



### De risico's van de zakelijke werkplek

Dat de mens de grootste risicofactor is, is bekend. Regelmatig verschijnen er rapporten waaruit blijkt dat er nog veel aan het beveiligingsbewust gedrag van mensen valt bij te sturen.

Zo heeft Surf Control onlangs een rapport uitgebracht: "Trust and Risk in the Workplace". Het onderzoek is door Dr Monica Whitty aan de Queens University in Belfast uitgevoerd en betreft het gedrag van mensen m.b.t. de (zakelijke) werkplek.

Het onderzoek is uitgevoerd onder 1058 personen uit Australië, Singapore, Engeland, de VS en Nederland.

Uit het onderzoek is gebleken dat 2/3 een USB stick gebruikt in combinatie met de zakelijke PC.

Verder bleek dat 26% wel eens muziek download op de zakelijke PC, terwijl 21% wel eens computerspelletjes speelt op de PC van de zaak.

Meer dan 50% gebruikt de PC tevens voor telebankieren. Ook het gebruik van Instant Messaging (MSN, Yahoo etc) op de zakelijke PC komt relatief veel voor: 46% van de mannen en 35% van de vrouwen.

Tegelijkertijd wordt de PC gebruikt voor het verzenden van gevoelige (zakelijke) data via de email. Bedacht moet worden dat de werkelijke percentages wel eens hoger kunnen liggen, omdat vaak het effect optreedt van het geven van sociaal gewenste antwoorden.

Het rapport is te downloaden op de site van surfcontrol:

[http://www.surfcontrol.com/uploadedfiles/SurfControl\\_trust\\_and\\_risk.pdf](http://www.surfcontrol.com/uploadedfiles/SurfControl_trust_and_risk.pdf)

#### Beleid m.b.t. bedrijfsgegevens

Een benadering die vanuit beveiliging vaak wordt genomen is het zo veel mogelijk dichtzetten van de PC. Zo kunnen USB poorten worden dichtgezet voor mass storage devices en kan worden voorkomen dat software wordt geïnstalleerd. Ook kan een antivirusbeleid en een patchbeleid voor security fixes worden afgedwongen.

De vraag in hoeverre een zakelijke PC moet worden dichtgezet versus de vrijheid van de gebruiker en functionaliteit van de PC, blijft altijd een belangrijke vraag.

Voorstanders van de benadering vanuit de eigen verantwoordelijkheid van de gebruiker willen vooral de nadruk leggen op bewustwording.

Deze benadering blijkt in de praktijk niet voldoende te werken. Een combinatie van technische maatregelen, bewustwording, een sanctiebeleid m.b.t. het niet nakomen van afspraken over het gebruik van de PC en controle mogelijkheden (surfgedrag, controle op lokaal geïnstalleerde software) geeft in de praktijk de meest optimale beveiliging.

Van belang is dat er in organisaties wordt nagedacht over het beleid m.b.t. bedrijfsgegevens. De vraag moet worden gesteld of (kritische) bedrijfsgegevens lokaal op mobiele apparatuur zoals laptops of PDA's en op mass storage devices thuis horen, dan wel alleen in encrypte vorm lokaal mogen worden opgeslagen. Ook moet worden nagedacht over de uitwisseling van deze gegevens.

#### Instant messaging

Een ander fenomeen wat steeds populairder wordt in het zakelijk gebruik is instant messaging (IM). Gartner verwacht dat in 2001 instant messaging met tekst, voice en videomogelijkheden de defacto communicatiestandaard zal zijn in het zakelijke verkeer. De populaire instant messaging software, zoals MSN blijkt gevoelig voor aanvallen.

Naast het security issue m.b.t. IM zelf zal ook moeten worden nagedacht op welke wijze informatie uitwisseling moet plaatsvinden en moet worden beveiligd. Het is verstandig om na te denken over een IM security beleid.

Bronnen:

[http://www.surfcontrol.com/uploadedfiles/SurfControl\\_trust\\_and\\_risk.pdf](http://www.surfcontrol.com/uploadedfiles/SurfControl_trust_and_risk.pdf)

<http://www.gartner.com/it/page.jsp?id=507731>

#### Nieuws op assutools.com

In de siteline kunt u een en ander lezen over Cross Site Request Forgery technieken. Lees op onze site: <http://www.assutools.com/news/strategies/cross-site-request-forgery.htm> meer over dit type aanvalstechniek.

### Actueel

Beveiligingsystemen gevoelig voor CSRF aanvallen

Checkpoints safe@office apparaten (geïntegreerde routers / firewalls) bleken gevoelig voor Cross Site Request Forgery (CSRF-) aanvallen.

Indmiddels is deze vulnerability overigens gefixed. Check Point heeft de Safe@Office firmware version Embedded NGX 7.0.45 GA Release uitgebracht om het probleem op te lossen.

Indien een slachtoffer tegelijkertijd via de web browser is ingelogd op zijn checkpoint apparaat en naar een kwaadaardige site surft met de bewuste malware, kon vanaf deze site de besturing van het betreffende checkpointapparaat worden overgenomen. Het is ook mogelijk om, indien de gebruiker bijvoorbeeld het default wachtwoord van de firewall / router nog niet heeft gewijzigd om via de browser van de gebruiker in te loggen op de firewall / router. De remote access toegang kan vervolgens worden opengezet, waarna er vrij toegang is tot het apparaat. De gevoeligheid voor cross site request forgery ontstaat doordat de website de user die is ingelogd vertrouwt. Een CSRF aanval is bijvoorbeeld een form met een nieuwe user. Omdat de website de user vertrouwt zal deze gewoon worden uitgevoerd.

Calyptix Security, die de ontdekking heeft gedaan geeft aan dat het zeker is dat er nog veel meer router / firewall apparaten zijn die gevoelig zullen zijn voor dit type aanvallen.

De beste remedie is om het default wachtwoord altijd te wijzigen én niet gelijktijdig ingelogd zijn op de firewall / router en naar het internet browsen.

Bron:

<http://labs.calyptix.com/CX-2007-04.php>