AUTOMATION AND CYBER SECURITY TRENDS

FOR 2018 AND BEYOND

Enterprise Integration | entint.com | 888-848-9332 | info@entint.com

EXECUTIVE SUMMARY

In starting out the new year of 2018, several important cyber security issues still remain from 2017. Ransomware, the Internet of Things (IoT) and consumer and personal devices have stayed at the top of the list and are immediately followed by the continuing attacks on the healthcare industry and other institutions as well the growing threat of weaponized artificial intelligence (AI). Making matters worse, a widespread shortage of cybersecurity professionals also continues to be a trend as well.

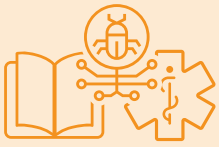
While businesses are beginning to understand the need for improved security, hackers and cyber-criminals are meeting those advancements with increasingly sophisticated attacks. Any company that uses computer systems or digital devices is now, and will continue to be, at risk.

Ransomware has topped the trends list since 2015 and continues to be a major concern. Ransomware typically takes one of two forms. The first is one where the user is made to believe that their computer has been locked and only paying the ransom will unlock it. The other, more damaging form encrypts some or all of the user's data files and demands payment to provide the decryption key. Organizations with understaffed security departments or insufficient information security or incident response programs are most susceptible to these types of attacks.

In targeted ransomware attacks, hackers often look for organizations that have valuable, mission-critical

"...INCREASINGLY SOPHISTICATED ATTACKS."

"...GROWING THREAT OF WEAPONIZED ARTIFICIAL INTELLIGENCE(AI)."



"TWO COMMON TARGETS ARE EDUCATIONAL INSTITUTIONS AND MEDICAL FACILITIES."

data to protect, but that typically have inadequate information security programs or incident response plans. Two common targets are educational institutions and medical facilities. These organizations have large amounts of critical data, but frequently lack sufficient funding, expertise or staffing to protect it.

"**ATTACKS** ON **IOT DEVICES** HAVE ALSO **INCREASED** SINCE **2016**"

Attacks on IoT devices have also increased since 2016, and with the increasing number of connected devices hitting the market, the rate continues to climb. IoT devices tend to be feature-driven and under market pressure to keep prices low. This results in devices where security is an after-thought; if it is a factor at all. To make matters worse, most consumer IoT devices are difficult or even impossible to update. This means that any security vulnerability discovered in one of these devices is very likely to remain unpatched for the entire life of the device.

ANY SECURITY VULNERABILITY DISCOVERED IN ONE OF THESE DEVICES IS ***VERY LIKELY TO REMAIN UNPATCHED*** FOR THE ENTIRE LIFE OF THE DEVICE.

Hackers and unpatched devices aren't the only things that organizations have to defend against. The use of artificial intelligence and machine learning in cyberattacks is just beginning to become a credible threat, but in years to come that threat is only expected to grow.

From personal devices like health sensors to robots, smart cars and facial recognition, the latest innovations that make life easier and more connected can also open up the user and their companies to attacks due to lack of adequate

security. Regulatory compliance, such as HIPAA, is another consideration when storing or processing personal data collected by these devices.

The incidents of security breaches and events continue to increase and there is a world-wide shortage of cybersecurity specialists available to combat the rampant rise in attacks. With businesses both large and small, current staff are unable to handle advanced threats or even become aware of them which leads companies to turn to different workforce strategies to connect with talent and also employ agencies that can provide virtual security teams (for example, vCISO) with the skills and experience to protect their organizations.

Ransomware, attacks on institutions, hacking of IoT and consumer devices and the weaponizing of AI, are all key areas that will be threats in 2018 and into the future. High net worth individuals, as well as the small businesses that work with them and their corporations, will become likely targets. Politics will also play a major role as the impact of hacking plays a larger role in future elections. And, finally, cryptocurrency the payment method of choice of cyber criminals will be under greater scrutiny by regulatory agencies.

INTRODUCTION

With so many cyberattacks happening each year, companies are finding it harder and harder to determine what mechanisms to put into place to and who to hire to provide the security they need to continue running their businesses. Insider threat is one of the easiest ways that hackers gain access to systems and new technical advances. Key factors for companies, agencies and institutions to be prepared to handle the cyber security issues facing them in 2018 should include planning, training, automation and management.

RANSOMWARE

According to the MIT Technology Review "Ransomware is a relatively simple form of malware that breaches defenses and locks down computer files using strong encryption. Hackers then demand money in exchange for digital keys to unlock the data." With that, ransomware has two categories: 1) system is locked and user is tricked into thinking that unlocking it requires paying a ransom, or 2) files saved to the user's hard drive and network shares are encrypted then the data is "held" for ransom.

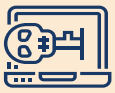
In May 2017, it is believed that North Korean agents targeted computers running the Windows operating system and spread the malware through an exploit known as EternalBlue. Though Microsoft had released patches prior to the attack to close the vulnerability, organizations that were hit were those that had not kept current on system updates.

Taking patch maintenance into consideration, the best methods to protect against ransomware is to ensure vendor-supplied antivirus updates and patches are applied as soon as possible, and to diligently perform system backups. Having a patch management schedule and a good tested backup process allows organizations to restore systems to a pre-encrypted state further allowing organizations to ignore the ransomware extortion.

CURRENT TRENDS TO WATCH

- **Malware** will be a serious issue and organizations need to have processes in place to automatically keep system patches up-to-date.
- **Cyber criminals** continue to conduct ransomware campaigns but will be choosing smaller targets with higher rewards.

RANSOMWARE CATEGORIES



system is locked and user is tricked into thinking that unlocking it requires paying a ransom

files saved to the user's hard drive and network shares are encrypted then the data is "held" for ransom

INSTITUTIONAL ATTACKS

Hackers have a history of looking for institutions without many cybersecurity resources, such as hospitals, schools, and universities. Hospitals are often targets because of medical records and for the fact that a hospital's resources are directed toward helping patients. Schools and universities handle many personal records and have limited security safeguards. The best defense against attacks like The Dark Overload where the school district's data was breached and allowed the release of student information that lead to threats of violence against the students is for schools and universities to incident response plans in place.

THE RECORDS OF OVER 18,000 PATIENTS AT RISK

Hospitals and medical facilities had numerous and various breaches in 2017. A Detroit healthcare system had email credentials stolen which put the records of over 18,000 patients at risk. In Georgia, a university medical center fell victim to a phishing attack and even though the breach caused minimal damage, it was the second breach of its kind to hit the center and resulted in a fine of nearly $500,000. And

HAVING LAX CYBER SECURITY **COST BUSINESSES MILLIONS** IN FINES, REPARATIONS

BIGGEST RISK for a **SECURITY BREACH**

HOSPITALS

SCHOOLS

UNIVERSITIES

finally, a mid-western imaging center suffered a breach of its computer system and was fined for not reporting the incident in a timely manner. In addition to the fines, the center paid to provide identity and theft protection to those affected. Having lax cyber security cost businesses millions in fines, reparations, and in having to bolster their systems after the attacks. To prevent attacks before they happen, organizations need to be aware of what measures to take to safeguard themselves, their associates, and clients. Having incident response plans and insider threat training helps to make sure employees know how to prevent attacks as well as manage them when they occur.

Information security assessments can determine if vulnerabilities exist within the organization and having a team available to provide incident response when in-house systems have been compromised goes a long way to reducing risk. Both academic and medical institutions can benefit from having incident response plans in place while also conducting drills to handle possible cyberattacks directed at students and patients.

CURRENT TRENDS TO WATCH

- **Healthcare facilities, medical offices and academic institutions** will continue to be **targets** due to their wealth of sensitive data. These organizations need to **bolster** their security posture by contacting third party consultants who conduct security assessments and help dedicated in-house **security staff** with mitigating vulnerabilities.
- Organizations will increasingly rely on **cyber insurance** to mitigate the impact on their business from a breach or cyberattack.

BOTH ACADEMIC AND MEDICAL INSTITUTIONS CAN BENEFIT FROM HAVING INCIDENT RESPONSE PLANS IN PLACE WHILE ALSO CONDUCTING DRILLS TO HANDLE POSSIBLE CYBER ATTACKS DIRECTED AT STUDENTS AND PATIENTS.

INTERNET OF THINGS (IOT) HACKS

With the vast number of products rolling out that are connected to the internet, organizations may be more vulnerable to security breaches. Often these IoT products don't have adequate security measures in place to protect business' information. Gartner Inc. estimates that 20.8 billion connected things will be in use by 2020 and with that many products, the risks have increased and security struggles to keep pace with the growing number of devices.

Organizations should take time to evaluate their security posture and have a third party provide a security assessment. Other measures might include restricting access to critical systems, only allowing employees enough connectivity and access to successfully complete their jobs/tasks. Additionally, organizations should conduct a full asset inventory to identify what is connected, where the asset is located and be aware of what data is being transmitted. IT teams within the organization can verify that proper protocols are in place for the network and that every effort is being made to eliminate potential back doors. If purchasing off the shelf (OTS) software, conduct extensive research on how the product was tested and identify any potential security risks. Also, verify that the devices allow default credentials to be changed, require a username and password and can receive security updates.

GARTNER INC. ESTIMATES THAT 20.8 BILLION CONNECTED THINGS WILL BE IN USE BY 2020 AND WITH THAT MANY PRODUCTS, THE RISKS HAVE INCREASED AND SECURITY STRUGGLES TO KEEP PACE WITH THE GROWING NUMBER OF DEVICES.

Similarly included in the growing category of IoT is robots, health sensors, smarter cars and facial recognition programs. These are all examples of consumer products that may record, collect, & store personal data such as who you are, where you are, where you use the device and how you interact with it.

The connection and communication between multiple devices on the Internet will continue to grow and automation is fast becoming the best way to keep pace with the vast amount of ever-changing and increasingly connected data. Automating asset discovery helps organizations track hardware and software assets and provides insight into information technology systems. Discovering what assets are available and their uses allows for a more complete security assessment to be conducted.

AUTOMATION IS FAST BECOMING THE BEST WAY TO KEEP PACE WITH THE VAST AMOUNT OF EVER-CHANGING & INCREASINGLY CONNECTED DATA

CURRENT TRENDS TO WATCH

- Linux powers the IoT devices and is the **perfect target for cyber criminals** who exploit the weak default security settings.
- **More threats** will be directed toward the Cloud and smaller Cloud data companies, without the resources of larger Cloud companies (Google, Amazon), will be the first to fall prey to cyber criminals.

IT TALENT SHORTAGE

According to the 2015 (ISC)2 Global Information Security Workforce Study, 62% of organizations have too few information security professions and this gap is largely due to an insufficient pool of suitable candidates. The study predicted that there will be shortfall of 1.5 million security analysts by 2020. Companies have increased security spending for technology, personnel and training and salaries have risen drastically to retain the security professions currently working within organizations.

62% OF **ORGANIZATIONS** HAVE TOO FEW INFORMATION SECURITY PROFESSIONS

As cyber criminals have grown their talent pool and become more aggressive, organizations are struggling to fill their IT security ranks. Companies have taken measures to combat the current shortage of cybersecurity specialists by re-examining their workforce strategy. They are rethinking the traditional 4-year-tech-degreed analyst and opening up their organization to those with more varied skillsets. Training and security awareness have also become company-wide concerns and other departments are educating end-users to be security-conscious. Additionally, organizations are searching for consultants, vendors and interns to supplement their internal talent pool. Many companies want to improve engagement with prospective talent and have built local cyber security networks within colleges and universities. Additionally, outreach programs to government organizations, law enforcement, computer forensics and cyber security professional organizations like ISACA have proven helpful in obtaining access to prospective security talent. Some companies are utilizing

CYBER CRIMINALS HAVE GROWN THEIR TALENT POOL AND BECOME MORE AGGRESSIVE

AI to assist in overcoming the skills shortage which allows for automated handling of minor security issues while allowing security to focus their efforts on more serious incidents.

Enlisting the assistance of a third-party consultant or hiring a Virtual Chief Information Security Officer (vCISO) provides an experienced and credentialed leader without the cost of a full-time CISO. The role would have access to enterprise tools, best practices and processes as well as offer oversight and thought leadership.

CURRENT TRENDS TO WATCH

- Until new cyber security professional can be trained and are available to handle the onslaught of attacks, security teams will continue to feel overwhelmed. Between studying the latest exploits, patching vulnerabilities and countering the latest attacks against system security, organizations will continue to struggle to secure their data.

ARTIFICIAL INTELLIGENCE IN THE HACKING WAR

Hackers have been and will continue to weaponize AI to accomplish their end of hitting more targets, but luckily, the security protections being developed with similar AI technology are able to help combat cybercriminals.

Top leaders in the fields of AI such as MIT and the Defense Advanced Research Projects Agency (DARPA) have begun to address the issue of weaponizing AI. MIT indicates that

cyber security professionals have been using machine-learning models and other AI technologies to recognize the likelihood of an attack. Hackers are able to leverage artificial intelligence to target and attack more systems in less time, reducing their personal risk and giving them an advantage over defenders. Cyber criminals have used robots to mimic users and utilized those programs to infiltrate companies using harvested user credentials.

DARPA created a challenge that set AI against AI with the idea that the AI systems would act at machine speed and scale to perform software security analysis, counter bugs, and search millions of lines of code to identify possible vulnerabilities. The Cyber Reasoning Systems (CRS) were designed to hunt down and patch vulnerabilities and protect the host machines. The challenge proved that AI systems could be effective by analyzing, discovering and automatically fixing the vulnerabilities before they become problems and could do so faster and more efficiently than the humans who designed the systems.

Security protection like an automated digital robotic engine seems like science fiction; however, these systems are currently available and can be used to combat AI hackers.

AI SYSTEMS COULD BE EFFECTIVE BY ANALYZING, DISCOVERING & AUTOMATICALLY FIXING THE VULNERABILITIES BEFORE THEY BECOME PROBLEMS AND COULD DO SO FASTER AND MORE EFFICIENTLY THAN THE HUMANS WHO DESIGNED THE SYSTEMS.

CURRENT TRENDS TO WATCH

- Artificial intelligence will continue to be used in attacks and cyber criminals will escalate these attacks as the AI learns more about the targets.

ENTERPRISE INTEGRATION

Enterprise Integration powered by Digital Robotics

delivers Managed Services to clients, transforming their IT operations

to world class standards, so they can focus on their business.

DELIVERING THE PROMISE OF IT.

7601 Centurion Parkway | Jacksonville, FL 32256 | 904.733.4349

REFERENCES

Cyber Security: Trends from 2017 and Predictions for 2018
(n.d.). Retrieved March 10, 2018, from http://mindstarsecurity.com/

Six Cyber Threats to Really Worry About in 2018
(January 2, 2018). https://www.technologyreview.com/s/609641/six-cyber-threats-to-really-worry-about-in-2018/

The Biggest Healthcare Breaches of 2017
http://www.healthcareitnews.com/slideshow/biggest-healthcare-breaches-2017-so-far?page=1

DARPA Cyber Grand Challenge (CGC) (n.d.). Retrieved March 20, 2018 from
https://www.darpa.mil/program/cyber-grand-challenge

Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015 *(November 2015)*
https://www.gartner.com/newsroom/id/3165317

Frost & Sullivan - Global Information Security Workforce Study
(April 2015)
https://www.iamcybersafe.org/gisws/

https://iamcybersafe.org/wp-content/uploads/2017/01/FrostSullivan-ISC%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf