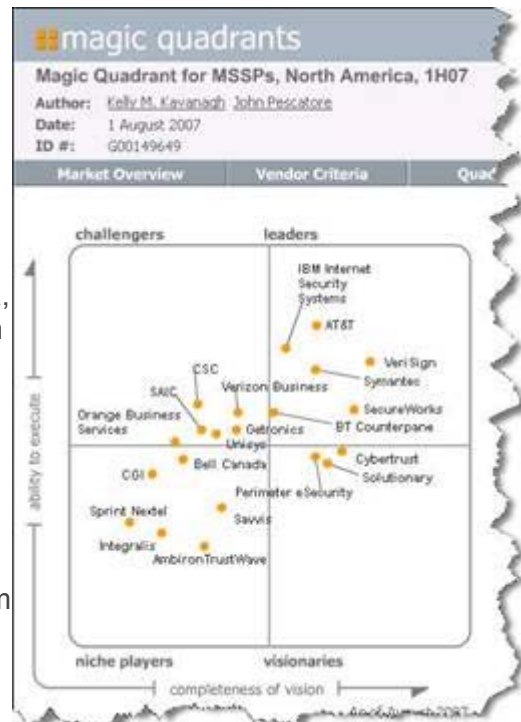


Artikel Zin en Onzin

Security.nl Door Peter Rietveld op dinsdag 11 december 2007 10:55

In het kader van de themaweek Managed Security vorig jaar betoogde ik dat het uitbesteden van beveiliging een hoge mate van maturiteit in de organisatie vraagt: je moet immers weten wat je aan beveiliging moet doen, voordat je dat door een ander kan laten doen. Om een smart buyer te zijn moet je méér materiedeskundigheid hebben dan als je het zelf doet, want bij zelf doen geval kun je nog 'iteratief' kennis opbouwen. En bijgevolg zul je er meer van moeten weten dan je leverancier. Maar goed, dit jaar wil ik iets minder filosofisch naar deze materie kijken.

Het concept Managed Security Service Provider (MSSP) lijkt bedacht te zijn door Counterpane – nou ja, dat zeggen ze zelf. Gartner heeft dit MSSP concept eind vorige eeuw omarmd en massaal aanbevolen. Volgens het magic quadrant Noord Amerika van 1/8/07 staat Verisign bovenin (zowel in visie als in het vermogen tot uitvoering), op de voet gevolgd door IBM, AT&T en Symantec en meer op afstand gevolgd door BT en onze eigen KPN (nou ja, Getronics dan). In de Europese Magic Quadrant van April 2007 staan eigenlijk alleen Cybertrust en Integralis als partijen die een geschiedenis hebben in Security, de rest zijn dezelfde doorsnee mix van systeem integrators en telco's die alles aanbieden wat een beetje potentie lijkt te hebben. Wat overigens niets hoeft te zeggen over de kwaliteit. In dit licht moet je ook de overname van GPR door de KPN zien: BT heeft Counterpane, Deutsche Telecom heeft debis en dan kun je niet achterblijven. Deze 'me too' scenario's spelen een grote rol, waardoor grote bedragen worden gependend om het portfolio op hoofdlijnen vergelijkbaar met dat van de concurrentie te maken. De vraag of het allemaal even zinvol is voor de klant, krijgt minder aandacht zo te zien.



De uitkomst van Gartner is niet verwonderlijk, als je je realiseert dat het zwaarst wegende aspect in deze weging de omvang van de firma en de financiële positie is. Met dit soort vergelijkingen zul je als je een auto koopt thuiskomen met een Opel of een Fiat. Prima auto's hoor, maar als je naast iemand parkeert in een Donkervoort of een Spyker, steekt het wat schraal af. Als je een auto moet hebben om indruk te maken op de burens, is een Kadett of een Panda duidelijk een mismatch. En helemaal als je nog geen rijbewijs hebt – het gaat op den duur toch opvallen dat je er nooit in rijdt.

Wat is er te koop?

Managed Security is een containerbegrip, waarin allerlei beveiligingszaken in een doosje met een strik erom aangeboden worden. Om te voorkomen dat je appels en peren vergelijkt, is een korte rondgang noodzakelijk. Bij het vergelijken van abstracte, samengestelde proposities als Managed Security moet je nu eenmaal onder de motorkap kijken om te zien wat het aanbod nu precies inhoudt.

Het resultaat van een rondgang langs de aanbieders lijkt dat het beheer van security devices geouttasked wordt. Security Devices variëren een beetje, waarbij sommige leveranciers zich beperken tot de klassieke firewalls, maar het merendeel woont inmiddels wat hoger de OSI

stack in door ook allerlei IDS/IPS-achtigen en crypto spul te beheren. De meeste aanbieders concentreren zich bij het beheer van devices op de netwerk perimeter, sommigen durven de sprong het interne netwerk in, aan. Een specifieke categorie zijn de aanbieders van Managed PKI services, maar in de praktijk lijkt deze markt zeer beperkt. Nu ja, de meeste bestuurders krijgen nog steeds puistjes als je PKI roept.... Als toefje op de taart wordt over het algemeen 'threat management' in allerlei varianten aangeboden, waarbij je eerder dan de rest van de wereld weet dat er een gat zit in een stuk software, zonder dat je daarvoor zelf allerlei bronnen in vele talen moet gaan doorwaden om deze informatie te vinden.

Om eens te gaan kijken wat je aan Managed Security zou hebben of wat je zou willen aanbieden, moeten we nader ingaan op de verschillende onderdelen van de dienstverlening.

Managed Security Devices

Deze categorie omvat het bulk van alle aanbieders. Met het uitbesteden van het beheer van een stel appliances is op zich niets mis, omdat die dingen ook beheerd moeten worden. Bij de producten die zich op de applicatielaag begeven is er een behoorlijke patchcyclus en als het volgende gat in een rar of chm parser gepubliceerd wordt, zal een externe leverancier wellicht sneller patchen dan je dat zelf zou doen. Doen dus.

Als je vervolgens leest dat 'Managed Firewall Services' een 'totaaloplossing voor de implementatie en beheer van een effectief Security beleid binnen een organisatie' bieden "door inzet van ervaren, gecertificeerde security engineers en consultants", ga je toch weer twijfelen. Firewalls die uitstekend helpen binnen een netwerk? Is dit een leverancier die voldoende kennis heeft?

Het in de lucht en gepatched houden van een firewall, een VPN concentrator, een IDS of een log correlatiedoosje is het simpelste stuk, je moet echter nog steeds iets dóen met dergelijke apparaten. Zeker met de meer geavanceerde. Zoals ik laatst als predikte op dit platform moet je als bewaker weten wat je bewaakt omdat je anders niet weet wat je ziet. Dit houdt in dat je als MSSP-klant je leverancier in detail op de hoogte moet brengen van wát en wie er bewaakt wordt en of er intern (of extern) operationeel iets speelt waardoor normaliter valide verkeer dat op eens niet hoeft te zijn. Dat kan zoiets banaals zijn als een medewerker die uit dienst is gegaan. Het "detecteren van afwijkingen in het netwerk van de klanten en het onmiddellijk op de hoogte brengen van de klant" is dan ook grotendeels wensdenken: alle beperkingen en nuances van bewakingssystemen gelden, ongeacht of deze nu in-house dan wel geoutsourced bediend worden.

Managed Security Devices zal helaas zelden meer voorstellen dan het in de lucht houden van onderbenutte geavanceerde doosjes. De bijdrage aan de veiligheid is dan ook gering, de rationale is puur kosteneffectiviteit. Hoewel effectief, je geeft minder uit aan iets wat je net zo goed kan laten, omdat je er nog niet aan toe bent. Haal eerst maar je rijbewijs voordat je die Panda koopt.

Managed Secure Internet Hosting

Feitelijk is dit gewoon hosting met een modieus verkooppraatje, vrijwel iedere echte hosting provider regelt de beveiliging goed. Ze moeten wel. Dit is de meest volwassen vorm van Managed Security.

Managed Secure Internet Access

Deze vorm kan wel interessant zijn om te outsourcen: voor je inbound proxy staat een filtering proxy die virussen en spyware vangt en de meest omineuze sites op een blacklist zet. Deze extra laag kan veel ellende voorkomen. Hierbij geldt dat dit alleen het algemene basisniveau kan leveren. Een nadeel om in de gaten te houden dat een filter op de proxylaag de feitelijke bandbreedte aanzienlijk beperkt. Dit is ondanks de uitvoerbaarheid en het evidente nut verassend genoeg een weinig gangbaar product bij de grote MSSP. Het

concept wint wél terrein bij de reguliere ISP's, waar het waarschijnlijk beter past.

Managed Secure E-Mail

Deze categorie wordt door een paar gespecialiseerde aanbieders geleverd, en maakt vaker deel uit van een pakket van weer een andere aanbieder. Het beveiligen van mail laat zich goed outtasken, zo lang de afnemer niet verwacht dat het fire and forget is en een tamelijk algemeen beveiligingsniveau vraagt, net als bij de Secure Internet Access. Een aandachtspunt is mail integratie met andere functies zoals webmail: mailscanners werken op SMTP niveau waardoor de eigen mailinfra niet meer extern zichtbaar mag zijn. Het kan daardoor conflicteren met webmail en de wens op userniveau verschillende regels neer te zetten.

Het wordt anders als je bijvoorbeeld meer dan de standaard beveiligingsfuncties vraagt; wil je dat alles wat positief herkend wordt als virus of spam verwijderd wordt zijn er tal van prima aanbieders die dit wellicht goedkoper kunnen dan je het zelf zou doen met dezelfde standaardproducten. Wil je dat informatielekken door eigen medewerkers of alle 0-day's worden tegengehouden, dan zul je merken dat iets anders dan een kadett niet in het assortiment zit.

Managed Threat Management

Wat je uitbesteedt met deze dienst is het afspeuren van de boze buitenwereld op nieuwe bedreigingen. Je MSSP koopt het op haar beurt weer in bij een hierin gespecialiseerde speler. Threat Management is prima etalagemateriaal, want je laat zien dat je proactief goed op de hoogte bent wat je bedreigd. En de besparing kan op het eerste gezicht reëel zijn, omdat het doorlezen van duizenden berichten per dag in allerlei moeilijke talen op zoek naar dat ene puntje dat een eigen systeem kan raken wellicht niet kosteneffectief is. Maar de vraag is wát je er überhaupt aan hebt. Immers, je hebt een tijdje eerder het nieuws dat er een gat zit in een PHP script op een specifieke Linux distro of je kent eerder de details over een gat in Excel. Bij de eerste moet je je afvragen of je dat script eigenlijk wel hebt, en of het in een kwetsbare opstelling draait, en bij het tweede of de organisatie het gaat vreten dat je een tijdlang – tot er een fix is – het gebruik van Excel uitsluit. En als er géén fix komt, dat je het hele product per direct overboord gooit.... Hetzelfde geldt de gedetailleerde informatie over virussen: wat heb je aan de informatie in realtime, als je antivirus producten het vervolgens niet kunnen onderscheppen? Ga je de internetpijp dichtgooien omdat er mogelijk een virus aankomt? Wanneer mag die dan weer open? Kennis zonder dat je er iets mee kunt veranderen, leidt hooguit tot een gefrustreerde Security Officer.

Zonder een zeer goed functionerende beheerorganisatie en/of een dringende behoefte een hoog veiligheidsniveau te realiseren, is Threat Management dan ook meer bezigheidstherapie voor Security-knutselaars dan zakelijk zinvol. Hoewel je de directie goed de stuipen op het lijf kunt jagen met het aantal bedreigingen waar je geen middelen tegen hebt. Maar of en wanneer het nuttig is je eigen onvermogen zo te etaleren behoort tot de arena der politiek.

Andere diensten

Naast deze vormen van managed service worden incidenteel nog andere zaken onder de noemer geschaard, om een nog breder en indrukwekkender portfolio te bouwen. Forensische Opvolging, Managed Vulnerability Management of Managed Security Audit zijn niet meer dan terugkerende diensten in deze of gene vorm. Kan helemaal zijn wat je zoekt, maar ik zou dit onder koppelverkoop scharen; het woord Managed staat ongeveer gelijk aan een strippenkaart of een abonnement en ik zou het feit dat ik iedere twee weken de Bobo door de brievenbus krijg toch niet als Managed Service durven omschrijven.

Het Managen van Managed Security

Een vereiste voor iedere managed service is dat je een manier hebt om de resultaten te

meten. Tenminste, als het goed is, je gaat toch geen contract afsluiten vanwege een buikgevoel en mooie taartpunten en stoplichten? Nou dan!

Security Metriek geldt als een soort holy grail, net zoiets als ROSI (Return On Security Investment) dat is. Uitbesteding geeft nog een extra dimensie aan deze queeste. De uitdaging der metriek is in Managed Security van een hele andere orde grootte dan bij normale outsourcing, en ga er van uit dat de gemiddelde service manager hier inhoudelijk niet op voorbereid is. Een Security incident is geen storing die 'opgelost' is als de stack van een doosje weer antwoord geeft op een ping. Eindgebruikerstevredenheid zegt bij Security niet of de gestelde doelen bereikt zijn, misschien eerder het tegendeel. De klassieke KPI's gelden hier niet.

Het gaat meestal mis in de discussies als het subtiele verschil tussen de beveiliging en de resulterende veiligheid niet voldoende onderkend wordt. Het meest realistische is het meten van de inspanning van de leverancier in plaats 'resultaten'. Als je de leverancier op de resulterende veiligheid wilt afrekenen, moet je immers de detaillering van het beveiligingsbeleid en de dagelijkse interpretatie overlaten aan de leverancier. En dat wil je wellicht niet, niet in het minst omdat je dan maar één leverancier kunt hebben. Je kunt de bewaker van de voordeur niet afrekenen op het resultaat, behalve als je geen achterdeuren hebt én dat aan kunt tonen. Je loopt bovendien al gauw vast in oeverloze discussies over hoe dat virus op het netwerk is gekomen of waarom je niet gezien hebt dat de echtgenoot van een ex-medewerkster informatie uit een systeem steelt. Forensisch onderzoek kan dan – in sommige gevallen – uitsluitsel geven, maar de zakelijke relatie staat op dat moment al zó onder druk, en digitale bewijsvoering is zó ondoorgrondelijk en inhoudelijk betwistbaar, dat je die kant écht niet op moet willen.

Het laatste aandachtspunt dat ik mee wil geven, is het verschil is tussen het meten van de beveiligingsinspanning en het meten van goede bedoelingen. Dat een Managed Security provider ISO27001/CMM-SSE of whatever gecertificeerd is, zegt niet noodzakelijker wijze iets concreets over hoe goed deze de informatie van een klant beveiligd. De gangbare methodes zijn te abstract voor een dergelijk gebruik. Ze stellen statische doelen, zonder beschrijving van de middelen, en zijn niet gedimensioneerd op uitbestedingsrelaties waarbij een leverancier meerdere partijen met verschillende beveiligingsbehoeftes bedient. Deze noodzakelijke nuanceringen maken het er niet verkoopbaarder op, behalve als de afnemer bereid en in staat is diep op de materie in te gaan. Of blind te tekenen.

'Managed Security' is al met al een gemengd pakket van onrijpe en rijpe diensten. Voor de meeste organisaties zal de bezuiniging van uitbesteden inhouden dat ze minder uitgeven aan iets wat ze net zo goed kunnen laten, behalve als ze het doen met het expliciet doel ervaring op te doen. Als ze deze eerste horde genomen hebben en een echte smart buyer zijn geworden, is het verantwoord bepaalde diensten in te kopen. Ik acht de kans groot dat ze dan weer té goed weten wat de beperkingen van de meeste proposities zijn, en hoeveel ze nog steeds zelf moeten doen, zodat ze het liever helemaal zelf blijven doen.

Peter Rietveld, Senior Security consultant bij [Traxion](#) - *The Identity Management Specialists*

UBM Global > Indien een leverancier kiest om Managed Security Service Provider (MSSP) te zijn, dan passen de producten van CenterTools DriveLock hierin, temeer alle producten dezelfde look-and-feel hebben als de Microsoft producten en naadloos integreert met Active Directory en eDirectory.