

Artikel De toekomst van beveiliging is een tank

Door Redactie security.nl op maandag 29 oktober 2007 11:42

De stelling van deze week is afkomstig van security architect Sjaak Laan.

De meeste bedrijven slaan hun data op in hun eigen rekencentra. Om deze data te bereiken, moeten gebruikers worden geauthenticeerd op servers en door firewalls worden geleid. De dataopslag lijkt op de opslag in een kasteel. Kastelen hebben dikke en hoge muren en hebben een poort die bewaakt wordt door een poortwachter. De poortwachter zorgt dat alleen bekende mensen naar binnen komen.

Dit model van dataopslag werkte tot voor kort vrij goed, maar mensen willen ook buiten de kantoor muren kunnen werken en moderne aanvallen komen niet meer van buitenaf, maar van binnen af. Als mensen PC's, PDA's, laptops en smartphones gebruiken die niet door het bedrijf worden beheerd, is het erg lastig een betrouwbare authenticatie te krijgen.

Dit is waarom steeds meer partijen onderzoeken of het mogelijk is de data zelf te beschermen, in plaats van de toegang tot de data. Dit lijkt op het plaatsen van al je data in een legertank. De tank kan vrijelijk rondrijden, maar de data binnenin is beschermd en kan niet bereikt worden. Als dit wordt doorgevoerd, zijn er geen firewalls meer nodig om data te beschermen. Het is zelfs niet meer nodig om data binnen de bedrijfsmuren te houden en bedrijfs PC's kunnen direct aan het Internet gekoppeld worden, net zoals de thuis PC's van de werknemers. De stelling van deze week luidt derhalve: **De toekomst van beveiliging is een tank**

UBM Global is het met deze stelling eens, en heeft daarvoor de volgende DriveLock edities:

- *DriveLock Basic. Poort- en randapparaatcontrole en autorisatie plus netwerkprofielen.*
- *DriveLock Encryption. Versleutelen van informatie op verwijderbare drives.*
- *DriveLock Security Reporting Center. Verzamelen en rapporteren van DriveLock events.*
- *DriveLock Application Filter. Applicatiecontrole en -autorisatie.*
- *DriveLock Terminal Services. DriveLock functionaliteiten voor Terminal Server sessies.*