Group Project 4: Security

Brian Bergstrom

ITCO 251

4/21/17

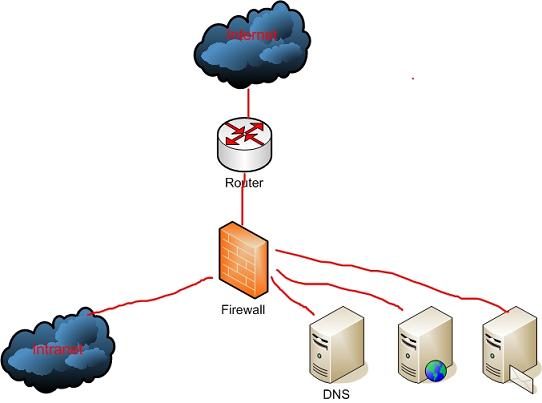
AIU Online

Michael Pry

It is important for the network administrator to monitor the security of the network. Lots of things can happen to a network if it is unprotected and not cared for properly. Hackers are always looking for small vulnerabilities to infiltrate themselves into a company network to steal sensitive consumer information that can do a lot of damage for both the company and the people involved. That is why it is important to practice good security measures to keep valuable information safe.

Everyone in the company should be very familiar with the company policy regarding even the most basic computer use rules. Simple things like creating a good password and not sharing your password may seem like common sense, but it’s simple mistakes in those areas that can allow unauthorized access on the network. Much of the security breaches that happen in companies are not external, but internal, meaning the attack was done from inside the company. In 2016, “IBM found that 60% of these attacks were carried out by insiders” (Zadelhoff, 2016). Who has access to what should also be made clear and monitored. No one should have administrator access to the router or network unless they are qualified personnel approved by the company. Employees should report any suspicious activity they see immediately. Waiting can cost in the long run.

How the network is configured is also a very important factor to consider. Isolating subnets is way of controlling where a virus or malware might go so it does not spread throughout the entire network (Parker, 2006). This is especially key for larger organizations.



(Parker, 2006).

The router is the first thing something will encounter when entering the network. It is vitally important the administrator keeps a tight lock and key on access to it virtually and physically. Unauthorized access again can cause a lot of damage to the network and cost the company a lot of money in repair costs. Following safe practices saves money in the long run, even if extra money is spent on keeping security lock tight. By the year 2020, “organizations are expected to spend $101.6 billion on cybersecurity (Vanlan, 2016). A company that spends little on security will be very unsecure and may lose business due to customers getting their information hacked so security breaches occurring on a regular basis.

Before anything gets inside the network, it has to go through a firewall. This is the shield that protects against idle threats and other harmful things. Each building should have one as it is the last line of defense before the breach can occur. Securing the firewall might be a pain, blocking certain access to other things, but it is necessary for security to run smoothly across the board. One hole, and intruders can take advantage and make one regret not investing in it.

Conducting what is called a posture assessment is another great idea to assess the level of security a company has. A posture assessment is “a thorough examination of each aspect of the network to determine how it might be compromised” (Dean, 2013, p.495). This could mean hiring an independent party to try and hack the network to test and asses the vulnerability of the network at each level. When the assessment is done by an accredited third party, it is known as a security audit. This should be done on a regular basis as threats are growing more and more sophisticated as the days go by. Keeping everything up do date and secure will prevent any unauthorized attempts from happening.

There are two common types of security risks hackers can take advantage of: people and hardware. “By some estimates, human errors, ignorance, and omissions cause more than half of all security breaches sustained by networks” (Dean, 2013, p.496). That is why it is very important that all personnel are educated about the proper procedures and what to look out for. Someone claiming to be an authority will probably never ask for your login credentials. These credentials should never be given out except to authorized parties within the company. Acquiring credentials to a well-protected network is known as social engineering because the attacker gets creative when trying to obtain such information. The hacker is counting on employees and users to be ignorant. Educating everyone about these kinds of threats makes them aware and prevents passwords from getting into the wrong hands.

Hardware is the second thing that is very vulnerable. Physical access must be heavily protected and secured. This involves the Physical, Data Link, and Network layers of the OSI model. NIC cards, routers, and switches all are included in these layers. An example would be an intruder listening in on transmissions through a switch on something called a protocol analyzer. This method is very sophisticated and requires certain expert level in skill. Transmissions can also be intercepted and redirect sensitive information to another location unknown to anybody but the hacker (Dean, 2013, p.498). masking internal subnets can also be a good practice. Otherwise, intruders can read private addresses. Passwords for switches routers and other hardware should not be easily guessed and probably should be long and complicated to make it more secure and harder to hack. Storing the information in a safe place is also critical. It might be best to write it down or print it out instead of store it electronically. Another risk is to have open ports. Having them open just gives an intruder an invitation in (Dean, 2013, p.498). Educating the proper staff on these procedures and rules is critical so the entire company can be on the same page.

Security is a very expensive ting to have, but in the long run, it saves the company a lot of time and money. Education and regular practice can prevent mistakes from happening and can help improve the overall security of company data.

# Works Cited

Dean. (2013). *Network+ Guide to Networks, 6th Edition*.

[Bookshelf Online]. Retrieved from https://online.vitalsource.com/#/books/9781133608196/

Parker, D. (2006, August 16). *Network design and defense.* Retrieved from TechGenix: http://techgenix.com/Network-design-defense/

Vanlan, J. (2016, October 12). *Here's how much businesses worldwide will spend on cybersecurity by 2020.* Retrieved from Fortune: http://fortune.com/2016/10/12/cybersecurity-global-spending/

Zadelhoff, M. v. (2016, Septmebr 19). *The biggest cyber security threats are inside your company.* Retrieved from Harvard Business Review: https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company