ACA, cybersecurity

Geert Rademakers

HACKERS ZIJN AAN DE WINNENDE HAND

Op maandagochtend aangestaard worden door een schermvullend doodshoofd en de mededeling dat de bedrijfsinformatie gekaapt is. Of je even een bitcointransactie wilt doen om je eigen bestanden terug te krijgen. Zelfs als je bereid bent te betalen, blijft het de vraag of de hacker over de brug komt, want in slechts acht procent van de gevallen heb je te maken met een ‘eerlijke’ crimineel. Misdaad loont in de drukbevolkte wereld van hackers, digitale sleepnetten en ransomware.

TEKST: MARTIJN VAN DER VEN

Waren computerhacks tot een paar jaar geleden nog een hoofdpijndossier voor banken en multinationals, in 2021 is elke onderneming een potentieel doelwit. Eind juni haalde de Mandemakers Groep het nieuws na een aanval met ransomware. De operationele systemen werden door hackers geblokt. Gevolg: het meubel- en keukenconcern lag plat en klanten kregen hun bestelde spullen niet geleverd. Kort daarvoor werd Bakker Logistiek te grazen genomen door cybercriminelen, waardoor shoppers bij Albert Heijn een week lang misgrepen op strooikaas en plakken jong belegen. En onlangs werd softwareontwikkelaar Kaseya in één klap wereldberoemd na een ransomware-aanval door de aan Rusland gelieerde REvil-groep. Hierdoor werden computersystemen van maar liefst 200.000 bedrijven geïnfecteerd die gebruik maken van Kaseya’s software. Het losgeld, zo’n 70 miljoen dollar, werd volgens Kaseya niet betaald, maar de claim-, herstel- en imagoschade was fors. Ontelbare paniekerige klanten nog daargelaten.

Ransomware-pandemie

RTL Nieuws becijferde dat het aantal ransomware-aanvallen vorig jaar wereldwijd steeg met een duizelingwekkende 715 procent. De Britse verzekeraar Hiscox schat dat de jaarlijkse schade 6.000 miljard dollar wereldwijd bedraagt. Interpol rept zelfs over een ‘ransomware-pandemie’. „Het is niet de vraag óf jouw bedrijf aan de beurt komt, maar wanneer”, bevestigt IT-expert en directeur van ACA IT-Solutions Geert Rademakers. Volgens Rademakers leven we in een bijzondere tijd. Bijzonder beangstigend, blijkt al snel. „Wat we nu zien gebeuren, is dat elk bedrijf doelwit kan zijn van cybercriminelen. Dat heeft te maken met de veranderde modus operandi van hackers. Tot circa 2015 werden doelbewuste aangevallen uitgevoerd op grote, kapitaalkrachtige bedrijven met een hoog risicoprofiel. Daar viel immers de buit te halen. Inmiddels hebben de multinationals hun beveiliging op orde gebracht. Dus verschuift de aandacht van de digitale inbrekers naar het midden- en kleinbedrijf. Maar ook de plaatselijke basisschool en het verpleeghuis blijven niet buiten schot. Ook daar zijn mooie bedragen op te halen.”

Vissen naar zwakke plekken

Rademakers wijst op het bestaan van criminele marktplaatsen. Verborgen handelsplekken waar voor een paar dollars bestanden te koop zijn die gegevens

bevatten over commerciële bedrijven, instanties en zelfs hobbyclubs die allemaal gebruikmaken van software met zwakke plekken, in IT-taal ‘exploits’ genoemd. In zulke bestanden is het prettig vissen. Niet alleen gebruikersnamen en wachtwoorden, maar ook informatie over de diverse applicaties die een organisatie gebruikt

‘HET IS NIET DE VRAAG ÓF JOUW BEDRIJF AAN DE BEURT KOMT, **MAAR WANNEER’**

zijn traceerbaar. Daar hoef je zelfs geen computerexpert meer voor te zijn. Ook de puberende zolderkamerhacker kan er rustig zijn sleepnet uitwerpen en via de kieren van bijvoorbeeld niet-geüpdatete softwarepakketten binnendringen bij zoveel mogelijk organisaties. Eenmaal binnen heeft de crimineel vrij spel. „Soms zelfs weken of maanden achter elkaar”, licht Rademakers toe. „De hacker brengt in dat geval onopgemerkt en op geraffineerde wijze de processen van een bedrijf in kaart, zoals het betalingsverkeer. Als je als ondernemer op een zondagavond ineens een verzoek krijgt van je financieel manager om een ongebruikelijke betaling te valideren, dan is de kans reëel dat je een cybercrimineel tegenover je hebt. Les één is dan ook: blijf alert en doe je updates! Zeker wanneer je op dit moment denkt dat jouw bedrijf vast niet interessant genoeg is voor hackers.”

Juridisch moeras

De woorden van Rademakers roepen vragen op, zoals waarom de autoriteiten niet keihard optreden tegen de criminele marktplaatsen. „Er is een continu kat- en muisspel gaande tussen overheden en de aanbieders van gegevens, enigszins te vergelijken met de strijd van een paar jaar geleden tegen het illegaal downloaden van muziek en films”, zegt Rademakers. „Het ligt juridisch ongelooflijk ingewikkeld, want een hacker die op zoek gaat naar kwetsbaarheden in ICT-systemen kan net zo goed een maatschappelijk doel dienen. Bijvoorbeeld om softwarefabrikanten aan te kunnen spreken. Het vervelende is dat er altijd mensen zullen zijn die misbruik maken van deze informatie. Zijn ze goed georganiseerd en zitten ze bijvoorbeeld in China of Rusland, dan sta je nagenoeg machteloos. Denk aan de beïnvloeding van de Amerikaanse verkiezingen ten tijde van Trump. Bovendien wordt gebruik gemaakt van cryptovaluta, waardoor betalingen van ransomware niet traceerbaar zijn. Cybercriminelen hebben alle tijd en spelen het spelletje meedogenloos. Ondernemers die cybersecurity niet serieus nemen moeten beseffen dat de criminelen aan de winnende hand zijn.”

Goed van vertrouwen

Een andere vraag is waarom met name het midden- en kleinbedrijf de digitale achterdeur wagenwijd open laat staan voor kwaadwillenden. Rademakers ziet een mix van onderschatting, onwetendheid en naïviteit. „Het besef dat ICT een cruciale rol speelt in bedrijfsprocessen begint nu pas door te dringen. Terwijl de continuïteit van veruit de meeste ondernemingen er direct van afhankelijk is. Investeringen in deugdelijke beveiliging en back-upsystemen bleven jarenlang hopeloos achter en in coronatijd werd er zelfs op bezuinigd. Cybercriminelen weten dit ook. Daar komt bij dat ondernemers in het mkb van nature veel ruimte geven aan hun medewerkers. Vertrouwen in het personeel wordt gezien als een groot goed. Maar als diezelfde medewerker thuiswerkt en verbonden is met de zaak, zonder de noodzakelijke beveiligingen op zijn apparaat, dan ontstaat er een levensgroot risico voor het hele bedrijf. Hetzelfde

‘OOK EEN PUBERENDE ZOLDERKAMERHACKER KAN BIJ JE BEDRIJF BINNENDRINGEN’

vertrouwen zie ik vaak richting toeleveranciers van de ondernemer. Besef dat je leverancier ook jouw organisatie kan meetrekken in de ellende als hij ‘de deur’ niet goed heeft afgesloten. Les twee: analyseer de kwetsbaarheden in de ICT-systemen op alle niveaus van je organisatie en los die op. Betrek ook de medewerkers en beleidsbepalers hierbij.”

Slot op de digitale deur

Rademakers pleit dus voor bewustwording en voor beveiliging aan de voorkant. Wie z’n zaakjes niet op orde heeft, loopt een reëel risico om op een maandagochtend tegen dat digitale doodshoofd aan te kijken. Is betalen in zo’n geval de enige optie? „Niet per se. Als je de noodzakelijke stappen hebt genomen, ‘bubbels’ hebt gecreëerd in je datasystemen en je back-ups op orde hebt, valt er vaak nog veel te redden. Lukt dat niet, dan kun je ervoor kiezen om te betalen, al raad ik dat om meerdere redenen af. Je doet immers geen zaken met een bonafide bedrijf en garanties zijn er niet. Los van het feit dat je over je eigen principes moet stappen, levert de cybercrimineel in slechts acht procent van de gevallen na betaling daadwerkelijk de digitale sleutel waarmee je je bedrijfsgegevens kunt ontsluiten. Recente onderzoeken tonen aan dat bedrijven die bereid zijn te betalen een grote kans lopen nógmaals gehackt te worden. Je moet maar hopen dat je dus te maken hebt met een ‘respectabele hackersgroep’, hoe cynisch dat ook klinkt. Daarom tot slot les drie: zorg dat je data altijd ergens veilig staan. Mocht een hacker je bedrijf binnendringen en je systemen versleutelen, dan is er altijd een kopie om op terug te kunnen vallen.”

Wil je een overzicht van de actuele cyberbedreigingen en wat je kunt doen om je organisatie veiliger te maken? ACA IT-Solutions heeft een whitepaper die je hier kunt downloaden: **aca-it.nl/tips**