WEI INSIGHTS WHITE PAPER

EFFECTIVELY MANAGING CYBER SECURITY: THE TOP 5 ENTERPRISE THREATS

Modern hackers are strategic. Hackers of today are exhibiting more patience, planning, and boldness than ever before. They are also getting better at hitting higher value targets such as C-level executives. They are creative and adaptive, working collaboratively as teams or leveraging lower-level security vulnerabilities to launch a more serious attack. Yes, they are still out to steal and sell credit-related personal data, but they are better at identifying buyers for additional types of data such as trade secrets, health insurance data, information used for blackmail, and credit-related business data.[1] In short, hackers are acting more like business people.

Today's hackers also have access to an arsenal of tools, thanks in part to an anonymous and hidden area of the Internet called the Dark Web. Payment for purchases made there is typically in the international digital currency Bitcoin, which offers a fairly high level of privacy. On the Dark Web, hackers buy and sell tools such as malicious software that allow hackers to secretly control people's computers, website scrapers that duplicate an entire website so users don't realize they've been redirected there, and skimmers that attach to ATMs and gas pumps to capture credit card information. Hackers can buy or sell proprietary information, passports, driver licenses, fake bank accounts, credit card numbers, and login credentials for social media and financial accounts. Hackers can also hire consultants on the Dark Web.

So what does this mean for your enterprise? Technology is evolving quickly and hackers are evolving along with it. It might be time to get in the mind of the hacker to ensure you've taken the right steps to safeguard your network.

Before the next review of your security strategy and best practices, learn about the top five cyber security threats to the confidential and proprietary information on your network.

1. HACKERS WILL CONTINUE TO ATTACK YOUR ORGANIZATION THROUGH YOUR EMPLOYEES.

Hackers are actively developing new ways to compromise your employees by leveraging longstanding techniques. These include sending email that contains malicious links or attachments, attacks through social media, and attacks that launch from a legitimate website.

Attacks through malicious email

Known as phishing, malicious emails that trick an employee into opening a bad website or attachment are still the tool of choice for hackers who want to penetrate your network.

Attackers know that the best way to get someone to open an email is to make it appear that a trusted source sent it to an individual or a group to which the individual belongs, which is called spear phishing. In 2012, Trend Micro found that 91% of targeted attacks, those that focus on an individual or a company, involved spear phishing emails.[2]

One of the most effective phishing methods is to pose as a trusted coworker. Attackers pose as employees. They create believable scenarios such as your CFO asking Accounts Payable to process an unexpected invoice or your Security team asking employees to log into a new portal using current network credentials. An attacker either compromises a company email account or creates a convincing external email that appears to be internal. In the 2012 research referenced above, Trend Micro found that nearly half of employee email addresses could be found through a Google search, and half of those remaining could be easily guessed based on a predictable pattern.

An attacker also can pose as an employee in person by cloning an employee badge, in an attempt to physically access secure areas.[3]

Attacks through LinkedIn and other social media

Just a year ago, a LinkedIn user could identify most fake LinkedIn accounts. Fake accounts had telltale signs such as no connections, no recommendations, or unbelievable or absurd information. Today, a hacker might create several fake accounts that write recommendations for each other.[4] In addition, hackers are launching multi-stage and bolder social attacks. For instance, an attacker might pose as an employee on LinkedIn and build credibility for the ruse by linking to dozens of your lower level employees before linking to people in your C suite, which contains the highest value targets. Symantec discovered that real users will even endorse the fake LinkedIn profiles.[5]

Attacks by redirecting website traffic or by planting malware on legitimate sites

Attackers sometimes use websites that are frequented by targeted employees or targeted industries as watering holes to attract victims. The attackers either secretly redirect traffic from the legitimate website to a fake one or plant malware on the legitimate sites.

With some early conversations about the practice in 2012[6], watering hole attacks have become more frequent recently.[7] For instance, in 2013, hackers compromised the website of a law firm that serves the energy industry.[8] The website visitor downloaded a piece of malicious code that checked the system configuration before downloading malware that was appropriate for the internet browser being used.

2. ENTERPRISES WILL CONTINUE TO UNDERESTIMATE MALICIOUS INSIDERS.

In Spring 2015, the FBI and Justice Department began investigating employees at the St. Louis Cardinals for using knowledge of a reused password to break into a Houston Astros database.[9] The database contained information about trades, proprietary statistics, and scouting reports. Employees at the Cardinals may have been able to guess the password from Astros' General Manager Jeff Luhnow's time with the Cardinals.

One of the best known examples of a rogue insider is Edward Snowden, a government contractor turned hacktivist (hacker with political or social motivation) who gave journalists thousands of documents about US national security.

Some researchers group together breaches caused by malicious insiders and unintentional insider-initiated breaches, as in a PwC report[10] based on a 2014 security survey. Therefore, there is a shortage of good statistics about the prevalence of malicious insiders. In addition, awareness may remain low because affected companies often don't prosecute. About 75% of organizations that responded to PwC's survey said they didn't take legal action against insiders, defined as current and former employees, customers, and third-party partners such as service providers, consultants, vendors, and suppliers.

3. CYBER ATTACKS WILL IN SOME CASES CAUSE PHYSICAL DAMAGE.

The Stuxnet incident of 2010 was the first known case of a cyber attack that resulted in physical damage.[11] Stuxnet disrupted and damaged a nuclear centrifuge in Iran. The next known cyber-physical attack was in late December 2014, when Germany's Federal Office for Information Security announced that hackers attacked a steel mill's business office with a malicious email and gained access to plant systems. As a result, a blast furnace could not be properly shut down, which resulted in "massive" damage, according to the announcement.

These types of attacks are focused on cyber-physical systems, systems in which computer applications and networks control physical systems, and embedded systems, a computer system or component performing a specific function within a larger mechanical or electrical system. Cyber-physical systems also include GPS-based technologies, according to Homeland Security,[12] which has launched a GPS Vulnerability Assessment as part of its Critical Infrastructure Project. Many enterprises have not secured cyber-physical and embedded systems, so these systems

present attractive attack surfaces for hackers. In the years ahead, more enterprises will sustain physical damage as a result of attacks launched through these systems.

4. LARGE, WELL-FUNDED TEAMS OF HACKERS WILL CONTINUE TO LAUNCH SUBTLE, LONG-TERM ATTACKS AGAINST ENTERPRISES.

In cyber security, an advanced persistent threat (APT) is an attack that sends out tiny packets of confidential or proprietary information over extended periods of time that are masked as normal network activity. "Once 'inside' and disguised as legitimate traffic, they can establish covert, long-term residency to siphon your valuable data with impunity," according to a McAfee white paper on APTs.[13]

APTs often focus on information that can be sold or used for competitive advantage such as trade secrets, intellectual property, source code, and personal information about customers or employees that can be used to open credit.[14] Imagine large organizations of hackers working together, sometimes for years. An APT is a software project that involves target identification, target and environment research, exploit design and development, testing, deployment, and plans for future releases as technology changes.[15]

In November 2014 at a US House of Representatives Intelligence committee hearing, National Security Agency Director Admiral Michael Rogers warned manufacturers and utility companies of the growing risk of economic espionage by nation states[16], which are thought to sponsor many of these sophisticated and prolonged attacks. In fact, APT techniques are being used against an increasingly wide variety of industries and companies.[17] For example, the organization that launched Operation Shady RAT, an attack initiated in 2006 and discovered by McAfee in 2011, successfully penetrated 71 companies across 31 industries.[18] As enterprises get better at detecting APTs, security industry experts are realizing that APTs are a much more common problem than previously thought.

5. RANSOMWARE WILL APPEAR ON MOBILE DEVICES, THE INTERNET OF THINGS, AND NETWORKS.

Ransomware is malicious software that either locks a system or locks electronic files and documents until a fee is paid. In effect, it holds the data or system hostage. The number of ransomware attacks more than doubled between 2013 and 2014, according to Symantec's 2015 Internet Threat Report.[19]

A couple of years ago, ransomware started appearing on Android-based mobile devices.[20] While acknowledging that mobile devices are still not considered a mainstream cyber attack vector, a report by security technology firm Blue Coat[21] reports an uptick in mobile ransomware and other mobile attacks and suggests care. "The sky is not falling – but putting on a helmet is a good idea," the report says.

Meanwhile, IoT devices, which communicate with other devices without human prompting, have become known for security problems in their short history.[22] In 2014, the Open Web Application Security Project (OWASP) developed its first top 10 list of vulnerabilities for the IoT. [23] Many enterprises rely on systems that are riddled with embedded IoT devices such as data centers, smart industrial control and manufacturing systems, smart inventory systems, smart building technology, and the smart power grid.

Forrester Research is making a similar IoT security prediction on the consumer goods side.[24] Forrester predicts that the world will begin to see ransomware attacks on wearable devices and embedded medical devices like pacemakers, which also of course impacts the enterprises that manufacture these devices. Some also predict ransomware for large ticket items such as cars and refrigerators[25].

IBM predicts that attackers will increasingly graduate from extorting individuals to extorting large organizations and enterprises[26]. The start of this trend is already evident. For instance, several police departments have suffered ransomware attacks[27]. And in March 2015, attackers demanded more than $100,000 to release the files of a school district[28].

CONCLUSION

As the number of devices that access corporate networks continues to rapidly grow and systems become smarter by communicating with other systems, hackers are exploring larger attack surfaces with far more potential entry points into your network. At the same time, thanks to social media, attackers have access to personal information about many of an organization's employees, which again expands the attack surface.

Attackers are discovering new ways to use tried-and-true attacks such as phishing scams, are inventing new attacks such as ransomware, and are learning how to exploit emerging technologies such as mobile devices and the Internet of Things.

Meanwhile, the best offense for enterprise IT leaders continues to be a good defense. Enterprises are keeping attackers outside of the perimeter with better monitoring tools and a better trained workforce. Security teams are responding swiftly and decisively to security incidents thanks to better planning. And IT leaders are working with highly-experienced technology consulting teams who can help their organizations securely implement new enterprise technologies.

Sources

1. Ablon, Lillian, Libicki, Martin, and Golay, Andrea. Markets for Cybercrime Tools and Stolen Data: Hacker's Bazaar (White Paper, 2014). RAND Corporation. Web.
(http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.
2.TrendLabs APT Research Team. Spear-Phishing Email: Most Favored APT Attack Bait (2012): 1. Trend Micro Incorporated. Web.
<http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf>.
3.Kerner, Sean Michael. RFID Susceptible to Cloning, Other Hacks (August 12, 2015). Quinstreet Enterprise. Web.
<http://www.esecurityplanet.com/network-security/rfid-susceptible-to-cloning-other-hacks.html>
4.Kopan, Tal. Report: Iran-based hackers spy using fake LinkedIn profiles (October 7, 2015). Cable News Network. Web.
<http://www.cnn.com/2015/10/07/politics/iran-hackers-linkedin/index.html>.
5. Narang, Satnam. Fake LinkedIn accounts want to add you to their professional network (December 2, 2015). Symantec Corporation. Web.
<http://www.symantec.com/connect/blogs/fake-linkedin-accounts-want-add-you-their-professional-network>.
6. Krebs, Brian. Espionage Hackers Target 'Watering Hole' Sites (September 25, 2012). Krebs on Security. Web.
< http://krebsonsecurity.com/tag/watering-hole-attack>.
7 Symantec Security Response Team. New Flash Zero-Day Linked to Yet More Watering Hole Attacks (February 21, 2014). Symantec Corporation. Web.
<http://www.symantec.com/connect/blogs/new-flash-zero-day-linked-yet-more-watering-hole-attacks>.
8.LightOut Is Latest Cyber Threat to Target Energy Sector (March 15, 2014). Reed Exhibitions, Ltd. Web.
(http://www.infosecurity-magazine.com/news/lightout-is-latest-cyber-threat-to-target-energy).
9. Schmidt, Michael. Cardinals Investigated for Hacking Into Astros' Database (June 16, 2015). New York Times. Web.
<http://www.nytimes.com/2015/06/17/sports/baseball/st-louis-cardinals-hack-astros-fbi.html>.
10. Managing cyber risks in an interconnected world: Key Findings from The Global State of Information Security Survey of 2015 (September 30, 2014). PwC. Web.
<http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf>.
11. Zetter, Kim. A Cyberattack Has Caused Confirmed Physical Damage for the second Time Ever (January 8, 2015). Wired Magazine. Web.
<http://www.wired.com/2015/01/german-steel-mill-hack-destruction>.
12. Cyber Physical Systems. US Department of Homeland Security. Web. <https://www.dhs.gov/science-and-technology/cyber-physical-systems>.
13. Combating Persistent Threats (White Paper, 2011). McAfee. Web. < http://www.mcafee.com/us/resources/white-papers/wp-combat-advanced-persist-threats.pdf>.
14. Advanced Persistent Threats: Understand the Threat, Motives tab. Dell SecureWorks. Web.
<http://www.secureworks.com/cyber-threat-intelligence/advanced-persistent-threat/understand-the-threat>.
15. Finkle, Jim, and Menn, Joseph. Suspect in 'Blackhole' cybercrime case arrested in Russia (October 13, 2013). Reuters. Web.
<http://www.reuters.com/article/net-us-cybercrime-arrest-idUSBRE99714Y20131013>.
16. Paganini, Pierluigi. The looming threat to America's backbone (November 25, 2014). Fox News. Web.
< http://www.foxnews.com/tech/2014/11/25/looming-cyberthreat-to-americas-backbone.html>.
17. Advanced Persistent Threats: Understand the Threat, Targets tab. Dell SecureWorks. Web.
<http://www.secureworks.com/cyber-threat-intelligence/advanced-persistent-threat/understand-the-threat>.
18. Alperovitch, Dmitri. Revealed: Operation Shady RAT (White Paper, 2011). McAfee. Web. < http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>.
19. 2015 Internet Security Threat Report, Volume 20. Symantec. Web. <http://www.symantec.com/security_response/publications/threatreport.
jsp?cid=70150000000diToAAI&om_sem_cid=biz sem_273692754025047|pcrid|9711531381|pmtle|plcl{placement}|pdvlc>.
20. Pichel, Abigail. Ransomware Moves Mobile (May 26, 2014). Trend Micro. Web. <http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-moves-to-mobile>.
21. 2015 Mobile Malware Report. Blue Coat Systems. Web. <http://resources.idgenterprise.com/original/AST-0158766_bcs_2015_Mobile_Malware_Report_EN_v1e.pdf>.
22. Hill, Kashmir. The Half-Baked Security Of Our 'Internet of Things' (May 27, 2014). Forbes. Web.
<http://www.forbes.com/sites/kashmirhill/2014/05/27/article-may-scare-you-away-from-internet-of-things/>
23. Top 10 IoT Vulnerabilities (2014) Project. Open Web Application Security Project. Web.
<https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Top_10_IoT_Vulnerabilities__282014_29>.
24.Hayes, Nick, Holland, Rick, et al. Predictions 2016: The C-Suite and Cybersecurity (November 12, 2015). Forrester Research. Web.
<https://www.forrester.com/Predictions+2016+The+CSuite+And+Cybersecurity/fulltext/-/E-RES121701>.
25. Donohue, Brian. Ransomware Is the Future of Consumer Cybercrime (December 4, 2014). Kaspersky Lab.
< https://threatpost.com/ransomware-is-the-future-of-consumer-cybercrime/109724>.
26. IBM X-Force security research team. IBM Security IBM X-Force Threat Intelligence Quarterly, 3Q 2015 (White Paper, August 2015). IBM. Web.
< https://www-01.ibm.com/marketing/iwm/dre/signup?source=swg-WW_Security_Organic&S_PKG=ov38487&S_TACT=C41303YW&dynform=20131>.
27. Peters, Sara. Police Pay Off Ransomware Operators, Again (April 14, 2015). InformationWeek. Web.
<http://www.darkreading.com/attacks-breaches/police-pay-off-ransomware-operators-again/d/d-id/1319918>.
28. Bisson, David. Ransomware Holds School District Computer Systems Hostage (March 25, 2015). Trip Wire. Web.
< http://www.tripwire.com/state-of-security/latest-security-news/ransomware-holds-school-districts-computer-systems-hostage/>

ABOUT WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. *Because we go further.*

At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 25 years.

info@wei.com

800.296.7837

www.wei.com

43 Northwestern Drive
Salem, NH 03079

TALK TO WEI TODAY

Enterprises are investing in cyber security more than ever before, and yet damaging breaches occur all too often. Learn about our free Security and Threat Prevention Assessment which identifies vulnerabilities in your network and provides personalized recommendations for improved security.