Bedrijven zijn BYOD-bang

Jude F5, 2013-16-12

BYOD en flexibel werken zijn inmiddels gemeengoed bij veel bedrijven, maar het valt niet te ontkennen dat beide door sommigen nog steeds met een zekere scepsis worden bekeken. De beslissing van Yahoo eerder dit jaar om thuiswerken uit te bannen, was voor verschillende andere bedrijven een teken dat initiatieven teruggedraaid moesten worden of voorlopig uit te stellen. De angst voor beveiligingsrisico's is hierin leidend.

Deze zorgen zijn begrijpelijk - er zijn reële beveiligingsrisico's verbonden aan flexwerken en het onbeperkt gebruik van eigen apparaten (en we laten voor het gemak de productiviteitskwestie even buiten beschouwing). Deze risico's zijn echter niet onoverkomelijk en er zijn ook voordelen te behalen voor bedrijven die de risico's weten te ondervangen.

Om passend met de gevaren om te gaan, is het van cruciaal belang dat uw netwerk "context-aware" is. Hiermee bedoel ik een netwerk dat de bron van netwerkverkeer kan identificeren op basis van geografische locatie, type apparaat en authenticatie en dat op basis van die gegevens intelligente beslissingen kan nemen. Stel dat u of een van uw (collega)managers bestanden op de server probeert te openen vanaf zijn laptop. Als de juiste beveiligingssoftware is geïnstalleerd en de netwerktoegang is beveiligd, is dat geen probleem. Maar als de beveiliging van de verbinding of het apparaat niet duidelijk is, zou het netwerk een intelligente beslissing kunnen nemen en alleen-lezen toegang kunnen geven tot de bestanden. Zo kan ongewenste toegang tot het netwerk worden voorkomen terwijl u of uw collega gebruik kan maken van de gewenste bestanden. Dat is een win-winsituatie. Het netwerk is veilig en u kan gewoon doorwerken.

Gebruik van particuliere apparaten is een andere zaak. Een netwerk met besef van zijn context kan helpen om de juiste contentsoorten af te leveren aan een mobiel apparaat (bijvoorbeeld afbeeldingen met een lagere resolutie voor kortere laadtijden bij mobiele apps), maar de beveiligingsimplicaties van een mix van zakelijke en persoonlijke gegevens op hetzelfde apparaat zijn daarmee niet weggenomen. Ik begrijp dat maar weinig mensen het leuk vinden als hun persoonlijke communicatie en bestanden worden gecontroleerd door hun bedrijf, maar dat is vaak de benadering die wordt gehanteerd bij de huidige generatie tools voor het beheer van mobiele apparaten. Het is veel beter om de zakelijke apps en bestanden te scheiden van de persoonlijke. Dit kan door beheer op applicatieniveau in plaats van apparaatniveau door te voeren.

Het beheer van mobiele applicaties voegt een beveiligingslaag toe aan applicaties voor zakelijk gebruik, waarbij gegevens worden versleuteld en alleen veilige verbindingen worden gebruikt. Dit betekent dat bedrijfstoezicht beperkt wordt tot de bedrijfsfuncties van het apparaat, waardoor gebruikers probleemloos hun apparaten voor persoonlijke en zakelijke toepassingen kunnen gebruiken, terwijl het bedrijf beschikt over het benodigde toezicht.

het artikel verscheen eerder op Managersonline.nl op 9 december 2013, via deze link

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com