Tien tips om de pijlen van Cupido te ontwijken

14-02-2017 09:42

Door Alastair Paterson
Ceo en co-founder van Digital Shadows

Vandaag is het weer Valentijnsdag. Cupido zal zijn jaarlijkse ronde gaan maken en geliefden met zijn pijlen in het hart raken, zodat zij op elkaar verliefd worden. Wie wil er nu niet door zo'n pijl geraakt worden? Tot zover de romantische versie van Valentijnsdag, want rondom Valentijnsdag circuleren er ook pijlen die je als retailer liever wilt ontwijken. We hebben het hier over cybercriminaliteit. Voor veel cybercriminelen is de periode rondom Valentijnsdag dé tijd om toe te slaan bij retailers, recht in het hart van hun business.

In februari 2016 constateerden wij dat veel online bloemisten een flinke stijging in hun websitetraffic hadden. Al gauw bleek dat deze traffic boost niet alleen veroorzaakt werd door klanten die last-minute nog een bloemetje wilden bestellen voor hun geliefden. Deze boost werd veroorzaakt door cybercriminelen. Met een DDoS-aanval wisten zij vele online bloemisten rondom hun drukste tijd van het jaar flink te hinderen. Dit heeft tot veel problemen geleid en er zelfs voor gezorgd dat sommige websites volledig plat kwamen te liggen of vergrendeld werden. De getroffen retailers moesten vervolgens een borgsom betalen voordat zij hun werkzaamheden konden voortzetten. In die tussentijd liepen ze veel aankopen mis.

Het komt relatief vaak voor dat cybercriminelen speciale piekmomenten, zoals Valentijnsdag of Kerst, uitkiezen om toe te slaan. Dan valt er voor de retailers immers het meeste te verliezen en zijn zij gewilliger om

losgeld te betalen. Cybercriminelen kijken daarbij zorgvuldig hoe zij zoveel mogelijk winst kunnen maken met minimale inspanningen en dus gaan ze op zoek naar zwakke plekken in IT-systemen. Digital Shadows monitorde dat cybercriminelen in 2016 tijdens Valentijnsdag Shellshock gebruikten, een kwetsbaarheid dat in veel Linux, UNIX en Mac OS X-systemen zit. Deze kwetsbaarheid hadden zij het jaar daarvoor ontdekt. Ze hebben geduldig een jaar gewacht en zich uitvoerig kunnen voorbereiden op hun aanval.

Meerdere momenten in het jaar, tijdens speciale dagen of specifieke actualiteiten, kunnen een golf aan aanvallen triggeren die gericht zijn op een specifieke branche of regio. Het is daarom belangrijk dat organisaties weten waar hun kwetsbaarheden zitten, zodat zij de juiste security-maatregelen kunnen treffen. Hier zijn tien acties die je kunt ondernemen om het risico op cyberaanvallen en afpersing in te perken.

1. Breng zwakke plekken in kaart: De juiste configuraties en het uitvoeren van een patch zijn belangrijke onderdelen van je verdedigingsstrategie. Wanneer het hier misgaat, zet je de deur open voor kwaadwillenden. Zorg dat je weet waar welke zwakke plekken zitten, zodat je ook beter kan prioriteren welke kwetsbaarheden je als eerste gaat herstellen of opnieuw gaat configureren.

2. Train gebruikers: Zorg dat je medewerkers bewust zijn van het feit dat zij slachtoffer kunnen worden van ransomware of een DDoS-aanval. Train hen in het herkennen van het gevaar, maar zorg ook dat ze weten hoe ze een aanval moeten rapporteren. Daarbij dienen ze ook geïnformeerd te worden over de risico's van nalatig wachtwoordgebruik.

3. Maak regelmatig back-ups: Maak back-ups van je data in de cloud of on-premise en verifieer of deze locaties waar je de data plaatst veilig zijn. Zorg dat deze back-ups los staan van het bedrijfsnetwerk en van de apparaten die gekoppeld zijn aan het bedrijfsnetwerk.

4. Houd data gescheiden: Categoriseer data op basis van waarde. Vervolgens kan een fysieke of logische scheiding van de netwerken worden gemaakt voor de verschillende functies.

5. Beheer van het gebruik van accounts met beperkte rechten: Zorg ervoor dat het principe van het gebruik met minimale rechten wordt toegepast, niet alleen voor data, maar ook voor toegang tot bestanden, directory en het netwerk.

6. Wachtwoordbeheer: Maak gebruik van een enterprise password management oplossing. Dit is niet alleen nuttig voor een veilige opslag en het delen van data, maar het helpt ook om sterke en diverse wachtwoorden te creëren. Zorg ervoor dat je, in het geval van een noodsituatie, een password reset proces paraat hebt. Hier dienen alle accounts van de gebruikers in te worden opgenomen, niet alleen Microsoft Active Directory-accounts. Mochten je wachtwoorden in verkeerde handen vallen, dan kun je alles eenvoudig aanpassen.

7. Check de authenticiteit van de gebruikers: Dit doe je door meerdere authenticatie-stappen in te bouwen bij het gebruik van externe services, zoals Microsoft Outlook Web Access, Secure Sockets Layer Virtual Private Networks, maar ook voor software-as-a-service diensten, zoals applicaties van Google, Office365 en Salesforce.

8. Ontwikkel een plan van aanpak: Het is verre van ideaal als je pas gaat nadenken welke acties je kunt ondernemen tegen een aanval als je er middenin zit. Ontwikkel daarom interne processen op voorhand. Zie het als een soort evacuatieplan. Wie moet je inschakelen voor hulp, wat moeten we uitschakelen, maar ook: wat communiceren we aan onze klanten? Wees hierin zorgvuldig, zodat je een volledig draaiboek ter beschikking hebt dat je direct kunt uitrollen in het geval van een dergelijke calamiteit.

9. Verdiep je in dreigingen: Als je begrijpt hoe cybercriminelen te werk gaan en van welke tools zij gebruikmaken, is het makkelijker om je hiertegen te wapenen. Het stelt je verder in staat om prioriteiten te stellen, omdat je beter weet welke dreigingen specifiek voor jou gelden. Er zijn organisaties, zoals Digital Shadows, die nauwkeurig kunnen monitoren welke dreigingen voor jouw onderneming gevaarlijk zijn.

10. Prioriteer services: Bepaal welke diensten echt noodzakelijk zijn om je business draaiende te houden. Maak voor deze diensten de beste security-afspraken met je leverancier of IT-dienstverlener. Bedenk eens goed wat downtime betekent voor je organisatie. Hoeveel verlies draai je als je een uur, of een dag niet bereikbaar bent? Weegt dit bedrag op tegen de securitykosten? Maak op basis van deze inzichten een zorgvuldige afweging.

Cybercriminelen zullen altijd misbruik blijven maken van speciale events, zoals Valentijnsdag, bij hun aanvallen. Op dergelijke dagen kunnen ze immers de meeste schade aanrichten en zijn hun slachtoffers gewilliger om de borgsom te betalen. Je kunt je hiertegen wapenen. Bewustwording is hierbij de belangrijkste eerste stap. Als je weet hoe cybercriminelen te werk gaan en weet wat de kwetsbaarheden binnen je organisatie zijn, neem dan concrete stappen om proactief je data, infrastructuur, medewerkers en klanten te beschermen.