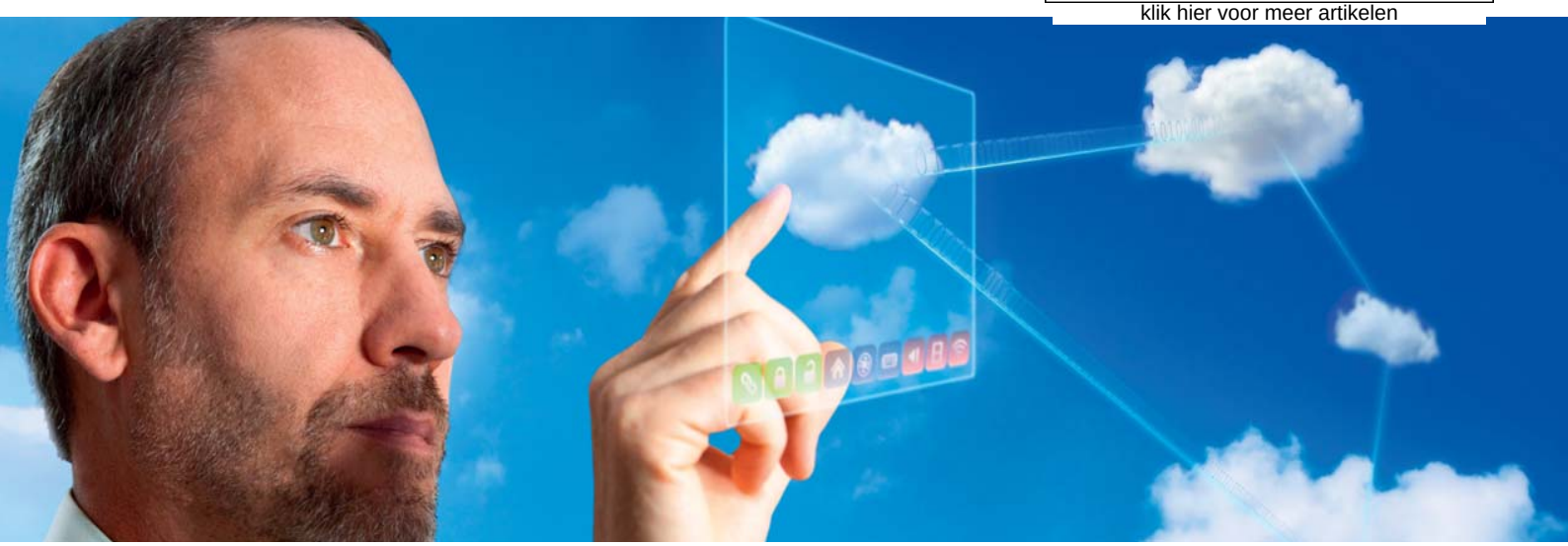

Profiteren van mobile computing alleen mogelijk als risico's worden onderkend

RSA, de security-divisie van EMC, heeft een onderzoeksrapport van de Security for Business Innovation Council (SBIC) onthult. In het rapport gaat de adviesraad in op hoe bedrijven moeten omgaan met de toenemende risico's van mobiele bedreigingen. Deze ontwikkelen zich snel en veranderende technologieën zorgen voor nieuwe zwakheden in de beveiliging.

Ook krijgen steeds meer consumententoestellen toegang tot het bedrijfsnetwerk en slaan deze zakelijke informatie op. Dit leidt echter ook tot potentieel grote consequenties. Bedrijven zouden daarom risicomanagement moeten integreren in hun mobiele visie. Volgens de raad is profiteren van de kansen van mobile computing immers alleen mogelijk als bedrijven de risico's kennen en weten hoe ze deze moeten beheren.

Het rapport "Realizing the Mobile Enterprise: Balancing the Risks and Rewards of Consumer Devices" is samengesteld op basis van de kennis en praktijkervaringen van 19 vooraanstaande security-deskundigen. Deze zijn werkzaam bij onder meer eBay, ABN Amro, Intel en Coca-Cola. Het rapport identificeert de belangrijkste risicobronnen voor mobiel zaken doen en werpt een blik op de toekomst. Het gaat daarbij onder meer in op kritische vragen als: Wat zijn de belangrijkste beleidsbeslissingen ten aanzien van mobiel en wie zou deze moeten maken? Wat moet er opgenomen worden in een zogenaamde Bring Your Own Device overeenkomst? Wat zijn de vereisten voor het ontwerpen van veilige mobiele apps?

Vijf strategieën

De adviesraad presenteert daarnaast vijf strategieën voor het ontwikkelen van effectieve en flexibele mobiele programma's:

Stel mobile governance in – Organisaties moeten teams uit verschillende disciplines betrekken om basisregels op te stellen. Ieder mobiel project moet starten met het opstellen van bedrijfsdoelen inclusief de verwachting voor kostenbesparingen of extra omzet. Daarbij moet het risiconiveau dat bedrijven hierbij willen accepteren vastgesteld worden.

Maak een actieplan voor de korte termijn – Mobiele beveiligingstechnologieën ontwikkelen zich snel wat het lastig maakt voor bedrijven om security-investeringen voor de lange termijn te doen. In het rapport geeft de adviesraad de belangrijkste stappen die in de volgende 12-18 maanden moeten worden gezet.

Bouw aan kennis over de beveiliging van mobiele apps – Het vergaren van kennis over de ontwikkeling van mobiele apps is essentieel om de veiligheid van bedrijfsinformatie te borgen. Toch hebben veel teams die zich bezig houden met informatiebeveiliging niet de juiste expertise. Het gaat hierbij immers niet alleen over beveiliging, maar ook om de functionaliteit en architectuur van de app.

Integreer mobility in een lange termijn visie – Veel trends hebben invloed op risicoplanning op de lange termijn. Organisaties moeten hun benadering vernieuwen zodat security ook rekening houdt met flexibele authenticatie, netwerksegmentatie, datagebaseerde beveiligingsbeheer en cloud- gebaseerde ingangen.

Zorg voor up to date kennis en bewustzijn – Security teams moeten continu op de hoogte blijven van de laatste ontwikkelingen in het mobiele ecosysteem. ■