

Security: The devil is in the detail

The Financial Times

Paul Taylor
January 9, 2012

If you ask corporate IT managers what their biggest concern about providing employees with desktop access to cloud-based applications on mobile devices, or enabling employees working remotely to access these applications on their desktop machines, most will answer quickly 'security.'

But are these concerns justified, or simply an excuse from the IT department for restricting access to company networks, applications and data to those inside the firewall perimeter? I posed this and other questions about desktop services to Rainer Enders, chief technology officer for San Francisco-based NCP engineering.

Since 1986, NCP Engineering has specialised in delivering software that allows businesses rises to rethink their secure remote access and overcome the complexities of creating, managing and maintaining remote network access for staff.

Here are Mr Ender's answers:

What are the security issues for companies considering providing their employees with access to desktop services?

Traditional desktop management strategies have to adapt to a more seamless approach that takes mobility into account. Desktop services must focus on key security technologies with endpoint security at its core such as identity management and device management.



The two main security issues with desktops are software downloaded from the internet or brought into the company from outside using portable devices, and devices brought into and connected to the company network.

Mobile and networked devices can be used to breach security by injecting malicious traffic onto the network, bridging the internal network to the outside world. In addition, external portable data storage devices can be used to move sensitive data outside the company where it is uncontrolled and unprotected.

Are these issues the same for remote employees?

Compromises occur most frequently in mobile devices that tend to be out of compliance (not updated with the latest security software) regularly. For stationary remote desktops, the lack of physical security poses a security risk. In addition, because stationary desktops are increasingly being converted into mobile desktops, every traditional office employee is effectively becoming a remote employee

With mobile devices the blind spot for what we call 'thread monitoring' as well as the 'attack footprint' are much larger than with a stationary device that is located within confined network boundaries. In particular, frequent changes in network connectivity - for example LAN, Wi-Fi, public hotspots and perhaps cellular wireless broadband - presents challenges in keeping the device secured, managed and up-to-date.

The exposure to various networks and network neighborhoods represents a tremendous risk potential. Additionally there are more subtle points of security vulnerabilities represented by connection technologies that are unique to mobile devices, such as Infrared, Bluetooth and wireless LAN. And obviously the physical security of the device itself is a major security concern as the device can be lost or stolen.

So how can desktop services best be secured?

It is most important to control all access to the device, and to use both device and port locking. In addition, it is important to always use strong authentication for logon purposes. At a minimum this is a username and password logon, which ideally can be combined with a multi-factor authentication using an access card, a smartcard, or a biometric device. Device locking mechanisms such as screensavers that lock the desktop at regular idle time intervals should be common practice.

At the network security level, network managers have to focus on device management and on device and end user identity. They also need to manage traditional network security functions, such as the perimeter firewall, at the device level. The best approach is to place the emphasis on how the device can protect itself rather than providing a safe network environment which it would take as a given.

A hostile environment should always be assumed, and protection and security measures should be developed and deployed accordingly. Technologies such as managed VPNs (virtual private networks) and client device firewalls, replacing traditional static computer firewalls, should be deployed to control secure network communication.

How about providing services to mobile devices Does this require additional steps to ensure a safe and secure environment?

Mobile devices require even closer monitoring, management and control and specific features and functions should be deployed to assert device security.

Physical security can be addressed by device locking as well as disk encryption and remote wipe functionality. Network security requires a dynamic network protection approach, which can be achieved by a dynamic and managed client firewall deployed in conjunction with a managed VPN.

As for the application and operating system security it is important to maintain up-to-date status of all deployed software on the device, in particular security software such as anti-virus and Internet security software and components. This typically requires an 'endpoint' protection approach that should be tied into the managed VPN service. Endpoint checking combined with remediation and access enforcement constitutes a vital component in mobile device security.

Are private clouds inherently more secure than the public cloud?

No, they are not. Assume the following scenario. In one situation you have a public cloud, a shared and hosted internet datacenter solution, where knowledgeable network security engineers deploy best practices security along with controlled and monitored security. It is equipped with a managed VPN and endpoint security.

In the other case, you have a network system administrator deploying a private cloud using the same type of shared and hosted internet datacenter resources, but under the company's own internal control. This kind of private cloud is often referred to as virtual private cloud. I specifically use this particular type of cloud because it is the most challenging. This implementation lacks critical access security components and as such provides many points of security vulnerabilities.

All things begin equal, with any technology and hosting approach, the devil is in the detail of the implementation.