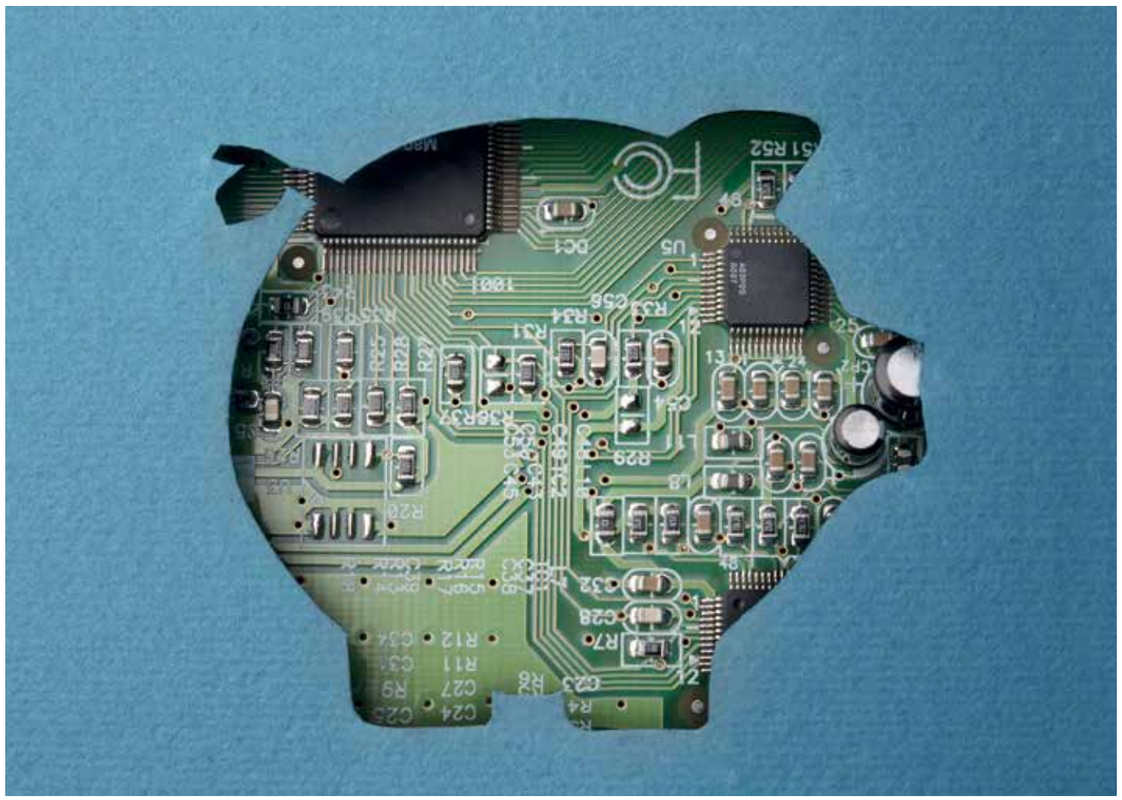
ONLINE BANKIEREN MET HET **VEILIGSTE** ENDPOINT-DEVICE

Als het gaat om geldtransacties is online bankieren voor ons de standaard geworden, zowel zakelijk als privé. Dat komt door drie belangrijke zaken: het is handiger en sneller voor de klant en goedkoper voor de bank zelf. Deze combinatie verklaart de populariteit van online bankieren en maakt het erg aantrekkelijk voor beide partijen.

Maar rechtmatige gebruikers zijn niet de enige geïnteresseerden in online bankieren - ook cybercriminelen houden de ontwikkelingen nauwlettend in de gaten. Het is dan ook niet verwonderlijk dat online bankieren steeds vaker succesvolle aanvallen te verduren heeft. Elk jaar verliezen bedrijven miljoenen euro's en banken zijn druk bezig deze toename een halt toe te roepen door hun beveiligingsinfrastructuur te verbeteren. Zo voegden ze bijvoorbeeld mechanismen toe die geldstromen analyseren en direct reageren als zich nieuwe en vreemde patronen voordoen aan de kant van de server. Tegelijkertijd werkten ze aan de klantinterface. Daar kwamen ze met nieuwe mechanismen die garanderen dat de identiteit van degene die inlogt en de integriteit van de transacties kloppen. Waarschijnlijk heb je een aantal van deze mechanismen al gezien: 2FA, TAN-nummers, mTAN, chipTAN, enzovoort. Cybercriminelen houden echter niet zomaar op als ze eenmaal een grote kans als online bankieren hebben ontdekt. Zij blijven hun tools verbeteren, zodat ze altijd de technische capaciteit hebben om al deze mechanismen aan te kunnen. Een escalerend actie-/reactie-conflict tussen banken en cybercriminelen dus. Banken hebben hierbij twee tegenstrijdige taken: enerzijds het beveiligen van de transactie - wat enorm veel controles en checks met zich meebrengt - en anderzijds het bieden van gebruiksgemak, wat betekent dat ze niet te opdringerig kunnen zijn bij het bevestigen van de identiteit en integriteit.



Als CTO van Qualys praat ik veel met securityprofessionals en IT-beheerders bij bedrijven die de beveiliging van hun online-bankierenomgeving willen verbeteren. Het is duidelijk dat de endpoints die gebruikt worden voor online bankieren de meest interessante doelwitten zijn. De gebruikers van deze endpoints zijn aan te wijzen door het gebruik van professionele netwerken als Xing en LinkedIn, wat hen ontvankelijk maakt voor phishing-aanvallen. Gelukkig kunnen wij als IT-beheerders genoeg doen om cybercriminelen een stap voor te blijven en zo niet het slachtoffer te worden van de strijd. Het belangrijkste is ervoor te zorgen dat de computing-uitrusting die we gebruiken niet over te nemen is door cybercriminelen. Je bedrijf heeft een aantal technische mogelijkheden om de endpoints in online bankieren te beveiligen. Ik zet ze op een rij, van minst veilig tot veiligst.

1. Een Windows-pc, die ook wordt gebruikt voor normale kantoorwerkzaamheden

Windows is veruit het populairste besturingssysteem voor desktops en laptops en wordt veel gebruikt voor e-mail, surfen en het bewerken van documenten. Helaas is het ook het populairste besturingssysteem om aan te vallen. Denk aan phishing-aanvallen die binnenkomen via je zakelijke en privémail en 'watercooler'-aanvallen, die profiteren van jouw surfgewoonten. Microsoft en andere softwareleveranciers als Adobe (Adobe Reader en Adobe Flash) brengen elke maand updates van hun software uit. Hiermee pakken ze de kritieke kwetsbaarheden aan die geliefd zijn bij cybercriminelen. Maar zelfs als de IT-afdeling de Windows-pc's volledig gepatcht onderhoudt en een up-to-date beveiligingssuite installeert, kunnen cybercriminelen hun gang gaan. Ze kunnen pc's infecteren met malware, je gebruikersnamen

Wolfgang Kandek

en wachtwoorden opslaan en 2FA- en TAN-verzoeken onderscheppen en omleiden. De cybercriminelen gebruiken zogeheten zero-day-kwetsbaarheden, zowel in Windows als in geïnstalleerde applicatiesoftware. Zero-day-kwetsbaarheden zijn niet bekend bij Microsoft en de grote securityleveranciers. Vaak blijft dat maandenlang zo en ondertussen gebruiken cybercriminelen ze in hun aanvallen. Met de huidige technologie op pc-gebied is de bescherming tegen zero-days bijzonder lastig.

Gebruik je een normale kantoor-pc voor online bankieren? Dan kun je de situatie iets verbeteren door een andere browser dan Internet Explorer te gebruiken voor je banktransacties. Op deze manier ontwijk je een klein deel van de infecties gericht op Internet Explorer. Ik raad de Google Chrome-browser aan als krachtig alternatief. In de afgelopen jaren is die het meest veerkrachtig gebleken in vergelijkende onderzoeken gericht op browsermisbruik. Maar zelfs met Chrome kan ik het niet aanraden te bankieren met een Windows-apparaat dat ook voor normale kantoorwerkzaamheden gebruikt wordt.

> 'Een bedrijf heeft een aantal technische mogelijkheden om de endpoints in online bankieren te beveiligen'

2. Pc's met andere besturingssystemen

De kans dat pc's met een besturingssysteem als Mac OS X of Linux worden aangevallen is minder groot dan bij hun Windows-soortgenoten. Beide besturingssystemen hebben echter hun eigen kritieke kwetsbaarheden. Denk aan de recente kritieke 'Shellshock'-kwetsbaarheid die Linux op een nogal eenvoudige manier binnentrad. Desalniettemin focussen cybercriminelen niet zozeer op deze besturingssystemen. De cybercrimetoolkits, verkrijgbaar op de zwarte markt, zijn over het algemeen alleen gericht op Windows. Een pc met een ander besturingssysteem dan Windows is een goede keuze voor als je online wil bankieren.

3. Een Windows-pc, die alleen voor bankieren gebruikt wordt

Een Windows-pc toewijzen voor alleen online bankieren is een goede keuze - daardoor is hij zeer bestendig tegen cyberaanvallen. Als je het apparaat up-to-date houdt met patches en beveiligingssoftware en je gebruikt de computer niet voor andere taken, dan verklein je het aantal mogelijke aanvallen aanzienlijk. De overige aanvalsvectoren zijn dan andere geïnfecteerde apparaten op je netwerk. De meest kritieke issues zijn gestolen beheerdersgegevens. Zo'n issue houd je onder controle door verschillende inloggegevens voor elk apparaat in te stellen. Kies dus voor een Windows-pc die je alleen gebruikt voor online bankieren. En dat is niet alleen mijn mening; Europese en Amerikaanse banken adviseren hetzelfde.

4. Mobiele platformen, tablets en smartphones

Tablets en smartphones hebben besturingssystemen die een generatie jonger en beter zijn dan je normale pc. Deze besturingssystemen zijn ontworpen met in het achterhoofd de ervaring met besturingssystemen voor algemene doelein-

den, zoals Windows, Mac OS X en Linux. Met dergelijke besturingssystemen weten we niet precies hoeveel gebruik klanten van het apparaat zullen maken en dus moeten we maximale flexibiliteit hanteren. Cybercriminelen misbruiken deze kracht en flexibiliteit. En dat heeft ons gebracht tot de situatie zoals hij nu is: we vernieuwen oude besturingssystemen met beveiligingsprogramma's, zoals automatische updaters, integriteitschecks en inbreukdetectiesystemen. Besturingssystemen voor tablets en smartphones zijn doelgericht geschreven met als uitgangspunt een krachtige beveiliging. Denk maar eens terug aan de eerste versies van de iPhone/iOS-combinatie van Apple, waarbij de scheiding tussen applicaties zo ver was doorgevoerd, dat kopiëren en plakken niet mogelijk was. Een aantal van deze beperkingen is soepeler geworden in de loop van de tijd. Het idee van een sterke beveiliging blijft echter van kracht. Het aantal infecties op mobiele apparaten is nu zeker twee orden van grootte kleiner dan in de pc-wereld. Bij de iPad en iPhone van Apple zijn infecties nagenoeg niet bekend. Een tablet is dus een erg goede keuze voor online bankieren.

5. Chromebase en vergelijkbaar

Google wilde zijn browser de universele applicatie voor consumenten maken en kwam daarom met een nieuw besturingssysteem: ChromeOS. In essentie is ChromeOS de Chrome-browser aangevuld met een minimaal aantal opties die noodzakelijk zijn om de browser te laten draaien, zoals netwerk- en gebruikersbeheer. Dat maakt ChromeOS nog beperkter in zijn mogelijkheden dan een mobiel besturingssysteem. Een aantal hardwareleveranciers heeft het nieuwe besturingssysteem gelicenseerd en kwam met computers die draaien op ChromeOS: laptops (de zogeheten Chromebooks) en desktops (Chromebox en Chromebase). Deze apparaten zijn mogelijk veel minder krachtig dan je gemiddelde pc, wat resulteert in een langere acculevensduur en een lagere prijs. Daarnaast zijn ze binnen een aantal seconden opgestart. Ook blijven ze altijd up-to-date door hetzelfde bewezen mechanisme voor continue, automatische updates als de Chrome-browser zelf. Tot op heden zijn securityonderzoekers er niet in geslaagd in te breken in een ChromeOS-apparaat, ondanks de uitgeloofde behoorlijke beloning van

100.000 dollar. Een Chromebase, -book of -box is een uitstekende keuze voor online bankieren (zelf gebruik ik nu bijna een jaar een Chromebase voor online bankieren, en hoewel mijn creditcard in die tijd twee keer vernieuwd is, voel ik me nog steeds veilig op dit platform).

En dat is 'm dan, mijn persoonlijke ranglijst voor online bankieren. Ik weet zeker dat er andere mogelijkheden zijn die ik niet behandeld heb, maar die wel aantrekkelijk zijn vanuit beveiligingsoogpunt. Ik heb bewust pc's die draaien vanaf LiveCD uitgesloten. Dit is een uitstekende manier om de integriteit van het besturingssysteem te garanderen, omdat het wordt geladen vanaf een alleen-lezen-medium (een cd of dvd). Toch denk ik dat het voor de meeste gebruikers onhandig is om steeds dat nogal trage proces, dat bij de meeste LiveCD's komt kijken, te doorlopen. Dat varieert natuurlijk per gebruiker, maar ik denk dat het voor de meesten te omslachtig is.

In mijn ogen is online bankieren een geweldige kans om beveiligingsmaatregelen afgestemd op het datagebruik van de gebruiker te implementeren. Vaak is het voor IT-beheerders een uitdaging om te bepalen tot hoeveel bedrijfskritische data een eindgebruiker toegang heeft. Maar in dit geval zijn gebruikers en het risico op verlies behoorlijk duidelijk gescheiden. IT-beheerders kunnen de beveiliging van het online bankieren binnen hun bedrijf verbeteren door te kiezen voor een van de hierboven genoemde opties - met uitzondering van het gebruik van een normale Windows-pc. Maar de klant beveiligen is slechts een van de componenten van je banktransacties. Het is verstandig om met je eindgebruikers te praten over het beveiligen van de instellingen aan de kant van de bankierenapplicatie. Als de bank two-factor authenticatie (2FA) biedt, zou het geactiveerd moeten zijn. Ik ben voorstander van apparaten speciaal voor 2FA. Ik geef dus eerder de voorkeur aan ChipTAN dan aan mTAN, aangezien de kans dat een aanvaller de transactie manipuleert veel kleiner wordt met een apart device. Evenzo is het slim om notificaties voor belangrijke transacties in te stellen. Hier kies ik liever voor sms- dan voor e-mailnotificaties, simpelweg omdat sms over het algemeen veel meer opvalt dan e-mail. Daarbij is versleuteling belangrijk om je bedrijfsdata en transacties die in behandeling zijn te beschermen. Zorg er dus meteen voor dat je eindgebruikers checken of ze een versleutelde verbinding hebben als ze inloggen op de website van je bank. Dit houdt in dat de pagina waar ze hun persoonlijke gegevens, zoals rekeningnummer en/of wachtwoord, intypen al versleuteld moet zijn. Ook moeten ze bevestigen dat ze een groen slot zien in de url-balk van de browser en dat de url overeenkomt met de naam van de bankwebsite waarop ze willen inloggen. Uitzonderingen hierop mogen ze niet accepteren. Dat garandeert dat ze daadwerkelijk een verbinding aangaan met de website die ze willen.

Wolfgang Kandek is CTO van Qualys