Network security

From Wikipedia, the free encyclopedia

In the field of networking, the specialist area of **network security**[1] consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources.

Contents

The first step to information security

The terms network security and information security are often used interchangeably. Network security is generally taken as providing protection at the boundaries of an organization by keeping out intruders (hackers). Information security, however, explicitly focuses on protecting data resources from malware attack or simple mistakes by people within an organization by use of data loss prevention (DLP) techniques. One of these techniques is to compartmentalize large networks with internal boundaries.

Network security concepts

Network security starts from authenticating the user, commonly with a username and a password. Since this requires just one thing besides the user name, i.e. the password which is something you 'know', this is sometimes termed one factor authentication. With two factor authentication something you 'have' is also used (e.g. a security token or 'dongle', an ATM card, or your mobile phone), or with three factor authentication something you 'are' is also used (e.g. a fingerprint or retinal scan).

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users.[2] Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS)[3] help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network and traffic for unexpected (i.e. suspicious) content or behavior and other anomalies to protect resources, e.g. from denial of service attacks or an employee accessing files at strange times. Individual events occurring on the network may be logged for audit purposes and for later high level analysis.

Communication between two hosts using a network could be encrypted to maintain privacy.

Honeypots, essentially decoy network-accessible resources, could be deployed in a network as surveillance and early-warning tools as the honeypot will not normally be accessed. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis could be used to further tighten security of the actual network being protected by the honeypot.[4]

Security management

Security Management for networks is different for all kinds of situations. A small home or an office would only require basic security while large businesses will require high maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

Small homes

- A basic firewall or a unified threat management system.
- For Windows users, basic Antivirus software. An anti-spyware program would also be a good idea. There are many other types of antivirus or anti-spyware programs out there to be considered.
- When using a wireless connection, use a robust password. Also try to use the strongest security supported by your wireless devices, such as WPA2 with AES encryption.
- If using Wireless: Change the default SSID network name, also disable SSID Broadcast; as this function is unnecessary for home use. (However, many security experts consider this to be relatively useless. http://blogs.zdnet.com/Ou/index.php?p=43)
- Enable MAC Address filtering to keep track of all home network MAC devices connecting to your router.
- Assign STATIC IP addresses to network devices.
- Disable ICMP ping on router.
- Review router or firewall logs to help identify abnormal network connections or traffic to the Internet.
- Use passwords for all accounts.
- Have multiple accounts per family member, using non-administrative accounts for day-to-day activities. Disable the guest account (Control Panel> Administrative Tools> Computer Management> Users).

- Raise awareness about information security to children.[5]

Medium businesses

- A fairly strong firewall or Unified Threat Management System
- Strong Antivirus software and Internet Security Software.
- For authentication, use strong passwords and change it on a bi-weekly/monthly basis.
- When using a wireless connection, use a robust password.
- Raise awareness about physical security to employees.
- Use an optional network analyzer or network monitor.
- An enlightened administrator or manager.

Large businesses

- A strong firewall and proxy to keep unwanted people out.
- A strong Antivirus software package and Internet Security Software package.
- For authentication, use strong passwords and change it on a weekly/bi-weekly basis.
- When using a wireless connection, use a robust password.
- Exercise physical security precautions to employees.
- Prepare a network analyzer or network monitor and use it when needed.
- Implement physical security management like closed circuit television for entry areas and restricted

zones.
- Security fencing to mark the company's perimeter.
- Fire extinguishers for fire-sensitive areas like server rooms and security rooms.
- Security guards can help to maximize security.

School

- An adjustable firewall and proxy to allow authorized users access from the outside and inside.
- Strong Antivirus software and Internet Security Software packages.
- Wireless connections that lead to firewalls.
- Children's Internet Protection Act compliance.
- Supervision of network to guarantee updates and changes based on popular site usage.
- Constant supervision by teachers, librarians, and administrators to guarantee protection against attacks by both internet and sneakernet sources.

Large government

- A strong firewall and proxy to keep unwanted people out.
- Strong Antivirus software and Internet Security Software suites.
- Strong encryption.
- Whitelist authorized wireless connection, block all else.
- All network hardware is in secure zones.
- All host should be on a private network that is invisible from the outside.
- Put web servers in a DMZ, or a firewall from the outside and from the inside.
- Security fencing to mark perimeter and set wireless range to this.

References

1. ^ Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". *Lecture Notes in Computer Science* **3285**: 317–323.
2. ^ A Role-Based Trusted Network Provides Pervasive Security and Compliance (http://newsroom.cisco.com/dlls/2008/ts_010208b.html?sid=BAC-NewsWire) - interview with Jayshree Ullal, senior VP of Cisco
3. ^ Dave Dittrich, *Network monitoring/Intrusion Detection Systems (IDS)* (http://staff.washington.edu/dittrich/network.html) , University of Washington.
4. ^ *Honeypots, Honeynets* (http://www.honeypots.net)
5. ^ Julian Fredin, Social software development program Wi-Tech

Further reading

- Security of the Internet (http://www.cert.org/encyc_article/tocencyc.html) (*The Froehlich/Kent Encyclopedia of Telecommunications vol. 15*. Marcel Dekker, New York, 1997, pp. 231-255.)
- *Introduction to Network Security* (http://www.interhack.net/pubs/network-security) , Matt Curtin.
- *Security Monitoring with Cisco Security MARS* (http://www.ciscopress.com/bookstore/product.asp?isbn=1587052709) , Gary Halleen/Greg Kellogg, Cisco Press, Jul. 6, 2007.
- *Self-Defending Networks: The Next Generation of Network Security* (http://www.ciscopress.com/bookstore/product.asp?isbn=1587052539) , Duane DeCapite, Cisco Press, Sep. 8, 2006.
- *Security Threat Mitigation and Response: Understanding CS-MARS* (http://www.ciscopress.com/bookstore/product.asp?isbn=1587052601) , Dale Tesch/Greg Abelar, Cisco Press, Sep. 26, 2006.
- *Deploying Zone-Based Firewalls* (http://www.ciscopress.com/bookstore/product.asp?isbn=1587053101) , Ivan Pepelnjak, Cisco Press, Oct. 5, 2006.
- *Network Security: PRIVATE Communication in a PUBLIC World*, Charlie Kaufman | Radia Perlman | Mike Speciner, Prentice-Hall, 2002. ISBN .
- *Network Infrastructure Security* (http://www.springer.com/computer/communications

/book/978-1-4419-0165-1) , Angus Wong and Alan Yeung, Springer, 2009.

See also

- Cloud computing security
- Crimeware
- Data Loss Prevention
- Wireless LAN Security
- Timeline of hacker history
- Information Leak Prevention
- Network Security Toolkit
- Metasploit Project
- TCP sequence prediction attack
- TCP Gender Changer
- Netsentron
- Cyber security standards

External links

- [1] (http://www.deepnines.com/secure-web-gateway/definition-of-network-security) Definition of Network Security
- Cisco IT Case Studies (http://www.cisco.com/web/about/ciscoitatwork/case_studies/security.html) about Security and VPN
- Debate: The data or the source - which is the real threat to network security? - Video (http://www.netevents.tv/docuplayer.asp?docid=102)
- OpenLearn - Network Security (http://openlearn.open.ac.uk/course/view.php?id=2587)

Retrieved from "http://en.wikipedia.org/wiki/Network_security"
Categories: Computer network security