Whitepaper

Houd cybercriminelen buiten de deur

PinkWeb

Share. Care. Anywhere.

PinkWeb
Share. Care. Anywhere.

Whitepaper

Houd cybercriminelen buiten de deur

‘Your files have been encrypted! To decrypt the files, follow these instructions…’ Het is het schrikbeeld van elk bedrijf; op een dag ontdekken dat cybercriminelen het netwerk zijn binnengeglipt. Het systeem ligt plat, data van klanten zijn in handen van kwaadwillenden. Er wordt misschien een grote som geld geëist. Cybercriminaliteit is momenteel één van de grootste uitdagingen voor mkb-kantoren. Hackers worden professioneler en opereren vaker in georganiseerd verband.

Neem de dreiging serieus. Laat tegelijkertijd de angst niet regeren. Met een aantal basismaatregelen en goede ICT-hygiëne houd je cybercriminelen op afstand en blijft de schade beperkt als het toch misgaat. Honderd procent veilig ben je immers nooit. Lees in deze whitepaper hoe ook jouw kantoor de basis op orde krijgt en waarom je met goede en veilige software weerbaarder bent tegen het digitale inbrekersgilde.

Houd cybercriminelen buiten de deur

Inhoud

Cyberaanval
Dagelijks worden 42 bedrijven aangevallen

Datalek
70% van de datalekken ontstaat door menselijke fout

Failliet
60% van de bedrijven die wordt gehackt, gaat binnen 6 maanden failliet door verloren productietijd

Kans op
De kans op een cyberaanval is 1 op 5, de kans op een fysieke inbraak is 1 op 250, de kans op brand is 1 op 8000

De toename van het aantal cyberincidenten is zorgwekkend. Daarbij worden mkb-bedrijven vaker slachtoffer, ook in de accountancysector. Wat zijn de trends en ontwikkelingen? Laat de cijfers een wake-up call zijn (als je nog niet wakker was).

Losgeld
Ransomware is meest voorkomende cyberincident, gemiddeld wordt 2 tot 5 % van de jaaromzet aan losgeld geëist

Stilstand
10 dagen is de gemiddelde bedrijfsstilstand na een cyberaanval

Gemiddelde schade
300.000 euro is de gemiddelde schade bij een cyberincident

Hoofdstuk 1 Trends en ontwikkelingen in cyberland; een wake-up call

Ons leven is een stuk makkelijker geworden dankzij digitalisering: we winkelen online, boeken met een paar swipes onze vakantie en regelen onze bankzaken en administratie digitaal. Ook ondernemen werd een stuk efficiënter. Zo'n driekwart van de accountancykantoren heeft zijn processen en klantcontact min of meer gedigitaliseerd.
Maar er is een keerzijde: het zekerstellen van onze veiligheid is complexer geworden. Terwijl kostbaarheden vroeger achter slot en grendel lagen, opereren criminelen nu op afstand en anoniem. De impact is vele malen groter. Hackers kunnen vitale sectoren ontregelen, zoals de stroomvoorziening of het openbaar vervoer. Een crimineel die het netwerk van een bedrijf binnendringt, kan het systeem platleggen en aan de haal gaan met gevoelige informatie.

Verontrustende groei

Cybercriminaliteit neemt elk jaar verontrustend toe. Het is wereldwijd de snelst groeiende vorm van misdaad. Volgens diverse onderzoeken is cybercriminaliteit inmiddels lucratiever dan de internationale drugshandel. Ook in Nederland is de schade fors, cybercriminaliteit kost het bedrijfsleven vele miljarden euro's. De dreiging blijft zorgelijk, stelt het Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Organisaties worden weliswaar weerbaarder tegen cybercriminelen, maar dat gaat langzamer dan de toenemende dreiging.

ABN Amro constateert dat het aantal bedrijven dat te maken kreeg met een cyberaanval in 2022 sterk steeg. De bank ondervroeg 233 bedrijven. In 2021 had 29% last van cybercriminelen, dit jaar is het 45%. Vooral bedrijven met meer dan 10 miljoen euro omzet kregen het afgelopen jaar vaak te maken met cyberaanvallen: zo'n 63%. In het mkb kreeg 33% bezoek van cybercriminelen. De onderzoekers verklaren de toename door de groeiende digitalisering. Als gevolg van corona wordt er vaker thuisgewerkt en ligt er minder prioriteit bij informatiebeveiliging.

Nederland: een paradijs voor hackers

Ook weinig opbeurend: Nederland is opvallend geliefd bij cybercriminelen vanwege snelle en betrouwbare internetverbindingen. Daarnaast worden ook veel websites gehost in Nederland, het Amsterdamse AMS-IX-knooppunt is een van de grootste internetknooppunten ter wereld. Nederland is een van de meest gedigitaliseerde landen en dat trekt cybercriminelen aan.

Cybercriminelen professioneler

Een hacker is allang niet meer de whizzkid die op een zolderkamertje op eigen houtje aan het hacken is. Tegenwoordig spreken we over criminelen, deze cybercriminelen worden professioneler. Ze zijn steeds vaker georganiseerd in internationale netwerken en communiceren op ondergrondse fora. Met geautomatiseerde software richten ze hun pijlen op gaten in de digitale netwerken van organisaties. Er is bovendien een levendige handel ontstaan in kant-en-klare-pakketten. Dankzij deze Cybercrime-as-a-Service (CaaS) kunnen criminelen zonder enige digitale kennis inbreken en hun slag slaan. Kortom, er is een volwassen industrie ontstaan, die steeds groter wordt.

Accountantskantoren onderschatten risico's

Ondanks de toenemende dreiging, onderschatten veel mkb-bedrijven de risico's van cybercriminaliteit. De helft van de mkb-bedrijven heeft geen actueel stappenplan klaarliggen, blijkt uit onderzoek van verzekeraar Allianz. Daarnaast heeft maar één op de drie ondernemers kennis in huis om de onderneming te beschermen tegen cybercriminelen. In de accountancysector is het beeld wisselend. Er zijn kantoren waar het onderwerp hoog op de agenda staat, maar er zijn genoeg kantoren die hun kop in het zand steken, en denken: ik ben niet interessant genoeg. 'Onterecht', stelt Marvin Jansen van Visma | PinkWeb. 'Natuurlijk valt er bij grote bedrijven meer te halen. Maar veel mkb-ondernemers hebben nu de digitale achterdeur openstaan en zijn zo een makkelijk doelwit. Cybercriminelen scannen continu op zwakke plekken in ICT-sytemen. Zorg dat je niet bij die groep hoort. Hoe hoog staat het onderwerp bij jou op de agenda?'

‘Zorgvuldig omgaan met klantgegevens is een morele en wettelijke plicht voor accountants’

Marvin Jansen

Cybersecurity (nu nog) een USP

Vooral accountantskantoren mogen de ogen niet sluiten voor de risico’s van cybersecurity, vindt Jansen. ‘Je verwerkt data van klanten, daarmee heb je morele en wettelijke plichten om netjes met deze persoonsgegevens om te gaan. Een kantoor wekt vertrouwen en toont professionaliteit als het zorgvuldig met gegevens omgaat en op de meeste veilige manier gegevens uitwisselt.’ Jansen meent dat kantoren zich nu nog kunnen onderscheiden in de markt als zij op een zorgvuldige manier omgaan met klantgegevens. ‘Nog niet alle kantoren hebben informatiebeveiliging namelijk op orde. Het is nu nog een USP, maar in de toekomst zal het de norm zijn.’ Waar volgens Jansen kansen voor verbetering zijn? ‘Medewerkers zetten bijvoorbeeld de tweefactorauthenticatie uit omdat het zo omslachtig is. Natuurlijk, gaat veiligheid ten koste van gebruiksgemak. Maar dat is met een urgente reden.’

Azen op persoonsgegevens

Cybercriminelen richten zich daarbij steeds vaker op het stelen van persoonsgegevens, constateert de Autoriteit Persoonsgegevens. De privacywaakhond registreerde vorig jaar 25.000 datalekken. Daarvan ontstond 9% door cyberaanvallen. Een jaar eerder was dat nog 5%. De schade voor kantoren is vaak fors. Cybercriminaliteit kan een organisatie dagen platleggen, gegevens kunnen verloren gaan. Daarnaast schaadt het klantenrelaties met je klanten en de reputatie van kantoren als blijkt dat je niet zorgvuldig omgaat met gevoelige informatie en kun je rekenen op boetes van de Autoriteit Persoonsgegevens. Sinds 2016 zijn ondernemers verplicht datalekken te melden aan AP.

Ransomware en phishing favoriet

Zorgelijk is bovendien dat cybercriminelen tegenwoordig vaker losgeld eisen. Met behulp van ransomware versleutelen kwaadwillenden software en gegevens, ze dreigen vertrouwelijke informatie openbaar te maken of door te verkopen als je niet betaalt. Dankzij de introductie van de Bitcoin is het voor cybercriminelen makkelijk om snel en relatief anoniem geld te ontvangen. Jansen: ’Het advies van de overheid is niet te betalen om dieven te ontmoedigen, maar als de bedrijfscontinuïteit in het geding is, trekt een ondernemer soms toch zijn portemonnee.’ Favoriet blijft ook phishing - via een link in een e-mail ‘hengelen’ naar persoonlijke gegevens. Een op de vijf medewerkers klikt op zo’n gevaarlijke link. ‘Deels komt dat doordat phishingmails niet langer vol fouten staan; ze worden steeds echter’, weet Jansen. Tenslotte blijven DDoS aanvallen populair in het bedrijfsleven. Cybercriminelen sturen ontzettend veel verkeer naar een computernetwerk. Hierdoor wordt het netwerk overbelast en onbruikbaar.

Materiële en immateriële schade groot

De schade kan fiks zijn als cybercriminelen je accountantskantoor binnendringen. Je organisatie ligt misschien dagenlang plat, dat alleen al kost flink wat geld. Maar misschien moet er ook veel werk opnieuw gedaan worden als je niet onlangs nog back-ups hebt gemaakt. Als je pech hebt, wordt er bovendien een flinke som losgeld geëist. Cybercriminelen hebben je gegevens gegijzeld, die je pas terugkrijgt als je bitcoins overmaakt. De gemiddelde som losgeld ligt tussen de 2 en 5% van de jaaromzet, volgens cijfers van de Rabobank.

Maar naast de materiële schade loop je als accountantskantoor immateriële schade op. Je verwerkt immers privacygevoelige gegevens van de klant. Het vertrouwen loopt een deuk op als bekend wordt dat data mogelijk in verkeerde handen is gekomen. Je loopt vooral imagoschade op als blijkt dat je informatiebeveiliging niet serieus nam.

Hoofdstuk 2 Zorg dat de basis op orde is

De dreiging van cybercriminaliteit zal alleen maar toenemen. Je kunt veel leed voorkomen als enkele triviale zaken op orde zijn. Zorg tegelijkertijd dat cybersecurity leeft op kantoor. 'Je kunt technisch alles hebben geregeld, als medewerkers onvoldoende alert zijn, gaat het alsnog mis', aldus Harmen Thiewes, Information Security Officer van Visma | PinkWeb.

Veel cyberaanvallen zijn te voorkomen als bedrijven enkele basiszaken regelen. De crimineel rammelt weliswaar aan de deur, maar probeert het elders als het teveel moeite kost. Dit zijn de 10 basismaatregelen.

1. Inventariseer kwetsbaarheden;

Breng in kaart waar de meest waardevolle (klant)gegevens van jouw bedrijf zich bevinden en hoe goed deze beveiligd zijn. Een accountantskantoor heeft vaak verschillende applicaties waarin grote hoeveelheden gevoelige data worden verwerkt. Denk aan bankrekeningen, salarissen, fiscale gegevens voor de aangifte inkomstenbelasting en BSN/RSIN-nummers. Breng ook de technische afhankelijkheid van leveranciers in kaart. Denk na wat het betekent als een bepaalde applicatie wordt geraakt.

2. Voer altijd updates uit

Houd besturingssystemen en programma's altijd up-to-date. Schakel indien mogelijk de optie in om updates automatisch te installeren. Software veroudert als je geen updates doet; cybercriminelen zoeken voortdurend naar kwetsbaarheden in verouderde software en kunnen zo binnenkomen. In het geval van cloud software word je hierin ontzorgt door de leverancier. Als je apparaten en software up-to-date zijn, loopt je bedrijf minder risico op virussen en cyberaanvallen.

3. Word weerbaarder tegen virussen en kwaadaardige software

Malware, ofwel kwaadaardige software, verstoort, verzamelt of versleutelt informatie. Zorg dat malware niet in computers, smartphones of netwerken belandt. Zodra de malware binnen is, infecteert het andere apparaten of gebruikers. Het is zo gebeurd: een medewerker kan een geïnfecteerde e-mail of bijlage openen, een foute website bezoeken of een USB-stick gebruiken met een besmet bestand. Er zijn vier maatregelen om malware te voorkomen: Stimuleer veilig internetgedrag van collega's, gebruik een antivirusprogramma, download apps veilig en beperk de installatiemogelijkheden van software. Je kunt niet voorkomen dat het een keer gebeurt, maar je kunt het risico op virussen en kwaadaardige software wel verkleinen.

4. Gebruik sterke wachtwoorden

Om in te loggen op de systemen is het raadzaam sterke wachtwoorden te gebruiken, die niet makkelijk te achterhalen zijn. Welkom01 of 0000 zijn bijvoorbeeld geen goed idee. 'Het is een veelgebruikte misvatting rondom wachtwoorden en veiligheid om regelmatig je wachtwoord te veranderen. Regelmatig veranderen is niet aan te raden, het gevaar bestaat dat medewerkers gaan variëren met enkel cijfers.', ervaart Thiewes. 'Welkom01 wordt dan al snel Welkom02. Het beste is om gebruik te maken van een goede wachtwoordmanager in combinatie met tweefactorauthenticatie. Deze genereert een sterk wachtwoord, die automatisch wordt opgeslagen. Zo hoeft de gebruiker zijn wachtwoord niet zelf te onthouden en ben je goed beschermd tegen misbruik.'

5. Gebruik tweefactorauthenticatie.

'Uit de praktijk blijkt dat veel medewerkers binnen accountantskantoren geen gebruik maken van tweefactorauthenticatie.

Het wordt vaak ervaren als ongebruiksvriendelijk en lastig.' aldus Thiewes. Er is vaak geen beleid rondom tweefactorauthenticatie. Accountantskantoren moeten het gebruik van tweefactorauthenticatie verplichten waar mogelijk. Medewerkers moeten periodiek worden gecontroleerd op het gebruik van tweefactorauthenticatie en het belang moet constant worden toegelicht. Door tweefactorauthenticatie te gebruiken beperk je het risico dat er toegang verkregen wordt met gestolen of gehackte inloggegevens.

6. Maak - en houd - medewerkers bewust van de cyberrisico's

'Je kunt alles technisch tot in de puntjes geregeld hebben, medewerkers moeten voldoende alert zijn op verdachte mails, telefoontjes of whatsapp-berichten. Vertel ze regelmatig hoe en waarom ze zorgvuldig omgaan met de bedrijfslaptop. Blijf hameren op het belang van tweefactorauthenticatie en veilig uitwisselen van gegevens.' Thiewes heeft nog een tip: 'Stuur eens zelf een nep-phishingmail uit en ontdek hoeveel collega's toch op gevaarlijke links klikken. Zorg daarnaast dat het regelmatig aandacht heeft. Als partner of eigenaar van het kantoor is het belangrijk het onderwerp uit te dragen en natuurlijk zelf het goede voorbeeld te geven.'

7. Gebruik de cloud als digitale kluis

Bewaar en beheer de meest gevoelige data in de cloud. Dat is veiliger dan op lokale servers. Softwareleveranciers hebben de kennis en kunde om de clouddienst voortdurend te bewaken, zij zorgen voor een goed slot op de digitale kluis. Zorg dat je ook weet hoe de veiligheid bij je softwareleverancier(s) is geborgd.

8. Beperk toegang

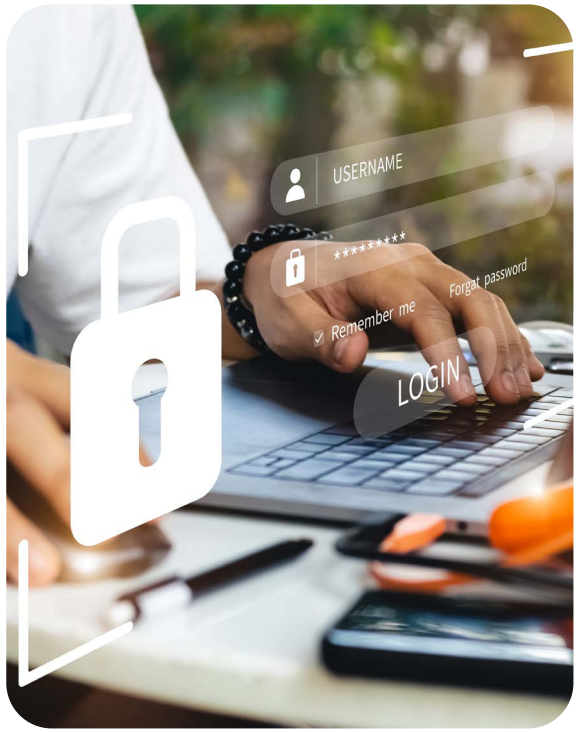
Denk goed na welke medewerker je toegang geeft tot welke data en systemen. Geef medewerkers alleen toegang tot data en systemen die nodig zijn voor het uitvoeren van hun taak. Zo beperk je de handelingen die een aanvaller kan uitvoeren indien deze zich toegang verschaft tot een account.

9. Krijg grip op belangrijke back-ups

Maak inzichtelijk wanneer en waar back-ups worden gemaakt. Ontwikkel een schema zodat je precies op de hoogte bent wanneer en in welke software applicaties back-ups worden gemaakt. Maar controleer ook waar deze bewaard worden. Controleer hoe software leveranciers omgaan met het maken en bewaren van back-ups. Als er iets misgaat, beschik je over de meest recente gegevens. Maak ook back-ups van je netwerk en systemen. Bewaar deze in de cloud, als een digitale kluis. Controleer periodiek of backups compleet zijn en teruggezet kunnen worden.

10. Kies voor de cloud en wees kritisch op ICT-leverancier

Veel kantoren maken gebruik van eigen servers voor hun boekhoud- en aangifteprogramma's. 'Dat maakt je als ondernemer kwetsbaar', zegt Security Officer Thiewes. 'Zeker mkb-bedrijven hebben niet altijd de middelen en kennis om de veiligheid te waarborgen. Het is daarom raadzaam om gebruik te maken van een clouddienst. Maar ga wel in gesprek met de betreffende ICT-leverancier hoe het bedrijf cybersecurity borgt', benadrukt Thiewes. 'Ook al ben je niet thuis in de materie, er bestaan checklists waarmee je een softwarepartner kunt ondervragen. Beschikt de leverancier over veiligheidscertificaten? Hoe ziet de beveiligingsstrategie eruit? Dat zijn belangrijke vragen, die al in de acquisitiefase gesteld moeten worden.'



Hoofdstuk 3 Honderd procent veilig bestaat niet; Zorg voor een calamiteitenplan

Wen maar aan het idee: vroeg of laat zullen cybercriminelen toch binnen weten te dringen. Bereid je daarom voor met een calamiteitenplan. Zo voorkom je paniek en beperk je de schade.

Een traag netwerk of helemaal niet meer kunnen inloggen. Een zwart scherm met een doodshoofd of de onheilspellende boodschap dat je 'files have been encrypted'. Ga ervan uit dat je bedrijf vroeg of laat een keer doelwit wordt van cybercriminelen. 'Als je een draaiboek hebt klaarliggen en vooraf hebt nagedacht over dit scenario kun je de schade beperken', weet Information Security Officer Harmen Thiewes van Visma | PinkWeb.

Communicatie is het allerbelangrijkst op het moment van een cyberincident. 'Wie is het eerste aanspreekpunt, welke collega's en externe partijen moeten worden geïnformeerd? Wie brengt het personeel op de hoogte? Hoe breng je het nieuws naar buiten? Wie doet aangifte bij de politie en informeert de Autoriteit Persoonsgegevens in geval van een datalek? Wees transparant naar buiten toe', adviseert Thiewes. 'Lange tijd hebben gehackte bedrijven het onder het tapijt willen vegen, uit angst voor imagoschade. Doe dit niet; gedupeerden hebben het recht te weten dat ze risico lopen door een datalek bij jouw bedrijf. Gelukkig zijn steeds meer bedrijven open over een cyberincident en informeren ze leveranciers en klanten om hen te waarschuwen voor mogelijk gevaar.'

Wat staat er in een ICT-calamiteitenplan?

Het is raadzaam een calamiteitenplan te maken. Zo ben je voorbereid bij een cyberincident, heb je de juiste gegevens bij de hand en weet je welke stappen je moet nemen om het netwerk weer snel in de lucht te krijgen.

1. Een inventarisatie van de ICT-infrastructuur.
Hierin staan alle gegevens over servers, pc's maar ook je internetverbinding. Maar ook informatie over het telefoonnetwerk en randapparatuur, zoals printers en scanners, mag niet ontbreken.

2. Zorg dat je een crisisteam paraat hebt staan.
Denk na over welke personen binnen je organisatie bij elkaar wilt hebben in het geval van een calamiteit. Dan hoef je daar op het moment zelf niet over na te denken. Het helpt ook om met dit team periodiek de plannen door te nemen en te controleren op actualiteit.

3. Een analyse van de bedrijfsprocessen.
Hierin staat per afdeling wie de verantwoordelijke medewerkers zijn, welke systemen en data zij nodig hebben om te functioneren. Maak onderscheid tussen noodzakelijke systemen (die met spoed zou moeten herstellen) en minder essentiële systemen (waaraan je later zou kunnen werken).

4. Maak een overzicht van je back-ups
Weet waar back-ups van bestanden, systemen en je netwerken te vinden zijn in de cloud. Zorg ervoor dat je op elk tijdstip toegang tot je (goed versleutelde) data hebt.

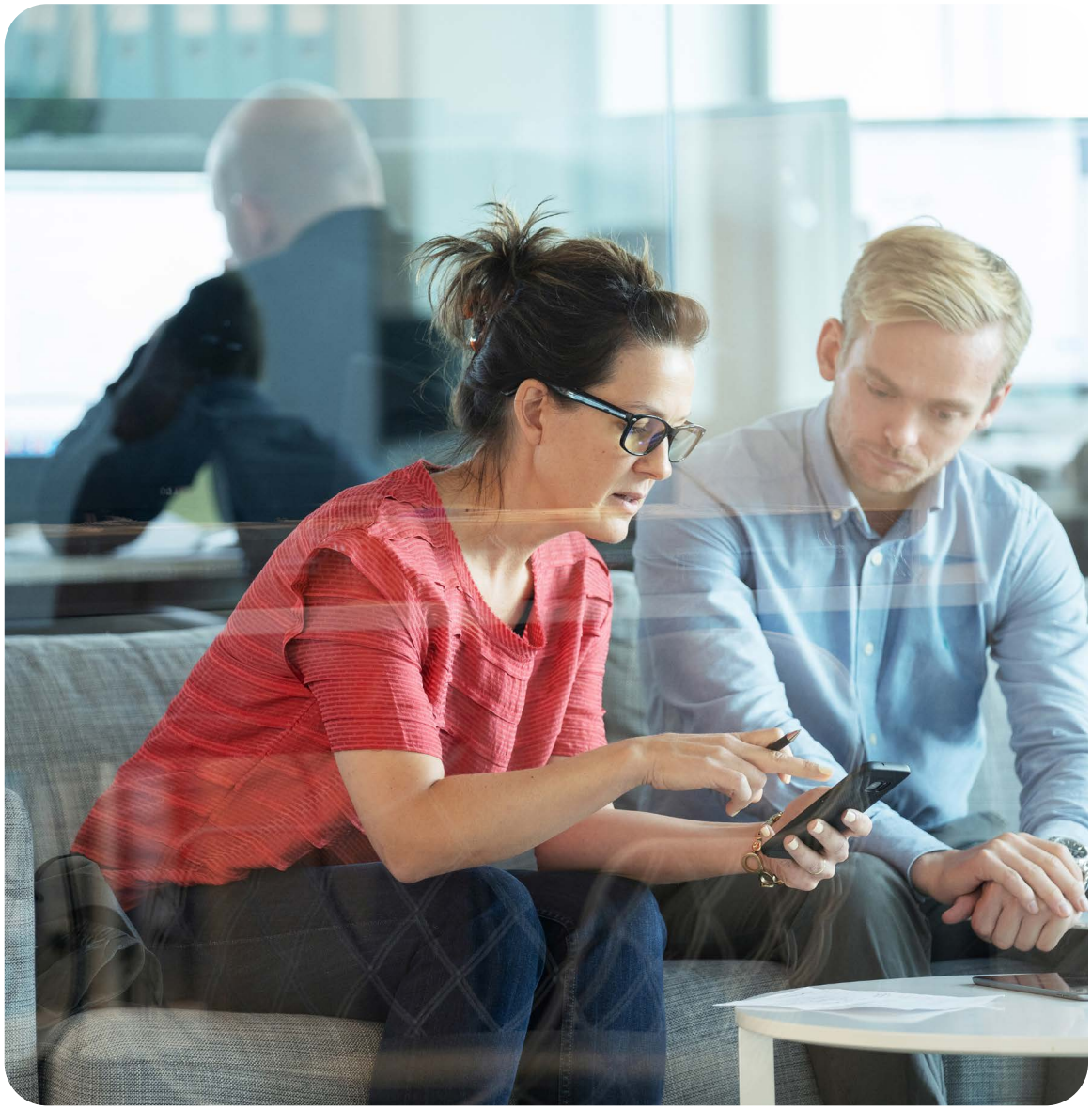
5. Een hersteldraaiboek
Welke acties zijn nodig om je bedrijf na een cyberincident op te kunnen starten? Welke personen en partijen informeer je? Wat is je uitwijklocatie en hoe kom je aan vervangende hardware? Bepaal de volgorde waarin je het herstel laat plaatsvinden. Bedrijfskritische systemen komen eerst.

Actualiseer regelmatig

Omdat de IT-infrastructuur voortdurend verandert, is het ook nodig om het IT-calamiteitenplan regelmatig te actualiseren. Kijk regelmatig kritisch naar onderdelen van het plan en test de plannen periodiek.

Is er sprake van een datalek?

Ga na of er sprake is van een datalek. Daarvan is sprake als er persoonsgegevens verloren zijn gegaan bij een beveiligingsincident. Sinds 2016 bestaat de meldplicht datalekken bij de Autoriteit Persoonsgegevens. Dit moet ‘zonder onredelijke vertraging’, maar uiterlijk binnen 72 uur gebeuren. Ook betrokkenen, van wie de gegevens mogelijk in verkeerde handen zijn gekomen, zul je moeten informeren. Bijvoorbeeld als je direct passende maatregelen hebt getroffen waardoor gelekte persoonsgegevens onbegrijpelijk zijn geworden voor onbevoegden.



Hoofdstuk 4 Do's en don'ts voor het veilig uitwisselen van gegevens met klanten

Om te voorkomen dat (cyber)criminelen gevoelige informatie stelen, is het voor elk accountantskantoor essentieel zorgvuldig om te gaan met klantgegevens. Dat betekent niet alleen dat je informatie goed beschermd bewaart, maar ook dat je gegevens veilig uitwisselt met klanten en instanties. Wat zijn de do's en don'ts?

Don't - Vergeet de schoenendoos

Nog altijd leveren veel klanten hun administratie aan in een schoenendoos of plastic tas, met de mededeling: 'Kijk maar wat je kunt gebruiken'. Voor accountants is dit niet zonder risico. Stel dat de doos wordt gestolen of kwijtraakt: dan weet je niet wat je in huis had. Bespreek met de ondernemer of hij de papieren bonnen via een beveiligde software applicatie kan aanleveren.

Don't - Stop met mailen van vertrouwelijke informatie

Gevoelige informatie versturen via e-mail is een absolute don't. Het mailen van bsn-nummers, een kopie van een paspoort, een loonstrook, jaarrekening of andere gevoelige informatie is simpelweg niet veilig. Toch gebeurt het nog altijd op accountantskantoren. Het medium is makkelijk en snel, maar helaas ook kwetsbaar. Zo'n 40 procent van alle datalekken komt door verkeerd en onjuist mailverkeer. De AVG, waar elk accountantskantoor aan moet voldoen, keurt het gebruik niet af, maar adviseert vertrouwelijke inhoud te versleutelen. Het beste is echter om gegevens via een veilig portaal te delen.

Don't -Voorkom gebruik van gratis clouddiensten

Ook het uitwisselen van documenten via een gratis clouddienst als WeTransfer is geen goed idee. Het kan gebeuren dat je bij het uploaden van het bestand per ongeluk een verkeerd e-mailadres invult: de downloadlink blijft dan een bepaalde periode beschikbaar en het bestand is uitleesbaar voor iedereen met de link. Bovendien zijn dergelijke diensten gratis omdat ze gegevens verkopen aan derden voor marketingdoeleinden.

Do - Kies voor een klantenportaal

Een belangrijk voordeel van een klantenportaal zijn de integraties. Vanuit je lokale dossier, Sharepoint, CRM of DMS deel je een document met 1 klik op de knop. Minder kans op fouten, gegarandeerd gedeeld met de juiste cliënt of relatie en persoon. En andersom: klanten leveren veilig documenten en informatie aan in het portaal. Deze komen geautomatiseerd op de juiste plek in je eigen dossier. De meest veilige en gebruiksvriendelijke manier om gegevens en documenten uit te vragen, te delen en te ondertekenen is via een klantenportaal. In deze digitale omgeving kunnen accountantskantoren en klanten volgens de hoogste veiligheidsnormen samenwerken en documenten uitwisselen. Controleer bij de softwareleveranciers op welke manier zij de informatiebeveiliging waarborgen en wat zij doen om cybercriminelen buiten de deur te houden. Ook klanten zullen een hoge mate van veiligheid ervaren. Ze krijgen immers met een unieke login toegang tot informatie die alleen voor hen bestemd is. De klant heeft zo zelf controle over zijn gegevens. Pluspunt is bovendien dat informatiestromen naar uitvragende partijen zoals bijvoorbeeld de Belastingdienst, de Kamer van Koophandel en banken geautomatiseerd en veilig plaatsvinden.

Do - Voed de klant op

Je kunt als kantoor weliswaar afspreken geen financiële cijfers of documenten te versturen per mail, de klant staat er misschien minder bij stil. Informeer hem of haar over de risico's en wijs op de voordelen van samenwerken in een klantenportaal. Nodig eens verschillende ondernemers uit om te vertellen over samenwerken in een klantenportaal en hoe veel veiliger dit is.

Do - Beperk rechten en rollen

Wees kritisch op wie je toegang geeft tot welke informatie en ook welke rechten je collega's toekent. Collega's op kantoor hebben verschillende taken en expertises, pas de rechten en functionaliteiten binnen het klantenportaal daarop aan. Misschien ben jij tekeningsbevoegd, maar je collega (nog) niet. Je collega hoeft dan geen autorisatie te hebben om documenten te kunnen ondertekenen. Door de toegang te beperken - ook aan klantzijde - wordt het risico op verlies van vertrouwelijke gegevens kleiner. Cybercriminelen die een account hebben gehackt, kunnen zo niet zomaar bij alle informatie komen. Nog een tip: vergeet bij het vertrek van collega's ook niet om deze accounts met rechten stop te zetten.

Hoofdstuk 5 Interview ACA-IT. Gegijzeld - hoe ziet een hersteloperatie eruit?

Al meer dan 15 jaar houdt Michael Waterman zich bezig met cybersecurity. Aanvankelijk bij softwarereus Microsoft, tegenwoordig bij het Eindhovense ict-bedrijf ACA IT Solutions. Als securityspecialist maakte hij vele cyberincidenten en hersteloperaties mee, zag stoere ondernemers huilen. 'De impact is onvoorstelbaar groot.' Welke lessen heeft Waterman voor mkb-accountantskantoren?

Michael Waterman was negen jaar lang cybersecurity engineer bij Microsoft, reisde de hele wereld over en vergaarde veel kennis over informatiebeveiliging. Vier jaar geleden stapte hij over naar ACA IT Solutions, een Eindhovens ICT-bedrijf dat mkb-bedrijven adviseert over cybersecurity-vraagstukken. De eerste jaren in Nederland waren een behoorlijke realitycheck voor Waterman. 'Ik was bij Microsoft de hoogste beveiligingsniveaus gewend. Bij mijn eerste contacten met mkb-klanten dacht ik: onder welke steen hebben jullie de afgelopen 15 jaar geleefd? Bedrijven wisten nauwelijks welke risico's cybersecurity met zich mee brengt. De ICT-systemen waren vaak een grote gatenkaas.' Waterman kan het wel verklaren: 'Tot 2018 bleef de mkb-sector redelijk gespaard. Cybercriminelen vielen vooral grotere organisaties aan. Maar dat veranderde toen grotere bedrijven zich steeds beter konden weren. Bovendien werden er op het Darkweb*, de digitale onderwereld, relatief goedkope tools verkocht waarmee ook criminelen zonder ICT-kennis hun slag konden slaan.' Waterman spreekt liever niet van 'hackers'. 'Dat klinkt te romantisch; het zijn geen amateurs meer die op zolderkamers wat uitproberen. Het zijn criminelen die in de echte wereld een pistool op je hoofd zouden zetten.' De impact is enorm: 'Ik heb stoere ondernemers zien huilen als kleine jongens omdat ze werden afgeperst. Het incident werkte door op hun gezinnen, collega's en klanten.'

Flink aan de bak

Menig mkb-bedrijf klopte inmiddels bij ACA IT Solutions aan voor een preventieve aanpak. Maar ook assisteerde het bedrijf al menig keer bij een cyberincident. Waterman die als manager cybersecurity een team van specialisten aanstuurt, schetst hoe dat gaat: 'Vaak begint het met een belletje midden in de nacht of in het weekend. Het calamiteitenplan wordt uit de kast gehaald: pas dan zal blijken of de procedures die vooraf zijn bedacht, ook werken. Er wordt in allerijl een crisisteam gevormd, met it-mensen, directieleden en externe specialisten. Softwareleveranciers en verzekeringsmaatschappij(en) moeten worden gebeld. Collega's en klanten worden geïnformeerd.'
Voordat het crisisteam aan de slag gaat, wordt meestal een digitaal forensisch bedrijf, zoals bijvoorbeeld het in Nederland gevestigde Northwave, ingeschakeld. 'Hooggekwalificeerde specialisten onderzoeken hoe ernstig systemen zijn geraakt en of er informatie is gestolen. En of - onverhoopt - backups niet zijn geraakt. Dat gebeurt door analyse van log-bestanden. Het is fenomenaal wat deze forensische onderzoekers boven water krijgen', aldus Waterman.
Als de diagnose duidelijk is, moeten techneuten flink aan de bak. Alle getroffen apparatuur en netwerken moeten worden opgeschoond. Dat is volgens Waterman een intensief proces. 'Met sommige hardware ben je een paar uur bezig, maar als er veel data op staan, kan het zomaar dagen duren. Getroffen bedrijven moeten daarbij de afweging maken welke processen voor hen het belangrijkst zijn. Het is bij cyberincidenten al heel knap als je binnen een week bepaalde bedrijfsprocessen - zoals de e-mailfunctie - weer kunt starten. Of binnen twee weken het bedrijf weer kan laten draaien.'

* Het Darkweb is een deel van het internet dat niet vindbaar is voor zoekmachines. Cybercriminelen gebruiken het voor hun illegale activiteiten.

Voorkom spookverhalen

Bij de verschillende cyberhersteloperaties die Waterman van nabij meemaakte, leerde hij een aantal belangrijke lessen. ‘De focus ligt op het zo snel mogelijk laten draaien van een organisatie. Vaak wordt vergeten welke impact het heeft op de mensen die erbij betrok-

‘Zorg dat dieven niet zomaar kunnen doorstoten naar je kroonjuwelen’

Michael Waterman

ken zijn. Ze maken weken van soms 16 uur per dag. Er drukt een zware verantwoordelijkheid op hun schouders. In het begin draaien medewerkers op adrenaline, maar op een gegeven moment hakt de stress er enorm in. Ik heb meegemaakt dat collega’s na de hersteloperatie thuis kwamen zitten met een burnout.’ Voor de directie van een geraakt bedrijf is het volgens Waterman raadzaam om vanaf de zijlijn betrokken te blijven. ‘Je kunt niet veel doen, de techneuten moeten het werk doen. Steun ze door bijvoorbeeld koffie te halen of ze van broodjes te voorzien.’ Wat daarnaast heel belangrijk is: ‘Vergeet je medewerkers niet te informeren. Als je als ICT-manager of directeur in het crisisteam zit, weet je wat er speelt. Het is belangrijk relevante informatie regelmatig te delen. Bijvoorbeeld via Whatsapp-groepen als de e-mail nog niet werkt. Voorkom dat er spookverhalen rondgaan. Collega’s willen weten of ze nog een baan hebben of het bedrijf niet failiet gaat.’

Data isoleren

De cybersecurityspecialist benadrukt dat het een illusie is te denken dat je niet interessant bent of niet geraakt gaat worden in deze tijd. Daarom is het - zeker voor accountantskantoren - een must om informatie zo goed mogelijk te beveiligen. ‘Cybercriminelen zijn erop uit om je af te persen. Dat doen ze op diverse manieren. Allereerst door data te versleutelen, maar ze zullen ook proberen om gegevens - van klanten of van medewerkers - te kopiëren. Ze dreigen om deze op het Darkweb te zetten als je niet betaalt. Dat wil je niet.’ Een belangrijke boodschap daarbij is: zorg dat je netwerk uit verschillende compartimenten bestaat. ‘Zorg dat dieven niet zomaar kunnen doorstoten naar je kroonjuwelen. Er zijn technologieën die ervoor zorgen dat data geïsoleerd blijven en dat een geïnfecteerde laptop van een medewerker niet het hele bedrijf zal besmetten.’ Ook is het raadzaam om dieven een stap voor te zijn. ‘Door gegevens automatisch te versleutelen en vooraf data op waarde te classificeren. Zo hebben criminelen er niets aan.’

Lage pakkans

ACA IT Solutions helpt het mkb al enige jaren weerbaarder te maken tegen cybercriminelen. Het bedrijf ontwikkelde diverse ‘security diensten, waaronder een assessment. ‘Daarbij checken we de ict-infrastructuur van een bedrijf op 24 basismaatregelen - het gaat bijvoorbeeld om de back-up strategie, het wachtwoordbeleid en de e-mailbeveiliging. Niet zelden komt een bedrijf niet verder dan de helft van de criteria.’ Dat is zorgelijk, vindt Waterman, ‘We kunnen en moeten beter worden. Gemiddeld vragen cybercriminelen 2 tot 5 procent van de jaaromzet aan losgeld. Bij een gemiddeld mkb-bedrijf komt dit al snel neer op enkele tonnen. Voor cybercriminelen is het mede door de lage pakkans een lucratieve business.’ Maar Waterman wil vooral ook een morele oproep doen. ‘Ik vind dat ondernemers hun verantwoordelijkheid moeten nemen. ‘Als je het niet goed regelt, loopt je bedrijf risico. Daarmee dupeer je collega’s als ze door de nasleep van een cyberincident hun baan kwijtraken. Criminelen gaan aan de haal met gegevens van klanten. Het is bijna arrogant als je je schouders ophaalt voor de risico’s.’

Hoofdstuk 6 PinkWeb - ‘state of the art’ beveiligd

Cybercriminaliteit is een serieus gevaar van deze tijd. Gelukkig zijn er software-oplossingen die aan de hoogste veiligheidsnormen voldoen. Met het PinkWeb hoef je je geen zorgen te maken over de veiligheid van klantgegevens. Hoe borgt Visma | PinkWeb deze hoge mate van veiligheid?

Visma | PinkWeb is al jaren gecertificeerd volgens de ISO:27001 norm, we werken aan onze ISAE 3402 certificering, zijn AVG-proof en kijken continu naar ontwikkelingen op het gebied van cybersecurity. Het betekent onder meer dat er elk jaar een penetratietest plaatsvindt, waarbij ethische hackers proberen in te breken in de applicatie. Deze professionals kijken kritisch naar kwetsbaarheden in de software die kunnen worden misbruikt. Uit zo’n penetratietest komen altijd nuttige tips voor verbetering.

Dochter van Visma: groot voordeel

Sinds PinkWeb onderdeel is van Visma valt het klantenportaal ook onder het Visma Security Program. Dit is een uitgebreid en hoogwaardig programma dat bestaat uit verschillende beveiligingsonderdelen:

• De security-experts binnen Visma | PinkWeb monitoren voortdurend op kwetsbaarheden in het klantenportaal. Dat gebeurt aan de hand van checklisten die voortdurend volgens de laatste standaarden worden geüpdatet en realtime checks vanuit beveiligingssoftware. Telkens als er een zwakke schakel wordt opgespoord moet dat worden gerepareerd. Het is een continu proces, de controles zijn streng. Er is een puntensysteem aan gekoppeld, de zogenaamde Security Index, waarmee deelnemers punten kunnen scoren of verliezen. Omdat alle Visma-bedrijven deelnemen aan het Visma Security Program is er sprake van een competitie-element. Eind vorig jaar behaalde Visma | PinkWeb de Gold Status. Dat houdt in dat de beveiliging van de applicatie op het juiste niveau is voor de gevoeligheid van de gegevens die worden verwerkt. Dat betekent niet dat het Visma | PinkWeb-team achterover kan leunen, cybersecurity is een ‘ongoing process’.

• Het is een groot voordeel dat Visma | PinkWeb onderdeel is van het Noorse softwaregroep Visma. Het moederbedrijf heeft de middelen om de meest professionele cybersecurity talenten aan te trekken. Deze forensische hackers zitten in het Visma Cyber Threat Intelligence team. Zij speuren bijvoorbeeld het Darkweb af om te kijken of er aanvallen worden voorbereid op Visma | PinkWeb of andere Visma-bedrijven. Het doel is om cybercriminelen een stap voor te zijn en blijven. Deze state of the art-technieken zijn onderscheidend. Dat gebeurt niet bij veel bedrijven.

PinkWeb ontzorgt accountantskantoren

Kantoren die voor PinkWeb kiezen hebben de beschikking over één herkenbare en veilige omgeving om documenten uit te vragen, te delen en te ondertekenen. Door Document Sharing kunnen accountants veilig vertrouwelijke documenten uitwisselen zonder te kiezen tussen gemak en veiligheid. Als mkb-kantoor heb je de menskracht en kennis niet in huis om de informatiebeveiliging op zo’n hoog peil te brengen én houden. Mocht het toch eens misgaan - 100% veiligheid bestaat immers niet - dan staat Visma | PinkWeb in ieder geval met de beste teams voor je klaar. Wil jij meer weten over PinkWeb? Plan dan een demo in.

Vraag een demo aan