Global Knowledge®

Expert Reference Series of White Papers

10 Ways Everyone Should Approach Cybersecurity in 2015

10 Ways Everyone Should Approach Cybersecurity in 2015

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

Introduction

Many security breaches over the last year have taught us new lessons (or clarified ones we should have already learned). This paper reviews these key issues and focuses attention on 10 responses that we all need to adopt in our approach to security in 2015. The security breaches of 2014 were more numerous than in any previous year. They ranged from nuisance hacks to identity theft to the attempt to extort a major motion picture organization. Many of these attacks were preventable, mostly because prior security breaches have demonstrated flaws, misconfigurations, and design mistakes that many other organizations continue to have. Too many fail to learn from the mistakes and losses of others. If we hope to get ahead of the onslaught of hacks and attacks in the future, we have to learn from others. Here are 10 key lessons we need to learn (or learn again) from compromises.

1. Email Is Not Private

Email has always been a plain text communication medium. However, many have forgotten that or have become confused about its security over time. Those who use a web browser to access their email often see an https as the prefix of the URL, meaning their connection to their email is secure. But that SSL/TLS-encrypted connection only provided protection for accessing and reading your messages, not when sending or receiving them. Likewise, email client users may have configured SSL/TLS connections to their email server at their ISP or office. This type of connection provides security for the sending and receiving of messages, but only between the client and your local email server. Messages sent to other recipients across the Internet and received from others are often sent in plain text.

Email messages sent and received across a public Internet link are likely sent in their original plain text form. Several email service providers, such as Google, Microsoft, and Yahoo, have announced that they are in the process of setting up encrypted email transmissions for messages between their own members and others that join in their initiative. However, it may be years before a majority of messages are encrypted for transit. And I would not ever make the assumption that all messages will be encrypted for the foreseeable future.

There are two approaches I want you to consider when dealing with email. First, minimize the transmission of information across email that could cause you problems (or heartache) if it was intercepted in transit, whether by your employer, family, government, or hackers. Seek out a more secure form of information transference, such as encrypted file exchange, text chat, or video conferencing, for those items of importance of value. Second, start using an email encryption utility yourself. This is currently a mechanism available mostly to users of standalone email clients, such as Thunderbird and Outlook, but may be available to web-based email through the use of browser plug-ins. S/MIME is an email encryption and digital signature solution that you might already be using at work, as it is a standard and integrated well with smart cards, Common Access Card (CAC), and Personal Identity Verification (PIV) devices. Another encryption mechanism to consider is that of PGP (commercial), GPG (GNU licensed), or OpenPGP (Open source). The primary drawback to client-based email encryption solutions is that your recipient must have a corresponding solution installed in order to decrypt your messages or verify your digitally signed messages.

If you fail to encrypt your emails, there are others who are more than willing to read them without your knowledge or consent.

2. No Network Is Fully Secure

If you have attended any security training, I'm sure you were informed of the fact that security is never a completed project, it is always a journey whose destination changes often. There is no perfectly secure network and it is impossible to construct one. There are always means to breach security, whether through technical exploits, physical breaches, or social engineering. However, many organizations seem to act like their security is complete, that their network is unbreachable, and that their environment can be fully trusted. In 2014, hundreds of organizations realized that their networks were not perfect when hackers broke in to cause damage and steal confidential information.

All of us need to realize that the technology we use is rather young and it has not yet had the time to mature. We often strive to grab the latest and greatest gadget or upgrade to the newest release of a product. However, "new" means untested and thus its flaws and exploits are unknown. We are placing too much faith in the developers, manufactures, and programmers of our hardware and software. I'm not suggesting we run from technology and return to pen and paper, but I am suggesting that we take a more cautious approach to using technology to store and protect our most important information and assets.

We need to have more reliable backups as well as more backups. A backup is worthless if you cannot recover data from it. A single backup protects you only from data loss if the damaging event does not also destroy the backup. Everyone needs to follow the 3-2-1 rule of backups:

3) Always have three copies of your data—the original and two backups
2) Use two different types of media to store or host the backups (such as a hard drive and cloud storage)
1) Do not store both backups in the same physical/geographical location

We can also learn from this issue that no network is fully secure. We need to add additional layers of security to the existing infrastructure including storage encryption, using multi-factor authentication, tracking/auditing all access attempts, having stateful inspection firewalls, and monitoring it all with intrusion detection and prevention systems (IPDs).

3. Large Organizations Cannot Be Trusted

Just because a company has been successful and grown into a large corporation does not imply that it offers the best security to its customers. Often the priorities and obligations of a large organization are counter to the desires and interests of its individual customers. Never assume that you are a company's top concern. Think twice about putting your most important or personal information online. Whether a social network, a cloud storage solution, or an e-commerce site, you are putting yourself at risk when you post private, sensitive, or valuable information online.

Always set your account information to private when that option is made available. Provide only the minimum amount of information in the creation of an online account, especially for new services you might not continue to use. Consider having a separate email address for use with new sites so you don't expose your primary email address before you understand more about an online site or service. Have a credit card that is used only for online purchases and nothing else. Monitor this account for any questionable activity often, such as weekly or daily depending on your level of concern. Automation of your bill-pay, paycheck deposit, and retirement investing can be a huge time saver and assist in you actually saving money for retirement. However, you need to check on those systems regularly (e.g., monthly) to make sure the numbers are correct and the procedures are

working as you defined them. If you find a mistake or an error quickly, it can be corrected with little consequence. But failing to notice a problem could cause you to lose your retirement savings or screw up your credit with unpaid bills. You must be an advocate for yourself.

4. Information on Social Networks Is False

As humans, we trust that which is familiar—whether it's the last two miles on our drive home where we don't pay as much attention or a co-worker that we ask to watch over our belongings while we step away. Hackers and media outlets know this and work hard to become as familiar to you as possible. This is why you hear and see the same advertisements too often in so many different mediums (print, radio, TV, online, etc.) and companies establish trademarks for their products. This same concern applies to many other aspects of our lives, both in the real world and online.

We all trust our friends, that's why we call them friends and not enemies. However, when communicating with a friend through a social network, you are at risk of impersonation attacks. If an attacker can take over the account of a friend, then the communications from that account to you are no longer from your friend but from the attacker. Initially you won't know this and are likely to be tricked into believing something false or downloading and installing something malicious. Be slow to believe information seen online, especially through social networks, even when related to someone you know and trust. If something seems odd or out of character, then contact that person through some other means (*not* the same social network site), to inquire about the concern.

There is also a wide range of people who enjoy crafting false information for the purpose of misleading everyone. Sometimes they want to stir up a group, sometimes they want to get a strong reaction, sometimes they want to sell a product, and sometimes they want to use the farce as a distraction. Online information sources, even news agencies, need to be filtered through a lens of skepticism. Take the time to investigate a claim, report, posting, or headline. Find out the source, consider opposing viewpoints and perspectives, and don't believe it just because it was posted online.

5. Your Online Activities Are Being Tracked

Tracking is a fact of online activity. Most websites are free because advertisers pay them. This payment is not just for the privilege of showing you advertisements, but to track your activities and develop a dossier about your habits and interests. This type of tracking is big business and it is a huge part of your online activities. You may have become aware of several initiatives to reduce tracking, such as a Do Not Track flag set on your browser to inform websites of your wish to not have your activities monitored and sold off to third parties. There are other steps you can take to reduce the amount of tracking that targets you, these include:

- Use the incognito mode or private browsing mode of your web browser
- Disable third-party cookies
- Set your browser to delete all cookies at shutdown
- Use a browser plugin to control website content, such as NoScript for Firefox and ScriptSafe for Chrome
- Use a cookie tracker to become more aware of the amount of tracking taking place, such as Collusion for Chrome
- Use advertisement blockers and tracking blockers, such as AdBlock Plus, Do Not Track Plus, Ghostery, Disconnect, and Privacy Badger
- Install the HTTPS Everywhere plugin for Firefox and Chrome to force the request of encrypted web communications, as this will reduce the ease by which third parties can monitor and track your activities

These suggestions will greatly reduce the amount or level of tracking that targets you, however, they are insufficient to block all tracking. There are techniques, commonly labeled as super-cookies, which cannot be easily

blocked. These techniques take an inventory of your web browser and related or accessible sub-systems in order to create a unique fingerprint of your system. Since they don't deposit anything on your system, there is nothing to block. If your system remains configured relatively the same over time, then your unique fingerprint can be recognized each time you return to the site.

I think everyone should consider using some form of tracking blocking or filtering mechanism. But I do want to present an important alternative perspective regarding online tracking. If we as consumers of the Internet are able to successfully block all tracking (and subsequently all target advertisement), then many of the websites and online services that we currently use for free will have to start charging us for their use. It might be a worthwhile trade off to allow some level of anonymous bulk tracking for the purposes of targeting advertising so we can continue to use online content without having to pay more than our initial connection fee to our ISP.

6. Staying Anonymous Is a Challenge

News reports of hackers being apprehended often state that the offenders were using anonymization services, but they made some mistakes. Often those mistakes are failing to use their anonymization tool each and every time they connected to their attack target. When attackers forget to use their tools, they often leave behind a trail that can be followed by investigators—you need to be aware of as well.

I'm neither condoning attacking nor encouraging you to commit crimes or even act unethically, but there are valid reasons to be anonymous when using some Internet services. Whether needing to report a crime, seeking help due to an abusive relationship, or needing advice when involved in an embarrassing situation, there are some valid and ethical reasons for needing online anonymity. However, for the typical user, being anonymous is extremely difficult. This is mostly due to the fact that so many criminals use anonymization services to hide their identity while committing crimes, that law enforcement has spent considerable effort to breach the anonymity of those mechanisms.

However, if you find yourself in need of being anonymous (again, for a legitimate and ethical reason), here are some suggestions to keep you as anonymous as reasonably possible for the any non-criminal:

1. Don't use your personal system for any communications that you need to be anonymous. Don't use your smart phone, tablet, or the main OS on your primary computer.
2. Install a virtualization or hypervisor product, such as Virtual Box (which is a free product from Oracle), onto a computer. This can be your primary system or a second system you dedicate for this purpose.
3. Run a live or ISO version of Ubuntu in a virtual machine. Ubuntu is a simple-to-use version of Linux that any Windows user can operate. The live or ISO version of an OS will not save or retain any changes across reboots.
4. From Ubuntu, install and use the TOR anonymization service, see torproject.org for instructions
5. Use a different browser than the one included with the TOR tool. You will have to set the proxy setting for this alternate browser to use TOR, typically the address of 127.0.0.1 and port 9150.
6. Use the incognito or private browsing mode of the alternate browser.
7. While accessing the Internet, do not log onto any site for which you have an existing account.
8. If accounts are needed for certain services, do not use anything about yourself in the registration process. Set up a temporary email address (search on "temporary email") and do not use your real name, real email address, real phone number, or any other identifying factors when setting up an account.

These steps are not convenient, but they will provide you relatively reliable anonymity while using online services. Be careful. While it may be easy to be anonymous, it is difficult to stay anonymous. Most of the time, anonymous users give themselves away by being infected by tracking tools, failing to use their proxy properly, forgetting to

use the proxy, or accidentally outing themselves by providing personal information or logging into their normal online accounts.

7. Vendor Code May Have Backdoors

A backdoor is a means to gain access to a system that bypasses or avoids the frontdoor. The frontdoor is normal regular authentication using valid account credentials. Backdoors are mostly known as being planted by a hacker once they have compromised a system through some other means. However, we have learned that a number of widely used products and services happen to have backdoors in them that were planted by the vendors on purpose or by an unscrupulous member of their development team.

Early in 2014 it was discovered that Cisco, Linksys, and Netgear wireless access point devices (and possibly many others), which use components manufactured by Sercomm, could be accessed with full control just by connecting to port 32764. The firmware of these devices was later updated to require a knock packet before gaining access, but this only reduced the threat, it did not eliminate it.

A flaw in the widely available BASH shell on UNIX and Linux was discovered which allows a hacker to gain access to a command shell in order to run arbitrary commands on a system as the root. This issue was branded Shellshock and Bashdoor. The flaws have existed in the BASH code since September 1989. A patch is now available, but it will be years before a majority of deployed UNIX and Linux systems are properly updated to seal this hole.

Another example of vendor-supplied code having a backdoor was revealed in late 2013. D-Link wireless access points had a backdoor planted by programmers sometime during the firmware development. It granted an attacker the ability to access the management interface without providing authentication credentials just by setting the web browser's user agent to "xmlset_roodkcableoj28840ybtide". Updated firmware is now available, but it has not been universally installed.

The problem that vendor code may have backdoors is a difficult issue to address because these issues are often unknown issues until they are discovered and made public. I would recommend keeping a closer watch on security discussions and vulnerability postings. And be aware that the systems you trust and rely upon today, may be shown to be flawed and insecure tomorrow. Don't place all of your trust in a single vendor or a single security protection. Having a heterogeneous environment and security designed with defense-in-depth in mind are essential to being prepared for the unknown.

8. Segmentation/Compartmentalization of Networks Is Essential

It is simpler to set up a private network as one internal group. A single collective of clients and servers is much easier to manage and it also much more convenient for accessing resources. However, this openness, freedom, and convenience is also a vulnerability. We must take on the perspective that our company's security will fail at some point. When that happens, how easy have we made our environment for the discovery and access of our most valuable assets? Companies need to reconsider their network deployment. Segmentation or compartmentalization is key to limiting damage and access once malware has gained a foothold or when a remote access Trojan has allowed a remote hacker into your organization. Different departments, processing groups, or value/sensitivity leveled systems should be separated from one another in subnets with unique IP address assignments, enforced by firewalls, and monitored by IPDes.

9. Clarification of Incident Response

Many companies that experienced breaches in 2014 discovered that they were ill prepared to respond to the violations. This resulted in attacks lasting longer than necessary, allowing more systems to be compromised, making it more difficult to track down the perpetrators. This can be addressed by your organization by making the effort to clarify your incident response. You need to have a written policy, a trained team of responders, and perform regular drills and simulations. We must understand that we operate in a world where security breaches are inevitable. So, in addition to buttressing up our defenses to reduce the chance of compromise, we must also be prepared to deal with a compromise if and when it occurs. A well-managed incident response procedure is a good example of preparedness.

10. Respect the Reports and Alerts from Your Security Products

Many of the compromises we learned about in 2014 were detected long before the majority of the attacks or information leaks took place. The attacks were allowed to continue as the reports of these breaches were either overlooked or ignored. Details have surfaced that reveal the Sony attack of 2014 and the Target attack of 2013 were both detected months before the main offensive of the attacks took place. If the officers in those companies had respected the reports and alerts from their security products, a significant portion of the compromises they experiences could have been averted.

Yes, there are going to be false positives. But the proper way of addressing false positives is to respond to and investigate each and every alert. Then tune and adjust the detection system to avoid being triggered by the same false event. When millions of customers' personally identifiable information (PII) and financial information, the reputation of the company, and millions of dollars are at risk, it is essential to respect the reports and alerts from your security products.

Conclusion

There are solid lessons to be learned from every mistake, accident, compromise, and attack. It is smart to learn from the failings of others rather than making the same mistakes and experiencing the same loss. Whether in our personal lives and online activities or related to a global corporation, we need to grow up and become much more mature in regards to our security management. We have to make these changes ourselves. So, keep an eye out for new compromises on the horizon, but don't forget to learn from the security failures of both individuals and organizations.

Learn More

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

- Social Media Security Professional (SMSP) Prep Course
- Cybersecurity Foundations
- Fundamentals of Information Systems Security

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; 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.