Is jouw webshop bestand tegen hackers?

Het midden- en kleinbedrijf staat nog nauwelijks stil bij zijn digitale veiligheid. Cybercriminelen slaan dan ook in toenemende mate hun slag bij kleine ondernemers. Wat moet je doen om te voorkomen dat je website of webshop wordt gehackt – met alle financiële gevolgen van dien?

TEKST: WILKE WITTEBROOD

Het is een misverstand dat er vooral in dure wijken met veel koopwoningen wordt ingebroken. Inbrekers richten zich niet per se op huizen waar veel te halen valt, maar op huizen waar ze gemakkelijk binnenkomen. Ook 'digitale inbrekers' gaan vaak voor de weg van de minste weerstand. Uit onderzoek van het Centraal Planbureau blijkt dat het midden- en kleinbedrijf veel minder maatregelen neemt om zich te wapenen tegen internetcriminelen dan grote bedrijven. En dat maakt deze groep kwetsbaar, zegt René van Etten, de algemeen directeur van cybersecuritybedrijf ThreadStone. "Voor de campagne Veilig Zakelijk Internetten van VNO-CNW en MKB-Nederland hebben we ruim tweeduizend websites binnen het mkb op veiligheid getest. 85 procent bleek onvoldoende beveiligd." Uit het Cybersecurity Bewustzijnsonderzoek van Alert Online blijkt dat internetcriminelen in 2018 bij ruim de helft (52%) van de kleine bedrijven (met een tot negen werknemers) hebben geprobeerd in te breken. Grofweg een op de vijf ondernemers leed daardoor financiële schade, zegt Rutger Leukfeldt. Hij is senior onderzoeker cybercrime bij het NSCR (Nederlands Studiecentrum Criminaliteit en Rechtshandhaving) en lector Cybersecurity in het mkb bij de Haagse Hogeschool. "Daarbij kun je denken aan afpersing via ransomware (gijzelsoftware), maar ook aan de rekening van de IT-man om gehackte systemen weer in de lucht te krijgen." Toch lijkt driekwart van de ondernemers zich weinig zorgen te maken om hun digitale veiligheid, blijkt uit cijfers van Alert Online. Leukfeldt: "Ondernemers zijn zich wel bewust van de risico's, maar denken: zoiets overkomt mij niet. Dit komt doordat cybercriminaliteit zo abstract is. Het is niet tastbaar. En veel ondernemers wanen zich veilig omdat ze denken dat er bij hen toch niet zo veel te halen valt."

Afpersing en identiteitsfraude

Wat maakt het mkb interessant voor internetcriminelen? Leukfeldt: "Of het nu om jongeren of ouderen gaat, kleine of grote bedrijven – alles en iedereen is interessant voor ze. Cybercriminelen willen geld verdienen. Via welke weg, dat maakt ze verder niet uit." Een van de 'verdienmodellen' is afpersing via een DDoS-aanval (Distributed Denial of Service). Bij een DDoS-aanval worden computers of netwerken overbelast door in korte tijd heel veel internetverkeer op een server of groep servers te richten. Hierdoor kunnen webshops bijvoorbeeld onbruikbaar worden, wat tijdens piekmomenten tot een grote schadepost kan leiden. Cybercriminelen kunnen dreigen een webwinkel volledig stil te leggen, tenzij de aanval wordt afgekocht. Ook aan (het stelen van) data valt grof geld te verdienen. Via een zogenaamde SQL-injectie, ofwel het van buitenaf plaatsen van commando's op plekken waar data ingevoerd worden, zoals bij een bestelformulier, kunnen hackers de database van een website of webshop kraken en in zijn geheel overnemen. Persoonsgegevens zoals namen, adressen en telefoonnummers worden vaak in bulk doorverkocht, bijvoorbeeld aan marketing- of advertentiebedrijven. "Het wordt nog vervelender als hackers ook de wachtwoorden van gebruikers leesbaar uit een database kunnen halen", zegt Roland van Kortenhof, manager Operations & ICT bij Thuiswinkel.org. Consumenten loggen in op een webshop met hun user-ID, een combinatie van e-mailadres en wachtwoord. "Die combinatie is – in de wetenschap dat 40 tot 50 procent van de mensen wachtwoorden hergebruikt – niet zelden de 'sleutel' tot allerlei andere accounts, zoals iemands social media en e-mail. Dan kan leiden tot identiteitsfraude." In de zomer van 2018 werden er duizenden gekraakte accounts van klanten van onder meer Bol.com, Zalando en Wehkamp doorverkocht aan criminelen. Zij bestelden vervolgens online dure producten op naam van de accounthouder en verkochten die spullen op andere websites door. Omdat je bij veel webshops achteraf kunt betalen, viel de rekening uiteindelijk bij het slachtoffer op de deurmat.

'Iedereen is interessant voor cybercriminelen. Zij willen geld verdienen en via welke weg, dat maakt ze verder niet uit'

Verkeerde aannames

Het probleem is dat veel ondernemers niet weten wie er precies voor de veiligheid van hun webshop verantwoordelijk is, zeggen de voor dit artikel geraadpleegde experts. "Kleinere bedrijven gaan er vaak vanuit dat hun leverancier – in het geval van een webshop zijn dat de webdeveloper en/of webhoster – automatisch ook het onderhoud en de beveiliging op zich neemt", zegt René van Etten van ThreadStone. "Dat is niet het geval. Een webdeveloper bouwt je webshop, een webhoster


Stock.adobe.com

zorgt ervoor dat deze via de domeinnaam te bereiken is." Al is het een begrijpelijke aanname, vindt Van Kortenhof. "Ik vergelijk het altijd met het bouwen van een huis. Daarbij ga je er ook van uit dat de aannemer een huis bouwt dat goed in elkaar zit en veilig is, en dat is meestal ook zo. In de ICT is dat helaas nog niet zo vanzelfsprekend. Sommigen nemen cybersecurity niet mee bij de oplevering van een product. Anderen willen wel, maar zijn bang dat hun diensten dan te duur worden en ze klanten verliezen. Cybersecurity kost geld, maar is ook een essentieel onderdeel van de bedrijfsvoering. Een veilige webshop is iets waar zowel de webdeveloper en webhoster als dienstverlenende partij, en zowel de retailer als afnemer naar zouden moeten streven." Van Etten: "Maar voor het zover is, moet je daar zelf om vragen."

Beveiligde verbinding

Waar moet je dan precies om vragen bij je leverancier? Als onderdeel van de campagne Veilig Zakelijk Internetten heeft ThreadStone een document opgesteld met de tien belangrijkste vragen en de antwoorden die je van je webdeveloper of webhoster mag verwachten (zie kader). Thuiswinkel.org werkt met een soortgelijke checklist. De belangenvereniging voor omnichannel- en webwinkeliers is vooral bekend vanwege het Thuiswinkel Waarborg Keurmerk. Dit is een kwaliteitskeurmerk voor webshops, dat consumenten zekerheid biedt dat ze hier veilig en betrouwbaar online shoppen. Meer dan 2.200 retailers hebben het keurmerk al ontvangen, waaronder Omoda, Nelson, Schuurman Schoenen, Topshoe.nl, Van den Assem en Winkelstraat.nl. In dit artikel lichten we de drie door de experts als belangrijkst genoemde punten uit. Vereiste nummer één is een SSL-certificaat. Ofwel: de https-verbinding met slotje in de adresbalk. Daarmee wordt vertrouwelijke informatie, zoals de communicatie tussen klant en webshop, versleuteld verzonden. "Je kunt niet meer zonder, zeker omdat Google het actief meldt wanneer een website onvoldoende is beveiligd", zegt Danny Bakker, e-commercemanager bij de luxe schoenenketen Nolten. Een SSL-verbinding is een belangrijk onderdeel in de beoordeling die Google aan websites geeft, en de bijbehorende vindbaarheid.

Data versleutelen

Het tweede uitgelichte punt betreft het beveiligen van de persoonsgegevens die je als retailer verzamelt. Met ingang van 25 mei 2018 is in de Europese Unie een nieuwe privacywetgeving van kracht geworden, de Algemene Verordening Gegevensbescherming (AVG). "De nieuwe wet verplicht ondernemers maatregelen te nemen om persoonsgegevens, zoals klantgegevens die worden verzameld via online bestellingen, te beschermen", zegt Roland van Kortenhof van Thuiswinkel.org. "Retailers mogen naw-gegevens en wachtwoorden nog wel in een database opslaan, mits de gegevens versleuteld worden. Wachtwoorden moeten niet terug te decoderen zijn. Als hackers inbreken in je database, kunnen ze dáár in elk geval niet bij. Heb je de 'wachtwoord vergeten?'-knop wel eens gebruikt? Als je een mail krijgt met je wachtwoord, weet je zeker dat het niet op de juiste manier is opgeslagen. Webshops zouden de wachtwoorden van de user-ID's niet moeten kunnen lezen."

> **'Veel ondernemers wanen zich veilig omdat ze denken dat er bij hen toch niets te halen valt'**

Scan op kwetsbaarheden

Als derde punt adviseren de voor dit artikel geïnterviewde experts om je webshop regelmatig te (laten) controleren op kwetsbaarheden, door middel van een zogenaamde webapplicatie-scan. Op de website https://veiligzakelijk-internetten.cyberstatus. kun je je website of webshop gratis laten checken door ThreadStone, als onderdeel van de overheidscampagne Veilig Zakelijk Internetten. Maak vervolgens een plan om een dergelijke scan periodiek uit te voeren en spreek dit met je webdeveloper of webhoster door. René van Etten: "Ons advies is om dit minimaal één keer per jaar te doen." Nolten heeft ontwikkelpartner Divide de opdracht gegeven om jaarlijks een securityscan uit te

voeren, in samenwerking met cybersecuritybedrijf Forus-P. Ook Thuiswinkel.org laat (toekomstige) leden door Forus-P scannen op de meest voorkomende beveiligingslekken. “Het komt erop neer dat Forus-P tijdens de scan probeert kwetsbaarheden te vinden”, legt Roland van Kortenhof van Thuiswinkel.org uit. “Een enkele webapplicatie-scan kost ongeveer €75,- en is dus redelijk betaalbaar. Hierbij worden eventueel geconstateerde risicovolle fouten handmatig gecontroleerd. Wanneer men meer scans afneemt, bijvoorbeeld maandelijks of wekelijks, dan is de scanprijs nog lager. Bovenop de webapplicatie-scan kun je nog een handmatige test laten uitvoeren, de zogenaamde penetratietest (pentest). Dit om eventuele kwetsbaarheden bloot te leggen die met geautomatiseerde scanning tools moeilijk te testen zijn.” Al is een penetratietest een relatief zwaar middel. Het is vaak voordeliger om te beginnen met een geautomatiseerde securityscan. Niet alleen vinden deze scanners al veel kwetsbaarheden, ze geven ook inzicht in onderdelen in de IT-infrastructuur die nader onderzoek vergen. “Dat laatste helpt weer om de scope van een eventuele pentest te bepalen”, schrijft Jan Martijn Broekhof, de algemeen directeur van cybersecuritybedrijf Guardian360, in een blog op de bedrijfswebsite.

Digitaal sleepnet

Als retailer moet je tegenwoordig van alle markten thuis zijn. “Van in- en verkoop tot marketing, e-commerce en ICT”, somt Van Kortenhof op. “Kleinere ondernemers moeten alles zelf doen. Soms is het ook gewoon te veel. Daardoor kunnen zaken als digitale veiligheid blijven liggen.” Cybersecurity kost inderdaad tijd en geld, maar het is een investering die loont. Sites met beveiligingslekken zijn laaghangend fruit voor hackers. “Sommige cybercriminelen gooien bij wijze van spreken een sleepnet over het internet uit om te kijken wat ze kunnen binnenhalen”, knikt van Etten. “In dat geval gaat het erom dat jouw webshop net iets beter beveiligd is dan die van je buurman. Anders wordt je eruit gepikt.”

Nieuw: het Digital Trust Center

Eind 2017 is het Digital Trust Center (DTC) opgericht, een initiatief van de ministeries van Economische Zaken & Klimaat en Justitie. De missie van het DTC is om bedrijven weerbaarder te maken tegen cyberdreigingen. Dat gebeurt op twee manieren: door bedrijven betrouwbare en onafhankelijke informatie te verschaffen over digitale kwetsbaarheden en concreet advies op het gebied van online beveiliging te geven, en door cybersecurity samenwerkingsverbanden te stimuleren. Kijk voor meer informatie op www.digitaltrustcenter.nl.

CHECKLIST CYBERSECURITY

Is jouw website of webshop goed beveiligd? Dit zijn de belangrijkste vragen die je aan je webdeveloper of webhoster moet stellen:

- ☑ **1.** Wie is er verantwoordelijk voor het uitvoeren van het onderhoud op mijn website?
- ☑ **2.** Maken we gebruik van SSL-certificaten voor beveiligde gegevensoverdracht?
- ☑ **3.** Wordt er periodiek een controle op kwetsbaarheden uitgevoerd?
- ☑ **4.** Op welke wijze worden belangrijke data en (privacy) gevoelige data opgeslagen?
- ☑ **5.** Maakt mijn site gebruik van de nieuwste internetstandaarden?
- ☑ **6.** Is mijn site beschermd tegen DDoS-aanvallen?
- ☑ **7.** Hebben we een back-up-procedure?
- ☑ **8.** Welke (groepen) gebruikers hebben rechten voor beheer en onderhoud op de website?
- ☑ **9.** Op welke wijze is er bij de opzet van onze website al voor gezorgd dat security is ingebed in het systeem?
- ☑ **10.** Wordt er gebruikgemaakt van een Intrusion Detection System (IDS) en/of Intrusion Detection Prevention (IDP) systeem?

Voor meer informatie kun je terecht op www.veiliginternetten.nl/academy.