G DATA BIEDT PARTNERS EXTRA HANDVATTEN OM CYBERBEWUSTWORDING TE STIMULEREN

Beveiliging mobiele apparaten onder-geschikt bij meeste organisaties

Steeds vaker zien we berichten over de impact van cyberaanvallen op mobiele apparaten. Recentelijk melde de politie nog een toename in Flubot sms-berichten. Uit onderzoek van G DATA CyberDefense blijkt dat veel gebruikers valse sms-berichten domweg negeren. Bovendien wordt er ook bijna geen melding gedaan van valse sms-berichten. Volgens het bedrijf heeft het negeren flinke impact. Want wat niet geregistreerd is, is niet bekend en kan niet gebruikt worden bij het zoeken naar bronnen en oplossingen. *Tekst: Hans Steeman*

We spraken met Jihane Abid, de internationale salesmanager bij G DATA CyberDefense, over de stand van zaken rond mobiele dreigingen en welke aanpak G DATA daarvoor bedacht heeft. Het is een combinatie van software, training en opvoeding voor de bedrijven en hun medewerkers.

Te weinig meldingen

Uit onderzoek van G DATA CyberDefense, blijkt dat maar liefst 79% van de Nederlanders geen melding maakt van valse sms-berichten, zoals de Flubot sms-berichten die de Nederlandse markt recent hebben overspoeld. Het onderzoek van G DATA is daarover duidelijk. Het melden van valse sms-berichten en andere vormen van cybercrime is cruciaal, omdat alleen op deze manier onderzoek kan worden gedaan naar de daders. Alle aangiftes samen maken het mogelijk de informatie te combineren en geven inzicht in de handelswijze van cybercriminelen. Hoe meer informatie, hoe groter de kans dat een onderzoek succesvol kan worden afgerond. Jihane Abid: "Cyberrisico's voor mobiele apparaten worden vaak onderschat door mensen. Daar moet aan gewerkt worden. Onderzoek maakt ook duidelijk dat bijna niemand beschermende software op zijn mobiel heeft of een cyber-awarenesstraining volgt."

"Cyberrisico's voor mobiele apparaten worden vaak onderschat"

Extra handvatten voor partners

Volgens Abid is het belangrijk om zowel oplossingen te bieden op technisch vlak als op menselijk vlak. Het installeren van een securityoplossing voor je mobiel[1] is een eerste stap. Installeer daarnaast ook alleen applicaties die worden verspreid door bekende app-stores en gebruik de instellingen van je telefoon om het downloaden van apps van andere bronnen uit te schakelen. Dit klinkt eenvoudig, maar toch hebben de meeste mensen geen mobiele securityoplossing op hun telefoon. Sterker nog, de meeste

telefoons voor zakelijk gebruik (78,3%) zijn niet eens beveiligd, terwijl er toch vaak vertrouwelijke informatie op staat. Mobiele apparaten worden vaak getroffen door phishing, omdat gebruikers een bericht krijgen van een onbekende met een kwaadaardig linkje. Bij een goede mobiele securityoplossing wordt een dergelijke aanval onmiddellijk onderschept zodra je toch op dat linkje klikt.
Daarnaast is het belangrijk om vooral goed op te letten en waakzaam te blijven. Soms zijn accounts gehackt, waardoor het net lijkt alsof een bekende uit je netwerk een bericht stuurt. Als bijvoorbeeld een bekend iemand in één keer een sms stuurt met een link, terwijl deze normaliter altijd via social media communiceert, moeten de alarmbellen gaan rinkelen. Het is daarom verstandig voor organisaties om medewerkers structureel te trainen[2], zodat menselijke fouten kunnen worden voorkomen.

MKB moet in actie komen

Met name MKB-bedrijven nemen vaak geen maatregelen om cyberbewustzijn te verbeteren onder medewerkers. Om bedrijven ewrmee te confronteren dat cyberbewustzijn wel degelijk belangrijk is om cyberaanvallen te voorkomen, biedt G DATA nu phishing simulatietests aan.
Jihane Abid: “Met onze phishing simulatie kunnen klanten een (fake) phishing mail sturen naar de medewerkers. Op deze manier kunnen medewerkers geconfronteerd worden met hun gedrag. Iedereen die op de link klikt, krijgt via de landingspagina direct gerichte feedback over de signalen waaraan je phishing kunt herkennen. Zo zijn je medewerkers beter voorbereid op een volgende phishingaanval. Er is een ruime selectie aan meertalige phishing-templates om medewerkers te confronteren met realistische phishing e-mails en sms-berichten op elk gewenst apparaat.”
Partners van G DATA kunnen deze phishing simulatie nu ook aanbieden. Volgens Abid biedt dit een uitermate goede kans om bedrijven die twijfelen aan een cyber-awarenesstraining over de streep te trekken. “Gezien onze phishing simulatie ook per keer is af te nemen, kunnen partners het ook eenmalig aanbieden bij bedrijven die twijfelen. Hierdoor zullen ze zelf ervaren hoe vaak er menselijke fouten worden gemaakt. Het is echter niet de bedoeling om medewerkers te ‘shamen’ omdat ze op een verkeerd linkje hebben geklikt, maar juist de directie te overtuigen dat ze stappen moeten ondernemen om hun veiligheidscultuur te verbeteren.”


Jihane Abid

79%

van de slachtoffers meldt een sms-aanval niet

Succesvol ondernemen doe je samen

Daarnaast gaat G DATA ook zijn fysieke events weer oppakken om partners te updaten en te trainen over hun nieuwste oplossingen. Verder is het bedrijf ook altijd op zoek naar nieuwe partners die het verschil kunnen maken. Abid: “Wij zijn altijd op zoek naar nieuwe partners, schroom daarom niet om contact op te nemen met het lokale team. Bovendien is het fijn dat we weer kunnen nadenken over fysieke events. Succesvol ondernemen, doe je immers samen en het is leuker als je elkaar ook regelmatig ziet.” ■

[1] *www.gdata.nl/mobile-security-android*

[2] *www.gdata.nl/bedrijven/security-awareness-training*