ONLINE BANKIEREN IS HYPERBEVEILIGD

MAAR HOE **VEILIG** GEDRAGEN WE ONS IN DE **DIGITALE WERELD**?

Op een regenachtige middag ontmoet ik Alexandre Pluvinage voor een interview over cyberbeveiliging in de financiële wereld. "Als je me dingen gaat vragen over de bankbeveiliging bij ING, dan kan ik je daar niks over vertellen. Strikt geheim", valt hij met de deur in huis. Maar al snel blijkt dat cybersecurity, bij banken en elders, veel meer inhoudt dan supergesofisticeerde en streng beschermde IT-goocheltrucs. Als hoofd van het Fraud & Cybersecurity Awareness team bij ING België, stuurt hij een wake-up call de wereld in.

AUTEUR: AN REKKERS

De tijd dat we onze centen in een oude sok onder onze matras bewaarden, is wellicht definitief voorbij. Het aantal Vlamingen dat anno 2018 niet online bankiert daalt met de dag. De tools voor de klanten, zoals PC-banking of smart banking via mobiele apps worden zeer zwaar beveiligd en alle gegevensstromen van online en mobiel bankieren tussen de servers van de bank en je eigen toestel (computer, tablet of smartphone) zijn onontcijferbaar versleuteld. Elke zichzelf respecterende bank heeft op zijn website een of meerdere uitgebreide pagina's over hoe je veilig met de ter beschikking gestelde tools aan de slag kan. Een vergrendelcode op je smartphone instellen, geen persoonlijke gegevens zoals rekeningnummers of identiteitsgegevens op je toestel bewaren, de apps enkel downloaden via de officiële websites van iTunes of Google Play Store, het zijn maar enkele tips om fraude te voorkomen.

BIG BUSINESS

Maar hoe uitgebreid de beveiliging en de maatregelen aan de bankzijde ook zijn uitgewerkt, of hoe gedetailleerd praktijken als phishing ook staan gedocumenteerd, als een klant zijn pincode bij zijn bankkaart bewaart of telefonisch zijn codes doorgeeft, dan staat de bank op zich daar uiteraard machteloos tegenover. En daar knelt volgens Alexandre Pluvinage ook vaak het schoentje. "We hebben allemaal een brandverzekering, terwijl een woningbrand – gelukkig – zelden voorkomt. Maar tegen cybercriminaliteit beschermen we ons nauwelijks, terwijl hacking, virussen of fraude dagelijkse kost zijn. Sinds een jaar of twee, drie levert cybercrime wereldwijd meer geld op dan drugstrafiek. Het is gemakkelijk, je wordt nooit gearresteerd met een virus in je rugzak. We krijgen in de toekomst gegarandeerd te maken met meer fraude, meer malware (software die gebruikt wordt om computersystemen te verstoren). Je hebt nu ook malware as a service: je koopt geen virus meer, je least het virus net zoals je een auto least. Gratis updates, alle onderhoud inbegrepen in het forfait en als je een probleem hebt, word je met een simpele chat verder geholpen. Cybercrime is big business geworden. Een tijdje geleden doken de virussen Petya en Wannacry op. Het gaat om cryptoware, een vorm van malware die computerbestanden en back-ups versleutelt

"Sinds een jaar of twee, drie levert cybercrime wereldwijd meer geld op dan drugstrafiek."

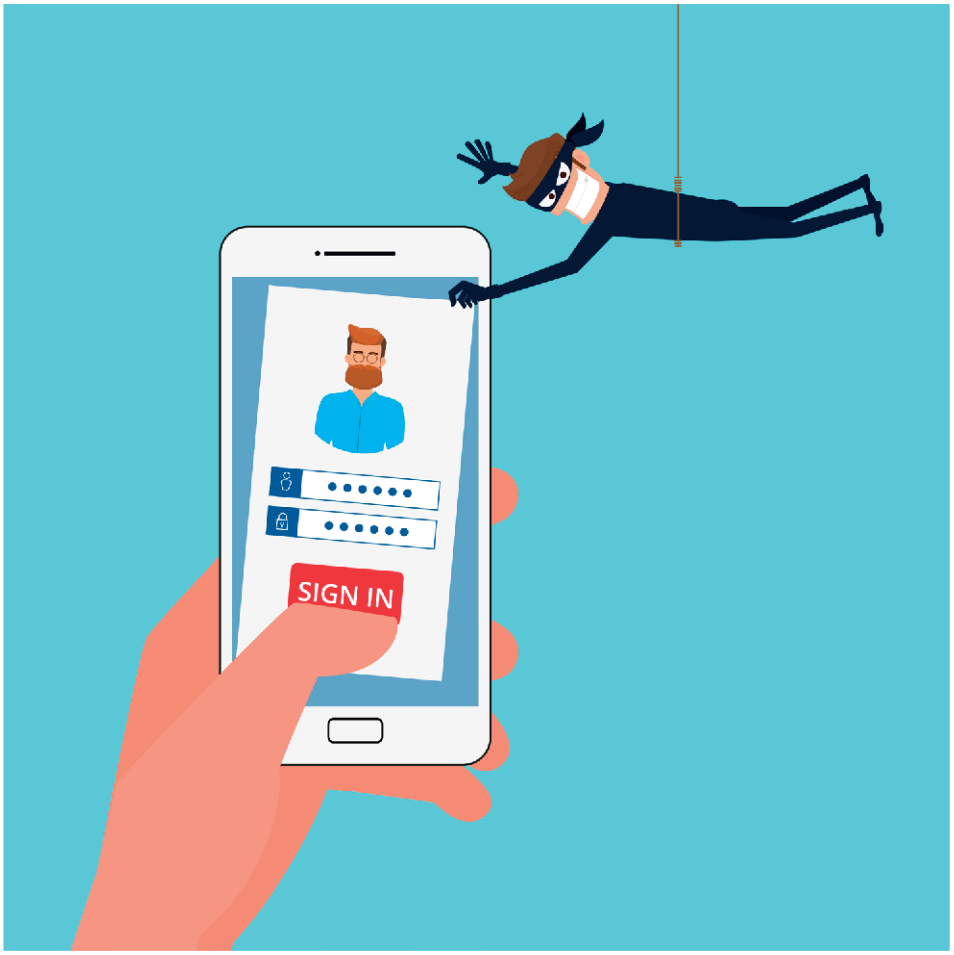
zodat ze niet meer bruikbaar zijn. Ze dringen je pc of netwerk binnen via het Windows-systeem en worden verstuurd via e-mails of bijlagen. Met een schermbericht eisen de cybercriminelen losgeld (vandaar ook de naam ransomware), dat binnen een paar dagen moet worden betaald en waarna je een code krijgt om het systeem te herstellen. Er waren bedrijven die zo zwaar waren geïnfecteerd dat niks meer werkte. Van één pc die geblokkeerd was tot heel het systeem van productielijn, stockage, verkoop … "

HYGIËNE

Cyberbeveiliging, zowel bij een bank als bij andere bedrijven, is volgens Alexandre Pluvinage dan ook geen opdracht voor de IT-afdeling alleen. "Vanuit mijn functie bij ING ben ik afgevaardigd in de Belgian Cyber Security Coalition (www.cybersecuritycoalition.be/) die sleutelfiguren uit de academische wereld, de overheid en de private sector samenbrengt om cybercriminaliteit te bestrijden. Ik ben er hoofd van de 'Awareness Track', waarmee we tal van initiatieven nemen om bedrijven te sensibiliseren voor cyberveiligheid. We hebben er een laagdrempelige, gratis te downloaden Cyber Security Kit voor bedrijven ontwikkeld, om organisaties én hun werknemers 'cyber safe' te maken. Wat we doen in de afdeling Cyber Security Awareness, is eigenlijk een gedragsverandering teweeg brengen. Als ik vandaag praat met CEO's, dan verwijzen ze allemaal naar hun IT-afdeling, in het volste vertrouwen dat die alles onder controle hebben en kunnen beveiligen. Volgens mij is het fout om te denken dat IT een heel bedrijf kan beveiligen. Niet omdat ze er technisch niet toe in staat zijn, maar omdat cyberveiligheid een hele bedrijfsstrategie vraagt. Als bij de grootste frietproducent van België de website twee dagen niet werkt, zal dat het verkoopsresultaat misschien niet drastisch beïnvloeden. Maar als Amazon twee minuten offline is, gaat het om miljoenen verlies. Als bij diezelfde frietproducent de productielijn stilligt, is dat een veel grotere ramp. Voor hen is die productielijn zo cruciaal dat ze zich geen virus kunnen veroorloven. Dat zijn vragen die het management wel kan beantwoorden. Het is aan het management om, in overleg met de IT-dienst, te bepalen waar de heikele punten zitten: moet e-mail meer beveiligd worden, vraagt de website meer bescherming of zijn de proces- of productiefactoren cruciaal?

Alexandre Pluvinage

Bij de typische grote bedrijven zoals banken of telecombedrijven wordt er gigantisch veel in cyberbeveiliging geïnvesteerd. Aan de andere kant heb je de kleine bedrijven, die vaak een probleem hebben met wat we cyberhygiëne noemen, de basis van cyberveiligheid. Meer dan 99% van de aanvallen in bedrijven gebeurt via medewerkers. Stuur een e-mail naar 10 mensen in een bedrijf met 100 medewerkers en één ervan zal klikken. En als die klikt, zit het virus binnen. Waarom zou je dan proberen door de veiligheidsmaatregelen en firewalls door te breken, als je zo makkelijk een virus ingeplant krijgt? Het probleem is dat bedrijven investeren in back-ups, in firewalls, in anti-virusprogramma's, maar ze trainen hun mensen niet. En dat is een van hun grootste risico's."



NEUROCHIRURG

ING Belgium organiseert op regelmatige basis lezingen voor zijn professionele klanten over cyberveiligheid en cyberfraude. Alexandre Pluvinage maakt hen wegwijs in begrippen als cyberfraude, CEO-fraude, factuurfraude, fishing, praktijken waar bijzonder veel geld mee is gemoeid. Hij legt uit hoe criminelen tewerk gaan en hoe je je bedrijf kan beschermen tegen hun aanvallen. ING en de Cyber Security Coalition bieden deze trainingen aan omdat er vandaag zeer weinig opleidingen over fraude en cyberveiligheid bestaan. Ook in IT-opleidingen wordt er volgens Pluvinage te weinig aandacht besteed aan cyberbeveiliging. En toch leggen heel wat bedrijven al hun eieren in de mand van de IT-er. "IT moet vaak voor alle veiligheid zorgen, terwijl software-ingenieurs of programmeurs niet noodzakelijk in beveiliging zijn gespecialiseerd. Je kan een IT-er eigenlijk wel vergelijken met een huisarts. Hij is de perfecte eerstelijnshulp, maar inzake beveiliging heb je eigenlijk een neurochirurg nodig. Je zal nooit naar je huisarts gaan en zeggen, kijk, ik heb hier een kleine tumor, kan je die niet even weghalen. Daarvoor ga je naar een specialist. Vandaag laten we alle beveiliging aan IT, aan de huisarts, over. Je hoort me daarmee niet zeggen dat een IT-er dat niet kan, maar net zoals bij een huisarts of een neurochirurg gaat het om een andere specialisatie."

Ook in de opleiding van programmeurs en software-ontwikkelaars ontbreekt er volgens Pluvinage een cruciaal luik over cyberbeveiliging. "Onze scholen leiden fantastische software-ontwikkelaars op, die schitterende apps kunnen creëren. Maar als je kijkt in die code, is dat een ramp qua veiligheid. Je kan het vergelijken met een bestseller auteur die om de tien regels een schrijffout maakt. Die 'schrijffouten' in de programmeertaal maken de veiligheid van een app zwakker. Er bestaan programma's die automatisch checken op de meest bekende fouten en er zijn bedrijven die penetration testing doen (als test proberen om de programma's te hacken), vooraleer programma's of apps op de markt worden gebracht. Maar voor heel veel apps gebeurt die basischeck niet. Daarom moeten we ook de leraars trainen om op de veiligheidsaspecten te wijzen. Maar dat geldt evenzeer in andere opleidingen: wie een cursus boekhouden volgt, leert niks over factuurfraude. Maar bedrijfsaccountants kunnen er wel mee te maken krijgen."

DERTIG TEKENS

We zijn eerlijk gezegd wat met verstomming geslagen door de omvang van het probleem. Kan dan niemand cybercriminelen opsporen, vroegen we ons af? Zijn er dan geen organisaties die cybermisdaad bestrijden? "Alle landen hebben vandaag eigenlijk letterlijk een leger van cyberexperts," vertelt Pluvinage. "Frankrijk heeft een systeem van reservisten gelanceerd. In Duitsland zijn er in de nabije toekomst meer cyberexperten dan mariniers. Naast de National Security Agency (NSA) krijgen de Verenigde Staten een Cyber Command, de cybercrime afdeling van de Amerikaanse veiligheidsdiensten. Ook de Belgische Defensie beschikt over een legertje cyberexperten."

Ons land richtte ook het Center for Cyber Security Belgium op (www.ccb.belgium.be/nl). Het CCB geeft tips over veilig surfgedrag, adviseert over hoe computers en computernetwerken te beschermen op het werk en geeft info over opleidingen, lesmateriaal en internetveiligheid op school. Het CCB zet ook projecten op om vitale sectoren in België te beschermen tegen cyberaanvallen (sectoren die als cruciaal worden beschouwd voor de veiligheid van de bevolking: energie, mobiliteit, telecom, financiële sector, drinkwater, volksgezondheid en overheid). Hiervoor werd een Nationaal Cybernoodplan ontwikkeld.

Na het gesprek met Alexandre Pluvinage ben ik relatief gerustgesteld over de veiligheid van mijn spaarcentjes. Maar voortaan verzin ik tweemaal per jaar nieuwe paswoorden van minstens dertig tekens. U toch ook?

"Meer dan 99% van de aanvallen in bedrijven gebeurt via medewerkers."