Achter Het Nieuws

In deze rubriek geven enkele IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over de informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kunt u sturen naar ibmagazine@pvib.nl

VLUCHTEN VAN LOT POLISH AIRLINES GEANNULEERD DOOR CYBERAANVAL

Meer dan 1000 passagiers strandden onlangs op het vliegveld van Warschau nadat hackers op de systemen van het grondpersoneel hadden ingebroken. Door de hack kwamen verschillende vluchten te vervallen en raakten er een aantal vertraagd. Wat betekent zo'n hack voor de passagiers en wie heeft er baat bij om de controle over deze systemen over te kunnen nemen? Onze redacteuren laten er hun licht over schijnen.

Rachel Marbus

Laten we eens verder doordenken waarom een aanval op luchtvaart interessant kan zijn. Stel je nu eens voor dat ze daadwerkelijk een goede ingang vinden. Je gegevens zullen maar zo op straat komen te liggen! Vluchtgegevens omvatten dankzij de verplichte uitwisseling daarvan inmiddels een schat aan informatie. Niet alleen wie je bent (tot in detail), maar ook waar je woont, waar je heen reist, hoe lang, met wie, alsook financiële data. Ik kan me heel goed voorstellen dat dit een zeer gewilde database is om te kraken. In een mum van tijd heb je van honderden mensen alle mogelijke gegevens om zonder enige moeite rekeningen leeg te trekken en identiteitsfraude te plegen. Om nog maar te zwijgen over het feit dat ze weten waar je woont en wanneer je dus niet thuis bent. Over die vertraging zou ik me dan ook niet zo'n zorgen maken.

André Koot

Het zal je maar gebeuren, heb je 'State of the Art' computer-systemen en dan word je gewaarschuwd door het CERT van je overheid dat je wordt aangevallen. State of the Art wil zeggen dat je het nieuwste van het nieuwste in huis hebt. Als je dan wordt aangevallen, dan is dat niet alleen een probleem voor je eigen organisatie, maar zeker ook voor andere organisaties die minder dan State of the Art ICT in huis hebben. Ja, serieuze problemen. Inmiddels zijn we al een paar dagen verder en is er iets meer duidelijk over de aanval: we weten ook na heel veel onderzoek niet precies wat er is gebeurd. Het lijkt op een DDoS aanval op de grondsystemen. Hierdoor werd het maken van vluchtplannen onmogelijk gemaakt. En het ergste is, het gaat om systemen die ook andere luchtvaartmaatschappijen gebruiken. Dus iedere andere maatschappij is kwetsbaar…

Een DDoS-aanval? The first attack of it's kind? Dan ben ik meteen geprikkeld om een boel rare dingen te zeggen. Een DDoS-aanval impliceert dat heel veel computers tegelijkertijd aanvragen sturen naar een IP-adres of domein. Dat gebeurt alleen nooit toevallig, het is niet zo dat ergens een idioot stuk voor stuk alle IP-adressen aanvalt. Nee, dat gebeurt vanaf het openbare internet naar specifieke domeinen of services. Die moeten ook op het openbare internet beschikbaar zijn. Eerste misschien wel domme vraag is dus: Waarom zijn de grondsystemen op het openbare


Rachel Marbus


André Koot


Dennis Baaten


Maarten Hartsuijker

internet aanwezig? Tweede vraag zou dan zijn: hoe weet iemand dat te vinden? Er zijn zoveel IP-adressen, hoe weet je zoiets te vinden en aan te vallen. Nee, dat geldt dus niet alleen voor deze grondsystemen, dat geldt voor elke service op het internet. Geen DDoS zonder publieke aanwezigheid. Dus wat doet zo'n besturingssysteem op het internet?

Onlangs was er al enige commotie over de dreiging dat passagiers in een vliegtuig toegang zouden kunnen krijgen tot de in-flight systemen van het vliegtuig. Ook hier weer de vraag: Waarom zou dat het geval kunnen zijn? Publieke, onvertrouwde systemen horen niet op interne vertrouwde systemen thuis. Dat heeft niets te maken met cyber, dat is gewoon een gevolg van het hanteren van het need-to-know principe. Maar ja, we weten allemaal dat er veel meer interne systemen gewoon op het internet hangen, de meeste daarvan niet eens beveiligd ("Veere" – "Veere" is een fraai voorbeeld). Voor de meeste van die systemen is een DDoS-aanval misschien niet eens heel spannend, als de nood aan de man komt kun je altijd in plaats van remote beheer, fysieke toegang gebruiken om de besturing over te nemen. Maar waarom een grondsysteem van een luchtvaartmaatschappij open en bloot op het internet? Dan vraag je om ongelukken. Ik vrees dat ze bij LOT nog wel meer (niet State of the Art) security problemen hebben.

Overigens zijn er inderdaad ook berichten dat er ongeautoriseerde toegang tot het netwerk van LOT was verkregen. Ongeautoriseerde toegang? Dat klinkt als een ander probleem. Ik denk dan meteen aan social engineering. En daar is niets State of the Arts aan. Dat is gewoon een teken van onvoldoende awareness. Maar dat past niet meer in mijn reactie.

Dennis Baaten (gastbijdrage)

Security Consultant bij Baaten ICT Security

Wat een hacker motiveert, is vaak moeilijk te achterhalen. Soms wordt de motivatie duidelijk omdat een aanval wordt opgeëist door een bepaalde groepering, maar dat is hier vooralsnog niet het geval. Dan kan ik alleen maar raden naar de motivatie van de hacker, en dan kom ik op fanatisme, activisme of terrorisme. Feit is dat er altijd wel iemand baat heeft bij het hacken van een computersysteem. Het is dus niet de vraag of je slachtoffer wordt van een aanval, maar wanneer. Als het zover is, kan een bedrijf zich alleen nog onderscheiden door de wijze waarop men op een dergelijke situatie reageert. Met name in 'gevoelige' branches zoals de luchtvaartindustrie, is een snelle en adequate reactie misschien wel letterlijk van levensbelang. Doordat dergelijke aanvallen (of pogingen daartoe) een grote impact hebben op de publieke moraal, krijgen ze vaak veel media-aandacht. Als gevolg hiervan kan de reputatie van een luchtvaartmaatschappij behoorlijk beschadigd raken, waardoor het vertrouwen van reizigers snel kan teruglopen. Niemand stapt tenslotte graag in een vliegtuig van een maatschappij die de beveiliging van zijn computersystemen (mogelijk) niet op orde heeft. In een reactie liet de luchtvaartmaatschappij dan ook weten dat "de veiligheid van passagiers niet in het geding is geweest", en dat "er gebruik wordt gemaakt van moderne computersystemen, en de methode van de aanval mogelijk gevolgen heeft voor andere luchtvaartmaatschappijen". Het is onbekend wat er daadwerkelijk is gebeurd, maar marketingtechnisch is de gegeven reactie een slimme zet. Feitelijk ongetwijfeld correct, maar door te stellen dat dit ook bij de concurrent had kunnen gebeuren, wordt het incident gerelativeerd in de hoop dat het vertrouwen voortduurt. Onder de noemer "never waste a good crisis" zou het mooi zijn wanneer dit incident resulteert in meer veiligheid. Medewerkers van de vliegtuigmaatschappij worden weer even op scherp gezet, waardoor momentum ontstaat dat je slim moet gebruiken om noodzakelijke veranderingen door te voeren. Dan is de overlast voor al die passagiers in ieder geval niet voor niks geweest.

Maarten Hartsuijker

Dagelijks hebben vele bedrijven te maken met de gevolgen van computermisbruik. Ze lopen door computerinbraken financiële schade op of hebben te kampen met verstoringen (bijvoorbeeld na de installatie van een Cryptolocker). Een computerinbraak in een netwerk van grondpersoneel op een Poolse luchthaven is eigenlijk geen bijzonder nieuws meer. Maar sinds 9/11 zijn we collectief natuurlijk extra verontrust als er iets misgaat in de luchtvaartsector. De vraag of er vluchten gevaar hebben gelopen, is dan snel gesteld. Het antwoord kwam ook erg snel. Binnen 5 uur was het probleem "verholpen" en konden er weer vluchtplannen verwerkt worden en vliegtuigen vertrekken. Als je zelf wel eens een inbraak in een netwerk hebt moeten analyseren weet je dat 5 uur heel erg snel is. Verder dan symptoombestrijding kom je vrijwel zeker niet, tenzij je ervan overtuigd bent dat het iets kleins is geweest. Op internet waren er dan ook diverse beveiligingsspecialisten die hun twijfels hadden bij deze "cyberaanval". Maar of het nu een cyberaanval is geweest, of een interne medewerker die ongeautoriseerd een domme fout heeft gemaakt: het voorval maakt weer eens overduidelijk hoe afhankelijk we zijn van IT en hoe belangrijk een goede business continuity planning is.