Bring your own device (BYOD) hype

FORESTALLING A FREE-FOR-ALL AT THE WORKPLACE

Nearly every company is having its own experiences on IT issues now, with its employees' growing consumption in this area. More and more employees want to log into the system with their own smartphone or laptop, putting them right in step with the "bring-your-own-device-to-work" (BYOD) trend. The first task is to create secure access to the network.

by Casha Frigo Schmidiger, Publicist

Gartner's 2012 report assigns the BYOD trend a top ranking on this year's list of major hypes. This US market research institute says each new technology goes through five phases. In the middle of the cycle, the technology reaches the "peak of inflated expectations" (before plunging into the "trough of disillusionment").

In many companies, employees are slightly irritated that the IT equipment their employer makes available to them does not keep pace with their own devices and applications that they use in their personal lives. The pressure on IT managers to integrate private devices in the business environment is therefore mounting enormously.

This BYOD concept is gaining significance for companies because its advantages seem quite enticing: employees pay for their own hardware and arrange for support for the devices themselves. But most importantly, this step is supposed to improve productivity, cut costs and increase employee satisfaction. It goes without saying that companies should not lower their security standards in the process.

Diva generation on the rise

The first generation of people using their own devices in the company network is nonetheless a challenge for corporate IT systems[1]. More than one third of this Y-generation (aged 20 to 29) would violate company guidelines prohibiting them from using their own devices during work or for professional purposes. This figure is from a study carried out by Fortinet, a company specialising in network security. The survey was conducted in fifteen countries in May and June 2012 with over 3,800 employees in the above age bracket. The survey emphasises that these employees in particular pay too little attention to the subject of security. The results indicate the urgency with which companies should develop their security strategies to render BYOD activities secure and to manage these activities.

On average, all the employees polled use their private devices primarily because these devices give them constant access to the applications they prefer, particularly social media and private communication tools. Another reason employees openly use their own devices is to show others that they own a status symbol.

Desire for social media beats risk awareness

The first generation of BYOD employees is aware of the associated risks for their company. They believe the biggest risk for the company is a potential loss of data and endangerment from malevolent IT attacks. This risk awareness does not keep them from circumventing the company's guidelines, however, which should be a cause of concern for IT departments. In fact, more than one third of those polled said they already had circumvented or would circumvent the company guidelines forbidding them from using their own devices for professional purposes. India ranked first on this question among the 15 countries in the survey.

Companies faced with big challenges

The survey clearly shows the huge challenges facing companies. Although employees often like to use their own devices for personal convenience at work and also expect to be able to do so, they do not want to hand over responsibility for the security of their devices to the company. In this type of environment, organisations must go beyond mobile device management and gain back control over their IT infrastructure by rendering all data connections fully secure over the corporate network. Companies cannot rely on a single technology to resolve security challenges arising from BYOD. The most effective network security strategy requires detailed monitoring of users and their applications, not just their devices.

Secure remote access is the key

Every company, every authority, thus urgently needs a BYOD strategy to ensure protected communication in its own network. The IT managers must be aware that any of their employees' mobile devices that access the internal company network also have a bearing on sensitive data. They must therefore answer the following questions:

- Should all employees be allowed to log into the company network with their own devices?
- Which services and applications should be able to be accessed from the personal devices?
- Should equal access be given to all types of devices and user profiles or should special treatment be given only to certain devices (e.g. smartphones) and only to certain user profiles?

For instance, some companies grant internal access only to iPhones because they can or want to pay for support and adapted security measures only for this type of device. In addition, the strategy must allow guest users and temporary employees to access data in the network via secure remote access.

Secure Remote Access from Crypto AG

Crypto AG makes available its Secure Remote Access solution for laptops to enable remote access to company data. This solution involves the use of a technology that only shows the "surface" of the given site instead of downloading the actual data at the given site. This "thin client" technology does not allow users to download and save data locally. It is as if one looks at the data through a telescope with encryption protection. Any effected changes occur securely at the physical location of the company's data server that was called and are saved there. This type of processing leaves no traces at all at the local workstation as soon as the connection is terminated. Secure transitions between zones provide the network back home with sufficient protection. Users can process data in the way described above if they employ encryption units HC-7825 or HC-7835 when using commercial laptops.

Secure Remote Access is therefore a solution that ensures protected communication from the outside (remote location) with a laptop over an untrustworthy network (e.g. the Internet). It is an uncomplicated but secure and fully protected solution for communicating from the outside. Secure access to the network exists worldwide.

Source:
[1] Ictk, 4 July 2012