



Network Security: 30 Questions Every Manager Should Ask



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

Network Security: 30 Questions Every Manager/Executive Must Answer in Order to Track and Validate the Security of Their Organization

1. What does your network/security architecture diagram look like?

The first thing you need to know to protect your network and systems is what you are protecting. You 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 of devices used (routers, switches, etc.)
- Location of DMZs
- IP address ranges and subnets
- Use of NAT

In addition, you must know where the diagram is stored and that it is regularly updated as changes are made.

2. What resources are located on your DMZ?

Only systems that are semi-public should be kept on the DMZ. This includes external web servers, external mail servers, and external DNS. A split-architecture may be used where internal web, mail, and DNS are also located on the internal network.

3. What resources are located on your internal network?

In addition to internal web, mail, and DNS servers, your internal network could also include databases, application servers, and test and development servers.

4. Where is your organization's security policy posted and what is in it?

There should be 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 policies to address for individual systems. Most importantly, the policies should address the appropriate use of computing resources. 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.



5. What is your organization's password policy?

A password policy should require that a password:

- Be at least 8 characters long
- Contain both alphanumeric and special characters
- Change every 60 days
- Cannot be reused after every five cycles
- Is locked out after 3 failed attempts

In addition, you should be performing regular password auditing to check the strength of passwords; this should also be documented in the password policy.

6. What applications and services are specifically denied by your organization's security policy?

Your organization's security policy should specify 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
- Use of unencrypted remote connections such as Telnet and FTP

7. What types of IDSs does your organization use?

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.

8. Besides default rulesets, what activities are actively monitored by your IDS?

IDSs come with default rulesets to look for common attacks. These rulesets must also be customized and augmented to look for traffic and activities specific to your organization's security policy. For example, if your organization's security policy prohibits peer-to-peer communications, then a rule should be created to watch for that type of activity. In addition, outbound traffic should be watched for potential Trojans and backdoors.



9. What type of remote access is allowed?

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), unsecured wireless access points, and other vulnerable methods of remote access should be prohibited.

10. What is your wireless infrastructure?

Part of knowing your network architecture includes knowing the location of wireless networks since they create another possible entry point for an attacker. You must also confirm whether they are being used for sensitive data and are they secured as best as possible.

11. How is your wireless infrastructure 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 your wireless network should not be used for sensitive data. Consider moving to the 802.11i standard with AES encryption when it is finalized.

12. What desktop protections are used?

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 must also be centrally managed and controlled.

13. Where, when, and what type of encryption is used?

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.

14. What is your backup policy?

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.



15. How is sensitive information disposed?

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 destroyed. Simply deleting a file is not sufficient to prevent attackers from undeleting the file later. If you are disposing of a computer system, be sure to erase all sensitive files from the hard drive by using a wipeout utility.

16. What is included in your disaster recovery plan?

Your disaster recovery plan (DRP) should include recovery of data centers and recovery of business operations. It should also include recovery of the accrual physical business location and recovery of the business processes necessary to resume normal operations. In addition, the DRP should address alternate operating sites.

17. How often is your disaster recovery plan tested?

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

18. What types of attacks are you seeing?

Typically an organization sees a constant stream of port scan attacks. These are a regular occurrence on the Internet as a result of attackers and worms. An organization should not be seeing many substantial attacks such as compromises, backdoors, or exploits on systems. This would indicate that the security defenses are weak, patching may not be occurring, or other vulnerabilities exist.

19. How often are logs reviewed?

Logs should be reviewed every day. This includes IDS logs, system logs, management station logs, etc. Not reviewing the logs is one of the biggest mistakes an organization can make. Events of interest should be investigated daily. It can be a very tedious task for a single person to do this job as their only assignment (unless they really enjoy it). It is better to have a log review rotation system amongst the security team.

20. How often are you performing vulnerability scanning?

An organization should be performing vulnerability scanning as often as possible, depending on the size of the network. The scanning should be scheduled to allow adequate time to review the reports, discover anything that has changed, and mitigate the vulnerability.



21. What physical security controls are in place in your organization?

Physical security is a large area that must be addressed by an organization. Examples of physical controls includes 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.

22. What are your critical business systems and processes?

Identifying your 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 necessary security controls. 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.

23. What are the specific threats to your organization?

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. You should consider both 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.

24. What are the tolerable levels of impact your systems can have?

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

25. Are you performing content level inspections?

In addition to the content level inspection performed by the IDS, specific content inspections 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 in legitimate communications, attacks with malicious data, and unauthorized application usage.



26. How often are your systems patched?

Systems should be patched every time a new patch is released. 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. You must schedule regular maintenance downtime 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.

27. How are you protecting against social engineering and phishing attacks?

The best way to protect against social engineering and phishing attacks is to educate the users. Employees should attend security awareness training that explains these types of attacks, what to expect, and how to respond. There should also be a publicly posted incidents email address to report suspicious activity.

28. What security measures are in place for in-house developed applications?

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 standard requirements and testing procedures. Code reviews should be conducted by a test team 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.

29. What type of traffic are you denying at the firewall?

There should be a default deny rule on all firewalls to disallow anything 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.

30. How are you monitoring for Trojans and backdoors?

In addition to periodic vulnerability scanning, outgoing traffic should be inspected before it leaves the network, looking for potentially compromised systems. Organizations often focus on traffic and attacks coming into the network and forget about monitoring outgoing traffic. Not only will this detect compromised systems with Trojans and backdoors, but it will also detect potentially malicious or inappropriate insider activity.



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

