Cybersecurity: What Have We Learned?

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
October 9, 2011

Introduction

During the years that have lapsed since the Estonia attacks in late April of 2007, cyber hackers around the globe have grown in both numbers and sophistication, using an array of techniques that have resulted in significant losses of financial resources, intellectual property, personal information, and vital intelligence to private sector and government organizations at all levels. However, with each attack, we learn more and more about ways to prevent them altogether, mitigate the damage, or shorten the recovery time when attacks succeed. A number of government, research, and cybersecurity agencies have studied some of the more costly attacks and have prepared and published lessons learned from each cyber incident. As part of our homage to the 8th annual National Cyber Security Awareness Month, NSCI recently reviewed many of these documents with an eye towards consolidation of lessons learned, best practices, and preventive measures into a single source document. We have organized these into four areas: people, policy, hardware/software, and data. Recognizing the perishable nature of such information, we hope to provide periodic updates to these lessons learned as technologies and threats continue to evolve – something they seem to be doing at a stunning pace. The most famous example of this is the Stuxnet worm.

In late April of 2007, the small country of Estonia experienced an initial barrage of Distributed Denial of Service (DDoS) attacks targeting government and financial industry networks that would bring the country's banking, telecommunications, and government to a state of virtual paralysis over the next few weeks. Because of the magnitude and sophistication of these attacks against one of the world's most "wired" nations, the events over the next few weeks constituted the first publicized, large-scale realization of a scenario that had been a concern of governments and IT professionals for a number of years.

Since it's been over four years since the Estonia attacks, it might be helpful to provide a brief refresher. Many of you may recall the lead-up: following some nine months of controversy, including protests from ethnic Russian citizens and strained diplomatic relations with Russia, the Estonian government took action to move a Soviet-era statue commemorating Red Army soldiers killed in WW II from the central square in the capital city of Tallinn to a nearby military cemetery. Cyber attacks commenced within hours after workers had disassembled the statue, with denial-of-service attacks against government systems and the defacing of a number of government websites. Over the next few weeks, this barrage continued, targeting government, banking, media, and telecommunications networks and employing a virtual army of zombies from all over the world to carry out the attacks. At the peak of this DDoS flooding, government websites that had been receiving 1,000 visits each day were suddenly inundated with 2,000 per second.

During the summer of 2009 and again in the spring of 2010, Stuxnet was used to attack equipment used in Iran's production of enriched uranium, setting back that country's nuclear weapons capabilities by what many experts believe will be at least five years. Stuxnet was unquestionably the most complex and "intelligent" piece of malware we've ever seen. If you've never read the details of this event, you owe it to yourself to do so. This is especially true if you have any professional responsibilities or personal dependence – which we all do – on SCADA systems. Stuxnet is probably the most researched malware in history, and there are a number of interesting stories on how it worked. One such discussion, "Is Stuxnet the 'best' malware ever?" is available at *ComputerWorld's* website.

People – The Weakest Link

Even with all its technical sophistication, Stuxnet could not have succeeded without some sort of human failure contributing. The insider threat, resulting from either complacency or a lack of understanding of the possible ramifications, is frequently cited in most after-action reporting of cyber attacks. In spite of this, companies are sometimes reluctant to expend the additional resources and accept the (at least temporary) loss of productivity that often accompanies employee training and education programs. However, even the most advanced technologies can be rendered useless without well-informed, attentive people serving as the first line of defense. Experts advise leaders and managers to *not* focus on the threat because it is always changing – the "finger in the dike" approach is simply not very effective. Instead, we're told to focus on our vulnerabilities. For most of us, the number one vulnerability is our people.

The most commonly used tactic in exploiting people vulnerabilities is spear phishing, used in the infamous hacks and data breaches of RSA and Epsilon, among others. In both of these cases, employees were victimized by spear phishing e-mails and either opened an infected attachment or followed a link to a website requiring them to reveal their user names and passwords. The fact that employees of RSA, an industry leader in network security, could be tricked by such a tactic is proof positive of the need for ensuring employees are well-trained and that cybersecurity education programs remain a top priority throughout government, industry, academia, and the public at large.

A similar case – the latest in the long-running controversy between Google and China – involved spear phishing against the Gmail accounts of American government officials and military personnel in China, resulting in the compromise of passwords. Although the amount of damage remains unknown, this case points to the importance of conducting official government business using only government accounts. We paraphrase suggestions from a poster on HP's Input/Output blog below:

- Don't use personal accounts for work-related correspondence
- If an email or a website attempts to take you to a login screen, alarms should sound
- Pay careful attention to displays on login screens. Spear phishers attempt to replicate authentic displays but frequently create pages containing subtle differences. Compare the details before adding information[1]

Any effective security policy has to begin with the organization's leadership. There is no other way to inculcate best practices without senior leaders leaving no doubt in the minds of worker bees that cybersecurity is a priority. The attack and slow response by Sony during the massive breach of its PlayStation Network in April seems to point to a lack of leadership at the company. According to Alan Paller, research director of the SANS Institute, the breach may be the largest theft of identity data information on record. There have been reports that names, addresses, and even credit card numbers of up to 77 million customers may have been compromised. Paller suggests that, "Sony probably did not pay enough attention to security when it was developing the software that runs its network. In the rush to get out innovative new products, security can sometimes take a back seat." [2] The company knew months in advance of the attack that their server was outdated and had no patches or firewalls installed, yet did nothing to remedy the situation. Then, after the first series of attacks, Sony failed to properly respond with password resets, bringing on even more breaches. This represents a significant lapse in leadership.

As stated by Erick Chickowski on the Dark Reading website, "A corporate culture devoid of security emphasis can cost a company a fortune in this day and age. According to reports..., Sony has spent $171 million so far on customer remediation, legal costs, and technical improvements in the wake of the breach

[1] "Lessons Learned from the Government Gmail Hack," by slfisher, 8 Jun 2011, available at http://h30565.www3.hp.com/t5/Policy-Watch/Lessons-Learned-from-the-Government-Gmail-Hack/ba-p/101

[2] "Sony PlayStation suffers massive data breach," by Liana B. Baker and Jim Finkle, Reuters, 26 Apr 11, available at http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426

– and that cost is only rising. Recovery from such a massive breach can be not only expensive, but also embarrassing and damaging to the brand."[3]

Policy & Process

> *" A policy is a temporary creed liable to be changed, but while it holds good it has got to be pursued with apostolic zeal." Mohandas Gandhi*

Among the many organizations that have studied the Stuxnet attacks was a team of security researchers from Tofino Security, Abterra Technologies and ScadaHacker.   This team actually created a simulated nuclear plant network and configured it with all the best IT security available during the time frame of the Stuxnet attacks. Working from this model, they analyzed the sequence of events of the actual attacks, down to the most minute detail, to determine whether this best-available-security model would have prevented the infections. Their ultimate conclusion: Stuxnet was simply too tough an opponent. Their report, "How Stuxnet Spreads – A Study of Infection Paths in Best Practice Systems," goes on to provide some excellent policy guidance: don’t focus on the threats; focus on your company’s vulnerabilities. All other security initiatives should support that overarching strategy.

In July 2011, Pacific Northwest National Laboratory detected a cyber attack against its technical infrastructure and quickly took action to secure its network and minimize the damage. CIO Jerry Johnson has since been very forthcoming about this "zero-day" attack, sharing lessons learned at the Information Week 500 Conference in a session entitled, "Anatomy of a Zero-Day Attack." We provide those seven lessons, reprinted from *Information Week*, below:[4]

> **"1. There's danger in multi-level security environments.** The lab had a well-protected IT security perimeter, but the attacks made it through anyway. An advocate of "defense in depth," Johnson is putting increased emphasis on protecting the data itself.
>
> **"2. Purge legacy, minority technologies.** The Web server in the first attack was based on a little-used technology at the lab, Adobe ColdFusion. Such out-of-sight, out-of-mind technologies are inherently vulnerable because they don't get the same degree of attention as an organization's primary platforms.
>
> **"3. Monitor cybersecurity events 24 x 7.** Advanced persistent threats like those that hit PNNL are just that--persistent--and require constant vigilance. Across federal government, agencies are investing in "continuous monitoring," with a goal of obtaining a near real-time view into the status of computer system security.
>
> **"4. Maintain a core forensics capability.** If your network does get hacked, security teams must be able to reconstruct events and assess the damages. What you learn can help prevent a relapse.
>
> **"5. Include a senior project manager on your response team.** Responding to a breach requires not only attention to detail and carefully coordination, but an ability to engage top management at a moment's notice and, if necessary, escalate decision making.

[3] "Five Infamous Database Breaches So Far In 2011," by Ericka Chickowski, Dark Reading, 27 May 11, available at http://www.darkreading.com/database-security/167901020/security/attacks-breaches/229700130/five-infamous-database-breaches-so-far-in-2011.html

[4] "7 Lessons: Surviving a Zero-Day Attack," by John Foley, *Information Week*, 19 Sep 11, available at http://www.informationweek.com/news/security/attacks/231601692

> **"6. Be prepared to call for help, and don't wait.** You may need to bring in security experts, business partners, law enforcement, or other outsiders. At PNNL, Johnson alerted the public affairs office, in order to prepare for the inevitable media inquiries.
>
> **"7. Have an emergency communications continuity plan.** When PNNL pulled the plug on its network, the hackers lost their ability to inflict further damage. Unfortunately, the decision also meant that lab employees lost network services, including email and voice mail. Be prepared for that eventuality by sharing cell phone numbers and alternative email address in advance."

Another spear phishing attack occurring earlier this year involved the e-mail marketing firm Epsilon. Companies such as JP Morgan Chase, Best Buy, Capital One, Kroger, Hilton, Marriott, Home Shopping Network, and TiVo – all of whom employ Epsilon to provide email marketing to customers on their behalf – learned of a large data breach that compromised names and email addresses of those customers. The attack, which took place on March 30th, targeted Epsilon, but the issue was clouded by the fact that the compromised personal information belonged to customers not of Epsilon, but of Epsilon's client companies. Epsilon represents 2,500 such companies and distributed for those companies some 40 billion marketing emails last year. Although there are also data segregation lessons to be learned from this incident, the policy takeaway is that you're not off the hook just because a business partner – and not you – loses your customers' data. Choose your partners wisely and consider the risks when entering into contractual relationships with other companies.

Does your organization have a sound policy for passwords? Have you assigned passwords for your programs, or are you still using the "default" passwords installed by the manufacturer? Do all your employees have unique IDs and passwords? Are the passwords regularly changed? In March, the Briar Group, which operates a number of restaurants in Massachusetts, agreed to pay $110,000 in damages stemming from its 2009 loss of customer credit card data. After investigating the case, the Massachusetts Attorney General cited all the above as failures by Briar. According to a report by the *Boston Globe,* Briar "...failed to change default usernames and passwords on its point-of-sale computer system; allowed multiple employees to share common usernames and passwords; failed to properly secure its remote access utilities and wireless network; and continued to accept credit and debit cards from consumers after Briar knew of the data breach."[5]

What about your corporate policy regarding the selection of passwords. The main impediment standing between a hacker and our data are the passwords we choose. Unfortunately, most of us take the easy route: passwords that are short, easy to remember, easy to type, and multi-purpose. Hackers use software designed exclusively to crack passwords – software with code written to exploit these vulnerabilities. The speed with which a password can be cracked depends on the speed of the hacker's computer and internet connection, along with the length and complexity of the password. Additional characters in a password result in an exponential increase in the amount of time required to crack it. For example, the sequential increase from six characters, to seven, eight, or nine results in an increase from five minutes, to two hours, to two days, to two months. Further, by mixing special characters, numbers, upper-, and lower-case letters, the hacker's problem gets very tricky. According to blogger and *Geek Beat* host John Pozadzides, "Adding just one capital letter and one asterisk would change the processing time for an [all lower-case] 8-character password from 2.4 days to 2.1 centuries." [6] That's even longer than it takes to get season tickets at Fenway Park.

[5] "Privacy breach case is settled," by Jenn Abelson, Boston Globe, 29 March 2011, available at http://articles.boston.com/2011-03-29/business/29360782_1_data-breach-customer-data-credit-and-debit

[6] " How I'd Hack Your Weak Passwords," by John Pozadzides, in *One Man's Blog*, 26 March 2007, available at http://onemansblog.com/2007/03/26/how-id-hack-your-weak-passwords/

However, the above discussion might be a bit too simplistic, as password hackers have given much thought to the subject, and their software programs are written accordingly. For example, they know from experience that many people use exclamation marks at the end of their passwords, often capitalize only the first letter, and frequently enclose their passwords with a pair of asterisks. Also, they know all about the preference of many to use "@" for "a" and "1" for "L" in spelling passwords. Rather than provide detailed lessons learned about password selection here, we strongly recommend the following articles to reinforce our point. First, Errata Security CEO Robert Graham, who has much experience in penetration testing, authored an excellent piece for *Dark Reading* in January 2009.

There is also the article by the above-mentioned John Pozadzides, "How I'd Hack Your Weak Passwords." It contains some interesting tips and includes a time-to-crack table, based on using all lower case vs. a mixture of characters. Very interesting.

If you aren't yet convinced of the importance of a sound password policy, consider this: Pozadzides believes that 95% of all security breaches begin with a password compromise.[7] Longer, more complex passwords are infinitely more secure than their easy-to-remember, easy-to-type kin.

A case involving the Texas state comptroller points to the importance not only of sound, well-understood policy, but also of systems and processes in place to ensure policy is complied with. State comptroller employees – in violation of departmental procedures – posted sensitive information on state employees and retirees on a public website between January and May of 2010. However, this activity went undetected for nearly a year before the breach was discovered. The result was the possible theft of personal information – SSNs, addresses, drivers' license numbers, and dates of birth, among others – from nearly 3.5 million people. The state now faces the prospect of a class-action lawsuit that is likely to cost $1,000 per citizen affected. For the math-challenged, that works out to $3.5 billion – a significant amount of money by anyone's standards. The lesson here is that policy and procedures are meaningless unless there is an accompanying process to provide enforcement. [8]

Security assessments, testing, external audits, and periodic self-inspections can also play a key role in helping to avoid incidents such as the one in Texas. These have the potential to identify potential vulnerabilities and thus decrease the probability of a successful attack. For those organizations that collect credit card information, a self-assessment or an independent assessment conducted by a qualified specialist can help to ensure compliance with Payment Card Industry Data Security Standards (PCI DSS).

Do you have a process in place to recognize that a cyber attack is taking place and to answer the "what hit me?" question afterwards? In January 2011, the Fox Business Network published some tips from Monte Robertson, CEO of Software Security Solutions, on how to differentiate between the various types of attacks:

> *Attacks from Scareware are easily discovered because the attackers say if you give them money, the "infection" that THEY put on your computer will be removed*
>
> *Attacks from BOTS can mean the compromised machines are sending out spam e-mail or you see a jump in network traffic coming from those infected machines-monitor for those signs.*

[7] " How I'd Hack Your Weak Passwords," by John Pozadzides, in *One Man's Blog*, 26 March 2007, available at http://onemansblog.com/2007/03/26/how-id-hack-your-weak-passwords/

[8] "Five Infamous Database Breaches So Far In 2011," by Ericka Chickowski, Dark Reading, 27 May 11, available at http://www.darkreading.com/database-security/167901020/security/attacks-breaches/229700130/five-infamous-database-breaches-so-far-in-2011.html

> *Attacks from viruses have taken a back seat and are not as common as they used to be. Viruses are written differently and their results vary. Watch for e-mail and file propagation levels to jump throughout the network and the slowing down of computing resources, which can be you've been infected.*
>
> *Attacks from Trojans are very common these days. They are usually delivered from surfing on the web or via BOT. They are stealthy and do not want to be discovered. Watch for critical data leaking out of the network.*
>
> *Attacks from Password Crackers, Keyloggers and Malware are also difficult to detect and are delivered from surfing the web and BOT infection. Watch for unknown programs being installed on computers (Antivirus alone will not usually help here).*
>
> *Attacks on databases are designed initially to be stealthy and take place over time. This threat surface area is now getting the attention it needs. Watch database logs for who is accessing what data, who is querying what data, what data is moving where in the database. Watch the logs. Watch for and do everything you can to prevent SQL Injection attacks.*
>
> *Attacks from the Internet happen all day and night, every day of the year. Watch the firewall logs to make sure you know what kind of attacks are happening and when. This monitoring and reporting should be done in real time.*

Robertson also added, “Keeping up with network security requires regular maintenance, just like anything else you use on a daily basis.”[9]

Technology

Using Your Wares (hard- and soft-)

While it's critical to exert strong leadership, train and educate employees, and implement sound cybersecurity policy, it's equally important to smartly employ technical solutions in securing your networks. The following is a list of hardware and software lessons learned from various sources, in no particular order.

In an article from 2008, the *High Tech Backup* (HTB) website provided tips on protecting your systems from viruses, worms, and Trojan Horses. Step one is to ensure an up-to-date operating system, essential for Windows machines. Next, anti-virus software is a must, including frequent updates providing fixes for all the latest fads in viruses, worms, and Trojan horses. You'll also need to make sure your anti-virus program has the capability to scan e-mail and files as they are downloaded from the Internet. There's also a need to run full disk scans periodically. This will help prevent malicious programs from ever reaching your computer.

You should also have firewalls installed. Capable of preventing unauthorized access to computers, firewalls can be either hardware or software. "Hardware firewalls provide good protection from most forms of attack coming from the outside world and can be purchased as a stand-alone product or in broadband routers. However, for viruses, worms and Trojans, a hardware firewall may be less effective than a software firewall, as it sometimes ignores embedded worms in outgoing e-mails and sees them as regular network traffic."[10]

[9] Types of Cyber Attacks and How to Recognize Them, by Cindy Vanegas, 26 Jan 2011, available at http://smallbusiness.foxbusiness.com/technology-web/2011/01/26/types-cyber-attacks-recognize/

[10] "Combating Viruses, Worms and Trojan Horses," 30 Jan 2008, available at http://kb.htbackup.com/kb/article-436.html

For individual home users, the best firewall choice is a software firewall. A good software firewall will protect your computer from outside attempts to control or gain access your computer, and usually provides additional protection against the most common Trojan programs or e-mail worms. The downside to software firewalls is that they will only protect the computer they are installed on, not a network.

As the HTB knowledgebase further stated, "It is important to remember that on its own a firewall is not going to rid you of your computer virus problems, but when used in conjunction with regular operating system updates and a good anti-virus scanning software, it will add some extra security and protection for your computer or network." [11]

Fundamental to mitigating the risks of a cyber attack is an understanding – in advance – of the operational impact when such an attack occurs. Step one is a simple knowledge of your internet service provider, your networks, and their associated "wiring diagrams." Following the July 2009 DDoS attacks on the U.S. and South Korea, Alan Paller, director of research at the SANS Institute, a security research organization, explained it this way: "Too many federal agency security people did not know which network service provider connected their Web sites to the Internet." This lack of knowledge of a simple item prevented these agencies from contacting their providers to have them filter out the bad traffic and thus reduce the load on their servers.[12]

No discussion of technology lessons learned would be complete without those gleaned from the Stuxnet attacks. Writing on the *Dark Reading* website, Michael Davis provided the following excerpts from a detailed report, " *Stuxnet Reality Check: Are You Prepared For A Similar Attack."* We quote here from his column:

> *"USB drives are the first lesson. Removable drive infections are common. Malware is placed on a USB drive or an external hard drive and moved from PC to PC. What makes the Stuxnet version of this kind of attack much deadlier is the use of the zero-day shortcut vulnerability, which does not require any user interaction beyond inserting the drive into the computer.*
>
> *"The best defense is removable storage device security software, available from numerous security vendors, that prevents unknown or unauthorized USB drives, CDs/DVDs, external drives, digital music players and so on from being mounted and loaded by a computer. These tools should be reinforced with policies that specify which, if any, removable storage devices can be used on a particular computer and by whom.*
>
> *"Lesson No. 2 is propagation. Stuxnet relied on network exploits and buried itself into WinCC project files to ensure it would be executed at designated times. This type of propagation requires peer-to-peer communication between workstations.*
>
> *"You can prevent this type of propagation by using host firewalls to filter out potentially dangerous traffic, such as services that let one PC communicate directly with another. Stuxnet used an exploit to send a crafted RPC message from workstation A to workstation B and caused it to execute code that downloaded the malware. If workstation B had had a firewall enabled that prevented inbound connections, the exploit would have failed.*
>
> *"Lesson No. 3 is authentication. Stuxnet provided a Windows rootkit that did something the security industry hadn't seen before. It used a legitimate certificate from a legitimate company that makes Windows drivers to mask its identity.*

[11] "Combating Viruses, Worms and Trojan Horses," 30 Jan 2008, available at http://kb.htbackup.com/kb/article-436.html
[12] "U.S.-South Korea Cyberattack: Lessons Learned," by JR Raphael, PC World, 9 Jul 2009, available at http://www.pcworld.com/article/168160/ussouth_korea_cyberattack_lessons_learned.html

> *"Hiding in plain sight, Stuxnet didn't have to worry about bloating its code with all the complicated obfuscation techniques that other malware has to use. If you were an administrator, would you question a file in the Windows\System32 folder named MrxNet.sys, written by RealTek and verified with a legitimate certificate?*
>
> *"What you can do today is use file hash and change management tools from companies such as Tripwire to detect these "hide-in-plain-sight" type of techniques? A change management tool monitoring critical Windows driver folders issues an alert when a new driver is installed. If this install was not on your schedule, it might be someone operating without following change management procedures, or it might be something nasty, like Stuxnet."*[13]

In our "Policy & Process section," we mentioned a Stuxnet study jointly conducted by Tofino Security, Abterra Technologies and ScadaHacker. From this study was a white paper entitled "How Stuxnet Spreads – A Study of Infection Paths in Best Practice Systems." This paper had a number of recommendations:

- Consider all possible infection pathways and have strategies for mitigating those pathways, rather than focusing on a single pathway such as USB keys
- Recognize that no protective security posture is perfect, and take steps to aggressively segment control networks to limit the consequences of compromise,
- Install ICS-appropriate intrusion detection technologies to detect attacks and raise an alarm when equipment is compromised or at risk of compromise,
- Deploy, operate and maintain at maximum effectiveness ICS-appropriate security
- technologies and practices, including firewalls, antivirus technology, patching systems and whitelisting designed for SCADA/ICS, to make attacks by sophisticated malware much more difficult,
- Look beyond traditional network layer firewalls, towards firewalls that are capable of deep packet inspection of key SCADA and ICS protocols,
- Focus on securing last-line-of-defense critical systems, particularly safety integrated systems (SIS),
- Include security assessments and testing as part of the system development and periodic maintenance processes. Identify and correct potential vulnerabilities, thereby decreasing the likelihood of a successful attack, and
- Work to improve the culture of industrial security amongst management and technical teams[14]

In another of the many post-mortems on Stuxnet, Francis deSouza, senior vice-president of the Enterprise Security Group at Symantec, has this advice for those involved in protecting SCADA systems:

- Take advantage of managed security services
- Implement and enforce device control policies
- Install, and if necessary lobby for the ability to install, host-based intrusion prevention systems
- Ensure your tempo of software certificate revocation updating is appropriate
- Use endpoint management software to ensure adequate patching procedures
- Capitalise on effective data loss prevention solutions

[13] "Stuxnet: How It Happened And How Your Enterprise Can Avoid Similar Attacks," by Michael Davis, Dark Reading, 17 May 2011, available at http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/229500805/stuxnet-how-it-happened-and-how-your-enterprise-can-avoid-similar-attacks.html

[14] "How Stuxnet Spreads – A Study of Infection Paths in Best Practice Systems," white paper by Eric Byres, Tofino Security; Andrew Ginter, Abterra Technologies; and Joel Langill, SCADAhacker.com, published 22 Feb 2011

- Where able, employ automated compliance monitoring to root out default password use[15]

As the Briar Group incident revealed, your customers are at risk if your business is using outdated technology in its point-of-sale (POS) terminals. Hardware and firmware should be routinely updated to comply with new data security standards and PCI DSS requirements.

Data

Separating the True Artist from the Mere Dilettante

As previously mentioned, an important lesson to be learned from the Epsilon data breach is the segregation of data as a damage control technique. Tim 'TK' Keanini, CTO of nCircle, agrees, saying, "It's hard to say exactly what Epsilon did wrong, but from the magnitude of the data that was taken, it would appear that they could have segmented the data such that if there was loss, it would only be partial. It appears that everything was centralized and when the attackers got at the data, they got it all."[16]

Further, this lesson will become especially critical as organizations transition responsibility for processing and data storage to third-party cloud providers. It will be important to maintain sensitive data in separate silos so that a breach of one customer database is not a breach of all.[17]

A case involving HBGary Federal, a security firm providing support to the U.S. government, serves to demonstrate that no organization is immune to attack. HBGary Federal was in the process of gathering information on the Anonymous hacking community for the purpose of selling it to the FBI. In the meantime, Anonymous hacked into HBGary's database, stealing credentials that would provide them access to company executives' email and social media accounts. The lesson learned here is that SQL injection hacks remain a prime method of database compromises. Also, in spite of HBGary's mission, they were still using an outdated MD5 and hadn't upgraded to the Secure Hashing Algorithm (SHA) family, generally regarded as stronger hashing tools.

Ericka Chickowski, writing in Dark Reading, recently published the "Five Worst Practices in Database Encryption," a list of mistakes commonly cited by security experts. We quote Ericka, verbatim, below:

> ***1. Storing Keys In The Wrong Place***
>
> *According to some security experts, one of the worst sins of database encryption is to comingle your encryption keys with the data they're used to encrypt.*
>
> *"If you're encrypting sensitive data in your database, then one of the worst practices is to store either the key used to encrypt the data or the authentication credentials that are used to get that key in the same database as the encrypted data," says Luther Martin, chief security architect for Voltage Security. "Doing that gives you the illusion of security, but actually provides very little real security."*
>
> *To really protect your data, keep the management of encryption keys separate from the database that stores the data encrypted with those keys.*

[15] "Preparing your organization for Stuxnet-like attack," Homeland Security Newswire, 2 May 2011, available at http://www.homelandsecuritynewswire.com/preparing-your-organization-stuxnet-attack

[16] "Lessons Learned from the Epsilon Data Breach," by Tony Bradley, *PC World,* 7 April 11, available at http://www.pcworld.com/businesscenter/article/224615/lessons_learned_from_the_epsilon_data_breach.html

[17] Ibid

2. Failing To Centralize Key Management

Many times keys end up in the wrong place -- and poorly secured, at that -- because the organization is simply too overwhelmed to keep track of them.

"One of the main issues is the sheer number of encryption keys and digital certificates in use within organizations," says Jeff Hudson, CEO of Venafi. "Research shows that it is not uncommon for an organization to be managing certificates and keys in the thousands, if not tens of thousands."

Many organizations are sold encryption, but not the means or knowledge to manage it, Hudson says.

"Encryption is only half the solution. IT departments must track where the keys are and monitor and manage who has access to them. Organizations need to quickly come to terms with how crucial encryption keys are to safeguarding the entire enterprise," he says. "This heightens the need for both a deepened understanding of encryption best practices, as well as automated key and certificate management with access controls, separation of duties, and improved polices."

Ideally, organizations should endeavor to centralize key management as much as possible in order to know what the organization has in its inventory, where keys are located, and how they're protected.

3. Depending On Home-Brew Solutions

Most IT people are tinkerers, and there's nothing so thrilling for a technology geek than to save his shop some dough by building a homegrown system in-house. But unless your staff consists of cryptographic experts with years of experience, building home-brew encryption or key management systems is just setting your organization up for disaster.

"Failed homegrown database encryption key management deployments are forcing even the largest of retailers to turn to specialized vendors," says Ulf Mattsson, CTO of Protegrity. "What is dangerous is it looks so easy at a distance."

4. Leaving Backups Unencrypted

If you encrypt your databases but leave backups of that data unencrypted, then you're setting your organization up for a fall.

"In this day and age, with all the stories of tapes falling off the back of trucks and laptops being lost, there is no excuse," says Nishant Kaushik, chief architect at Identropy.

Alan Wlasuk, CEO of 403 Web Security, agrees, stating that encryption of back-ups should become a matter of course for all databases.

"Back up all databases in an encrypted format 00 even if they have no value," he says. "Database backup will end up in places you would never imagine; it is easier to sleep if you know they are safe from prying eyes."

5. Using Out-of-Date Cryptographic Algorithms

Part of the reason why Gawker was so embarrassingly breached last December was because the password information exposed was "protected" by encryption using decades-old encryption technology. This is hardly a unique practice. Many organizations encrypt their data, but depend on old cryptographic algorithms that are about as secure as a paper mache suit of armor.

> *"Some older systems continue to use algorithms that have been broken years ago," Wlasuk says. Organizations have to be mindful not only that they encrypt their databases, but that they encrypt with technology that leverages new algorithms.*[18]

Conclusion

What did we learn today, class?

The above lessons learned may not be news to many of you. We offer them here merely as a refresher and a one-stop-shopping source. And although we acknowledge that we'll never achieve perfection, there is still much work to be done. We hope the above collection of lessons learned will help to increase the awareness of cybersecurity lessons as a result of previous incidents. There are plenty of cybersecurity holes and mistakes yet to be discovered; if you are looking to make the headlines, you have ample opportunity without "reinventing the wheel."

US CERT periodically publishes Technical Security Alerts to advise managers and system administrators on items of interest and other considerations to enhance cyber security. One such recent alert from July contains recommended measures across all of the categories discussed in this paper. We have included the alert at Appendix 1.

We close with a few words from the white paper jointly authored by Tofino, Abterra, and SCADAhacker. Although they specifically address the cyber threat to SCADA systems, they serve as excellent advice for all of us who are interested in protecting our networks and computers:

> *"First, the industry needs to accept that the complete prevention of control system infection is probably impossible. Determined worm developers have so many pathways available to them that some assets will be compromised over the life of a system.*
>
> *"Instead of complete prevention, the industry must create a security architecture that can respond to the full life cycle of a cyber breach. One area that needs attention is in the early identification of potential attacks. Currently, there are limited products available... However, many benefits can be realized from network behavior analysis and existing intrusion detection technologies that use normal traffic patterns to capture anomalies indicating potential threats...*
>
> *"Next, the industry needs to focus on containment of attacks when prevention fails...*
>
> *"These changes to improve defense-in-depth postures...are needed urgently. Waiting for the next worm may be too late."*[19]

[18] "Five Worst Practices in Database Encryption," by Ericka Chickowski, Dark Reading, 5 Oct 2011, available at http://www.darkreading.com/database-security/167901020/security/news/231900083/five-worst-practices-in-database-encryption.html?pgno=2

[19] "How Stuxnet Spreads – A Study of Infection Paths in Best Practice Systems," white paper by Eric Byres, Tofino Security; Andrew Ginter, Abterra Technologies; and Joel Langill, SCADAhacker.com, published 22 Feb 2011

Cybersecurity: What Have We Learned?

Appendix 1: US CERT Recommendations

Jim Ed Crouch, NSCI
Larry K. McKee, Jr., NSCI
October 9, 2011

National Cyber Alert System
Technical Cyber Security Alert TA11-200A

1.1 Security Recommendations to Prevent Cyber Intrusions

Original release date: July 19, 2011
Last revised: July 21, 2011
Source: US-CERT

1.2 Overview

US-CERT is providing this Technical Security Alert in response to recent, well-publicized intrusions into several government and private sector computer networks. Network administrators and technical managers should not only follow the recommended security controls information systems outlined in NIST 800-53 but also consider the following measures. These measures include both tactical and strategic mitigations and are intended to enhance existing security programs.

Recommendations

- Deploy a Host Intrusion Detection System (HIDS) to help block and identify common attacks.
- Use an application proxy in front of web servers to filter out malicious requests.
- Ensure that the "allow URL_fopen" is disabled on the web server to help limit PHP vulnerabilities from remote file inclusion attacks.
- Limit the use of dynamic SQL code by using prepared statements, queries with parameters, or stored procedures whenever possible. Information on SQL injections is available at http://www.us-cert.gov/reading_room/sql200901.pdf.
- Follow the best practices for secure coding and input validation; use the secure coding guidelines available at: https://www.owasp.org/index.php/Top_10_2010and https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/coding/305-BSI.html.
- Review US-CERT documentation regarding distributed denial-of-service attacks: http://www.us-cert.gov/cas/tips/ST04-015.htmland http://www.us-cert.gov/reading_room/DNS-recursion033006.pdf.
- Disable active scripting support in email attachments unless required to perform daily duties.
- Consider adding the following measures to your password and account protection plan.
    - Use a two factor authentication method for accessing privileged root level accounts.
    - Use minimum password length of 15 characters for administrator accounts.
    - Require the use of alphanumeric passwords and symbols.
    - Enable password history limits to prevent the reuse of previous passwords.
    - Prevent the use of personal information as password such as phone numbers and dates of birth.
    - Deploy NTLMv2 as the minimum authentication method and disable the use of LAN Managed passwords.
    - Use minimum password length of 8 characters for standard users.
    - Disable local machine credential caching if not required through the use of Group Policy Object (GPO). For more information on this topic see Microsoft Support articles 306992 and 555631.
    - Deploy a secure password storage policy that provides password encryption.
- If an administrator account is compromised, change the password immediately to prevent continued exploitation. Changes to administrator account passwords should only be made from systems that are verified to be clean and free from malware.
- Implement guidance and policy to restrict the use of personal equipment for processing or accessing official data or systems (e.g., working from home or using a personal device while at the office).
- Develop policies to carefully limit the use of all removable media devices, except where there is a documented valid business case for its use. These business cases should be approved by the organization with guidelines for their use.
- Implement guidance and policies to limit the use of social networking services at work, such as personal email, instant messaging, Facebook, Twitter, etc., except where there is a valid approved business case for its use.

Appendix 1: US CERT Recommendations

- Adhere to network security best practices. See http://www.cert.org/governance/ for more information.
- Implement recurrent training to educate users about the dangers involved in opening unsolicited emails and clicking on links or attachments from unknown sources. Refer to NIST SP 800-50for additional guidance.
- Require users to complete the agency's "acceptable use policy" training course (to include social engineering sites and non-work related uses) on a recurring basis.
- Ensure that all systems have up-to-date patches from reliable sources. Remember to scan or hash validate for viruses or modifications as part of the update process.