Information Security Updates

Monthly Update

Security Incident

Hackers hit leading UK climate research unit

On 20 Nov 2009, Reports are coming in that hackers have breached the servers of one of the world's major climate research units (CRU), posting around 61 megabytes of emails and documents to an FTP server in Russia.
(http://www.infosecurity-magazine.com/view/5406/hackers-hit-leading-uk-climate-research-unit/)

Legislative Update

There are no updates in this section.

I. General Users

Case Study

Stanford University Laptop Theft Calls for Proper Data Backup in Enterprises

A laptop at Stanford University was stolen in Jun 2008 that contained over 72,000 pieces of personal data. The authority has led a task force to review the University's policies and procedures for data protection. Thefts of data storage devices are not exceptional. If the theft is taken place in an enterprise, the loss on critical data may create disastrous problems in business operations. Therefore, it is essential to adopt a proper and reliable backup solution in enterprises.
(http://www.prlog.org/10081187-stanford-laptop-theft-calls-for-proper-data-backup-in-enterprises.html)

Mobile devices, such as laptops, smart phones are portable information systems which are often used to store confidential information, such as contact list, passwords, and personal data. While these devices provide a means for convenient information processing and communication, they also pose a risk of data loss in the event of theft or breaches. Below are some good practises to reduce the risk of data loss for your mobile devices.

Dos

- Use password management tool on start-up of mobile devices.
- Keep your mobile devices in a secure place, especially when not in use.
- Install antivirus software and a personal firewall on your mobile devices.
- Use encryption to lock sensitive data on the mobile devices.
- Regularly back up data of mobile devices (e.g. PDA) to a PC to prevent damage from PDA-specific viruses and worms.
- Remember to remove any memory cards before returning a rented mobile device.

Don'ts

- Don't leave a mobile device unattended, even for a moment.
- Don't download or accept programs and content from unknown or untrusted sources.
- Don't allow common wireless connections from unknown or untrusted sources on your device.
- Don't accept unsolicited file transfers from other devices via Bluetooth, SMS, etc.

Read More [1]

Footnote 1:
http://www.infosec.gov.hk/english/yourself/handheld.html

Technology glossary

Wi-Fi encryption

Wi-Fi provides two encryption methods to enhance confidentiality of data traffic: Wired Equivalent Privacy (**WEP**) and Wi-Fi Protected Access (**WPA**).

WEP encrypts data traffic between the Access Point and the client. The **WEP** standard defines a 64-bit WEP key (with 40-bit secret key) or a 128-bit WEP (with 104-bit secret key). The client and the Access Point must agree on a shared key before communication can be established.

WPA, and its second generation version **WPA2**, provide the same function as **WEP**, but **WPA** is much harder to break then **WEP**.

WEP is no longer a good practice in Wireless security. An experienced hacker can break it in minutes. Using **WEP** as Wi-Fi encryption is regarded as a vulnerability nowadays.

II. Management

10 Steps to Creating a Campus Security Master Plan

Incorporating construction plans, ensuring equipment interoperability and determining future security personnel needs are just some of the measures campuses should incorporate to improve their overall safety and security.

1 **Assemble Your Committee** – Build momentum in the development of a physical security program is to create a physical security committee, which consists of members in strategic positions of influence, such as administration, IT, operations, safety, security, risk and planning.
2 **Determine What Must be Protected** – Understand what concerns, risks or fears may exist on campus and why. The responses are often constructive and enlightening.
3 **Think About Your Long-term Needs** – The security master plan's development should also include long-term system compatibility, communication infrastructure, product obsolescence and growing demands on the security staff.
4 **Find Out What Works, What Doesn't** – The committee should survey current operational risk mitigation measures and determine their effectiveness.
5 **Incorporate Campus Construction Plans** – Understand how new buildings, parking lots, garages, walkways and other projects will affect the current physical security master plan.
6 **Can Legacy and New Security Technology Mix?** – With the convergence of new physical security technologies, the integration of existing security hardware into new security platforms can be a challenge.
7 **Determine Security Personnel Needs** – Documenting responsibility, service and deliverables will assist in setting the groundwork of the return on investment (ROI) and temper the overall approval process.
8 **Upgrade Your Security Operations Centre** – The increase in response, consistency and accuracy can make the difference in a variety of situations throughout the campus.
9 **Don't Forget About Your Infrastructures** – Critical infrastructures are areas within the campus that rely on the continuous, reliable operation of a complex set of interdependent infrastructures: electric power, gas, transportation, water, communications and more.
10 **Regularly Audit and Assess Your Plan** –to validate the operation and consistency of the security systems, security processes and protection of assets.

Read More [1]

Footnote 1: http://www.campussafetymagazine.com/Articles/?ArticleID=252

Technology glossary

DMZ - Demilitarized Zone

A DMZ (Demilitarized Zone) is a part of an (or the complete) Intranet which is assumed to match a security standard superior to the network outside of the DMZ. A DMZ usually is separated from other networks (less secure parts of the Intranet and/or the Internet) by a Firewall or a similar way of filtering out potentially harmful network traffic.

Proxy

A Proxy is a special kind of Gateway, acting like a Server when being accessed by a Client. However, instead of servicing a request from a Client, the Proxy forwards the request to a Server, waits for the Server's response, and then sends it back to the Client. A Proxy is often combined with other typical Gateway functionality, such as Firewall or Cache.

III. IT Professional

Best Practices for Firewall

Organizations should be as concerned with the origins and kinds of Internet-directed traffic as they are with incoming requests. Below are some good practises that organizations can improve their risk profile by implementing traffic filtering.

Limit the addresses allowed to send traffic to Internet destinations by configuring policies such as these:

- Only allow source addresses from the IP network numbers you assign to trusted segments behind your firewall(s), including DMZ networks.
- Apply appropriate subnet masks to trusted networks, i.e., masks that are sufficiently long to identify only that fragment of the IP network number that you are using.
- Block broadcasts from traversing the firewall's interfaces. While most broadcasts will not pass across LAN segments, take measures to ensure this is especially true for Internet-bound packets - or packets destined for any untrusted segment.
- Block outbound traffic from VLAN workgroups or entire network segments that have no business establishing client connections to Internet servers.

Limit the destination ports on Internet-directed traffic in the following ways:

- Allow outbound connections only to those services your security and acceptable use policies allow for client hosts.
- If you operate an HTTP proxy, or a proxy system that performs some form of web URL or content filtering, only allow outbound connections through your firewall from the proxies.
- If you provide DNS internally, or use a split DNS, use internal servers as forwarders for your trusted network, and only allow outbound DNS requests from your DNS servers so configured.
- Unless your firewall is participating in routing, block routing protocols at your firewall. This is important for entities which use a firewall to exchange and negotiate PPP over Ethernet (PPPoE).
- Certain network and security vendors use unique ports for proprietary (and secure) management access. Permit these ports only from hosts used by the administrators of such equipment.

Read More [1]

Footnote 1: http://securityskeptic.typepad.com/the-security-skeptic/firewall-best-practices-egress-traffic-filtering.html