

Spyware voorkomen is beter dan genezen

Iedereen kent inmiddels het verschijnsel computervirus of Trojaans paard en weet dat je om je daartegen te beschermen niet alleen antivirussoftware moet installeren maar deze ook regelmatig moet opwaarderen. Virussen zijn niet het enige probleem dat vanuit internet kan binnendringen; internetgebruikers worden ook geconfronteerd met spyware. Voor de meeste privé-gebruikers is spyware nog geen probleem. Voor organisaties ligt dat anders. Veel medewerkers gebruiken beroepsmatig internet en kunnen ongewild ook spyware op hun werkstation ophalen. Een besmetting van minimaal twee spyware-programma's per werkstation en een terugval van 10 procent van de prestaties van het bedrijfsnetwerk is naar onze ervaring in de praktijk geen uitzondering. Dit kan een flinke verlaging van de productiviteit van de medewerkers die afhankelijk zijn van het netwerk veroorzaken.

Vele gedaantes

Spyware-besmetting richt zich net als virussen op de werkstations, op het eindpunt van een verbinding. Versleuteling van verbindingen naar het netwerk kan het lekken van gevoelige informatie door spyware niet voorkomen. Het is dan ook zaak om het bereik van de netwerkbeveiliging te verleggen naar de eindpunten en het voorkomen en bestrijden van spyware daarin op te nemen.

Volgens een definitie van de Amerikaanse overheid is spyware een programma dat (onder valse voorwendsels) op een computer is geplaatst en de activiteiten daarop bekijkt of persoonlijke informatie doorsluisst naar een derde partij.

Spyware heeft vele gedaantes. De 'onschuldigste' versie is een cookie dat clickgedrag op websites registreert en doorstuurt naar een bepaalde internetserver om zo marketinginformatie verzamelen (al dan niet geanonimiseerd). Soms kan dit ook tot gevolg hebben dat ongewilde advertenties op het beeldscherm worden geplaatst. Dan spreken we van adware. Alleen al deze besmetting kan het starten van een werkstation met een factor twee vertragen.

Afstandwerkers

Een volgende besmettingsbron vormt freeware: gratis programma's die populair zijn bij privé-pc-gebruikers. Dat weten freeware-ontwerpers ook. Ze bundelen vaak spyware met freeware om zo hun software te sponsoren en geven dat ook aan in hun eindgebruikerlicentieovereenkomst. Soms is de gebruiker zich niet bewust van de gevolgen hiervan, maar het komt ook voor dat hij bewust deze spyware accepteert omdat hij het betreffende programma graag wil gebruiken. Kazaa is een voorbeeld van een p2p-programma (peer-to-peer) dat spyware installeert. Niet alleen de software om p2p-netwerken te benaderen, maar ook de netwerken zelf zijn bronnen van spyware. In illegale software die via deze netwerken wordt uitgewisseld, voegt de aanbieder soms spyware toe. Een nietsvermoedende gebruiker installeert dan niet alleen illegale software, maar ook de bijbehorende spyware.

Lang niet alle medewerkers zijn intern aangesloten op het bedrijfsnetwerk. Vanwege hun mobiliteit hebben ze vaak op afstand toegang nodig. Tot voor kort staken organisaties veel energie in beveiliging van die verbindingen. Een versleutelde verbinding via internet voor beveiliging van uit te wisselen gevoelige gegevens is echter niet meer voldoende. Spyware op een werkstation op afstand kan deze data onderscheppen op het eindpunt en daarmee de beveiliging van de verbinding onderuithalen. Een aanvaller die specifieke informatie zoekt, verlegt daarmee zijn bereik van het netwerk naar het eindpunt. Om adequaat te reageren op deze ontwikkeling moeten organisaties het bereik van de beveiliging eveneens uitbreiden naar het werkstation. Dit geldt niet alleen binnen de organisatie, maar ook voor alle werkstations die verbinding kunnen maken met het haar netwerk.

Speciale aandacht verdienen de thuiswerkplekken van waaraf een werknemer een verbinding kan opzetten met het bedrijfsnetwerk. Een medewerker kan buiten werktijd op zijn laptop tijdens het surfen op een kwaadaardige website terecht komen. Daarnaast kan je van medewerkers niet verwachten dat ze op hun privé-pc geen freeware installeren. De meeste mensen hebben wel een virusscanner op hun werkplek op afstand, maar die kan meestal de installatie van spyware niet voorkomen. De kans dat een werkplek op afstand (bedrijfs-laptop of privé-pc) besmet raakt met spyware is dan ook veel groter dan bij een werkplek binnen de organisatie.

De consultants van Secure Connection BV kunnen uw adviseren omtrent geïntegreerde virus-oplossingen. Denk hierbij bijvoorbeeld aan de implementatie van een organisatiebrede antivirus policy. Deze toepassing zorgt voor een veilige afstemming tussen bedrijfsnetwerk en thuiswerkplek.

Bron: www.computable.nl

Actueel

17 november 2005

Spyware nog gevaarlijker!

Spyware is nog altijd een van de grootste bedreigingen op het internet waar gebruikers meer te maken kunnen krijgen, zo waarschuwt Webroot in haar State of Spyware Report. Dit kwartaal waren de grootste spywarebedreigingen actiever en gevaarlijker dan ooit tevoren. De afgelopen zes maanden gebruikte spywareverspreiders steeds vaker encryptie algoritmes en code van Trojaanse paarden om hun software te verstoppen.

Spyware kan zich hierdoor net als virussen installeren, en doordat sommige dreigingen over polymorfische engines (engines die zich in meerdere vormen kan presenteren) beschikken zijn er nieuwe oplossingen voor detectie en verwijdering nodig.

Webroot ziet als grootste spywarebedreigingen van dit moment:

- CoolWebSearch
- AbetterInternet
- EliteBar
- ISTbar
- Look2Me
- ShopAtHomeSelect
- SurfSideKick
- VirtuMonde
- WebSearchToolbar
- 180SearchAssistant

Verder komt uit het rapport naar voren dat 8% van alle kantoor PC's met spyware geïnfecteerd is en 1,5% met trojaanse paarden.

Bron: www.headliner.nl