



Security Best Practices



Author: Dr. Eric Cole
Chief Security Strategist
Secure Anchor Consulting

Security Best Practices

Create Security Policy Statements

The most important security practice, that which all other security controls and protections are based on, is the creation and enforcement of security policies. Every organization must have an overall policy that establishes the direction of the organization and its security mission as well as roles and responsibilities. There can also be system specific rules to address the policies for individual systems and data. Most importantly, the appropriate use of computing resources must be addressed. In addition, policies can address a number of security controls from passwords and backups, to proprietary information. There should be clear procedures and processes to follow for each policy. These policies should be included in the employee handbook and posted on a readily accessible intranet site.

The organization's security policies should address applications, services and activities that are prohibited. These can include, among others, viewing inappropriate material, spam, peer-to-peer file sharing, instant messaging, unauthorized wireless devices and the use of unencrypted remote connections such as Telnet and FTP. Appropriate use policies should outline users' roles and responsibilities with regard to security. They should provide the user community with an understanding of the security policy, its purpose, guidelines for improving their security practices, and definitions of their security responsibilities. If an organization identifies specific actions that could result in punitive or disciplinary actions against an employee, these actions and ways to avoid them should be clearly explained in the policy.

In addition to user appropriate use policies, an organization should also create a partner appropriate use policy. This provides partners with an understanding of the information that is available to them and the expected use of that information. It should address actions that are considered unacceptable and the consequences if the actions are detected.

It is also a good idea to create an administrator acceptable use policy. This policy addresses procedures for user account administration, policy enforcement and other administrator specific roles and responsibilities. Administrator requirements should be included in training and performance evaluations.



Create and Update the Network Diagram

It is surprising how many organizations don't even have a network diagram. In order to implement the best security practices, an organization must know what it is protecting. An organization must know the:

- Physical topologies,
- Logical topologies (Ethernet, ATM, 802.11, VoIP, etc.),
- Types of operating systems,
- Perimeter protection measures (firewall and IDS placement, etc.),
- Types and location of devices used (routers, switches, etc.),
- Location of DMZs,
- IP address ranges and subnets, and
- Use of NAT.

In addition, the location of the diagram must be known and it must be regularly updated as changes are made. Network management software, such as HP Openview, can perform network device discovery to make this effort easier. It can then produce an alert when new devices come online. One word of caution regarding a network diagram being made available publicly: this type of information is very valuable to attackers and therefore should be kept private.

Place Systems in Appropriate Areas

To protect systems from unauthorized access, they must be placed in areas of the network that give users of the system the least amount of privileges necessary. Only systems that are semi-public are kept in the DMZ. This includes external web servers, external mail servers and external DNS. Limited access to these systems is allowed from the Internet. A split-architecture may be used where internal web, mail and DNS are also located on the internal network. In addition to internal web, mail and DNS servers, the internal network also includes databases, application servers, test and development servers. Access to these systems is limited to internal users only and they are not accessible from the Internet.

Protect Internal Servers from Outbound Communications

Internal servers should not connect out to the Internet. Sometimes organizations have had administrators who use internal servers as their personal systems and perform normal activities on it such as accessing the Internet and checking email. Internal and other servers should never be used as personal systems. It is also a good idea to add rules to the internal firewalls



to block internal servers from outbound traffic. If the server needs to access other network segments, a specialized rule can be created for that, or just block the internal server's outbound access at the Internet connection perimeter firewall. If effect security controls are used on the firewalls and intrusion detection systems, not only will the servers be denied access outside the network, but if the server attempts to access the outside, an alert will be generated and the administrator notified of a potential problem.

Assess the Infrastructure

Identifying the critical business systems and processes is the first step an organization should take in order to implement the appropriate security protections. Knowing what to protect helps determine the security controls, and knowing the critical systems and processes helps determine the business continuity plan and disaster recovery plan process. Critical business systems and processes may include an e-commerce site, customer database information, employee database information, the ability to answer phone calls, the ability to respond to Internet queries, etc.

In addition to identifying the critical business systems and processes, it is important to identify the possible threats to those systems as well as the organization as a whole. Considerations should be made for external and internal threats and attacks using various entry points (wireless, malicious code, subverting the firewall, etc.). Once again, this will assist in implementing the appropriate security protections and creating business continuity and disaster recovery plans.

An organization must understand how an outage could impact the ability to continue operations. For example, it must be determined how long systems can be down, the impact on cash flow, the impact on service level agreements and the key resources that must keep running.

Protect the Perimeter

Multiple layers of security should provide protection at the perimeter. This includes a border router with access control lists that perform ingress and egress filtering, a stateful inspection firewall and application proxy firewalls. Intrusion detection systems should also be placed at the perimeter. There should be a default deny rule on all firewalls to disallow traffic that is not explicitly permitted. This is more secure than explicitly denying certain traffic because that can create holes and oversights on some potentially malicious traffic.



Create a Strong Password Policy

Most system compromises are the result of weak passwords. Users create easy to guess passwords, administrators often forget to remove default accounts and passwords on devices and unused accounts contain passwords that don't change. For systems which rely upon password protection for authentication, users should select good passwords and periodically change them. Password guessing and cracking attacks are common ways of gaining unauthorized entry to networks, and even the best passwords can eventually be broken, given enough time. The use of strong passwords provides a firm deterrent against password guessing attacks and buys additional time against cracking attacks.

The following guidelines enforce a strong password policy:

- The password must be at least 8 characters,
- It should contain both alphanumeric and special characters,
- A user can't reuse his/her last 5 passwords,
- Passwords must change every 60 days, and
- Accounts are locked out after 3 failed login attempts.

UNIX systems should be using the shadow password feature. Previously the encrypted user passwords were readable in the `/etc/passwd` file. Shadow password removes the encrypted passwords to a protected `/etc/shadow` file.

A strong password policy is one of the best security measures to prevent unauthorized access. However, encouraging users to adhere to the policy is difficult since they will want to create passwords which are easy to remember and don't change. Most operating systems now have mechanisms to enforce strong password policies. The following examples allow the enforcement of the password policy at the operating system level:

- Password aging: Allows forcing the user to change his password periodically,
- Minimum length: Allows the enforcement of a minimum password length,
- Non-dictionary words: Allows stopping the user from selecting a password that is in a standard dictionary,
- Password uniqueness: Allows specifying the number of new passwords that a user must select before they can reuse a previous one, and
- New password: Allows setting a minimum number of characters required for the new password that is different from the previous password.



Create Good Passwords

The following best practices provide additional guidelines for creating strong passwords:

- Use passwords with upper and lower case letters. Don't just capitalize the first letter, but add other uppercase letters as well,
- Use a combination of: uppercase, lowercase, numbers, and special characters,
- Create a password that can be typed quickly without having to look at the keyboard. This deters "shoulder surfers" from attempting to steal passwords,
- The more critical an account, the more frequently it should change. Root and Administrator passwords should be changed more frequently than users' passwords,
- Never use the username in any form as a password,
- Never use first names, middle names, last names, initials, or nicknames as a password,
- Don't use words contained in dictionaries,
- Don't use personal information that is easily identified, such as pet names, children's names, car make or model, address, etc,
- Don't use a password containing just numbers or just characters,
- Don't write down passwords,
- Don't tell anyone a password,
- Don't use shared accounts,
- Don't use a password that is overly long. Long passwords are difficult to remember and it is more likely that it will have to be written down, and
- Make a password easy to remember but hard for others to guess.

Audit Passwords

Regular password auditing should be performed to check the strength of passwords and to enforce the password policy. Make sure before performing any password auditing that approval is received from the legal department. Once this is done, create a process for regular password auditing. Password cracking tools such as L0phtcrack or John the Ripper can also be used. When the password cracking is complete, note the passwords that do not follow the proper policy and lock out the accounts of those in violation. Next, send an email to the users of these accounts with a copy of the password policy.



Require them to sign a copy of the policy before unlocking the account. Multiple violations may result in disciplinary action.

Be sure when performing password cracking to perform the cracking on an offline system and do not store the cracked passwords on a computer. If these are forgotten about and left on the system an attacker or malicious user may stumble across them and use them to his advantage.

Use Strong Authentication

Since passwords are created, managed and used by humans, there are still vulnerabilities with their use. If something more secure is desired, use some other form of strong authentication. One example is a one time password system such as SecurID by RSA. With one time passwords, if an attacker did compromise the password token, it would only be good for that one session. One time passwords are becoming more common for Administrator accounts and for remote users.

Remove Service Accounts

As mentioned previously, administrators often forget to remove default accounts and passwords on devices. These default accounts are usually service accounts that allow maintenance or other privileges. They often have either system or domain administrator level privileges. These accounts are often forgotten about and left unused for long periods of time. Attackers regularly scan for these accounts and their default passwords. An attacker who discovers or cracks the password of a service account inherits the privileges of that account and can often use the account for long periods of time undiscovered.

Create a Patching Policy

It is a common best practice to patch systems as soon as a new patch is released. Unfortunately, many organizations don't patch regularly and tend to not patch critical systems because they don't want to risk downtime. However, critical systems are the most important to patch. Unpatched systems have been the leading contributor to the recent worm attacks. The Blaster and Slammer worms are two good examples of exploits that could have been easily mitigated had patches been applied in a reasonable amount of time. A worm finds an unpatched system, exploits the vulnerability and uses that system to continue scanning for other unpatched systems in order to propagate. Thus, a worm that is wreaking a lot of havoc on the Internet means there are a lot of unpatched systems!



Regular maintenance downtime must be scheduled to patch systems. As vulnerabilities are discovered, attackers often release exploits even before system patches are available. Therefore, it is imperative to patch systems as soon as possible. Security patches from the system vendors can close most of the known security holes. These are also called service packs, maintenance updates, software updates and security patches. New releases of patches from the vendors of the systems must be monitored. Some systems offer an automatic update process, however others require a visit to the website or subscribing to an email list. Subscribing to a vendor's patch release bulletin and having support contracts with vendors is one way to make sure to get the latest information automatically.

Different strategies may be adopted when applying security patches suitable to the system architecture. One method is to apply every applicable, available security patch to operating systems and applications. Another method is to verify the need for a particular patch to the system and install it if required. In either case, whenever a new security patch is available, carefully study the details of vulnerability and its impact on the systems and environment. Depending upon the risk, it is necessary to decide how to proceed with the patching strategy.

Some points about patching to keep in mind include:

- Fully patch systems before connecting them to the network,
- Continually update systems as patches are released,
- Re-patch the system if adding an additional service or application to the system,
- Test patches in a lab environment before applying them to check for adverse effects,
- Keep system backups in case there isn't time to test a patch first, or in case the patch does cause problems even after testing,
- Keep a list of patches and service packs that are applied to critical systems in case of a rebuild,
- Make use of the free automated tools such as the Microsoft Baseline Security Analyzer, and
- Incorporate scanning for patch level compliance into regular vulnerability assessments.



Perform Regular Vulnerability Assessments

Regular vulnerability assessments are essential to maintaining the ongoing security of an organization and should be performed as often as possible. The scanning should be scheduled to allow adequate time to look through the reports and discover anything that has changed and mitigate the vulnerability. Awareness of vulnerabilities allows organizations to take corrective action before an attacker exploits them. There are various commercial and open source tools available for vulnerability scanning, such as ISS Internet Scanner, Retina, and Nessus. These tools scan systems and look for open holes and known exploits. Vulnerability scanners must be updated with new signatures as they are released, similar to anti-virus tools. The scanning tool will provide a report of the results with a criticality rating of each vulnerability and recommended corrective actions. However, it is up to the administrator to analyze each vulnerability, assess its impact and apply the appropriate corrective actions. Critical vulnerabilities should be addressed immediately. Otherwise, plan on fixing any non-critical vulnerabilities during scheduled system downtime. Lastly, once a corrective action is applied, scan the system once more to make sure the vulnerability no longer exists. It is not uncommon for one patch to undo a certain corrective action from a previously applied patch. It should be assumed that every time a system is altered, a vulnerability could exist. Thus, by repeated scanning after each alteration, it can be assured that the system is secure.

Enable Logging

Some administrators don't enable logging because they get a barrage of log events and it ends up being too much information. However, it is critical to log events. Focus on logging only those events that either alert administrators to problems or in some way help manage the system better. Too much logging will generate useless data and hide the important information. Logs provide an audit trail and evidence in case of an attack. Once attacked, without logs, there is little chance of discovering what the attacker did. Without that knowledge, it isn't clear as to whether a system should be completely rebuilt or a certain problem be fixed. It will also be unknown how long the attack was taking place, so backups could be compromised as well. Logs provide the detail of what is occurring, what systems are being attacked or misused, what systems are having unauthorized access and what systems have been compromised in some way. Enabling system logging is usually an easy task for most operating systems.



Review Logs

Enabling logging only does good if the logs are being reviewed. One of the biggest mistakes an organization can make is failure to review logs. Logs should be reviewed every day. This includes IDS logs, system logs, management station logs, etc. Events of interest in the logs should be investigated daily. However, it can be a tedious task for a single person to perform log review every day (unless they really enjoy it). It is better to have a log review rotation system amongst the security team. Log review is also typically part of a penetration test. The penetration testing team will purposely leave traces of their activities in logs to test whether the security administrators are actually reviewing the logs.

Typically a constant stream of port scan attacks will be present in the logs. These are a regular occurrence on the Internet as a result of attackers and worms. The log should not report many substantial attacks, such as root compromises, backdoors, or exploits, on systems. This would indicate that the security defenses are weak, patching may not be occurring, or other vulnerabilities exist.

A centralized logging and event correlation system assists with log review. Some products provide summaries and statistics in graphic or tabular format to make analysis easier. Some products also have sophisticated correlation engines to understand the big picture. These tools can also be used to analyze trends in the network or on systems and assist in mitigating performance issues. By using a centralized syslog server and automated tools, the administrator can easily review logs on a regular basis, recognize security alerts, perform system analysis and save logs offline for future reference.

Lastly, an important aspect of logging, especially when using a centralized log server is to protect the logs. Attackers love to gain access to logs, to see if they were detected and possibly cover their tracks. They may also use logs to gain valuable information about a network or system and the services installed. A properly configured and locked down centralized log server makes it much more difficult for an attacker to access logs or edit them.

Use Multiple Detection Methods

To provide the best level of detection, an organization should use a combination of both signature-based and anomaly-based intrusion detection systems. This allows both known and unknown attacks to be detected. The IDSs should be distributed throughout the network, including areas such as the Internet connection, the DMZ, and internal networks.



IDSs come loaded with default rulesets to look for common attacks. These rulesets must also be customized and augmented to look for traffic and activities specific to the organization's security policy. For example, if the organization's security policy prohibits peer-to-peer communications, then rules should be created to watch for that type of activity.

Monitor Outgoing Communications

Oftentimes, organizations focus on traffic and attacks coming into the network and forget about monitoring outgoing traffic. Outgoing traffic should be inspected before it leaves the network, looking for potentially compromised systems. Not only will this detect compromised systems with Trojans and backdoors, but it will also detect potentially malicious or inappropriate insider activity.

Perform Content Inspection

In addition to the content level inspection performed by the IDS, specific content inspection should also be performed on web server traffic and other application traffic. Some attacks evade detection by containing themselves in the payload of packets, or by altering the packet in some way, such as fragmentation. Content level inspection at the web server or application server will protect against attacks such as those that are tunneled within legitimate communications, attacks with malicious data, and unauthorized application usage. The types of content checking that should be performing include:

- Binary code in HTTP headers: Attacks can be launched by including executable code in HTTP headers. This violates the HTTP protocol standard, however most firewalls don't check for this type of content,
- HTTP or HTTPS tunneling: Various types of communication can be tunneled through HTTP and HTTPS ports 80 and 443. This includes peer-to-peer (P2P) file sharing and instant mail and remote management software such as GotoMyPC. They comply with protocol standards, so most firewalls do not block them. Tunnels also provide a means for attackers to install sniffers and Trojan programs, allowing them to eavesdrop on network communications and create backdoors. Malicious traffic can also be tunneled over other protocols that are normally permitted by a firewall, such as DNS and SMTP,
- URL directory traversal: Directory traversal involves using the "... " notation within a file system to access restricted files and directories, and possibly execute code on the web server. This is a very trivial attack to execute. By exploiting directory traversal vulnerabilities an attacker can access files in other directories, such as the cmd.exe program on Windows, or the passwd file on UNIX. Another way to traverse directories



is by using escape codes and Unicode in the URLs. All URL requests should be inspected and rejected if they contain any escape or Unicode characters,

- Excessive URL header length: HTTP URL and header length is not restricted in the HTTP protocol standard. However, excessive URLs and headers can be used in buffer overflow attacks. Buffer overflows can be exploited by excessive lengths in URLs, GETs, POSTs, and header fields,
- Cross-site scripting: Cross-site scripting (XSS) attacks exploit the client-server trust relationship on the web by using specially crafted URLs containing malicious code. This code, usually JavaScript, VBScript, ActiveX, HTML, or Flash, can be hidden and inadvertently executed by unsuspecting users when they interact with the web application,
- Malicious URLs: Malicious data can enter the network by being embedded in URLs and executed by the user, or automatically by a mail client,
- Inspect file transfers: Content filtering and access control should be performed at the application layer to regulate the transfer of file names containing certain keywords. For example, a firewall could deny the transfer of files with the words “passwords” or “proprietary” in the names. Likewise access control should also be applied to the content of the files. Files containing the words “password” or “proprietary” anywhere in them could be denied too, and
- Inspect mail attachments: Content filtering and access control should also be performed on incoming and outgoing mail attachments. Viruses and worms often spread via mail attachments, therefore both incoming and outgoing mail should have the attachments inspected for malicious code, and then sanitized or blocked.

Control and Monitor Remote Access

Remote access should be tightly controlled, monitored, and audited. It should only be provided over a secure communication channel that uses encryption and strong authentication, such as an IPSEC VPN. Desktop modems (including applications such as PCAnywhere and GoToMyPC), unsecured wireless access points and other vulnerable methods of remote access should be prohibited.

Organizations don't always consider wireless networks when referring to remote access. Part of knowing the network architecture includes knowing the location of wireless networks, since they create another possible remote entry



point for an attacker. It must also be determined whether they are being used for sensitive data and are they sufficiently secured.

Wireless access must at least use WEP with 128-bit encryption. Although this provides some security, it is not very robust, which is why the wireless network should not be used for sensitive data. Consider moving to the 802.11i standard with AES encryption when it is finalized.

Use Defense in Depth

Defense in depth means applying security in multiple layers. We mentioned previously how that can be applied at the perimeter. Defense in depth is actually applied throughout the network from the perimeter down to the actual desktop. In addition to routers with filters, stateful firewalls, proxies and intrusion detection, system level protection must be implemented. Desktops should have a combination of anti-virus software, personal firewall and host-based intrusion detection. Each of these software packages must be regularly updated as new signatures are deployed. They should also be centrally managed and controlled.

Another layer of defense in depth is monitoring for any unauthorized modification of system files and configuration files. There are various tools available that allow those monitoring to see if files are created or deleted or if permissions are modified. Typically these tools will build a database that includes information such as file size, permissions, digital signatures, number of files on the system, etc. It then periodically computes a new database and compares it to the old one for changes. Tripwire is an example of a tool that performs file system level protection. Tripwire checks to see what has changed on the file system and provides an extensive report.

Secure Communications

Secure communications such as VPNs should be used for remote access and other sensitive communication. IPSEC is a great choice for this purpose. Strong encryption protocols such as 3DES and AES should be used whenever possible. Web access to sensitive or proprietary information should be protected with 128-bit SSL. Remote system administration should use SSH. Sometimes file system encryption is also used to protect stored data.

Backup Frequently and Regularly

As much as we would like to think that nothing bad would ever happen to our computer, unfortunately hardware does fail, systems are compromised and other disasters make our systems unusable. Thus backing up a system is



always a good practice. It is imperative to business continuity and disaster recovery to implement a reliable backup and recovery process. Built-in backup software included with the operating system or third party solutions can be used. Some important considerations when planning a backup strategy include:

- Asses how frequently data should be backed up and what the best time is to backup,
- Decide how much data there is to back up,
- Determine if full configurations or partial (incremental/differential) configurations will be saved,
- Select the type of backup media to use (tape, disk, server, other location),
- Choose the software which will be used to back up systems (e.g. ArcServe, BackupExec, Networker, NTBackup, Norton Ghost, etc.),
- Verify which administrators will have primary and secondary backup responsibilities,
- Determine the location of offsite storage for backups,
- Decide how long the backup data should be stored,
- Prepare secure storage of the backup data, and
- Good documentation of the backup and recovery process.

A good backup policy includes weekly full backups with incremental backups performed daily. This includes all critical systems. In addition, the backups should be stored at an offsite location. Since backups include very valuable, easily accessible information, only trusted individuals should be performing them and have access to them. An organization should also encourage users to perform local backups as well.

Every organization should maintain full and reliable backups of all data, log files, and anything else that is necessary or useful for normal operations. Make sure to back up configurations, such as the Windows registry and configuration files used by the operating systems or applications. Also, archive all software, upgrades and patches off-line so they can be reloaded when necessary. Some other best practices for backups include:

- Verify and log that backups were completed successfully,
- Maintain a written log of media usage and properly labeled media,
- Write protect media as appropriate,
- Check the media before usage,



- Determine the length of time the media will be saved and whether or not it will be reused, and
- If using a hardware backup system, seek training if appropriate and review the manufacture recommendations for device maintenance.

The backup and recovery process is not complete until it is tested. Be sure to document the backup procedures and test them. Test the recovery process periodically to ensure that data is being backed up correctly and that the recovery process is correct and easy to follow.

Protect Sensitive Information

Sensitive and proprietary information is knowledge that might give an advantage if revealed to persons not entitled to know it. It must be protected because its unauthorized disclosure, alteration, loss, or destruction will, at the very least, cause perceivable damage to someone or something. Thus, due care should be taken to protect sensitive information when in use, storage, transit, and disposal. We have previously addressed protecting data in storage and in transit by using encryption. There are also special methods of safely disposing of sensitive information. Hard copies of sensitive information should be destroyed by pulping, shredding or incinerating. Sensitive information on hard drives and disks should be completely erased using special software or the disks must be destroyed. Simply deleting a file is not sufficient to prevent attackers from undeleting the file later. When disposing of a computer system, be sure to erase all sensitive files from the hard drive by using a wipeout utility.

Create and Test a Disaster Recovery Plan

The destruction caused by this recent natural disasters supports the fact that every organization must think about such disasters and have a plan in place to maintain business operations and handle the recovery. A disaster recovery plan (DRP) should include recovery of data centers and recovery of business operations. It should also include recovery of the actual physical business location and recovery of the business processes necessary to resume normal operations. In addition, the DRP should address alternate operating sites.

The DRP is no good unless it is tested regularly, at least once a year. The test will iron out problems in the plan and make the plan more efficient and successful if/when it is needed. Testing can include walkthroughs, simulations or full out implementations.



Control and Monitor the Physical Space

Physical security is a large area that must be addressed by an organization. An example of physical controls include physical access controls (signs, locks, security guards, badges/PINs, bag search/scanning, metal detectors), CCTV, motion detectors, smoke and water detectors and backup power generators.

Critical system consoles should be physically protected. The system should be located in a secure area where only authorized personnel are allowed. An unprotected console allows an attacker to easily access the system. There are bootable CDROMs that can reset or bypass root passwords. Most systems also have some sort of console password recovery procedure to break into the system as well. Do not leave the console logged in at any time while away. Make it a practice to logout or lock the screen every time after completing a task. If the system supports a timeout feature for the system console, be sure to use it.

Educate Users

Humans are always the weakest links in the security architecture. We have already addressed the human tendency to create weak passwords. Humans also tend to give out too much information about the network and systems, or to fall for attacker tricks out of compassion, sympathy or plain ignorance.

Two common attacks that exploit the human factor are social engineering and phishing. A typical social engineering attack is known as the helpless user, usually combined with being remote or on travel. Here the attacker masquerades as a remote user with an important deadline to meet, often impersonating someone high up in the organization. Helpdesk or other support personnel may be pressured into giving out passwords, or resetting them, or providing other types of information to the attacker because people tend to genuinely want to help the helpless. On the other side, another typical social engineering attack is when the attacker pretends to be a technical support person and gets information out of an innocent (but ignorant) user. This is often the easiest and best way to get passwords. Often, rank helps in this scenario too. Phishing is a newer social engineering email-based attack that tricks users into going to a web page, which they think is authentic and entering in their credentials. However, the web page is an imitation used by an attacker to collect information such as account numbers, usernames, passwords and credit card information. This attack has been popular for eBay and PayPal accounts. It is also closely related to identity theft.

The best way to protect against these types of attacks is to educate the users. Employees should attend security awareness training that explains the types of



attacks, what to expect and how to respond. There should also be a publicly posted incidents email address to report suspicious activity. Users should also be constantly reminded and updated on secure practices through a security awareness program.

Don't Forget About the Code

For a long time, security was driven at the network and system level. Not as much attention was given to application development security. Any development that is taking place in house should include security from the beginning of the development process. Security needs to be a part of the requirements and testing. A test team should conduct code reviews to look for vulnerabilities such as buffer overflows and backdoors. For security reasons, it is not a good idea to subcontract development work to third parties.

Secure UNIX Systems

Over the past few years, the popularity of freeware versions of UNIX has increased. This is due to the low cost, variety of supported hardware and increased ease-of-use of the operating systems. However, due to this fact, the number of security incidents involving UNIX systems has also risen. This was mainly due to the fact that freeware UNIX operating systems were inherently insecure out of the box, however this is changing. Any organization or user running a UNIX operating system needs to make a serious and ongoing commitment to securing and maintaining the security of that system. Some general best practices for the security of UNIX systems include:

- Never let the root password travel the network in the clear; make sure to use SSH, SFTP, and other encrypted communications,
- Enforce a strong password policy,
- Get on a vendor's patch notification list,
- Remove unnecessary services from `/etc/inetd.conf`,
- If providing a mail service, use the latest version of sendmail,
- Use a version of UNIX that comes with source code. These tend to be more secure due to the public scrutiny of the source code. NetBSD and FreeBSD are typically the most secure. NetBSD is configured with security by default, making it generally more secure than most modified UNIX installations,
- Review logs and investigate unusual events, and
- Run a file integrity software program such as Tripwire.



Install Only Essential Services

It is best to maintain systems and servers with the minimum services and packages (applications) as possible. The more services and packages they are running, the greater the risk of exposing the system to exploitation. During the operating system installation, minimize the service components and packages installed. Install only essential services that are required for running the packages that are in use on the system. Additional services and packages can always be installed later as needed. Similarly, if the decision is made to remove an application package from a system later, remember to remove the associated underlying services if they are not necessary for other applications. The method used to disable services depends on the operating system. It may be necessary to disable it through the Services window in the GUI or by editing a services file such as `/etc/inetd.conf`.

Also, make sure to close any unused TCP/UDP ports. Ports that are open can be found with the `netstat` command or by running a port scanning tool such as `nmap`. Open ports could indicate services that weren't closed, services that were unknown or even backdoors. Any open TCP/UDP port offers an attacker a possible entry point into the system. Thus, having any port open that is not absolutely necessary should be avoided.

Deploy Single-Use Servers

Multiple-use servers lead to multiple vulnerabilities. When running servers, it is best to run a dedicated server for each package, for example a mail server, a web server, a DNS server, etc. Installing all of those packages on a single server not only creates performance issues but also opens up many avenues of attack on three critical systems in a single shot.

Perform Configuration Management

It is a good practice to document any change in the system configuration, whether it be hardware or software. This assists in the disaster recovery process, intrusion detection, trouble-shooting, etc. This becomes a big issue when several system administrators are managing the same systems. It facilitates good communication and keeps everyone on the same page. It is recommended to maintain additional copies of the documentation on software backups or as a hard copy stored offsite. Taking configuration management one-step further, implementation of a configuration control board (CCB) is an option. This way, whenever a change needs to be made to a system, it must be approved by the CCB. Depending on the organization, this can be for major changes, such as adding a new package to a system, or even for smaller



changes. The CCB reviews the change to assess its impact and possible consequences and then approves or denies the request. The CCB usually encompasses representatives from various parts of the organization including network administrators, system administrators, project managers, etc.

Use Firewalls and IDS Beyond the Perimeter

This practice goes along with defense in depth. The perimeter is secured with multiple layers and the servers and desktops are secured with multiple layers. But don't forget about internal networks. If an attacker does successfully breach the network's perimeter, there must be other hurdles to protect internal network segments. For example, an attacker could also compromise a system in a department such as HR and use it to attempt to access another system in Accounting. Deploying firewalls to protect internal departments can stop these types of attacks. Additionally, using internal firewalls can protect against a malicious insider and worm propagation.

In order to implement firewalls between internal networks, the network must be segregated. This means that different departments should be physically and logically separated on the network. Different departments can be physically connected to different edge switches or use VLANs to perform the segregation. Unless there is a specific reason, internal departments should not need access to each other, for example, Payroll having access to Research and Development. A properly segregated network will cut down on the potential for insider abuse and limit the damage that an attacker who does gain entry can make since they would be limited to only a small portion of the internal network. Internal firewalling and network segregation also makes troubleshooting and pinpointing events easier.

If there is a breach in security or if some other malicious or unauthorized activity occurs, the IDS on the internal networks will detect this. IDSs should be deployed within each segment of the network and designed in a distributed fashion for centralized reporting. This allows the administrator to monitor a single alert station while having awareness of the entire network. The goal of internal firewalls is to prevent unauthorized access; the goal of the internal IDS is to alert to unauthorized access and therefore mitigate any damage before it can occur.

Question Trust Relationships

Beware of who is trusted when creating partner and extranet networks. Just because all of the protections necessary to ensure the security of a network are applied, that doesn't mean that other organizations do the same. Even other, separate parts of the same organization may not be as secure. Attackers, who



compromise a system on a network that an organization network trusts, can use that trust relationship to come right into the network. Anything that connects from an organization's network to another network can be considered a trusted relationship. When connecting to another entity, consider the following:

- Is this connection necessary,
- How much access does the connection require,
- What additional security controls will be needed to protect the trust relationship,
- What security controls does the other entity use, and
- What policies does the other entity have in place?

Make sure there is a clear policy between each organization and the outside entities that outlines appropriate use and actions that will be taken in the event of inappropriate and unauthorized activity. A good way to secure the trust relationship is to segregate the trusted connections into the DMZ. Anything that can be done to limit trusted access will help in ensuring that the network remains secure and will not be comprised by another's lack of security.

Use Anti-Virus Software

Today's viruses are very capable of hiding themselves and covertly monitoring the system and performing actions, such as keystroke logging and other malicious events. Install anti-virus protection systems at critical points and keep them current. Critical points include servers (scanning files) and mail (scanning inbound and outbound email attachments).

Protect System Accounts

Unused and unprotected accounts are an attacker's gold mine. Make sure to remove all unnecessary accounts. Simply disabling an account is not sufficient to protect it. Attackers can enter a system through one account and re-enable a disabled account to escalate privileges. In multi-administrator networks, a system administrator might not consider an account being re-enabled a problem since another administrator probably did it. This is where configuration management would be necessary. It is particularly dangerous to disable (instead of remove) a privileged account of an administrator, power user or executive when they leave the organization. Some organizations simply disable the accounts until someone new comes to take that person's place. These placeholder accounts are very inviting to an attacker. When someone leaves an organization, no matter who it is, the account should be removed, not merely



disabled. Also, be sure to remove default accounts such as maintenance accounts, guest accounts, etc.

Another good practice is to rename default administrative accounts. Renaming these accounts makes it more difficult for the attacker to determine which accounts are privileged. This will slow down a skilled attacker, but will also defeat most automated tools and techniques used by script kiddies.

Name Servers Securely

A name can say too much. Servers should be named in a way that does not give any information about them or their purpose. For example, people tend to name database servers db1, db2, etc. Host names such as these advertise to a potential attacker a server's primary service or purpose. So then he will start looking for the latest database vulnerabilities and exploits for that system. A server named "test" tells an attacker this could be an unsecured server, a server that is not likely to be monitored, a server with default accounts, a server that may be in a lab and not used everyday or a server that could be used as a stepping stone to other servers. The same goes for names like lab, dev, and temp. It's also not a good idea to name servers after the departments that use them, like HR, Payroll, Research, etc. This gives an attacker an idea of goods these servers contain. It is best to pick an interesting but easy to remember and understand naming scheme and stick to it, for example, presidents, animals, flowers, or, my favorite, Star Wars planets.



About Secure Anchor Consulting

Secure Anchor Consulting provides information protection services to a great number of Fortune 500 industries, as well as government, military, energy, IT and legal industries. We have coalesced the expertise of well-known and widely respected security professionals, many of whom are respected authors and frequent speakers at venues around the globe, including the SANS Institute and BlackHat conferences.

For More Information:

Visit our website:

www.secure-anchor.com

Email us:

info@secure-anchor.com

