Voorkomen is beter dan genezen

Continuous Security Monitoring vanuit de cloud

door: Wolfgang Kandek

Bedrijven realiseren zich steeds vaker dat traditionele beveiligingsmethoden niet langer werken tegen de dynamiek van cyberbedreigingen. Daar komt bij dat deze methoden bedrijven vaak beperken in hun schaalbaarheid. Door het groeiende aantal apparaten en de toename van het gebruik van de cloud, worden infrastructuren van bedrijven steeds heterogener. Security managers moeten tegenwoordig zowel de fysieke datacentra als ook de virtuele en remote datacentra van de organisatie beschermen. Dit vormt een nieuwe, gecompliceerde beveiligingslaag tegen cyberaanvallen.

De internationalisering en hogere mobiliteit van medewerkers zijn eveneens van invloed op de complexiteit van de bedrijfsbeveiliging. Werknemers en apparatuur bevinden zich niet langer op één plek, maar in verschillende kantoren (vaak in verschillende landen), onderweg en bij klanten. Inzicht in de informatie die bij een organisatie binnenkomt en uitgaat is daardoor moeilijk te controleren. Hoe meer kantoren hoe meer hardware en endpoints binnen een organisatie.

Het risico van endpoints

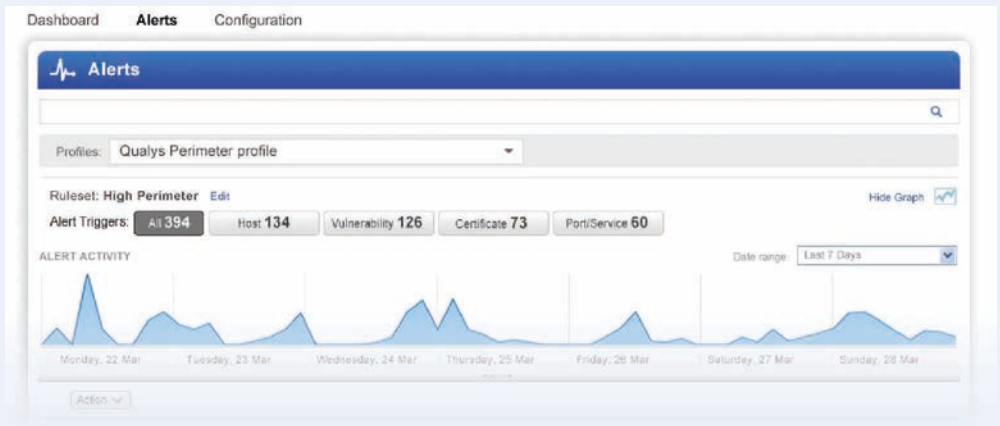
Mobiele endpoints waren zelfs voor de opkomst van de cloud en BYOD al lastig te beveiligen vanwege hun mobiele karakter. Nu krijgen endpoints overal toegang tot het bedrijfsnetwerk; direct, via een netwerk van een provider of via een draadloos (openbaar of beveiligd) Wi-Fi-netwerk. Het aantal endpoints is enorm toegenomen en zal nog meer toenemen: naast de desktop zijn er nu ook laptops, tablets, smartphones, printers en smartwatches. Wanneer de beveiligingsoplossing van een organisatie deze endpoints niet continu in de gaten houdt, kunnen beveiligingsproblemen over het hoofd worden gezien. Door de toenemende mobiliteit hebben apparaten die worden gebruikt om op afstand te werken soms dagen of weken geen verbinding met het bedrijfsnetwerk. Veelal zijn de huidige beveiligingstools die organisaties gebruiken niet ingericht of niet in staat om de activiteit van deze apparaten te monitoren wanneer zij zich buiten het bedrijfsnetwerk bevinden. Daardoor is het niet mogelijk om te bepalen of het apparaat of de applicatie beschikt over de laatste beveiligingsupdate of kwetsbaar is voor cyberaanvallen.

De gevolgen van de cloud

Omdat we steeds meer werken in de cloud, is het voor bedrijven belangrijk om snel te reageren op beveiligingsbedreigingen. Het belang van continue beveiliging neemt toe door de nieuwe methoden van cyberaanvallen, zoals via lekken in cloud-applicaties. De enige manier om een bedrijf effectief te beveiligen tegen cyberaanvallen, is met een cloud-georiënteerde beveiligingsarchitectuur die continu kan monitoren en informatie kan verzamelen in elk type omgeving. Maar voordat de overstap gemaakt wordt naar continue beveiliging, dienen de grootste beveiligingsuitdagingen voor de organisatie in kaart worden gebracht.

Asset Tagging

Een van de grootste zakelijke beveiligingsuitdagingen is asset discovery. Hoe kun je systemen beveiligen als je niet weet dat het bestaat? Helaas is er op dit moment nog geen hulpmiddel te koop waarmee je één compleet overzicht van je assets krijgt. Met een accurate en up-to-date inventarisatie van je it-assets door asset tagging kom je echter al een heel eind. Met geautomatiseerde asset discovery en management monitor je voortdurend welke assets je organisatie binnenkomen en uitgaan. Zo wordt het veel eenvoudiger om een veilige omgeving te behouden.



Vulnerability Management Solution

Inzicht krijgen in het bedrijfsnetwerk is nog niet zo eenvoudig, vooral met de huidige virtuele netwerken en kantoren op afstand. De meeste systemen binnen een bedrijf maken gebruik van een internetverbinding, maar vaak blijft verborgen welke informatie het netwerk binnenkomt of verlaat. Met continue monitoring beoordeel je niet alleen accuraat je netwerkomgeving, maar krijg je ook het broodnodige inzicht in de data die zich via het netwerk verspreiden, door automatisch te scannen op kwetsbaarheden.

Kwetsbare webapplicaties

Kwetsbaarheden in webapplicaties vormen, als ze niet worden gepatcht of opgelost, een belangrijk risico voor de applicaties en data van een bedrijf. Sterker nog, zwakke plekken in webapplicaties zijn op dit moment de belangrijkste oorzaak van ruim 55 procent van alle serverbeveiligingsproblemen. Webapplicaties hebben verschillende zwakke plekken. Bij veel cyberaanvallen worden zogeheten 'fault injections' gebruikt, die profiteren van de kwetsbaarheden in de syntax en semantiek van een applicatie. Ook SQL injection en cross-site scripting worden vaak gebruikt. Gevolg van dit soort aanvallen is dat hackers controle krijgen over een applicatie en eenvoudig toegang hebben tot de server, database en andere back-end it-bronnen.
Veel netwerkmanagers zijn niet op de hoogte van de zwakke plekken van webapplicaties die bij cyberaanvallen misbruikt worden door hackers om de traditionele netwerkbeveiligingen te omzeilen, tenzij een bedrijf bewust tegenmaatregelen neemt. Helaas is daar nog geen wondermiddel voor verkrijgbaar. Wel zijn veelvoorkomende zwakke plekken te detecteren met een automatische scanner, waarmee bedrijven beveiligingsproblemen kunnen inschatten, volgen en herstellen.

Continue beveiliging

We zeiden reeds dat endpoints door hun grotere bereik altijd een uitdaging zijn geweest voor bedrijven. Met de mobiliteit van de huidige endpoints is het moeilijk om te zien wat er wordt gedownload, welk proces er loopt via deze endpoints en welke poorten zij misschien hebben geopend. Feit is dat, wanneer een endpoint geïnfecteerd is, het dagen of zelfs maanden kan duren om dit ontdekken, tenzij er continue monitoring plaatsvindt. Een hulpmiddel dat de overweging waard is, is een analysetool die alle verkeer controleert van en naar een webserver op het openbare internet.
Uiteindelijk moet een organisatie zichzelf kunnen beschermen tegen verschillende soorten aanvallen, of er nu sprake is van een wereldwijde hack waarbij de hackers geen speciaal doel hebben, of een doelgerichte aanval om specifieke informatie of data te onderscheppen.
Met een succesvol beveiligingsprogramma richt een organisatie zich op het beheer van beveiligingspatches, continue monitoring en het verzamelen van intelligentie door te kijken naar alle veranderingen die plaatsvinden binnen de infrastructuur van een bedrijf. Een cloud-georiënteerde beveiligingsarchitectuur kan al deze mogelijkheden bieden en stelt organisaties in staat om hun meest waardevolle assets continu te beveiligen.

De ethiek van cyberbeveiliging

De discussie over het wel of niet bekend maken van zwakke plekken in computersystemen, werd recent weer aangewakkerd door het besluit van Microsoft om te stoppen met zijn publieke notificatiesysteem. Tegelijkertijd besloot Google om details te publiceren over een beveiligingsprobleem in Windows, de dag voordat Microsoft de oplossing bekend maakte. Moeten we beveiligingsproblemen nu wel of niet vrijgeven? En zo ja, binnen welke termijn? Dienen we als security community misschien het proces van bekendmaken van vulnerabilities te heroverwegen? In het geval van full disclosure maakt een beveiligingsonderzoeker een probleem zo snel mogelijk publiekelijk, omdat mogelijke slachtoffers van een cyberaanval ethisch gezien net zoveel recht hebben op deze informatie als hun hackers. Bij responsible disclosure wordt het beveiligingsprobleem pas bekend wordt gemaakt als er een oplossing is, omdat cybercriminelen vaak sneller een aanval uitvoeren, dan dat er een oplossing voor het probleem beschikbaar is. Hierbij moet de beveiligingsonderzoeker het probleem op vertrouwelijke wijze rapporteren aan het desbetreffende bedrijf. Daarnaast moeten hij en het bedrijf in goed vertrouwen een periode bepalen waarin een oplossing wordt ontwikkeld. En tot slot maakt de onderzoeker, wanneer de oplossing beschikbaar is, het probleem dan publiekelijk bekend.
Aangezien er dagelijks belangrijke beveiligingsproblemen worden in veelgebruikte software, is het duidelijk: deze discussie dient opnieuw gevoerd te worden.

Over de auteur
Wolfgang Kandek is Chief Technical Officer, Qualys