

Meetbare beveiliging

SecPoint Protector en Penetrator

Beveiliging: het blijft een belangrijk onderwerp. Beveiligingsoplossingen zijn er genoeg, maar de vraag is altijd hoe effectief die zijn en hoe veilig het netwerk is. De Protector en Penetrator, twee oplossingen van SecPoint, zorgen niet alleen voor een goede beveiliging, maar maken de beveiliging ook meetbaar. *Frank Everaardt*

Wat was het een tiental jaren toch makkelijk: computers waren niet met het internet verbonden en hooguit was er een verbinding met een huurlijn met een ander netwerk. Een modem of een geïnfecteerde diskette was hooguit de bedreiging waarmee je rekening moest houden. De opkomst van het internet heeft niet alleen voor veel nieuwe mogelijkheden gezorgd, maar ook zijn de beveiligingsrisico's er flink door toegenomen. Hierdoor is het beheer een stuk complexer geworden, maar vooral is de noodzaak van beveiliging op vele fronten uiterst belangrijk geworden. Inmiddels moet je rekening houden met netwerkverbindingen thuis, internetgebruik op het werk en tal van digitale criminelen die via de internetverbinding of draadloze verbindingen toegang proberen te krijgen tot jouw netwerk.

Penetrator

Firewalls, antivirussoftware, procedures, mailscanners en tal van andere producten worden geïnstalleerd om de beveiliging binnen het netwerk te garanderen. Helaas ontcom je bijna niet aan een wildgroei en is het zeker in een groter netwerk eigenlijk niet goed meer mogelijk om een goed beeld te vormen van de beveiligingsstatus. SecPoint speelt hier op in met zijn Penetrator, een product dat kan nagaan hoe goed de beveiliging nu werkelijk is met behulp van een groot aantal tests.

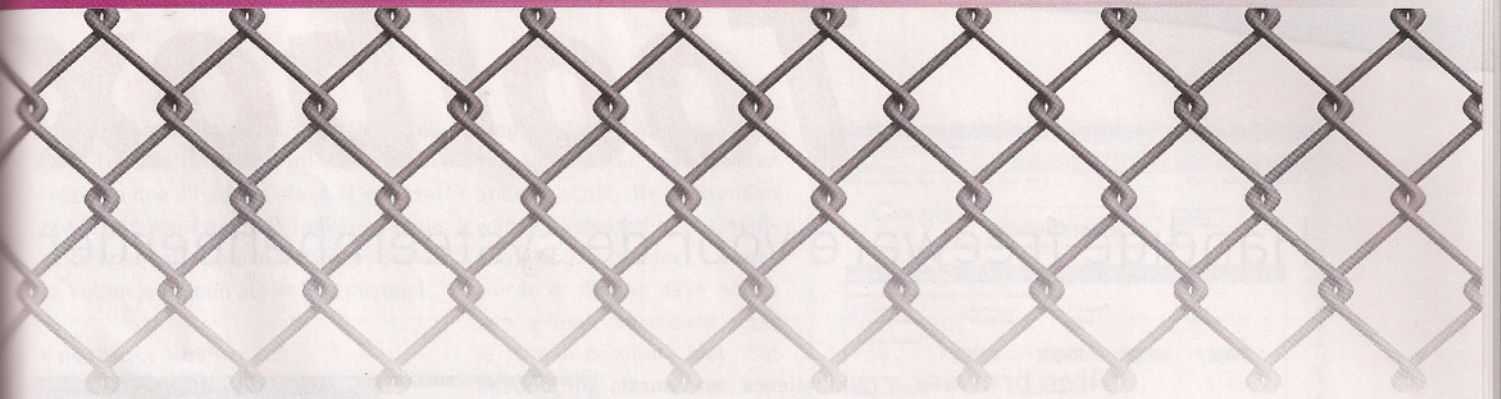
De Penetrator van SecPoint is een slim apparaat. Gevat in een paarsblauwe behuizing maakt dit apparaat al direct duidelijk dat het iets bijzonders is. De Penetrator is geschikt om zowel te worden gebruikt in productieomgevingen als in een labtest. Feitelijk heb je in dit paarse doosje een gerobotiseerde hacker zitten, die niet zeurt om betaling en test na test kan herhalen totdat het gewenste resultaat is behaald. Het apparaat kan netwerken testen aan de hand van tienduizend signatures en kan tal van verschillende hack-methoden uitvoeren om je netwerk tot het uiterste te controleren op beveiligingslekken. De database met signatures wordt bovendien dagelijks ge-update met nieuwe bedreigingen, zodat je continu je netwerk op het hoogste niveau kunt testen.

DoS-aanval

De Penetrator gaan vrij ver in de uit te voeren tests. Het is zelfs mogelijk om een echte Denial of Service- of DoS-aanval uit te voeren op je servers en te kijken hoe je netwerk hiertegen is opgewassen. Het is zelfs mogelijk om verschillende Penetrators te koppelen - binnen en buiten het netwerk - om zo vanaf verschillende plaatsen het netwerk 'aan te vallen'. De gekoppelde Penetrators kunnen gezamenlijk vanaf een enkele locatie worden beheerd en geadmistreerd. Behalve het simpele virtueel kloppen op de deur en kijken of de deur open is of het kijken of een digitale looper past op je virtuele voordeur bevat het systeem ook de mogelijkheid om websites aan een uitgebreid onderzoek te ontwerpen. Zo is



Afbeelding 1.
De Penetrator



het mogelijk om onder meer SQL-injecties te doen. Ook kun je de Penetrator de site laten doorlopen om er zo achter te komen of de website wel volledig werkt. Alle mogelijkheden van de Penetrator zijn eenmalig of op regelmatige basis uit te voeren en als resultaat meldt het apparaat zich met duidelijke rapportages naar wens in xml-, pdf- of html-formaat. Het beheer in de praktijk van het apparaat is reuze eenvoudig. Aan de voorzijde bevindt zich een viertal netwerkaansluitingen die naar wens is te gebruiken voor verschillende netwerksegmenten of bijvoorbeeld ook een verbinding met buiten. Verschillende beheerders kunnen tegelijk het apparaat beheren en gebruiken. Van de Penetrator bestaan een aantal verschillende uitvoeringen die verschillen in kracht. In het programma bevindt zich één buitenbeentje, de Portable Penetrator. Deze speciaal uitgeruste laptop is naast de mogelijkheden die je van de 19 inch-units bent gewend ook geschikt om draadloze netwerken

te testen met de verschillende gangbare encryptiemethoden, waaronder wep, wpa en wpa2.

Protector

Behalve de Penetrator waarmee je de beveiliging van je netwerk kunt controleren biedt SecPoint ook de Protector. De kennis en kunde die het bedrijf heeft opgebouwd met de Penetrator wordt hier op de omgekeerde manier gebruikt. In plaats van (gecontroleerd) beveiliging te testen zorgt dit product voor een totale beveiliging van je netwerk. De Protector kan zowel binnen als buiten de firewall worden opgesteld. De Protector controleert aangeboden data op een groot aantal verschillende manieren. Om te voorkomen dat je netwerk wordt gehackt, maakt het apparaat gebruik van dezelfde database als voor de Penetrator wordt gebruikt. Daarnaast controleert het systeem op vreemde en gekke datapakketjes. Tot slot kan het apparaat het verkeer uitgebreid con-

trollen op virussen. Daarvoor gaat de Protector niet over één nacht ijs, want hierbij kan worden gebruikgemaakt van verschillende antivirusprogramma's. De Protector kan samenwerken met BitDefender, Kaspersky, Norman en ClamAV. Ook spam krijgt dankzij de Protector geen kans. Mocht het nu toch nog misgaan, dan is het mogelijk om de Protector ook ongewenst uitgaand verkeer te laten tegenhouden.

Beveiliging is een hot topic, maar in plaats van je af te vragen hoe veilig je netwerk is, weet je door middel van de Penetrator van SecPoint hoe veilig het echt is. Gemoedsrust en zekerheid dus. Dankzij de verregaande automatisering en de goede rapportage is de SecPoint Penetrator een waardevolle aanvulling op het netwerk. Dat geldt zeker ook voor de Protector die je netwerk op vrijwel alle denkbare manieren beschermt tegen de boze buitenwereld van het internet. <