WHITEPAPER CYBERAANVAL PETYA

IEDEREEN KAN SLACHTOFFER WORDEN VAN EEN HACK

Deze whitepaper behandelt de meest recente cyberaanval die de wereld trof; het Petya virus. Nog steeds zijn er mensen die denken dat het zo'n vaart niet zal lopen en dat zij geen slachtoffer worden. Niets is minder waar. Daarom in deze whitepaper uitleg over het virus en hoe u zichzelf hiertegen, en tegen andere aanvallen, kunt wapenen.

WHITEPAPER CYBERAANVAL PETYA

IEDEREEN KAN SLACHTOFFER WORDEN VAN EEN HACK

Wat is er aan de hand?

Dinsdagmiddag 27 juni werden wereldwijd bedrijven getroffen door een nieuw ransomwarevirus. Dit virus trof o.a. het Deense scheepvaartbedrijf Maersk en dochteronderneming APM Terminals in de Rotterdamse haven. Het virus verscheen oorspronkelijk in de Oekraïne maar heeft zich inmiddels uitgebreid over de hele wereld.

Beveiligingsonderzoekers van het Amerikaans antivirussoftwarebedrijf en BrainCap-partner Webroot bevestigen dat dit virus, net als het Wannacry-virus, Windowssystemen aanvalt. Wat er met uw bedrijf gebeurt als u wordt aangevallen moge duidelijk zijn. Uw bedrijfsvoering ligt stil en uw bestanden zijn niet langer beschikbaar. Om over het financiële verlies nog maar te zwijgen.

Wat doet het virus?

Het is nog niet duidelijk of het virus een variant is op het Petya virus, dat eerder ingezet werd bij een cyberaanval, of een nieuw virus. Het wordt daarom ook wel NotPetya genoemd. Aanvankelijk werd gedacht dat het virus de Master File Table (MFT), een bestand dat cruciaal is voor de harde schijf, versleutelde maar inmiddels is gebleken dat het virus delen van de schijf wist. In de praktijk betekent dit dat het virus het hele systeem uitschakelt, dat daardoor niet meer op kan starten. De eindgebruiker krijgt een op DOS lijkend bericht in zijn scherm te zien, dat om betaling van 300 dollar in Bitcoins om losgeld vraagt.

Hiermee leek het om ransomware te gaan, omdat het slachtoffer in eerste instantie zijn bestanden alleen terug kon krijgen door losgeld

DE WERELD ONDER VUUR

Het is onduidelijk wie achter (Not)Petya zit.

Omdat het gijzelvirus zeer geavanceerd is, speculeren beveiligingsonderzoekers dat een overheid verantwoordelijk zou kunnen zijn. Dat kan echter zeer lastig te bewijzen zijn.

aan de cybercrimineel te betalen. Echter, het e-mailadres dat wordt gebruikt door de hacker is geblokkeerd door de provider. Dit betekent dat slachtoffers hun bestanden niet terug kunnen krijgen, zelfs niet na het betalen van het losgeld. De kans is daarom groot dat het niet om ransomware gaat, maar dat het enige doel van het virus is om schade aan te richten.

Petya, of NotPetya, is complexer dan WannaCry en probeert om via het netwerk toegang te krijgen tot andere computers, waardoor ook computers met de laatste updates besmet kunnen raken. Hoe bedrijven in de eerste plaats met de nieuwe ransomware besmet raken is nog niet duidelijk. Vermoed wordt dat in ieder geval malafide e-mails een rol spelen.

Wanneer word je slachtoffer van een cyberaanval?

Iedereen kan slachtoffer worden van een hack want ook hier geldt: gelegenheid maakt de dief. Net als bij een fysieke inbraak gaat een inbreker niet selectief te werk. Hij breekt in bij het eerste huis dat niet goed beveiligd is. Hetzelfde geldt voor een hacker. Of het nu gaat om een relatief kleine MKB-er of een multinational, als de voordeur dicht is en de achterdeur open, dan kan een hacker zo naar binnen. Met andere woorden, slachtoffer worden van een hacker hangt af van een combinatie van factoren.

Wat betekent dit voor u?

In ieder geval dat u méér nodig heeft dan alleen antivirus en anti-malware en dat u ook zaken als patchmanagement, een back-up oplossing, awareness bij uw personeel, wachtwoordmanagement en gebruikersrechten goed op orde moet hebben. In het geval van Petya kon het virus toeslaan omdat bij de slachtoffers niet de laatste patches waren geïnstalleerd. Dat kon dus bij een bedrijf als Maersk gebeuren.

Wat kunt u ertegen doen?

Door een bedrijf constant te monitoren, te beheren en in te grijpen indien nodig, zijn veel gevaren te voorkomen en is een bedrijf zo veilig mogelijk. Dit geheel van maatregelen valt onder de noemer Managed ICT Services. Het specifiek laten testen of uw bedrijf gehackt kan worden, wordt gedaan door certified ethical hackers en valt onder Cyber Security.

Endpoint security is een belangrijk onderdeel in het pakket van maatregelen dat u nodig heeft om uw niveau van beveiliging zo hoog mogelijk te maken. In de afgelopen twee cyberaanvallen was dit voldoende, maar dit is niet altijd het geval. U kunt ervan uitgaan dat de volgende aanval nog slimmer is. Maar wist u bijvoorbeeld dat het gebruik van Dropbox of OneDrive bij uitstek een manier is waardoor virussen zich op eenvoudige wijze kunnen verspreiden?

Hoe kunnen wij u beschermen?

Een efficiënte manier om uw bedrijf te beschermen, is door een managed services provider uw huidige online veiligheid te laten beoordelen. Dit kan BrainCap op verschillende manieren voor u verzorgen. Met een eenvoudige en vrijblijvende checklist waarin we cruciale ICT-punten nalopen, uitgebreider met de (betaalde) BrainCap Cyber Security QuickScan, een netwerkmonitortest waarbij de focus op beveiliging en kwetsbaarheden ligt, of met de BrainCap Baseline Security Check, waarmee we uw totale managed services onder de loep nemen. We komen graag bij langs om te inventariseren wat uw behoefte is.

Het belangrijkste: geen paniek

Webrootgebruikers en klanten van BrainCap Managed ICT Services die BrainCap Endpoint Security hebben, zijn beschermd tegen deze nieuwe variant van het Petya virus. En wanneer u was voorbereid naar aanleiding van WannaCry en de kwetsbaarheden waar dat virus gebruikt van maakte heeft verholpen, dan bent u veilig voor de Petya variant.

Ondanks alle verhalen die nu de ronde doen, zijn er maatregelen te treffen om een hack te voorkomen. BrainCap Managed ICT Services verzorgt dit voor zowel het MKB als voor grotere organisaties. Wanneer wij uw bedrijf in beheer hebben, kunnen wij zien of de patches gedraaid zijn, zoals bij het Petya virus van gisteren. Bij klanten waarbij de patches niet up-to-date waren, is dit virus tegengehouden door Webroot.

Wilt u niet langer het risico lopen dat uw bedrijf enkele dagen niet operationeel is, met alle bijkomende kosten van dien, en neemt u uw online veiligheid serieus, neem dan contact met ons op via info@braincap.nl

PS Al onze klanten hebben de afgelopen aanvallen overleefd.

BRAINCAP
SOFTWARE & SERVICES