Public Service Announcement

Increase in Insider Threat Cases Highlight Significant Risks to Business Networks and Proprietary Information

23 September 2014

Summary:

There has been an increase in computer network exploitation and disruption by disgruntled and/or former employees. The FBI and DHS assess that disgruntled and former employees pose a significant cyber threat to US businesses due to their authorized access to sensitive information and the networks businesses rely on.

Exploitation of Computer Network Access:

The exploitation of business networks and servers by disgruntled and/or former employees has resulted in several significant FBI investigations in which individuals used their access to destroy data, steal proprietary software, obtain customer information, purchase unauthorized goods and services using customer accounts, and gain a competitive edge at a new company. The theft of proprietary information in many of these incidents was facilitated through the use of cloud storage Web sites and personal e-mail accounts. In many cases, terminated employees had continued access to the computer networks through the installation of unauthorized remote desktop protocol software. The installation of this software occurred prior to leaving the company.

Additionally, multiple incidents were reported in which disgruntled or former employees attempted to extort their employer for financial gain by modifying and restricting access to company Web sites, disabling content management system functions, and conducting distributed denial of service attacks.

Insider Threat Definition:

DHS/US-CERT defines the insider threat as a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems.

Costs of Incidents:

A review of recent FBI cyber investigations revealed victim businesses incur significant costs ranging from $5,000 to $3 million due to cyber incidents involving disgruntled or former employees. Businesses reported various factors into their cost estimates, to include: calculating the value of stolen data, Information Technology (IT) services, the establishment of network countermeasures, legal fees, loss of revenue and/or customers, and the purchase of credit monitoring services for employees and customers affected by a data breach.

Recommendations:

- Conduct a regular review of employee access and terminate any account that individuals do not need to perform their daily job responsibilities.
- Terminate all accounts associated with an employee or contractor immediately upon dismissal.
- Change administrative passwords to servers and networks following the release of IT personnel.
- Avoid using shared usernames and passwords for remote desktop protocol.
- Do not use the same login and password for multiple platforms, servers, or networks.
- Ensure third party service companies providing e-mail or customer support know that an employee has been terminated.
- Restrict Internet access on corporate computers to cloud storage Web sites.
- Do not allow employees to download unauthorized remote login applications on corporate computers.
- Maintain daily backups of all computer networks and servers.
- Require employees change passwords to corporate accounts regularly (in many instances, default passwords are provided by IT staff and are never changed).

Additional Resources:

For additional information on the characteristics, behavior, and detection of a potential insider threat, please refer to "Combating the Insider Threat" available at https://www.uscert.gov/security-publications/Combating-Insider-Threat.

Incident Reporting:

The FBI encourages recipients to report information on suspicious activity to the local FBI field office, http://www.fbi.gov/contact/fo/fo.htm or file a complaint online at http://www.ic3.gov.