Assessing and Monitoring Telecommunications Security and Costs

- Authentication
- Firewalls
- Intrusion Prevention Systems
- Intrusion Detection Systems
- Encryption
- Wireless
- Certificate Authority
- Catching the Successful Hack
- Physical Security
- Penetration Testing
- Telecommunications Costs

Authentication

Authentication is the means of identifying yourself to the computer systems. Most authentication systems are weak relying on the simple logon ID/password features that have existed for, well, since computers were invented

QUESTIONS:

1 How does the user identify them to the computer (Logon ID's? Nothing special here).

2 What are the password formatting standards? Do they include at a minimum the following:

- 8-10 character passwords
- Not allowing the use of English language words
- No allowed to be repeated for at least 10 generations
- Not allowed to change a password more often than twice-a-day
- Forced to change the password every 60-90 days
- And the big one…TWO level authentication. This means the user is required to enter their password and then a second authentication, usually in the form of a token key. At a BARE MINIMUM, two level authentication should be required for remote access

TESTING:

1. Attempt to circumvent the various password configuration controls using your own logon ID or a guest logon ID provided by IT.
2. Match the list of all current logon ID's to the current employee master file. Any unmatched logon ID's may belong to former employees or consultants who have moved on.

Firewalls

OK. Repeat after me. Firewalls are STUPID. Ya. It's OK to say it. Firewalls are stupid. They do not look at the content of the transmission. They do not stop viruses. They do not stop most denial of service attacks. The main thing they do is verify the message originates from a trusted location, typically by IP address or URL. And, since most Hacks know how to cloak themselves, even that feature is of limited use. BUT, we have to have firewalls to provide basic protection and to protect us from ourselves.

QUESTIONS:

1. Does your organization have at least two levels of firewalls? The first firewall allows people from the outside into the DMZ. This firewall will be quite porous and let most everybody into the DMZ where our information web sites are. You know. The ones that show our corporate headquarters, our organizational commitment to fair practices, and has a picture of a group of smiling employees all working happily together. And then also an identification of our products and services.
   Then there should be a second firewall that is much more restrictive and allows only authenticated (Logon ID/Password) users in and into the corporate computers.
2. Who maintains the firewalls? Are these Firewall Administrators technically skilled and possessing the qualification to perform technical work of this kind?
3. Is there a Firewall Policy that provides the foundation for how the firewalls are configured?
4. Are the Firewall Policies authored by a committee consisting of IT, end user, and executive management?

5. Are the Firewall Administrators required to update the firewall configurations to comply with the Firewall Policies?
6. Does a separate IT manager routinely ensure the firewall configuration complies with the Firewall Policies?
7. Are there firewall restore plans?
8. Does the firewall include a "timeout" feature so administrator logons automatically disconnects after 10 minutes of inactivity.
9. Are there redundant firewalls?
10. A BIG QUESTION: Are the firewalls STATEFUL firewalls? Stateful firewalls will protect internal addresses by only allowing in traffic that is invited in, significantly reducing the risk of outsiders probing for open ports.
11. Are the firewall "Websense" signature databases up-to-date. The vendors that provide the firewalls also provide signature databases that identify sources of known "baddies" to filter or not let in. The Firewall Administrators should install the updates to the signature databases as provided by the vendors, or have an explanation why not.
12. How do the Firewall Administrators monitor the firewalls? HINT: Since firewalls are stupid, not much monitoring is necessary. Monitoring is done with the more powerful telecommunications tools such as the intrusion prevention systems and intrusion detection systems.

TESTING:

1. Obtain the Firewall Policies. Ensure they have been updated in the last 6 months.
2. Review the Firewall Policies and ensure they include the following:
   - No FTP or Telnet allowed (These allow unencrypted transmissions)
   - The firewall after the DMZ should default to "Deny Any Any". In other words, no traffic is allowed through the firewall unless specifically allowed.
   - Firewall Policy authors should not be implementing the firewall rules.
   - A customized list of URLs to filter or not let through the firewalls.
   - Requirements that the firewalls remain in the Stateful condition
   - Block all inbound traffic in which the source IP address is private, loopback, or echo-requesting
   - A list of specific web sites to not allow employees to access. (Sorry folks. No ESPN.Com)
3. Working with the Firewall Administrators, obtain proof that the above policies are actually implemented into the firewalls.
4. Obtain evidence that the firewall restore plans have been tested or applied in the last year.
5. Ask the Firewall Administrator to logon to their administrator logon and then do nothing. Verify the logon automatically times out and disconnects after 10 minutes.

Intrusion Prevention System

OK. HERE is where the real telecommunications protection is. Behind the firewalls, and doing all the real work of protecting our computers is the Intrusion Prevention System (IPS). The IPS looks at the content of the transmissions and will identify patterns, viruses, and attacks. And, the cool thing is, they are relatively simple to maintain and audit.

QUESTIONS:

1. Does your organization have an IPS?
2. Are the IPS Administrators (typically the same people who are the Firewall Administrators) technically skilled and possessing the qualification to perform technical work of this kind.
3. Is the IPS set to default to DENY?

4. Is the IPS signature database up-to-date? The IPS vendor provides signatures, i.e., characteristics, of known attacks, probes, and vulnerability exploiters. If the content of the message matches the signature database, access should be DENIED.
5. Determine how the IPS Administrators monitor the IPS system for attacks. Are the Administrators able to be notified and respond in a timely manner? A 6 hour gap between attacks and follow-up is inadequate.
6. Are attacks automatically logged?

TESTING:

1. Obtain from the IPS vendor a list of the signature database updates issued in the last three months. Select a sample of at least 20 of these signatures and require the IPS Administrators to prove that these updates were implemented. HINT: There are a LOT of updates issued. Focus our testing on the high risk vulnerability updates. The IPS vendors issue a color coded list of updates to highlight the high risk vulnerability updates (typically RED) so finding them in the lists will be easy.
2. Ask the IPS Administrator to display the IPS logs from yesterday, 3 weeks ago, and 6 months ago to ensure the logs have been functioning for the entire audit period.
3. Ask the IPS Administrator to identify two recent attacks, explain how the attacks were identified, and what was done for follow-up.

Intrusion Detection System

Behind the firewalls, behind the Intrusion Prevention System, is the Intrusion Detection System (IDS). The IDS system does the monitoring and reporting of bad stuff trying to get through or attack our systems. The goal of the IDS is not to stop anything, but to notify IPS Administrators that something needs to investigated. The IDS signature database has all the signatures of the IPS signature database, plus also customized with a lot of other potential attack and probe characteristics that your organization may want to be aware of.

QUESTIONS:

1. Does your organization have an IDS?
2. Are the IDS Administrators (typically the same people who are the Firewall Administrators) technically skilled and possessing the qualification to perform technical work of this kind.
3. Is the IDS set to LOG.
4. Is the IDS signature database up-to-date? The IDS vendor provides signatures, i.e., characteristics, of known attacks, probes, and vulnerability exploiters. If the content of the message matches the signature database, access should be LOGGED for Monitoring.
5. Has the IDS signature database been customized to include additional telecommunications vulnerabilities and concerns unique to your organization? Did a security committee of IT, end-user, and executive management decide what customizations should occur? How does the committee ensure these customizations were actually implemented by the IDS Administrator?
6. Determine how the IDS Administrators monitor the IDS system.
7. What types of IDS vulnerabilities and attacks get the IDS Administrators extra attention? Are the Administrators able to be notified and respond in a timely manner? A 6 hour gap between occurrence of the threat and follow-up is inadequate.
8. Are threats automatically logged?

TESTING:

1. Obtain from the Security Committee the list of customizations to the IDS signature database they have authorized in the last six months. Select a sample of at least 20 of these

customizations and require the IDS Administrators to prove that these customization requests were implemented. HINT: All of these customizations are risky; otherwise the committee would not have requested the customizations.

2. Ask the IDS Administrator to display the IDS logs from yesterday, 3 weeks ago, and 6 months ago to ensure the logs have been functioning for the entire audit period.
3. Ask the IDS Administrator to identify two recent high-risk attacks that were flagged by the IDS but not the IPS. Ask the IDS Administrator to explain how the attacks avoided the IPS, explain how the attacks were identified by the IDS, and what was done for follow-up.

Encryption

Despite all the organizational telecommunications controls, data leakage and theft are still a problem. Hence the need for encryption. Encryption is based on KEYS, so KEY MANAGEMENT is a major issue for controlling encryption. And *somebody* has to manage these keys. Those people would be called the "Trusted Source", and they are the primary people you will talk to about this section.

QUESTIONS:

1. Who are the "Trusted Source" employees? Are they long-time employees with technical skills who can be trusted?
2. Are there Data Classification Policies that clarify what confidential information needs to be encrypted?
3. Are encryption keys 2048 bits long? Anything shorter is using older technology.
4. For data transmission, does your organization use public key/private key encryption technology? How does the Trusted Source keep the private key confidential?
5. For data at rest (stored data), is a data classification policy used to determine what should be encrypted, and is this encryption based on a private key? How does the Trusted Source keep the private key confidential?
6. When was the last time the Trusted Source changed the private keys? If the private keys have not been changed in the last two years, there is unnecessary increased vulnerability to deencryption attacks.

Testing:

1. Obtain electronic evidence of the last time the private keys were changed. Any keys older than two years is too old.
2. Ask to view the private keys. The Trusted Source should REFUSE. NOBODY except the Trusted Source should d be able to view the private keys. Not even auditors should be allowed to view the keys
3. Review the Data Classification policies and verify they have been reviewed and updated by a security committee in the last year.
4. Selecta sample of obvious data elements that should be encrypted (social security numbers, employee pay rates, customer credit card information, and password tables are good examples). Verify they are noted for extra security in the Data Classification Policies.
5. With the assistance of the Trusted Source and Telecommunications Administrators, ask to view on the telecommunications controller console data during transmission. Ask the Telecommunications Administrators to transmit confidential data, and observe that this data during transmission cannot be viewed unencrypted on the telecommunications controller console.

6. With the assistance IT management, ask to view a sample of raw, confidential data stored on the computerized master files (The sample of data elements you used in Test #4 above is a good list). Observe that these data elements cannot be viewed unencrypted.

Wireless

Wireless is the scourge of all security professionals. The technology is still so new that good security provisions have no fully been invented. That said, there are ways to manage wireless to reduce the risk of vulnerabilities. The key is to allow only athorized and monitored wireless on your office campus, and to encrypt any business information sent over wireless networks.

QUESTIONS:

1. Does the organization have policies prohibiting unauthorized wireless routers and connections?
2. Does the organization have some form of airwave software to "ping" or search for unauthorized wireless networks?
3. Does the organization have air sniffers to search for wireless signals that disrupt or override legitimate organizational wireless signals?
4. Are wireless transmissions automatically encrypted by such technology as SSL (for transmission encryption) and WPA2 (for authentication encryption)?
5. Are unused wall ports disabled?

TESTING:

1. Meet with the airwave software administrator and ask this person to demonstrate how the software works.
2. With the assistance of network administrators, install an unauthorized wireless router into any of the active wall ports used in office area. Then wait to see if the airwave software administrator contacts you within 6 hours with a request to uninstall your unauthorized wireless router.
3. Using an Ethernet cable and your laptop, connect to various unused wall ports throughout the office campus and then try to connect and log in. Hopefully, the ports are disabled and nothing will happen.
4. War Walking - Walk around your office campus with a wireless-enabled laptop, seeking wireless signals. Try to connect through any signal found. Hopefully any signal is secured and will not let you in without a logon ID/password. Keep a record of the wireless signals you find (they each have a name assigned to them), and share this list with the airware software administrator to determine if these signals are internal authorized, internal unauthorized, or a harmless signals from external organizations such as nearby restaurants offering free Wi-Fi.

Certificate Authority

All reputable organizations wanting to do business through the Internet want to be "certified" by a Certificate Authority such as VeriSign. The purpose of a Certificate is to allow customers, vendors, and employees to gain positive assurance that when they attempt to access your organization over the Internet they are really reaching your organization and not a hacking operation pretending to be your organization. To obtain a certificate, your organization is required to identify a "Trusted Source" who is the only person the Certificate Authority will communicate with.

QUESTIONS:

1. Determine who the Trusted Source is. Verify this person is a long-term and trusted employee.

Catching the Successful Hack

No matter how many telecommunication controls and security measures are put in place, hackers will find ways to circumvent and beat them. Build a 20 foot tall fence and they will build a 22 foot ladder. SO IT should install methods to catch successful hackers or at least notify IT security administrators that a hacker has broken in.

QUESTIONS:

1. Does your IT security administrator maintain Honeypots? Honeypots are attractively named databases that contain junk and are 100% access restricted. The moment anybody ever tries to access the honeypot database, the security administrator is automatically and instantly notified.
2. Does your IT security administrator maintain Honeynets? Honeynets are attractive looking network IP addresses that contain fake information that could be of interest by hackers performing port scans. The Honeynet is 100% access restricted. The moment anybody ever tries to access the Honeynet, the security administrator is automatically and instantly notified.

TESTING:

1. Working with the Network Administrators, attempt to gain access to the Honeypot. Determine if the Security Administrator is notified in a time manner.
2. Working with the Network Administrators, attempt to gain access to the Honeynet. Determine if the Security Administrator is notified in a time manner.

Physical Security

Firewalls, telecommunications devices such as routers and bridges, and telecommunications capacity monitors are hardware devices that must be physically secured, typically in telecommunications closets.

QUESTIONS:

1. Meet with Network Administrators to determine where telecommunications hardware is stored.

TESTING:

1. Visit these areas several times during your audit, verifying they are physically secured.

Penetration Testing

All telecommunications security (Firewalls, IPS, IDS, encryption) can become stale or out-of-date and expose your organization to vulnerabilities. Therefore, penetration tests by qualified security professionals should be performed at least annually.

QUESTIONS:

1. Meet with IT management to determine if penetration tests are performed at least annually.

TESTING:

1. Obtain the results of the most recent tests. Ensure the tests were performed by qualified security professionals (NOT internal security, firewall, IPS, and IDS administrators who may be motivated to hide security exposures and holes).
2. Verify the tests are performed at least annually.
3. Obtain evidence that another penetration test is planned and scheduled in the next year.

Telecommunications Costs

Telecommunications costs are quite challenging to figure out. Some telecommunications costs are buried in bizarre line item budgets. Some telecommunications costs are viewed as variable (transmissions) and some are viewed as fixed or capitalized (hardware and software). You COULD attempt to find and quantify all the telecommunication costs (difficult and may be unique to your operation so no benchmarks to compare to). Or, you could take advantage of what is already being done (EASY and comparable to others in your industry). What am I referring to? CHARGEBACK! Telecommunications costs are typically charged back to users and departments based on either 1) usage or 2) fixed fee. Regardless of the method, it provides a window into the costs of telecommunications.

QUESTIONS:

1. What is the chargeback formula for telecommunications costs? Obtain the chargeback tables and rates.
2. What were the chargeback formulas for telecommunications costs for each of the last 5 years?

TESTING:

1. Compare your organization's chargeback rates to those of other organizations in your industry or as published by industry IT trade publications. Require IT to explain extreme variances (There will be some difference, never exactly the same.)
2. Review chargeback rates for the last 5 years. If major changes have occurred in the rates, require IT to explain why.

Tom Salzman
IT Audit Manager, Illinois State University
tomsalzman@ilstu.edu
309-438-3332