DEALING WITH DANGERS FROM WITHIN

By Siti Suharti Abu Sujak and Zahri Yunos

National ICT Security and Emergency Response Centre (NISER)

(This article was published in the STAR InTech on 23 March 2006)

Developments in Information and Communications Technology (ICT) and growing dependencies on information systems have made it more difficult to protect and defend confidential and critical data. And, if defending against intruders and their increasingly sophisticated and powerful tools isn't bad enough, ICT security professionals also have to deal with attacks involving people from within the organisation who already have access to the computer systems. These people take advantage of their knowledge and access privileges to infiltrate networks.

Apart from disgruntled employees wishing to express anger or outrage, these insiders may also have other intentions such as stealing information for competitors.

A report by U.S. Secret Service (USSS) & Computer Emergency Response Team Coordination Centre (CERT/CC) on cases between 1996 and 2002 shows that the highest cases involving insiders are sabotage, followed by fraud and information theft mostly in the banking and finance sectors [1].

These threats become greater with the increase in outsourcing programming that involve contractors or suppliers who have been given privileged access to critical information such as company accounts, employees data, system configurations, and others.

Carelessness also leads to certain unprivileged users gaining access to sensitive data after having obtained access information such as usernames and passwords. This is often done by “shoulder surfing” or watching for username and password pairs entered by other users.

Best Practices

Organisations should take preventative measures to protect against these threats before it harms the entire operation and employ certain best practices in the organisations. There are several recommendations that can and should be implemented by organisations:

- ***Screening the Employees***

Most of studies showed that employees become the greatest risks for the access facility they have. As such, organisations should screen or conduct a background check on the employees especially those who are responsible in areas with critical and confidential information by studying their background, work histories and perhaps, their personalities.

- ***Password and Account Management***

A strict password and account management policy should be implemented to ensure that only eligible personnel can access the network. Also, upon resignation or termination, a former employee’s access account must be deactivated immediately.

- ***Security Awareness Training***

Employees should be aware of and understand the issues of information security in their organisations. Organisations should educate their staff on how their actions can threaten the enterprise. Periodic security awareness training is needed for the staff to increase the knowledge in information security such as desktop security and password management.

- ***Monitoring and Audit***

Organisations should employ system monitoring or logging to monitor and audit especially for employees who have privilege to access the system remotely, and ensure that no system irregularity or changes to sensitive information and data.

- ***Backup and Recovery***

To avoid the loss of important data due to accidental deletion or file corruption, a proper backup and recovery strategy should be implemented to ensure organisation's information systems are functioning even in the event of attack.

Conclusion

Threats from intruders within the organisation can cause plenty of damage to a company's computer systems, financial data, business operations and ultimately, reputation. As such, organisations should take preventative measures.

Without firm restrictions and policy enforcement, insider attacks can have far reaching and deeply devastating effects on any business.

REFERENCE

[1] Keeney, Michelle, Eileen Kowalski, Dawn Cappelli & Andrew Moore. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. May 2005. Carnegie Mellon University Software Engineering Institute's CERT Coordination Center and United States Secret Service. November 2005 <*www.cert.org/archive/pdf/insidercross051105.pdf*>.