere trend is dat ondernemers steeds meer 'in de cloud' werken. Daar passen cybercriminelen hun werkwijze op aan. Ze vallen nu direct de cloudsystemen aan in plaats van de computersystemen van een ondernemer.

10 tips voor risicobeperking

De techniek blijft zich ontwikkelen en de criminelen ontwikkelen mee. Daarom is cybercriminaliteit nooit 100 procent tegen te gaan. Toch is er veel wat u kunt doen om het risico te beperken.

Cybersecurity draait om drie pijlers: People, Proces en Techniek. De techniek om risico's zoveel mogelijk te elimineren, is er. Met het opstellen van procedures en protocollen houd u uw systemen veilig. Maar het komt uiteindelijk aan op de mens (people). Deze is vaak de zwakste schakel in de keten. Mensen moeten de procedures naleven, alert blijven en kennis up-to-date houden.

Werk daarom constant aan uw digitale veiligheid, maar laat u ook niet bang maken. Met gezond verstand, veilig gedrag en deze 10 tips komt u een heel eind:

Tip 1. Stel automatische updates in

Zwakke plekken in de software zijn een risicofactor. Door periodiek, liefst automatisch, uw software te updaten kunt u misbruik ervan voorkomen. Doe dit voor alle software op alle systemen in uw bedrijf: in ieder geval voor het besturingssysteem op uw computer(s). Maar vergeet niet ook alle andere software te updaten, zoals op laptops, tablets en smartphones, in apparatuur als routers en firewalls of software van uw website of webshop.

Tip 2. Installeer beveiligingssoftware

U kunt niet zonder goede beveiligingssoftware. Deze houdt veel malware zoals virussen en ransomware buiten de deur. Maar het houdt ook ongewenste binnenkomende en uitgaande netwerkverbindingen tegen. Het beschermt bovendien tegen spam, phishing of onveilige websites. Natuurlijk is het zaak deze beveiligingssoftware altijd up-to-date te houden. Zoek op internet op 'vergelijk beveiligingssoftware' om te bepalen welke variant bij uw bedrijf past.

Tip 3. Gebruik tweestapsverificatie
Het is belangrijk dat u voor alle online diensten een goed wachtwoord kiest. Gebruik dit wachtwoord niet opnieuw bij andere online diensten en wijzig het regelmatig. Toch kan het nóg veiliger met tweestapsverificatie. Dit is bij steeds meer online diensten in te stellen. Een cybercrimineel heeft dan niet meer genoeg aan de gebruikersnaam en wachtwoord, bijvoorbeeld verkregen uit een datalek bij een leverancier van een online dienst. Met tweestapsverificatie is bij het inloggen een extra toegangscode vereist die u ontvangt via een vertrouwd apparaat zoals uw smartphone.

Tip 4. Maak backups
Maak regelmatig backups om verlies van data te voorkomen. Gebruik de 3-2-1 backup-methode. Maak altijd drie kopieën van uw data: minstens twee in het bedrijf en dan op verschillende systemen en minstens één buiten het bedrijf, bijvoorbeeld online. Maak het nog veiliger door deze backups te versleutelen (zie tip 5). Test ook regelmatig of het terugzetten van een backup wel écht lukt.

Tip 5. Beveilig de data
Klantgegevens zoals adressen en facturen kunnen privacygevoelig zijn. Daarom is het belangrijk om die gegevens, maar ook overige bedrijfsinformatie, in kaart te brengen en veilig op te slaan om datalekken te voorkomen. Het is verstandig om dit soort belangrijke gegevens te versleutelen (met een wachtwoord te beveiligen). Sinds 1 januari 2016 bent u verplicht om ernstige datalekken direct te melden bij de Autoriteit Persoonsgegevens. Vanaf 25 mei 2018 geldt de nieuwe privacywetgeving (AVG).

Tip 6. Beveilig draadloze netwerken
Gemak dient de mens. Even het internet op met uw smartphone, tablet of laptop. Dit kan eenvoudig via een draadloze WiFi-verbinding in uw bedrijf. Maar, wie kan het draadloze netwerk (gewenst of ongewenst) nog meer gebruiken? Beveilig uw WiFi-netwerk daarom altijd minimaal volgens de WPA2-standaard. Wees extra alert als u onderweg een openbaar WiFi-netwerk gebruikt. Werk dan altijd via een VPN-verbinding over dit draadloze netwerk.

Tip 7. Maak veilig gebruik van online diensten
We maken allemaal dagelijks gebruik van online diensten (clouddiensten). Denk bijvoorbeeld aan e-mail en online betalen. Ook telewerken is te beschouwen als het gebruik van een online dienst. In al deze gevallen benadert u uw data via het internet. Het is belangrijk dat dit via een beveiligde (VPN-)verbinding gebeurt en dat u tweestapsverificatie hebt ingesteld. Er zijn nog twee zaken om op te letten:

- Telewerken en webmail
  Hierbij hebben werknemers externe toegang tot het bedrijfsnetwerk. Zijn hun thuiswerkplekken net zo goed beveiligd als de werkplekken in het bedrijf?
- Online diensten
  Hoe en waar slaat de leverancier van de dienst uw data eigenlijk op? Kunt u uw data desgewenst eenvoudig meenemen naar een andere leverancier? Vraag dit na bij de diverse leveranciers en verzeker u ervan dat het goed geregeld is.

Tip 8. Houd rekening met de zwakste schakel
Een keten is zo sterk als de zwakste schakel. Helaas is dat bij digitale veiligheid vaak de mens. Uw systemen kunnen nog zo goed beveiligd zijn voor de buitenwereld, maar dan installeert een medewerker opeens onveilige software of steekt hij een onbekende USB-stick in de computer. Maak medewerkers bewust van zaken rondom digitale veiligheid en hanteer een informatiebeleid. Spreek af wie binnen het bedrijf toegang heeft tot welke informatie en leg vast wie verantwoordelijk is voor uitvoering en controle van dat beleid.

Tip 9. Schakel expertise in
Het installeren, beheren en onderhouden van systemen is vakwerk. Schakel altijd een professionele partij in die de ICT en de beveiliging daarvan voor zijn rekening neemt. Wees kritisch want niet elke ICT-leverancier heeft specifieke kennis van digitale veiligheid of ervaring met het tegengaan van cybercrime. Vraag uw ICT-leverancier ook naar een Service Level Agreement (SLA).

'Als ethisch hacker word ik samen met mijn team door bedrijven ingehuurd om in te breken in hun computersystemen en check of er gaten zitten in de beveiliging.' Lees hier de tips en ervaringen van ethisch hacker Stan Hegt.

Tip 10. Blijf ademhalen
Werk constant aan uw digitale veiligheid, maar laat u niet bang maken. Het kan immers nooit 100% veilig zijn. Het gaat om de balans tussen risicobeheersing en gebruiksgemak. Blijf dus rustig ademhalen en geniet van de voordelen die digitalisering en internet met zich meebrengen. Met gezond verstand, veilig gedrag en deze 10 tips komt u een heel eind.

Wees altijd alert op afwijkingen. Een hogere energierekening kan komen doordat uw laptop is gekaapt om bitcoins te minen. Een zakenrelatie die opeens mailt met een ander mailadres kan een phishingmail zijn.

Als u slachtoffer bent van fraude of oplichting, doe dan altijd aangifte bij de politie. Afhankelijk van de situatie kan dat op verschillende manieren.

Fraudehelpdesk

Naast aangifte bij de politie kunt u fraude ook melden bij de Fraudehelpdesk. De Fraudehelpdesk heeft juristen in huis die gespecialiseerd zijn in acquisitiefraude, maar kan u in andere fraudegevallen doorverwijzen naar de juiste instanties en experts.

Ook bij het vermoeden van fraude kunt u contact opnemen met de Fraudehelpdesk. Mogelijk is dit type fraude al bij de helpdesk bekend en kunnen ze u voorzien van nuttige adviseren. Zo voorkomt u slachtoffer te worden. De fraudehelpdesk is te bereiken via www.fraudehelpdesk.nl of telefonisch via 088 -786 73 72.

Onder de nieuwe privacywetgeving (AVG) moeten datalekken gemeld worden bij de Autoriteit Persoonsgegevens (AP). Dit geldt voor lekken waarbij persoonsgegevens van gevoelige aard gelekt zijn. Dit moet bovendien binnen 72 uur gebeuren. Informeer ook altijd direct de betrokkenen.

‘Het gevoel van machteloosheid als je bedrijf in handen van een hacker is, dat wens ik niemand toe.’ Ondernemer Frank Landhuis kreeg in zijn bedrijf te maken met cybercriminaliteit. Lees hier zijn hele verhaal.

Wat doet de KvK met het thema cybersecurity

Wij zien het als onze taak om ondernemers voor te lichten over de risico’s van fraude, de preventie en de maatregelen tegen fraude en cybercrime. En wanneer u getroffen bent door fraude of cybercrime helpen we u met informatie over wat te doen en de te nemen maatregelen. Daarom publiceren we actuele en betrouwbare content op alle eigen digitale kanalen: kvk.nl, ondernemersplein.nl, KvK Connect-app en social media. Ook bieden wij persoonlijke voorlichting en advies via telefoon 088-585 15 85, e-mail, chat en fysieke bijeenkomsten.

Meer weten?

Kijk op www.kvk.nl/cybersecurity

Begrippenlijst

Uitleg van begrippen, die regelmatig gebruikt worden in het kader van cybersecurity

Acquisitiefraude

Acquisitiefraude is een vorm van oplichting waarbij producten worden aangeboden die geen waarde hebben, of kosten in rekening worden gebracht voor diensten die niet zijn geleverd of waarvoor geen opdracht is gegeven.

AVG

De Algemene verordening gegevensbescherming (AVG) is de Europese privacywetgeving die per 25 mei 2018 actief is.

Backup

Een back-up of reservekopie is een kopie van gegevens die zich op een gegevensdrager of binnen een applicatie bevinden om deze te kunnen herstellen mochten ze beschadigd raken. Indien nodig kan een back-up weer op een vergelijkbare originele drager teruggezet worden.

CEO fraude

CEO-fraude is er in verschillende varianten. Vaak ontvangt een medewerker op de financiële administratie van een bedrijf een e-mail van de allerhoogste baas, de CEO of CFO. Deze draagt hem op een fors bedrag over te maken naar een buitenlandse rekening. Ter verificatie van gegevens kan hij een advocatenkantoor bellen. Dit 'advocatenkantoor' zit in het complot.

In een andere variant doen oplichters zich voor als de IT-leverancier met de boodschap dat een geldoverboeking getest moet worden. In werkelijkheid gaat het om een echte overboeking. Ook komt het voor dat brieven worden verstuurd over een nieuwe bankrekening waar betalingen in de toekomst naartoe moeten. Dat is natuurlijk de bankrekening van de oplichter.

Cyberaanvallen

Een cyberaanval is een poging de functies van een computergebaseerd systeem aan te tasten of te schaden. Er zijn vele vormen van cyberaanvallen, waaronder die met malware en ransomware.

Cybercrime

Computercriminaliteit, cybercriminaliteit of cybercrime is criminaliteit met ICT als middel én doelwit Cybersecurity.

Datalekken

Er is sprake van een datalek als persoonsgegevens in handen vallen van derden. Dat zijn personen en organisaties die geen toegang tot die gegevens mogen hebben. Een datalek kan het gevolg zijn een beveiligingsprobleem, of het onzorgvuldig handelen van iemand. In de meeste gevallen gaat het om uitgelekte computerbestanden via een hack of eigen medewerkers. Maar een gestolen laptop of gestolen geprinte klantenlijst kunnen ook een datalek vormen.

DDoS-aanval

Denial-of-service-aanvallen (DoS-aanvallen) en distributed denial-of-service-aanvallen (DDoS-aanvallen) zijn pogingen om een computer, computernetwerk of dienst niet of moeilijker bereikbaar te maken voor klanten. Het verschil tussen een 'gewone' DoS-aanval en een distributed DoS-aanval is dat in het laatste geval de aanval door meerdere computers tegelijk wordt uitgevoerd.

Encryptie
De procedure van het coderen en decoderen van gegevens wordt encryptie genoemd. Dit gebeurt op basis van een bepaald algoritme. Deze versleutelde gegevens kunnen nadien weer gedecrypteerd worden zodat men de originele informatie weer terugkrijgt.

Firewall
Een firewall houdt ongewenste binnenkomende en uitgaande netwerkverbindingen tegen.

Malware
Malware is elke software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen.

NAS – Network Attached storage
Een NAS is een opslagapparaat dat is aangesloten op een netwerk (network-attached storage). Dit apparaat vormt een centrale locatie waar bevoegde netwerkgebruikers en verschillende computers gegevens op kunnen slaan en op kunnen vragen. In feite is het een soort privécloud voor uw kantoor. Het is sneller, goedkoper en heeft precies dezelfde voordelen als een openbare cloud, maar bij een NAS heeft u zelf de totale controle.

Pen(etratie)test
Een penetratietest of pentest (binnendringingstest) is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om in deze systemen in te breken. De persoon die een penetratietest uitvoert wordt vaak een ethische hacker genoemd.

Phishing
Phishing is een vorm van internetfraude. Het bestaat uit het oplichten van mensen door ze te lokken naar een valse (bank)website, die een kopie is van de echte website, om ze daar – nietsvermoedend – te laten inloggen met hun inlognaam en wachtwoord of hun creditcardnummer.

Ransomware
Ransomware is een chantagemiddel en wordt om die reden ook vaak gijzelsoftware genoemd. Ransomware is malware die een computer en/of gegevens die erop staan blokkeert en vervolgens van de gebruiker geld vraagt om de computer weer te ‘bevrijden’.

Service Level Agreement (SLA)
Een Service Level Agreement (SLA) is een contract tussen de leverancier en klant waarin de kwaliteit van de diensten die worden geleverd staat beschreven. Dankzij een SLA is een afnemer op de hoogte van de invulling en kosten van de diensten die hij inkoopt en kan de leverancier erop worden afgerekend als hij niet de afgesproken kwaliteit levert.

Social engineering
Social engineering of social hacking, is een techniek waarbij een computerkraker een aanval op computersystemen tracht te ondernemen door de zwakste schakel in de computerbeveiliging, namelijk de mens, te kraken.

Tweestapsverificatie
Bij tweestapsverificatie wordt behalve uw vertrouwde wachtwoord, een extra middel gebruikt ter identificatie. Dit middel is alleen in uw bezit, zoals een sms die naar een telefoon wordt gestuurd, of een e-mail naar een mailadres dat bij u hoort. Een gevonden of gestolen wachtwoord alleen is dan niet meer genoeg om oneigenlijk toegang te krijgen tot uw gegevens.

Virusscanner

Deze software probeert computervirussen te identificeren, tegen te houden en te verwijderen.

VPN-verbinding

VPN staat voor virtual private network. In de praktijk betekent dit dat er een privénetwerk van computers gecreëerd kan worden met de infrastructuur van een publiek netwerk. Over het internet wordt dan een versleutelde beveiligde verbinding gemaakt tussen verschillende lokale netwerken en/of computers. Hierdoor is het mogelijk om op een veilige manier data uit te wisselen.