The Absence of Information Security

Chase Franse

Saint Leo University - COM 203

Introduction

There are individuals and businesses in every corner of the world that have sensitive information that they don’t want other people to find - from a simple private home server, to a hospital’s patient records, to a multimillion-dollar company’s financial files. However, simply wanting these records to remain private is not always enough; as long as there are people who want the data you have, the need for information assurance and security will always exist. The problem is that the majority of people have the preconceived notion that it isn't their job to protect their data. In a business, most employees will say that it is the IT department's job. When it comes to their personal data, most people might say that they bought some form of antivirus and that is some kind of magical, silver bullet against all forms of threats against their data. All of these people, however, would be *wrong*. This mindset, and therefore people's lack of proper information assurance, is one of the biggest issues with technology today.

Information Assurance

Information Assurance (IA) is defined, very officially, by the National Information Assurance Glossary as procedures that ensure the protection of information systems by assuring the defense of their availability, authentication, confidentiality, integrity, and non-repudiation (Wilibanks, 2008). But let's dial back the computer speak for a moment; at its simplest, information assurance is the protocols that are put in place to protect data from corruption and/or theft. Doesn't seem so scary, now does it? Based on my research, are three major categories in information assurance:

- Digital Security
- Interpersonal Security
- Physical Security

All three of these categories are vital to the success and protection of everyone’s data. Digital security is the most complicated of the three and physical security being the least complicated. While there are varying levels of complexity with just these three, seemingly simple, categories, no category is any superior to another. They are all equally essential to the protection of the user's data, and the purpose for this research project is to inform people of the threats they face in regards to their information.

Digital Security

Digital security is what the majority of the world thinks of when approaching the topic of information assurance. Digital security is certainly the most common way to protect data, it is not, however, the only way. This category includes all types of software that attempt to protect data on a user's system: antivirus, anti-malware, anti-phishing software, etc. The most common attempt to get confidential information from a person or company's information system is through faulty digital security. There are a large number of types and styles of attack while keeping everything in the fantastical realm of computers. Some of the digital attacks that are common include:

- Viruses
- Trojans
- Rootkits
- Spyware
    - Keyloggers
- Ransomware
- Rogue Antivirus
- Etc.

Viruses, rootkits, spyware, and ransomware are all programs created with malicious intent, that are installed onto a user's system from the outside. Sometimes, in the case of trojans in specific, someone downloads a program from the internet that looks legitimate, however, it is sometimes actually this malicious software that is intended to either provide access to your device, or to simple wreak havoc on it. Trojans are special because they masquerade as legitimate programs, until they are activated to do any number of nasty things to your computer or information systems.

Rogue antivirus malware is also particularly special because they don't just pretend to be any old program, no, these programs are running around wearing the mask of a legitimate antivirus or other security program. These false antivirus programs will eventually tell the user that their computer is infected with a virus and they must pay the antivirus company for a malware removal tool. However, as you can probably guess, this "malware removal tool" isn't real, and the user who falls for this has just literally paid for more malware to be installed on their system. The majority of people believe that all of this can be avoided by simply installing and/or paying for a legitimate antivirus or other system security tool, but they are very wrong. Bruce Schneier, a computer security professional, is known to have said, "Security is not a product, it's a process" - and he couldn't be more right.

Interpersonal Security

Similar to Benjamin Franklin's famous quote about death and taxes being inevitable, Albert Einstein is known to have said, "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former." Social engineering (SE), is the uncontestably *weakest* link in the chain of information assurance and security, and it is made successful because of human stupidity just a much as much as ignorance. SE is a combination of a plethora of different techniques that are designed and used to exploit a person into giving restricted information to people who aren't supposed to have that information. Social engineers employ a number of different tactics in order to trick people into giving them the information they're after. The engineer might pretend to be someone of higher authority in your company who needs a confidential document from you, or maybe they'll pretend to be someone in the IT department who wants to perform an update on your computer - the possibilities are endless, which is why it is such a big problem.

Just as there are different types of digital attacks, there are a few different types or styles of SE attacks. The two most common are *phishing* and *pharming*. Phishing is more common and is usually seen as a nuisance, but not usually particularly dangerous. Many people believe they're safe from phishing (or scam) emails and the such because they believe their email's spam filter is guaranteed to stop any malicious emails from ending up in their inbox. However, as mentioned before, there is no silver bullet in information assurance. Even though they're a common occurrence, people fall for phishing scams all the time. In 2014, a *Target* employee fell for a phishing scam and accidently exposed the confidential data of 110 million customers (Silic, Back, 2016).

Pharming is different than phishing - while they are both SE attacks, pharming poisons a DNS server with false URLs and then the hacker has to simply wait for someone to fall into the trap they've set; that's why pharming is scarier than phishing - users don't have to do anything out of the ordinary to fall for a pharming attack (Leon, 2005). Think about it this way; when you go fishing you put bait on a hook, throw it in the water, and wait. When you are farming, you plant the seeds, and wait for the results to show. It's the same with phishing and pharming - social engineers can send out emails and wait for you to take the bait, or they can plant their malicious seeds and wait for you to spring their trap.

Physical Security

Physical security is the easiest category to understand, and the easiest to assure. This category of information assurance and security is concerned with the actual, *physical* information systems and connected nodes throughout a business or home network. If a company computer is stolen, the chances that company's network will be broken into skyrockets. If a company's server room was open to the public, literally anyone could go an plug a USB in, with some form of malicious code on it, and the entire information system would be compromised.

Potential Solution

The solution seems absurdly simple, but it is sometimes the simplest solutions that work the best. That solution is education. Lots of companies already do this, but if people really knew what they were up against, they might just be better equipped to handle it when, not “if,” it happens to them People need to understand that there is no one-stop-shop for information assurance, but instead there are a number of steps that are involved to really make sure your data is secure and protected. A good place to start would be with a good antivirus program, a locked server room with restricted access, and a good knowledge of SE - this includes teaching your employees about SE as well.

Summary

There are three main sub-categories of information assurance: digital, interpersonal, and physical security. Digital security encompasses what you'd expect: viruses, malware, spyware, antivirus programs, etc. Interpersonal security is the part that most people forget about entirely. Social engineering is a big part of this category - social engineering is defined as the method or process by which an attacker persuades or deceives another person into achieving the attacker's goal. This goal could be to gather confidential information, it could be to gain access to a restricted location, or just about anything else that benefits the attacker in some way, shape, or form.

Two of the most common forms of social engineering are phishing and pharming. Phishing is usually found in emails that are sent from a seemingly trustworthy source, when in reality they are manufactured with malicious intent and will almost certainly affect your computer or information system in one way or another should you be unlucky enough to fall for one. Pharming is a little different.; instead of you falling for a trick as you would if you were hit with a phishing scam, you could be hit by a pharming attack without any unusual input on your part. Pharming is when attackers "plant seeds" to fake websites in a DNS server, and when you go to access a site that would normally work legitimately, you would be sent to a facade of a site that is designed to steal your information.

Finally, the third category of information assurance is physical security. This is the easiest to accomplish and the simplest to fully understand. Physical security is concerned with the actual location of the information system and all the nodes that are given access to said information system. All of these things are majorly important to the security and success of any business, large or small, and the problem is that the majority of people today neglect their responsibilities in regard to the security of their information, but they still expect their data to remain secure. The solution to this problem is to simply send them back to school, albeit, a little more specialized this time. If people knew what they were responsible for and how to protect their data, chances are that they'd be more vigilant about it, and we'd all be making the black hat hackers’ jobs a little harder.

References

Barwise, M. (2014). “What is Risk?”, *ITNOW, 56*(2), 28–29.

Mitchell, J. (2017). Information systems assurance, *Itnow*, *59*(2), 10-11.

Harris, S. (2018, September 12). Cyber security threats against small businesses on the rise in 2018.

Wilbanks L. (2008). , "Need to Share vs. Need to Assure," *IT Professional*, vol. 10, no. 3, pp. 64-64.

Khan, M. K., & Alghathbar, K. (2010). Special Issue - Information assurance and security engineering. *IETE Technical Review*, *27*(3), 201–202.

Bunker, G. (2012). Technology is not enough: Taking a holistic view for information assurance, Information Security Technical Report, 17(1/2), 19–25.

Mitnick, K. & Simon, W. (2002). *The Art of Deception: Controlling the Human Element of Security,* New York, NY: John Wiley & Sons, pg. 12.

Xin Luo, Brody, R., Seazzu, A., & Burd, S. (2011). Social Engineering: The Neglected Human Factor for Information Security Management, *Information Resources Management Journal*, *24*(3), 1–8.

Gupta, B B & Arachchilage, Nalin & Psannis, Kostas. (2017). Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions. Telecommunication Systems.

Silic, M., & Back, A. (2016). The dark side of social networking sites: Understanding phishing risks, *Computers in Human Behavior*, *60*, 35–43.

Leon, M. (2005). The Looming Threat of PHARMING. *InfoWorld*, *27*(23), 39–42.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios, Computers & Security, 59, 186–209.

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept, *Computers & Security*, *73*, 102–113.

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks, International Journal of Advanced Computer Research, 6(23), 31–38.

Wilson, K. S. (2013). Conflicts among the pillars of information assurance, *IT Professional*, 15(4), 44–49.

Voas, J., & Wilbanks, L. (2008). Information and quality assurance, *IT Professional*, 10(3), 10–13.

Hamill, J. T., Deckro, R. F., & Kloeber Jr., J. M. (2005). Evaluating information assurance strategies, *Decision Support Systems*, 39(3), 463–484.

Ezingeard, J.-N., McFadzean, E., & Birchall, D. (2005). A model of information assurance benefits, *Information Systems Management*, *22*(2), 20–29.