Personal data management - whose data is it anyway?

Thorsten Freitag, 2013-11-07

IT Pro in the UK recently reported that Gartner is calling for tighter control over personal data management. We all know we should keep our personal and professional data separate and that we need to take the necessary measures to secure it, but many of us are guilty of leaving our data vulnerable to attack. According to a survey F5 carried out at Infosecurity Europe in April, 83 per cent of respondents said they were less than fully confident that their organisation has consistent security and availability policies across their entire IT infrastructure. It seems that many people doubt their data is safe in their company's IT system, yet continue to leave it at risk.

Gartner predicts that 90 per cent of organisations will have personal data stored on IT systems they don't own or control by 2019. That is a vast amount of data which will be a very attractive proposition for cyber criminals who see personal data as valuable in its own right as well as being as a stepping stone to company data. Cyber criminals know that IT departments are tightening security measures on enterprise data and see access via personal data as an easy inroad.

By introducing formal personal data management regulations, employees will know exactly what they can and can't store on company IT systems, protecting their data as well as the business infrastructure. However, while personal data management regulations will doubtless improve the issue, combining this with a network that is contextually aware could help to solve it altogether.

If a business network can identify the source of traffic geographically, by type of device and by authentication, it can make intelligent decisions based on this information. It will understand if an employee is accessing a personal email, company data or using an app – it could also recognise if it's being intercepted by a cyber-criminal. If there was any question over the security of the connection or the device, the network could intelligently protect itself before any damage can be done. The network is secure and the right employees receive the right data, at the right time, allowing them to work efficiently without risk of coming under attack.

Gartner claims that more companies are choosing to entrust external service providers with credit card data rather than having it on their own systems, and this could soon become the case for personal data. Drawing a strict line between personal and professional data is a step in the right direction but context should also play a key role in keeping both types of data secure and available.

Technorati Tags: mobility,access,security,byod,sso,gartner

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