Dit document wordt u aangeboden door:
Office Magazine.nl
klik hier voor meer artikelen

Beschermen in plaats van detecteren

ICT vergroenen – naar groene datacenters en cloud? -
Digitale criminaliteit

Beschermen in plaats van detecteren

Regelmatig wordt de IT-wereld weer opgeschrikt doordat er weer een nieuw virus de kop opsteekt. De figuren die dergelijke virussen ontwikkelen, doen dat omdat ze het op een rare manier leuk vinden, of omdat ze er fors geld mee kunnen verdienen.

Moderne misdaad vindt plaats via de computers en internet. Cybercrime is de algemene term daarvoor, of het nu gaat om identiteits-diefstal of financiële fraude. In beide gevallen is er grof geld mee gemoeid. Met cybercrime is het net zoals met 'gewone' misdaad: ondanks de vele beschermende maatregelen gebeurt het toch, en achteraf kun je die maatregelen weer aanpassen om een herhaling te voorkomen. Heeft het dan geen zin om beschermende maatregelen te nemen?

Geen probleem

De technologische vaardigheden van de ontwikkelaars van wat we met een generieke term malware noemen, zijn inmiddels zo ver gevorderd dat het voor hen eigenlijk geen probleem meer is om computers te infecteren en zo informatie te stelen, of, nog erger: te zorgen dat een geheel netwerk crasht. Daar zit een particulier niet op te wachten, en voor een organisatie kan dit het einde betekenen. Gerichte aanvallen en zogeheten social engineering worden in combinatie met geavanceerde malware gebruikt om computers thuis en op kantoor te infecteren of kapot te maken. Welkom in de wereld van de high-tech misdaad.

Malware kan overigens losjes gedefinieerd worden als elk software-programma dat niet direct of indirect de eigenlijke taak van het computersysteem ondersteunt. Sommige vormen van malware kunnen de invoer en de systeemgegevens van de gebruiker 'kapen' en deze via het internet naar een andere computer ergens ter wereld sturen. Denk hierbij aan zogeheten 'keystroke loggers' (houden bij welke toetsen worden aangeslagen), 'screen-scrapers' (kopiëren wat op het scherm verschijnt) en 'session recorders' (leggen vast wat de gebruiker doet met de pc). De gegevens die hiermee worden gestolen, worden gescand op voor de dief waardevolle informatie, die vervolgens wordt misbruikt of doorverkocht.

Geen compromissen

De aanvallen die vandaag de dag worden uitgevoerd, beginnen gewoonlijk met technisch of sociaal slimme

processen die computers infecteren met malware. Met andere woorden; geïnfecteerde computers geven problemen. Het beveiligen van met het netwerk verbonden computers is tegenwoordig een cruciale taak voor de IT-afdeling en behoort bij veel organisaties tot de speerpunten van hun totale beveiligingsstrategie. Vanuit een technologisch oogpunt bekeken zijn de meeste deskundigen op dit gebied het er wel over eens dat het afschermen van computers tegen infecteren maatregelen vereist op zowel de computers zelf als op het gehele netwerk. Host-based software (op de computer zelf dus) zoals persoonlijke firewalls en anti-malware programmatuur vormen een noodzakelijk onderdeel van het computergebruik. Netwerkgebaseerde technologieën zoals firewalls, inbraakdetectiesystemen en inbraakpreventiesystemen kunnen een sleutelrol vervullen in de beveiliging van de infrastructuur.

In het afgelopen decennium hebben we een evolutie kunnen meemaken op het gebied van de netwerk-gebaseerde beveiliging. Die was eerst gericht op het 'buiten houden van de boeven' met behulp van firewalls en 'laten we eens kijken wat er door die firewall heen kan komen' met behulp van inbraak-detectiesystemen (intrusion detection systems, IDS). Tegenwoordig is het beleid gericht op het buiten houden van de rommel met behulp van state-of-the-art technologieën zoals inbraak preventie systemen (intrusion prevention systems (IPS).

Deze evolutie op het terrein van de netwerk-gebaseerde beschermingstechnologie werd geïnitieerd door de noodzaak om bij te blijven bij de zich razendsnel ontwikkelende wereld van bedreigende software. De huidige, meest moderne systemen die gebruik maken van hoogwaardige netwerk IPS-technologie waarmee bedreigingen kunnen worden gedetecteerd en geblokkeerd, kunnen uiterst effectief zijn in het terugdringen van het risico dat beschermde computers worden geïnfecteerd. Echter, IDS- en IPS-technologieën hebben gewoonlijk dezelfde eigenschap die hun uiteindelijke effectiviteit kan beperken. Ze zijn namelijk gewoonlijk gericht op het identificeren van de schadelijke en/of malafide netwerk-transacties, en het blokkeren hiervan.

Onlangs bracht IDC Research een rapport uit waaruit bleek dat technologieën zoals inbraakdetectiesystemen slechts 70 procent van alle inbraken opmerkt. Waarmee is bewezen dat ook die inbraakpreventiesystemen niet geheel effectief zijn en het netwerk dus nog steeds niet waterdicht is. Hoeveel dijken en sluizen je ook opwerpt, een hacker kan blijkbaar altijd wel een nieuw gaatje vinden om binnen te komen. Deskundigen op het gebied van netwerkbeveiliging zijn het er wel over eens dat echte beveiliging pas wordt gerealiseerd door middel van opleiding, procestraining en met een gelaagde benadering van technologie.

Instelling

Voorkomen is beter dan genezen. Met de blik gericht op de toekomst kunnen organisaties hun perspectief beter uitbreiden van het detecteren van bedreigingen naar het voorkomen, dus het afdoende afschermen van hun gegevens.

Het implementeren van een strak beleid met betrekking tot encryptie en tot plaatsen waar bedrijfskritische informatie wordt verzameld, bewerkt en/of opgeslagen heeft pas zin als dat beleid ook wordt gehandhaafd, met andere woorden: als er forse sancties staan op handelingen die tegen dat beleid ingaan. Alleen dan kunnen de risico's worden verminderd die gepaard gaan met problemen die ontstaan als er sprake is van fysieke verliezen, zoals de diefstal van laptops, usb-sticks of zelfs van back-up tapes.
Het implementeren van een streng authenticatie- en toegangsbeheer kan de gevaren die van binnen de organisatie komen, verminderen en tevens ongeoorloofde toegang tot gevoelige bedrijfs- of klantengegevens voorkomen. Met het organisatiebreed implementeren van processen voor document klassificatie-systemen kan een basis infrastructuur worden gecreëerd waarin een beleid voor de bescherming van informatie kan worden gehandhaafd.

Bij het verbeteren van de infrastructuur van hun netwerkbeveiliging zouden organisaties technologieën moeten toepassen die verder gaan dan het detecteren van bedreigingen, en een echte bescherming vormen van de gegevens. Inbraakpreventiesystemen die niet alleen toegangscontrole en bescherming tegen bedreigingen bieden, maar daarnaast ook een streng en acceptabel beleid voor het gebruik van applicaties, en zelfs een beleid voor het beheren van documenten (digitaal evenals fysiek) kunnen pas echt zorgen voor een succesvolle bescherming van de gegevens.

De constante toename van geavanceerde, gerichte bedreigingen, het telkens weer ontdekken van 'gaten' in zakelijke software en de grote media-aandacht voor het verlies van gevoelige klanten- en medewerkersgegevens zouden bij alle professionals in de branche een alarm moeten doen afgaan dat ze hun focus zouden moeten richten op de bescherming van gegevens, in plaats van op het detecteren van bedreigingen. Organisaties zouden hun medewerkers meer opleiding en training moeten geven, en nieuw beleid moeten invoeren – en handhaven – voor het omgaan met bedrijfskritische informatie. Tevens zouden ze aanvullende technologische oplossingen moeten invoeren zoals inbraakpreventiesystemen en werkelijk afdoende maatregelen moeten nemen tegen het 'lekken' van informatie. ■

Vrij naar een blog van Mike Paquette, chief strategy officer bij Top Layer.