Cybersecurity innoveert!

Nieuwe dreigingen vereisen een nieuwe aanpak. De cybersecurity-industrie bewandelt dan ook nieuwe paden, met aandacht voor 'big data', artificiële intelligentie en een rist nieuwe ideeën.

Guy Kindermans

Naast de bestaande en gekende securityproducten hebben de voorbije jaren een aantal start-ups alternatieven ontwikkeld om zakelijke en industriële informatie-omgevingen te beveiligen. Een deel van hen presenteerden zich op de twintigste editie van NetEvents, in het hart van Silicon Valley.

GECONTESTEERDE AI

Het meest in de kijker liep Cylance, een securitybedrijf uit Irvine, Californië, dat 'artificiële intelligentie, een algoritmische aanpak en machine learning' aanwendt om eindgebruikerssystemen te beveiligen. Dankzij die aanpak zouden de systemen zonder (of met minimale) updates ook tegen 'zero day' aanvallen (op basis van nog ongekende kwetsbaarheden) beschermd zijn. Cylance 'berekent' het potentiële gevaar van een element (een code, een bestand enzovoort) op basis van een groot aantal kenmerken. Het bedrijf werd mee opgericht door 'Hacking exposed'-co-auteur Stuart McClure en onderstreept dat met zijn product het datalek van 21,5 miljoen militairen en nationaal veiligheidspersoneel bij de Amerikaanse overheid werd ontdekt.

Op NetEvents meldde het Canadese Wedge Networks (Calgary, Alberta) dat het een licentie op Cylance's technologie heeft genomen, om in netwerken een 'advanced malware block' aan te bieden. Zo worden ook niet-Windows systemen beschermd, inclusief het gebruik van persoonlijke toestellen (BYOD). Het zou bovendien mogelijkheden openen in het Internet of Things.

Van de 'next generation' securityproducten is Cylance evenwel ook een van de meest omstreden. Zo wijzen onder meer de 'klassieke' antivirusbouwers op Cylance's onwil om deel te nemen aan gereputeerde vergelijkende producttesten, terwijl informele vergelijkende testen de superioriteit van Cylance ten opzichte van klassieke AV-producten niet meteen aantonen, wel integendeel.

MISLEIDING EN ISOLATIE

Het uit Israël afkomstige Javelin Networks hanteert een andere aanpak om uiterst snel inbrekers of malafide interne medewerkers te ontdekken. Daarvoor bezaait Javelin een bedrijf met een groot aantal 'valse' systemen, met ogenschijnlijk echte data en dies meer. Na de inbraak doorzoekt een aanvaller steevast de systeemomgeving en als hij daarbij een van de valse systemen bezoekt, verraadt dat meteen zijn aanwezigheid. Vervolgens kunnen de securitydiensten van het bedrijf hem volgen (onder meer voor forensische doeleinden) en uiteindelijk zijn aanval verijdelen. Javelin positioneert zich als alternatief voor 'intrusion detection' en 'deep packet inspection' systemen.

Menlo Security (uit Menlo Park, Californië) mikt met zijn 'isolation platform' dan weer op een veilig internetgebruik door tegen gevaarlijk sites en *(spear) phishing* - aanvallen te beschermen. Daartoe beschouwt het bedrijf ronduit alle elementen van buitenaf (zoals bestanden en mails) als *bad* en controleert het die in strikte isolatie op tientallen verdachte kenmerken. De gebruiker krijgt enkel een veilig beeld van dat element te zien. Desgewenst kan de interactie ermee worden geblokkeerd door een 'read only' instelling.

Niet dat er op deze NetEvents geen ruimte was voor gevestigde producten. Netwerkbeheerspecialist Netscout, die diensten optimaliseert via een *big data* kijk op netwerkverkeer, verwierf door de recente overname van Danaher Communications onder meer Arbor Networks. Dat is van oorsprong een verdediging tegen DDos-aanvallen, maar Arbor biedt nu in combinatie met de informatie uit de Netscout-producten en de eigen 'threat intelligence' ook mogelijkheden voor proactieve bescherming. De eigen Atlas- (datacorrelatie) en Asert- (data-analyse en *response*) technologieën helpen nu tegen aanvallen beschermen. De cyberaanvallers hebben zeker nog niet het rijk voor zich alleen.