CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH

NETWORK CYBERSECURITY CHEAT SHEET

① Threats

Every Business faces threats from many directions. Each time you add devices, users, and applications the more vulnerable your network becomes

② Network Security Basics

Operations designed to protect the integrity and functionality by targeting a variety of threats and stopping them from entering or infiltrating through your data and computer systems is referred to as network security. It includes management of both hardware and software technologies. Using a combination of defensive security layers at the network edge and throughout the system, it executes policies and controls that block malicious actors from deploying their exploits and attacks while providing access to employees supporting business operations.

③ Network Security Benefits

Network security protects your reputation by protecting proprietary information from attack while delivering the services your customers and employees demand.

Network Security for SMB ④

1. Closely monitor all traffic - Monitor the activity logs for network traffic coming into and out of your firewall. It is important that these reports are read and analyzed carefully. You can not simply rely on alerts to flag dangerous activity. Assign someone on your team who thoroughly understands the data and is trained to take the necessary action.

2. Stay up on the latest threats - Watch for the discovery of any new threats as they are posted online. I recommend subscribing to email alerts from the U.S. Computer Emergency Readiness Team (US-CERT, a division of Homeland Security) on any recently confirmed software vulnerabilities and exploits.

3. Update frontline defenses regularly - It is important that you have a strong frontline defense at your network edge. Make sure your firewall and antivirus, anti-malware software is secure by enabling regular updates.

4. Employee Awareness Training - Employee regular training for employees to assure they maintain security awareness understand your acceptable use policy. Whenever you make changes to your policies be sure to provide training on why the changes were made, how it affects them and why the changes were necessary.

Continue reading on next page >

NETWORK CYBERSECURITY CHEAT SHEET

④ Network Security for SMB (con't)

Everyone is responsible for security. If anyone in your organization notices anything suspicious or out of the ordinary they should notify the appropriate person immediately.

5. Protect against data loss - Data loss prevention (DLP) solutions protects your sensitive business data and information from data breaches or unwanted compromise of sensitive data. These systems identify, classify, and track the movement of confidential data throughout the enterprise preventing unauthorized disclosure of data with disclosure policies.

⑤ Security Solutions

There are a number of security solutions that extend your perimeter defenses and can assist you in protecting your network while promoting expeditious business operations.

1. Anti-Virus and Anti-Malware Software: These products are commonly used interchangeably as they both refer to software designed to detect, protect against, and remove malicious software. While antivirus software uses a method of signature-based threat detection to protect you from viruses and it works to a degree. Anti-malware on the other hand, detects threats by using heuristic techniques that look for malicious behavior and suspicious activity by scrutinizing the overall structure, programming logic, and data. It looks for things like unusual instructions or junk code to identify threats it has never seen before.

(CONTINUED)

Security Solutions (con't) ⑤

2. Access Control - The principle of least privilege (POLP), is a security design principle that restricts user and program privileges to only those necessary for the required job.
   a. Make least privilege the default for all accounts.
   b. Elevate privileges on a situational and timed basis only.
   c. One-time use permissions are a good way to provide necessary access while maintaining control.
   d. Monitor and track all network activity, including individual logins, system changes, and access requests.
   e. Ensure a flexible access management platform is in place so that privileges can be securely elevated and easily downgraded.
   f. Identify and separate high-level system functions from lower-level functions.
   g. Regularly audit privileges granted to users and applications for relevance.
3. Application security - Application security encompasses the hardware, software, and processes you use to close those vulnerabilities in applications that attackers can use to breach and infiltrate your network.
4. Behavioral analytics - These types of tools automatically discern activities that deviate from the norm. They are used to better identify indicators of compromise that pose a potential problem and quickly remediate threats.
5. Data loss prevention - These technologies tools can stop people from uploading, forwarding, or even printing critical information in an unsafe manner.
6. Firewalls - Create a barrier between your trusted internal network and untrusted outside networks, such as the Internet using a set of defined rules to allow or block traffic. These come as either a hardware, software, or both.

NETWORK CYBERSECURITY CHEAT SHEET

(CONTINUED)

③ Security Solutions (con't)

6. Intrusion Protection System (IPS) - Scans all network traffic to actively block attacks by correlating huge amounts of global threat intelligence to not only block malicious activity but also track the progression of suspect files and malware across the network to prevent the spread of outbreaks and reinfection.
7.Mobile Device Security - Cybercriminals are increasingly targeting mobile devices and apps. You need to control which devices are allowed to access your network and configure their connections to keep network traffic private.
8. Network Segmentation - Using software-defined segmentation allows network traffic to be classified differently in order to make enforcing security policies easier. With these systems can assign access rights based on role, location, and more so that the right level of access is given to the right people and suspicious devices are contained and remediated.
9. Virtual Private Network (VPN) - Is responsible for encrypting the connection from an endpoint to a network, often over the Internet. Using IPsec or Secure Sockets Layer to authenticate the communication between device and network.
10. Web Security - A web security solution will control your staff's web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud.

Get Started Now ⑥

1. Policies and Rules - At minimum you should implement and enforce the following:
    - Acceptable Use Policy
    - Internet Access Policy
    - Email and Communications Policy
    - Network Security Policy
    - Remote Access Policy
    - BYOD Policy
    - Encryption Policy
    - Privacy Policy
2. Provision Servers - Your servers are where most of your company's most valuable data resides. Create a server deployment checklist, and make sure each of the following steps are performed before any server is put into production.
    - Create Server list
        - Name
        - Purpose
        - IP.address
        - Date of service
        - Service tag (if physical)
        - Rack location or default host
        - Operating system
        - Responsible person
    - Assign Responsible party per server
    - Use Naming convention
    - Configure Network
    - Install IP Address Management (IPAM)
    - Perform patching
    - Install Anti-Virus/Anti-Malware
    - Install Host Intrusion Protection
    - Install Remote Access
    - Employ UPS and Power Saving
    - Rename administrator account and set password
    - Set local group memberships and assign permissions
    - Create organizational units with appropriate policies

Continue reading on next page >

NETWORK CYBERSECURITY CHEAT SHEET

⑥ Get Started Now (con't)

- Confirm reporting to management consoles
- Disable unnecessary services
- Configure SNMP
- Install Agents
- Perform complete backup
- Restore from backup
- Perform Vulnerability Scan
- Sign into Production

3. Deploy Workstations
   - Create Workstation list
   - Assign the user
   - Use naming convention
   - Configure the network
   - Perform Patches
   - Install Anti-Virus/Anti-Malware
   - Configure Host Intrusion Prevention/Firewall
   - Enable Remote Access (one method)
   - Deploy Power Saving
   - Assign Domains
   - Create Administrator Account
   - Set local group memberships and assign permissions
   - Create organizational units with appropriate policies
   - Confirm reporting to management consoles
   - Perform complete backup
   - Restore from backup
   - Set Encryption
   - Perform Vulnerability Scan

4.Network Equipment
   - Create Network Hardware List
   - Configure Network
   - Install IP Address Management (IPAM)

(CONTINUED)

Get Started Now (con't) ⑥

   - Perform patching
   - Install Remote Access
   - Use unique credentials
   - Configure SNMP
   - Perform complete backup
   - Restore from backup
   - Perform Vulnerability Scan

Switches
   - Server
   - Computers (Desktops/Laptops)
   - Printers/Scanners
   - Network Switches
   - ADSL Modem
   - Use VLANs for Segregation
   - Set port restrictions of promiscuous devices and hubs
   - Disable ports not assigned to specific devices
   - Firewalls
     - Explicit Permits/Implicit Denies
     - Logging & Alerts
     - Routers & Routing Protocols

Vulnerability Scans
   - Weekly external scan
   - Compare differences weekly
   - Internal Scans monthly

Backups
   - Tape/Hard Disk Rotation
   - Destruction of Old Tapes/Disks
   - Secure Offsite Storage
   - Encryption
   - Restricted Access to Backup Operators Group
   - Regularly Complete full restores

Remote Access
   - Set up Approved method
   - Maintain
   - Two-Factor Authentication

Continue reading on next page >

NETWORK CYBERSECURITY CHEAT SHEET

⑥ Get Started Now (con't)

Regular reviews
Set and enforce strong lockout policies
Configure VPNs

8. Wireless Networking
   SSID
   Encryption
   Authentication
   Guest Network
   BYOD
9. Email
   Email Filtering - inbound and outbound
   Confirm edge device rejection rules
   Deploy mail filtering on full range of email threats
10. Internet Access
    Encryption
    Malware Scanning
    Bandwidth Restrictions
    Port Blocking
11. File Shares
    Remove "the everyone" and authenticated user groups
    Least Privilege
    Groups
    Avoid Deny Access
12. Log Solution and Correlation
13. Time Management for syncing