Insiders guide to cyber security

Deel 1: Wat is de impact van cybercrime op uw organisatie?

internedservices.nl | 0299 476 185

kpn internedservices

IN DEZE WHITEPAPER

In deze whitepaper worden verschillende gevaren omschreven en wordt ingegaan op de impact van cybercriminaliteit op het bedrijfsleven.

We spreken in dit document over cybercrime: cybercriminelen die geld verdienen aan data. Overige vormen van laster worden achterwege gelaten waaronder hacktivisten, terroristen, vandalen en jonge wizkids. Tevens wordt er gesproken over de dreiging op IT-systemen. De dreiging op mobiele netwerken is niet minder belangrijk maar is op moment van schrijven nog altijd vele malen lager.

Nu met moderne techniek wordt ingezet op een "connected" wereld - eentje die altijd online is en waarbij organisaties en devices gebruikmaken van elkaars data - is er geen weg meer terug. De beschikbaarheid van data en IT zijn een noodzakelijke voorwaarde voor de dagelijkse bedrijfsvoering. Deze afhankelijkheid maakt ook kwetsbaar voor cyberaanvallen. De steeds verdergaande digitalisering van de bedrijfsvoering, dienstverlening en businessmodellen vraagt daarom om een waterdicht cybersecurity-beleid.

Data is geld waard

Het wordt voor criminelen steeds interessanter om een kijkje in uw digitale keuken te nemen. Data kan veel prijsgeven over business-strategieën en is waardevol voor concurrenten. Met klantgegevens kan gefraudeerd worden. Data kan stemgedrag of beurskoersen beïnvloeden of kan worden 'gekaapt' waarna losgeld wordt geëist. De schade kan in sommige gevallen oplopen tot in de miljarden euro's. Het moge duidelijk zijn: zolang data waarde heeft, blijven cybercriminelen toeslaan.

Samenwerken tegen cybercrime

Al jaren slaan cloudproviders, het bedrijfsleven, de wetenschap en de politiek de handen ineen en doen er alles aan om deze vorm van criminaliteit tegen te gaan. De website internet.nl, een initiatief van onder andere het Ministerie van Economische Zaken en de Dutch Hosting Providers Association, is daar een goed voorbeeld van. Tevens werden er de laatste jaren verschillende nieuwe richtlijnen en wetten opgesteld waaronder recentelijk de Meldplicht datalekken en heeft de Nederlandse overheid meerdere awareness campagnes gelanceerd. Dit soort initiatieven verbetert het inzicht in het type en aantal aanvallen op het bedrijfsleven. Met deze kennis in pacht worden organisaties steeds beter in het nemen van maatregelen tegen cybercriminaliteit.

Toch kan nog lang niet iedere organisatie zich voldoende weren tegen cybercrime. En dat is op zijn zachtst gezegd opmerkelijk. Juist nu het internet onmisbaar is geworden, is een goede voorbereiding het halve werk.

Deze whitepaper bestaat uit twee delen. In dit eerste deel zal ingegaan worden op de gevolgen van cybercrime en de meest voorkomende vormen ervan. Met een aantal concrete voorbeelden wordt duidelijk gemaakt hoe eenvoudig het kan zijn voor cybercriminelen om schade aan te richten, niet alleen financieel, maar ook ten aanzien van reputaties en zelfs op landelijk politiek niveau. In het tweede deel van deze whitepaper zal uitgebreid aandacht zijn voor het opstellen van een cybersecuritybeleid dat kan voldoen aan de constant veranderende eisen van deze tijd.

DE IMPACT VAN CYBERCRIME

Cybercriminaliteit is kostbaar voor de organisaties die ermee te maken krijgen. Door data buit te maken of data tijdelijk te blokkeren (ransomware) kan relatief makkelijk geld worden verdiend door cybercriminelen. Veel organisaties gaan snel over tot betaling aangezien de schade van het niet kunnen werken vaak vele malen groter is dan het gevraagde losgeld.

Lang niet iedere cybercrimineel gaat voor het snelle geld. Met een “integrity hack” neemt de aanvaller de tijd en ontwerpt een aanval die in potentie nog veel meer schade kan aanrichten. Nadat de aanvaller het bedrijfsnetwerk is binnengedrongen, wordt een klein stukje van het communicatie- of transactieproces herschreven. Een bekend voorbeeld is een hack van financiële instellingen door de criminele organisatie Carbanak. Tijdens de aanval werd onder andere een stukje code in het transactietraject aangepast voor een select type bankrekeningen. Zo konden ongemerkt bedragen worden weggesluisd, naar schatting leverde dit de aanvallers 1 miljard dollar op[1].

De impact van een digitale aanval kan moeilijk worden overschat. Een hack kan alleen al intern voor verwarring zorgen. Daarnaast kost een aanval in bijna alle gevallen veel geld. Zelfs als er geen directe nadelige gevolgen zijn, zal geïnvesteerd moeten worden in het op peil brengen van de cybersecurity van de organisatie.

Niet alleen is een digitale aanval kostbaar, cybercrime heeft ook gevolgen voor de integriteit van uw systemen en uw reputatie. **Op de volgende pagina ziet u een een aantal voorbeelden van mogelijke schades.**

Cybercriminelen organiseren zich steeds beter en door de toenemende connectiviteit, wordt cybercrime steeds volwassener. Of u zich nu richt op de veiligheid van uw eigen systemen of zich zorgen maakt over de impact van cybercrime op veel grotere schaal: u kunt het zich niet meer veroorloven om stil te blijven zitten.

[1] https://www.computable.nl/artikel/nieuws/security/5230422/250449/cyberbankrover-carbanak-steelt-miljard-dollar.html

INTEGRITEITSSCHADE DOOR EEN DIGITALE AANVAL

Reputatieschade
klanten, businesspartners of de concurrent kunnen vraagtekens plaatsen bij de veiligheid van uw systemen of werkwijze wanneer een hack wereldkundig wordt gemaakt. Reputatieschade is meestal de reden waarom bedrijven een aanval stilhouden.

Politieke reputatieschade
In sommige gevallen verkondigen cybercriminelen ideologische of politieke boodschappen via de gehackte website of social-mediakanalen van een bepaalde organisatie. Vaak zijn dit boodschappen die haaks staan op de boodschap van deze organisatie en de opvattingen van haar doelgroep. Deze vorm van cybercriminaliteit komt niet veel voor in Nederland.

Verminderde bereikbaarheid
Een DDoS-aanval levert meestal geen permanente schade op maar zorgt ervoor dat een website enige tijd niet bereikbaar is. In het geval van een grote webshop of een SaaS-oplossing richt een tijdelijk slechte bereikbaarheid directe financiële schade aan. Wanneer de aanval in het nieuws wordt besproken is reputatieschade een tweede gevolg van verminderde bereikbaarheid.

Niet voldoen aan wet- en regelgeving
Als persoonsgegevens op straat komen te liggen naar aanleiding van een hack, is een organisatie verplicht dit te melden bij de Autoriteit Persoonsgegevens. Als blijkt dat de beveiliging van deze data niet op orde was, kunnen forse boetes worden opgelegd.

VEEL VOORKOMENDE VORMEN VAN CYBERCRIME

In de jaren ‘90 waren de meeste huishoudens en organisaties redelijk goed voorbereid op een virus-aanval op computers. Tegenwoordig is het beveiligen van het eindpunt - het device - al lang niet meer afdoende en is netwerkbeveiliging het belangrijkste focuspunt.

Uit onderzoek blijkt dat cybercriminaliteit Nederlandse organisaties jaarlijks 10 miljard euro kost.[2] Lang niet iedere crimineel gaat echter hetzelfde te werk: waar de één verstand van zaken heeft en zichzelf ongemerkt door uw netwerk manoeuvreert kan de ander met relatief weinig kennis en kant-en-klare software uw website uren platleggen. Mede door de vele vormen van cybercrime is het moeilijk te bestrijden.

Het saboteren van systemen

Eén van de meest zichtbare online bedreigingen is een DDoS-aanval. DDoS staat voor Distributed Denial of Service, oftewel het saboteren van een website, de IT-infrastructuur of systemen. In een periode van 30 minuten tot enkele uren - in enkele gevallen zelfs dagenlang - worden de servers waarop een website of private cloud-omgeving draait bestookt met een eindeloze hoeveelheid verbindingsverzoeken of informatie. Het gevolg: servers die vastlopen waardoor websites of diensten langere tijd onbereikbaar zijn.

DDoS-aanvallen kunnen veel schade aanrichten. Grote webshops lopen inkomsten mis en de reputatie van bijvoorbeeld overheidsinstellingen wordt er niet beter op wanneer media een aanval publiekelijk maken.

[2] http://www2.deloitte.com/nl/nl/pages/over-deloitte/articles/cybercriminaliteit-kost-nederlandse-organisaties-10-miljard-euro-per-jaar.html

In sommige gevallen is het platleggen van servers niet het voornaamste doel van de DDoS-aanval maar wordt deze gebruikt als rookgordijn. De cybercrimineel kan met de aanval eenvoudig verbloemen dat hij elders op het bedrijfsnetwerk belangrijke data inziet of schadelijke malware installeert. Daarmee zijn - naast webshops en overheidsinstellingen - grote organisaties, het MKB, software ontwikkelaars of de servers in een datacenter steeds vaker het doelwit.

Toegang via uw eigen software

Een bijna onzichtbare vorm van cybercrime is het plaatsen van malware (malicious software). Dit is ongewenste software die de normale werking van door u gebruikte software verstoort. De malware kan toegang geven tot data, blokkades opwerpen, functies overnemen of permanente schade aanbrengen aan het netwerk, (mobiele) devices of servers.

Het gebruik van malware neemt de laatste jaren sterk toe; mede dankzij kant-en-klare exploit-kits - software die geïnstalleerd wordt op een omgeving om kwetsbaarheden te ontdekken en kwaadaardige code uit te voeren - kan een crimineel snel en soms zelfs zonder enige IT-kennis aan de slag. Experts daarentegen passen bestaande malware naar eigen inzicht aan voor specifieke doeleinden. Daardoor wordt al snel duidelijk dat de hoeveelheid en de verscheidenheid van kwaadaardige programma's alleen maar toeneemt, en het voor organisaties alleen maar moeilijker wordt om malware tijdig te detecteren. Hieronder vatten wij de bekendste vormen van malware voor u samen:

DE BEKENDSTE VORMEN VAN MALWARE

- Ransom- en Cryptoware - Ransomware heeft als doel de toegang tot systemen te blokkeren, na het betalen van losgeld (vandaar de term ransom) wordt de blokkade verwijderd. Met cryptoware wordt niet de toegang tot het systeem ontzegd maar wordt data versleuteld. Zonder de encryptiesleutel is deze data onbruikbaar. Deze sleutel wordt na betaling vrijgegeven.
- Betalingsfraude - Een ander voorbeeld van malware is Point-of-Sale malware (POS malware) waarmee verkooppunten zoals kassasystemen worden geïnfecteerd. Een Remote Access Trojan (RAT) geeft toegang tot betaalomgevingen. Zo kan met behulp van besmette software betalingsfraude worden gepleegd.
- Fileless malware - In tegenstelling tot andere malware draait fileless malware in het werkgeheugen van een systeem en wordt daardoor ook niet of nauwelijks opgemerkt door virusscans. Er is nog weinig bekend over deze relatief nieuwe vorm van cybercrime.

DE ZWAKSTE SCHAKEL

Cybercriminelen kunnen op verschillende manieren het bedrijfsnetwerk binnendringen. Zo leggen zij contact met medewerkers, maken gebruik van kwetsbaarheden in gebruikte hard- en software of zoeken een ingang via routers en sensoren. De manier waarop een crimineel probeert een bedrijfsnetwerk binnen te dringen, is natuurlijk van belang voor de tegenmaatregelen die genomen moeten worden. Er is hierbij één leidend principe: voorkomen is beter dan genezen. In hoofdstuk 1 werd er al op gewezen dat de impact van een succesvol uitgevoerde cyberaanval groot is en dat het moeilijk is om de gevolgen effectief te beheersen. Daarom zal in dit hoofdstuk niet alleen beschreven worden hoe cybercriminelen te werk gaan, maar ook met een aantal voorbeelden concreet worden gemaakt wat het kan betekenen als zij daarbij succesvol zijn.

Social engineering

Eén van de meest vernuftige manieren om malware te verspreiden is door gebruik te maken van de zwakste schakel in de IT-beveiliging: de mens. Deze techniek wordt social engineering genoemd en is gericht op het verkrijgen van vertrouwelijke informatie door de nieuwsgierigheid van de gebruiker te wekken of de gebruiker bang te maken. Met de verkregen informatie - waaronder gebruikersnamen en wachtwoorden - kan de cybercrimineel ongemerkt binnenkomen op het bedrijfsnetwerk. Om deze informatie boven water te krijgen gaat hij als volgt te werk:

- Hij zoekt telefonisch contact en stelt vragen over de werkzaamheden, software en bepaalde accounts van de medewerker.
- Hij neemt een kijkje op locatie. Door bijvoorbeeld prullenbakken, bureaus en bewakingscamerabeelden te onderzoeken komt de cybercrimineel aan wachtwoorden of andere informatie zoals de gewenste werkwijze of zelfs de bedrijfsetiquette waardoor hij straks tijdens zijn hack nauwelijks opvalt.
- Hij zoekt contact via e-mail (spear phising).

Spear phising

Door brutaalweg contact te zoeken via e-mail wordt informatie vakkundig losgeweekt, bijvoorbeeld door de lezer te verwijzen naar een website waar hij zijn NAW-gegevens kan aanvullen. Of er wordt malware verspreid via links of bijlagen. Wanneer deze worden geopend installeert de malware zichzelf op het device van de gebruiker. De cybercrimineel krijgt toegang tot het bedrijfsnetwerk en de daarop aanwezige data zodra het device zich op het netwerk aanmeldt.

De e-mails die tegenwoordig worden verspreid, staan al lang niet meer vol met stijl- en schrijffouten. Integendeel: de e-mail, de website waarnaar wordt verwezen en de bijlagen zijn niet meer van echt te onderscheiden. De cybercrimineel heeft zijn huiswerk gedaan en weet exact in te spelen op de lezer.

Net als veel organisaties combineert ook hij verschillende datasets om zijn doelwit beter te leren kennen. Met de verrijkte data modelleert hij een doeltreffende e-mail die op het gevoel, interesse of de dagelijkse bezigheden inspeelt van zijn individuele doelwit.

EÉN SUCCESVOLLE SPEAR PHISING MAIL KAN MILJOENEN KOSTEN

In juni 2015 verloor het Amerikaanse Ubiquiti Networks, leverancier van hardware voor service providers en ondernemingen, bijna $47,- miljoen door spear phising. De e-mails werden naar de financiële afdeling van Ubiquiti Networks gestuurd en leken op opdrachten van executive managers binnen het bedrijf om transacties te doen aan derde partijen. De e-mails waarin opdracht gegeven werd tot deze transacties, waren niet van echt te onderscheiden, waardoor de medewerkers bij de financiële administratie geen argwaan kregen.

De dreiging van spear phising wordt groter nu steeds meer werknemers gebruikmaken van privé-devices op de werkvloer. In de meeste gevallen zijn medewerkers zelf verantwoordelijk voor het device maar beschikken ze niet altijd over de beste securitytools.

Aanvallen via software

Ook software kan worden gebruikt om het bedrijfsnetwerk te infiltreren. Software blijft mensenwerk waardoor er altijd een achterdeur is die open kan. Vaak weet de cybercrimineel deze eerder te vinden dan de software-ontwikkelaar en kan hij ongemerkt binnendringen.

Eens in de zoveel tijd wordt de software verbeterd; niet alleen de functionaliteiten worden herzien, er wordt ook aandacht besteed aan het verbeteren van eventuele kwetsbaarheden. Door de toegezonden updates regelmatig uit te voeren worden deuren definitief gesloten voor cybercriminelen en is de organisatie beter beveiligd tegen datalekken en malware die het systeem kunnen verstoren, beschadigen of blokkeren.

Malvertising

Online advertentienetwerken worden eens in de zoveel tijd gekraakt. Cybercriminelen kopen net als ieder ander advertenties in en verspreiden

vervolgens geïnfecteerde ads over honderden websites. Omdat deze activiteiten buiten het zicht vallen van de website zelf, kan bijvoorbeeld een grote nieuwswebsite ongewild malware verspreiden.

Ook het CMS van een website kan een ingang zijn. Wellicht is de website zelf niet het doelwit, maar hebben kwaadwillenden het gemunt op de bezoeker van de website. Ongemerkt wordt er malware geïnstalleerd in een online advertentie. Daarna is het slechts een kwestie van tijd voor het doelwit hierop klikt. De gemiddelde website kan te maken krijgen met tientallen web attacks per week. Naar verwachting worden dit er alleen maar meer.

GROTE NEDERLANDSE WEBSITES VERSPREIDEN REGELMATIG ONGEWILD MALWARE VIA ADS

Populaire websites zoals Nu.nl, Marktplaats en Buienradar hebben de afgelopen jaren één of meerdere keren malware verspreid via hun advertentienetwerken. Een dergelijk incident heeft zich in april 2016[4] nog voorgedaan en het is niet ondenkbaar dat dit weer zal gebeuren. Daarmee wordt duidelijk hoe moeilijk het kan zijn om deze vorm van cybercrime te bestrijden, mede door de afhankelijkheid van derde partijen, in dit geval de advertentienetwerken die de advertenties op de genoemde websites verzorgen. De verantwoordelijkheid voor het verspreiden van malware ligt duidelijk niet bij de getroffen websites, maar zij hebben wel te maken met reputatieschade die het gevolg is van deze vorm van cybercrime.

[4] https://blog.fox-it.com/2016/04/11/large-malvertising-campaign-hits-popular-dutch-websites/

Aanvallen via hardware

De cloud is niet meer weg te denken uit het bedrijfsleven. Bijna iedere organisatie maakt gebruik van de verschillende geboden service-modellen waaronder Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) en/of Infrastructure-as-a-Service (IaaS). Het laatste model betreft het gebruik van de hardware in een datacenter. Deze is voor verschillende organisaties identiek en middels virtualisatie kan deze grootschalig worden aangeboden en beheerd door experts. In het datacenter wordt niet alleen hardware gedeeld, ook operating systems en libraries worden door meerdere organisaties gebruikt door middel van images. Vandaar de groeiende interesse van cybercriminelen: door aan te vallen in de onderste laag, dringen cybercriminelen niet één bedrijfsomgeving binnen maar liggen er mogelijk meerdere omgevingen binnen handbereik.

Een aanval op één van de 200 miljard devices

In de nabije toekomst vormt de concentratie aan smartphones, gadgets, sensoren in gebruiksvoorwerpen, tablets en wearables die tegelijkertijd gebruikmaken van het internet een risico. Deze concentraties ontstaan zowel op de werkvloer waar ze worden beheerd door de IT-afdeling als thuis. Vanwege onwetendheid van de gebruiker zijn de privé-devices en sensoren kwetsbaar. Niet alle updates worden netjes uitgevoerd. Wachtwoorden die voor meerdere doeleinden worden gebruikt - onder andere voor zakelijke software - duiken ook hier op of er wordt geen gebruik gemaakt van de beste securitytools. Straks kan een cybercrimineel wellicht via een privénetwerk binnendringen in één van de verwachte 200 miljard devices[5] en daarmee data verzamelen om binnen te dringen op het bedrijfsnetwerk.

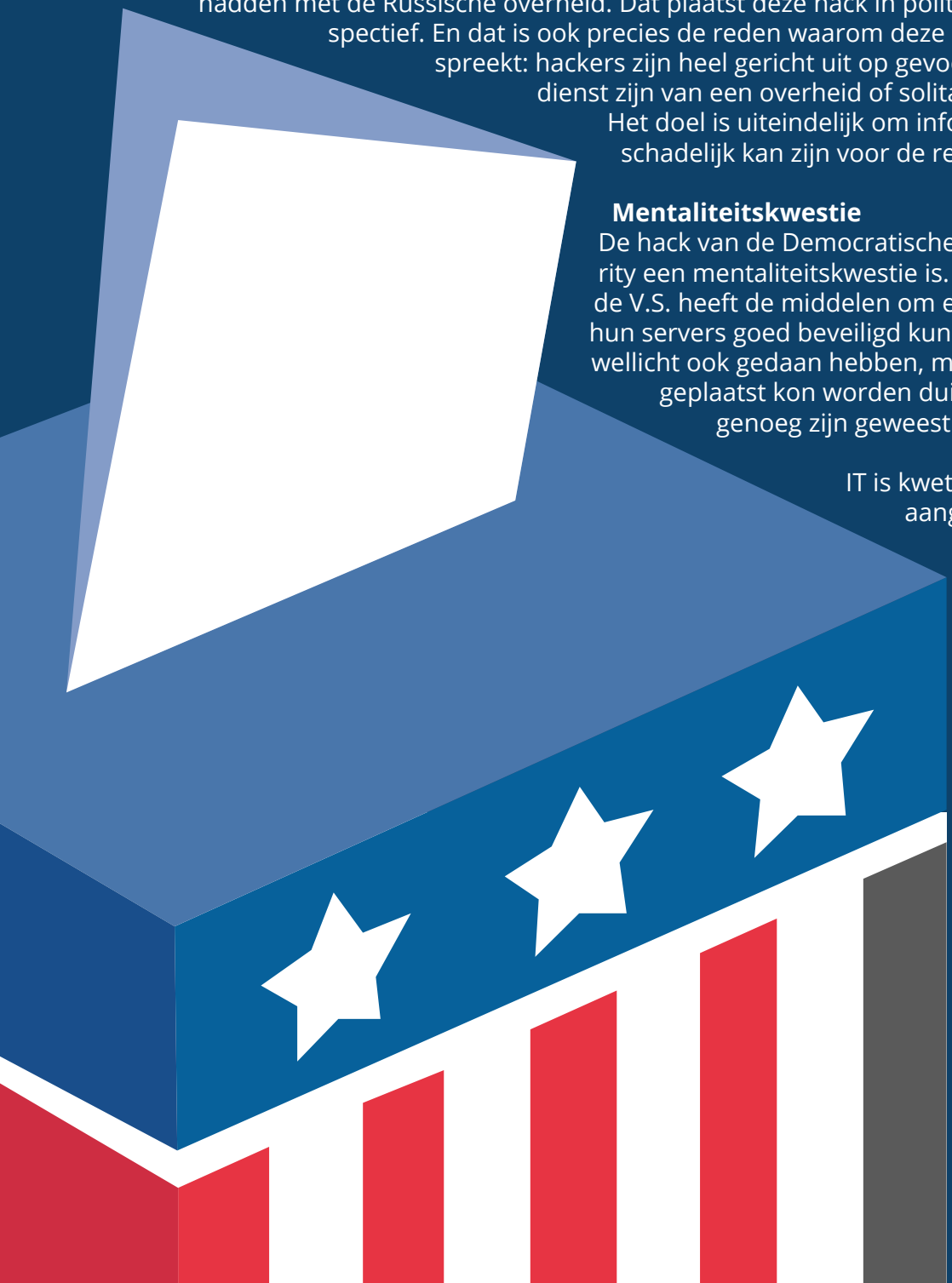
In een connected wereld waarin olievelden, waterzuiveringsinstallaties, energiecentrales, medische apparatuur en zelfs gebruiksvoorwerpen als koelkasten online zijn, is het niet ondenkbaar dat criminelen deze gebruiken om kritieke infrastructuren aan te vallen. Zo kunnen zij niet alleen schade aanrichten of bedrijven afpersen: chaos creëren in de samenleving kan een opzichzelfstaand doel zijn. Zover is het nog niet, dit soort aanvallen vraagt een enorme voorbereiding en dat is voor de criminelen waar we in deze whitepaper aandacht aan besteden tot op heden geen interessant businessplan gebleken.

[5] https:// www.cnbc.com/2016/02/01/an-internet-of-things-that-will-number-ten-billions.html

EEN HACK IN POLITIEK DAGLICHT

Verkiezingscampagnes gaan er in Amerika vaak hard aan toe. In 2016 werd daar een heel nieuwe dimensie aan toegevoegd. Servers van de Democratische Partij werden gehackt. Het gevolg: de campagnestrategie van de Democraten kwam op straat te liggen en de namen van meer dan 100 grote donateurs aan de campagne werden bekend. Dat ligt in de V.S. erg gevoelig, want politieke voorkeur is in het algemeen niet iets waarover wordt gesproken, en dat geldt zeker voor grote donateurs. Het is privacygevoelige informatie die net zoals medische of financiële gegevens absoluut geheim moet blijven. Het uitlekken van de campagnestrategie leidde uiteindelijk tot het opstappen van de campagnevoorzitter. Tevens spinde de Republikeinse tegenkandidaat Donald Trump er wekenlang garen bij en steeg flink in de peilingen. Het is een aansprekend voorbeeld van de reputatieschade en privacyschending als gevolg van cybercriminaliteit.

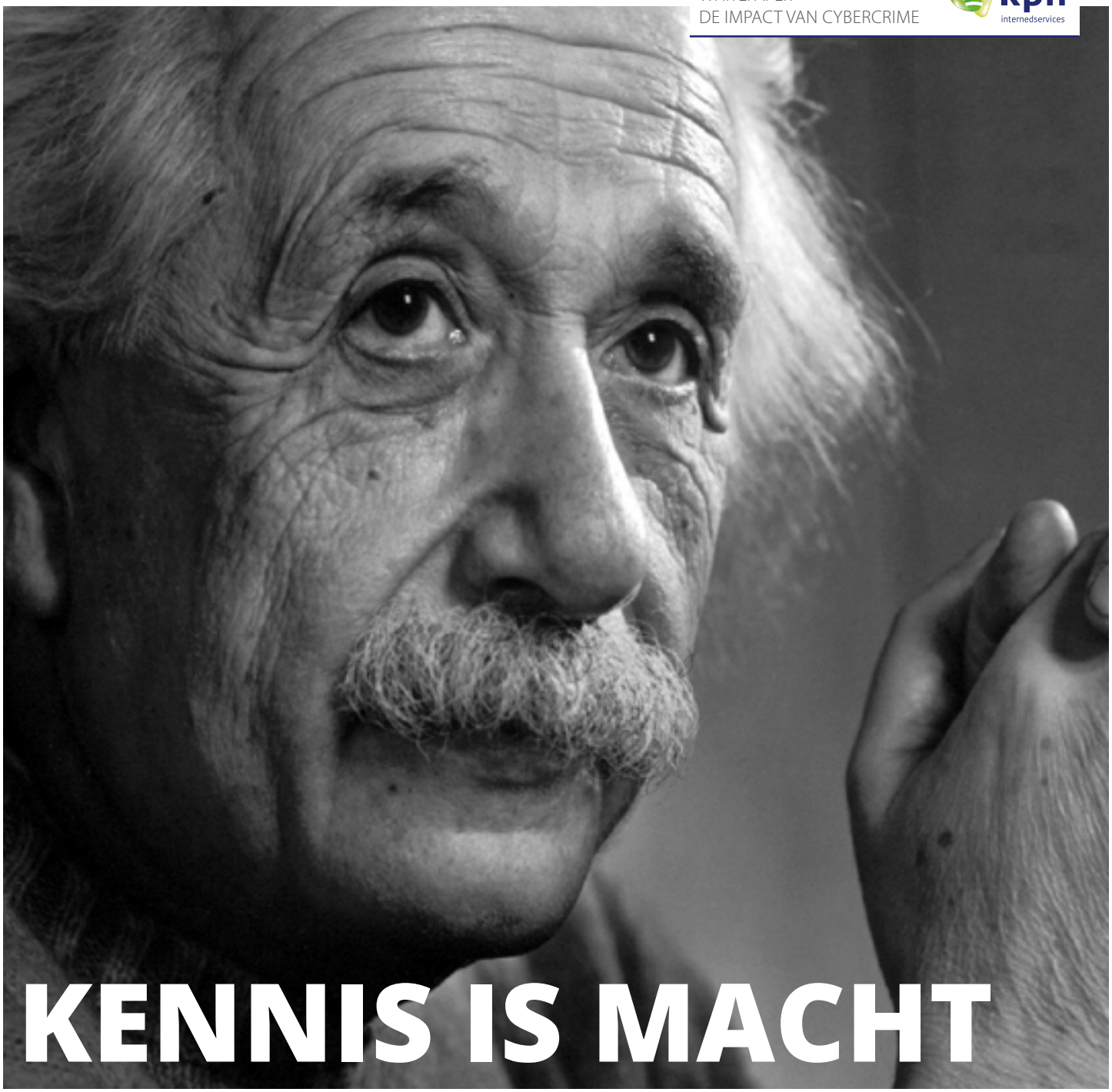
De hack van de Democratische Partij werd geplaatst door Russische hackers, die waarschijnlijk banden hadden met de Russische overheid. Dat plaatst deze hack in politiek en internationaal perspectief. En dat is ook precies de reden waarom deze hack zo tot de verbeelding spreekt: hackers zijn heel gericht uit op gevoelige informatie. Of zij in dienst zijn van een overheid of solitair opereren doet er niet toe. Het doel is uiteindelijk om informatie buit te maken die schadelijk kan zijn voor de reputatie van een organisatie.



Mentaliteitskwestie

De hack van de Democratische Partij illustreert dat security een mentaliteitskwestie is. De Democratische Partij in de V.S. heeft de middelen om expertise in te zetten zodat hun servers goed beveiligd kunnen worden. Dat zullen ze wellicht ook gedaan hebben, maar het feit dat de hack geplaatst kon worden duidt erop dat ze niet alert genoeg zijn geweest.

IT is kwetsbaar voor inbreuken. En aangezien informatiestromen vrijwel alleen nog digitaal zijn, is iedere organisatie die te maken heeft met gevoelige gegevens verplicht om hierover na te denken. Allereerst natuurlijk om de integriteit van bedrijfskritische informatie te beschermen. Maar ook voor de privacy van klanten, cliënten en burgers. Want één ding is zeker: zodra dit soort informatie publiek wordt, loopt uw reputatie onherroepelijk schade op.



KENNIS IS MACHT

Cybercrime kan grote schade aanrichten. Maar dat betekent niet dat u zich er niet tegen kunt wapenen. Het tegengaan van cybercrime begint met kennis: kennis over hoe cybercriminelen te werk gaan, maar ook over hoe zij bestreden kunnen worden. Dat laatste kan deels op eigen kracht met eenvoudige maatregelen, waarop in deel twee van deze whitepaper ingegaan zal worden.

Wat in ieder geval zeker is, is dat u er niet alleen voor hoeft te staan. U kunt zelfs twee vliegen in één klap slaan: door uw IT-infrastructuur onder de loep te nemen en te moderniseren, kunt u gelijktijdig een betere weerbaarheid tegen cybercrime realiseren. Steeds meer bedrijven en organisaties kiezen precies om die reden voor gedeeltelijke of volledige migratie naar de cloud.

Moderne cloudproviders hebben niet alleen aandacht voor uw IT-behoeften, maar zijn ook toegewijd aan uw IT-security. Zelfstandig een uitgekiend security beleid formuleren en up-to-date houden is arbeidsintensief en kostbaar waarbij het de vraag is of het ook effectief zal zijn. Samen met een cloudprovider vormt u een sterk team en kunt u gerichter uw security beleid vormgeven, waarbij u ook kunt putten uit de kennis die bij de cloudprovider van uw keuze aanwezig is.

Nu cybercrime steeds grotere vormen aanneemt, is passiviteit een reëel risico geworden. Aarzel daarom niet en laat u door een betrouwbare partij voorlichten over de security voordelen die een overstap naar de cloud u kan bieden.

De diensten van KPN Internedservices

Wij geloven dat onze klanten nog succesvoller kunnen worden met de oneindige mogelijkheden die ICT biedt. Daarom nemen wij onze klanten en partners actief mee naar het beste wat onze industrie te bieden heeft. Wij leveren premium Cloud & IT-services op abonnementsbasis. Omdat u eenvoudig op- en afschaalt en alleen betaalt voor wat u gebruikt, groeit uw IT-capaciteit mee met uw bedrijf. Net als uw kosten. Dat vinden wij van deze tijd. Net als de drievoudige ISO-certificering en 24/7 support waar u op kunt rekenen.

Wij ontwerpen, bouwen en beheren bedrijfskritische IT- en cloud-oplossingen die bijdragen aan het succes van onze klanten. Dit doen wij volgens de hoogste standaarden, met de hoogste kwaliteit en de beste mensen. Of het nu gaat om de hosting van uw e-business activiteiten, een werkplek in de cloud of het managen van uw (internet)verbindingen.

Daarnaast biedt Internedservices uiteenlopende diensten om uw omgeving optimaal te laten presteren en/of uw IT-organisatie te ontlasten.

Meer dan twintig jaar ervaring en ruim 30.000 klanten. Sinds het ontstaan in 1996 heeft Internedservices tienduizenden klanten geholpen met IT- en cloud-vraagstukken. Daardoor begrijpen we de uiteenlopende IT-behoeften van onze klanten. Omdat Internedservices het wiel niet steeds opnieuw hoeft uit te vinden kunnen we u de snelste, beste en voordeligste oplossing bieden.

Heeft u vragen over deze whitepaper, wilt u kennismaken of advies inwinnen over onze security-oplossingen? Neem dan contact met ons op.

KPN Internedservices
Wielingenstraat 8
1441 ZR Purmerend

Tel: 0299 476 185
E-mail: info@internedservices.nl

Contact met een expert

Benieuwd hoe Internedservices u kan helpen met uw cybersecurity.

Onze experts staan voor u klaar

Anti DDoS

DDoS houdt in dat heel veel computers een groot aantal verbindingsverzoeken doen naar een server. De server kan deze verzoeken niet verwerken en kan daardoor onbereikbaar worden. Anti DDos beschermt u hier tegen.

DRaaS

Met Disaster Recovery as a Service (DRaaS) wordt uw organisatie beschermd tegen het verlies van kostbare data en applicaties als gevolg van een ramp of verstoring.

Web Application Firewall

De Threat Manager intrusion detection monitort 24/7 het netwerkverkeer en de actieve nodes binnen de beveiligde omgeving. Bij een security incident nemen onze security experts direct de benodigde maatregelen.

Log Manager

Log Manager van Internedservices is een cloud-gebaseerde log management oplossing die is ontworpen om de complexiteit en kosten van het log managen te drukken.

Content Delivery Network

Uw website op topsnelheid houden, en een gegarandeerde top performance? Met een Content Delivery Network (CDN) optimaliseren we het laden zonder afbreuk te doen aan de functionaliteit van de website.