CYBER SECURITY

RANSOMWARE

Ransomware: hoe voorkom of beperk je de schade voor jouw organisatie?

Door: Anoud Groot

Het risico dat ook jouw bedrijf wordt getroffen door een cyberaanval groeit continu. Nu al behoort het tot de vijf grootste bedrijfsmatige risico's, becijfert het World Economic Forum in zijn Global Risk Report 2021 [1]. Cybercriminelen worden steeds professioneler, en verkrijgen steeds sneller toegang tot je gevoelige IT-systemen. De vakterm *break out time* staat voor de tijd die cybercriminelen na het forceren van toegang nodig hebben om door te dringen tot andere belangrijke IT-systemen. In 2019 bedroeg de gemiddelde break out time ruim viereneenhalf uur. Vorig jaar was dat nét anderhalf uur.

Elke IT-medewerker somt moeiteloos een aantal potentiële cyberdreigingen op: van DDoS-aanvallen tot *ransomware* of *phishing*, en soms ook *zero day exploits*, *SQL-injecties* of *DNS tunneling*. Toch schatten veel professionals het risico dat hun eigen organisatie door zo'n aanval wordt getroffen te laag in. En te vaak ontbreekt het aan kennis over de concrete gang van zaken bij zo'n aanval, stellen security-experts. Hoe gaan de criminelen of kwaadaardige software te werk? En wat gebeurt er dan precies op de eigen IT-systemen? Dat kennisgebrek geldt zeker voor de snel groeiende plaag van ransomware.

Ransomware is malafide software die de toegang van gebruikers tot bestanden, applicaties of systemen verhindert, en die alleen na betaling van losgeld weer vrijgeeft. Met name in het MKB onderschatten veel ondernemers de kans dat ook hun organisatie daardoor wordt getroffen.

"Bijna de helft van alle Nederlandse MKB-bedrijven heeft ervaring met ransomware die probeert bestanden of IT-systemen te gijzelen tegen losgeld"

Dat geldt ook voor ziekenhuizen, gemeentes en andere overheidsorganisaties, die juist steeds vaker worden getarget door cybercriminelen. Verschillende deskundigen becijferen de schade door Nederlandse ransomware aanvallen op vele miljoenen of zelfs miljarden euro's, en bijna de

[1] https://www.weforum.org/reports/the-global-risks-report-2021

helft van alle Nederlandse MKB-bedrijven heeft ervaring met deze vorm van cybercriminaliteit.

De steeds professioneler opererende daders richten zich nu bovendien ook vaker op het 'gijzelen' van kritieke IT-systemen, zodat potentieel levensbedreigende situaties ontstaan. In deze publicatie gaan we daarom nader in op de vele risico's van ransomware. Aan de hand van een concrete case geeft een ervaren security expert uitleg en tips, en krijg je meer informatie over de laatste ontwikkelingen. Wat gaat er vaak fout, tot welke situaties kan dat leiden en welke maatregelen kun je als organisatie nemen om schade door ransomware te voorkomen, beperken en herstellen?

Ransomware is een wereldwijd probleem dat snel in omvang toeneemt.

Volgens het Amerikaanse Financial Crimes Enforcement Network (FinCEN) betaalden Amerikaanse slachtoffers in de eerste helft van 2021 ruim 5 miljard dollar aan losgeld [2]. Dat was meer dan in heel 2020. De totale schade die deze aanvallen veroorzaken is bovendien vaak veel groter, al is die niet eenvoudig te becijferen. "De schattingen over de Nederlandse ransomware schade lopen uiteen van miljoenen tot miljarden", vertelt hoofdofficier Michiel Zwinkels, die bij het Openbaar Ministerie verantwoordelijk is voor de portefeuille cybercrime. "Het feit dat liefst 46 procent van alle MKB-bedrijven al ervaring heeft met ransomware, betekent dat we voor een ongekende uitdaging staan."

"De schattingen over de schade die wordt veroorzaakt door Nederlandse ransomware aanvallen lopen uiteen van miljoenen tot miljarden euro's"

Het aandeel ransomware-aanvallen in de totale hoeveelheid cybercrime in Nederland groeit ook enorm. Volgens Cyberveilig Nederland, de belangenvereniging van de cybersecurity sector, besteedden haar leden liefst 90 procent van hun *incident respons* capaciteit aan het helpen van door ransomware aanvallen getroffen organisaties.

"Daarom is het geen individueel probleem meer, maar een maatschappelijk probleem", constateert Petra Oldengarm. De directeur van Cyberveilig Nederland noemt het mede daarom 'zorgwekkend' dat veel slachtoffers van ransomware niet hadden verwacht dat hun organisatie een potentieel doelwit voor cybercriminelen zou kunnen zijn.

Als het in de media gaat over ransomware aanvallen, gaat het immers vaak vooral over grote organisaties met potentiële miljoenenschades en andere omvangrijke consequenties. Zoals de aanval op het Amerikaans oliebedrijf Colonial Pipeline in mei 2021. Opeens was het bedrijf niet meer in staat zijn dagelijkse 2,5 miljoen vaten olie richting de Amerikaanse Oostkust te pompen, zodat in verschillende staten de helft van de pompstations droog stonden. Of de aanval op het centrale IT systeem van VDL Nedcar in oktober 2021. Driekwart van de 4000 lokale medewerkers

[2] https://www.pymnts.com/news/security-and-risk/2021/fincen-logs-5-2b-in-bitcoin-ransomware/

van het industrieconcern kon een week niet aan het werk. Hoewel er geen details zijn over betaling van losgeld, veroorzaakten beide aanvallen een miljoenenschade.

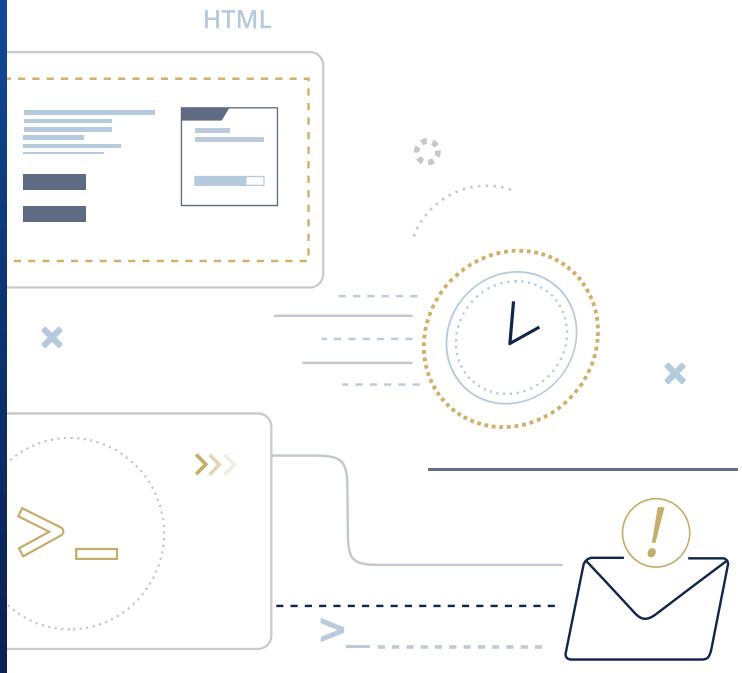
Volgens de experts van het Financial Crimes Enforcement Network gaat het bij deze grote zaken steeds vaker om gerichte aanvallen. De cybercriminelen zoeken daarbij bewust naar bedrijven met zwakke plekken in de beveiliging waar in potentie snel veel schade kan worden veroorzaakt. Ze orkestreren ook persoonlijk elke fase in de navolgende aanval. Door deze zogenaamde *hands-on keyboard* werkwijze neemt de kans dat de organisatie snel veel losgeld betaalt immers ook aanzienlijk toe. Gezien de hoeveelheid vereiste kennis en tijd zijn vormen dit soort gerichte aanvallen echter (nog) slechts een zeer klein percentage van het totale aantal ransomware-incidenten.

"Het is zorgwekkend dat veel slachtoffers van ransomware niet hadden verwacht dat hun organisatie een potentieel doelwit zou kunnen zijn."

"Bij vrijwel alle incidenten waar wij zijn ingeschakeld werd de malware als een 'schot hagel' richting potentiële slachtoffers verspreid", bevestigt Sander Brouwer. De founder en directeur van IT-dienstverlener SBA werd afgelopen jaren tientallen keren ingeschakeld om schade door een ransomware aanval te voorkomen of verhelpen. "Daarbij valt op dat verreweg de meeste gevallen relatief eenvoudig hadden kunnen worden voorkomen. Dat komt vaak doordat verantwoordelijke medewerkers basale IT-kennis missen, en stuk voor stuk de risico's te laag inschatten."

Ook om die reden is het volgens Brouwer bijzonder nuttig om een vrijwel dagelijks voorkomende ransomware aanval van dichtbij te bekijken. Met zo'n nauwkeurige analyse kun je de kans dat jouw eigen organisatie schade oploopt door zo'n aanval aanmerkelijk verkleinen.

DONDERDAG 17 JUNI, 17.21 UUR: NOG EVEN SNEL EEN FACTUUR DOWNLOADEN



Het is einde middag als er bij Rob een mail met factuur binnenkomt. De jonge administratief medewerker wil net afsluiten, maar besluit de factuur toch nog even mee te pikken. Rob werkt pas een paar maanden bij zijn nieuwe werkgever: een reisorganisatie met bijna zestig medewerkers en rond de 20 miljoen euro omzet. Hij heeft zijn digitale kennis op zijn cv wat 'aangezet', maar maakt dat kennisgebrek goed met dubbele inzet.

Rob fronst zijn wenkbrauwen als hij ziet dat hij deze factuur moet downloaden. Ongebruikelijk, maar Rob gaat ervan uit dat dit wel vaker voorkomt. Wel irritant dat de download nu lijkt vast te lopen. Zijn geïrriteerde tik op het keyboard wordt beloond met een melding: "Er is een fout opgetreden bij het downloaden van deze factuur." Dat is voor Rob het teken om alsnog uit te loggen: die factuur zien we morgen wel weer.

Sander Brouwer:
"Veel cyberaanvallen slagen door veelal onbewuste assistentie van eigen medewerkers. Onoplettendheid is een belangrijke oorzaak, regelmatig gekoppeld aan een gebrek aan basale IT-kennis. Relatief weinig werkgevers nemen ook de moeite om de ICT-kennis van nieuwe medewerkers te toetsen. In dit geval gaan er kennelijk geen rode lampjes branden als blijkt dat de factuur niet gewoon als pdf- of xml-bestand bij de mail zit. Iedereen die regelmatig met een computer werkt zou oog moeten hebben voor de extensies achter de namen van te downloaden bestanden."

INSTALLEER UPDATES OM RANSOMWARE BUITEN TE HOUDEN

Naast onoplettende medewerkers richten cybercriminelen zich ook nadrukkelijk op bekende zwakheden in veelgebruikte software, zoals het besturingssystemen, mailprogramma's of webbrowsers. Om de kans daarop te beperken is het cruciaal die software regelmatig te updaten. Dat geldt uiteraard met name voor de beveiligingsupdates oftewel security patches die vaak specifiek beschikbaar worden gesteld om deze kwetsbaarheden te verhelpen. Dat klinkt logisch, maar veel organisaties nemen deze cruciale maatregel onvoldoende serieus, weet Brouwer.

Gezien de vaak grote hoeveelheid beschikbare updates adviseert hij organisaties te focussen op risicovolle systemen die veel online zijn, zoals een website of webshop, modem en router, de reeds genoemde mailprogramma's en webbrowsers en zeker ook smartphones. Een speciale vermelding krijgen de legacy systemen die hij nog regelmatig tegenkomt. "Ik zie bijvoorbeeld nog te vaak organisaties met software werken die al zo oud is dat de ontwikkelaar deze niet meer ondersteunt", vertelt hij. "Zo zie ik Internet Explorer nog regelmatig in gebruik, ruim 2 jaar nadat Microsoft de ondersteuning staakte. Dan leg je als organisatie dus echt de rode loper uit."

DONDERDAG 17 JUNI, 17.25 UUR: KWAADAARDIGE COMPUTERCODE IN ACTIE

Helaas ziet Rob geen enkele aanleiding nog eens goed naar zijn laatste download te kijken voor hij uitlogt. Terwijl zijn scherm zwart wordt, komt de executable die hij heeft binnengehaald in actie. De zogenaamde factuur blijkt in werkelijkheid

"Iedereen die regelmatig met een computer werkt zou oog moeten hebben voor de extensies achter de namen van te downloaden bestanden."

een stukje kwaadaardige computercode dat luistert naar de naam Locky. Vanaf zijn nieuwe onderkomen tussen de downloads genereert de malware een AES-encryptiesleutel. AES staat voor *Advanced Encryption Standard*, oftewel geavanceerde versleutelingsstandaard: een veel gebruikte methode om belangrijke gegevens te versleutelen.

Het algoritme verbruikt slechts een kleine hoeveelheid lokale rekenkracht en geheugen om bestanden te versleutelen op een manier die alleen tegen hoge kosten door een zeer krachtige computer ongedaan kan worden gemaakt. Nadat Rob's bestanden in no-time onleesbaar zijn gemaakt, richt de malware zich op andere locaties waar Rob toegang toe heeft. Terwijl het steeds meer bestanden in hoog tempo versleutelt, plaats de malware met vaste regelmaat ook een readme-bestand tussen de versleutelde bestanden. Het zijn gedetailleerde instructies voor betaling van één bitcoin aan een anoniem bitcoin adres: de reisorganisatie is slachtoffer van een ransomware aanval.

Sander Brouwer:
Als regel is betaling altijd de laatste optie. Al was het maar omdat je in 42 procent van de gevallen waarin je betaalt, nooit meer iets van de cybercriminelen hoort. Als je de aanval vroeg vaststelt, is het mogelijk de encryptiesleutel te achterhalen. De malware is immers actief in de eigen IT-omgeving, en maakt gebruik van de sleutel om de bestanden te coderen.

Natuurlijk moet je dan wel heel goed weten wat je doet: er zijn veel verschillende manieren om data te *encrypten*, en bovendien gaat de malware ondertussen gewoon door met versleutelen van je bestanden. Omdat de snelheid waarmee malware opereert doorlopend toeneemt kan die in korte tijd grote schade aanrichten.

"In 42 procent van de gevallen waarin het geëiste losgeld wordt overgemaakt, hoort de betalende organisatie nooit meer iets van de verantwoordelijke cybercriminelen."

DONDERDAG 17 JUNI, 19.05: ALS EEN LOPEND VUURTJE DOOR DE X SCHIJF

Hoewel Rob geen toegang heeft tot het gehele IT-systeem van de reisorganisatie, heeft hij onvermijdelijk wél toegang tot de algemene X schijf. Net als veel andere bedrijven bewaart zijn werkgever daar onder meer een grote hoeveelheid algemene sales- en marketingbestanden. Inclusief het volledige klantbestand met duizenden persoonlijke reisprofielen. De ransomware is al uren aan het versleutelen als een van Rob's collega's een Excel-bestand wil openen. In plaats van het vertrouwde groene Excel-logo ziet hij nu een grijze postzegel op zijn scherm. De bestandsnaam is identiek, maar heeft een onbekende extensie. En als de medewerker daar toch op klikt, vraagt het systeem: "Met welk programma wilt u dit bestand openen?"

Eén blik van een gewaarschuwde IT-collega is voldoende om alarm te slaan. Het volgende telefoontje is naar de externe consultant die het gehele digitale platform van de reisorganisatie heeft opgezet. Die beoordeelt de situatie direct op basis van twee criteria: impact en prioriteit.

Het aantal medewerkers dat hinder ondervindt van de vastgestelde dreiging bepaalt de impact. De prioriteit neemt toe met de mate waarin de aanval het uitvoeren van werkzaamheden belemmert. Aangezien zeker tien medewerkers op dat moment al geen toegang meer heeft tot benodigde bestanden escaleert de IT-consultant deze ransomware-dreiging direct tot het hoogste niveau.

Sander Brouwer:
"Eerste actie is dan uiteraard het isoleren van de dreiging. In dit geval heeft de verantwoordelijk administratief medewerker alleen toegang tot de algemene X schijf. De management- en directieschijf blijven daardoor buiten schot. Door het relatief late alarmzijn alle bestanden op de X schijf helaas wel al versleuteld. Na het maken van een paar screenshots voor de opdrachtgever moet je dan direct de exacte aard van de aanval achterhalen."

"Google is ook hier vaak je beste vriend. In dit geval levert een zoekopdracht naar de nieuwe Locky-extensie achter alle versleutelde bestandsnamen direct een grote hoeveelheid informatie. Bestudeer de beschikbare informatie altijd nauwgezet: het gebeurt bijvoorbeeld regelmatig andere partijen bijvoorbeeld de encryptiesleutel hebben achterhaald, of een andere manier hebben gevonden de gevolgen te beperken."

CYBERCRIME AS A SERVICE

In het in juni 2021 verschenen **Cyber Security Beeld Nederland (CSBN)** schetst de Nationaal Coördinator Terrorismebestrijding en Veiligheid een onthutsend beeld van het complexe ondergrondse criminele ecosysteem dat inmiddels is ontstaan rond ransomware. Volgens in samenwerking met OM en politie verricht onderzoek ontstaat er een ransomwareketen met steeds meer geprofessionaliseerde spelers: de bouwers van de software, de specialisten die zorgen voor distributie en de criminelen die slachtoffers 'klemzetten' om het veelal via cryptovaluta uitbetaalde losgeld los te krijgen. Veel van deze partijen werken ad hoc met elkaar samen: 'cybercrime as a service' dus, waarbij met name opvalt dat veel partijen inmiddels internationaal opereren.

MAANDAG 21 JUNI: AFLOOP MET EEN (DURE) SISSER

Voor de reisorganisatie blijft de online zoektocht naar een snelle oplossing helaas zonder resultaat. Een snelle check leert bovendien dat de ransomware de *shadow copies* die Windows automatisch maakt van elk bewerkt bestand zonder uitzondering heeft gewist. Maar er is ook goed nieuws: er is een back-up van de X schijf, die bovendien niet is geïnfecteerd door de ransomware. Dat beperkt de schade aanzienlijk, maar voorkomt die niet helemaal. Doordat de back-up met een vertraging van vier uur plaats vindt, is een flink deel van de op de dag van de infectie bewerkte bestanden niet te redden.

Het restoren van de gekopieerde bestanden naar de getroffen X schijf vereist daarbij ook een dag werk van twee gespecialiseerde consultants, die in het proces logischerwijs ook een grote hoeveelheid dataverkeer genereren. Tijdens deze 'terugzetdag' kan een deel van de medewerkers van de reisorganisatie ook niet bij hun vertrouwde bestanden, zodat hun serviceniveau aanzienlijk onder de gebruikelijke standaard ligt. Zo loopt de schade al snel op tot vele duizenden euro's, en de reputatieschade bij de klant.

Sander Brouwer:
"Maar natuurlijk was de schade vele malen groter geweest als alle versleutelde bestanden verloren waren gegaan. Belangrijke factor in deze 'afloop met een sisser' was het feite dat deze klant gebruik maakte van Virtual Private Servers van TransIP. Naast de grote flexibiliteit van deze oplossing stond de back-up in een andere cloud, zodat de kans dat die ook geïnfecteerd zou worden veel kleiner was. Bovendien controleert TransIP ook of back-ups daadwerkelijk op afgesproken wijze plaatsvinden. Het gebeurt regelmatig dat bedrijven rekenen op een back-up die niet of onvolledig plaatsvindt."

Direct na deze wake up call nam de reisorganisatie verschillende andere maatregelen om herhaling te voorkomen. Door de activering van AppLocker kunnen medewerkers nu alleen nog maar *executables* vanuit het eigen systeem opstarten. Deze effectieve functie zit gewoon in Windows, is dus goedkoop en kan makkelijk worden uitgerold. Eerder wilde deze organisatie daar niet aan vanwege de impact op de bewegingsvrijheid van medewerkers. Zo kunnen ze bijvoorbeeld niet de executable voor het deelnemen aan een call starten. Dit moet je dus goed doorspreken, want je medewerkers vinden bij te strakke beveiliging vaak risicovolle alternatieven. Hier ligt direct ook de belangrijkste maatregel: wij verzorgen nu elk kwartaal een opfriscursus om het veiligheidsbewustzijn onder het volledige personeelsbestand – dus óók de directie – op peil te houden."

CYBERVERZEKERING KEERT OOK LOSGELD UIT

Mede vanwege de toenemende dreiging overwegen of nemen steeds meer bedrijven ook een cyberverzekering. Verzekeraars als AIG, Hiscox en Nationale Nederlanden vergoeden voor slachtoffers van ransomware het inhuren van specialisten en schadevergoedingen. Ook het betaalde losgeld valt onder bepaalde voorwaarden onder deze dekking. Volgens critici houden de verzekeraars het verdienmodel van de cybercriminelen daarmee in stand; het ministerie van Justitie en Veiligheid onderzoekt om die reden een verbod.

Geen goed idee, meent juriste Nynke Brouwer, die er promotieonderzoek naar deed. "Niemand wil criminelen betalen die je bedrijf bezetten", **vertelde ze oktober 2021 in het NRC Handelsblad**. "Vaak is er echter geen acceptabel alternatief. Vooral voor kleinere bedrijven kan zo'n cyberverzekering ongelofelijk waardevol zijn. Je krijgt een noodnummer waar je 24/7 assistentie kan krijgen. Snelheid is bij cyberincidenten belangrijk. Een cyberverzekering zie ik als een laatste vangnet voor bedrijven, dat net het verschil kan maken tussen wel of niet kopje onder gaan."

VIJF CRUCIALE MAATREGELEN TEGEN RANSOMWARE

1. Pas security patches en andere updates consistent direct toe

Het lijkt logisch, maar te veel bedrijven vergeten (security) updates snel en consistent toe te passen. Bij kleinere bedrijven ontbreekt vaak een degelijk ingericht patchmanagementbeleid. Brouwer: “En bij grotere bedrijven is het voor de verantwoordelijke IT-afdeling vaak lastig overzicht en controle te houden op geïnstalleerde software en de stroom patches en updates. In beide gevallen kan het daarom nuttig zijn om gebruik te maken van Remote Management Software die automatisch alle cruciale updates implementeert en ook waarschuwt bij onregelmatigheden. Vergeet trouwen niet álle lagen van een virtuele server te updaten, dus bijvoorbeeld ook het OS.”

2. Gebruik moderne beveiligingssoftware

Naast patchen is het belangrijk dat een organisatie beschermd wordt met de juiste beveiligingssoftware. Moderne security-oplossingen werken met intelligente mechanismen zoals heuristiek, gedragsanalyse en een exploit-beveiliging die misbruik van bekende ‘zwakke plekken’ in software voorkomt. “Ook hier is Remote Management Software heel nuttig”, vertelt Brouwer. “Zo voorkomt die software bijvoorbeeld dat medewerkers hun virusscanners uitzetten of updates uitzetten omdat dit even niet uitkomt.”

3. Maak regelmatig back-ups

Om te voorkomen dat ransomware bestanden permanent onleesbaar maakt is het belangrijk om met regelmaat een back-up te maken. Uiteraard moet het back-up medium zo goed mogelijk worden afgescheiden van de locatie van de gekopieerde bestanden, om de kans dat malware

'overspringt' zo klein mogelijk te maken. "Het gebeurt ook regelmatig dat organisaties die back-up niet goed inregelen", vertelt Brouwer. "Bijvoorbeeld door procedurefouten, conflicterende software of doordat Kees dacht dat Piet het zou regelen. Het is dus belangrijk dat er standaard back-ups staan ingeregeld en dat je bijvoorbeeld ook nog de mogelijkheid hebt om de retentie van je back-ups te verhogen en off-site back-ups kunt maken. En test ook gewoon af en toe of je gekopieerde bestanden daadwerkelijk kunt terugplaatsen."

4. Test je beveiliging regelmatig

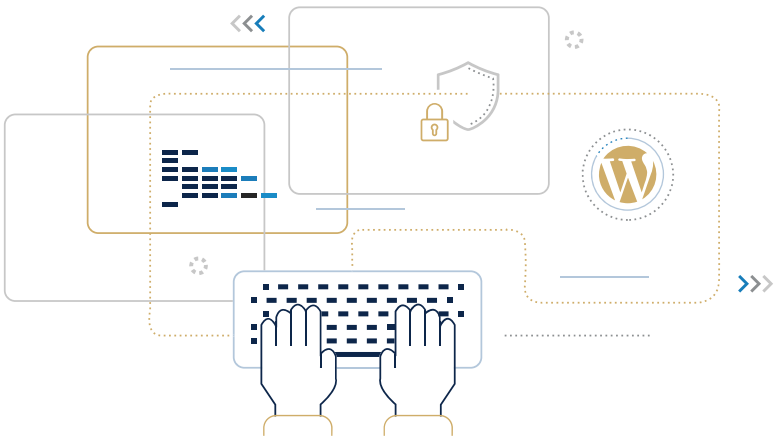
De inkoop van moderne digitale beveiliging is een goede eerste stap. Zorg er echter ook voor dat er regelmatig wordt gecontroleerd of die zijn werk wel doet. Brouwer: "Met een Open Vulnerability Assessment System, oftewel OpenVAS, kun je die controle redelijk goedkoop automatiseren. Het loont echter de moeite om af en toe ook een partij in te huren voor een audit of penetratietest. Dat is wat duurder, maar levert je wel een objectieve evaluatie van je beveiliging op. Voor veel organisaties is dat een echte eye-opener."

5. Werk doorlopend aan de securitybewustheid van je medewerkers

In de jarenlange ervaring van Sander Brouwer beginnen negen van de tien door ransomware veroorzaakte problemen door een gebrek aan kennis of waakzaamheid bij een medewerker. "In het geval van de reisorganisatie zie je bijvoorbeeld dat de verantwoordelijke medewerker klakkeloos een executable download en geen oog heeft voor de extensie achter de bestandsnaam", vertelt hij. "Verder zien we ook vaak dat medewerkers vaste procedures omzeilen omdat ze nog even snel iets willen regelen. Dat soort fouten kun je alleen voorkomen door je medewerkers doorlopend scherp en geïnformeerd te houden. Bijvoorbeeld met een regelmatig terugkomende informatiebijeenkomst of workshop. De besproken reisorganisatie heeft die nu in ieder geval elk kwartaal op de agenda."

Profiel Sander Brouwer

Sander Brouwer is de founder van SBA. Sinds de oprichting in 2005 ondersteunt deze IT-dienstverlener organisaties met diensten zoals remote support, klantspecifieke web-applicaties, hosting, VPN-oplossingen en cloud computing. Met 8 medewerkers werkt SBA onder meer voor Domino's Pizza, KLM en Hogeschool Rotterdam.



Over TransIP

TransIP biedt self-managed infrastructuurdiensten aan vanuit zijn vestigingen in Nederland. Het portfolio bestaat uit domeinregistratie, webhosting, cloud computing en cloud-applicaties. Onder het motto ‘Make Advanced Simple’ zorgt TransIP ervoor dat meer dan 190.000 klanten het meeste halen uit hun digitale bestaan.

Ga voor meer informatie of producten naar www.transip.nl