

# IT security tot 2012



**Thanks firewall ... *but we need more***

M. van Eemeren\*

marcelvaneemeren@on2it.net

J. Scheerder\*

jeroenscheerder@on2it.net

14 januari 2008

## Inhoudsopgave

<b>1 Firewall gekraakt</b>	<b>2</b>
<b>2 Verklaard</b>	<b>4</b>
2.1 Hoe werkt een firewall . . . . .	4
2.2 Noodzaak van inhoudelijke scanning . . . . .	4
2.3 Exploits . . . . .	4
2.4 De ernst (maar waarom) . . . . .	5
2.5 Patchen van software . . . . .	5
2.6 Virtual patch . . . . .	6
2.7 Kennis is essentieel . . . . .	7
<b>3 Onion-beveiligingsmodel</b>	<b>8</b>
3.1 Drie stappen voor verbetering . . . . .	9

---

\*ON2IT Security, Waardenburg, The Netherlands.

## 1 Firewall gekraakt

**Waarom kraakt de firewall?** De firewall heeft last van een eigentijds probleem: *groei*. Het verkeer naar, maar ook de verwevenheid met andere netwerken neemt alsmaar toe. Om de groei te realiseren worden steeds meer poorten op de firewall opengezet en worden er steeds weer slimmere, complexere protocollen ontwikkeld. Daarnaast bieden software onvolkomenheden (fouten; bugs) gelegenheid om "moeiteloos" infrastructures binnen te dringen.

Om veilig te kunnen werken is een Next Generation firewall nodig. Die beschikt over verschillende technieken om het verkeer volledig te inspecteren en ongewenste zaken te weren. Deze technieken waren tot voor kort voorbehouden aan grotere organisaties, maar zijn in de Next Generation firewall geïntegreerd.

*"By the end of 2007, 75 percent of enterprises will be infected with undetected, financially motivated malware that evaded their traditional defenses."*

— Gartner: *Gartner Predicts 2007 and Beyond*, #144546

**Achter de deur** Langs de achterdeur van netwerken ("backdoor") worden "insider attacks" uitgevoerd. In feite wordt de firewall vaak op een onschuldige en/of onachtzame wijze moeiteloos gepasseerd. Enkele voorbeelden hiervan zijn:

De intensiteit van netwerkcommunicatie, het aantal verbindingen met vestigingen, telewerkers of "third party" beheerders neemt toe, en dat gaat vaak versleuteld. Dit betekent dat het verkeer niet aan een inspectie kan worden onderworpen.

Laptop, intelligente telefoons en/of PDA gebruikers beschikken veelal over de hoogste rechten. Dit betekent dat zij in principe alles mogen en kunnen. Op deze wijze kan iemand door simpelweg een mooie vakantiebestemming te googelen op besmette websites terecht komen, en zo malicieuze programmatuur meenemen naar de zaak en het gehele bedrijf besmetten.

Met sites als logmein.com of gotomypc.com kan er een versleutelde 'terugverbinding' vanuit thuis naar de PC op het werk worden aangemaakt. Op eenvoudige wijze wordt de firewall gepasseerd.

De meeste netwerken zijn zo ingericht dat iedereen op het netwerk als "trusted" wordt beschouwd. Wat wanneer een gebruiker besluit omwille van de flexibiliteit een draadloos accesspoint mee te nemen naar de zaak om draadloos te werken? In feite kan via iedere willekeurige netwerkaansluiting in het gebouw netwerktoegang worden verkregen. Als gast kan ik zonder meer met simpele gereedschappen verbinding met het Internet maken.

**Te koop** Een eenvoudige oplossing is om de bestaande firewall te vervangen door een geïntegreerde oplossing: de Next Generation firewall. Deze beschikt over verschillende instrumenten die op een innovatieve wijze in harmonie gelijktijdig het verkeer inspecteren en zo malicieuze zaken stoppen voordat de bedrijfscontinuïteit in de knel komt.

Deze geïntegreerde oplossingen zijn te koop bij verschillende fabrikanten, ieder met een verschillende zwaartepunt. De IBM Security Solutions oplossing draait naast Intrusion Prevention om kennis.

Om malicieuze activiteit te voorkomen moet die eerst kunnen worden herkend. IBM ISS is uitvinder van het Intrusion Detection System, dat het verkeer inspecteert met een gepatenteerde Protocol Analysis Module (PAM). Inmiddels worden meer dan 170 protocollen volledig gedecodeerd. Dit Intrusion Detection System is met het toevoegen van tegenmaatregelen geëvolueerd tot een Intrusion Prevention System dat op basis van gedrag malicieuze activiteit herkent en blokkeert.

Kennis is onontbeerlijk voor het Intrusion Prevention System van IBM ISS. Hiervoor is IBM X-Force (voorheen ISS X-Force) actief is met meer dan 300 medewerkers sinds 1994. IBM X-Force is het meest vooraanstaande onderzoeksinstituut op security-gebied ter wereld. IBM X-Force kennis zorgt iedere dag opnieuw dat informatiesystemen tegen de gevaren van morgen zijn beschermd. Een product kopen kan immers, maar IBMs X-Force zorgt met haar kennis iedere dag weer opnieuw voor de bescherming van morgen...

**Focus** ON2IT herkende al vroeg de symbiose van reactieve- in combinatie met proactieve-technieken en koos hierbij voor de oplossingen van IBM. Redenen hiervoor zijn:

- IBM biedt een betere beveiliging door de integratie van verschillende technieken;
- IBM oplossingen zijn beter en voordeliger te beheren door de integratie van verschillende instrumenten;
- IBM oplossingen zijn aantrekkelijk geprijsd door de integratie;
- IBM oplossingen bieden de bescherming voor morgen door X-Force research;
- IBM is geëncmitteerd aan een betere beveiliging van organisaties.

*Nov 1 2007: "We understand that security is a very important concern for your business. That's why we plan to spend \$1.5 billion on security-related efforts in 2008 to help global businesses, like yours, fend off threats. We look forward to sharing our progress with you in the weeks and months ahead. In the meantime, we encourage you to contact your IBM Account Leader to learn about the solutions that are available today to help reduce risk in your operation."*

ON2IT beschikt door focus over een brede expertise voor het auditeren, implementeren en beheren van security oplossingen.

## 2 Verklaard

### Waarom is een firewall niet toereikend?

Een stellige bewering! Waarom hebben we eigenlijk niet genoeg aan een firewall?

### 2.1 Hoe werkt een firewall

Een firewall beslist op basis van statische regels of netwerkverkeer wel of niet doorgang krijgt. Een goed geconfigureerde firewall blokkeert alles, behalve dat wat absoluut onmisbaar is voor een goede werking van bedrijfstoepassingen. Het kan bijvoorbeeld wenselijk zijn om email binnen te laten komen. Hoe ziet een firewall nu dat een stukje netwerkverkeer bij inkomende email hoort? Heel eenvoudig. De standaarden die gelden voor Internet mail schrijven voor dat email gestuurd wordt een bepaalde netwerkpoort (25), en de mailserver heeft een bepaald Internet-adres. Hetzelfde geldt voor bijvoorbeeld poort 80 voor websites, poort 443 voor beveiligde SSL-websites (https), enzovoorts.

Een firewall maakt van deze 'poort'-eigenschap die bij een verbinding hoort handig gebruik. Als je alleen email wilt toestaan, kun je tegen een firewall zeggen: "blokkeer alles, behalve verkeer dat aan deze voorwaarden voldoet: het doel IP-adres is het IP-adres van de mailserver, en de poort is 25." Het enige verkeer dat de mailserver kan bereiken verkeer is dan het verkeer naar poort 25. En dat zou dan in principe dus e-mailverkeer moeten zijn – al is dat op basis van alleen poortnummer geen zekere zaak. Dit is de eerste stap in beveiliging. Wat je met deze firewall regel bijvoorbeeld kunt voorkomen, is dat buitenstaanders kunnen inloggen op de mailserver via de beheerders console, of dat

ze een aanval uitvoeren op (doorgaans zwak beveiligde) Windows-poorten.

### 2.2 Noodzaak van inhoudelijke scanning

De firewall gaat er dus van uit, dat het verkeer dat hij doorlaat op poort 25, legitiem email verkeer is. Er vindt dus geen inhoudelijke controle op het verkeer plaats. Er zijn dus aanvullende maatregelen nodig. Het probleem zit op verschillende niveaus. Voor email is algemeen bekend: een email kan een bijlage bevatten met een virus. Een firewall zal dat inkomende virus slechts herkennen als "iets dat op poort 25 binnen komt". Door de instructies die we hebben gegeven zal de firewall de verbinding toestaan. Toch is de inhoud van de email gevaarlijk. Hiervoor hebben we dus een aanvullende, inhoudelijke, scan nodig, zoals controle op de aanwezigheid van virussen (en meer nog, maar dat even terzijde). Maar dit is niet alles.

### 2.3 Exploits

Stel, we zijn in staat om een email bijlage inhoudelijk te scannen, en daarmee vast te stellen of de ontvangen email legitiem is. Dan zijn we er nog niet. Tijdens het ontvangen van de email wordt namelijk informatie uitgewisseld tussen de mailserver en de verzender van de email. Dit gaat gestructureerd volgens een vast protocol. Bij email het dat protocol SMTP. Als iedereen zich netjes aan het protocol houdt, gaat alles goed. Echter, een aanval doet dit nu juist niet: mailservers bevatten bugs waar een aanval gebruik van kan maken. Tijdens de communicatie stuurt de ver-

zender bijvoorbeeld het doel-emailadres naar de mailserver. Stel dat je een mailadres van 10.000 tekens gebruikt? Hoe gaat de mailserver daarmee om? Sommige bugs in software leiden ertoe dat er in een dergelijk geval een zogenaamde “buffer overflow” optreedt: de e-mail server software houdt er simpelweg geen rekening mee dat iemand een email adres van 10.000 tekens gebruikt. In sommige gevallen is het zo erg, dat te herproduceren valt dat je hiermee de server kunt laten crashen of zelfs de controle kunt overnemen: dit is een zogenaamde “exploit”. We zeggen dan dat de server “vulnerable”, kwetsbaar, is voor deze exploit.

Er zijn talloze voorbeelden van dergelijke exploits in software. Overigens is vast te stellen of een systeem *op dit moment* kwetsbaar is voor bekende problemen. Dit gaat door middel van een softwarepakket dat systemen onderzoekt, en de bevindingen vergelijkt met een database met kennis over software met bijbehorende vulnerabilities. We noemen dit Vulnerability Assessment. Dit beperkt zich logischerwijs tot bekende vulnerabilities: niets vinden betekent niet dat er niets te vinden is. Sterker nog, hoogstwaarschijnlijk schuilen er fouten die later nog gevonden zullen worden.

## 2.4 De ernst (maar waarom)

Sommigen vragen zich af: wie vindt het interessant, en heeft ook nog eens de kennis om mij aan te vallen? Of: waarom heb ik er last van wanneer iemand op mijn systeem zit? Ten eerste: moedwillig aanvallen van een bedrijf of instelling komt inderdaad minder vaak voor, hoewel zo iets natuurlijk lastig te meten is. Echter, het grootste probleem zijn structureel opgezette massale aanvallen, die – net als spam dat doet – in het wilde weg gemikt

zijn, in de hoop min of meer toevallig ergens een keer raak te schieten. Doel: controle krijgen over het aangevallen systeem. Een aanvaller die veel systemen onder controle heeft kan deze misbruiken voor allerlei doelen. Om er een paar te noemen:

- Uitvoeren van aanvallen vanaf verschillende systemen tegelijk, die bovendien niet terug te herleiden zijn naar de echte aanvaller ongestraft versturen van spam;
- Zoeken naar gegevens als creditcard nummers;
- Opslag en verspreiding van illegale bestanden.

Er zijn op internet allerlei programma's te downloaden, waardoor je met één simpele klik van de muis op een systeem binnen kunt komen. Bijvoorbeeld het 'metasploit project'. Download en installeer de gratis software, kies een aan te vallen server, kies de exploit(s) die je wilt gebruiken, en klik! Je bent binnen.

En de last? Systemen die aangevallen zijn functioneren vaak (gedeeltelijk) niet meer, of zijn traag. Bedrijfsgegevens kunnen worden ontvreemd, of worden gewijzigd. Aanvallen naar derden komen vanaf uw netwerk. Enzovoorts, enzovoorts.

## 2.5 Patchen van software

Er zijn dus mogelijkheden om bepaalde fouten in software te misbruiken. Om dit op te lossen dient in beginsel de bug in de software, die het probleem uiteindelijk veroorzaakt, gerepareerd te worden. Dat is een lange weg. Het probleem is ten eerste dat je, in ieder geval bij 'closed source' software, afhankelijk

bent van de ontwikkelaar van de betreffende software. Bovendien dient de bug eerst bekend te zijn, daarna opgelost te worden. Als u boft doet de softwaremaker dat voor de huidige versie van uw software, maar het komt ook maar al te vaak voor dat bugs in bestaande versie pas opgelost worden in een nieuwe versie, wat naast extra kosten ook nog allerlei problemen met zich mee kan brengen.

Tenslotte moet de oplossing, als die al komt, nog op uw servers geïnstalleerd worden: het zgn. patchen van software. Windows Update is een bekend voorbeeld. Aanvallen zijn typisch gericht op nog onbekende of pas kort bekend geworden fouten in de software, waarvoor nog geen oplossing is: de zogenaamde "zero-day" aanvallen.

Het direct patchen van software kan behalve problemen oplossen zelf ook weer risico's met zich meenemen. Systemen kunnen zich opeens anders gaan gedragen, en patches kunnen incompatibel zijn met andere software. De praktijk is in elk geval dat in het gros van de gevallen de tijd tussen het vinden van een vulnerability en de uitrol zijn van de bijbehorende patch eerder maanden dan weken bedraagt. Kortom, we hebben een betere oplossing nodig.

## 2.6 Virtual patch

In veel gevallen ligt 'oneigenlijk gebruik' van een protocol aan de basis van een aanval: een aanval zoekt een grens op, waar de ontwikkelaar van software niet op gerekend heeft. Dit is precies waar Intrusion Prevention techniek een oplossing voor biedt. Een IPS (Intrusion Prevention System) is een apparaat dat 'inline' in het netwerk staat. Al het verkeer stroomt eerst door de IPS, en gaat dan pas naar (in ons voorbeeld) de mailserver toe. Zo kan de IPS

meekijken in de lopende datastroom, controleren of de standaarden gevolgd worden, en of de waarden die gebruikt worden reëel zijn. Bovendien kan een IPS ingrijpen. Als iemand een email adres van 10.000 tekens gebruikt, is dit waarschijnlijk niet de bedoeling. De IPS genereert intern een 'event'. De reactie van de IPS is dat deze de verbinding verbreekt. En het mooie is: dat email adres van 10.000 tekens is nooit op de mailserver aangekomen, zodat de aanval is mislukt.

Dit is slechts één voorbeeld van een type aanval dat een IPS blokkeert. Er zijn talloze technieken die de IPS gebruikt om na te gaan of verkeer legitiem is. Een paar voorbeelden van controles die uitgevoerd worden:

- gegevens stromen in pakketjes met een nummer dat de volgorde aangeeft. Wanneer er zonder reden twee keer een pakket binnen komt met hetzelfde nummer, kan dat duiden op een aanval die probeert 'ertussen' te komen, met allerlei mogelijke ellende ten doel. Dit kan een IPS blokkeren.
- een zgn. DoS (Denial of Service) aanval kenmerkt zich doordat zich in korte tijd abnormaal veel verbindingen opgezet worden met de server. Doel: de server overbelast maken. De IPS herkent dit, en blokkeert de aanval voordat de aanval de server bereikt.
- een oude bug is: "Teardrop" in Windows 98. Oud, maar wel karakteristiek. Die werkt zo: stuur een pakketje gegevens naar het aan te vallen systeem. In het pakketje staat de lengte van het pakket, zeg 1000 tekens. Maak het pakket dat je stuurt echter 990 tekens lang. Windows 98 bleef oneindig wachten op de laatste 10 tekens, en

het systeem was vastgelopen. (Geen groot probleem: na een herstart werkt alles weer. Maar stel dat een systeem in het bedrijfsnetwerk structureel alle machines zo'n pakket blijft sturen.) Oplossing van de IPS: controleer of een pakket dat zegt 1000 tekens lang te zijn, ook echt 1000 tekens lang is. Zo niet: blokkeer het pakket.

Alles bij elkaar maakt dat het plaatsen van een IPS vóór een systeem dat we willen beschermen, het effect heeft dat exploits niet bij het beschermde systeem aankomen en er dus geen effect op hebben – en dat terwijl fouten in software er niet gepatcht (hoeven te) zijn. Dit is wat we willen. We noemen dit effect ook

wel 'virtual patch'. We hebben tenslotte virtueel (op netwerkniveau) de bugs gepatcht.

## 2.7 Kennis is essentieel

Dit systeem valt of staat natuurlijk bij de kennis die het apparaat benut over exploits en protocollen die het apparaat tegen kan komen wanneer het in het netwerk staat. Die kennis wijzigt van dag tot dag: er komt nieuwe software uit, er worden nieuwe exploits bekend en er worden nieuwe (versies van) protocollen gebruikt. Ook aanvalstechnieken veranderen. Er is dus doorlopend onderzoek nodig naar exploits, bugs in software, protocollen die gebruikt worden, enzovoort.

### 3 Onion-beveiligingsmodel

De keuze “in hoeverre gaan we beveiligen” is altijd een afweging. Dit vraagstuk is tot op zekere hoogte te vergelijken met het beschermen van een polder door middel van dijken. Ten eerste moet de zeedijk goed genoeg zijn om de zee te keren (perimeter security). Daarnaast zijn er andere dreigingen, zoals hevige regen en rivieren die water vanaf de andere kant laten komen. Het is dus verstandig de polder op te delen, zodat niet meteen de hele polder overlooft als ergens onverhoopt iets misgaat. Maar waar leg je de dijken? Twee factoren zijn hier van belang: hoe groot is het risico? En wat is de schade als 't mis gaat?

Terug naar netwerkbeveiliging. De eerste factor, de kans op problemen wordt in belangrijke mate bepaald door de aanwezigheid van een aantal risicofactoren. Uiteraard is elke verbinding met internet een belangrijk risico. Bescherming hiervan is in alle scenario's vereist. Voorbeelden van interne risicofactoren zijn werkstations van gebruikers op de kantoorlocaties, draadloze netwerken en locaties waar onbekende systemen in het netwerk kunnen worden 'ingeprikt' – maar denk bijvoorbeeld ook aan eventuele netwerkpoorten voor laptops van beheerders. De tweede factor, de (financiële) impact van een segment dat problemen ondervindt.

#### IT security 'onion layer'

De infrastructuur evolueert tot een open business tool, oftewel een utiliteit. Een eigentijdse beveiliging van de infrastructuur en dus uw informatie vraagt om een gelaagde aanpak.

#### Laag één: perimeter of border security

Op verbindingen tussen netwerken onderling – ook het Internet is er een – kunnen de verkeersstromen bewaakt worden. Een Next Generation firewall, met o.a. Intrusion Prevention System en Anti Virus Gateway, wordt geplaatst tussen netwerken. Het onderscheid tussen Local Area- en Wide Area Netwerk vervaagt door de toenemende verbindingsmogelijkheden (fiber, sds, mpls, etc.). Alle deelnetwerken moeten worden bewaakt, en het is aan te raden om bedrijfsnetwerken op te delen om dat handzaam en gericht te kunnen doen. Zo blijft een mogelijke infectie beperkt tot een deel van de infrastructuur. De verschillende netwerken worden met Intrusion Prevention techniek onderling beschermd.

#### Laag twee: host security

Servers in het netwerk bevatten nu vaak software om virussen te detecteren. Antivirus software biedt geen 100% veiligheid. Gebruikers mailen en surfen over het Internet. Wanneer servers dit doen is dit niet best. Toch vertrouwen we de communicatie tussen de gebruikers en de servers. We inspecteren niet. Hierdoor stellen we de servers, die alle (vertrouwelijke) informatie bevatten, bloot aan alle gebruikersgevaaren. In feite zijn de servers een apart netwerk dat door Intrusion Prevention tegen de andere systemen zou moeten worden beschermd.

Onder de definitie 'host' vallen ook alle gebruikers en andere apparatuur (netwerkprinters). De gebruikers beschikken steeds vaker over een mobiele werkplek (laptop, blackberry, smartphone) waarmee ze overal werken. Ook gebruiken ze vaker toepassingen (m.n. "Web 2.0") die met versleuteling

werken. Versleutelde communicatie kan niet worden geïnspecteerd. Maar dat gebeurt allemaal ook steeds vaker over poort 80, die altijd openstaat, en dus de perimeter security functie direct ondermijnt. De gebruikers moeten dan ook beschermd worden met meerdere beveiligingstechnieken, zodat malicieuze zaken op basis van gedrag herkend worden.

**Laag 3: toezicht** De noodzakelijke flexibilisering van de infrastructuur vraagt om techni-

sche middelen bij het toepassen en controleren van het gestelde beleid. Naast één geïntegreerd beheer (ook mail en web filtering) van de border- en host-security is een Network Access/Admission Control (NAC) een vereiste. Er is nl. standaard geen controle of de desktop wordt bijgewerkt (antivirus e.a. software updates) en er is geen automatische controle wie van de infrastructuur gebruik mag maken en wat iemand expliciet niet mag. Zonder NAC wordt een gebruiker die buiten de gestelde paden treedt niets in de weg gelegd.

### 3.1 Drie stappen voor verbetering

#### Fase 1: Betere afscherming van Internert – Proventía MX

De Proventía MX next generation firewall wordt geplaatst. De verschillende instrumenten zorgen voor een preventieve bescherming door de combinatie van noodzakelijke reactieve (bestaande: rule based) met preventieve technieken.

**Protocol Analysis Module (PAM)** Meerdere detectie technieken zorgen voor een ongeëvenaarde nauwkeurigheid.

**VirtualPatch™ technology** bestaat uit “vulnerability-focused” algorithmes die bescherming bieden tegen hele families malicieuze codes die gebruik maken van software onvolkomenheden (lekken).

#### Fase 2: Betere afscherming van kritische systemen – Proventía GX, Proventía Server

De Proventía GX wordt geplaatst voor kritische servers. Op deze wijze worden een

#### De Proventía MX voordelen

- Betere beveiliging door integratie (enig instrument voor het stoppen van worm-verspreiding);
- Betere beveiliging nu en in de toekomst door IBM X-Force;
- Beter te beheren door integratie;
- Beter geprijsd door integratie (v.a. € 995).

scheiding en al het verkeer naar de servers geïnspecteerd. De Proventía GX is een dedicated Intrusion Prevention toestel. Aangezien

prestatie een bepalende factor is voor de prijs en encrypted verkeer pas op de server gede- crypt wordt adviseren wij het gebruik van Pro- ventia Server. Proventia Server is een soft- ware applicatie die verschillende technieken combineert.

#### De Proventia Server voordelen

- Betere beveiliging door de integratie van verschillende technieken;
- Meer betrouwbare server door data integriteit- en systeemactiviteit con- trole;
- Betere beveiliging nu en in de toe- komst door IBM X-Force;
- Aantrekkelijk geprijsd (v.a. € 825).

#### Fase 3: Betere afscherming van “in- siders” – Mirage Networks Network Access Control

De Mirage Networks NAC oplossing is een instrument voor de controle op de toegang tot de infrastructuur. De conditionele toe- gang zorgt ervoor dat gast verkeer moge- lijk is, ongeautoriseerde en/of geïnfecteer- de gebruikers worden geweerd en hacker in- strumenten en ongewenste netwerkhardwa- re niet kan worden gebruikt. Proventia Ser- ver is een software applicatie die verschillen- de technieken combineert.

#### De Mirage NAC voordelen

- Betere toegangscontrole op het net- werk;
- Meer betrouwbare dor het controleren op patch en security niveaus van syste- men;
- Betere beveiliging door “virtual inline” datastromen te blijven onderzoeken;
- Geen netwerk aanpassingen of cliënt software vereist.