Infosecurity Europe 2008

TOENEMENDE AANDACHT VOOR SECURTITYOPLOSSINGEN MOBIELE GEBRUIKER

Hoe veelomvattend het arsenaal aan beveiligingsoplossingen rond server, pc, laptop en smartphone tegenwoordig is, was wederom goed te zien tijdens Infosecurity Europe 2008 in Londen. Meer dan driehonderd exposanten gaven er een evenwichtig beeld van het groeiende aanbod van securityoplossingen. *Laurens van Aggelen*

Op de eerste beursdag, 22 april jongstleden, was het al meteen een drukte van belang. Niet verwonderlijk, Infosecurity Europe is uitgegroeid tot het belangrijkste evenement op het gebied van beveiligingsoplossingen in Europa. Nergens vind je zoveel belangrijke en minder grote marktspelers op een beursvloer die overzichtelijker is dan die van de CeBIT in Hannover. Het aanbod van producten gaf een mooi beeld van nieuwe trends en de risico's die gebruikers lopen door de steeds vernuftigere werkwijze van datadieven, spammers en andere onverlaten die de digitale snelweg als een lucratief walhalla zien.

Opvallend tijdens de beurs was de duidelijk toenemende aandacht voor de gevaren die mobiele gebruikers lopen, ongeacht of zij daarbij gebruikmaken van een notebook, pda of smartphone. Hoewel nog wel eens wordt beweerd dat de aandacht voor beveiligingsproducten voor smartphones vooral een marketingtruc zou zijn die gebruikers de angst in de benen jaagt voor gevaren die nauwelijks spelen, is het niet zonder reden dat spelers als Symantec en F-Secure met hun eerste producten voor de dag komen. Hoewel de kans last te hebben van bijvoorbeeld phishing, virussen en malware op smartphones en pda's aanzienlijk kleiner is dan op een pc of notebook, is het verstandig om in ieder geval alert te blijven ten aanzien van de gevolgen die het toenemende risico op den duur met zich meebrengt.

Phishing

Omdat het voor cybercrimelen die uit zijn op financieel gewin op dit moment nog niet erg lucratief is om massaal de aanval op mobiele werkers te openen, is het aanbod van beveilingsproducten voor deze doelgroep nog relatief beperkt. Op de stands van F-Secure en Symantec was te zien dat zij er in ieder geval al wel mee bezig zijn. Zo heeft Symantec de software Norton Smartphone Security ontwikkeld, de eerste mobiele beveiligingsoplossing voor Windows Mobile en Symbian. Daarbij gaat het om een combinatie van Norton AntiVirus-technologie met een firewall en een antispamprogramma voor tekstberichten (sms). Symantec heeft Norton Smartphone Security ontworpen om de gebruikers van smartphones dezelfde veiligheid te bieden als voor laptops en andere computers.

Bij dergelijke oplossingen zou je je wel af kunnen vragen hoe snel gebruikers van mobiele apparaten tot de aanschaf van dergelijke producten te bewegen zijn. Uit onderzoek van G DATA blijkt namelijk dat bijna de helft van alle pc-gebruikers nog altijd zonder bescherming over het net surft. Volgens G DATA veroorzaken cybercriminelen jaarlijks miljardenschade door diefstal, verkoop en misbruik van gestolen data. Daarbij heeft de datadief het steeds meer voorzien op het ontfutselen van online-identi-

teiten en specifieke informatie die op het systeem van de gebruiker staat.

De demo's die we tijdens Infosecurity Europe zagen over het misbruiken van online-identiteiten, was ontluisterend. Daarnaast werd geïnteresseerden getoond hoeveel we zelf eigenlijk onbewust over onszelf prijsgeven door deel te nemen aan allerlei netwerksites zoals Hyves en LinkedIn. Om gerichte phishing-aanvallen te doen, is het daardoor een fluitje van een cent geworden om via Google belangrijke informatie over een persoon bij elkaar te zoeken. In de demo die we zagen, ging het om persoonlijke gegevens die we liever niet aan de grote klok hangen, maar die toch boven water te halen zijn. Veelal doordat we bij het gebruik van internet nog altijd onderschatten dat onze privacy aardig op de tocht is komen te staan.

Malware

Op de stand van Kaspersky was er behalve aandacht voor de gevaren die mobiele werkers lopen, ook de mogelijkheid om presentaties bij te wonen waarbij werd ingegaan op de evaluatie van malware. Volgens experts van Kaspersky Lab zal er dit jaar een vertienvoudiging plaatsvinden van nieuwe malware. Kaspersky verwacht in 2008 maar liefst één miljoen nieuwe signatures toe te voegen die de ruim twintig miljoen nieuwe kwaadaardige programma's moeten neutraliseren.

Het antwoord van Norman op deze ontwikkelingen is Norman Network Protection (N.N.P.), een antimalware-gateway die de netwerkinfrastructuur van organisaties beschermt tegen aanvallen van bekende en onbekende malware. N.N.P. beschermt het netwerk van binnenuit. Zowel intern als extern netwerkverkeer wordt gescand, waardoor malwarebesmettingen van binnenuit voorkomen worden. Dit gebeurt in realtime, in tegenstelling tot de gebruikelijke proxytechnieken, waarbij data gebufferd wordt. N.N.P. biedt een gedetailleerde malwareanalyse van nieuwe of onbekende malware, zoals virussen, wormen, Trojaanse paarden en spyware. Daarnaast is er sprake van een actieve bescherming met blokkering en uitsluitingen op IP, Mac-adres en VLAN-niveau. Scannen van binnenkomende én uitgaande netwerkdatastromen is mogelijk voor diverse protocollen (FTP, HTTP, SMTP, POP_3, RPC, TFTP, IRC en CIFS/SMB). Ook is in malware-uitbraakbeveiliging en schadecontrole voorzien.

Software- en contentprotectie

Ook aanwezig op Infosecurity Europe was Wibu-Systems, ontwikkelaar van DRM-technologie (Digital Rights Management) voor het beheren van licenties en gebruikersrechten. Het product dat daarbij hoort heet CodeMeter (CM). Het is een prima oplossing voor de elektronische distributie van software en IP-content, zoals elektronische boeken, muziek en ontwerpgegevens. Op een CM-stick kunnen tot duizend licenties worden opgeslagen. Het werkt als volgt. Een gebruiker koopt eenmalig zo'n CM-stick. Vervolgens downloadt hij via internet de betreffende beveiligde software die hij wil hebben. Hij heeft op dat moment dus nog geen licentie en kan de software nog niet gebruiken. Nadat hij de CM-stick op zijn pc heeft aangesloten, surft hij naar de website van de verkoper van de software, bestelt de software en betaalt ervoor, waarna de licentie en de activeringssleutel op de CM-stick worden bewaard. De gebruiker kan de software nu offline gebruiken. Hij hoeft daarvoor alleen de CM-stick met de licentie op zijn pc aan te sluiten.

Op Infosecurity Europe presenteerde Wibu zijn onlangs gelanceerde uitbreiding op het CodeMeter-concept. Het betreft CodeMeter Identity, een two-factor authenticatieoplossing die op diverse vlakken kan worden toegepast. Wibu oppert als meest voor de hand liggende toepassing het leveren van SaaS (Software as a Service) of documenten aan een selecte 'geauthentiseerde' groep gebruikers. •

ENDPOINT DEVICE CONTROL WAAKT OOK OVER OUTPUTPRINTER

"Het lekken van bedrijfsgevoelige informatie via de lokale poorten of door het uitprinten ervan, gebeurt sneller en vaker dan door netwerkaanvallen en onvolkomenheden in software", aldus Alexei Lesnykh, Business Development Manager bij DeviceLock. Voor de Europese pers was er tijdens Infosecurity Europe 2008 de introductie van DeviceLock 6.3. Ten opzichte van de eerdere versies van deze eindgebruikers-toegangscontrolesoftware zijn er een aantal belangrijke nieuwe features toegevoegd. De belangrijkste, zeker ten opzichte van wat de concurrentie te bieden heeft, is dat nu ook voorzien is in het schaduwen van lokale, netwerk- en virtuele printers. Primair was de software altijd bedoeld voor het monitoren en het voorkomen van het kopiëren van documenten daar waar dit binnen een organisatie niet wenselijk is. Daarnaast biedt de software ook de mogelijkheid om per gebruiker of gebruikersgroep te definiëren wat er tijdens het synchroniseren van een pda, met Windows Mobile of Palm als besturingsysteem, wel en niet uitgewisseld mag worden met de desktop- of notebook-pc op kantoor. Dit om te voorkomen dat bedrijfsconfidentiële informatie, al dan niet moedwillig, in verkeerde handen terecht kan komen.

Tijdens de demo liet een woordvoerder van DeviceLock ons weten dat er later dit jaar ook een versie van deze software beschikbaar zal komen voor toestellen die Symbian als OS gebruiken, zoals ook het grote legioen BlackBerry-gebruikers van een eigen versie zal worden voorzien.

Met DeviceLock 6.3 focust DeviceLock, de endpoint-solutionleverancier die tot voor kort nog onder de naam SmartLine opereerde, op zowel kleine als grote bedrijven. Het instellen van de rechten die gebruikers binnen een netwerk hebben, is vrij eenvoudig en vraagt geen diepgaande kennis van beveiligingstechnologie of wat dies meer zij. Alle op een netwerk aangesloten computers kunnen centraal worden voorzien van de instellingen die voorkomen dat belangrijke informatie naar buiten zou kunnen lekken. Een gebruiker die inlogt krijgt steeds automatisch een eventuele update op zijn systeem binnen met daarin besloten de eventuele wijzigingen van toegangsrechten. Bij het synchroniseren met een pda of smartphone kan door de systeembeheerder of securitymanager uitgebreid worden gedefinieerd wat er bij het synchroniseren overgezet mag worden, zoals de agenda, contactgegevens en attachments.

Met DeviceLock is het mogelijk om de aanwezigheid van elk soort mobiel apparaat te detecteren, ongeacht welke lokale interface ermee in verband staat. Daarnaast kan de beveiligingsverantwoordelijke ook de installatie of de uitvoering van toepassingen op mobiele apparaten centraal blokkeren of toestaan. Daarbij ondersteunt DeviceLock op gedetailleerd niveau het registreren, schaduwen, controleren en rapporteren van alle soorten data die heen en weer gaan tussen pc's en mobiele apparaten.