



Een overzicht van belangrijke informatiebeveiligingsbedreigingen in 2010 voor Belgische ondernemingen en overheid

European Security Innovation Network
www.securityinnovationnetwork.com

Leaders In Security - LSEC
www.leadersinsecurity.org

Belgian Information Security Initiative
www.bissi.be

Maart 2011 V.2.0
email : report2010@lsec.be



Inhoudstafel

European Security Innovation Network www.securityinnovationnetwork.com 1

1. Inleiding 3
2. Observaties in 2010 4
 1. De Chinese Technical Persistent Attacks (TPA) 4
 2. Het wikileaks fenomeen en de consequenties voor databeveiliging 6
 3. Anonymous en andere georganiseerde DDOS campagnes 9
 4. Stuxnet of de geheime codewissel in een kritische infrastructuur 10
 5. Botnets komen en gaan maar hun gevaar zal altijd blijven bestaan 12
 6. DLL injection laat je nieuwe functies toevoegen aan een programma 13
 7. De onveilige website als uitnodiging voor spammers en hackers 15
 8. Uw website is gehacked en u staat dus even voor aap 17
- Het belang van een lokale professionele ISP, en host of cloud service (minsten voor uw meest bedrijfskritische onderdelen) 17
9. Conflicker of het bewijs dat je (nog) niet op je ISP moet rekenen..... 18
10. De informatie over informatiebeveiliging is erg gefragmenteerd en complex 19
3. Vooruitzichten in 2011..... 20
 1. Mobiele risico's 20
 2. De krakende encryptie..... 20
 3. meer hardware aanvallen..... 20
 4. Security as a Service, Virtualisatie, professionele virusaanvallen en sandboxing... 20
 5. Data Breach Notification : meldplicht in Europa komt er aan..... 21
4. Enkele Belgische indicatoren 21
 1. invloed van de preventieve acties van dns.be * 21
 2. Nog nooit werden zoveel .be websites gehacked-gedefaced..... 22
 3. De invloed van de interventies van het CERT.Be in 2010 (bron CERT.BE) 23
 5. .be websites die virussen installeren volgens malwaredomainlist.com 23
 6. .be Phishingsites 2010 in Phishtank.com voor enkele Belgische netwerken 24
 7. 2500 Belgische IP adressen met Conficker (2008) (Shadowserver.org) 24
5. enkele opmerkingen 25
6. aanbevelingen voor een beter informatiebeveiligingsbeleid..... 27
 - 4.1 oprichting van een informatiebeveiligingsstructuur voor België, dat normen en voorwaarden kan inrichten voor haar infrastructuur en bedrijven 27
 - 4.2 De industrie kan zelfreguleren en een eigen certificatie kunnen opstellen 27
 - 4.3 Verdere verbetering van CERT.be, en betere samenwerking van FCCU.be en de andere initiatieven..... 27
 - 4.4 ISP's vormen een onderdeel van de kritische infrastructuren, een gecoördineerd beleid is nodig..... 27
 - 4.5. verbeteren van de wetgeving en noodzaak van betere opleiding 28



1. Inleiding

We leren uit het verleden dat we telkens opnieuw dezelfde stommititeiten begaan. Dat is geen nieuwe uitspraak, maar ze is eveneens toepasselijk op de toestand van de informatiebeveiliging in België.

Als vereniging van actoren (leveranciers, gebruikers, adviseurs, integratoren, overheid en industriegroeperingen) van informatiebeveiliging, willen we vanuit LSEC met dit document geen stenen werpen naar de ene of de andere. We willen het publiek, overheid en industrie informeren over vaststellingen die we hebben kunnen doen in het afgelopen jaar, en er enige context bijgeven. Op die manier zijn we in elk geval zeker dat ze niet onherkenbaar voorbij zijn gegaan, zodat we hopelijk in de toekomst minstens kunnen leren over de fouten uit het verleden.

Een aantal van onze leden zijn prominente internationale bedrijven en figuren uit de wereld van de informatiebeveiliging. Ze worden gevraagd op de belangrijkste conferenties en bijeenkomsten van de VS tot in Azië en doorheen Europa, om ondermeer een inzicht te geven in de belangrijkste bedreigingen en ontwikkelingen op het vlak van informatie beveiliging. Met dit document willen we ook hun perspectieven kaderen in een Belgische situatie.

Dit document is tot stand gekomen dankzij de inzichten en invullingen van verschillende bedrijven en experts doorheen het afgelopen jaar.

De ambitie is dit document jaarlijks te publiceren, met de medewerking van de belangrijkste internationale en lokale spelers en te voorzien van voldoende materiaal zodat we telkens kunnen beschikken over een historisch archief en een referentiekader voor iedereen die zich in informatiebeveiliging interesseert of dient te interesseren.

Voor wie kiest de commentaren en relevante gegevens naast zich neer te leggen, en geen verantwoordelijkheid op te nemen om acties te ondernemen, zal zich op een of ander moment toch moeten verantwoorden. Een overweging van kosten en baten is relevant, maar zal in de toekomst ook moeten afgewogen worden in het kader van sociale verantwoordelijkheid. Botnets op uw netwerk impacteren de hele economie. Onvoldoende beveiligde controlesystemen kunnen gevolgen hebben voor de veiligheid van mens en milieu. Het ontbreken van strategie, actieplan en het bewust negeren van internationale voorbeelden en signalen uit de eigen markt, resulteren in een politieke zelfmoord.

Dit is een privé-initiatief, maar verwelkomt de ondersteuning van de overheid om jaarlijks een onafhankelijk en volledig overzicht van de Belgische data- en netwerkveiligheid samen te stellen.

Over de auteurs : LSEC is Belgische vereniging van informatiebeveiligingsbedrijven en informatiebeveiligingsexperts. Dit document is samengesteld op basis van uitgebreid werk van verschillende vrijwillige onderzoekers en onafhankelijk gecompileerd door LSEC, in samenwerking met het European Security Innovation Network, een verband van beveiligingsclusters in Europa. Het wordt mee ondersteund door het Belgian Information Security Initiative, dat pleit voor een beter informatiebeveiligingsbeleid in België.



2. Observaties in 2010

Onze onderzoekers verzamelden de volgende belangrijke activiteiten die plaatsvonden in 2010 en een belangrijke stempel zullen drukken op de informatiebeveiliging van de komende maanden en jaren:

1. De Chinese Technical Persistent Attacks (TPA)
2. Het wikileaks fenomeen en de consequenties voor databeveiliging
3. Anonymous en andere georganiseerde DDOS campagnes
4. Stuxnet of de geheime codewissel in een kritische infrastructuur
5. Botnets komen en gaan maar hun gevaar zal altijd blijven bestaan
6. DLL injection laat je nieuwe functies toevoegen aan een programma
7. De onveilige website als uitnodiging voor spammers en hackers
8. Uw website is gehacked en u staat dus even voor aap
9. Het belang van een lokale professionele ISP, en host of cloud service (minsten voor uw meest bedrijfskritische onderdelen)
10. Conflicker of het bewijs dat je (nog) niet op je ISP moet rekenen
11. De informatie over informatiebeveiliging is erg gefragmenteerd en complex

1. De Chinese Technical Persistent Attacks (TPA)

Reeds geruime tijd wordt het verschil gemaakt tussen zogenoemde "script kiddies" en de meer gespecialiseerde hackers. Ondertussen kwamen er verschillende soorten andere soorten aanvallers bij, maar de ontwikkelaars en uitvoerders van TPA software worden hoe dan ook beschouwd als de superhackers die langzamerhand de grootste prioriteit worden in de verdoken cybersquirmishes op het netwerk. Er wordt vermoed dat ze vaak in opdracht werken van andere instanties, maar zeker niet altijd. Volgens de gespecialiseerde Amerikaanse veiligheidsfirma HBGary – wiens emails werden gehacked en gepubliceerd in 2011 – zouden ongeveer honderd groepen in China verantwoordelijk zijn voor 90% van de TPA aanvallen. TPA's kunnen alle huidige bestaande verdedigingsmiddelen omzeilen of bijna probleemloos doorstaan.

Een definitie van TPA dringt zich op, temeer omdat TPA zich vandaag te gemakkelijk door de mazen van het net laten wringen. Volgens gepubliceerde emails van HBGary kan worden afgeleid dat zelfs instellingen zoals NATO, Morgan Stanley of leveranciers aan het Amerikaanse leger geïnfecteerd werden.

TPA zijn **gericht** tegen een specifieke afdeling of persoon **gebaseerd op de kennis die via online (sociale) media** verzameld is over de persoon waardoor de mogelijkheid dat betrokkene de attachment opent of de website bezoekt groter is. (Bijvoorbeeld indien men weet dat de CEO van een bedrijf een verzamelaar is van sigaren dan is de kans groter dat hij een PDF met aanvalscode over een nieuwe collectie sigaren opent groot.)

TPA zijn "**low level**" aanvallen die qua intensiteit en herhaling zodanig zelden voorkomen dat ze in verhouding tot de andere spam- en scancampagnes niet worden opgemerkt door de monitors.

TPA maken gebruik van **voordien ongekende veiligheidslekken** en worden soms uitgevoerd in verschillende stappen. Sommige aanvallen zijn **soms zelfs specifiek geschreven** voor de werkomgeving of IT-beveiliging van de betrokkene.

Het belangrijkste **doelwit is het extracteren** (naar buitensturen) **van informatie** - al dan niet via tunneling via ongewone poorten zoals DNS - **of het monitoren of onderscheppen van transacties en communicaties.**



TPA aanvallen zijn persistent wat betekent dat ze aangehouden worden en steeds op dezelfde manier zullen blijven zoeken naar die kleine veiligheidslekken of die mogelijke aanvalsscenario's die hen tijdelijk de nodige toegang verschaffen.

Ze zijn een voorbeeld van een "perfecte aanval", waarmee wordt bedoeld dat **nadien alle sporen worden uitgewist** en ervoor zorgt dat niemand goed weet welke informatie naar wie is vertrokken. Indien de doelstelling de destabilisatie van de firma of organisatie is dan kan het de bedoeling zijn zich te laten ontdekken door veel sporen rond te strooien - zelfs als die niet echt succesvol waren - zodat de organisatie tijdens de paranoia na de ontdekking drastische maatregelen neemt en elk vertrouwen in hetzij welk digitaal medium of digitale correspondent totaal verliest waardoor de organisatie veel van haar efficiëntie verliest.

Het belang van classificatie van de informatie en toegangscontrole

Het is belangrijk voor een organisatie of een firma om vast te leggen welke informatie of beheerssystemen zo belangrijk zijn voor het bedrijf of de organisatie dat ze enorme schade zou oplopen indien deze informatie of toegang al dan niet publiekelijk in handen zou komen van derden.

Vandaar het belang van de classificatie van informatie, toegangscontrole en de absolute scheiding van deze informatie binnen het netwerk en de workflow van een organisatie. In grotere netwerken of firma's kan men zelfs spreken van gescheiden netwerken waarbij er een totale gescheiden toegang is tussen de publieke computers met o.a. internettoegang en het interne netwerk waar het veiligheidsniveau veel hoger ligt. Desgevallend kan een apart intern netwerk zeker geen overbodige luxe zijn.

Dit netwerk moet uiteraard voorzien worden van de nodige versterkte beveiliging zoals een multi-factor authenticatie, een end-to-end encryptie en een monitoring door zowel technologie als mens.

In veel bedrijven of organisaties gaat het om bepaalde persoonslijsten, kritische R&D, financiële gegevens en onderhandelingen of informatie die een officieel statuut van geheimhouding heeft gekregen.

Het belang van filteren en monitoren.

Aan de ene kant is het zo dat er steeds krachtigere systemen bestaan om het internetverkeer te filteren in een omgeving. Daardoor ontstaat er soms een vals gevoel van veiligheid. De illusie bestaat immers dat alles onder controle is. De realiteit is dat bestaande, gekende risico's sneller en beter zullen onderschept worden, maar dat natuurlijk ook de complexiteit en kracht van de gevaren vaak sneller toenemen dan de oplossingen om ze te kunnen onderscheppen.

Het belang van data bescherming.

Een toenemend aantal oplossingen kan de onderneming ondersteunen in de classificatie van informatie en systemen. Eens geclassificeerd, zullen een aantal van die oplossingen ook voorzien in de toegangscontrole en de rapportering bij gebruik of toegang van de respectievelijke confidentiële informatie.

Het belang van enkele basisregels voor :



a) netwerkverkeer

- een interne firewall of toegangscontrolelijst op de switch die de toegang tot interne vertrouwelijke infrastructuur of diensten beperkt en controleert
- een aparte infrastructuur voor de geheime files met inbegrip van virtualisatie en backup die end to end encryptie voorziet naast de toegangscontrole en monitoring
- zorg ervoor dat DNS, email en internetverkeer via een gecentraliseerde interne infrastructuur verlopen die de enige is die via de firewall een connectie kan leggen naar deze diensten op het internet

b) internetverkeer

- gebruik altijd een proxy voor je internetverkeer
- blokkeer volledig alle interne infrastructuur die geen internetverkeer nodig heeft
- (overweeg om het internetverkeer te beperken tot bedrijfskritische specifieke websites, eventueel op bepaalde tijdstippen of van op bepaalde werkposten, ...)
- blokkeer het internetverkeer naar verre landen (zoals Rusland en China) waar je totaal 'geen zaken' mee hebt maar waar het veiligheidsrisico groot is (of voorzie hiervoor bepaalde aparte computers)

Het resultaat hiervan is dat het aantal logs die je nog zou moeten bekijken kleiner wordt, abnormaal gedrag op een netwerk vlugger te ontdekken is en dat de kans dat een gecompromitteerde installatie haar informatie naar buiten krijgt beperkter is.

Trend van "blacklisting" naar "whitelisting"

De algemene evolutie op het vlak van filtering is een tendens naar whitelisting waarbij enkel nog de toegestane bestemmingen en applicaties worden gedefinieerd en al de rest verboden is. Voor vertrouwelijke omgevingen is er geen alternatief. Tenzij men een zaal vol met veiligheidspersoneel ter beschikking heeft.

2. Het wikileaks fenomeen en de consequenties voor databeveiliging

Wikileaks werd een paar jaar geleden opgericht met geld van een Amerikaanse organisatie voor meer openbaarheid. De doelstelling in het begin was om dissidenten van over de hele wereld (en toen vooral uit China, Rusland en andere pseudo-democratiën of dictaturen) de mogelijkheid te geven om informatie te publiceren zonder hun eigen persoonlijke veiligheid in gevaar te brengen. Deze doelstelling is echter nooit gehaald. Het belangrijkste Belgische bestand was bijvoorbeeld een kopie van een deel van het dossier Dutroux dat zonder enige bescherming werd uitgedeeld aan de advocaten en pers indertijd. Tevens was de beveiliging van de vroegere Wikileaks site niet perfect en moest die verleden jaar een tijdje uit de ether gaan omdat ze niet meer over voldoende fondsen beschikte.



Het is dan ook niet verwonderlijk dat Assange - de rondreizende cyberanarchist - blufpoker wou spelen toen hij een enorme database met rapporten en video's van de oorlog in Irak, Afghanistan en vertrouwelijke Amerikaanse diplomatieke verslagen kreeg. De release van de video 'collateral murder' werd een echt media-evenement waarna het Pentagon begon met de planning van hoe men Wikileaks kon beperken of uit de ether halen. Toen de oorlogsverslagen uit Irak en Afghanistan volgden was de paniek compleet. Alhoewel er momenteel geen enkel direct bewijs bestaat dat personen die vernoemd worden in deze logs ondertussen enige hinder hebben ondervonden, was er toch zeer zware kritiek op de ongecensureerde publicatie van deze rapporten. Wikileaks wilde voor de publicatie van de diplomatieke verslagen samenwerken met de Amerikaanse overheid maar die kon niet meewerken aan het behandelen van in haar ogen 'gestolen materiaal'. De Amerikaanse regering wou dat men het gestolen materiaal teruggaf en sprak ook steeds dreigender taal. Ondertussen was er ook binnen Wikileaks een hevig debat ontstaan en zoals meestal het geval is in vrijwilligersgroepen ontstonden er kampen en verlieten een aantal mensen de organisatie. Het is trouwens vandaag totaal onduidelijk wie nog tot deze organisatie behoort. Sommige van deze personen of groepen hebben ondertussen varianten opgericht. Wikileaks wou echter niet dezelfde fout begaan en heeft niet alle diplomatieke verslagen zomaar op het internet gegooid. Er bestaat wel een verzekeringsfile met een zogenaamde encryptie (die niet sterk is volgens sommigen) die slechts kan worden geactiveerd als er 'iets' zou gebeuren met Assange.

Sommige grote mediagroepen hebben een kopie van de totale database gekregen en publiceren elk dagelijks een aantal diplomatieke verslagen nadat ze de namen en de echt vertrouwelijke zaken er hebben uitgehaald, al verschilt dit van media tot media. De meeste van die grote media zijn ondertussen wel gestopt met deze specifieke publicatie van deze gegevens. Men had waarschijnlijk sensationele uitspraken verwacht maar werd geconfronteerd met partiële maar professionele rapporten.

Binnen de Amerikaanse opiniemakers zijn er dan ook personen die vinden dat uiteindelijk de VS er niet zo slecht uitkomt omdat wat vooral uit zowel de oorlogsverslagen als de diplomatieke verslagen blijkt, is dat de Amerikaanse soldaten en het diplomatiek personeel op papier proberen om zo goed mogelijk hun werk te doen op een zo professioneel mogelijke manier in soms zeer moeilijke of vijandige omstandigheden. Het zijn vooral andere bedrijven en (ex)machthebbers die erdoor om verschillende redenen in het nauw kwamen.

De publicatie van de diplomatieke verslagen was de grootste druppel die het glas heeft doen overstromen en die heeft geleid tot wat men de eerste gecoördineerde overheidsactie kan noemen om een webdienst in een ander land uit de ether te halen. Consultants zeiden immers dat Wikileaks niet mythisch is omdat het op het internet staat. Het internet is een redelijk materiële aangelegenheid. Het gaat om hosting, dns, betalingen en andere webdiensten. Deze werden één voor één onder druk gezet om hun relatie met Wikileaks minstens tijdelijk te herzien zodat een redelijk goed georganiseerde 'machine' sterk werd ontregeld. De centrale servers staan wel op een bulletproof (onhackable) server in Zwitserland en de inhoud wordt wel verdeeld over honderden andere websites, maar de impact en 'mystiek' van de centrale wikileaksite is er niet meer. Het is tevens zo dat het voor buitenstaanders redelijk gevaarlijk wordt om nog met Wikileaks te gaan samenwerken omdat de vervolgers van Wikileaks momenteel in de laatste fase zijn aanbeland, namelijk de bedreiging en het in verdenking stellen van alle personen die in 2010 actief waren in en rond Wikileaks. Wikileaks heeft ondertussen wel aangekondigd dat ze in 2011 een lading gegevens zal publiceren over enkele financiële instellingen. Maar ook daar zouden ze op terugkomen omdat er nog veel 'werk' is aan deze 'unsexy' en gedateerde gegevens (een harddisk met gigabytes aan emails uit 2004).

(red.)



Wikileaks is uiteindelijk een **goed voorbeeld van "data leakage"**, informatie die de organisatie verlaat, zonder dat het geauthoriseerd is, of zelfs zonder dat de organisatie er iets van wist en het liet gebeuren.

De oorlogslogs- en de diplomatieke verslagen werden door een gefrustreerde soldaat afgegeven. Hij had via zijn werkpost toegang tot 'open internal intelligence' en kon die zonder probleem of logging kopiëren en op een cd naar buiten brengen. Deze gegevens hadden ook geen intrinsieke bescherming zodat ze op hetzij welke machine konden worden geopend.

Securityverantwoordelijken zien hierin een aantal zware fouten met betrekking tot de bescherming van dergelijke belangrijke informatie. Indien men deze gegevens niet had kunnen kopiëren, indien er een logging was geweest die onmiddellijk had gemeld dat iemand een hele dataset kopiëerde en indien er een intrinsieke bescherming was geweest op de data en men de 'geheime' omgeving niet kon verlaten met informaticamateriaal dan was deze soldaat of nooit buitengeraakt met de informatie of had men hem opgemerkt terwijl hij bezig was met de operatie. Het is vandaag ook technisch mogelijk om datasets van op afstand te vernietigen. Met de huidige proxytechnologie is het ook mogelijk om medewerkers gegevens of documenten enkel te laten lezen zonder dat ze deze kunnen kopiëren.

Het grote probleem is natuurlijk dat sinds 9/11 men probeert om zoveel mogelijke medewerkers en analisten zoveel mogelijk informatie te geven om te voorkomen dat er nog gevaarlijke individuen door de mazen van het net zouden kunnen kruipen omdat niemand nog een overzicht heeft van alle puzzelstukken.

Houdbaarheidsdatum voor gepubliceerde (gelekte) informatie : onbeperkt. Het internet is tijdloos en kan moeilijk (of niet) worden veranderd : éénmaal de gegevens op het internet zijn verschenen, zullen ze niet verdwijnen

Herhaaldelijk worden datasets met vertrouwelijke gegevens, e mails of lijsten met paswoorden op het internet gepubliceerd en meestal probeert men eerst om ze te doen verdwijnen door het vragen aan elke hoster of siteverantwoordelijke om ze te verwijderen op basis van één of andere wet of het gebruikersreglement. Dit is nuttig om de data in de marginaliteit van het internet te houden maar het zal ze nooit volledig doen verdwijnen. Iedere tijdelijke publicatie is hoe dan ook verantwoordelijk voor honderden downloads en eventuele nieuwe publicaties.

Het is geen overdreven investering om als groot bedrijf of instelling een procedure uit te werken waarin deze juridische notificaties reeds zijn opgesteld en waarbij enkel de dataset met hun links en de online diensten nog dienen te worden ingevuld.

Ook de digitale pen is krachtiger dan het zwaard : deze data kan alleen op het internet verschijnen omdat ze is gemaakt

Momenteel wordt zoveel geschreven en opgenomen dat het blijkt alsof we schrik hebben om al onze gedachten en gesprekken te vergeten indien ze niet ergens staan gedigitaliseerd. Zowel uit de oorlogslogs als uit de diplomatieke verslagen blijkt wel



meermaals dat het soms beter is om niet alles op te schrijven. Sinds Wikileaks vinden steeds meer vertrouwelijke vergaderingen plaats zonder dat iedereen alles zit te noteren. Eén secretaresse die één beperkt officieel verslag maakt is meer dan genoeg.

Ook voor informatiebeveiliging is crisiscommunicatie van belang.

De communicatieverantwoordelijken van grote bedrijven en belangrijke organisaties en instellingen dienen te beseffen dat eens ergens op het internet belangrijke data over hun werkgever zou kunnen verschijnen. Het is niet op moment dat men een communicatieplan moet ontwikkelen dat zowel de inhoud, de consequenties en de verschillende beslissingsprocessen vastlegt. Indien men een plan heeft, is het ook geen overbodige luxe om ze eens virtueel te testen op 1 dataset die op één van de tientallen 'leaks' sites zou staan.

Dit is natuurlijk geen oplossing want als men de beveiliging van de data zelf niet consequent doorvoert (classificatie, DLP, toegang, logging, encryptie, secure (remote) destruction) dan is de echte efficiëntie van deze kostbare voorbereiding minimaal.

3. Anonymous en andere georganiseerde DDOS campagnes

Anonymous was eerst een groep gebruikers van het nogal chaotische en soms erg studentikoze (volgens anderen wansmakelijke) Amerikaanse internetforum 4chan.org. Ze werden eerst bekend door hun aanvallen tegen mediabedrijven en copyrightverdedigers maar kwamen pas echt in het voetlicht met hun oproep om de campagne tegen Wikileaks te bestraffen. De arrestatie van de zwervende goeroe Assagne was hun orgelpunt. Net zoals ze vroeger al een hele reeks grote sites tijdelijk uit de ether hadden gehaald, gingen ze toen ook onder grote media-aandacht de webservices zoals Mastercard en Paypal aanvallen omdat die hun samenwerking met Wikileaks beëindigden. Het groepje ongeregeld kreeg toen ook intellectuele cyberactivisten in haar midden, wat zich nog versterkte toen ze zich in 2011 ook ging bezighouden met de Arabische protesten. 2011 zal trouwens het jaar worden waarop waarschijnlijk Anonymous in verschillende groepen

De gebruikte techniek van ondermeer Anonymous was niet zo verschillend van de zogenaamde 'cyberoorlogen' tegen Estonië, Georgië of de Cyberintifada (Gaza-oorlog). Een groep activisten zet op een aantal blogs of twitterkanalen software en vraagt haar 'soldaten' om die te installeren waardoor ze deze computers opdrachten kan geven tegen haar doelwitten. Anonymous gebruikte daarvoor de software LOIC dat een aanpaste performance-monitoringtool is, maar dat werd verbonden met een IRC kanaal en later ook een online versie kreeg. Er waren wel een aantal fundamentele problemen. Zo was het niet altijd duidelijk wie besliste wat de doelwitten waren, wie de IRC kanalen en dus de software bij al die gebruikers in handen had en of de software zelf wel zo veilig was.

De online versie kon men trouwens tegen hetzij welke site gebruiken, waaronder zelfs tegen wikileaks zelf. Het effect van de aanvallen was een grote media-aandacht maar die ging meestal niet verder dan de hype en zag niet dat meestal slechts een klein onderdeel van de webservice onbereikbaar was geworden. Om te bewijzen dat men een site uit de lucht had gehaald gebruikte men monitoringtools die werkten op basis van een ping. Indien een site die wordt aangevallen met een massale storm van pings als reactie alle pings tegenhoudt, dan worden ook alle pings van die monitortools tegengehouden en gedropt. Indien men de site gewoon intikte was de site meestal wel beschikbaar. Volgens



analyses nadien zou ook blijken dat het aantal aanvallers niet zo overdonderend veel was en dat de anonimiteit van de aanvallers beperkt was.

In 2011 wordt deze techniek nog altijd toegepast. Er zijn ondertussen tientallen Anonymous groepen met allemaal hun subgroepen en campagnes. Blijkt dat sommige van die groepen zelf begonnen zijn met het hacken van databases en het publiceren van gegevens zonder nog een beroep te doen op Wikileaks. De **Anonymous subculture** wordt zo steeds meer een echt 'disruptive event' dat kan toeslaan wanneer en waar het wil.

Er zijn ook andere, slimmere 'flashmob' aanvallen zoals het versturen van duizenden emails met grote bestanden naar de mailboxen zodat de mailbox en de mailserver vastlopen, het massaal zenden van faxen naar de faxnummers vanop het internet zodat die zonder papier komen te zitten etc....

Belang van internet- en oppositiemonitoring

Er is geen enkele reden waarom je geen passieve monitoring zou mogen opzetten van wat er over je bedrijf of organisatie op het internet wordt gepubliceerd.

Tegenstanders actief dwarsbomen of infiltreren; of door manipulatie en 'black SEO' virtuele opiniemanipulatie opzetten zijn een aantal stappen te ver. Dergelijke 'undercover'operaties komen meestal terug als een PR-boemerang en richten duizendmaal meer schade aan dan hun eventuele kortstondige 'positieve' effecten.

Belang van netwerkmonitoring en capaciteitsplanning

Het is zinvol om "normaal netwerkverkeer" naar je infrastructuur te meten. Op die manier kunnen er variaties worden vastgesteld en kunnen aanvallen worden opgemerkt. Overweeg mogelijkheden van duplicatie en gedistribueerde omgevingen. Je kan ook overwegen om het verkeer naar bijvoorbeeld eigen websites in goeie banen te helpen leiden, of indien nodig het verkeer om te leiden naar een externe hoster (bijv. in de cloud).

4. Stuxnet of de geheime codewissel in een kritische infrastructuur

Toen Stuxnet per ongeluk werd ontdekt in een elektriciteitscentrale in de Oekraïne was het wel duidelijk dat het een zeer gevaarlijk virus was omdat het een aantal zerodays gebruikte die Microsoft verplicht hebben om zeer snel een noodpatch uit te brengen. Zelfs nu heeft men nog geen volledig overzicht van alle facetten van deze aanvalscodes. Sommigen zijn minder onder de indruk omdat de code ook een aantal beginnersfouten bevatte, maar deze kunnen volgens anderen dan ook weer opzettelijk zijn toegevoegd om mensen op het verkeerde been te zetten zoals een goede 'black operation' beaamd.

In het hele verhaal wordt trouwens soms de technische analyse verdrongen door het zogenaamde politieke cyberwar-aspect. Volgens sommige analisten zou het ontworpen zijn (vb door Amerikanen en Israëli) om het Iraanse kernwapenprogramma te verstoren, vertragen of te onderbreken. Ondertussen heeft het wel duizenden industriële en 'electrische' installaties met dezelfde SCADA technologie van Siemens geïnfecteerd.

Stuxnet is niet zozeer een gespecialiseerde aanval omdat ze geschreven is om specifieke acties te ondernemen op een specifieke omgeving op een specifiek moment; maar omdat



het dit meestal kan doen zonder dat de operator dit ooit zal opmerken - zelfs niet als de patch tegen Stuxnet werd geïnstalleerd. Stuxnet werd immers zo geschreven dat ze zich installeerde zoals gewone authentieke broncode van de software. De normale controlesoftware en patch zouden haar niet ontdekken.

Het is natuurlijk belangrijk om erop te wijzen dat het virus zo gemakkelijk toegang had tot de SCADA software van Siemens omdat de administratieve paswoorden in de code van de software stonden en zelfs na de patching niet mochten worden gewijzigd.

Deze aanval is belangrijk omdat ze het toenemende belang van kritische infrastructuur (zoals elektriciteitsnetwerken) als mogelijke doelen voor aanvallen illustreert.

De aanval heeft immers duidelijk bewezen dat zelfs de meest gespecialiseerde en meest doelgerichte aanvalscodes toch nog over de hele wereld duizenden installaties kan infecteren en dat men - bij eventuele foute handelingen - met verschillende zware industriële en eventueel nucleaire gevolgen had kunnen ondervinden.

We berusten in de wetenschap vandaag, dat dit mogelijk is gebleken en dat soortgelijke aanvallen in de toekomst opnieuw zullen plaatsvinden.

Het belang van Stuxnet en soortgelijke incidenten :

Langs het sleutelgat naar binnen

Volgens de huidige kennis van het incident zou Stuxnet de Iraanse kerncentrale zijn binnengebracht via de laptops van Russische subcontractors die de SCADA software kwamen onderhouden of installeren. Het is niet de eerste keer dat zelfs veilige omgevingen of strikt beveiligde netwerken geïnfecteerd worden door usb-sticks of laptops. De aanvalscodes zijn vandaag zo vernuftig dat indien men een omgeving of netwerk werkelijk wil afschermen van hetzij welk extern risico dit ook volledig zo moet zijn en blijven.

Ongecontroleerde variaties in de code

We zijn er tot nu toe altijd vanuit gegaan dat gevaarlijke code zich aan normale code toevoegde of dat het de operaties van een software zo wijzigde dat het direct duidelijk was dat er gevaarlijke dingen aan waren toegevoegd. Het is waarschijnlijk de eerste keer dat aanvalscodes een onderdeel van de normale code wijzigt en zelfs na eventuele patching alles op het eerste zicht normaal laat functioneren.

In dergelijke belangrijke omgevingen is een strikte controle van hetzij welke wijziging van de code in een applicatie dan ook een basisvereiste. In dat geval had men de infectie opgemerkt ondanks het feit dat geen enkele andere controlefunctie iets had opgemerkt. Dergelijke codemonitoring heeft ook een ander kwalitatief voordeel dat een onmiddellijke return on investment is, men zal bij een bug of probleem altijd weten wat de laatste wijziging aan de code was en terug kunnen keren naar wat men de 'last working version' is gaan noemen.

Noodzaak van een betere beveiliging van controlesystemen en gedateerde systemen



5. Botnets komen en gaan maar hun gevaar zal altijd blijven bestaan

Botnets zijn geen nieuw verschijnsel en het ziet er ook niet naar uit dat ze zullen verdwijnen. Het is een organisatiemethode voor de cybercriminelen om zichzelf te beschermen (achter een hele reeks andere computers), nieuwe diensten aan te bieden (zoals een DDOS aanval) of om hun aanvallen sneller en massaal te kunnen uitvoeren (spambots en clickfraud).

Wat volgens veel onderzoekers opvalt zijn : zowel de bescherming van hun infrastructuur (bulletproofhosting), de overlevingskansen van hun netwerk (door iedere geïnfecteerde computer een organiserende (control and command) functie te geven), de massale aanpassingen van de aanvalscodes met een enorm aantal varianten en dat ze er vaak in slagen om voorbij de antiviruscontrole te geraken.

Het belang van de Domain Name Service (dns.be)

België heeft in 2009 en 2010 (voor Koobface, de Facebook worm) te maken gekregen met fastflux botnets. Een fastflux botnet gebruikt hetzelfde domeinnaam maar verandert de fysische locatie van de domeinnaam om de zoveel minuten door een dns-actie. Die servers kunnen zich trouwens in verschillende landen bevinden. Voor de politiediensten is dit fenomeen zeer moeilijk te bestrijden in een internationale context.

Gelukkig werd in 2009 een procedure opgestart tussen dns.be en de FCCU.Be waarbij dergelijke .be sites redelijk snel konden downgehaald.

Alleen heeft dit slechts zin indien er ook een preventieve monitoring gebeurt. Volgens onze onderzoeken verklaart DNS.be dat ze dit nu veel sneller opvolgen. Ook daar bleken ze immers nogal geschrokken van een internationaal rapport over de reputatie van domeinextensies waarbij de .be domeinextensie er toen redelijk slecht uitkwam door de late reactie tegen fastflux botnets in 2009. (Meer gedetailleerde gegevens kan je opvragen via www.lsec.be via zoekterm dnsbe.)

<i>network</i>	kwartaal 1	kwartaal 2	kwartaal 3	kwartaal 4
<i>Brutele</i>	41	6	15	19
<i>Mactelecom</i>	79	0	0	1
<i>Teledis</i>	23	0	0	0
<i>Belnet</i>	3	0	0	1
<i>Numericable</i>	3	0	0	0
<i>Scarlet</i>	3	0	0	0
<i>Proximus</i>	0	0	2	0
<i>Combell</i>	0	0	1	0
<i>Telenet</i>	0	0	1	6

(bron : Arbor Networks, maart 2011)

Japan, Duitsland en Australië hebben ondertussen specifieke acties aangekondigd tegen "Command and Control servers" terwijl sommige ISP's geïnfecteerde gebruikers een waarschuwing zullen geven indien ze op 1 van de lijsten van geïnfecteerde werkposten



staan. Sommige antivirusbedrijven hebben ook verleden jaar enkele "Command and Control servers" overgenomen en de lijsten van de verbonden werkposten gedownload, maar het is onduidelijk in hoeverre deze gegevens over soms honderdduizenden pc's doorgegeven werden aan de betrokken CERTs om de betrokkenen te waarschuwen. Er zijn geen verdere acties bekend van de Belgische ISP's in dit verband.

<i>network</i>	quarter 1	quarter 2	quarter 3	quarter 4
<i>Euroaccess</i>	0	6	6	0
<i>ITSS</i>	6	5	5	2
<i>EDPnet</i>	2	2	2	2
<i>Easyhost</i>	1	1	1	1
<i>SCARLET</i>	3	0	0	0

(bron : Arbor Networks, maart 2011)

Het belang van antibotnetdetectie in firewalls, appliances of via managed services

In feite gaat het over een aantal webservers en domeinnamen die hoe dan ook moeten geblokkeerd worden. Dit heeft echter slechts zin indien duidelijk is aangegeven dat een werkstation verbonden is aan een gekend botnet (en dat die lijst uptodate is) want het is slechts op die manier dat de betrokken werkpost uit het netwerk kan worden gehaald voor verdere analyse. Zelfs indien gratis en betalende beveiligingssoftware een groot deel van deze aanvalskode tegenhoudt gebruikt veel van deze gesofistikeerde aanvalskode technieken om niet opgemerkt te worden in standaard werkomgevingen.

Hou er ook rekening mee dat nieuwe botnets gebruik maken van https waarvoor je meestal specifieke bijkomende analysemodules voor nodig hebt. Een bijkomend probleem van het analyseren van https trafiek is dat je ook vertrouwelijke trafiek zult decrypteren en misschien bijhouden.

Voor firma's en organisaties die een hoge veiligheid moeten hebben zijn er specifieke antibotnet producten op de markt die soms kunnen integreren met andere standaard veiligheidsinstallaties.

Het belang van blokkeren van IRC en ICQ en andere specifieke poorten

In een ideale omgeving heeft een werkpost in een netwerk zelf geen directe toegang nodig tot het internet maar kan hij gebruik maken van het internet, email etc.... via interne relayservers die een zekere filtering kunnen invoeren. In elk geval dient men de toegang tot het internet via IRC, ICQ, telnet en andere specifieke poorten af te sluiten. De meeste oude en sommige nieuwe botnets gebruiken nog steeds deze poorten wat je toelaat om het volume aan op te volgen trafiek sterk te verminderen.

6. DLL injection laat je nieuwe functies toevoegen aan een programma

Er zijn twee verschillende soorten vulnerabilities waarvoor exploits kunnen worden geschreven die vervolgens toelaten om een machine over te nemen of om de machine



bepaalde transacties te laten uitvoeren.

De ene zijn de vulnerabilities die voorkomen door specifieke fouten, die met een specifieke patch kunnen worden opgelost waarna het probleem is opgelost en men zich op de volgende 100 fouten kan concentreren.

Het andere type van vulnerabilities zijn de structurele of logische fouten waardoor men door het foutief toepassen van een programmeerfunctie of installatie van een protocol te maken krijgt met een structurele fout waardoor niet alleen de machines absoluut moeten worden gepatched maar waardoor de fout ook moet worden opgelost in duizenden andere programma's en installaties. De DLL injection is een zware functionele bug die kan uitgroeien tot een groot probleem.

De ontdekking in 2010 leidde niet alleen tot een serie belangrijke patches maar tevens tot het opstellen van lijsten met kwetsbare software.

Volgens de voorschriften van Microsoft op het vlak van Secure Development Lifecycle dient men duidelijk goed te definiëren waar de verschillende onderdelen van een programma op de computer worden geïnstalleerd. Microsoft zegt dat het beter is om die volledig te definiëren terwijl sommige programmeurs het zichzelf gemakkelijk wilden maken door dit op een dynamische manier te doen waardoor de computer op zoek moet gaan naar dat bepaalde onderdeel.

De aanval bestaat erin om aanvalscodes met dezelfde naam in een folder te installeren zodat het programma die aanvalscodes gebruikt in plaats de normale code (die elders op de computer staat). Deze aanval kan enkel worden uitgevoerd bij een dynamische plaatsbepaling van de onderdelen van het programma. Indien je weet dat sommige programma's bestaan uit tientallen of honderden onderdelen heb je een idee van het werk dat programmeurs hebben als ze niet van in het begin de richtlijnen van de "Secure Development Lifecycle" hebben gevolgd. Er is een gouden regel dat bugs en veiligheidsproblemen 80% minder kosten om op te lossen indien men "Secure Software Development" principes toepast..

Ondanks het feit dat er geen duizenden aanvallen tegen alle soorten programma's werden ontdekt is het een nieuw lek dat zonder enige twijfel gebruikt zal worden in doelgerichte aanvallen. Het is tevens zo dat een programma dat dergelijke lekken bevat de aandacht zal trekken van schrijvers van malware omdat ze niet alleen een plaats hebben gevonden waar ze code ongemerkt kunnen toevoegen maar tevens een indicatie kregen dat de code waarschijnlijk niet voldoet aan de huidige kwaliteitsvereisten en dus waarschijnlijk meer fouten en veiligheidslekken bevat.

Het belang van updateprogramma's en patches voor alle software op de werkposten

Het behoud van veilige omgevingen, beginnende bij de werkposten zal betekenen dat voor alle belangrijke (en minder belangrijke) programma's op de pc een patch- en updatemechanisme moet voorzien worden. In kleine netwerken kan je dat doen via de automatische updates van de afzonderlijke programma's maar in grotere netwerken zal je best zoeken naar een gecentraliseerde oplossing die zorgt dat alle drivers en programma's tijdig deze belangrijke updates krijgen.

Indien dit gekoppeld is aan een whitelisting van de programma's die mogen geïnstalleerd worden op een werkpost kan je zelfs voorzien dat enkel werkposten waarvan de belangrijkste programma's die gebruikt worden tijdens internetzessies altijd uptodate zijn



(vb browser, flash, pdf,) vooraleer ze toegang krijgen tot het internet. Dat hun antivirus en algemene patching ook moet in orde zijn spreekt vanzelf.

Het belang van kwaliteitscontrole van de eigen software

Amerikaanse overheden schrijven momenteel steeds vaker in hun marktbestedingen dat de geleverde software geen fouten mag bevatten die vermeld staan in de OWASP 25. Deze 25 zware fouten in de programmering zijn immers verantwoordelijk voor meer dan 90% van de aanvallen. Indien een programma of software hieraan voldoet worden al deze geautomatiseerde aanvallen afgeslaan.

Andere marktbevestigingen vereisen dat de code voldoet aan de Secure Development Lifecycle of een andere Best of Practices. Het is trouwens goed om te voorzien dat deze nadien worden getest. Hiervoor bestaan trouwens voldoende gratis oplossingen.

Het belang van het updateproces en een veiligheidsinformatiesysteem voor de eigen software

Indien je zelf software maakt is het noodzakelijk dat je voorziet in een automatische updateprocedure waarbij de gebruiker op een simpele manier zijn software kan of moet updaten.

Als voorbeeld hanteren wij het voorstel van Firefox, waarbij het hele updateproces geautomatiseerd verloopt bij het opstarten. Firefox zorgt automatisch ook voor het uitschakelen en updaten van niet-compatibele extensies.

Het belang van communicatie

Dit zorgt voor de nodige frustraties bij gebruikers en dat is niet meer dan begrijpelijk. Het is daarom ook belangrijk om de gebruikers en collega's te informeren over mogelijke updates van zodra ze er staan aan te komen.

Een veiligheidscommunicatie op de website van je software-ontwikkelingswebsite - al dan niet enkel voor klanten - is de beste manier om klanten, partners en anderen op de hoogte te houden van patches, workarounds, mogelijke aanvallen en best-of-practices. Het is normaal dat elke belangrijke software die in België wordt ontwikkeld en verspreid over deze informatieplatformen beschikt voor haar gebruikers. De beste firewall is hoe dan ook steeds de geïnformeerde gebruiker.

7. De onveilige website als uitnodiging voor spammers en hackers

Elk jaar worden er honderdduizenden websites gehacked in Europa, België en daarbuiten. Dit aantal is in 2010 jaar aanzienlijk toegenomen.

Veiligheid van de websites wordt nog belangrijker omdat steeds meer malwareverdelers gebruik maken van links en scripts die ze aan populaire sites toevoegen om hun bezoekers te infecteren. In 2010 was het belangrijkste geval de toevoeging van dergelijke code aan de websites van Humo, Flair en enkele andere websites van die persgroep. Ze waren het slachtoffer geworden van "scriptinjection" waardoor de gebruikers konden worden afgeleid naar een gevaarlijke website of er downloads van konden krijgen in de background. Na de publicatie van deze informatie op de Belsec blog en overleg met de technisch verantwoordelijken werden de nodige maatregelen genomen om herhaling te voorkomen.



Indien men het advies vanuit het overzicht van de OWASP25 had gevolgd had dit vermeden kunnen worden.

Het grootste probleem zijn de duizenden vergeten websites die nog steeds interactieve functies hebben zoals een forum, chat of muur maar waar men ook vergeten is om ze af te sluiten, te controleren of te kuisen.. Dit is zelfs het geval voor bepaalde overheidssites. Het gevolg is dat deze websites een slechte internetreputatie kunnen krijgen en kunnen geblokkeerd worden (zelfs door Google). Een ander gevolg is dat men helpt malwaresites hogere plaatsen te krijgen in de Googleresultaten door de links die naar hun infecterende sites werden geplaatst en dat men in het slechtste geval bezoekers infecteert of doorstuurt naar malwaresites.

Een specifieke vorm van scriptaanval tegen bezoekers van gewone websites in het infecteren van de banners en publiciteit die op deze websites verschijnt (malvertising). Soms was het zelfs geen misbruikte publiciteit maar ze was aangekocht door de malwareverdelers.

Men dient er tevens rekening mee te houden dat de Belgische jurisprudentie op het vlak van het hosten van bepaalde links waartegen klacht wordt neergelegd nog in volle evolutie is en tot nu toe een zekere verantwoordelijkheid bij de eigenaar van de website kan leggen. Dit is zeker het geval als er sprake is van een gebrek aan toezicht en voorzichtigheid en zeker indien men niet reageert op klachten. Zorg dus steeds dat je WHOIS informatie juist is.

Het belang van het overwegen van de interactieve functionaliteiten van de websites (bloggen, fora, databases raadplegen, cms...)

Men moet overwegen welke interactieve functies men nodig heeft en hoe men het toezicht zelf of via gespecialiseerde firma's zal laten verlopen. Een forum heeft slechts een meerwaarde voor de website indien het er veilig en aangenaam vertoeven is. Indien dit niet het geval is, zijn er niet alleen risico's voor de bezoekers en de eigen website en netwerken maar zal het tevens een negatieve invloed hebben op de online reputatie.

Het belang van de controles op veiligheid en kwaliteit voor de lancering.

Dit maakt het goedkoper en gemakkelijker later om de site te upgraden, uit te breiden, over te plaatsen of te integreren en de nodige bijkomende beschermingen in te bouwen. Het is daarom ook nodig dat er over het project de nodige documentatie, bugcontrole en een library van veilige hoogstaande code bestaat.

Het belang van noodzakelijke logging en monitoring

In de eerste plaats is dit de logging en de controle van de beschikbaarheid. Met de contentcontrole kan wijzigingen in forums of gehackte pagina's direct gemeld krijgen. Er bestaan ook producten die regelmatig nieuwe aanvalscodes automatisch lanceren om na te gaan of de veiligheid van de site nog altijd voldoende is in de steeds onveiligere wordende omgeving.

Het belang van eenvoud in gebruik reflecteert in eenvoud in onderhoud



1. Hoe minder websites men dient te beheren, hoe minder mogelijke risico's zich kunnen voordoen
2. Hoe eenvoudiger de website, hoe minder risico's
3. Hoe moeilijker het webproject is, hoe beter het is dat je het overlaat aan gespecialiseerde dienstverleners
4. Ga er niet van uit dat uw host of ISP het allemaal wel doet voor u. Controleer zelf en vraag desnoods om de nodige aanpassingen uit te voeren, zodat u uw verantwoordelijkheid heeft opgenomen

8. Uw website is gehacked en u staat dus even voor aap

Verantwoordelijken voor websites binnen een organisatie en de personen die de ontwikkeling doen zijn meestal niet altijd bezig met de veiligheid van zowel de code als de processen en laten vaak hun beslissingen (gelukkig) in de eerste plaats leiden door vormgeving, functionaliteit en beschikbare middelen, maar vergeten (ongelukkig) te vaak om stil te staan bij de mogelijke veiligheidsrisico's waarmee een website vandaag en in de toekomst zou kunnen te maken krijgen.

Websites op het internet zullen hoe dan ook gescand en eventueel aangevallen worden en indien je als website al een paar keer bent aangevallen dan zal je zeker opnieuw worden aangevallen - het is alsof je in een favorietenlijst bent terechtgekomen die hackers onder elkaar uitwisselen. Het is dan ook verbazend om op te merken dat sommige websites toch keer op keer opnieuw worden gehacked zonder dat men de benodigde afdoende maatregelen neemt.

In het kader van de wet op de cybercriminaliteit kan er worden overwogen dat infrastructuur die herhaaldelijk gehacked wordt een gevaar betekent voor de rest van het Belgische netwerk en dus eerst opnieuw in orde moet worden gebracht vooraleer ze terug op het netwerk wordt aangesloten. Dit is zeker het geval bij gehackte ecommercesites waarvan het soms verwonderlijk is dat niemand zich totnogtoe zorgen heeft gemaakt over verlies van persoonsgegevens.

Het belang van een lokale professionele ISP, en host of cloud service (minstens voor uw meest bedrijfskritische onderdelen)

Sommige Cloudservices garanderen sinds kort een Europese hosting. Zo kunnen ze een antwoord bieden aan lokale Europese reglementering die dat vereist (Duitse of Luxemburgse privacyreglementering, ...). Het is ook belangrijk om de jurisdictie onder Belgische wetgeving te laten resorteren. Vraag uw hoster ook naar backup, antivirus en firewall voor uw website en de beveiliging van hun platformen en netwerken.

Eventueel het belang van eigen servers

Indien u kiest voor het goedkopere shared hosting dan moet u zeker zijn dat de beveiliging geïndividualiseerd is en dat niet iedereen totale toegang heeft tot de server en het volledige ontwikkelingsplatform. Het is enkel op dedicated hosting dat u de enige bent die toegang heeft tot het management van uw server en webdiensten. Met de huidige vormen van virtualisatie kan er natuurlijk heel snel worden gewisseld tussen servers of zelfs tussen verschillende netwerken, met behoud van de dedicated "virtual server".



Het belang van professionele software en programmeurs

Het is noodzakelijk dat de software die u gebruikt u snel de nodige veiligheidsupgrades kan leveren en dat de programmeurs alle Best of Practices van veilig programmeren en van die bepaalde software kennen. Verwacht ook niet dat 1 programmeur alle verschillende soorten software even goed kent maar zoek voor grote projecten eerder naar een team van verschillende specialisten. Sommige gratis softwarepakketten hebben (nog) niet de noodzakelijke professionaliteit. Men kan soms kiezen voor een professioneel pakket van een gratis software die betalend is en wel de nodige professionele dienstverlening heeft.

Het belang van een incidentprocedure, veiligheidsprofessionals en "don't touch"

Indien u dus de logs en monitoring hebt opgezet, gekozen hebt voor een professionele hoster in België en gebruik maakt van professionele programmeurs dan is dit normaal gezien redelijk eenvoudig. Indien het onvermijdelijke dan toch gebeurt, en u een incident hebt vastgesteld dient u in de eerste plaats de Federale Politie dienst FCCU te contacteren.

Laat de situatie in de staat waarin ze zich op dat moment bevindt, of vraag om professionele begeleiding van het informatiebeveiligingsincident. Alle mogelijke interventies door iemand anders dan de FCCU kunnen het incident compromitteren en de bewijslast onbruikbaar maken.

Desgewenst overhandigt u de politie de logs, voorziet u een redundante oplossing met uw gebruikelijke hoster als noodoplossing en maakt u gebruik van de last "clean copy" die u op een andere plaats hebt bijgehouden. U hebt tevens een interne procedure die bepaalt wie wat wanneer moet doen. Handig is te beschikken over een 'standby' fonds en autoriteit om dringende uitgaven te kunnen doen zodat uw website zo snel mogelijk weer online is.

Het belang van een plan voor een permanente patch- en upgradepolitiek van uw software en hardware

Hoe langer u op verouderde hardware of servers blijft en hoe langer u gebruik maakt van steeds sneller verouderende software of de nodige securitypatches vergeet hoe groter het risico wordt voor uw website. Hoe sneller u op de nieuwe stabiele versie van een nieuwe hardware of serveromgeving bent, hoe sneller u het risico vermindert. Regelmatige vergaderingen tussen de veiligheidsverantwoordelijken en de projectmanagers is een minimumvereiste.

9. Conficker of het bewijs dat je (nog) niet op je ISP moet rekenen

Eén van de belangrijkste discussies de afgelopen jaren en die ook verleden jaar in alle hevigheid toenam gaat over de rol van de ISP's in de beveiliging en monitoring van de malware.

Zonder in detail te willen ingaan op de langlopende discussie tussen verschillende partijen, waarbij meerdere belangen moeten afgewogen worden, en er uiteraard ook heel wat economische elementen meespelen, is het zinvol te weten dat ook in België de ISP's in België een zekere verantwoordelijkheid dragen voor het beschermen van de individuele computers van hun gebruikers.



Eindgebruikers en bedrijven worden nog steeds aangespoord om betrouwbare anti-virus, anti-malware, ... software te installeren, alvorens bijvoorbeeld bepaalde diensten te raadplegen. Een heleboel pakketten bieden vandaag ook andere functionaliteiten zoals white lists van websites, of bescherming van gegevens door hard disk encryptie. Microsoft biedt ook een zinvol gratis alternatief.

Het belang van netwerk- of installatie- beveiliging

Een installatie zonder antivirus, of firewall is zoals een auto zonder remmen. Een netwerk zonder centrale beveiliging (firewall, proxy, antivirus) is zoals een middeleeuwse burcht zonder fortificatie.

Bescherming dient op alle lagen, op alle componenten voorzien te worden (netwerk, server, werkpost) want dit biedt de beste garantie op een stabiel en veilig netwerk.

Het belang van encryptie van het gegevensverkeer

Omdat het internet zo open is en omdat er momenteel een veralgemeende situatie van totale onveiligheid heerst dient u uw belangrijke internettrafiek te encrypteren via een VPN, reverse proxy, SSL trafiek en dergelijke. Dit is is niet altijd perfect maar het biedt een bijkomende bescherming.

10.De informatie over informatiebeveiliging is erg gefragmenteerd en complex

Er bestaan verschillende online informatiebronnen die veiligheidsverantwoordelijken zouden moeten opvolgen, afhankelijk van hun gebruikte infrastructuur en het type transacties. Het is echter een enorme jungle met heel veel soms tegenstrijdige berichten. Een goede keuze van professionele informatie is daarom zeer belangrijk om snel en gericht te kunnen de juiste maatregelen nemen zonder te dramatiseren of te onderschatten.

Veiligheidsverantwoordelijken hebben gelukkig ook andere dingen te doen, en daarom zijn er ook verschillende diensten die hen kunnen ondersteunen met gepersonaliseerde beveiligingsinformatie.

Enkele belangrijke bronnen : Internet Storm center (<http://isc.sans.org>), berichten van uw softwareleveranciers over updates en patches. In een aantal landen nemen WARPS deze functie waar naar kleinere bedrijven en instellingen die niet over voldoende middelen beschikken om dit allemaal zelf te doen of waarvoor de externe diensten te uitgebreid zijn.

Het belang om zichzelf te informeren gebaseerd op verschillende bronnen

U zult echter merken dat er verschillende incidenten op een jaar plaatsgrijpen die meer aandacht vereisen en die soms zelfs hele concepten en frameworks weer in vraag stellen of een zekere bijsturing vereisen. U kunt zich hiervoor zelden op 1 bron baseren en zult hiervoor de tijd moeten uittrekken om 'wijd en in de diepte' te lezen. Sommige diensten stellen dergelijke nota's tegen betaling voor.



Soms zal u misschien tegenstrijdig advies krijgen om bijvoorbeeld een patch al dan niet te installeren, laat u daarom bijstaan door professionele expertise.

Het is in hetzelfde oogpunt ook zeer goed indien u regelmatig de nodige investeringen in knowledge management doet zoals opleidingen, boeken en beurzen of conferenties.

3. Vooruitzichten in 2011

1. Mobiele risico's

Mobiele risico's, in de eerste plaats via handhelds (mobiele telefoons, PDA's, smartphones, ...), maar in toenemende mate via andere devices (i- en andere pads, mp3- en mp4-spelers, ...) worden een steeds belangrijker uitdaging voor de veiligheidsverantwoordelijken. Enerzijds zijn er de uitdagingen van mobiele malware, dat steeds vaker voorkomt. Maar de mobiele toestellen vormen ook een bedreiging voor de rest van de organisatie: ze kunnen worden gebruikt als toegangsmiddel voor afluisteren, er kunnen foto's en filmopnames mee worden gemaakt, er kunnen bedrijfsgegevens worden mee vervoerd, ze bevatten soms bedrijfskritische en confidentiële emails, belangrijke contactbestanden, ...

Er is een belangrijke rol weggelegd voor de operatoren omdat de Belgische CERT vandaag niet verantwoordelijk is en ook niet is uitgerust om deze mobiele bedreigingen efficiënt en massaal op te volgen.

2. De krakende encryptie

De goeie manier ter bescherming van gegevens en belangrijke informatie zoals paswoorden, persoonsgegevens, documenten, gegevensdragers en transmissie is encryptie. Het is dan ook logisch dat men zal proberen om encryptie te doorbreken of te omzeilen. Dit betekent dat onze encryptiemethodes regelmatig moeten geëvalueerd worden, en indien nodig moeten verzaamd worden. Er moet ook rekening worden gehouden met de rest van de omgeving. Een totale encryptie gebeurt over de hele workflow, zelfs voor de backup en de archivering.

3. meer hardware aanvallen

In de loop van het jaar zal men steeds meer rekening moeten houden met de risico's van de toestellen zelf. Er worden immers ook minder geavanceerde toestellen in de omgeving gebracht, zoals printers en telefooncentrales die voorzien zijn van webserver en andere toegangen. Vaak worden ze over het hoofd gezien, en vormen ze een vorm van bedreiging. Er wordt ook verwacht dat steeds meer pogingen zullen worden ondernomen om op een specifieke hardwarematige beveiligde omgevingen aan te vallen. Dit kan gaan van gerichte acties tegen drivers, de poorten, de protocollen tot het toevoegen van volledig verborgen geïnfecteerde hardware. De complexiteit van dit soort aanvallen zal het noodzakelijk maken om ook het toezicht op deze mogelijke bedreigingen te automatiseren.

4. Security as a Service, Virtualisatie, professionele virusaanvallen en sandboxing

Voor strikt beveiligde omgevingen zal het steeds meer van belang worden om met een ingewikkeld systeem van controlelagen te werken en om zoveel mogelijk alle inhoud van



het internet van de werkposten te houden en enkel in een afgesloten externe hardware-omgeving ter beschikking te stellen. Dat kan bijvoorbeeld door middel van "sandbox" technologie, of virtualisatie op de computer zelf of in het netwerk.

In vele gevallen is het nog in een vroeg stadium, maar omgevingen in de cloud kunnen een oplossing bieden waardoor men de informatie, documenten en gegevens van op het internet kan controleren vooraleer het op het netwerk of de werkstations terecht komt. Meer aandacht dient besteed te worden aan email attachments zoals Adobe Acrobat PDF documenten, die verschillende activiteiten kunnen lanceren op het werkstation. Malwarelists en analysetechnologiën zullen toelaten om bepaalde omgevingen of computers een grotere veiligheid te garanderen.

5. Data Breach Notification : meldplicht in Europa komt er aan

In november 2010 werd een voorstel voor aanpassing van de Europese privacy richtlijn voorgesteld. De bedoeling is om binnen de lidstaten een verplichtte meldplicht in te richten bij het verlies van persoonsgegevens. Bedrijven en instellingen zullen moeten beschikken over een gegevensbeschermingsofficier, terwijl privacycommissies in de verschillende landen beter op mekaar afgestemd zouden worden. Voor de burgers zal niet alleen de mogelijkheid moeten bestaan om hun gegevens uit de gegevensbanken van bedrijven en instellingen, maar ook om de historiek te laten verwijderen. De Commissie onderzoekt ernstig de mogelijkheid om de controle-instellingen zoals in het Verenigd Koninkrijk hoge administratieve boetes te laten opleggen. Bedrijven zullen op basis van externe audits moeten kunnen aantonen dat ze conform zijn met deze regelgeving.

4. Enkele Belgische indicatoren

Naast de internationale activiteiten en acties voor meer veiligheid op het Belgische internet, vonden er ook enkele lokale acties hierover plaats. Ondanks het feit dat het vooral infrastructurele acties waren, zijn ze zeker het waard te vermelden omdat ze een invloed hebben gehad op de Belgische positie van informatiebeveiliging in een internationale context.

1. invloed van de preventieve acties van dns.be *

In 2010 werden door dns.be:

- 22 .be websites preventief geblokkeerd zodat ze niet meer konden worden opgezocht
- 2 .be websites werden geblokkeerd op basis van een bevelschrift
- 177 registraties van .be websites werden aangemaand om hun whois in orde te brengen, d.w.z. de juiste en volledige contactgegevens op te geven. Indien de eigenaren dit niet deden, werden de domeinnamen in quarantaine geplaatst.

Het belang van een preventief – pro-actief beleid

Naar aanleiding van het misbruik van .be websites in 2009 werd beslist om preventief een controle uit te voeren of de domeinnamen phishingnamen bevatten (vb ebayy.be of citiibank.be) of totaal irrelevante domeinnamen waren zoals de aanvalssites (meestal een opvolging van cijfers en letters zonder enige betekenis). Men wou immers ten alle koste



vermijden dat het .be domeinnaam opnieuw zou kunnen worden misbruikt voor dergelijke oprichtings- en aanvalsacties.

Een van de resultaten van de acties is dat de referentiewebsite <http://www.abuse.ch> meldt dat in 2010 geen fastflux .be domeinnamen voorkwamen

Waakzaamheid geboden

Nadeel is natuurlijk dat het .be domein internationaal wordt aangeboden als een domeinextensie, en dus gemakkelijk kan worden misbruikt.

2. Nog nooit werden zoveel .be websites gehacked-gedefaced

Volgens website zone-h.org werden er in 2010 16.134 .be website gehackt, een bijna verdrievoudiging van het aantal in 2007. Vooral in november 2010 (3.989) en december 2010 (2.245) werden telkens samen bijna evenveel sites gehackt als het volledige voorgaande jaar.

Het belang van de gegevens

De gegevens van zone-h.org zijn de oudste maar volgens onze onderzoekers ook de meest volledige. Ze bevatten ook niet alle hacks omdat ze gebaseerd zijn op de vrijwillige meldingen van de verschillende hackers die er een wedstrijdje van maken om zo hoog mogelijk in de rangorde te komen. Merendeel van de hacks blijven immers niet lang online en dus is dit het belangrijkste archief van de 'verwezenlijkingen'.

Er bestaan ondertussen wel een aantal bijkomende specifieke archieven (van turkse hackers, arabische hackers, etc...) waar rekening mee moet worden gehouden en soms wordt zone-h of één van haar varianten tijdelijk of permanent van het net geduwd of gehacked zodat meldingen moeilijker zijn. De gegevens zijn dan ook niet meer dan een indicatie, maar wel een indicatie die een goede polsslag is van het hackingwereldje op het internet.

Het belang van hacking statistieken

- nog nooit werden zoveel websites gehacked als in 2010, het cijfer van het **miljoen** werd ruim overschreden
- nog nooit werden zoveel **linux** servers gehacked (meer dan een miljoen, tegenover een 200.000 windows) en dus werden nog nooit zoveel Apache servers gehacked
- het werd de aanvallers gemakkelijk gemaakt door het open source programma **OScommerce** die een belangrijk lek gedurende maanden niet dichtte (terwijl het nochtans gebruikt werd door ecommerce sites) en een veiligheidslek in de kernel van Linux die sinds 2008 bestaat maar op duizenden webserveren nog altijd niet volledig gedicht werd.
- voor wat betreft de **windowsservers** is het trouwens belangrijk om te onderlijnen dat vooral **oudere webserveren** werden gehacked (10 keer minder een IIS 7 dan een IIS 6) of oudere OS (tien keer minder 2008 tegenover 2003 servers).



- De **geautomatiseerde massale aanvallen** zijn 6 keer belangrijker (1.200.000) dan de specifieke aanvallen waarbij 1 aanvaller 1 website onderuit haalt (200.000).

Onze onderzoekers stelden ook vast dat enkele grotere serverparken werden gehacked, waarbij enkele honderden .be websites het slachtoffer werden.

Een fout, onzorgvuldigheid van een hoster of een websitebeheerder kan als gevolg hebben dat men alle servers of gehoste websites heeft kunnen aanpassen zodat honderden websites het slachtoffer werden van dezelfde hackaanval.

3. De invloed van de interventies van het CERT.Be in 2010 (bron CERT.BE)

De Belgische CERT is begin 2010 effectief van start gegaan. Met beperkte middelen en doelstellingen, maar met enorme resultaten. In 2009 was België in de risico-index van Arbor Networks (een belangrijke internationale netwerkbeveiligingsfirma) regelmatig in de wereld top5 van meest onveilige netwerken. In 2010 is het algemene risico voor de Belgische netwerken sterk verminderd in de indicatoren van Arbor Networks en bevinden we ons bijna permanent tussen de 30e en de 40e plaats wereldwijd. Dit betekent dat door het behandelen van de incidenten en het preventief verwittigen van netwerkbeheerders het aantal incidenten en het gevaar van deze incidenten sterk verminderd werd.

Onze onderzoekers bekwamen van CERT.be de volgende gegevens voor 2010 :

- in totaal behandelden de 6 personen van de CERT.be 2135 incidenten in 2010 waarvan 1389 incidenten verder moesten onderzocht worden en waarvan 976 incidenten ernstig waren.
- een derde van de incidenten waren pogingen om accounts te stelen
- een vierde van de incidenten waren geïnfecteerde systemen of netwerken

Het is echter nodig om nu naar een tweede fase te gaan en van elk netwerk en van elke gebruiker op het Belgische internet de eerste antivirus en firewall te maken door te zorgen dat hij de nodige informatie heeft en beschikbare technische middelen om zichzelf en eventueel het netwerk en de installaties te beschermen en eventuele preventieve maatregelen te nemen voor bestaan en opkomende onveiligheidsfenomenen in België.

Een volgende fase moet er een zijn van voorlichting en het verduidelijken van een publieke strategie voor informatiebeveiliging.

•

5. .be websites die virussen installeren volgens malwaredomainlist.com

(voor de volledige lijst : bezoek www.lsec.be met zoekterm malware domain be)

Het groeiend aantal websites vergt een gecoördineerde aanpak van dns.be, eventueel respectievelijke hosters, en van de politiediensten om snellere acties te ondernemen. Het overgrote deel van deze aanvalssites met een .be domeinnaam worden immers niet in België gehost.



6. .be Phishingsites 2010 in Phishtank.com voor enkele Belgische netwerken

(voor de volledige lijst : bezoek www.lsec.be met zoekterm phishing domain be)

Onze onderzoekers stelden vast dat indien een site na een hack haar veiligheid niet in orde bracht, ze niet lang daarna opnieuw zal worden gehacked.

Het systeem werpt de vraag op voor een degelijke benadering van de problematiek en de noodzaak voor een protocol voor het onmiddellijk verwijderen van dergelijk sites. De sites zouden best pas weer online worden gezet nadat - de nodige acties werden ondernomen ter verbetering van de beveiliging van de sites.

7. 2500 Belgische IP adressen met Conficker (2008) (Shadowserver.org)

Volgens de organisatie shadowserver.org die de cijfers beheerd voor de 'International Conficker working Group' werden volgende meldingen van het conficker virus opgemeten in België.

Netwerk	All IP addresses	Unique Conficker IPs
Telenet N.V.	1,867,406	1,667
KPN Belgium Business NV	1,054,930	385
Brutele SC	786,292	332
be.mobistar	366,574	195
MAC Blue Tower,	32,766	87
EDPNET	80,364	64
schedom	59,378	19
WIN	20,476	17
Gateway Communications	19,656	15
Alpha Networks S.P.R.L.	8,190	11

(bron : shadowserver.org, maart 2011)

De laatste maanden verandert er weinig aan deze cijfers. Het aantal daalt maar veel te langzaam terwijl het toch gaat om veiligheidspatches die sinds 2008 hadden moeten geïnstalleerd zijn. De internationale 'Conficker Working Group' is erin geslaagd om de centrale infrastructuur van het virus over te nemen en alle binnenkomende communicatie van geïnfecteerde pc's te onderscheppen en te organiseren.

Het getal is in elk geval een grote verbetering tegenover het vorige jaar. Begin 2010 waren in totaal zo'n 5777 IP adressen nog geïnfecteerd met dit virus uit 2008 volgens shadowserver.org dat het onderzoek van de 'International Conficker Working Group'



bijhoudt. Een vernieuwde inspanning is dus beter dan te wachten op de mogelijke upgrade van de computers naar windows7 door de eigenaren.

5. enkele opmerkingen

Dit rapport bevat exclusieve gegevens over de internetonveiligheid en -beveiliging in België zonder volledig te willen (of kunnen) zijn.

1. We concentreren ons op het .be domein-extensie omdat het belangrijk is dat we er een zeer veilige domeinextensie van maken waar het safeto.be is.

Het is duidelijk dat dns.be sinds de incidenten in 2009 een aantal belangrijke preventieve maatregelen en controles heeft genomen die haar effect niet hebben gemist. Een 'fast response' door een geïntegreerde aanpak van het gerecht, FCCU en DNS.be blijft nodig om te vermijden dat .be domeinen elders in de wereld gemakkelijk zouden kunnen misbruikt worden als we het Belgische internet beter blijven beveiligen.

2. Uit andere exclusieve gegevens blijkt duidelijk dat de internetonveiligheid in België op een dramatische manier structureel is verbeterd sinds België een CERT heeft opgericht. Op een jaar tijd is de algemene onveiligheidsindex van Arbor Networks voor België 10 maal verbeterd. Daar waar in 2009 het Belgische internet regelmatig het vierde meest onveilige netwerk was in de wereld is dit in 2010 helemaal niet meer het geval. Het feit dat de CERT in 2010 meer dan 1000 belangrijke veiligheidsincidenten heeft behandeld heeft daar zeker aan bijgedragen. Een permanente versterking van de CERT en een uitbreiding van haar bevoegdheden moet dan ook een prioriteit blijven.

3. Nog nooit werden zoveel .be websites gehacked als in 2010. Dit is zowel te wijten aan een grotere onveiligheid van open source software als het massaal gebruik van shared hosting zonder de nodige individuele beveiliging van de websites. Indien men in 2011 hier een even belangrijk verschil zou willen maken als dns.be en de CERT in 2010 dan is de hosting en website-industrie een uitstekende kandidaat om in 2011 de nodige maatregelen en initiatieven te nemen om deze situatie alvast in België radikaal te beperken.

4. 2500 PC's in België zijn nog steeds geïnfecteerd met het Conficker virus uit 2008. Een gecoördineerde actie door de ISP's (Belgacom en Telenet) kan deze laatste restanten van dit eenvoudig te manipuleren veiligheidsgat doen verdwijnen van het Belgische internet. Dit betekent niet automatisch dat de gebruikers zullen extra moeten betalen.

5. In het algemeen hebben we in België slechts te maken met veiligheidsproblemen van een beperkte omvang waar we met een beperkte bijkomende inspanning direct en structureel op kunnen reageren. Een "synthese van alle Belgische Itsecurity indicatoren zal vb de netwerkbeheerders de mogelijkheid geven om beter te reageren op aanvallen tegen belangrijke infrastructuur en datacentra. Dit is nodig aangezien we het gastland zijn voor een enorm aantal belangrijke Europese, internationale en militaire organisaties.

Het aantal DDOS aanvallen tegen Belgische infrastructuur in 2010 bewijzen de noodzaak

<i>quarter report</i>	Number of DDOS	Max GBPS	Max PPS
-----------------------	-----------------------	-----------------	----------------



1	225	1.90	1.65
2	161	6.33	18.58
3	446	8.56	6.13
4	179	24.96	5.28

(bron : Arbor Networks, maart 2011)



6. aanbevelingen voor een beter informatiebeveiligingsbeleid

4.1 oprichting van een informatiebeveiligingsstructuur voor België, dat normen en voorwaarden kan opstellen voor haar infrastructuur en bedrijven

Door het vastleggen van veiligheidsvoorwaarden op het vlak van de kwaliteit van de code, de documentatie en opvolging van een informaticaproject of het opzetten, hosten en opvolgen van interactieve online diensten kan de overheid een markt ondersteunen van kwalitatieve veilige IT-diensten waardoor dit de norm wordt.

Een eerste stap is het pro-actief implementeren van een gegevensbeschermingsbeleid, met een meldingsplicht, alsook bepaalde normen voor hosters en .be dienstverleners.

4.2 De industrie kan zelf reguleren en een eigen certificatie opstellen

ISP's en hosters kunnen in samenwerking met bedrijfsfederaties overgaan tot vormen van zelfregulering om sneller te kunnen reageren op de internationale normen en mogelijke destructieve gevolgen van verkeerde acties. Een hoster zou moeten voldoen aan een aantal voorwaarden om één, twee of drie sterren te krijgen waardoor men een gedifferentieerde en duidelijke dienstverlening zal krijgen. Het zal tevens mogelijk zijn om in markten te bepalen of een website een hosting met één, twee of drie sterren moet gebruiken. Een externe audit en incidentmonitoring zal dit dynamisch houden.

4.3 Verdere versterking van de CERT.be met een betere samenwerking met de FCCU.be en andere initiatieven

Zelfs voor Belgische bedrijven, of zelfs experts in de informatiebeveiliging is het niet altijd transparant waar men terecht moet of kan voor welk probleem. Een verduidelijking en een algemeen meldportaal met de uitleg en een online klachtenformulier kan helpen. Naar analogie met dit dossier zou er jaarlijks een gezamenlijke Belgisch informatiebeveiligingsevaluatie moeten worden opgesteld, als een samenwerking tussen overheid, bedrijven en experts.

De lokale waarschuwings- en rapporteringsdienst (WARP) voor kleine bedrijven en instellingen kan dit in samenwerking met de CERT coördineren, filteren en optimaliseren.

4.4 ISP's vormen een onderdeel van de kritische infrastructuren, een gecoördineerd beleid is nodig

De ISP's doen momenteel in België al veel meer en sturen dit regelmatig nog bij, maar met de toename van het internetgebruik en van de complexiteit van de massale aanvallen tegen de gebruikers is het geen overbodige luxe om geïnfecteerde posten op hun netwerk beter te informeren over de gratis beveiligingsmaatregelen die ze kunnen nemen. Deze geïnfecteerde posten zijn immers de zwakste link van de veiligheid van hun netwerk – zelfs als men rond het netwerk zeer dure veiligheidsapparatuur heeft.

De overheid dient een gecoördineerd plan te realiseren waarbij wordt rekening gehouden met mogelijke risico's op kritische infrastructuren, waaronder ook ISP's. Cyberaanvallen kunnen resulteren in belangrijke milieuschade, en mensen in gevaar brengen maar zullen vooral economische schade aanrichten... Buurlanden zoals Frankrijk, Duitsland, Nederland



en het Verenigd Koninkrijk beschikken vandaag reeds over een strategisch cyberdefensieplan en gecoördineerde acties tegen cybercriminaliteit. België, als gastland van de Europese instellingen en de NATO blijft momenteel achter.

4.5. verbeteren van de wetgeving en noodzaak van betere opleiding

De oprichting van het Centrum voor Cybercriminaliteit wordt ook door de industrie toegejuicht, maar zal zeker niet volstaan om alle aspecten van cybercrime en juridische aspecten te behandelen.

De gestructureerde programma's, gecoördineerde actiedagen, algemene sensibiliseringscampagnes, specifieke gerichte acties en de uitbouw van specifieke en lokale waarschuwingsinfrastructuren blijft nodig.

Vooraf in het kader van bescherming van persoonsgebonden gegevens, zijn snellere acties nodig tegen internationale cybercriminaliteit, België heeft ook standaardnormen voor informatiebeveiliging naar analogie met Europese instellingen, de buurlanden en de Amerikaanse NIST Normen nodig. De Belgische wet op de computercriminaliteit zou best ook van uitvoeringsbesluiten worden voorzien.

