Information Security Updates

Security Incident Management

Issue 11

Statistical Report

Most Organisations Have Ineffective Security Processes

A survey polled more than 375 attendees at the 2011 RSA Conference and inquired about the effectiveness of critical security processes including incident response.

It reveals that most organisations perceive their log management, compliance reporting, real-time monitoring, forensic investigation and incident response processes to be ineffective or "somewhat effective" at best.

(http://www.thenewnewinternet.com/2011/04/01/survey-most-organizations-have-ineffective-security-processes/)

Related Article

How to Use 'Best Practices' in Security Incident Management

While a security breach is often a surprise, the genesis of how it came about seldom attracts people's attention. Surprise or not, quite often the security breach introduces complex situations that are difficult to remediate in a timely manner.

Although technology can help mitigate risk for an organisation, IT management's effort in security administration of IT networks and systems is of higher importance.

(http://www.eweek.com/c/a/Enterprise-Applications/How-to-Use-Best-Practices-in-Security-Incident-Management/

I. Background

Industry Story

Poor Incident Response Process That Failed to Protect Vital Data

In February 2011, HBGary, a technology security company, was found that its Gmail cloud e-mail service was compromised by an anonymous group. An interview with HBGary CEO, Greg Hoglund reveals that the anonymous group gained access to HBGary's Google-hosted e-mail service through a stolen password. Hoglund became aware that the service was compromised, but was unable to prove his own identity to Google's help desk quickly enough to have the service shut down before the anonymous group had downloaded HBGary's e-mail records.

This security incident was a successful attack against HBGary, not against Google's cloud-based e-mail. Google's standard mechanism for authenticating a customer making service requests involves asking the customer to place a file on its own website. This works well in normal circumstances but failed when HBGary needed to immediately turn off access to its Google services after having already been forced to shut down its own website. No alternate or emergency response mechanisms had been defined in advance. HBGary's management should have realised that attacks were likely and should have tested its incident-response processes

See the article:
(http://www.gartner.com/DisplayDocument?id=1600315&ref=g_sitelink&ref=g_SiteLink)

Security Incident Management Overview

Universities are now relying on sophisticated information systems and infrastructures with high connectivity for daily operations and academic research purpose. The complex nature behind these factors can be easily exploited by malicious parties, which makes security incidents inevitable.

An effective security incident management is a balance of driving the impact of the incidents down, while containing and resolving security incidents as efficiently as possible. A good security incident management will also help universities to prevent future incidents.

Reference:
http://computersecurity.buffalo.edu/presentations-07/shinil-UB_InfoSec_Workshop_Incident_Handling_part1.pdf
https://wiki.internet2.edu/confluence/display/itsg2/Information+Security+Incident+Management+(ISO+13)#InformationSecurityIncidentManagement%28ISO13%29-Overview

Related Article

Creating a Computer Security Incident Response Team: A Process for Getting Started

Keeping organisational information assets secure in today's interconnected computing environment is a true challenge with each new "e" product and each new intruder tool. Most organisations realize that there is no one solution or panacea for securing systems and data; instead a multi-layered security strategy is required. One of the layers that many organisations are including in their strategy today is the creation of a Computer Security Incident Response Team, generally called a CSIRT.

(http://www.cert.org/csirts/Creating-A-CSIRT.html#intro)

Related Article

Why Create a Security Incident Response Process

Combating malicious software in your environment is not just a matter of implementing the right technology solutions. Like all things in the IT world, effectively combating malicious software is a solution that combines those three classic, yet critical elements: people, processes, and technology.

This means that if your strategy is based solely on technology, your strategy is missing the equally critical elements of people and processes. In many ways, incident response process is the most important process element in a comprehensive strategy for dealing with malicious software.

(http://technet.microsoft.com/en-us/library/cc512623.aspx)

II. Management

Security Incident Response, Reporting and Escalation

Management should design an effective and efficient mechanism of detecting security incidents by utilising human resources (e.g. information security professional, trained users, universities' IT security staffs) and various technical controls (e.g. intrusion detection software and data leakage prevention tools). In particular, the following areas should be focused on:

- Defined personnel or team (e.g. IT Service Desk) as single contact point for handling any reported security incidents;
- Detailed procedures for identifying and reporting failures, weaknesses, and suspected activities that may indicate the existence of security incidents;
- Regular mechanism to recognise and detect flaws or vulnerabilities with universities' security measures, including IT internal controls, operational procedures and security tools; and
- Defined criteria for escalating security incidents to appropriate level of management.

Online real-time incident reporting and logging systems are highly recommended to facilitate immediate incident response and investigation. Manual incident logs should be used when the incident reporting and logging systems are out of service during total system failures. Management should also consider incorporating automated security incident detection functionality when developing or implementing new information systems.

Impact Assessment

To maximise the processing efficiency and minimise the incremental resources universities invest in dealing with the security incidents, an assessment should be carried out for each incident to determine the scope and effect over universities. Key factors to be considered for the impact assessment include:

- Whether the security incidents affect single or multiple information systems?
- Will the university suffer from reputation damage, financial loss, service interruption or litigations?
- Are there any inconveniences / distress / loss caused to relevant parties?

Management should establish clear instruction to assign severities for security incidents based on the impact assessment results, which is crucial in determining the next step for universities to handle the incidents.

Security Incident Monitoring

Due to the various characteristics of security incidents, it may take minutes, hours, days or even weeks to resolve them. Therefore, the status and handling stage of each incident should be closely monitored by universities and tracked throughout the whole process until the incident is closed.

Management should mobilise appropriate resources to eliminate any delay noticed in processing the security incidents and to avoid possible escalation in incident impact levels.

References:
https://wiki.internet2.edu/confluence/display/itsg2/Information+Security+Incident+Management+(ISO+13)#InformationSecurityIncidentManagement%28ISO13%29-Overview
http://www.ogcio.gov.hk/eng/prodev/download/g54_pub.pdf

II. Management (Cont'd)

Evidence Collection and Preservation

When security incidents are likely to result in legal proceedings, it is important to clearly document how all evidence, including the compromised systems, has been identified and preserved.

Evidence should be collected and preserved according to procedures that meet all applicable laws and regulations so that it is admissible in court. Whenever necessary, advice or instructions sought from legal staff, computer forensic professionals or law enforcement agencies should be sought by management.

Security Incident Resolution and Closure

Successful resolution of security incidents requires personnel with adequate knowledge and skills. Necessary tools and financial resources should also be made available to the personnel responsible for the incident resolution. Management must provide relevant trainings courses to universities' IT security staffs or engagement information security professionals if required.

Incident reporters and any other affected parties should examine the resolutions to ensure that the security impacts are gone. On the other hand, management should conduct root cause analysis to prevent recurrence of similar incidents in the future.

Post Security Incident Review

After a security incident is closed, it is critical for management to review the security protections and security incident management process, and to consider whether the process can be improved. This is especially valid for new types of incidents, particularly those having severe or costly impact over universities. The following aspects can be considered during the post security incident review:

- Gaps or difficulties encountered during the incident handling process, in terms of resources, information, internal controls and staff skills
- Damage caused by the incident, including monetary cost and reputation loss
- Experiences learnt that can improve the effectiveness and efficiency of the incident handling process

Based on the post security incident review outcome, management should be able to identify:

- Any vulnerabilities in existing security measures
- Any missing security incident management procedures, communications unclear, or stakeholders that were not appropriately considered
- Any undertrained IT security staff or lack of appropriate tools
- Any update to the impact assessment scheme

The ultimate objective of the review is to determine the improvements that lead to prevention of future incidents and reinforcement of existing information security controls.

Statistical Report

Information Security Breaches Survey 2010

This year's survey results show that the business environment is changing rapidly. Social networks and software as a service have moved Internet use beyond websites and email, creating new vulnerabilities. Criminals are also adapting their techniques and cybercrime is becoming more common.

The cost of security breaches appears to be rising fast. The most dramatic growth is in external attacks which have tripled since 2008.

(http://www.infosec.co.uk/files/isbs_2010_technical_report_single_pages.pdf)

Related Article

Insider Attacks: Identify the Anomaly

Few would doubt that insiders – those allowed access to certain IT resources within your organisation – have the potential to wreck considerable damage. That is true whether they are scheming to physically damage IT systems, destroy the data held within them, or steal customer or corporate data to sell to criminals or competitors.

According to Security Watch Survey, 33 percent of respondents view the insider attack to be more expensive than attacks coming from the outside. That is up from 25 percent in the prior year. And, an increasing number, 22 percent, of inside attackers are relying on sophisticated hacker tools, compared to only 9 percent in 2010.

(http://www.securityweek.com/insider-attacks-identify-anomaly)

References:
https://wiki.internet2.edu/confluence/display/itsg2/Information+Security+Incident+Management+(ISO+13)#InformationSecurityIncidentManagement%28ISO13%29-Overview
http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

Related Article

Incident Response: A User's Perspective

As part of any incident response plan it is imperative that you include specific responsibilities and instructions for general computer users.

Users of computing systems serve as the first line of defence against the realisation of a computer security incident. While a majority of user obligations generally tend to fall under the heading of "Appropriate Use", it is just as likely that a computer user may become involved in the spread of a computer virus, or be taken in by a new e-mail hoax.

(http://secureitexpert.com/incident-response/incident-response-from-a-users-perspective/)

Related Article

Incident Response: Lessons Learned from Georgia Tech, the University of Montana, and the University of Texas at Austin

Institutions should not overlook incident response in their overall IT operations, because "knowing how to respond to a security incident – be it a computer worm, hacker, or the mere suspicion of a problem – can save time, money, and even its reputation." Georgia Tech's Mullin concurred. "Incident-response policies are tools to help you to deal with the incident more effectively and more quickly. We were not paralysed when the incident occurred. After you get past the expletives, you have a process to follow. We tune it for the next round and we hope we never need it again – just like insurance."

(http://net.educause.edu/ir/library/pdf/ers0305/cs/ecs0307.pdf)

III. General Users

Roles and Responsibilities of the General User

As the first line of defence, security-conscious users will often be best placed to identify a potential security breach or a weak link. University staff and students should attend the security awareness trainings, workshop or online courses and familiarise themselves with the following:

- **Identification of security incidents** – understand what constitutes a security incident and potential security threats. Also, be able to determine the existence of security incidents and internal control weakness
- **Reporting procedures of security incidents** – understand the procedures to report security incidents and the specific individual responsible
- **Preserving evidence** – understand the importance of maintaining evidence related to security incidents and the proper ways to retain the information for subsequent investigation and resolution

Furthermore, the staff and students are responsible for:

- Report all (suspicious) security incidents to responsible party (e.g. IT Service Desk)
- Respond to requests required by universities' IT security staff, and engaged information security professionals or other incident handling parties for additional information in a timely fashion
- Assist in the resolution of security incidents in a timely fashion
- Examine resolutions and confirming that security incidents have been resolved

Conclusion

An effective security incident management process is not an isolated component, but rather consists of a number of operational and technical elements. These elements provide the necessary functions to support efficient handling of security incidents and continuous improvement on universities' information security environment.

References:
http://www.its.unimelb.edu.au/__data/assets/pdf_file/0004/366043/Roles-Responsibilities-Work-Practices-QRC-v1.pdf