CAYMANOBSERVER

SECTIONS
>LEAD STORIES
>LOCAL NEWS
>COMMENTARY
>FEATURES
>TODAY'S NEWSFLASH
>OBSERVER'S CORNER

DEPARTMENTS
>EDITORIAL
>ADVERTISING
>DISTRIBUTION
>BACK ISSUES
>OTHER PUBLICATIONS
>OBSERVER BUSINESS AWARDS

SERVICES
>FREE NEWS EMAIL
>CLASSIFIEDS
>SYNDICATION

CORPORATE
>ABOUT OBSERVER
>TERMS & CONDITIONS
>PRIVACY POLICY
>FORUMS POLICY
>COPYRIGHT POLICY

Email this article

Blocking Internet access at work

Micho Schumann of KPMG explains how businesses can block access to certain websites

Almost every organisation has Internet access on their corporate network. Some only grant access to a limited number of employees or to specific web sites, but most service-type organisations grant full access to everyone, from the CEO down to the junior staffers.

An issue discussed more and more is where businesses should draw the line with regards to work-time Internet surfing and the use of chat tools while keeping productivity high and assuring an adequate level of information security.

IT administrators are inclined to allow only the bare minimum Internet access to employees. With chat tools such as MSN Messenger, social networking sites such as MySpace and the use of webmail like Yahoo and Hotmail, there are many security and business risks that need to be managed. Along with security concerns such as viruses, Trojans, spyware and other undesirables, organisations must also consider that Internet use has an impact on worker productivity and consumes valuable and often costly resources such as network bandwidth and disk space.

Unfortunately, there is no silver bullet to determine what is acceptable or not; each organisation must determine what is best for itself. This article should serve as a roadmap for organisations to find the optimal level of Internet access, which balances the use of Internet in the workplace and information security.

The first step

Evaluate what are the real work-related Internet needs of employees, management and IT staff. A designated individual such as an internal auditor, IT manager or individual responsible for information security should hold meetings to determine what the legitimate business needs for Internet access are. This activity should include management and key employees; employees know and understand what tools their job requires.

Consider the level of access granted

Once the review is conducted and the organisation is ready to implement the changes, the consequences must be weighed. Blocking all or almost all Internet access may be counter-productive. Unless there is evidence of widespread abuse of the Internet access, blocking all but email and the internal Intranet, for example, may prompt employees to look for ways to circumvent the controls.This could be done by finding open wireless network connections, using dial-up modems or other more technical means such as using a Secure Shell (SSH).

In a nutshell, SSH encrypts all the data it carries and keeps it hidden from prying eyes, including those of the IT department. In a frequently seen scenario, a technically-inclined employee could use SSH to surf unauthorised web sites covertly. In fact, by connecting to a remote

Other stories in this section
Brac Informatics Centre

Gen X - more cynic than slacker

Over-controlling kills morale

Mobile Internet enhancements due

The growing popularity of online applications

Blocking Internet access at work

computer (for example, a home computer) via SSH, an employee could use that remote computer to surf the Internet unmonitored and with no restrictions. In a second and more sinister scenario, an employee could use SSH to covertly send confidential data to another system somewhere over the Internet. All the IT group would see is an outbound connection with encrypted data; it would be virtually impossible to know what data was sent.

Many organisations have also been struggling with widespread use of instant messaging applications such as MSN (now called Windows Live Messenger) and Yahoo! Messenger. Without any doubt, these applications should be prohibited on a corporate network. The SANS Institute, a well-regarded information security think-tank, lists instant messaging on its annual and widely-recognised list of the leading Internet security attack targets. These applications represent a serious security risk and are a drain on productivity.

Organisations should also consider investing in commercial software or device that filters website access. These applications restrict access to specific sites such as those containing adult-oriented material, pirated software and other material not suitable in the workplace.

Educate everyone in the organisation

Periodically, and when new employees are hired, organisations should offer an information seminar to employees about the risks of using the Internet. This will raise awareness about information security and inform employees that abusing the privilege of Internet access at work is not acceptable. Many organisations have gone the extra step by developing Internet and security policies, which must be read and signed by all employees. When developed, these documents should always be revised by a lawyer.

Get management support

Once the IT group has identified what needs to be restricted, obtaining management approval is critical. As with all IT security initiatives, without strong management support, the project is doomed. If management support is not obtained, individuals with some authority will soon be asking the IT group for exceptions. With management support, IT will have the authority to refuse those requests.

Finally, if the organisation chooses to implement changes and restrict certain levels of Internet access, alternatives should be offered to employees. A popular solution is to offer a few workstations for personal use. With public computers, employees can check their personal email, log into their MySpace profile or have a quick Internet chat with a friend during their break. For security purposes, those public computers should use a separate Internet connection segregated from the corporate network.

In conclusion, restricting Internet access will most certainly generate some complaints. However, with proper planning, management support and education, organisations should be able to maintain the right balance of employee Internet access, productivity and information security.

Micho Schumann is a senior manager with KPMG's IT Advisory group in the Cayman Islands. He can be contacted at michoschumann@kpmg.ky or on 949-4800 for information security questions and consulting services. He holds a masters degree in information systems and is a Certified Information Systems Security Professional and a Certified Information Systems Auditor. He has over seven years of IT security experience working extensively with financial institutions, government agencies and high-technology firms.

The views and opinions are those of the author and do not necessarily represent the views and opinions of KPMG. All information provided is of a general nature and is not intended to address the circumstances of any

particular individual or entity.

HOME | CONTACT US