INLEIDING

Volgens hackers zijn er slechts twee soorten bedrijven: bedrijven die al gehackt zijn en bedrijven die gehackt gaan worden. De digitalisering gaat zo snel dat de meeste mensen die niet kunnen bijbenen. Daarom zijn hackers en online oplichters steeds succesvoller. Jaarlijks worden zo'n twee miljoen Nederlanders slachtoffer van online criminaliteit. Vaak raken ze al hun spaargeld kwijt.

Bij bedrijven leiden succesvolle cyberaanvallen tot reputatieschade, grote verliezen en zelfs faillissement. Kleine ondernemers denken nog steeds dat hackers zich vooral op de bekende bedrijven richten, maar dat is allang achterhaald. De boeven maakt het echt niet

uit waar ze binnenkomen. Het is niet zo dat een Russische cybercrimineel een fietsenmaker in Lochem op het oog heeft of een transportbedrijf in Alkmaar, maar die worden wel allemaal gehackt. Meestal omdat ze een digitale deur vergeten zijn te sluiten. Niemand leert je hoe die digitale deuren eruitzien en hoe je ze kunt sluiten. Dit is het doel van dit praktische boek. Hoe kun je jezelf wapenen tegen cybercriminelen als je niet heel veel verstand hebt van computers? In dit boek kun je duidelijke voorbeelden en tips verwachten.

Hoe belangrijk het allemaal voor jou is, kun je beoordelen aan de hand van de volgende vraag: hoelang kun je door blijven werken zonder je computer? En wat als de criminelen al je bestanden versleuteld hebben?

In veel sectoren betekent dat een kleine ramp. Zelfs een bakker kan geen brood meer bakken, want alles is computergestuurd. In dit boek vind je veel voorbeelden van radeloze ondernemers, hoe ze zo'n hack opgelost hebben en wat het allemaal gekost heeft.

Nederlandse mkb'ers zijn gemiddeld een kwart miljoen euro kwijt aan een cyberincident, becijferde IT-beveiliger ESET.

Maken we het de cybercriminelen echt zo gemakkelijk? Het antwoord is 'ja' en dat komt vooral door onwetendheid. Want hoe weet je of een app kwaadaardig is? Hoe herken je een QR-code die je omleidt naar een website waar een virus op je staat te wachten? Hoezo kunnen cybercriminelen een valse link naar een meeting in je digitale agenda zetten zonder dat ze toegang tot je agenda hebben? Medewerkers gebruiken bovendien massaal voorspelbare wachtwoorden, omdat ze niet weten hoe ze tientallen ingewikkelde wachtwoorden moeten onthouden. Cybercriminelen zijn helaas heel goed in het geautomatiseerd raden van dat soort wachtwoorden.

Het doel van dit boek is dat je straks zo veel weet dat het simpel wordt om de trucs van de cybercriminelen te doorzien. De oplossingen zijn helemaal niet technisch en voor de meeste mensen is dat een grote geruststelling. Het leuke is ook dat je niet alles perfect

hoeft te doen. Als je het de cybercriminelen slechts iets moeilijker maakt, dan gaan ze meteen door naar de volgende. Hun tijd is ook geld waard.

Dit boek bestaat uit hoofdstukken die je in volledig willekeurige volgorde kunt lezen. Elk hoofdstuk bevat voorbeelden uit de praktijk en tips. De voorbeelden zijn allemaal waargebeurd.

1 WAT MOET ELKE ONDERNEMER OVER ONLINE VEILIGHEID WETEN?

Is elk bedrijf interessant voor hackers?

Veel ondernemers denken dat hun bedrijf niet interessant genoeg is voor criminelen. Dat dacht ook Xander Koppelmans, eigenaar van ontwerpstudio PHGR. Zijn ontgoocheling was groot toen hij op een dag ontdekte dat de servers leegliepen. Zijn bedrijf met klanten zoals Rijkswaterstaat en Nutricia was opeens alles kwijt: e-mails, boekhouding, duizenden foto's en videobestanden in opdracht van klanten. Ook de reserveservers waren gewist.

Het onafgebroken werken door Koppelmans om de schade enigszins te herstellen resulteerde in een burn-out. Zijn accountant adviseerde hem om faillissement aan te vragen. De schade – onder andere door rechtszaken – was al opgelopen tot 769.000 euro. De ondernemer raakte zijn bedrijfspand en zelfs zijn woonhuis kwijt, omdat de bank na het faillissement direct de hypotheekschuld opeiste.

Er zijn enkele redenen waarom juist kleine bedrijven interessant zijn om te hacken. Ze zijn vaak slecht beschermd en zijn bereid losgeld te betalen om hun klantgegevens en administratie terug te krijgen. Soms hebben ze als leverancier toegang tot grote bedrijven en zo hopen de cybercriminelen juist daar binnen te komen.

Mkb-ondernemers denken meestal dat de kans op een cyberaanval niet zo groot is. Vaak hebben ze wel een brandalarm geïnstalleerd zonder zich af te vragen hoe groot de kans is. De kans op brand is slechts één op 8.000. De kans om slachtoffer te worden van cybercrime is één op vijf.

TIP

Wat zijn de belangrijkste data van je onderneming? Bewaar altijd een kopie van je allerbelangrijkste gegevens. Heb je daar recent een offline back-up van gemaakt?

Is het strafbaar om cybercriminelen te betalen?

Directeur Richard van der Helm werd op een vrijdagnacht gebeld dat er een probleem was met de computers van zijn logistieke bedrijf. Ze waren allemaal gegijzeld.

We gaan niet betalen, dacht de directeur.

Twee dagen later betaalde hij wel.

Natuurlijk probeerden experts om de computers van Van der Helm Logistics te herstellen, maar er was slechts een twaalf uur oude back-up. Voor een logistiek bedrijf betekent dat dat ze van al hun goederen niet weten waar ze zijn. De voorraad opnieuw scannen en alles herstellen zou weken duren. Het bedrijf

zou mogelijk failliet gaan als ze de afspraken met klanten niet konden nakomen.

De cybercriminelen waren binnengekomen via een verouderde VPN-verbinding en een zwak wachtwoord. 'Welkom op onze helpdeskchat' was hun eerste bericht.

Van der Helm was verbluft hoe klantvriendelijk ze waren: als je betaalde, kreeg je meteen de sleutel tot je bestanden terug en kon je weer aan het werk. Zijn bedrijf moest bijna 200.000 euro overmaken. Van der Helm vond de emotionele schade veel erger.

Cybercriminelen betalen is op dit moment niet strafbaar, maar zeker geen goed idee. Door te betalen houd je hun verdienmodel in stand en worden steeds meer bedrijven en mensen slachtoffer. Op dit moment betaalt meer dan de helft van de gehackte bedrijven in Nederland aan de criminelen. Niet iedereen krijgt zijn bestanden terug. Soms worden alle klantgegevens alsnog doorverkocht aan andere criminelen.

TIP

Als je niets anders kunt en je gaat onderhandelen met de cybercriminelen, probeer dan korting te bedingen. Er zijn gespecialiseerde bedrijven die je ermee kunnen helpen.

Kun je op je IT-leverancier rekenen bij problemen?

Vier op de vijf mkb'ers rekenen op een IT-leverancier, zo blijkt uit onderzoek door SIDN. 58 procent van de IT-bedrijven geeft echter aan dat hun klanten onvoldoende beschermd zijn.

Dat ontdekte ook directeur Frank Landhuis van Almi Machinebouwers uit Vriezenveen nadat een medewerker op een link in een foute e-mail had geklikt. 1,4 miljoen bestanden in het computersysteem werden versleuteld. Het bedrijf had alles uitbesteed en verwachtte dat het goed geregeld was. De IT-leverancier

probeerde de back-ups terug te zetten, maar die bleken niet goed te werken.

Landhuis betaalde de cybercriminelen, met pijn in zijn hart, want een maand stilstand om alles op de normale manier aan de praat te krijgen is voor een productiebedrijf funest. Nu duurde het ontsleutelen van de bestanden een paar dagen. 'Het heeft ons zo'n 60.000 euro gekost,' zegt Landhuis. 'Externe IT-specialisten moesten alle laptops schoonmaken en het systeem opnieuw inrichten. De indirecte schade heb ik niet meegerekend. Veel bedrijven denken: mij overkomt het niet. De vraag is niet óf het je overkomt, maar wanneer. Vooral als je geen voorzorgsmaatregelen treft.'

TIP

Bespreek met je IT-leverancier hoe jouw belangrijkste gegevens beschermd zijn en of het simpel is om na een hack de back-ups terug te zetten.

Waarom zijn datalekken zo gevaarlijk?

Computersystemen bevatten veel persoonlijke gegevens van mensen. Na een datalek komen ze vaak in handen van criminelen terecht en worden ze verkocht en doorverkocht. Er zijn criminelen die bijvoorbeeld alleen de telefoonnummers willen hebben om iedereen boven de zestig namens de Belastingdienst of de bank te bellen. Omdat ze al zo veel weten over die persoon (rekeningnummer, adres, geboortedatum, enzovoort) komen ze heel overtuigend over. Veel ouderen raken al hun spaargeld kwijt.

Er zijn bedrijven die kopieën van paspoorten op een onveilige manier bewaren (bijvoorbeeld van medewerkers of sollicitanten), maar ook van klanten, zoals bij autoverhuurbedrijven en hotels in het buitenland. Vaak is een kopie van een paspoort voldoende om de volledige identiteit van iemand te stelen.

Boudewijn kreeg bijvoorbeeld een brief dat hij zich bij de politie moest melden. Iemand had huizen op zijn naam gehuurd en in die huizen had de politie wietplantages ontdekt. De politie liet hem de huur-

veilig online

Bezorgd over je online privacy? Bang dat je wordt gehackt?

Lees hoe cybercriminelen toeslaan en hoe je jezelf kunt beschermen. Hoe voorkom je identiteitsfraude? Hoe herken je een kwaadaardige QR-code? Hoe onthoud je tientallen ingewikkelde wachtwoorden? Hoe check je of je computer gehackt is?

Miljoenen Nederlanders werden al slachtoffer van cybercrime. Een op de vijf bedrijven is gehackt. Deze digitale ellende is simpel te voorkomen met iets meer kennis.

Maria Genova is een expert op het gebied van cybercrime en privacy. Ze trekt volle zalen met haar lezingen over de toenemende digitale gevaren.

Weinig tijd, maar veel ambities? Informeer jezelf snel en grondig met de boeken in de serie *Digitale trends en tools in 60 minuten*.

9 789461 265708