GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Internal SLA (Service Level Agreements) for Information Security

Overview

Information security typically suffers due to a lack of serious commitment by an organization on the prevention side of security breaches. Many systems are compromised even after patches or hotfixes have been publicized. The premise of this must be to understand the relationship between the information technology (IT) team and the information security (IS) team. The information security team must view themselves as customers of the information technology team. The IS teams must also see that their activities are common elements within the IT teams service to the enterprise. IS' three legged stool of Confidentiality, Integrity and Availability certainly coincides with IT's Total Cost of Ownership (TCO) and Quality of Service (QoS) initiatives.

Reactive versus Proactive

The purpose of this paper is to advocate for the establishment of internal SLAs between the Information Technology team and the Information Security team. Internal SLAs should be established for the following reasons:

Security prevention becomes institutionalized within the organization.
Information security remains a relatively immature discipline within most organizations. Incorporating IS into business processes that other departments or teams engage in is always beneficial. The advantage to the SLA approach is that emphasis is placed on substantive analysis of deficiencies so servers, workstations, desktops, and laptops are configured securely prior to deployment into the field.

Staff can be evaluated on their security skill set.
To aid the CIO in fully developing her staff, this process instigates a more complete evaluation of the staff to see if they can fully support the details of the SLA.

Training can be planned to enhance security skills.
This may be considered as a sub-component of the item above, however, it has a somewhat different angle because it puts the emphasis back on the IS team. For example, the IS team needs to determine if in-house or external training is needed or better clarification on policy or procedural issues.

Processes are established for resolving security deficiencies on a regular basis.
The IT organization "fights fires" all the time and unless there is a formal process designated, implementing mundane patches prior to a contingency may be pushed to the bottom of the queue.

Allocation of staff time can better be assigned.
While the IS SLAs will not cover every security related service, clear, documented expectations allow IT managers to better plan their resources. This may be an example of incorporating the security resolution into a trouble ticket for a particular server.

© SANS Institute 2000 - 2005 Author retains full rights.

Allocation of fiscal resources for the amount of security the organization determines it needs. This process presents a clearer, though not complete, picture of the commitment needed by the organization to fulfill its stated IS obligations.

What are SLAs?

Service Level Agreements (SLAs) may come in a variety of forms. These can range from internal agreements between departments or vendor to client agreements. Service Level Agreements for internal entities are also referred to as Service Level Requirements (SLRs). For this paper, SLA and SLR will maintain similar meanings and will be referenced by SLA. The SLA is an agreement between a perceived service provider and a perceived customer. The flavor of the agreement depends entirely on the parties involved. SLAs address the following fundamental questions: what is delivered; where is it delivered; when is it delivered?

In this type of arrangement, the IS team decides what it believes are the most important elements of the program to monitor. If a risk analysis was conducted, the results or recommendations from these reports should be used. A properly deployed defense-in-depth strategy will aid in the IS team's decision on the SLAs to negotiate. The key is to assure the IT teams that the IS program knows exactly what it wants and how it can be fairly measured. Each organization will have different threat vectors and will need to allocate resources in different manners.

There are some additional guidelines on the governance of SLAs. They should be reviewed regularly and changed as needed. These agreements must also be somewhat flexible for both parties without interfering with the integrity of the process. There must be some consideration for dependencies when implementing system related SLAs. One example may include a maintenance contract which requires vendor notification or assistance prior to any changes made on a particular server or application. Finally, while having SLAs begins the codifying process, it will require on-going management from the IS and IT teams.

Critical Areas for SLAs

The information security (IS) team must define the critical areas for the establishment of SLAs with the Information Technology team. This must focus upon those areas which the IT teams have the most profound effect and control to significantly impact the IS program. Additionally, the IS team needs to limit SLAs to the most critical items, otherwise the effect of these agreements is lessened. A risk analysis or a review of previous incidents may point toward the most critical components for a particular organization. The following topical areas should be prevalent in most instances:

Network Scanning

Many IS teams conduct scans to identify vulnerabilities on the network. Identifying the problems is merely the first part of the process. The next step is to determine how the problem should be resolved. The third step is how can it be incorporated into a process so that it should not arise in the future. Many organizations use commercial tools to automate the network scanning process. If ISS Internet Scanner is being used, this product will document vulnerabilities grouped into categories of High Risk, Medium Risk and Low Risk. The Help Index within the ISS Internet Scanner defines risk levels in the following manner.

© SANS Institute 2000 - 2005 Author retains full rights.

High
Any vulnerability that allows an attacker to gain immediate access into a machine, to gain superuser access, or to bypass a firewall. Examples include: A vulnerable Sendmail 8.6.5 version that allows an intruder to execute commands on mail servers, installation of BackOrifice, NetBus or an Admin account without a password.

Medium
References any vulnerability that provides information, degrades performance, or a has a high potential of giving system access to an intruder. Examples include: identification of an active modem on the network, zone transfers, writeable FTP directories.

Low
References any vulnerability that provides information that could potentially lead to a compromise. Examples include: Floppy drive is available to all users, IE may perform insufficient SSL validation, logon and logoff auditing is not enabled.

A value-add to the ISS tool is that it will provide recommendations and instructions on how to fix the vulnerability. In the report, the IT teams may see:

- Configuration changes
- Installation of service packs
- Installation of patches
- ACL (Access Control List) changes
- Registry edits
- Disabling services

The single greatest benefit these recommendations provide to the IT teams is reducing the time to research solutions to these problems, which should equate to faster implementation. Naturally, depending upon the severity of the vulnerability, this will determine the extent of the time required to resolve the deficiency. For example, High vulnerabilities must be resolved within 48 hours, Medium vulnerabilities resolved within one week and Low vulnerabilities resolved within one month.

Forensics
Forensics provides a wide umbrella for which many investigations can be covered. IS teams are routinely asked during an investigation what happened, when it happened and should it have happened. Conducting a forensics investigation without the benefit of log files normally results in failure.

For example, law enforcement subpoenas the company for which user(s) surfed on a particular

© SANS Institute 2000 - 2005 Author retains full rights.

website. In this example, the company has an Internet filtering software product but logs the user by IP address. Additionally, the company has a client/server environment using DHCP. For the IS team to fulfill (after Corporate Counsel's approval) the request within the subpoena, it will need to match the proxy logs and the DHCP logs together. To add to the complexity, the DHCP logs are maintained at each facility within the company's organization but use one Internet access point through the proxy server. Naturally, the first questions are: does the company retain the proxy logs and for how long. If the period in question is covered, the next set of questions are: does each individual site maintain the DHCP log and for how long; supplementing that question is what is the length of the reservation or lease for an IP address at each location. An added function is to research whether successful or failed logon and logoff attempts are being logged for that particular user or computer. Another prime example is attempting to investigate strange behavior on a client without the benefit of complete logging information. Logging will normally show if you have been "visited."

Therefore, SLAs pertaining to forensics may include:
- Proxy logs, firewall logs, server logs, syslogs, DHCP logs, client logs
- Length of time retained before being overwritten
- Threshold for moving the logs to a central logging server, portable media or off-site data storage.

Change & Documentation Management
In most situations, a well-run IT organization will normally equate to a well-managed data security program. In addition to the IT teams having the appropriate skill sets, proper documentation of IT processes, equipment and resources must be keep current for a proper implementation of an IS program.

When conducting risk assessments, network scanning or responding to contingencies or investigative requests, a properly documented network topology is necessary. While this may appear a reasonable request, networks are in a constant state of change. Changes to the documentation is slow due to the implementation of previous changes or forthcoming changes. An example of a SLA for the network topology is that each IT team must update the network topology on a monthly basis.

A more detailed example is the anti-virus countermeasure program. User education and investigations are conducted by the IS team, however, anti-virus software is administered by the IT teams. In this example, a company uses the TrendMicro family of products. The servers use Server Protect, the Exchange environment uses Scanmail and the clients use Office Scan. These three products may appear as only one application, however, each has its own peculiarities to be understood. Comparing and contrasting the three applications are as follows.

Common documentation elements are which network resource has which application, interval of system scanning, and what to do with infected files (move it, delete it, quarantine it). The OfficeScan product should have how the console managers are configured; ability for users to disable/enable the product; how pattern files are updated, i.e. on-the-fly, SMS, or through a logon script. Are special considerations are made for dial-up users as they may have to force a

© SANS Institute 2000 - 2005 Author retains full rights.

"manual" update of the pattern files. The ScanMail product has the option of stripping specific file types (.exe, .com, .vbs, .scr, .bat) prior to the user receiving it. ServerProtect may be installed on servers not necessarily connected to the network but still needing anti-virus support.

SLA elements may include designating critical applications that should have their documentation reviewed on a more frequent basis than others. For instance, the anti-virus documentation may need updating every quarter while the ERP access roles need semi-annual review.

Elements to address when compiling SLAs for the Change/Documentation Management area may include:
- changes in configurations
- network infrastructure changes
- API changes
- log of system failures and respective problem resolution
- frequency of documentation review
- detailed project description
- responsible individuals for each document
- written service and maintenance agreements

Data Back-ups
Data back-ups are the cornerstone to a strong IS program. After all is said and done, data back-ups still allow a company to recover its business either fully or from some established baseline. At one company, a financial database back-up was disabled to allow a back-up on the tape library in favor of a pre-production server that was testing a new software release component for the production ERP application. The failure of this individual to notify the process owner that this occurred adversely affected the company. Mr. Murphy visited this company in the form of a crashed and a corrupted database. Since the database had not been backed-up for nearly three months, a tremendous amount of unproductive labor went into recreating that data. Most companies have already experienced problems when attempting to restore a backed-up application and finding out that the tape was corrupted, contained no data, only contained a partial back-up or was infected with viruses/malicious software.

Some elements to determine when creating SLAs within the topic may include:
- Conceptual back-up documentation
- Verification that the data on back-up is valid
- Documentation of which server/applications are backed-up and the respective schedule
- Validation of restore through a regularly scheduled check
- Designation of an off-site storage location and the pick-up/drop-off schedule
- Designation of which back-ups contain company confidential or proprietary information
- Explanation of the labeling scheme used by the IT teams to track back-ups
- Documentation on how to conduct back-ups and the restoration of back-ups
- Anti-virus check prior to backing up

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Conclusion

The establishment of IS SLAs between the IT teams and the IS teams is necessary to assure the enterprise that proactive measures are implemented. This provides the IT teams with reasonable expectations and provides the IS teams with a definitive spot in the queue, other than last.

© SANS Institute 2000 - 2005, Author retains full rights

© SANS Institute 2000 - 2005 Author retains full rights.

List of References

Andress, Mandy. "Internal SLAs Benefit the Entire Company." Infoworld. April 27, 2001 URL: http://www.infoworld.com/articles/tc/xml/01/04/30/010430tcintersla.xml (December 1, 2001)

Bernard, Allen. "The SLAs They Are A'Changin." ASPnews.com. July 27, 2001 URL: http://www.aspnews.com/trends/article/0,2350,9921_792841,00.html (December 1, 2001)

Bolding, Jeb. "SLAs: Do They Hit the Mark?" Network World ASP Newsletter. July 16, 2001 URL: http://www.nwfusion.com/newsletters/asp/2001/00915560.html (December 1, 2001)

Cope, James. "12 Ways to a Better SLA." COMPUTERWORLD. November 12, 2001 URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO65569,00.html (December 1, 2001)

Koch, Christopher. "Put It In Writing." CIO Magazine, November 15, 1998. URL: http://www.cio.com/archive/111598/sla.html (December 1, 2001)

Lacerda, Cecinio Silva. "Service Level Agreement." www.whatis.com August 6, 2001 URL: http://whatis.techtarget.com/definition/0,289893,sid9_gci213586,00.html (December 1, 2001)

McAnally, Pat. "ERP and Business Continuity: What the Experts Won't Tell You." www.disaster-resource.com URL:http://www.disaster-resource.com/cgi-bin/article_search.cgi?id='21 (December 1, 2001)

Scalet, Sarah D. "Here Come the Lawyers." CIO Magazine, November 8, 2001. URL: http://www.cio.com/security/edit/a110801_legal.html (December 1, 2001)

Schroeder, Max. "A SLA Primer, Allen's Law: Almost anything is easier to get into, than get out of." Computer Telephony, March 5, 2001 URL: http://www.cconvergence.com/article/CTM20010216S0002 (December 1, 2001)

Wrobel, Leo A. "Components of a Successful LAN Disaster Recovery Plan." www.disaster-resource.com URL: http://www.disaster-resource.com/cgi-bin/article_search.cgi?id='95' (December 1, 2001)

Internet Security Systems – Internet Scanner Help Index – Version 6.1 www.iss.net

TrendMicro – OfficeScan, Server Protect and ScanMail product descriptions http://www.antivirus.com/products

© SANS Institute 2000 - 2005 Author retains full rights.