AccumeView: Executive Cybersecurity Pulse

The monthly executive review is intended to keep you informed of recent threats that can impact the confidentiality, integrity and availability of your data and information systems so that your institution can make the necessary technical and procedural changes to protect your institution.

Perspective: state of the marketplace

ATM Jackpotting has finally hit the US. In previous briefings, we have highlighted attacks in Asia, South America, Africa and the EU. In all reported cases, the bad actors physically compromised the ATMs using specialized tools to inject malware into the device. This is a good reminder that physical security barriers such as locks only slow down determined attackers – the root cause needs to be addressed wherever possible.

Cyber Incidents are a continued threat to institutions, but a recent report states that incidents have doubled, while an analysis of the incidents reveals that 93% of them are preventable through controls like patching and email authentication. These statistics should be an incentive to keep your security awareness program up to date, and continue the maturity progress of your overall IT control structure.

GDPR has another deadline on the horizon for institutions conducting business in Member States. Another wave of requirements around cyber security take effect as part of the NIS Directive covering network and information security that must be put into place across Member States by May 9, 2018. If you perform business in the EU, now is the time to ensure that you will be compliant, as there are penalties for non-compliance

SIM Hijacking is now becoming a threat that institutions should be aware of. As phone numbers become a de facto standard for password recovery, SIM Hijacking is an effective way of taking over a victim's cell phone, exposing their bank social media and email accounts.

The **SEC** has new guidance on security breaches, including additional requirements around information disclosure and communications. Primarily, they want public companies to provide investors more information on their cybersecurity incidents as well as risks. They also want to ensure that executives are not trading shares during the duration of an investigation

~Stay Secure

If you found this information valuable, we recommend taking a look at our weekly threat intelligence brief. For more information, contact us here.

Bob Gaines,
Director,
Information
Security

646.375.9500 x114

rgaines@accumepartners.com

Security Highlights

First ATM 'Jackpotting' Attacks Hit US: Five years ago, security researchers first spotted a strain of malware – nicknamed Ploutus – that was being used to infect ATMs in Mexico and drain them of them their cash, in what's known as a cash-out or jackpotting attack. Now, the U.S. Secret Service is warning ATM manufacturers that for the first time, such attacks have migrated to the United States. Source: https://www.bankinfosecurity.com/first-atm-jackpotting-attacks-hit-us-a-10610

Report: Number of cyber incidents doubled in 2017, yet 93 percent could easily have been prevented. Out of nearly 160,000 reported cyber incidents affecting businesses in 2017, 93 percent could have been prevented by following basic security measures such as regularly updating software, blocking fake email messages, using email authentication, and training employees, a new report claims. The overall number of reported incidents nearly doubled 2016's total of 82,000 incidents, according to the Online Trust Alliance (OTA), an Internet Society initiative, which released its 2017 Cyber Incident & Breach Trend Report on Jan. 25, in advance of Data Privacy Day. Source: https://www.scmagazine.com/report-number-of-cyber-incidents-doubled-in-2017-yet-93-percent-could-easily-have-been-prevented/article/739932/

Global Cybercrime Costs $600 Billion – More than 50% of attacks result in damages over $500K, two reports show. In cybersecurity it can sometimes be hard seeing the forest for the trees. Constant reports about new attacks, breaches, exploits and threats can make it hard for stakeholders to get a picture of the full impact of cybercrime. Source: https://www.darkreading.com/attacks-breaches/global-cybercrime-costs-top-$600-billion-/d/d-id/1331106

Crypto-Mining Attacks Emerge as the New Big Threat to Enterprises: Attackers looking to hijack systems for illegally mining digital currencies have begun eyeing business systems, security vendors say. In an ominous trend for businesses, hijacking computers for cryptocurrency mining appears to have become *the* go-to strategy for cybercriminals looking for a safe and reliable way to generate illegal revenues. Source: https://www.darkreading.com/attacks-breaches/crypto-mining-attacks-emerge-as-the-new-big-threat-to-enterprises/d/d-id/1330965

Regulatory Headlines

Europe's New Data Protection Rules Export Privacy Standards Worldwide: Europe wants to conquer the world all over again. Only this time, its killer app isn't steel or gunpowder. It's an EU legal juggernaut aimed at imposing ever tougher privacy rules on governments and companies from San Francisco to Seoul. When the region's regulators roll out the changes – known as the General Data Protection Regulation, or GDPR – it will represent the biggest overhaul of the world's privacy rules in more than 20 years. Source:

https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/

The GDPR Clock Is Running Out. Now What? On May 25, the European Union's General Data Protection Regulation (GDPR) goes into effect. The transformative new law is expected to have a profound impact on how businesses the world over collect, manage, and defend their data. But while companies have had more than two years to prepare for the ground-breaking legislation – passed in late 2015 – many organizations that will be impacted most by the new rules are still blind to some of the basics. https://www.darkreading.com/partner-perspectives/iboss/the-gdpr-clock-is-running-out-now-what-/a/d-id/1331030

Banks preparing for heightened New York cybersecurity laws to take effect. This week, senior executives from more than 3,000 banks, insurers and other financial services companies doing business in New York will have to personally certify that their computer networks are protected by a cybersecurity program appropriate for their organization's risk profile. The certification, imposed by the state's banking regulator as part of its state cybersecurity rules, is the first in a slew of new requirements that will come into effect this year in New York — one of the leading centers of the global banking system. Read More: https://www.cyberscoop.com/new-york-financial-cybersecurity-law-deadline-february-2018/

SEC: Companies Must Disclose More Info on Cybersecurity Attacks & Risks – New agency guidance statement also says company officials, execs can't trade stocks if they have unannounced information on a security breach at the company. The Securities and Exchange Commission (SEC) has issued updated guidance for public companies that calls for providing investors more information on their cybersecurity incidents – as well as risks – in a more timely fashion. Source: https://www.darkreading.com/endpoint/privacy/sec-companies-must-disclose-more-info-on-cybersecurity-attacks-and-risks/d/d-id/1331109

Social Engineering

Here are the 'most clicked' phishing email templates that trick victims. Wombat Security has released its fourth annual State of the Phish report. Wombat revealed that phishing rates in 2017 remained steady—76% of infosec professionals surveyed said that their companies experienced phishing attacks, roughly the same as 2016. Click rates have dropped to an average of nine percent, down from 15% in 2016, which is encouraging—users seem to be getting the message about the dangers of phishing. Source: https://www.techrepublic.com/article/here-are-the-most-clicked-phishing-email-templates-that-trick-victims/

Agari: Business Email Compromise (BEC) Attacks Reach 96 Percent of Organizations: Agari, a leading cybersecurity company, today published revealing research revealing that 96 percent of organizations

have received business email compromise (BEC) emails during the second half of 2017… According to the FBI, BEC attacks were responsible for more than $5.3 billion in exposed losses between 2013 and 2016. Source: http://news.sys-con.com/node/4227338

'I Lived a Nightmare:' SIM Hijacking Victims Share Their Stories. Last year, hackers found a bug that allowed them to access some personal information on any T-Mobile customer. The bug was so well known in the criminal underground that someone made a tutorial on how to exploit it on YouTube. The bug itself didn't expose anything too sensitive. No passwords, social security numbers, or credit card data was exposed. But it did expose customers' email addresses, their billing account numbers, and the phone's IMSI numbers, standardized unique number that identifies subscribers. Just by knowing (or guessing) customer's phone numbers, hackers could get their target's data. Once they had that, they could impersonate them with T-Mobile's customer support staff and steal their phone numbers. https://motherboard.vice.com/en_us/article/j5bpg7/sim-hijacking-t-mobile-stories

Study shows which phishing attacks most successful – People are very predictable when it comes to designing phishing attacks that appeal to potential victims with people most likely to click on messages concerning money. A recent KnowBe4 study sent phishing test emails to roughly 6 million and found users were most likely to click on the mock phishing emails when they promised money or threatened the loss of money. People were also likely to fall for phishing attacks appealing to their appetite offering free food or drinks, emails that evolved the fear of missing out on non-monetary opportunities and attacks that appealed to basic curiosity such as new contact requests or photo tags. Source: https://www.scmagazine.com/study-shows-most-clicked-phishing-attempts/article/743513/

Email Inboxes Still the Weakest Link in Security Perimeters– Over one-third of all security incidents start with phishing emails or malicious attachments sent to company employees, according to F-Secure. The single most common source of breaches analyzed in the report was attackers exploiting vulnerabilities in an organization's Internet facing services, which accounted for about 21 percent of security incidents investigated by F-Secure's incident responders. Source: https://www.helpnetsecurity.com/2018/02/23/weakest-link-security-perimeters/

Internal Threats

Cyber-attacks surge, ransomware leading the way. The Online Trust Alliance (OTA) found that cyber incidents targeting businesses nearly doubled from 82,000 in 2016 to 159,700 in 2017. Since the majority of cyber incidents are never reported, OTA believes the actual number in 2017 could easily exceed 350,000. OTA found that in 2017 there were 134,000 ransomware attacks on businesses, nearly doubling that of 2016. In mid-2017 another type of ransomware attack emerged—the ransom denial-of-service attack (RDoS). In this attack, criminals send an email to domain owners threatening a DDoS attack that will make a website inoperable unless a ransom (usually via Bitcoin) is paid. Source: http://threatbrief.com/cyber-attacks-surge-ransomware-leading-way/

Password Recovery Tool Shows Just How Easy It Is to Steal Windows Passwords. LaZagne is a software application whose role was to extract passwords from Windows computers, and in the previous versions, it could do that without even asking for credentials for the administrator account. The only requirement was to run the software on the target computer with the user signed in. A recent update powered by a component called LaZagneForensic (LZF) pushed things even further and allows the program to recover passwords either by extracting data from dump files from the target computer or by simply connecting the hard disk of the system to another machine. This pretty much eliminates the need for physical access to the system. Read more: http://news.softpedia.com/news/password-recovery-tool-shows-just-how-easy-it-is-to-steal-windows-passwords-519779.shtml

Fileless Malware: Not Just a Threat, but a Super-Threat. Fileless malware - in which hackers call malware routines remotely and load them into memory in order to compromise or steal data — is not new, but hackers increasingly have turned to that type of attack. According to McAfee, fileless threats with PowerShell malware grew by 119% in the third quarter of 2017 alone, and they have been such a rousing success that hackers plan to greatly expand their use this year, security experts are convinced. Source: https://www.darkreading.com/vulnerabilities---threats/fileless-malware-not-just-a-threat-but-a-super-threat/a/d-id/1331018

Mirai Variant Sets Up Proxy Servers on Compromised Devices – A newly observed variant of the infamous Mirai botnet is capable of setting up proxy servers on the infected Internet of Things (IoT) devices, Fortinet warns. Mirai is a distributed denial of service (DDoS)-capable malware family that emerged in late 2016. Targeting IoT devices to add them to a botnet and launch powerful attacks, Mirai has been involved on some massive incidents right from the start. Source: https://www.securityweek.com/mirai-variant-sets-proxy-servers-compromised-devices

Web/Internet Threats

Your website is under constant attack. Many people tell me that their websites are safe. Why? Because "Who will bother to attack my site?" Or "Our business is too small for anyone to hack." Oh please! There's this popular fallacy that attackers on the internet always target particular sites. They don't. Yes, some do. I'm looking at you Equifax. But most attacks are made by bots, which don't know a thing about you, your business, or your website. Bots don't care who you are or what you do. If you're on the web, you're a target. Source: http://www.zdnet.com/article/your-website-is-under-constant-attack/

Johnny Hacker Hauls Out NSA-Crafted Server Message Block Exploits, revamps 'em: Hackers have improved the reliability and potency of Serve Message Block (SMB) exploits used to carry out the hard-hitting NotPetya ransomware attack last year. EternalBlue, EnternalSynergy, EternalRomance and EternalChampion formed part of the arsenal of NSA-developed hacking tools that were used (in part) to mount the devastating NotPetya cyber-attack. Source: http://www.theregister.co.uk/2018/01/31/wannacry_smb_exploit_beefed_up/

FIs Hear Mobile Threat Drumbeats but Overlook Them: Verizon – Verizon's Mobile Security Index, found many organizations – including those in the financial services such as credit unions and banks – overlook basic mobile cybersecurity principles, leaving themselves and customers vulnerable to attacks. Organizations said mobile security risks are increasing. Company concerns center on the threats mobile devices pose to both their data and uninterrupted business operations. Source: http://www.cutimes.com/2018/02/22/fis-hear-mobile-threat-drumbeats-but-overlook-them

42% of the most popular websites are vulnerable to cyberattacks – Phishing attacks continue to grow more sophisticated, as 4,600 phishing sites use legitimate hosting services, according to Menlo Security. Many of what we consider the safest places on the web are actually quite risky for business professionals and consumers to visit, according to a new report from Menlo Security. Source: https://www.techrepublic.com/article/42-of-the-most-popular-websites-are-vulnerable-to-cyberattacks/

Data Breaches

Half of Norway's Population May Have Been Breached. A Norwegian healthcare provider is investigating an unauthorized intrusion into its IT systems which may have breached the personal data of over half the country's population. Helse Sør-Øst RHF (Health South-East RHF) delivers healthcare for the most populous part of the Scandinavian nation, including the capital, via 15 health trusts and a network of 19 pharmacies. This area is said to cover nearly three million of a population of a little over five million people. The country's healthcare IT security center, HelseCert, notified IT delivery partner Sykehuspartner HF (Hospital Partner HF) of "abnormal activity" at the beginning of the month, Health South East said in a statement last week. The breach was perpetrated by an "advanced and professional" player, with police having been notified. Source: https://www.infosecurity-magazine.com/news/half-norways-population-may-have/

Coincheck Admits theft of $533m of Cryptocurrency NEM – the Biggest Cyber Theft in History: Japanese cryptocurrency exchange Coincheck has admitted the loss of $533 million in NEM token from its digital wallets in a cyber theft that surpasses the Mt Gox collapse and which will go down in history as the biggest hack of all time. The company admitted the catastrophic hack at a press conference at 11:30 pm today in Tokyo. Source: https://www.v3.co.uk/v3-uk/news/3025443/coincheck-admits-theft-of-usd533m-of-cryptocurrency-nem-the-biggest-cyber-theft-in-history

Equifax Confirms 'Probable' Breached Data Was Indeed Stolen. Equifax says that its digital forensic investigators have found that while its tally of 145.5 million U.S. breach victims hasn't changed, more of them had their email addresses, tax identification numbers and driver's license information exfiltrated. Source: .https://www.govinfosecurity.com/equifax-confirms-probable-breached-data-was-indeed-stolen-a-10644

What Types of Hospitals Experience Data Breaches? – An estimated 16 million patient records were stolen in the United States in 2016, and last summer the British health system was crippled by a ransomware attack. While we know these events are on the rise, what do we know about the hospitals that are vulnerable to these attacks? A study in The American Journal of Managed Care took on this question, and found that while the network attacks in the headlines do affect millions of people, a more mundane problem – improper disposal or theft of paper records and patient films – happens more often, though fewer people are affected in each case. Source: https://www.helpnetsecurity.com/2018/02/20/hospitals-experience-data-breaches/

Threat Landscape

Leaked NSA Exploits Can Now Hack Any Windows Version – Exploits that were stolen from the NSA last year and which were believed to target older Windows releases have been tweaked to potentially impact all versions of Microsoft's operating system back to Windows 2000. Source: http://news.softpedia.com/news/leaked-nsa-exploits-can-now-hack-any-windows-version-519696.shtml

2017 was 'worst year ever' in data breaches and cyberattacks, thanks to ransomware. Businesses beware: Cyberattacks targeting businesses nearly doubled in the past year, from 82,000 in 2016 to 159,700 in 2017, according to a Thursday report from the Online Trust Alliance (OTA). And since the majority of cyberattacks are never reported, the actual number of incidents in 2017 could in fact be over 350,000, the report noted. This further highlights the need for enterprises to implement proper cyber hygiene practices and employee training to keep critical business systems and data secure. Source: https://www.techrepublic.com/article/2017-was-worst-year-ever-in-data-breaches-and-cyberattacks-thanks-to-ransomware/

Here's why the epidemic of malicious ads grew so much worse last year. Last year brought a surge of sketchy online ads to the Internet that tried to trick viewers into installing malicious software. Even credit reporting service Equifax was caught redirecting its website visitors to a fake Flash installer just a few

weeks after reports of a data breach affecting as many as 145.5 million US consumers. Now, researchers have uncovered one of the forces driving that spike—a consortium of 28 fake ad agencies. The consortium displayed an estimated 1 billion ad impressions last year that pushed malicious antivirus software, tech support scams, and other fraudulent schemes. By carefully developing relationships with legitimate ad platforms, the ads reached 62 percent of the Internet's ad-monetized websites on a weekly basis, researchers from security firm Confiant reported in a report published Tuesday. Source: https://arstechnica.com/information-technology/2018/01/malvertising-factory-with-28-fake-agencies-delivered-1-billion-ads-in-2017/

Recommended Actions to take

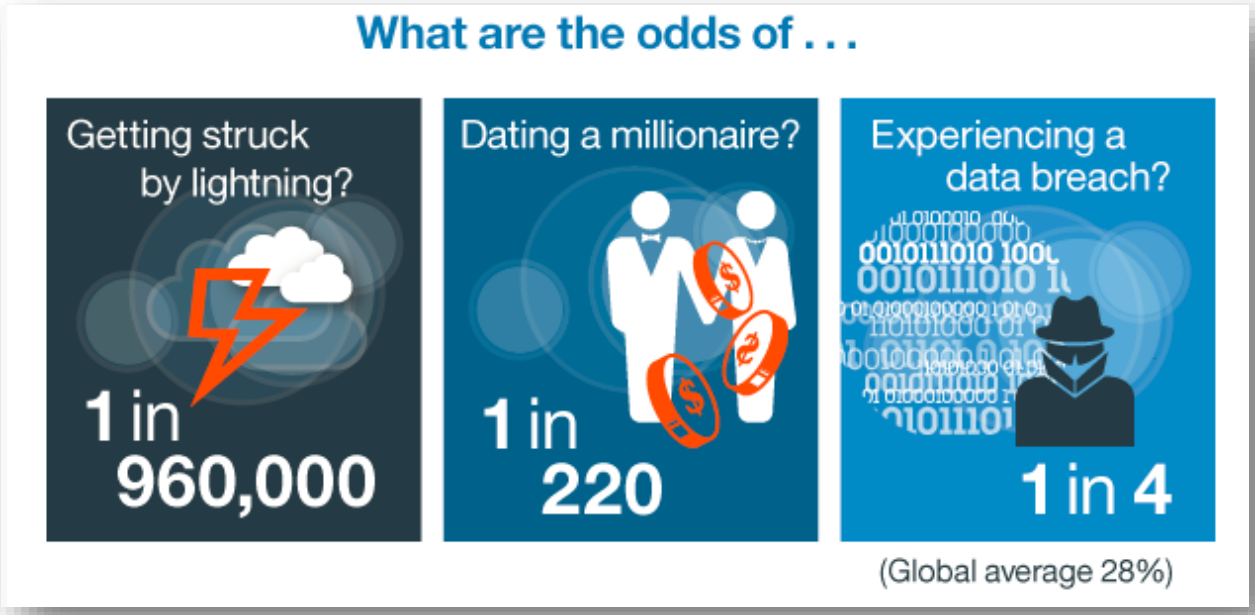
The following set of recommendations is based on the information provided above in the brief. For a more detailed set of recommendations, as well as vulnerabilities and indicators of compromise, please refer to Accume's weekly threat intelligence briefings.

- Ensure that your institution is aware of its requirements under GDPR and that it is taking the necessary steps for compliance if necessary.
- Ensure that your web filtering system can be dynamically updated against current threats
- Keep anti-virus systems up to date.
- Ensure that SMB is running and properly patched in your environment.
- Inform your employees about the risks associated with SIM Hijacking, especially if you use your mobile devices for multi-factor authentication.
- Make sure that your website gets tested regularly as a component of your external penetration testing.
- Explore the use of password management software for users such as "Last Pass" to assist with password security.
- Make sure that your incident response playbook is updated regularly to address the latest threats.

If you have questions about any of the above recommendations, or about their implementation, feel free to reach out to Accume for additional information.

If you found this information valuable, we recommend our weekly threat intelligence brief, which has additional operational details for you and your staff. For more information, contact us here.

According to the 2017 Verizon Data Breach Report, 62% of data breaches featured hacking. Ponemon's 2017 Cost of Data Breach Study estimates the cost of a data breach at $245.00 per exposed record.



Considering the odds, is your institution prepared to properly respond to [security incidents](#)? Accume can help!