Future Privacy and Security Controls

By: Michelle R. Sellers

April 13, 2016

Contents

Introduction

Technology is moving so quickly, it’s difficult to keep up with the security features that are needed to keep it secure. As a result; after a tool, device, or software are released, there is usually a security patch or several security patches that follow to secure it. Sometimes this security comes a little too late.

The future of technology is heading more towards mobility and ease of use. Employers want their employees to be able to work from anywhere and at any time. The problem with this is that with mobility and ease of use; also come security issues that need to be considered for better privacy and security controls.

For the purposes of this paper, we will discuss several technology issues that are leaning towards mobility and ease of use for users, we will discuss the reason these technologies are flawed, and discuss recommendations to reduce future privacy and security risks. We will also discuss three types of people that can be the cause of such security risks and the recommendations that can be used to significantly reduce these risks.

Technology Issues

There are many technologies that fit the description of being both mobile and easy to use. Listed below are the technologies we will discuss that fall within these categories. Of course, this is not an exhaustive list of technologies, and will only scratch the surface of technologies that need to be considered when analyzing the future of security in a technological aspect.

Cloud computing – According to Rouse, M. “Cloud computing is a general term for the delivery of hosted services over the Internet.” (2016)

Trusting for services or data to be hosted over the internet is a consideration that shouldn’t be taken lightly. Just because a company is putting their data in a new location doesn’t mean that it’s entirely secure. There are still risks that are involved, and there are still several problems that should be considered with cloud computing. An article by Rashid, F. (Mar. 2016) lists 12 threats that environments could face when using cloud computing; those are as follows:

1. Data Breaches
2. Compromised credentials and broken authentication
3. Hacked interfaces and APIs
4. Exploited system vulnerabilities
5. Account hijacking
6. Malicious insiders
7. The APT parasite
8. Permanent data loss
9. Inadequate diligence
10. Cloud service abuses
11. DoS attacks
12. Shared technology, shared dangers

This list of threats with cloud computing is almost as long as the list of threats from hosting your information and services internally. This means we can’t assume that just because data is in a different location and entrusted to someone else that it is safe. There are vulnerabilities in nearly every technology and cloud computing isn’t an exception to the rule.

Mobile Devices – According to WiseGeek, “A mobile device, or handheld, is an electronic device that enables some kind of computing, and which is small enough to be easily carried around.” (2016)

Mobile devices could include anything that can be easily transported. This could include cell phones, laptops, multimedia players, and tablets. Because of the portability of mobile devices this puts them at risk for being lost or stolen. There is also a risk associated with the possibility of the user connecting the device to a network that isn’t secure.

Wireless Communication – According to Kumar and Gambir (2014), “Wireless communication is the exchange of data between two or more points that are not joined by an electrical transmitter.” (p. 25).

A wireless network uses radio frequency transmissions such as electromagnetic waves for transmitting voice and data. There are currently 5 types of wireless communication, these are infrared, Bluetooth, Wi-Fi, radio, and cell phone. Because of the way these communicate through the open air, this makes them inherently difficult to secure and creates many avenues for attack. (Sellers, p5)

People Issues

Technology isn't the only security flaw. There are people that can also create security risks to an IT environment. The three types of people we will discuss as security risks are the IT administrator, the end-user, and the attacker. These are definitely not the only risks to an IT environment, but they are the most common.

The IT administrator – The biggest problem with the IT department is that they don't always take the necessary precautions to secure a network. With a busy IT department, it's easy for an admin to rush through the setup of a server or access point for example and inadvertently forget to set the proper security settings. Sometimes an admin will set up equipment and not know what the settings should even be. These types of things should be handled by a third party vendor if the department isn't knowledgeable enough to handle the task. One wrong setting can open up the entire network to an attacker and can go unnoticed until it's too late.

The end-user – Users tend to be one of the largest flaws in security. This has a lot to do with the fact that users lack the knowledge they need to keep their technology secure. Users will open email viruses, download software, install rogue devices, and even give away their password if asked sometimes. Another problem with the end-user is that unfortunately, they really just don't care enough. End-users have a false sense of security. They feel as if they are able to do anything online because the IT department is working diligently to keep all the bad stuff out. Occasionally a company will have to deal with a disgruntled employee that wants to commit malicious activity or one that commits a crime by stealing and selling data. This person is called an insider threat.

The attacker – Unfortunately there are attackers that attempt to break into networks with the intent of doing malicious activities. The attacker tends to be very knowledgeable in the art of hacking because they work very hard to find ways in.

There are several different types of hackers. The three main types of hackers are White Hat, Gray Hat, and Black Hat. The following are descriptions given by Hoffman, C. of How-To Geek. (2016)

> **Black Hat** – "Black-hat hackers violate computer security for personal gain (such as stealing credit card numbers or harvesting personal data for sale to identity thieves) or for pure maliciousness (such as creating a botnet and using that botnet to perform DDOS attacks against websites they don't like.)" These are the ones that can be considered the bad guys and are the types of attacks that can bring down an entire network and cause a company to go bankrupt.
>
> **White Hat** – "White-hat hackers are the opposite of the black-hat hackers. They're the "ethical hackers," experts in compromising computer security systems who use their abilities for good, ethical, and legal purposes rather than bad, unethical, and criminal purposes." A white hat hacker can be helpful, but at the same time if they are able to get into the network and spread the word via media, even without causing physical harm can cause harm to a company by way of making the company look bad.
>
> **Gray Hat** – "A gray-hat hacker falls somewhere between a black hat and a white hat. A gray hat doesn't work for their own personal gain or to cause carnage, but they may technically commit crimes and do arguably unethical things." The gray hat hacker is

sometimes considered the curious hacker. They typically want to break into a network just to see if they are able to, and for fun. They don’t usually want to cause harm, but sometimes may inadvertently do so.

The other less common types of hackers are known as Red Hat, Blue Hat, and Green Hat hackers. Red Hat hackers attempt to attack governments. Blue Hat hackers are usually a vengeful attacker that usually attacks only to seek revenge on someone. A Green Hat hacker is considered a inexperienced hacker also known as a “Noob”. (Volimer, 2010)

Process and Policy Trends

As technology changes, so does the need for updated policies and procedures. The most recent additions to company IT policies are the mobile device policies such as BYOD, the wireless/acceptable use policy, and the cloud-based security policy. Here we will discuss these policies and outline a few items that these policies should include.

Mobile Device Policy – According to TechTarget, "a bring your own device (BYOD) policy is just the first step in defining safe and productive mobile device usage." (2016)

A mobile device policy is effective in many things most importantly educating the user. Enforcing the use of a mobile device policy forces the user to follow requirements in order to be authorized for the use of mobile devices. Even if the user sometimes doesn't follow this policy, reading it will sometimes give the user the tools that are needed to know the difference between what is right and what is wrong.

- BYOD/MDM Policy - Policy should include:
    a. Device security requirements
    b. Lost or stolen device procedure
    c. Signed agreement annually

Wireless/Acceptable Use Policy – According to GFI Software, an Acceptable Use Policy should define which systems the policy covers. This policy should explicitly prohibit illicit behavior, distribution, and communications. It should establish privacy guidelines, and it should provide a clear description of the risks associated when a user is noncompliant. (2011) The policy should also include the following:

- Wireless/Acceptable Use Policy – Policy should include:

a. Signed agreement annually

b. Users agree to monitoring

c. Users agree to use the network for work use only

Cloud-Based Services Policy – According to Hazdra (2013) "The better you define your cloud policy, the better everyone will understand how to leverage the cloud and reduce the risk to your organization."

Cloud-based services policies should align somewhat with the companies acceptable use policy.

- Cloud-Based Services Policy – Policy should include:
    a. Sensitive data usage
    b. Information sharing
    c. Signed agreement annually

Recommendations

In order to reduce future privacy and security risks, it's important to be vigilant when thinking about the security and privacy of a future network. To do this, an admin should try to think like an attacker. If an admin is able to think like an attacker, they will be more likely to be able to cut an attacker off at the pass, before they are able to do significant amounts of harm to a system.

Following are a few improvement methods that are recommended methods used to reduce future privacy and security risks.

1. Encrypt all sensitive data and hard drives – it's important to use encryption on all sensitive data and hard drives. If for some reason a network does get compromised, the encryption of data will at least prevent data leaks and protect important information such as social security numbers and credit card information.
2. Use access controls/Principal of least privilege. Giving users only the access they need will help to prevent risks that could happen by the internal user. This also reduces the amount of damage that a disgruntled employee is able to cause.
3. Use Antivirus – Antivirus doesn't work as well as it used to. Hackers have found ways around most antivirus software, but it occasionally catches items as long as the definitions are kept up to date. It can catch virus files in email, and it can catch virus programs that are downloaded and installed by users. Install and maintain network level antivirus on all devices.
    a. Logs should be monitored daily for viruses.
    b. Virus definitions should be updated weekly.

c. Virus scans should be performed weekly.

4. Educate the user should become more prevalent – It's time consuming to spend the time it takes educating users in the security of systems, mobile devices, wireless activity, and email, but this is where most privacy and security flaws happen. The uneducated user unknowingly invites the attacker in. User training should be conducted monthly as a requirement for continued wireless access.
    a. Training should be verified by the training department
    b. Training should include email security, wireless security, password security, and internet security
5. Segment the networks by area, so containment is easier and less time consuming. If one segment on a network gets attacked, the rest of the network can remain safe. It also makes it easier to find the problem and gives the admin time to repair the vulnerability before it creates issues for the other segments.
6. Create and use policies such as BYOD, Wireless, Cloud-based Security, and Password policies. These policies should be made available to users on the network, and should be updated regularly.
7. Complete Wireless audits either internally, or by a vendor. These audits should be completed on a quarterly basis to make sure nothing has changed to compromise the network since the last time the network was audited.
8. When considering cloud computing, make sure to look at all of the options and use a trustworthy source. Even with data stored in the cloud, it's important to make sure there are working backups to prevent data loss.

Conclusions

In conclusion, it’s nearly impossible to completely secure a device without turning it completely off and locking it in a box. All technology was new technology at one point and the technology that is new now won’t be. There is such a rapid progression in technology that it’s nearly impossible to keep up with the demands of security. Hackers have a way with learning the vulnerabilities faster than software companies these days and that doesn’t appear to be changing any time soon.

I don’t see the future of privacy and security getting any easier for the technology departments of a company any time soon. The best defense is to detect and respond to intrusions as they happen rather than to just put up a wall and block everything.

References

Ashford, W. (Oct. 2015). New tech and collaboration key to future security, says expert panel. *ComputerWeekly.* Retrieved from http://www.computerweekly.com/news/4500255962/New-tech-and-collaboration-key-to-future-security-says-expert-panel

Sans (Oct. 2015). The CIS Critical Security Controls for Effective Cyber Defense. *CIS Critical Security Controls.* Retrieved from https://www.sans.org/critical-security-controls/

Sanchez, G. (Jun. 2015). Case Study: Critical Controls that Sony Should Have Implemented. *Sans.org Reading Room.* Retrieved from https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-sony-implemented-36022

Rouse, M. (2016). Cloud Computing. *TechTarget, SearchCloud Computing.* Retrieved from http://searchcloudcomputing.techtarget.com/definition/cloud-computing

WiseGeek. (2016). What are the Different Types of Mobile Devices? *WiseGeek, Clear Answers for Common Questions.* Retrieved from http://www.wisegeek.org/what-are-the-different-types-of-mobile-devices.htm

Kumar, U., and Gamhir, S. (2014). A Literature Review of Security Threats to Wireless Networks. *International Journal of Future Generation Communication and Networking.* Vol.7, No.4 (2014), pp.25-34 http://dx.doi.org/10.14257/ijfgcn.2014.7.4.03

Sellers, M. (Mar. 2016). Managing Security Risks in Wireless Networks.

TechTarget. (2016). Mobile device policy guide: How BYOD policies help IT manage devices. *TechTarget Search Mobiile Computing.* Retrieved from http://searchmobilecomputing.techtarget.com/essentialguide/Mobile-device-policy-guide-How-BYOD-policies-help-IT-manage-devices

Hoffman, C. (Apr. 2013). Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats. *How-To Geek.* http://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/

Rashid, F. (Mar. 2016). The dirty dozen: 12 cloud security threats. *InfoWorld.* Retrieved from http://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html

GFI Software. (2011). The importance of an Acceptable Use Policy. *GFI Software.* Retrieved from http://www.gfi.com/whitepapers/acceptable_use_policy.pdf

Hazdra, S. (Aug. 2013). Creating your first cloud policy. *NetworkWorld.* Retrieved from http://www.networkworld.com/article/2169329/tech-primers/creating-your-first-cloud-policy.html

Volimer. (Jan. 2010). Types of Hackers. *Urban Dictionary.* Retrieved from http://www.urbandictionary.com/define.php?term=Types+of+Hackers