JUNI 2021 / JAARGANG 9 / NUMMER 43

OnlineRetailer

DE INFORMATIEBRON VOOR INTERNET-ONDERNEMERS

Digital meeting
B2B E-commerce

E-commerce, PIM en ERP
in 1 totaaloplossing

Digital meeting
Cybersecurity

43

CYBERCRIME!

Sneller doelwit dan je denk!

www.onlineretailer.be

TEKSTEN: **Roel van Gils**
BEELDMATERIAAL: **OnlineRetailer**

Digital Meeting - Cybersecurity

Bescherm jouw kroonjuwelen

BRON: online RETAILER magazine, editie 43

Kranten en nieuwssites publiceren vrijwel dagelijks berichten van geslaagde hacking of ransomware attacks. Cybercriminaliteit is de meest lucratieve vorm van criminaliteit en gaat mondiaal ver boven mensenhandel of drugshandel. Het kan een enorme impact hebben, maar niemand spiegelt het aan zijn eigen onderneming. Men ziet het als een 'ver van mijn bed show' vooral vanwege gebrek aan kennis. Reden voor OnlineRetailer om een digital meeting te organiseren over het topic cybersecurity met een mooie mix aan cyberexperten.

IN HOEVERRE HERKENNEN ONDERNEMINGEN HET RISICO VAN CYBERCRIMINALITEIT?

Een veelgehoorde stelling is 'bij ons valt er niks te rapen'. Het bewustzijn is over het algemeen heel laag. Cybersecurity is een heel moeilijk gegeven, merken de experts. Ze zien overigens wel grote verschillen tussen type van bedrijven. Bepaalde sectoren waarin voornamelijk compliance een grote rol speelt en die onder de nichewetgeving vallen, beginnen nu toch wel serieus stappen te nemen in cybersecurity.

Bij de gemiddelde kmo is het bewustzijn zeer laag. Men vergeet dat iedereen een target kan zijn. Cybercriminaliteit is ook voor hen absoluut een risico. Bovendien ben je als onderneming zelf juridisch verantwoordelijk. Niet je websitebouwer of je hostingpartij. Het management heeft een bestuurdersaansprakelijkheid en kan zelfs persoonlijk op het eigen vermogen aangesproken worden, net zoals het personeel persoonlijk aansprakelijk kan worden gesteld.

Veel ondernemingen zien cybercriminaliteit dus als een 'ver van mijn bed show'. Het is iets fictiefs. Op de dag van vandaag zijn er ook te weinig officiële criminaliteitscijfers. Veel vendors staven met cijfers vanuit de eigen praktijk, die heel wat uit elkaar lopen. Er zijn geen wetenschappelijk objectieve gegevens. Wel zijn er internationale initiatieven om hier verandering in aan te brengen. Maar er is op vandaag geen uniform antwoord op de vraag wat het individuele risico is voor een onderneming en welke acties genomen moeten worden om voldoende cyberveilig te zijn.

Vanuit een keurmerk zoals Safeshops worden wel de nodige initiatieven genomen om meer aandacht te vestigen op cybersecurity. Zo is er anderhalf jaar geleden een website security groep in het leven geroepen, waarvan ook verschillende experts aan deze digital meeting deel uitmaken, met als doel om het bewustzijn in de markt te vergroten. Zo wordt er binnenkort zelfs een gratis scan ter beschikking gesteld.

HOE GAAN CYBERCRIMINELEN TE WERK? EN HOE KAN JE ZE VOOR ZIJN?

Er is natuurlijk een hele range aan mogelijkheden, maar de meest gekende zijn toch wel de ransomware attacks, phishing, DDOS-aanvallen, CEO-fraude en misbruik met paswoorden. 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'. Het komt regelmatig in de media, maar er is toch veel onwetendheid over.

Phishing kent eigenlijk twee varianten. De eerste gaat via personeelsleden. Ze krijgen een kwaadaardige mail binnen en na een paar clicks beginnen bestanden onbruikbaar gemaakt te worden. Bij de andere vorm wordt een website nagemaakt om klanten daar naartoe te lokken en geld af te troggelen met valse transacties. Het kan je ongewild een slechte reputatie en imagoschade bezorgen. Het is dus belangrijk om hier plannen voor klaar te hebben en jezelf erop voor te bereiden op zowel communicatief als technisch niveau. Ook het periodiek en frequent trainen van personeelsleden op dergelijke aanvallen, kan zeker helpen. Hiervoor zijn zelfs interessante tools beschikbaar om dergelijke aanvallen te simuleren.

Vele mensen gebruiken nog steeds zwakke paswoorden waardoor hun account kan overgenomen worden wat kan leiden tot succesvolle hacks. Om allerlei misbruiken met paswoorden te voorkomen, gaat de markt steeds vaker naar sterkere vormen van authenticatie. Toch blijft het volgens de experts een moeilijke. Je wilt aan de ene kant dat klanten zo gemakkelijk mogelijk kunnen inloggen, maar aan de andere kant moet het niet de deur openen voor criminelen. Omschakelen naar SSO-functionaliteiten (single sign-on) waarbij klanten met een Google- of Apple-account kunnen inloggen, zonder weer een nieuw paswoord te moeten aanmaken, kan wat soelaas bieden. ››

ROELAND LEMBRECHTS,
Sirius Legal
Na het behalen van een Master of Criminology aan de KULeuven in 2005 vervolledigde Roeland Lembrechts zijn Master in de Rechten aan de Universiteit Antwerpen in 2009. Sindsdien is Roeland aan de balie Provincie Antwerpen steeds actief geweest in het burgerlijk- en ondernemingsrecht met een bijzondere focus op contracten en aansprakelijkheden. Daarnaast was Roeland actief als bestuurslid van de vakgroep verbintenissenrecht van de balie Provincie Antwerpen en is hij gedurende zes jaar secretaris

SIEBE DE ROOVERE,
Toreon
Siebe De Roovere (Director - Software Development & KMO Markt) probeert van onze digitale samenleving een veiligere plek te maken om te werken. Hij doet dit door (mede) leiding te geven aan een team van security professionals die klanten in België ondersteunen bij al hun security uitdagingen. Siebe focust hierbij vooral op software bouwers en het KMO segment. Siebe heeft als security governance consultant 7+ jaar ervaring binnen cybersecurity. In deze rol ondersteunt hij organisaties om hun informatie te beveiligen door de implementatie van beheersystemen voor informatiebeveiliging gebaseerd op wettelijke vereisten (NIS, GDPR) en internationaal erkende standaarden (ISO27k, NIST) te begeleiden. Tot slot heeft Siebe ook ervaring als security trainer bij onder meer NCOI, het Data Protection Institute en gastlessen aan de Ugent.

BRON: online RETAILER magazine, editie 43

DIMITRI STEYAERT,
Combell
Dimitri is al senior system engineer bij Combell mee verantwoordelijk voor het uitbouwen, opzetten en beheren van hosted solutions op maat van het project van de klant.

KRIS JEHAES,
Sweepatic
Kris Jehaes heeft meer dan 20 jaar ervaring in IT & Security en is momenteel productmanager bij Sweepatic. Sweepatic is een online platform dat bedrijven help automatisch hun internet geconnecteerde IT assets te ontdekken, enkel op basis van hun domainnamen (bv mijnbedrijf.be). Het ontdekken loopt continue door, en aanvullende worden security risico's gevonden en geprioriteerd weergegeven. Een belangrijke focus is de technische complexiteit zo gebruiksvriendelijk mogelijk te brengen en heeft verschillende security use-cases in 1 handige tool.

Kris is industrieel ingenieur begon zijn carrière in 2000 als programmeur en evolueerde naar IT-beveiliging, netwerk- en infra-engineering, waarbij hij sterke technische hands-on rollen opnam. In de loop der jaren evolueerde hij naar security & infra architectuur domeinen en ander consulting projecten. Hij behaalde een Vlerick MBA in 2011. In 2014 startte Kris met een business partner een bedrijf op gespecialiseerd is in de verkoop van B2B Cyber Awareness phishing-oefeningen en interactieve e-learnings. Tijdens zijn carrière, als ingenieur, consultant en manager, heeft Kris gewerkt bij grote en kleine bedrijven in heel België.

Daarnaast zien de experts in België zeker ook incidenten met CEO-fraude, een vorm van fraude of oplichting waarbij er geprobeerd wordt om mensen geld te laten overmaken naar de bankrekening van de oplichter door zich voor te doen als een CEO of andere hooggeplaatste functionaris in een bedrijf. En ook aanvallen in DDOS-sfeer komen regelmatig voor met de bedoeling een website plat te leggen. Het gebeurt vaak op systemen waar de ondernemer wat minder aandacht voor heeft en die daarom juist vatbaar zijn voor aanvallen.

Bedenk dat criminelen vooral op zoek zijn naar geld. Data wordt eerder gezien als een middel dan als een doel. Bij slechts een klein aantal bedrijven in België situeert het risico zich op het niveau van industriële spionage. Dan is data wél het target.

IS EEN CYBERAANVAL BETER BESPREEKBAAR GEWORDEN?

Neen, klinkt het resoluut. Openlijke communicatie rondom een cyberaanval is volgens de experts nog niet evident. Zeker niet bij de wat kleinere bedrijven. Zelfs als je bedenkt dat de kosten én de reputatieschade kunnen worden opgevangen door een cyber insurance verzekeraar, merken de experts een enorme terughoudendheid om erover te praten.

Het is een cultureel verschijnsel. Als je ziet hoeveel meldingen er zijn geweest bij de Autoriteit Persoonsgegevens in Nederland, dan is dat een veelvoud vergeleken met België. Datzelfde geldt voor het aantal bedrijven dat bepaalde security certificaten heeft behaald. We lopen op vlak van cybersecurity toch wel wat achterop in België. De Belgische overheid heeft daarin ook een rol gehad. Zo werd de Belgische Gegevensbeschermingsautoriteit veel te laat actief, meer dan een jaar nadat het eigenlijk had gemoeten.

Positief is wel dat de overheid nu een serieuze inhaalslag wil maken en de ambitie heeft uitgesproken om tegen 2025 tot de top 5 landen te behoren op het gebied van cybersecurity. En daarvoor een nationaal plan heeft opgesteld. De VLAIO cybersecurity verbetertrajecten onderstrepen die ambities. De overheid betaalt maar liefst 45% van de kosten van kmo's die investeren in cybersecurity. Er zijn niet veel landen waar het zover gaat. Het bewustzijn is dus ook zeker bij de overheid gekomen.

CYBERCRIMINALITEIT STIJGT JAAR NA JAAR. WAT IS DE REDEN HIERVOOR?

Hoe digitaler je gaat als samenleving en maatschappij, hoe meer malafide partijen op de kar springen. Alle gegevens van iedereen staan online. Criminelen zullen op allerlei manieren proberen om een voet tussen de deur te krijgen en informatie te ontfutselen. Ze worden ook steeds profes- »

”Openlijke communicatie rondom een cyberaanval is volgens de experts nog niet evident”

frastructuurpartners gekoppeld met een onafhankelijk adviseur die verder het specialistisch advies kan geven. Dat laatste is aan te raden, gezien de vaak beperkte tijd, middelen en expertise op het vlak van cybersecurity bij kmo's. Neemt niet weg dat het wenselijk is om met een door een onafhankelijke derde partij aangeboden scanoplossing altijd een tegencontrole te doen.

Behalve de systemen IT-technisch te beveiligen, blijven awareness trainingen onverminderd belangrijk evenals het implementeren van beleidsmaatregelen inzake cybersecurity en het juridisch aftoetsen van concrete zaken. Omdat je nooit tot een nul-risico komt, is het verstandig een verzekering af te sluiten voor het restrisico. Een goede cyberverzekering kost vandaag het equivalent van twee tot drie autoverzekeringen.

CONCLUSIE: GEZOND WANTROUWEN

Vertrouw niet enkel op de blauwe ogen van je hostingpartij, websitebouwer of programmeur. Ze doen het goed, hebben alle kennis en doen oprecht heel veel voor je. Maar juridisch heb je altijd je eigen verantwoordelijkheid. Je moet altijd controleren of hetgeen wordt geleverd veilig is. Verantwoordelijkheid kun je niet outsourcen. Het advies is dus om met gezond wantrouwen alles te bekijken.

Daarnaast moeten we concluderen dat cyberbedreigingen nooit meer weg gaan. In de 17e eeuw hadden we te maken met piraterij en werden schepen aangevallen op zee op zoek naar kroonjuwelen. Vandaag zijn die kroonjuwelen de data en digitale oplossingen waarmee we samenwerken. Ben je ervan bewust dat als je op een digitale manier zaken doet, er altijd aanvallen kunnen gebeuren en dat je jezelf hiertegen moet beschermen.

Positief is dat de business rond cybersecurity heel matuur is geworden. Er zijn enorm veel standaarden waarop we kunnen aligneren en tools die ons kunnen helpen om aanvallen te detecteren en onderscheppen. We zien wel dat het voor veel ondernemingen moeilijk is om het bos tussen de bomen te zien en de juiste maatregelen te nemen die het meeste impact hebben op de beveiliging van de eigen onderneming. Vertrouw hiervoor op het advies van een onafhankelijke security partner. Start dus vandaag nog met jouw security journey en neem maatregelen om jouw kroonjuwelen te beschermen. Zorg dat de hygiëne goed wordt. De gemiddelde hacker geeft op na 200 uur, want dan wordt het te duur en zoeken ze een ander slachtoffer.

KOEN DRUYTS,
Cybercontract
Meer dan 25 jaar ervaring in het verzekeren van ondernemingsgebonden risico's, wens mijn onderneming op een gezonde en rendabele manier verder te laten groeien, zonder onze eigenheid te verliezen, en met een stabiele en betrouwbare dienst voor onze klanten als doelstelling.

"Vertrouw niet enkel op de blauwe ogen van je hostingpartij, websitebouwer of programmeur"

BRON: online RETAILER magazine, editie 43

DIGITAL MEETING CYBERSECURITY

sioneler. In principe kan iemand vanaf de andere kant van de wereld jou online aanvallen.

Corona is in die zin ook een 'goed jaar' geweest voor criminelen. Niet eerder zijn er zoveel bedrijven de mogelijkheden van e-commerce gaan ontdekken. En je hoeft tegenwoordig al geen IT-specialist meer te zijn om ICT-diensten online te brengen. Dat geeft de 'perfect storm' voor criminelen om meer geld te verdienen dan met een lokale drugshandel. Cybercriminaliteit is anno 2021 de meest lucratieve vorm van criminaliteit. Het is ook nog een vorm van criminaliteit waarbij de pakkans heel gering is en waarin je onder fijne omstandigheden kan 'werken' zonder een wapen te hoeven dragen. De gedroomde manier om geld te verdienen.

In bepaalde landen die minder ethisch zaken doen, genieten hackers zelfs een sterrenstatus. Zolang ze hun vaderlandse overheid en bedrijven geen onrecht aandoen, wordt het gedoogd. Sterker nog, ze ondersteunen dit soort criminelen gewoon en vragen zelfs af en toe wat klusjes te doen voor het vaderland. In Rusland en China is dat heel gebruikelijk. Overigens is Rusland er onlangs wel op aangesproken tijdens de G7. Het is daarnaast niet zo dat de politie in geciviliseerde landen onsuccesvol is, maar de opsporing duurt lang. Het is een kat-en-muisspel.

HOE KAN JE JE BEVEILIGING OP EEN STRUCTURELE MANIER INTEGREREN?

Het 'instapniveau' voor iedere onderneming zou moeten zijn dat je je hygiënefactoren op orde hebt. Met andere woorden, een continue check of de deur op slot zit, de ramen dicht zijn, de camera's actief zijn, enz. Dat kun je heel gemakkelijk toetsen en afdichten met een laagdrempelige analyse. Daarnaast moet je investeren in een stukje onderhoud van je IT-systemen. Net zoals je je auto onderhoudt, moet je ook je IT-systemen up-to-date houden.

Houden bovenstaande zaken serieuze criminelen buiten de deur? Natuurlijk niet, maar het kan wel afschrikken. Vervolgens is het raadzaam in zee te gaan met een professionele hostingpartij en slimme in- ››

"En je hoeft tegenwoordig al geen IT-specialist meer te zijn om ICT-diensten online te brengen"

VINCENT DEFRENNE,
Nviso
Vincent Defrenne is medeoprichter van NVISO, een Belgisch cyber security succesverhaal. Vincent leidt het CISO-as-a-Service team van NVISO. Dit team begeleidt grote organisaties met het verbeteren van hun cyber security en kleinere organisaties met het hands-on aanpakken van hun cyber uitdagingen. Daarnaast is hij ook de oprichter van de Cyber Security Challenge Belgium en draagt hij bij aan verschillende initiatieven om cyber security te promoten in België.

HANS BOUMAN,
TrustGuard/B2U
Hans was al in 1996, als e-commerce manager Visa Nederland, bezig met online betalen.
Vanuit zijn bedrijf Business to You (2001) heeft Hans, tussen 2002 en 2005, Ogone (nu Ingenico) met succes in Nederland geïntroduceerd.
Door de betrokkenheid met de creditcardverwerking, en gekoppelde PCI/DSS-regelgeving, is B2U sinds 2005 actief met het scannen van websites op de aanwezigheid van beveiligingslekken.
Inmiddels kunnen rapporten ook als ISO27001, OWASP, GDPR-versie gedownload worden en kan bij gebleken veiligheid een Trust Guard-logo op de website getoond worden.

Sinds 2015 is Hans ook gestart met PayByLink om met betaallinks via mail, SMS en QR-codes klanten snel, eenvoudig en veilig te laten betalen.

BRON: online RETAILER magazine, editie 43

TRUST GUARD

Hoe veilig is UW website?

Laat uw website regelmatig scannen op veiligheid. En vraag uw hostingbedrijf en sitebouwer de gevonden beveiligings-issues op te lossen. Want dat is namelijk uw juridische verantwoordelijkheid.

Webshops, KMO-ers, multinationals, overheidsinstellingen, stichtingen, iedereen wordt geacht de beveiliging op orde te hebben. Niet alleen op locatie, ook online. Regelmatig uw website scannen hoort bij uw beveiligingsbeleid.

Trust Guard biedt u, als onafhankelijke partij, deze websitescan.
Al vanaf € 110 per domein per jaar!

Vraag vrijblijvend een gratis testaccount aan via www.trustguard.eu.

WEBSITEBEVEILIGING IS UW VERANTWOORDELIJKHEID

ook IPv6

WEBSITEBEVEILIGING

Uw website wordt professioneel gescand vanuit de cloud, er is geen software nodig.

STANDAARD RAPPORTAGE

Periodieke scans en rapportage helpen om te voldoen aan standaarden zoals: PCI/DSS, OWASP, AVG/GDPR, ISO27001, HIPAA, SOX.

KLANTVERTROUWEN

Plaats het Trust Guard seal op uw site en vergroot het klantvertrouwen en verhoog uw conversie.