Global Knowledge®

Expert Reference Series of White Papers

Security Trends 2014

Security Trends 2014

James Michael Stewart, Global Knowledge Instructor, CISSP, CEHv3-8, CHFIv3-8, Security+

Introduction

Many security trends that occurred in 2013 are continuing into 2014, along with a few new trends that are beginning to emerge. Several security concerns examined in this paper have grown more significant over the last year, which demand your attention now more than ever because the risks are greater and the stakes are higher. It is our responsibility as IT administrators and users to keep watch for security trends and threats facing us in the coming year. New and unforeseen risks are sure to arise—likely from areas that we deemed safe as well as from areas we never considered.

Attacks against New and Legacy Platforms

Many new operating systems were released in 2012, such as Windows 8, Mac OS X Mountain Lion, Android 4, and iOS 6. Even with updates, service packs, and a few new major version releases, both PC and mobile devices in 2013 were under significant focus of attacks and exploits. In fact, Android seems to be the top target of malware on mobile devices, while Windows still remains the primary target on the traditional PC. There are exciting new versions of operating systems (OS) planned for 2014. Let's hope programmers have learned from the exploits revealed over the last few years to adjust their product's security infrastructure.

In addition to the unknown risks of new versions of an OS, we are also heading quickly into a new era in the computer age. As of April 8, 2014, support for Windows XP will formally be terminated. At least 30% of all Windows systems are still running Windows XP as of early 2014. Once support ends for Windows XP, there will be the largest number of systems running an unsupported legacy operating system. The end of support for Windows XP is not quite an end for everyone and everything thing. Businesses can pay for extended support for about $200 per seat per year. Also, Windows XP Embedded will continue until 2016.

Microsoft will continue to update Windows Defender, but will not provide XP updates, hot fixes, or service packs. Those who remain on Windows XP will face a serious threat—once hackers release new attacks for XP, the vulnerabilities they exploit will never be fixed. Expect an onslaught of security breaches occurring soon after April 8th.

More Targets More Places

In 2014, the Internet of Things is will continue to expand. This is the idea that devices not typically considered computers have been enhanced with embedded systems, which enables the devices to be connected to a network, interact with each other, potentially connect to the Internet, and be controlled over the Internet. Examples of these devices include smart home components, thermostats, burglar alarms, appliances, TVs, game consoles, IP cameras, vending machines, point of sale devices, GPS systems, and in-vehicle systems. If these devices are not designed and implemented with strict security controls, the number of potential targets that can be remotely controlled by hackers will increase.

Ransomware: CryptoLocker

Ransomware is malicious code that often encrypts drive contents of a victim's computer, and then extorts money for the release the hostage data. This type of malware obtained infamy in 2012. In 2013, CrytpoLocker took malware to a new level of success. CryptoLocker is not just another form of ransomware, it is one of the few malware products whose operation is nearly foolproof. This malicious software encrypts a wide range of files on a victim's machine, using the native crypto suites of the OS to "properly" use a combination of both symmetric and asymmetric cryptography. Once the encryption operation completed, the malware then demands payment within hours, otherwise the files will be inaccessible… forever. CryptoLocker requires payment via BitCoin of approximate value of $300 USD. BitCoin is a form of digital currency which allows for untraceable transactions. In just the last quarter of 2013, those behind CryptoLocker potentially stole over $40 million. CryptoLocker is likely to expand its victim list in 2014.

Imitation Is Not Flattery

With the perceived success of CryptoLocker, numerous copy-cat ransomware products have already appeared across the Internet. It is hard to imagine why anyone with a criminal leaning and the skill to write malware would choose any other option than that which provides them the greatest payout for the least work with the least chance of being apprehended. 2014 will likely be the year that ransomware is the dominant form of new malware release.

Blowback from Revealed Monitoring and Tracking

2013 brought revelations of the breadth and depth of the NSA's the monitoring and tracking tactics (as well as other branches of the US government), which has caused many of us to think twice about our electronic habits. Whether the courts find the actions of the NSA to be legal or otherwise, the innocence of the Internet is now long lost. In 2014 and beyond, we all need to be active both in our online actions as well as in speaking out. Whatever side of these issues you land, you need to communicate your thoughts to our elected leaders. If you do not wish to be monitored, you need to make the effort to choose those services which are designed to avoid or lessen tracking as well as employ encrypted communications whenever possible. However, assuming that you are not being watched because you have done nothing is an inaccurate assumption.

Mobile Attacks Galore

With the explosion in popularity of tablets and the ubiquitous smartphone, mobile attacks rose to a level rivaling that of PC attacks in 2013, and are likely to exceed PC attacks in 2014. Most mobile devices have only modest native security, and those security features are often disabled by default. The typical end user is often unaware of their devices' security features and is ignorant of the risks while using mobile devices. Often the cultivated app repositories, the in-your-pocket convenience, and the amazing capabilities of an always connected device at your fingertips overshadows the fact that these mini super-computers are just as vulnerable to attacks and malicious code as a desktop or server computer.

Every mobile device has already had malware developed for it. Mobile device malware can be found both in managed app stores as well as from third-party sources. Mobile devices often are used to store significant amounts of personal, private, confidential, and proprietary data for individuals as well as businesses. If these devices are lost, stolen, or just accessed remotely via malware, there is little protection for these valuable data sets.

The Bigger They Are

As we start 2014, the United States is almost the last remaining country whose banks are still using the old mechanisms of credit card transactions using the magnetic strip. The only other country using the magnetic strip is Turkey. Every other nation uses credit cards with a smart chip. Known as chip-and-PIN technology, this transaction mechanism requires the presence of the physical card in a smart card reader along with the PIN of the user/owner. Unfortunately, with US banks keeping its customers in the past, the world's criminals have focused their efforts on us. In late 2013, a security breach of POS (point of sale) devices at Target, Bloomingdales, and many other retailers has exposed over 130 million Americans to credit card fraud attacks. The ramifications of this exploit and the extent of those affected are still being discovered. It will be rough year in 2014 as the handing of credit card account takeover fraud is experienced by an ever increasing percentage of users. Some studies suggest that everyone (in the US) with a credit card has been put at risk due to the number of security breaches that have occurred in the last decade. As of 2014, some US banks now offer some of their credit card lines in a chip–and-PIN format. But it will still take several more years before all credit cards issued by all banks to adopt this much need security improvement.

BYOD may stand for Bring You Own Destruction

Bring Your Own Device (BYOD) is the popular concept that allows workers to bring their own mobile device to work and be able to use it (to some extent) on the company network. BYOD often generates increased job satisfaction for workers, but it is not often a satisfactory result for the business that deploy it. Dealing with the absurd variety of devices (each with their own flaws, configuration idiosyncrasies, and available security features), is a recipe for oversight, mistakes, and compromise. Additionally, determining who is responsible for the device, selecting which apps to install, which apps to disallow, and how to manage data are all complex issues. Many Mobile Device Management (MDM) products exist to ease the situation, but even then, allowing outside personally owned devices into a business network is not usually a wise security move. In 2014, the range of businesses supporting BYOD will increase. And due to this increase, a number of those businesses will be breached due to an attack or exploit making its way into their private network via a worker's mobile device.

Workers Shunning Private Tools

Internet sites and services are designed to be attractive and functional. They are often designed to be as simple to use as possible with the widest range of capabilities and features. Contrast that with the typical internal business application—especially those developed in-house or are older ones that were developed years (or decades) ago—since they still work, why change or replace them?. Internet savvy workers may choose to use Internet services in-spite of the company's own internal service. Even with company policies strictly prohibiting such practices. Don't underestimate the allure of a well-designed Internet service that solves a worker's problem, without the hassle of the company red tape. How often have you considered telling someone that rather than sending an attachment or link to your business email address, (which strips attachments, has a 2 MB limit, or blocks URLs or other encodings in messages) you have them send it to your Facebook account or your Gmail, Yahoo, or Live account where there are no such restrictions or limitations. In 2014, organizations need to be on the lookout for workers who shun internal solutions in favor of external ones. The risk of data leakage in such situations is not to be underestimated. Without oversight and training, works will often exchange convenience for security.

Cybersecurity: It is Not a Passing Fad

Trends and fads come and go all the time. Bell bottoms, disco, hosting your own DMZ, calling your private network an intranet, and not using encryption for communications. Cybersecurity seemed at first to be fad as well, at least as far as the term goes. Security has always been important, that's never going out of style. But distinguishing internal security from Internet security (or external security) seemed like a passing trend. However, in 2013 and now into 2014, trends show the concept solidifying and strengthening. Too many organizations were either not adopting sufficient security or were failing to address the risks of outsiders. The risk of the concept of Cybersecurity has garnered attention from C-level executives to the employee base. We are all realizing that security is not just the responsibility of IT department, but everyone in the organization has security responsibilities. And those responsibilities do not end when the shift whistle blows, or when we perform "personal" online activities, or whether we use company equipment or personally owned devices. If it takes a science-fiction sounding term to get everyone involved in security, then let's all start sounding nerds: CYBERSECURITY!

Trust No One

Trust No One (TNO) has been the battle cry of Steve Gibson (grc.com and the weekly show *Security Now!*). Trust No One implies that the only person you can fully trust is yourself. The more you trust in others, especially online, the more you become vulnerable to risk. This became clearly evident in 2013, and should remain front of mind throughout 2014. One of the principle tenants of TNO is to never let anything out of your control (i.e., surf the Internet without encrypting your computer first).. Assuming a service provider will protect your data is often misguided. Assuming your transmission will not be intercepted, eavesdropped, manipulated, hijacked, or man-in-the-middle attacked is only possible if you are completely ignorant of the state of the Internet. Every communication you initiate needs to be encrypted, whether TLS (formerly known as SSL), SSH, or other reliable VPN option. Even if you are using transmission encryption, it is also important to encrypt your own data before putting it online. Especially when using cloud storage and/or backup solutions.

More Specific Phishing and SPAM

We have all grown accustomed to the level of SPAM and other unwanted emails and messages we have to slog through on a daily basis. 2014 is poised for the growth of SPAM, phishing attacks, and other message-based social engineering exploits. The rate of new Internet users is increasing faster than ever before. The use of mobile devices to interact with the Internet is also increasing at a phenomenal rate. With such a target-rich environment, it will be hard for attackers to overlook the bounty of potential havoc they could wreak. With many large and popular retail outlets (such as Target) being compromised, hackers and SPAMers have access to the largest and most accurate user dataset that ever before. Once a hacker knows some information about a user, such as they are a customer of a specific organization, message crafted as if they originate from that company are even more likely to fool the victim.

Social Network Harvesting

Facebook, Twitter, Google+, and LinkedIn are all overwhelmingly popular social networking sites. However, they are not actually safe environments. Many assume that because they can communicate with friends, family, and co-workers, that they are in a private area. Usually that is not the case. Most communications on social networks are public. In fact, most of the content posted by a user is available for anyone to see, in spite of the pitiful privacy precautions a site might erect. Hackers often scour social networks when seeking information about an organization as well as individuals. The use of social networks as data-mining sources for benign and malicious purposes will continue throughout 2014. Think twice about what you post online. Never post anything that you don't want everyone, including your spouse, parents, children, law enforcement, or your boss to see—there is a good chance they could see it, eventually.

Insider Violations

In 2014, insider security violations are sure to be on the rise as well. Many of these will be unintended, as they will be the result of a worker attempting a personal online activity but inadvertently breaching company security. This will include a wide range of social engineering attacks that result in data leakage or remote access for the hacker. Unfortunately, there will likely be an increase of intentional malicious actions on the part of employees. There is a growing underground black market for the sale and distribution of product information and company secrets. Many workers are often attracted to the promise of a big payout just by selling company documents. There are also a growing number of workers who will be frustrated by company Internet policies and will intentionally violate those restrictions through installation of unauthorized hardware, using remote access tools, tethering of mobile access devices, and using encrypted covert channels. These means of accessing the Internet are not only a violation of company rules but expose the organization to malware infection and remote access attacks due to the unfiltered unauthorized communication pathway.

Insider threats are of such a serious nature due to the fact that someone on the inside already has physical access and likely a network user account. Outside hackers spend considerable time and effort to gain logical or physical access to a target. Your workers already have both. While a typical worker can choose to perform malicious actions or be tricked into them, it is also true that a hacker can go undercover and be hired by your organization. This would then allow them to attack from within. As corporations and nation states battle, this form of insider attack is sure to increase.

Compromises in the Cloud

Cloud compromises are another area of growing concern in 2014. It is important to realize that cloud computing and cloud services are mostly smoke and mirrors. Ultimately, a cloud service or product is software running on a computer situated somewhere that is accessed over a private link or public Internet. Most cloud providers actually host their services using virtualization products allowing them to scale quickly at a reduced cost. There is no reduction of risk when using a cloud solution. There is the promise of greater security, encrypted connections, encrypted storage, private transactions, and such. But due to the nature of remote connections, virtualization technology, operating systems, applications, encryption solutions, key storage and management, and the co-mingling of data on shared resources—there are ripe vulnerability fruit ready for picking. I prefer to use the phrase remote-virtualization rather than cloud computing, in order to maintain the distinctions.

Most cloud services and product providers are actively seeking to provide customers with security. However, it is my fear that, like many other online and local only products and services, something will be overlooked and hackers will find a way to exploit it. Providing large scale cloud products and services is a very complicated and often fragile endeavor. As cloud offerings become more widespread and popular, it will become a greater target for hackers.

Social Engineering

There will continue to be an increase in the level, complexity, and intensity of social engineering attacks in 2014. Social engineering targets the weak link of security—namely its employees. People are always the last line of defense as they can choose to violate security; or they can be either coerced or tricked into compromising security. Social engineering attacks have advanced considerably since the days of the travelling conman or the salesman huckster. Often professional social engineers are adopting psychological techniques, studying human behavior, and even performing pilot testing of their attacks as they prepare for a new assault against a specific target.

Social engineering is a type of attack that can be against any individual or everyone; it can be generic or very specifically targeted; it can focus on information-gathering or physical or logical access; it can be implemented over long or short periods of time; it can start from outside or inside; it can be performed in-person or through a communications network; and it has many other nuanced variations. There is no singular, all-encompassing definition for what social engineering is, does, or can do, other than describing it as an attack that takes advantage of human vulnerabilities.

As organizations and online services find ways of locking down their systems in order to defend against violations, the easy attacks against computers and physical locations are eliminated. However, it is quite difficult to sufficiently train all personnel to be defensive against social engineering attacks. Thus, these soft targets will always be a popular alternative.

Privacy Russian Roulette

As everyone (and everything) is online or will be so shortly; we will likely continue to experience a loss of privacy in 2014. We are using more things that share our lives with the rest of the world. Some of us do this on purpose; some of us don't realize that this is occurring. Sites and services seem to be changing their privacy policies, defaulting us into public rather than private settings, adding features that require sharing of data to be useful, and selling our gathered data to marketers. The reducing of our privacy, both online and offline, is likely to continue.

Approaching the End of Public Key Cryptography

2013 brought about the first clear indication that RSA's time is running out. RSA is the most widely used public key cryptography algorithm. This is quite impressive in that it was also the first of its kind, created back in 1977. The issue is that a group of hackers have been able to successfully discover the private keys of some organizations. However, this attack is a random attack at this point (i.e., the private key of a preselected specific target cannot be broken). The attack operates similar to that of password cracking attacks. A password crack requires that the attacker possess the target's password hash. Then the attacker uses a cracking tool to generate (or use from a list) a series of potential passwords. Each potential password is then hashed, and the resultant potential hash is compared to that of the target hash. If a match is found, then the target's password has been discovered, in other words cracked.

The RSA attack operates by the hackers gathering as many 1024 bit public keys as they can locate. Then they use a random number generator to create private keys. Each private key is then run through the RSA process to produce the corresponding public key. Each crafted public key is then compared to the collection of Internet sourced public keys. If there is a match between a generated and a harvested public key, then they know the private key used to produce the generated key, which in turn means they also know the private key of the organization that "owns" the harvested public key. In 2014, this attack is likely to gain the ability to target specific private keys rather than matching at random, as the issue is of computational capacity more than anything else. As hardware improves, attacks of this nature will improve as well. Public key based industries, such as certificate authorities, have already migrated upwards to using 2048 bit RSA public keys in response this random-target attack. Once this attack can be targeted, it will only be a matter of time before longer key lengths are affected as well.

Conclusion

As you can see, in 2014 we have a lot to lookout for, take precautions against, and be paranoid about. Don't forget that attacks don't get worse, they are always getting better. We still have some challenging times ahead. Information technology is still a very young concept and we humans have yet to fully understand and adjust to its existence. We have been too naive so far. Fortunately, security experts are working diligently to offer hope and protection. Stay alert. Be cautious. Avoid risk. Be skeptical.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

CISSP Prep Course

Certified Ethical Hacker v8

Cybersecurity Courses

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

James Michael Stewart has been working with computers and technology for over thirty years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job skill and certification courses, such as CISSP, ethical hacking/penetration testing, computer forensics, and Security+. He is the primary author of *CISSP Study Guide 6th Edition*, *CompTIA Security+ Review Guide: SY0-401* (to be released Q2 2014), *Security+ Review Guide 2nd Edition* (SY0-301), *CompTIA Security+ Training Kit (Exam SY0-301),* and *Network Security, Firewalls, and VPNs*. Michael has also contributed to many other security focused materials including exam preparation guides, practice exams, DVD video instruction, and courseware. In addition, Michael has co-authored numerous books on other security, certification, and administration topics. He has developed certification courseware and training materials as well as presented these materials in the classroom. Michael holds a variety of certifications, including: CISSP, CEH, CHFI, and Security+. Michael graduated in 1992 from the University of Texas at Austin with a bachelor's degree in Philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of-the-pants hands-on "street smarts" experience. You can reach Michael by email at michael@impactonline.com.