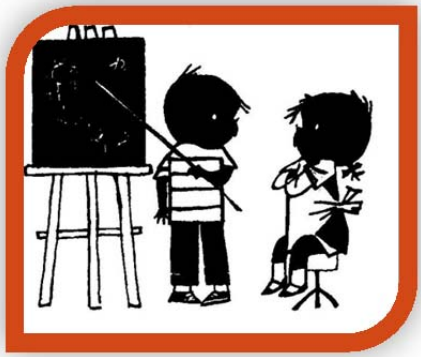
Academy: Security

Johan Molenaar
PostNL Data Services
30 juni 2015
johan.molenaar@postnl.com

Voorwoord



Dit document bevat de uitgeschreven tekst voor de PostNL Data Services Academy van dinsdag 30 juni 2015. Het onderwerp voor deze Academy is Security en is een introductie van een onderkend en onbegrepen vakgebied. Het doel van de Academy is dat vakspecialisten elkaar vertellen over hun vakgebied of interesse.

De aanleiding voor de Academy is de vorming van de afdeling Data Services binnen D&DM waar hard gewerkt wordt om de DataRotonde te ontwikkelen. De DataRotonde wordt een uitwisselingsplatform van interne- en externe data, die op intelligente manier wordt gekoppeld om enerzijds de *operational excellence* van PostNL te verbeteren, als anderzijds de data in te zetten om nieuwe business proposities te ontwikkelen.

Ik heb geprobeerd om een moeilijk onderwerp toegankelijk te maken voor een breed publiek, en ben mij bewust dat dit niet eenvoudig is. Het vertrekpunt van de Academy is een woninginbraak waar wij als gezin in de winter van 2014 slachtoffer van zijn geworden. Van deze inbraak en het rechercheren door de politie leg ik verbanden met een computerinbraak, oftewel een *hack*. Vervolgens een stukje theorie over computernetwerken ter introductie van de rest van Academy. Ik ga verder met een *case study* van de webshop. Hierin worden zo veel mogelijk elementen besproken die van belang zijn voor de beveiliging van een webshop, van de infrastructuur tot de gebruikersinterface. Na de webshop een stuk over het beveiligen tegen aanvallen van buiten, en vervolgens worden twee beveiligingstechnieken nader uitgediept. Daarna een recap van de woninginbraak, waarbij ik de overeenkomsten met een hack probeer te vinden. Met de hiervoor opgedane kennis zou dit moeten lukken. Als laatste geef ik mijn visie over de inrichting van Data Services 2.0, voor wat betreft de *Information Security* en *Information Protection Strategy*. Veel plezier, en laat mij weten wat je ervan vindt!

Inhoud

Woninginbraak

In de nacht van vrijdag 14 op zaterdag 15 februari 2014 is er in ons huis ingebroken. Wij waren vrijdags hals over kop naar Brabant vertrokken en hadden het gebruikelijke protocol, wanneer we een paar dagen weg zijn, niet gevolgd. De deur naar de achtertuin was afgesloten met een knip, maar niet op slot. De lamellen en gordijnen waren niet in hun juiste positie gezet. En de lampen in huis waren niet op de tijdschakelaar gezet, zodat het 's avonds net lijkt of er iemand thuis is.

Toen ik de volgende dag de voordeur opendeed, waaide deze uit mijn handen en zag ik dat de tuindeur openstond. In mijn naïviteit dacht ik eerst nog dat ik deze deur niet goed had dichtgedaan, maar nader onderzoek leerde dat deze open was gebroken…..

Het hele huis was overhoop gehaald, echter de tablets en laptops lagen nog op de keukentafel. Lades in de kamer van de meiden waren overhoop gehaald, terwijl in de slaapkamer van onze zoon geen sporen te vinden waren. Op onze slaapkamer en mijn werkkamer waren alle laden omgekeerd. De conclusie was dat er sieraden en waarde papieren buit was gemaakt.

Zo te zien een snelle actie, waarbij gezien de obstakels, alleen maar spullen zijn meegenomen die, en snel meegenomen konden worden en niet eenvoudig traceerbaar (tablets, computers enz.) zijn.

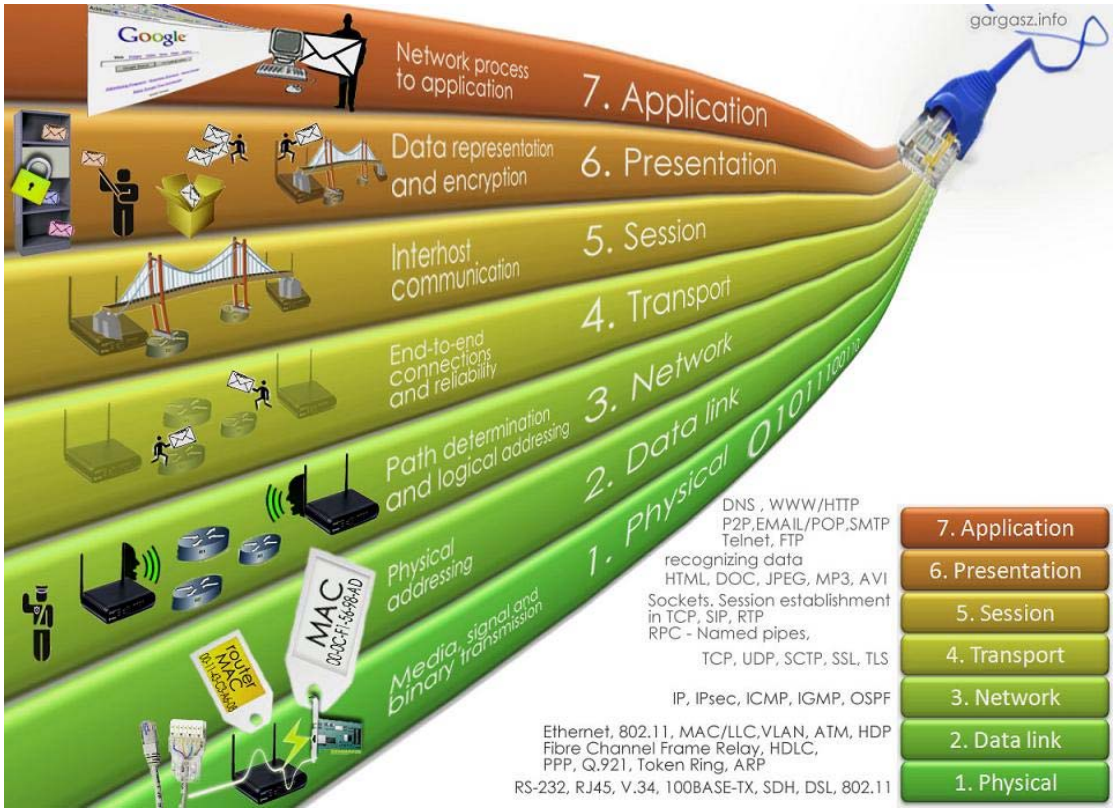
Wat is overeenkomst van een woninginbraak met een inbraak in een computersysteem? Daar wil ik jullie deze Academy over vertellen.

Computernetwerken

Het beveiligen van een computersysteem of data center lijkt complex en bijna onmogelijk, echter net als bij het beveiligen van je huis, is dit toch mogelijk mits je de juiste technologie gebruikt en procedures heel gedisciplineerd hanteert.

Bij het beveiligen van je huis kijk je naar zwakke plekken in de structuur van je huis. Dit zijn ramen, deuren, donkere plekken, enz. Bij het beveiligen van een computersysteem of -netwerk ga je op dezelfde manier te werk. Ook een computernetwerk heeft ramen en deuren, al zou je deze niet meteen herkennen. Om te begrijpen hoe een computernetwerk beveiligd kan worden, moet ik eerst iets vertellen over de logische opbouw van een computernetwerk.

In 1983 heeft het International Standards Organization (ISO) het Open Systems Interconnection Reference Model gedefinieerd. Kortweg wordt dit het OSI Reference Model of OSI model genoemd. Het OSI model bestaat uit 7 lagen die elk hun eigen functie vervullen bij het transporteren van data-eenheden in een computernetwerk. Elke laag geeft data en besturingsinformatie door aan de laag die er onmiddellijk onder komt, tot op die manier de onderste laag wordt bereikt. Laag 1 bevat het fysieke medium, waarover de feitelijke communicatie plaatsvindt. Elke laag gebruikt de diensten van een ondergelegen laag.



Figuur 1: OSI model.

Indien twee computers in een netwerk met elkaar communiceren, door bijvoorbeeld het verzenden van een e-mail, zal deze e-mail twee maal het OSI model doorlopen. Eerst bij de verzender, en vervolgens bij de ontvanger.

Voor het communiceren in een computernetwerk zijn netwerk protocollen gedefinieerd. Een *protocol* definieert hoe computers elkaar herkennen in een computernetwerk, de vorm van de data die verzonden en ontvangen wordt, en hoe deze informatie wordt verwerkt als deze zijn bestemming bereikt. Protocollen definiëren ook hoe te handelen bij verloren of beschadigde verzendingen (*packets*). Bekende netwerk protocollen zijn:

- TCP/IP (Internet Protocol)
- AppleTalk (Macintosh protocol)
- SMTP (e-mail)
- FTP (bestanden versturen tussen netwerken)
- NFS (bestanden versturen binnen een netwerk)
- Telnet (besturing van een server op afstand overnemen)

Zoals al gezegd zijn er 7 lagen binnen het OSI model gedefinieerd, hieronder een beschrijving.

Applicatie (laag 7)

De applicatie laag is de laag die gebruikt wordt door netwerkprogramma's. Dit kunnen internet browsers zijn, FTP clients, of e-mailprogramma's. Zulke programma's maken gebruik van protocollen die op de applicatie laag draaien zoals HTTP(gebruikt door de webbrowser), SMTP (gebruikt door e-mailprogramma's) en FTP (voor het verzenden van bestanden).

Presentatie (laag 6)

De presentatie laag fungeert als een vertaal laag waarop één taal gesproken wordt tussen twee programma's. Een netwerk kan computers met verschillende soorten besturingssystemen herbergen, zoals Windows, Linux en Apple. Deze besturingssystemen maken soms gebruik van een andere representatie van de data. De presentatie laag op de verzendende computer vertaalt data uit de applicatie laag (7) naar de gemeenschappelijke taal voordat het naar lager gelegen lagen stroomt en verzonden wordt. De presentatie laag op de ontvangende computer vertaalt data uit de sessie laag (5) naar de taal die door het programma op de applicatie laag (7) begrepen wordt. Naast vertalen zorgt de presentatie laag voor compressie en encryptie van data. De presentatie laag wordt niet altijd gebruikt, omdat vertalen, encryptie of compressie niet altijd nodig zijn.

Sessie (laag 5)

Waar laag 1 tot en met 4 zich vooral bezig houden met het verpakken (en uitpakken) van data en adressering is de sessie laag de eerste laag die zich direct met de software bezig houdt die van het netwerk gebruik maakt. De sessie laag maakt, onderhoudt en verbreekt sessies tussen twee programma's. NetBIOS is daar een voorbeeld van.

Transport (laag 4)

De transport laag verzorgt de datatransmissie tussen twee eindgebruikers met behulp van foutcontrole, hertransmissie en 'stroomcontrole' (timing). De transport laag zorgt ervoor dat hoger gelegen lagen (software uit de applicatie laag bijvoorbeeld) geen rekening hoeven te houden met de correctheid en de juiste timing van de datatransmissie. Het belangrijkste protocol in de transport laag is het Transfer Control Protocol (TCP). TCP zorgt voor een verbinding tussen twee computers op een netwerk en draagt zorg voor correcte datatransmissie tussen de computers. De data-eenheden op laag 4 heten segmenten. In een segment zijn onder andere het IP adres en het (TCP) poortnummer opgenomen. Een poort is te vergelijken met een kanaal van een *walki talki* waarover de communicatie plaatsvindt.

Netwerk (laag 3)

De netwerk laag verzorgt de functionaliteit die nodig is om data te verzenden tussen netwerken. De netwerk laag is verantwoordelijk voor *routing* (routeren), 'flow control' en

voor foutafhandeling. Het belangrijkste protocol van de netwerk laag is het Internet Protocol (IP). Routers gebruiken IP adressen om het dataverkeer tussen verschillende netwerken te regelen. Computers, routers en printers in een IP netwerk hebben naast een MAC ook een IP adres. De data op laag 3 is verdeeld in pakketjes. Pakketjes zijn data-eenheden waar onder andere het IP adres van de verzender en de (uiteindelijke) ontvanger in zijn opgenomen.

Indien een computer op de MAC access lijst (*whitelist*) voorkomt, zal deze van het netwerk ook een IP adres krijgen. Met een IP adres is een computer identificeerbaar in een computernetwerk en kan zo binnen dit netwerk communiceren. Naast een IP adres krijgt een computer ook een masker (MASK) en een *Default Gateway*. Een masker geeft aan welk segment van het netwerk de computer mag benaderen, en een Default Gateway geeft aan via welke server het netwerk wordt verlaten. Dit is meestal het IP adres van de (border)router.

Datalink (laag 2)

De datalink laag verzorgt de functionaliteit die nodig is om data betrouwbaar te kunnen versturen tussen netwerkapparaten in een netwerk. Met betrouwbaar wordt niet beveiligd, maar dat data dat wordt verstuurd, ook daadwerkelijk aankomt. Indien dit niet het geval is wordt de data opnieuw verzonden. De datalink laag gebruikt MAC of 'hardware' adressen om data naar de juiste plek te sturen. In een netwerk heeft elk apparaat een eigen (uniek) MAC adres dat ingebakken zit in de netwerkkaart van een computer of printer. De meest gebruikte techniek op de datalink laag is Ethernet. De data op laag 2 is verdeeld in 'frames'. Frames zijn data-eenheden die voorzien zijn van een header waarin de MAC adressen van de verzender en de ontvanger opgenomen zijn.

Fysieke (laag 1)

De fysieke laag zet de bits van de datalink laag om in elektrische signalen, licht- of radio golven. Kabeltypes, stekkers, de elektrische spanning op de kabels, de manier waarop kabels gevlochten moeten worden zijn gedefinieerd in de fysieke laag.

Wat kunnen we met deze informatie? Als we snappen hoe een computernetwerk werkt, zijn we ook in staat om een computernetwerk te beveiligen. Het volgende hoofdstuk geeft hier een voorbeeld van.

Case study: webshop

Stel we gaan een webshop bouwen waar klanten producten kunnen bekijken en bestellen. Als er een bestelling wordt geplaatst dient de klant in te loggen met zijn gebruikersnaam en wachtwoord, of zich te registreren op de website. Tijdens het registratieproces worden de naam en de adresgegevens ingevoerd en eventueel een bankrekening- en telefoonnummer. In dit voorbeeld is de gebruikersnaam het e-mailadres, zodat we een uniek ID van de klant hebben, en meteen een communicatie mogelijkheid. Het wachtwoord kan de klant zelf wachtwoord kiezen.

Bovenstaande zal bekend voorkomen, de vraag is nu hoe gaan we onze webshop bouwen en beveiligen?

Applicatie architectuur

We beginnen met het ontwerpen van een architectuur voor de applicatie. We bouwen de applicatie op uit drie lagen:

- Web
- Applicatie
- Database

De weblaag zorgt voor de opmaak, plaatjes en tekst (content) in de webbrowser. Deze content past zich aan de afmetingen van de browser aan, en zal een andere indeling hebben op een telefoon of een desktop scherm. In de browser worden alleen maar plaatjes en tekst getoond en worden er door de webbrowser besturingscodes voor de webbrowser meegezonden. Deze codes bepalen uiteindelijke opmaak in de browser.

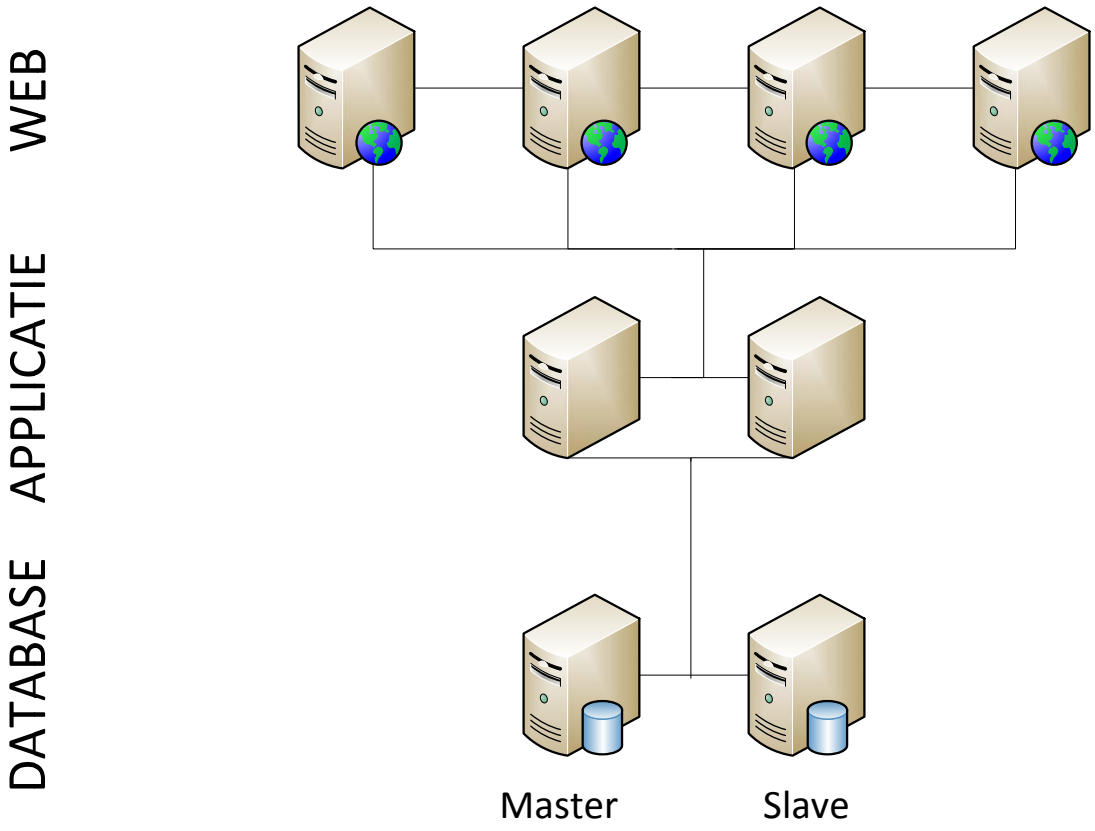
De applicatielaag bevat de business logica van de webshop en communiceert met de weblaag. Alle informatie in deze laag wordt vertaald naar de taal die de browser begrijpt. Ook communiceert de applicatielaag met de databaselaag.

De databaselaag bevat de content (ingeval van een CMS), maar ook de producten uit de catalogus voor de webshop. De producten staan wellicht in een ERP systeem, zodat bestellingen meteen verwerkt kunnen worden in het magazijn. We willen ook dat er betaald kan worden, dus staat de webshop in verbinding met ons financiële systeem en heeft deze een connectie met iDeal.

Belangrijk in bovenstaand ontwerp is dat de weblaag in geen geval toegang heeft tot de database, en de applicatielaag geen programmeercode naar de weblaag stuurt.

Hosting

We verwachten veel bezoekers en richten 4 webservers, 2 applicatieservers en ook 2 databaseservers in. De webservers handelen de bezoekers af, de applicatieservers zijn dubbel uitgevoerd zodat het rekenwerk van de business logica verdeeld kan worden. De database wordt ook dubbel uitgevoerd waarbij de één een kopie van de ander bevat. Hierdoor is het mogelijk om backoffice processen op de kopie database uit te voeren, om zo de database voor het bestelproces niet onnodig te belasten.



Figuur 2: Hosting webshop, volgens 3-tier.

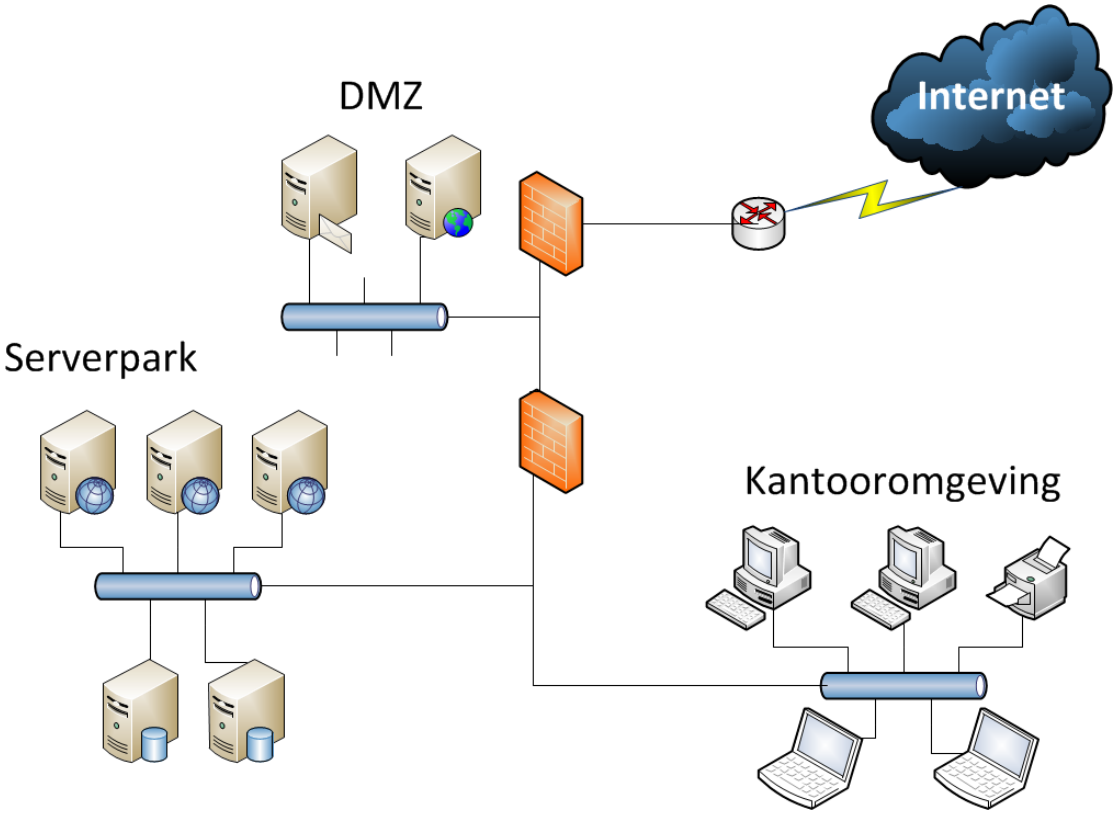
Netwerk architectuur

Nu gaan we het netwerk ontwerpen en verbinden de servers met elkaar en zorgen dat de klanten onze webshop via internet kunnen bereiken. Zoals eerder gezegd zijn routers apparaten om te communiceren tussen verschillende computernetwerken. We willen ons computernetwerk met het internet verbinden en dat doen we met een router. Dit wordt ook wel en borderrouter genoemd. Als ons netwerk via deze router met internet verbonden is, betekent het dat alle servers direct benaderbaar zijn via internet. Voor de webservers willen we dat graag, maar voor de applicatie- en databaseservers willen we dat natuurlijk niet. Daarom richten we een DeMilitariZed Zone (DMZ) in.

Een DMZ is een door een of meerdere firewalls gecreëerde plek in een computernetwerk waar servers geplaatst worden die met de buitenwereld communiceren, zoals web-, ftp- en mailservers. De servers in de DMZ worden door de firewall gescheiden van de rest van de computers in het netwerk. De toegang tot de rest van het netwerk wordt beveiligd door een tweede firewall, waarvan de poorten voor het web verkeer gesloten zijn. De poort waarover de communicatie tussen de applicatie- en de webserver plaatsvindt, is hier wel geopend en de poort voor web verkeer gesloten.

Echt vertrouwelijke gegevens zijn in een goed ingerichte DMZ niet te vinden. Die staan immers in het door de firewall bewaakte gedeelte. De DMZ wordt ook wel extranet genoemd.

De term DMZ in de informatica komt voort uit de Koreaanse DMZ uit 1953 en is een bufferzone tussen Noord- en Zuid-Korea. Het is een soort IJzeren Gordijn zoals dat tijdens de Koude Oorlog in Europa bestond. Aan weerszijden van de streng bewaakte grens staan de Noord- en Zuid-Koreaanse legers klaar om zich te verdedigen tegen de vijand. De grens is 248 kilometer lang. De DMZ is vier kilometer breed. In de zone bevinden zich naar schatting twee miljoen landmijnen.



Figuur 3: Voorbeeld van een computernetwerk voor een webshop.

Beschermen tegen aanvallen

De grote boze buitenwereld zit vol met aanvallen. Vele scriptkiddies struinen het internet af op zoek naar zwakke plekken in computernetwerken. Waar zijn ze naar op zoek, hoe gaan zij te werk? Leveranciers van computersystemen of netwerkcomponenten zoals routers en firewalls, komen regelmatig met software updates. Deze updates bevatten naast nieuwe functionaliteit ook reparaties van beveiligingslekken. Dit worden bugfixes genoemd. Welke aanvallen zijn er en hoe kunnen we ons ertegen beschermen?

Port scan

Een aanval begint over het algemeen met een portscan op je firewall. Zoals eerder verteld is een firewall een poortwachter, die alleen verkeer doorlaat, dat toestemming heeft om doorgelaten te worden. De rest wordt tegen gehouden. Bij een poortscan wordt er gekeken welk verkeer doorgelaten wordt, en a.d.h.v. deze bevindingen wordt er een aanvalsplan gemaakt. Indien de firewall niet voldoende beveiligd is, kan via deze route toegang verkregen worden tot het netwerk.

DDos aanval

Een andere manier om een webshop of website te saboteren is een DDos aanval. Hiermee worden miljoenen aanvragen op de website gedaan. Dit is in wezen een onschuldige aanval omdat er geen schade aan de website wordt toegebracht. Ook komt de aanvaller niet verder dan de website en dringt dus niet tot het computernetwerk achter de website door, echter kan niemand meer jouw webshop bezoeken, wat tot omzetderving of imagoschade i.g.v. een bank leidt. Middels intelligente software kan een DDos aanval afgewend worden door het verkeer vanuit deze computers op een blacklist te plaatsen.

Afluisteren

Het afluisteren is een andere manier, veel toegepast door de NSA, ook wel *snifferen* genoemd. Dit kan vermeden worden door de data te versleutelen, veelgebruikte voorbeelden hiervan zijn SSL/TSL voor http en FTP verkeer of een VPN verbinding tussen twee computernetwerken. VPN en SSL/TSL maken gebruik van cryptografie, hierover later meer.

Authenticatie en autorisatie

Authenticatie is het registreren of aanmelden op een computernetwerk, over het algemeen gebeurt dit via een gebruikersnaam en wachtwoord. Met deze gegevens ben je in staat om gebruik te maken van de functionaliteiten die het computernetwerk biedt. Het is aan de *administrator* (beheerder) van het computernetwerk te bepalen welke rechten en rollen jij als gebruiker krijgt. Dit wordt *autorisatie* genoemd. Ben jij slechts een klant bij een webshop of ben jij de medewerker die de orders van de webshop verwerkt? Wachtwoorden zijn het kwetsbaarste punt van een computernetwerk omdat dit meestal woordenboekwoorden zijn met als het meezit slimme andere tekens. Vandaar dat er voor websites met gevoelige informatie dubbele authenticatie wordt gebruikt, waarbij er naast een wachtwoord, ook een SMS wordt verstuurd. Bedrijven die de gebruiker helemaal niet vertrouwen, geven een calculator aan hun gebruikers die een wachtwoord genereert. Dit zie je bij banken veel gebeuren.

Brute Force Attack

Een methode voor hackers om toegang tot de webshop en wellicht de database te krijgen is te proberen om als *administrator* (beheerder) in te loggen. De gebruikersnaam is normaal gesproken administrator en Dit is vaak slechts beveiliging met een gebruikersnaam en wachtwoord. Door maak vaak genoeg te proberen, kan het wachtwoord geraden worden. Dit kan via het internet door een zogenaamde wachtwoord generator, die alle mogelijke combinaties probeert. Dit wordt een Brute Force Attack genoemd.

Intrusion Detection

Monitoring wat de bezoekers van je computernetwerk doen is minstens zo belangrijk. Wie logt erin, met welke rechten, wat doet hij, hoe lang is deze ingelogd. Probeert iemand ergens toegang te krijgen, dat niet lukt? Deze vragen dienen dagelijks gesteld te worden en wordt *Intrusion Detection* genoemd. Het bijhouden (loggen) van alle activiteiten die gebruikers doen is hiervan de basis, om op basis van patronen kwetsbaarheden te kunnen opsporen en ongenode gasten te herkennen.

Secure Programming

Een andere maatregel tegen hackers is *Secure Programming*. Dit is het besef van de programmeur dat elke programmeerfout of onzorgvuldigheid tot een inbraak kan leiden. Een van deze maatregelen is ervoor te zorgen dat van elk invoerveld de ingevoerde data wordt gecontroleerd tegen ongewenste invoer. Hierbij valt te denken aan database aanvragen middels een SQL opdracht, *SQL Injection*. SQL is een database programmeertaal, en als hier niet voldoende aandacht aan wordt geschonken, kan via het wachtwoord veld de tabel met gebruikers opgevraagd worden.

Fysieke beveiliging

De servers plaatsen we in onze computerruimte, sluiten de kabels aan op de switch, doen de kastdeur op slot, zetten de airco aan, doen de toegangsdeur van de computerruimte op slot en schakelen het alarmsysteem in. Toegang tot de computerruimte hebben alleen de inframedewerkers van IT, en toegang tot de kast hebben alleen de IT medewerkers van de webshop. Op dit niveau hebben we vooral fysieke beveiliging toegepast.

Governance

Tot slot zijn de processen voor het inrichten, wijzigen en gebruik van het computernetwerk erg belangrijk. Denk maar aan USB-sticks, dropbox, gevoelige informatie op laptops, enz. De laatste versie van het besturingssysteem, instellen van de persoonlijke firewall en natuurlijk de laatste updates van de virusscanner.

Beveiligingstechnieken

In het vorige hoofdstuk zijn de mogelijke beschermings- en beveiligingsmaatregelen besproken. In dit hoofdstuik wil ik inzoomen op twee specifieke technieken: cryptografie en eenvoudig sterke wachtwoorden kiezen.

Cryptografie

Cryptografie is een van de meest gebruikte methoden om data veilig over het internet te verzenden. De belangrijkste bestanddelen van cryptografie zijn een sleutel en een formule. Een beveiliging wordt beter indien de formule (algoritme) bekend is, daardoor hangt de kwaliteit van de beveiliging af van de sleutel. Deze sleutel is opgebouwd uit priemgetallen.

> *Een priemgetal is een geheel getal groter dan 1 dat alleen deelbaar is door 1 en door zichzelf, dus 1 is geen priemgetal.*

Waarom zijn priemgetallen zo belangrijk? Priemgetallen kunnen gebruikt worden om sleutels te maken voor het versleutelen van data. Als je twee priemgetallen met elkaar vermenigvuldigt, is deze alleen maar te ontbinden in deze twee priemgetallen. Stel je neemt de priemgetallen *5* en *3*. Het product van beide getallen is *15*. Dit getal is niet anders te ontbinden dan in *5* en *3*. Dit is een belangrijke eigenschap van priemgetallen, daarom worden priemgetallen gebruikt voor het coderen van data.

Hoe werkt het

Stel we willen data veilig verzenden en zorgen ervoor dat personen die met ons willen communiceren een publieke sleutel krijgen. Deze publieke sleutel is het product van 2 priemgetallen. De data wordt versleuteld met de publieke sleutel, en kan alleen ontcijferd worden met de 2 privé sleutels, de priemgetallen. Vergelijk het met een hangslot, iedereen kan het hangslot *dichtklikken*, maar alleen degene met de sleutel kan deze weer openen.

Het *dichtklikken* is vrij eenvoudig. Neem twee priemgetallen, bijvoorbeeld 19 en 29. De publieke sleutel is nu 551, want 19 × 29 is 551. Iedereen kan nu met deze publieke sleutel een bericht coderen. Maar om dit bericht vervolgens te ontcijferen zijn 19 en 29 nodig. En die weet alleen de maker. De gebruikte formule (algoritme) van het coderen is geen vermenigvuldiging of deling, omdat deze bewerkingen invers aan elkaar zijn. Het coderen met de publieke sleutel levert een restwaarde van een deling op, die weer ontcijferd kan worden met de twee privé sleutels

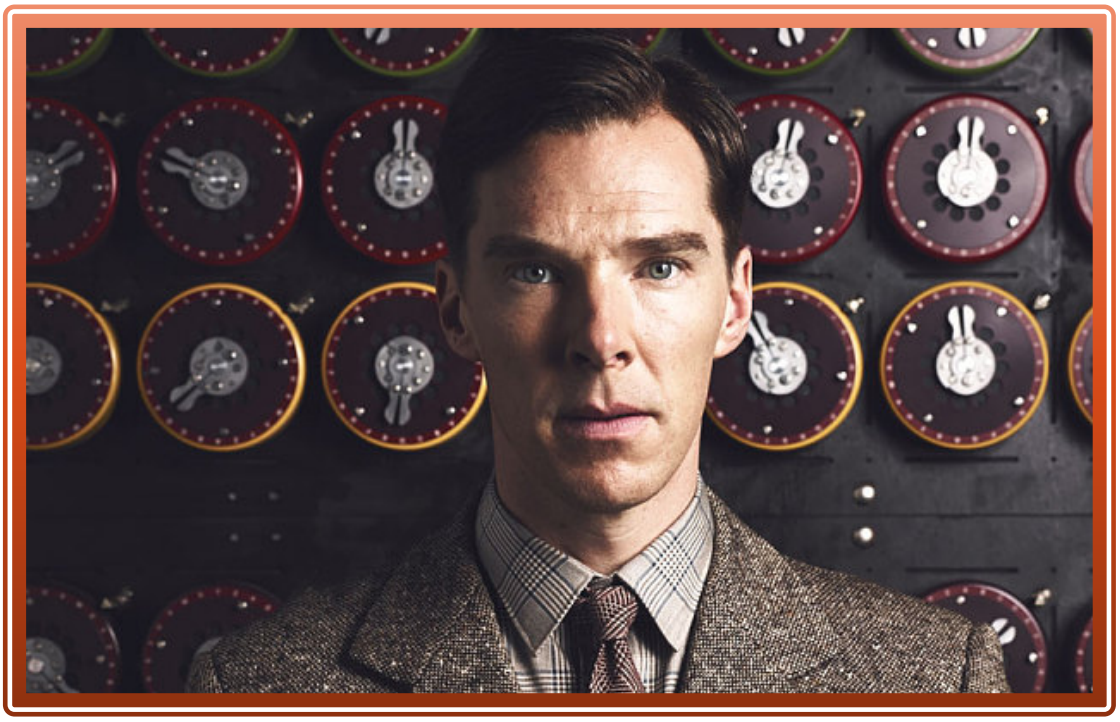
Dit is een goede beveiliging, want twee grote priemgetallen zijn vrij makkelijk te vermenigvuldigen, maar om een groot getal te ontbinden in priemgetallen kost heel veel rekenkracht. Daarvoor voldoen op dit moment de snelste computers niet eens. De boodschap is dus volstrekt veilig zolang de twee priemgetallen maar groot genoeg gekozen worden.

Diverse geheime diensten en veiligheidsorganisaties, zoals de Amerikaanse NSA (National Security Agency) verzetten zich om deze reden hevig tegen codering met priemgetallen. De sterke encryptie kan immers ook gebruikt worden voor illegale doeleinden zoals terrorisme,

drugshandel en belastingontduiking. De Verenigde Staten besteden miljarden dollars aan het ‘aftappen’ van onder andere telefoon- en e-mailverkeer, om zo bijvoorbeeld terroristische aanslagen te verhinderen. Maar als terroristen hun e-mails gaan versleutelen, hebben de terroristen vrij spel voor hun communicatie.

Alan Turing

In februari en maart van dit jaar was de film ‘The Imitation Game’ in de bioscopen te zien. Een film over het leven van de Britse wiskundige Alan Turing die in de oorlog bij MI6, de Britse geheime dienst, werkte om de Enigma code te kraken. De Enigma code was een cryptography om berichten van de Nazi legerleiding te versleutelen om zo commando’s aan het front door te geven. Het afluisteren werd al volop gedaan, dus wat de NSA en Nederlandse geheime dienst doen, is al zo oud als de weg naar Rome. Echter, waren de berichten versleuteld en konden niet ontcijferd worden. De sleutel die de Nazi’s gebruikten bestond uit miljoenen combinaties en werd elke dag vernieuwd. Turing had al snel door, dat met handmatig decoderen de sleutel nooit gevonden kon worden, en bedacht een machine om de code te ontcijferen. Met het vinden van deze sleutel konden de commando’s van de legerleiding onderschept worden. Er wordt beweerd dat de Tweede Wereldoorlog hierdoor 2 jaar eerder is afgelopen en miljoenen mensenlevens heeft gered.



Het trieste aan Alan Turing is zijn persoonlijke leven. Nadat de oorlog voorbij was werd bekend dat hij homoseksueel was. Tot in de jaren zestig van de vorige eeuw moesten homoseksuele mannen in Groot Brittannië of de gevangenis in, of zich chemisch laten castreren middels een hormonen preparaat. Hij heeft ingestemd met de behandeling om verder aan zijn machine te kunnen werken, echter merkte hij dat zijn brein achteruitging en heeft uiteindelijk zelfmoord gepleegd. 50 Jaar na het einde van de Tweede Wereldoorlog is pas bekend geworden dat hij en zijn team de Enigma code hadden gebroken. Dit heeft zolang geduurd omdat de Britten deze voorsprong in kennis wilden behouden. De Eerste Wereldoorlog was nog maar net afgelopen of de Tweede begon al. Op 24 december 2013 is Alan Turing door Koningin Elizabeth II gerehabiliteerd.

Turing test

In kunstmatige intelligentie (AI), wordt de Turing test gebruikt om te bepalen of een computer kan denken als een mens. Volgens deze test wordt een computer geacht kunstmatige intelligentie te hebben als het menselijke reacties onder specifieke omstandigheden kan nabootsen. Als de mens bij het uitvoeren van de test niet in staat is om consequent vast te stellen of een antwoord is gegeven door een computer of door een mens, dan is de test geslaagd. Een praktisch voorbeeld van bovengenoemde test is een Captcha. Een captcha **(C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part), wordt gebruikt om te voorkomen dat bots diverse online-diensten gebruiken. Captcha 's verhinderen automatische deelname van bots aan online-opiniepeilingen en automatische inschrijving voor gratis e-mailboxen (die dan kunnen worden gebruikt om spam te verzenden), en voorkomen dat bots spam versturen door de (niet herkende) afzender een captcha-test te laten afleggen alvorens het e-mailbericht te verzenden.

Wachtwoorden

In ons dagelijks leven geven we heel veel wachtwoorden op. Voor het account van twitter, e-mail server, facebook, enz. enz. Dit doen we, ondanks dat we weten dat een wachtwoord niet veilig is. Wachtwoorden zijn, indien de infrastructuur dit toe laat, eenvoudig te hacken middels een Brute Force hack, het net zolang proberen met verschillende combinaties. Het is dan een kwestie van tijd wanneer een wachtwoord wordt gekraakt. Zorg er dan ook voor dat deze tijd zo lang mogelijk is. Denk hierbij aan de beveiliging van je huis, als je alleen de voordeur achter je dichttrekt, terwijl je weggaat, is deze vaak met een bankpasje al te openen. Door de voordeur met de sleutel op slot te doen, en wellicht nog een extra slot bovenaan in de deur te gebruiken, maak je het de potentiele inbreker al moeilijker. Hierdoor zal hij veel te veel tijd nodig hebben, en jouw huis overslaan. Denk je nog wel aan de achterdeur!

Er zijn veel plaatsen waar wachtwoorden kunnen worden opgeslagen. In de browser, wilt u dit wachtwoord bewaren? Of in speciale programma's waar je alle wachtwoorden bij elkaar hebt, die je met één wachtwoord kunt openen. Heel erg handig maar is dit ook veilig? Hoe gaan banken om met jouw wachtwoorden? Banken vertrouwen de gebruiker al helemaal niet voor wat betreft het kiezen van wachtwoorden en delen speciale apparaten uit of sturen een toegangscode via een SMS, voordat je toegang krijgt tot jouw bankgegevens.

Nu we weten dat we onze data niet maximaal kunnen beveiligen met een wachtwoord, gaan we hier ook anders mee om. Veel mensen hebben voor alle websites waar zij een account hebben hetzelfde wachtwoord. Daarnaast is de gebruikersnaam van veel websites meestal het e-mailadres. Indien een van deze websites wordt gehackt, dan kan in potentie alle

websites waar jij een account hebt, worden gekraakt. Als bij een van die sites je creditcard nummer of je BSN geregistreerd is, is het eenvoudig om identiteitsfraude te plegen met alle gevolgen van dien.

Dit gezegd hebbende gaan we het vanaf vandaag allemaal anders doen. We gaan voor elke website waar we een account aanmaken, of al een hebben, deze wijzigen in een uniek wachtwoord. Indien er dan een website wordt gehackt, en jouw wachtwoord op straat ligt, is dit geen bedreiging voor alle andere websites waar je een account hebt aangemaakt. Om dit doeltreffend te doen, zodat het voor jou eenvoudig is om deze wachtwoorden te onthouden, en toch een sterk wachtwoord te gebruiken, geef ik hier een voorbeeld hoe je dit het beste kunt doen.

Ik stel voor om een wachtwoord uit 3 delen te laten bestaan:

- Een persoonlijk trefwoord
- Deel van de naam van de website
- Volgnummer

Een persoonlijk trefwoord is bijvoorbeeld de naam van je favoriete band/zanger/gitarist, you name it! In dit voorbeeld neem ik de naam van onze poes: *Knuffel*.

Het tweede deel van het wachtwoord is een deel van de naam van de website. Maak hier voor jezelf een afspraak, door de eerste 4 of 5 letters van de website waar je toegang toe wilt, te nemen. Voorbeelden zijn twit, faceb of de laatste 4 letters tter of ebook. De laatste variant is wellicht moeilijker te onthouden, dus neem ik voor dit voorbeeld de eerste 4 letters.

Het laatste deel van het wachtwoord is een volgnummer, omdat je bij sommige websites regelmatig een nieuw wachtwoord moet kiezen.

Als we de 3 onderdelen combineren komen we to het volgende wachtwoord voor respectievelijk facebook en twitter:

knuffelface01, knuffeltwit01

Bovenstaande is nog niet erg indrukwekkend. Er zijn veel websites waar je een combinatie van cijfers, letters en speciale tekens (!@#$) moet gebruiken. Maak hier voor jezelf een afspraak welke letters met getallen of speciale tekens je substitueert. Bijvoorbeeld 3 voor de e, 5 voor de S, ! voor i, | voor l, @ of ^ voor de a. Wissel daarnaast hoofd- en kleine letters met elkaar af.

|<NuFf3| of kNufF3|

F@c3 of f^c3

Zo wordt je wachtwoord voor facebook: |<uFf3|F@c301

en voor twitter: |<uFf3|Tw!t01

Gebruik je creativiteit en maak een lijstje met welke letters je voor welke cijfers of speciale tekens gebruikt. Als je een goede combinatie gevonden hebt, vernietig je dit lijstje en ga je één voor één nieuwe wachtwoorden aanmaken op de websites. Houd bij welke websites je hebt aangepast, zodat je weet welke je nog niet aangepast hebt. Na verloop van tijd type je het eerste deel van het wachtwoord heel eenvoudig in, en wordt de rest vanzelfsprekend.

En mocht je onverhoopt je wachtwoord zijn vergeten, dan klik je op de link: wachtwoord vergeten.

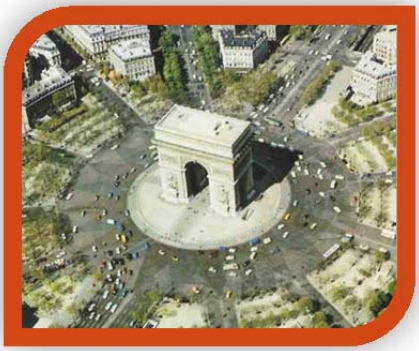
Woninginbraak 2

Bij de woninginbraak werd in ons geval de gelegenheid geboden omdat we niet zorgvuldig de gordijnen gesloten hadden, er ’s avonds geen lampen hadden branden en het belangrijkste de achterdeur niet voldoende afgesloten hadden. Dat de inbreker over de schutting klom en de achterdeur probeerde komt doordat uit een scan bleek dat wij niet thuis zouden zijn. Zie dit als een poortscan, waarbij een poort van de firewall open was.

Vervolgens is er gericht op zoek gegaan naar spullen die makkelijk te vervoeren en verhandelen zijn. Ook de inbreker liet sporen achter tijdens zijn zoektocht, analoog aan sporen van een inbraak in een computersysteem (logging). Het ligt dan aan de details van de data, of je wat met deze informatie kan. Heb je vingerafdrukken, of foto’s of video omdat je een camerasysteem hebt.

Wat je vaak ziet is dat mensen geld op tafel leggen, zodat de inbreker dit pakt en verder geen schade aanricht. Bij netwerkbeveiliging wordt dit ook wel toegepast, en wordt *honeypot* genoemd.

Data Service 2.0



De next step voor Data Services is een nieuwe Business Unit onder PostNL te vormen. Binnen deze nieuwe organisatie zullen in de toekomst de data activiteiten van PostNL plaatsvinden, waaronder de implementatie en het beheer van de DataRotonde, onze kroonjuwelen die goed beveiligd moeten worden.

Wat moeten we op het gebied van security doen om een solide en betrouwbare partij in de markt te zijn? Hoe zorgen we ervoor dat we bij een hack, zo snel mogelijk tot actie overgaan om deze te isoleren, het lek te repareren en de schade te herstellen. Het belangrijkste is dat we security en privacy respecteren en daar ook ruimte voor maken binnen de organisatie. Een IT Security & Privacy team zal moeten toezien dat de regels en procedures voor beide taakgebieden worden gecoördineerd, gerespecteerd en bewaakt.

Voor IT Security Management en Risk Management moet je denken aan:

- Ontwikkelen van een Information Protection Strategy
- Opstellen en implementeren van een IT Security Plan
- Behalen en behouden van ISO 27000 en/of SAS70 certificering
- Opstellen van een Responsible Disclosure
- Samenstellen van een Computer Security Incident Response Team
- Procedures voor het melden van datalekken

Information Protection Strategy

Om de continuïteit van de organisatie te waarborgen dient de organisatie te beschikken over een Information Protection Strategy (IPS). Een IPS bevat de volgende onderdelen:

- Backup and recovery
- Remote data movement
- Storage system security
- Data Lifecycle Management (DLM)
- Information Lifecycle Management (ILM)

Bovenstaande maatregelen zorgen ervoor dat in geval van een calamiteit de waardevolle data, onze kroonjuwelen, weer hersteld kunnen worden, en de verstoring van de commerciële activiteiten tot een minimum wordt beperkt.

Backup and recovery: het veiligstellen van data door het maken van offline kopieën van de data die hersteld kan worden in geval van een ramp of data verminking.

Remote data movement: het real-time of near-real-time verplaatsen van de data naar een locatie buiten het primaire storage systeem (database) of naar een andere plaats om de data te beschermen tegen fysieke beschadiging aan systemen en gebouwen. De twee meest gebruikte technieken zijn remote copy en replicatie. Deze twee technieken kopiëren de data van het ene systeem naar het andere op verschillende locaties.

Storage system security: het toepassen van best practices en beveiligingstechnologie om de opslag op de server en netwerk beveiliging te verhogen.

Data Lifecycle Management (DLM): het automatisch verplaatsen van kritische data naar online en offline opslag. Belangrijke aspecten van DLM is het plaatsen van finale data in een read-only opslag, zodat deze data niet meer veranderd kan worden. Daarnaast kan de data verplaatst worden naar verschillende soorten geheugen afhankelijk van de leeftijd van de data.

Information Lifecycle Management (ILM): een uitvoerige strategie voor het waarderen, categoriseren en beschermen van informatie dragers. Het is verplicht om dit regelmatig te toetsen. ILM, net als DLM, gaat over informatie, geen ruwe data. Besluiten die op basis van informatie worden genomen, vereisen procedures die rekening houden met de context van de informatie.

IT Security Plan

Een IT Security Plan helpt de organisatie bij het beleggen van een goed en betrouwbaar IT Security beleid. In dit plan zijn de volgende onderdelen opgenomen:

- Uitvoeren van periodieke Risk Assessments
- Documenteren van een organisatie breed security programma
- Organiseren van een security management team en het toewijzen van duidelijke security verantwoordelijkheden aan de leden van dit team
- Implementeren van een security beleid voor personeel
- Monitoren van de effectiviteit van het security programma, en daar waar nodig aanpassingen te doen.

Certificering

Het regelmatig laten toetsen van de technieken, processen en procedures geven een betrouwbare indruk aan de markt. Daarnaast houdt dit ons scherp en kunnen we daar waar nodig verbeteringen toepassen.

Responsible Disclosure

Een Responsible Disclosure is een statement op de website waarbij wij als bedrijf aangeven dat wij indien een hacker toegang heeft tot ons computersysteem, geen aangifte zullen doen. Een hacker mag dan, in overleg met ons informatie over het lek publiceren, nadat wij de tijd hebben gehad om dit te herstellen.

Computer Security Incident Response Team

Een Computer Security Incident Response Team (CSIRT) is verantwoordelijk voor het snel ontdekken van incidenten, het tot een minimum beperken van de data verlies of –

verminking, het nemen van mitigerende maatregelen van het datalek, en herstellen van de computers en informatie.

Meldplicht datalekken

De Eerste Kamer heeft op 26 mei 2015 een wetsvoorstel aangenomen dat een meldplicht datalekken regelt. Deze meldplicht houdt in dat bedrijven en overheden direct een melding moeten doen bij het College Bescherming Persoonsgegevens (CBP) zodra zij een ernstig datalek hebben. De datum van inwerkingtreding wordt bepaald bij koninklijk besluit. Het CBP gaat vooralsnog uit van inwerkingtreding per 1 januari 2016.

Maatregelen voor beveiliging (bron: CBP website)

Om datalekken te voorkomen, moeten bedrijven en overheden die persoonsgegevens gebruiken deze volgens de Wet bescherming persoonsgegevens (Wbp) beveiligen. De Wbp geeft aan dat ze hiervoor passende technische en organisatorische maatregelen moeten nemen.

Dit houdt in dat organisaties moderne technieken moeten gebruiken om persoonsgegevens te beveiligen. En dat ze niet alleen naar de techniek kijken, maar ook naar hoe ze als organisatie met persoonsgegevens omgaan. Wie heeft er bijvoorbeeld toegang tot welke gegevens?

Organisaties die persoonsgegevens gaan verzamelen, moeten vooraf nadenken over de beveiliging hiervan. En beveiliging van persoonsgegevens moet binnen een organisatie een blijvend punt van aandacht zijn.

Literatuurlijst

DASSELAAR, Arjan. (2005), **HANDBOEK DIGITALE CRIMINALITEIT**. Culemborg, Nederland: Van Duuren Media.

NORTCUTT, Stephen, Zeltser, Lenny, Winters, Scott, Kent Frederik, Karen, & Ritchy, Ronald W. (2003). **INSIDE NETWORK PERIMETER SECURITY**. Indianapolis, USA: New Riders.

ROOIJ, Jeroen de. (2005), **DE SIMPELE MAGIE VAN PRIEMGETALLEN IN GEHEIMSCHRIFT**. Geraadpleegd op 5 mei 2015, van http://www.kennislink.nl/publicaties/de-simpele-magie-van-priemgetallen-in-geheimschrift

SOMMERVILLE, Ian (2011), **SOFTWARE ENGINEERING**, 9th edition. Boston, USA: Addison-Wesley.

STALLINGS, William & Brown, Lawrie (2015), **COMPUTER SECURITY** – Principles and practice 3rd edition. Boston, USA: Pearson.

TANENBAUM, Andrew S. (1988), **COMPUTER NETWORKS**. New Jersey, USA: Prentice Hall.