[+] (IN)SECUREMagazine

Issue 55, 09/2017

AI FOR CYBERSECURITY: PROMISES AND LIMITATIONS

WHY END-TO-END ENCRYPTION IS ABOUT MORE THAN JUST PRIVACY

BUILDING A SUCCESSFUL INFORMATION SECURITY MONITORING PROGRAM

DESIGNING SECURITY POLICIES TO FIT YOUR ORGANIZATION'S NEEDS

TABLE OF CONTENTS

(IN)SECURE Magazine 55
CONTRIBUTORS LIST

- **Anton Goncharov**, CTO at Gemini Data
- **Kevin Magee**, Global Security Strategist at Gigamon
- **Aaron McKeown**, Head of Security Engineering and Architecture at Xero
- **Kumar Saurabh**, CEO at LogicHub
- **Mike Shultz**, CEO at Cybernance
- **Rush Taggart**, CSO at CardConnect.

Visit the magazine website at www.insecuremag.com

Feedback and contributions: Mirko Zorz, Editor in Chief - mzorz@helpnetsecurity.com

News: Zeljka Zorz, Managing Editor - zzorz@helpnetsecurity.com

Marketing: Berislav Kucan, Director of Operations - bkucan@helpnetsecurity.com

Security world

Organizations struggle to maximize the value of threat intelligence

Amidst growing concerns of large-scale cyber attacks, 84 percent of organizations participating in a Ponemon Institute survey indicated threat intelligence is “essential to a strong security posture.” However, many organizations struggle with an overwhelming amount of threat data and lack of staff expertise, which diminish the effectiveness of their threat intelligence programs.

Threat sharing remains a key priority for organizations, half of which report participating in sharing communities, but a majority of these organizations (60 percent) only receive community intelligence and do not contribute.

Key findings:

- 80 percent of North American organizations are currently using threat intelligence as a part of their cybersecurity program, up from 65 percent in 2016
- 86 percent of respondents indicate threat intelligence is valuable to their security mission, up from 77 percent the previous year
- 83 percent of North American respondents indicate a Threat Intelligence Platform (TIP) is necessary to maximize the value of intelligence data.

The Ponemon report revealed that despite overall improvement in threat intelligence usage, threat data overload continues to plague organizations.

Sixty-nine percent of respondents indicated that threat intelligence is too voluminous and complex to provide actionable intelligence. Other respondents cited difficulty in the integration of threat intelligence platforms with other security technologies and tools (64 percent), and a lack of alignment between analyst activities and operational security events (52 percent).

Additionally, 71 percent of organizations fail to keep more than three months of historical event logs online, posing a significant challenge in identifying existing threats within the organization.

User-targeted threats at all-time high despite rising education spend

The cost of security education for large enterprises is at an all-time-high of $290,033 per year per organization, and user education is rocketing up the CIOs' priority list. Yet despite those investments, the end user remains the greatest risk to the organization's security from targeted zero-day and nation state threats to common ransomware and phishing attacks, according to a survey conducted by Vanson Bourne.

The research is based on a survey of 500 CIOs from large enterprises in the US (200), UK (200) and Germany (100). Key findings include:

- 99% of CIOs see users as "the last line of defence" against hackers. This means the burden of securing the enterprise has shifted to user education and often stringent policies and procedures that limit teams' ability to get work done and puts a tremendous amount of personal responsibility on the end user.
- Based on an average of seven hours of cybersecurity training per employee, large enterprises waste $290,000 per year.
- Skilled employees in HR, Legal, IT and Risk spend an additional 276 hours a year helping to arrange and deliver in-house training.
- Most businesses (90%) have used external consultants for over 3 days (27 hours) a year to review and advise on security policies and procedures.
- 94% of CIOs have pushed for increased investment in user education following recent headlines around phishing and ransomware.

European Commission wants ENISA to introduce EU-wide cybersecurity certification scheme

"Cyber security attacks know no borders and no one is immune," European Commission President Jean-Claude Juncker noted in his recent State of the Union Speech. He also said they can be more dangerous to the stability of democracies and economies than guns and tanks.

With that in mind, the European Union needs a strong cybersecurity agency, and the Commission has submitted a proposal for a regulation aimed at strengthening the role of ENISA, the Union's Greece-based Agency for Network and Information Security.

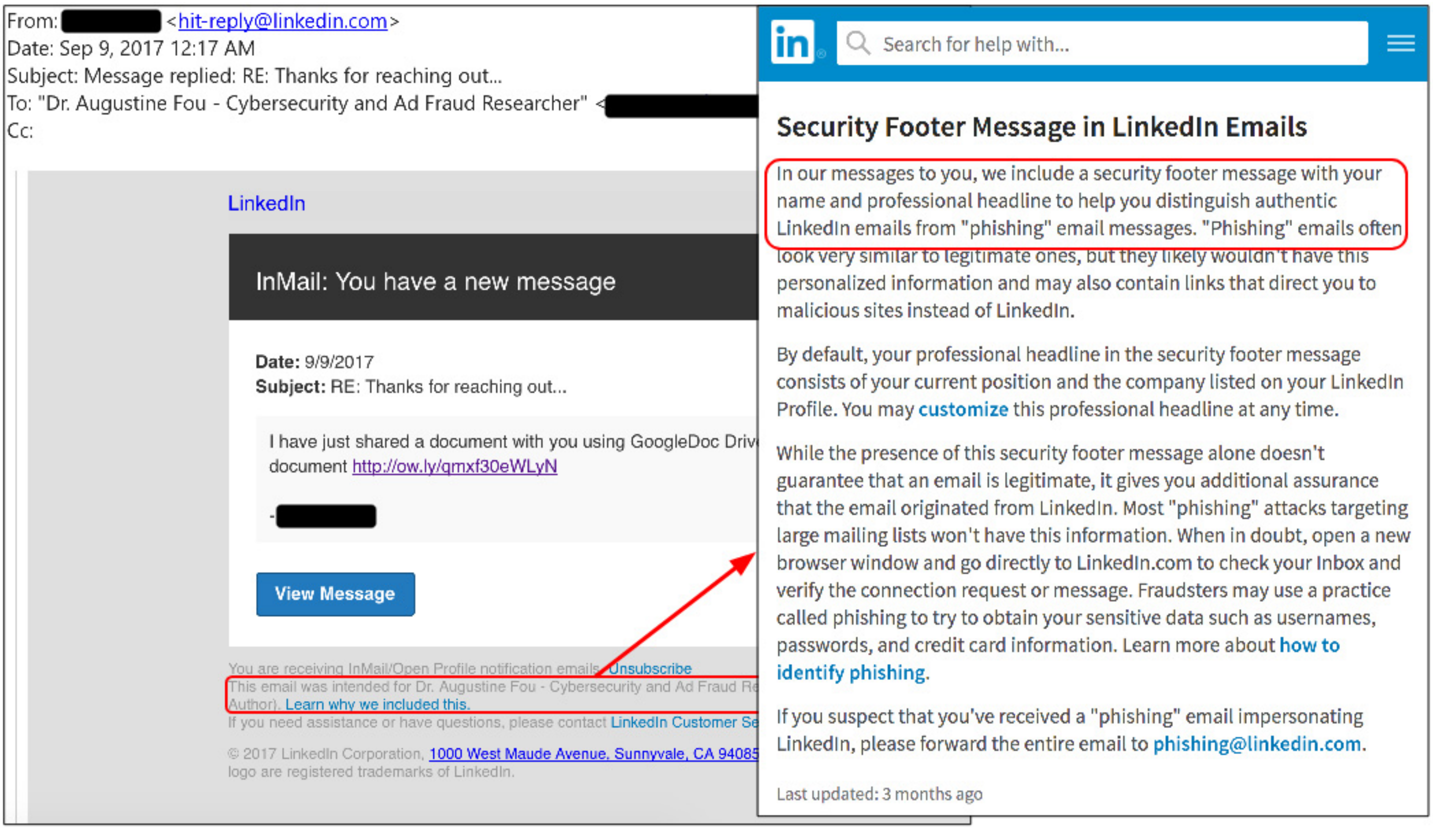
Under the new proposal, ENISA would be tasked with drafting certification rules that will apply to information and communications technology products across the EU.

"The general purpose of a European cybersecurity certification scheme is to attest that the ICT products and services that have been certified in accordance with such scheme comply with specified cybersecurity requirements. This for instance would include their ability to protect data (whether stored, transmitted or otherwise processed) against accidental or unauthorised storage, processing, access, disclosure, destruction, accidental loss or alteration," the proposal states.

"EU cybersecurity certification schemes would make use of existing standards in relation to the technical requirements and evaluation procedures that the products need to comply with and would not develop the technical standards themselves. For instance, an EU-wide certification for products such as smart cards, which are currently tested against international CC standards under the multilateral SOG-IS scheme, would mean making this scheme valid throughout the EU."

Such a EU-wide certification scheme will result in similar national ones ceasing to apply. The goal is to unify the effort, and make it so that companies don't have to be certified individually in each member state (with different testing methodologies, cybersecurity certification procedures, and on different technical requirements).

But, as certification can be a very expensive process and could, therefore, result in higher product/service prices, cybersecurity certification will remain voluntary.



From: [redacted] <hit-reply@linkedin.com>
Date: Sep 9, 2017 12:17 AM
Subject: Message replied: RE: Thanks for reaching out...
To: "Dr. Augustine Fou - Cybersecurity and Ad Fraud Researcher" <[redacted]
Cc:

LinkedIn

InMail: You have a new message

Date: 9/9/2017
Subject: RE: Thanks for reaching out...

I have just shared a document with you using GoogleDoc Driv
document http://ow.ly/qmxf30eWLyN

-[redacted]

You are receiving InMail/Open Profile notification emails. Unsubscribe
This email was intended for Dr. Augustine Fou - Cybersecurity and Ad Fraud Re
Author). Learn why we included this.
If you need assistance or have questions, please contact LinkedIn Customer Se

© 2017 LinkedIn Corporation, 1000 West Maude Avenue, Sunnyvale, CA 94085
logo are registered trademarks of LinkedIn.

Security Footer Message in LinkedIn Emails

In our messages to you, we include a security footer message with your name and professional headline to help you distinguish authentic LinkedIn emails from "phishing" email messages. "Phishing" emails often look very similar to legitimate ones, but they likely wouldn't have this personalized information and may also contain links that direct you to malicious sites instead of LinkedIn.

By default, your professional headline in the security footer message consists of your current position and the company listed on your LinkedIn Profile. You may customize this professional headline at any time.

While the presence of this security footer message alone doesn't guarantee that an email is legitimate, it gives you additional assurance that the email originated from LinkedIn. Most "phishing" attacks targeting large mailing lists won't have this information. When in doubt, open a new browser window and go directly to LinkedIn.com to check your Inbox and verify the connection request or message. Fraudsters may use a practice called phishing to try to obtain your sensitive data such as usernames, passwords, and credit card information. Learn more about how to identify phishing.

If you suspect that you've received a "phishing" email impersonating LinkedIn, please forward the entire email to phishing@linkedin.com.

Last updated: 3 months ago

Phishers targeting LinkedIn users via hijacked accounts

A new phishing campaign has been spotted hitting LinkedIn users via direct messages and the LinkedIn InMail feature.

They are sent from legitimate LinkedIn Premium accounts that have been hijacked, thus increasing the likelihood that recipients will trust the message and click on the link.

The messages/emails say that the sender has just shared with the recipient a document via GoogleDoc/Drive, and offers a shortened Ow.ly link to view it.

When sent through the InMail feature, which allows members with Premium accounts to contact LinkedIn users with whom they have no connection, they look pretty legitimate. Technically they are – LinkedIn is the one doing the sending, and they are sent from a legitimate account. It is just that the content cannot be trusted.

The link in the message redirects the victims to a web page that requires users to enter their Gmail, Yahoo or AOL login credentials and their phone number in order to access the document – a decoy Wells Fargo document hosted on Google Docs.

“We do not know how (malware, other phishing attacks, etc.) or how many LinkedIn accounts were compromised in this campaign,” Malwarebytes researcher Jerome Segura noted.

“It’s also unclear whether the shortened URLs are unique per hacked account or not, although we think they might be. The user whose account was hacked had over 500 connections on LinkedIn and based on Hootsuite‘s stats, we know 256 people clicked on the phishing link.”

But there is no way of knowing whether they followed through the process and entered their credentials in the phishing page.

Segura pointed out that this kind of attack via social media is not new, but it’s effective and difficult to block.

“If your LinkedIn account gets compromised, you should immediately review its settings to change your password and enable two-step verification,” he advises.

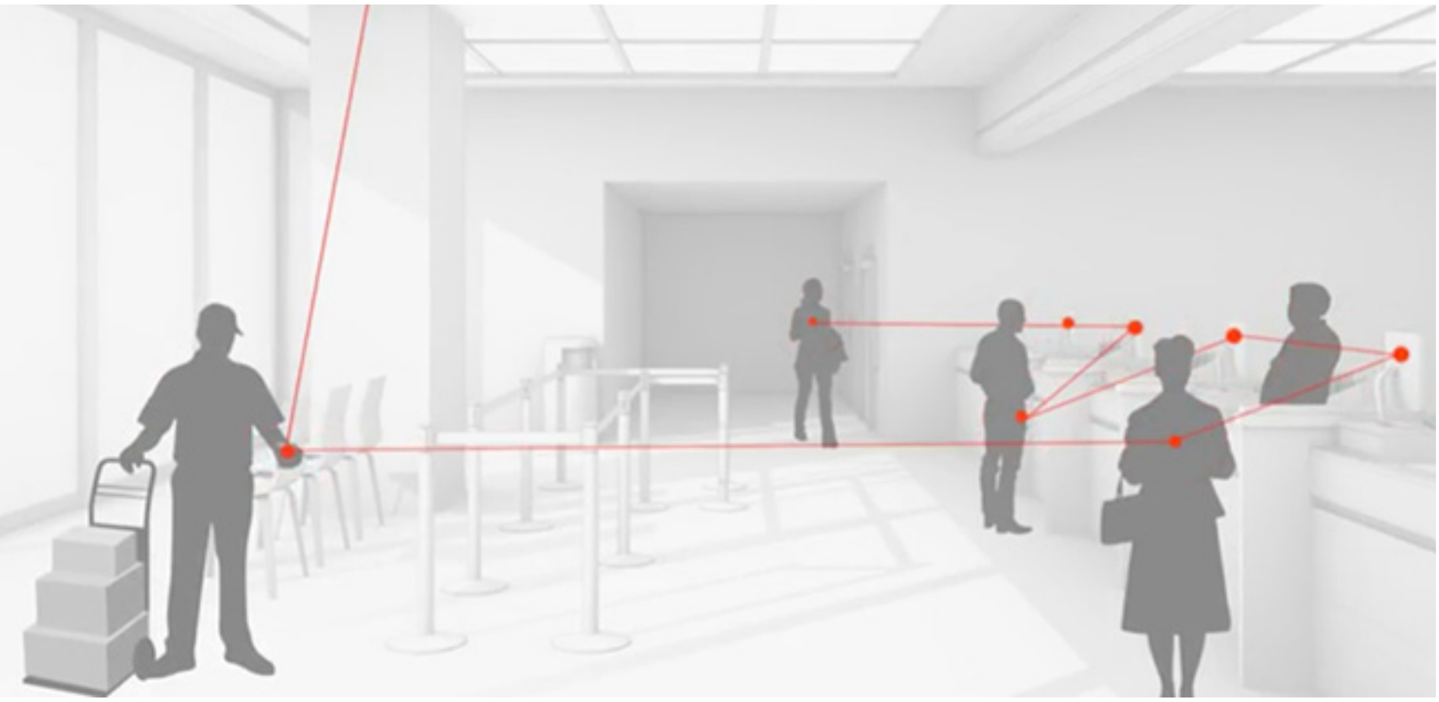
Billions of Bluetooth-enabled devices vulnerable to new airborne attacks

Eight zero-day vulnerabilities affecting the Android, Windows, Linux and iOS implementations of Bluetooth can be exploited by attackers to extract information from, execute malicious code on, or perform a MitM attack against vulnerable devices.

The vulnerabilities, collectively dubbed BlueBorne by the researchers who discovered them, can be exploited without users having to click on a link or download a questionable file. In fact, no action by the user is required to perform the attack. Also, attacks exploiting them spread through the air, so it's difficult to detect them and are highly contagious. Users will also not be able to detect whether they are being hit with a BlueBorne attack.

The only prerequisite for a successful attack is that Bluetooth, a widely used wireless communication protocol for exchanging data over short distances, is enabled on a target device. Unfortunately, it is often enabled by default on too many devices.

"Unlike the common misconception, Bluetooth enabled devices are constantly searching for incoming connections from any devices, and not only those they have been paired with," the researchers explained. "This means a Bluetooth connection can be established without pairing the devices at all. This makes BlueBorne one of the most broad potential attacks found in recent years, and allows an attacker to strike completely undetected."

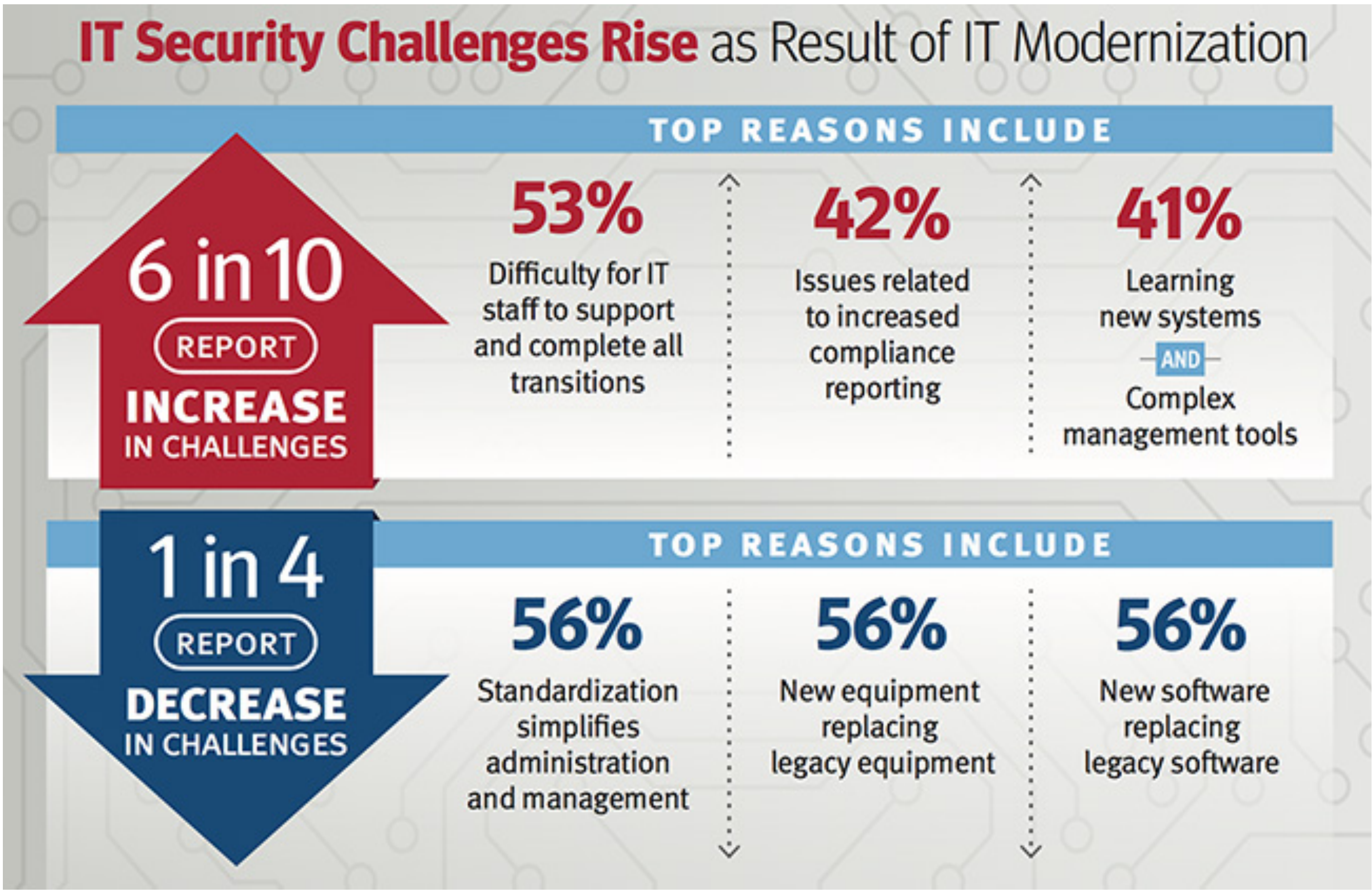


Most infosec pros believe election hacks are acts of cyber war

IT security professionals believe the effects of cyber attacks on elections go beyond diminishing confidence in the democratic process, according to a recent Venafi survey.

Seventy-eight percent said they would consider it an act of cyber war if a nation-state was found to have hacked, or attempted to hack, another country's election.

"The definition of an act of war is an action by one country against another which is an immediate threat to peace," said Jeff Hudson, CEO of Venafi. "An attempt at election hacking could easily be considered an act of cyber war. The intent is to undermine the foundation of government, which is responsible for protecting the country. Elections are being targeted by cyber attacks, and the potential repercussions of election hacking cannot be understated. Malicious actors have the ability to alter voting databases, delay vote counts and subvert trust in the election process."



IT Security Challenges Rise as Result of IT Modernization

6 in 10 REPORT INCREASE IN CHALLENGES

TOP REASONS INCLUDE

53% Difficulty for IT staff to support and complete all transitions

42% Issues related to increased compliance reporting

41% Learning new systems AND Complex management tools

1 in 4 REPORT DECREASE IN CHALLENGES

TOP REASONS INCLUDE

56% Standardization simplifies administration and management

56% New equipment replacing legacy equipment

56% New software replacing legacy software

Do IT modernization efforts increase security challenges?

Most government IT executives believe that IT modernization projects increase security challenges as opposed to alleviate them, according to a new study from Unisys. A large percentage of respondents to the study also reported concern about the excessive length of the procurement process and effectiveness of regulatory mandates – which they said lead to a “check-the-box” approach to compliance.

While nearly two-thirds of respondents (62 percent) rated cybersecurity as the top priority for agency modernization projects over the next year, nearly the same percentage (59 percent) reported that they think their agency’s IT modernization efforts have resulted in an increase in the IT security challenges they face. And when asked to grade their agencies’ modernization efforts, 43 percent graded those efforts at “satisfactory” or lower when it comes to improving cybersecurity.

“The results of this survey tell us that many federal agencies may not have adequate staff and resources to manage security challenges in today’s more complex and modernized IT environments, which in our view explains the feedback about modernization efforts exacerbating security challenges,” said Venkatapathi “PV” Puvvada, president of Unisys Federal. “To achieve successful digital transformation, agencies must make security a priority and embark on projects that enhance security at the core, as well as boost operational efficiency to meet mission-critical goals.”

The survey asked respondents about a broad range of facets of IT modernization and asked them to rate their agencies’ performance. When presented with a list of process and technology factors of modernization projects, only 10-16 percent of respondents graded their agencies with the top grade of “A” in any area.

Despite reporting that modernization makes security more challenging, cybersecurity was one of the areas graded highest by respondents, with 57 percent grading their agencies’ efforts as “A” or “B.” They were less generous when rating their agencies’ on technologies like “streamlined systems development” and “leveraging the cloud,” with 36 percent and 34 percent respectively, grading those efforts as “A” or “B.”

Samsung offers up to $200,000 for bugs in its devices, services

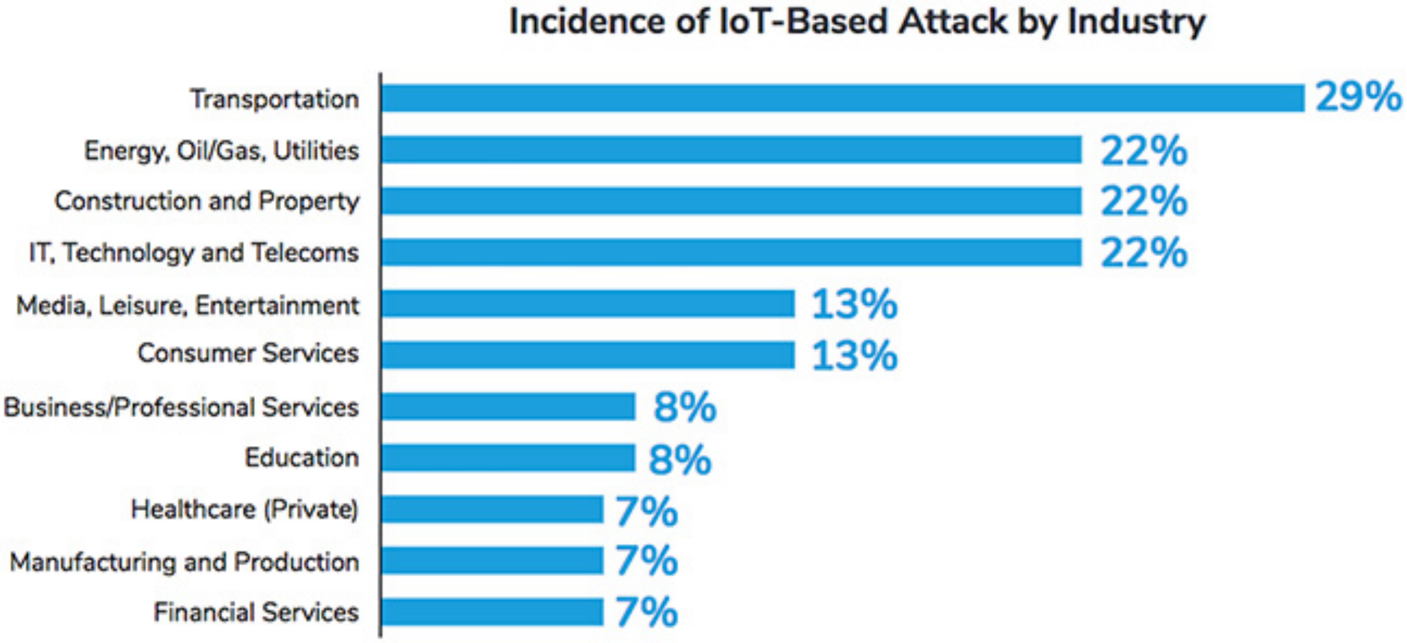
South Korean giant Samsung Electronics is now offering bounties for reported bugs in its mobile devices, software and services.

"The rewards program kicked off with a pilot in January 2016 to ensure an efficient and productive public introduction to the broader security community," the company explained. "Samsung's Mobile Security Rewards program is the latest initiative to demonstrate the company's steadfast commitment to enabling secure experiences for all its customers."

Researchers are instructed to search for vulnerabilities in:

- Active Samsung Mobile services, including Bixby, Samsung Account, Samsung Pay and Samsung Pass
- All Samsung mobile devices currently receiving monthly and quarterly security updates (Galaxy S, Galaxy Note, Galaxy A, Galaxy J, and Galaxy Tab series of devices)
- Applications developed and signed by Samsung Mobile, as well as third party applications specific to Samsung Mobile devices, applications or services.

"Depending on the severity level of the vulnerability, the rewards amount will range between USD $200 and USD $200,000 for qualified reports," the company noted, and pointed out that smaller rewards will be given for reports that don't include valid Proof-of-Concept, and no reward will be given to reports with no security impact.



13% of SMBs have experienced an IoT-based attack

One in four companies have already experienced a ransomware attack and one in eight have dealt with an IoT-based attack, according to Arctic Wolf Networks.

As mid-market companies continue to embrace IoT without implementing the necessary security tools, these attacks and vulnerabilities will persist. Despite the lack of precautionary measures, organizations are well aware of the threat, with over 70 percent of respondents expressing concern about an IoT-based ransomware attack.

"The next chapter in the story will raise the stakes with possible attacks on medical devices, electric grids and transportation systems, which could cause the loss of life," said Brian NeSmith, CEO of Arctic Wolf Networks. "Companies not spending millions of dollars on security will be at a severe disadvantage fending off criminals who are organized, well-funded and very sophisticated in their methods."

Security flaw affects 750,000 Estonian ID cards

An international group of cryptographers has flagged a serious security vulnerability in the chip embedded in Estonian ID cards, the country's Information System Authority has announced.

"Estonian experts assess there to be a possible security vulnerability and we will continue to verify the claims of the researchers," said Taimar Peterkop, Director-General of the agency. "We have developed the primary solutions to mitigate the risk, and will do our utmost to ensure that the security of the ID-card."

The vulnerability likely affects almost 750,000 ID cards issued starting from October 2014 (including cards issued to e-residents). ID cards issued before October 16, 2014, use a different chip and are not vulnerable.

"Theoretically, the reported vulnerability could facilitate the use the digital identity for personal identification and digital signing without having the physical card and relevant PIN codes. However, knowing the public key of the certificate is not enough to unlock the card – powerful and expensive computing power to calculate the secret key and special custom-made software for signing are also needed. The ID card software is not suitable because it requires an ID card to be placed in the card reader," the agency explained.

"The reported vulnerability is significant due to the increase in computing power in recent years. A few years ago, exploiting such a vulnerability would have been significantly more expensive and thus more unlikely than it was today."

Exploitation is still extremely difficult and not cheap, and the associated risk is still theoretical, the agency noted. "We do not know any cases where an attempt has succeeded," they added.

Hackers stole contact info of 6 million Instagram users and are selling it online

Instagram pushed out a patch for a bug in the service's API that allowed attackers to discover users' email address and/or phone number.

Kaspersky Lab researchers, who found the flaw and shared information about it with Instagram, said that while the attack process is relatively simple, it takes time and effort to pull off.

"Using the outdated application the attacker selects the reset password option and captures the request using a web proxy. They then select a victim and send a request to Instagram's server carrying the target's unique identifier or username. The server returns a JSON response with the victim's personal information including sensitive data such as email and phone number," they explained.

"The attacks are quite labor intensive: each one has to be done manually since Instagram uses mathematical calculations to prevent attackers from automating the request form."

Researchers reverse 320 million hashed passwords

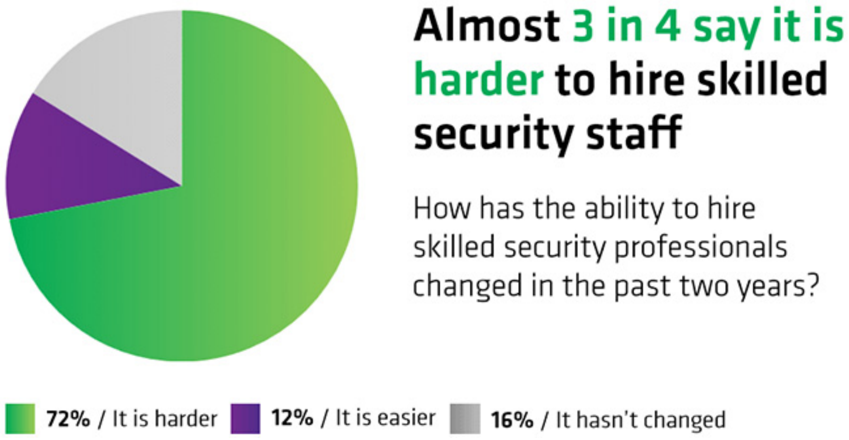
CynoSure Prime, a “password research collective”, has reversed the hashes of nearly 320 million hashed passwords provided by security researcher Troy Hunt through the Pwned Passwords searchable online database.

Their effort, pulled off with the help of two other researchers, revealed many things:

- Interesting statistics regarding these real world passwords exposed in data breaches
- The fact that this database also contains some 2.5 million email addresses and 230,000 email/password combinations (Hunt intends to purge that data from the database)
- Some bugs in the Hashcat password recovery tool.

“The longest password we found was 400 characters, while the shortest was only 3 characters long. About 0.06% of passwords were 50 characters or longer with 96.67% of passwords being 16 characters or less,” the collective shared.

“Roughly 87.3% of passwords fall into the character set of LowerNum 47.5%, LowerCase 24.75%, Num 8.15%, and MixedNum 6.89% respectively. In addition we saw UTF-8 encoded passwords along with passes containing control characters.”



Almost 3 in 4 say it is harder to hire skilled security staff

How has the ability to hire skilled security professionals changed in the past two years?

Skilled security staff are hard to find, security teams need to be creative

A study conducted in July by Dimensional Research examined how organizations are addressing the cybersecurity skills gap. Study respondents included 315 IT security professionals at U.S.-based companies with more than 100 employees.

According to the study, 93 percent of security professionals are concerned about the cybersecurity skills gap, and 72 percent believe it is more difficult to hire skilled security staff to defend against today’s complex cyberattacks compared to two years ago. Significantly, 81 percent believe that the skills required to be a great security professional have changed in the past few years. Twenty percent of respondents said their organizations had hired people with expertise not specific to security over the past two years, and another 17 percent stated they plan to do the same in the next two years. Additionally, the study found that 50 percent plan to invest more heavily in training their existing staff to help with the looming skills shortage.

“It’s evident that security teams are evolving and maturing with the rest of the cybersecurity industry, but the pool of skilled staff and training simply aren’t keeping up,” said Tim Erlin, vice president of product management and strategy at Tripwire. “For example, beyond their technical duties, security practitioners may now be expected to spend more time in boardrooms or in the CFO’s office to secure more budget. While the makeup of the cybersecurity workforce may be changing, the fundamentals of protecting an organization have not. It will be critical during this transition to ensure there’s a long-term strategy in place around maintaining their foundational security controls.”

Android unlock patterns are a boon for shoulder surfing attackers

The "swiping" unlock patterns typical for Android devices are considerably easier for attackers to discern than PIN combinations.

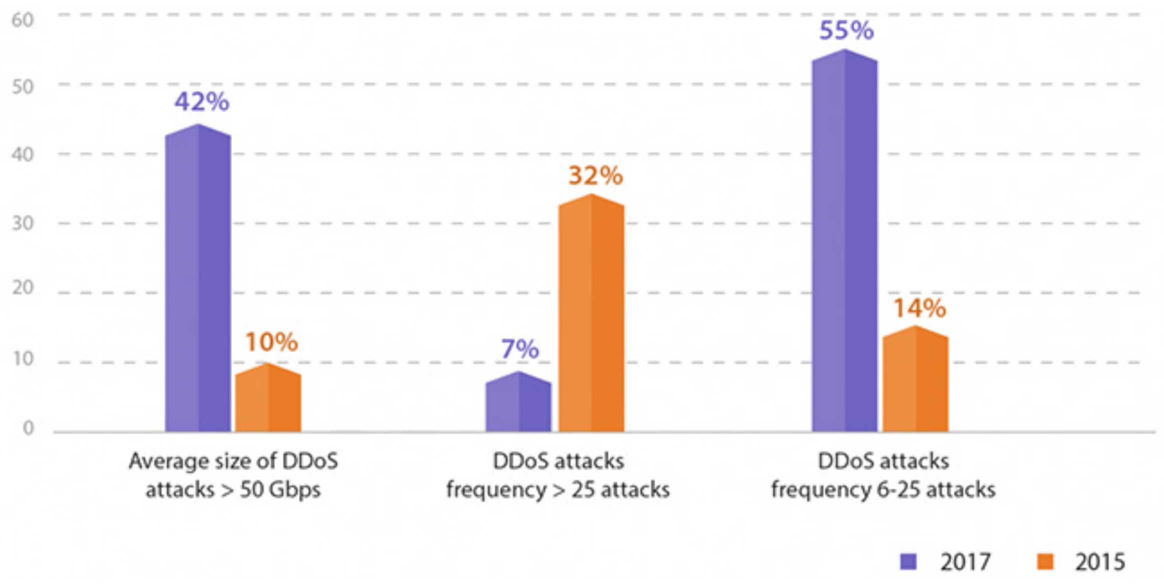
In fact, after only one observation of a user entering the pattern, 64% of shoulder surfing attackers will be able to reproduce it, a group of researchers from the US Naval Academy and the University of Maryland Baltimore County has found.

In comparison, only one in ten attackers could make out a six-digit PIN after one viewing.

The researchers tested the security of PIN/pattern mobile authentication schemes by showing videos of users unlocking different phones to 1,173 subjects recruited via Amazon Mechanical Turk. Then, to confirm the validity of the results, they later recruited 91 participants from their institutions. The unlocking was recorded from different angles and distances. The participants were asked to view a video of an authentication, then to attempt to recreate it.

"Analyzing the results, we find that in all settings, Android's graphical pattern unlock is the most vulnerable, especially when feedback lines are visible; a single observation successfully attacked the pattern 64.2% of the time with 79.9% for multiple observations of a 6-length pattern. Shorter patterns were even more vulnerable," the researchers noted.

"Removing feedback lines during the pattern entry improved the security, finding 35.3% successful attacks with a single view and 52.1% success with multiple views for 6-length patterns. PINs, however, proved much more elusive to attack than anticipated. A single observation was sufficient to attack just 10.8% of the 6-digit PINs, degrading to 26.5% after two observations."

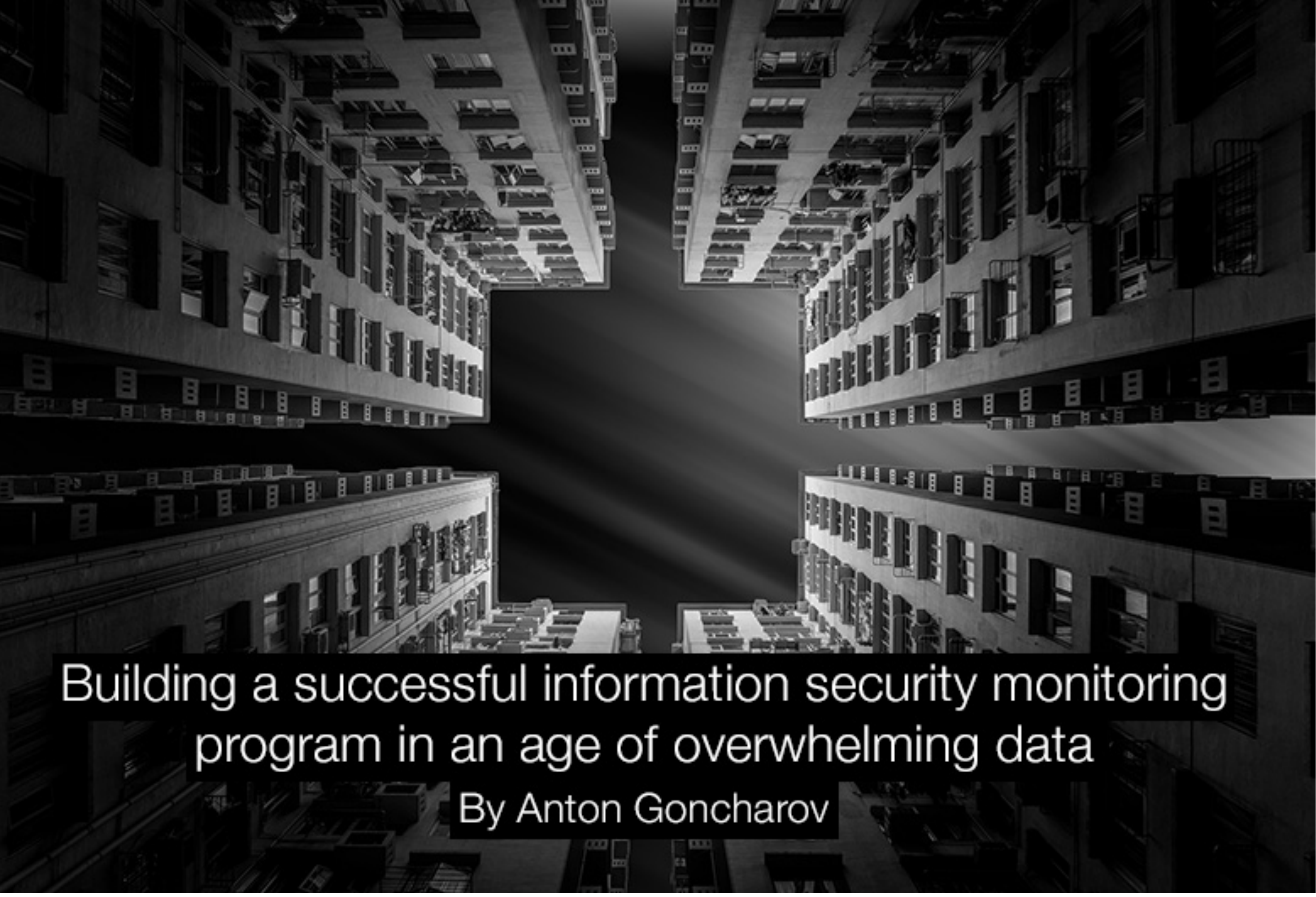


Large DDoS attacks over 50 Gbps have quadrupled between 2015 and 2017

Organizations are experiencing an increase in the magnitude of DDoS attacks, with the average size of attacks over 50 Gbps quadrupling in just two years, according to A10 Networks.

The study also found the gargantuan 1 Tbps attacks that started last year with the Mirai botnet have begun to leave their mark, with 42% of organizations reporting an average size of DDoS attacks greater than 50 Gbps, a significant increase from 2015, when only 10% of attacks were above that size.

Multi-vector DDoS attacks continue to increase and assault networks and applications at a rapid pace, according to the report, which found the percentage of organizations that experienced between 6 to 25 attacks per year has increased from 14% in 2015 to 57% in 2017.



Building a successful information security monitoring program in an age of overwhelming data

By Anton Goncharov

The majority of security analysts I know have a job that's made unnecessarily more difficult than it has to be. Everyday they're charged with finding the veritable needle in a haystack with tools – SIEMs and log management systems – that have struggled with the latest technology trends, such as big data and cloud services. As a result, analysts are wasting time with high volumes of low-value data, and they're missing valuable clues.

It's time to revisit our approach to information security monitoring. In an attempt to bring some sanity back to our industry, we must take a step back and consider what exactly we need to achieve when it comes to information security monitoring and response.

With security information management solutions fulfilling an important but limited need, organizations have invested in tools that focus on specific problems. This has led to a proliferation of point solutions both within security organizations and in the market at large. But information security monitoring isn't about tools – it's about capabilities.

Once we understand the capabilities we need, then we can consider the most effective ways of addressing them as part of a capability-driven architecture. The features and functionality should transcend the technology, instead focusing on enabling your preparedness to deal with the unknown and closing the gaps in your security coverage as efficiently as possible.

A word of warning before we dive into the details: trying to shortcut through these phases is a recipe for pain. For example, back in the day, intrusion prevention systems (IPS) could block a legitimate, business critical application without proper analysis because it behaved in a way the IPS didn't expect. Similarly, automation tools today may launch remediation jobs based on a false positive alert generated by a SIEM or other security tool.

Even assuming your alerts are 100% accurate (I know, just go with me here), trusting remediation efforts to an automated system without first determining a complete kill chain is certain to put members of your team in the hot seat.

That said, let's look at the information security monitoring framework and the capabilities needed in each phase.

Detection

Objective: Identify activity that may be indicative of malicious intent and/or has bypassed your preventive controls.

There are a ton of threat detection tools on the market, from inline network malware detection to end-point protection. You should pick the ones you like the most, with a couple of caveats.

Beware of kits that claim to boil the ocean. A detection tool is only as accurate as the environment in which it operates. This is very important. While an endpoint-based detection tool may have direct access to all the core aspects of a system, including file system and memory, it has no insight, for instance, into enterprise network transactions beyond the host. It would also do a poor job of understanding activity at the application or database-transaction level. This is why detection is one area where I give point solutions a high regard. Remember to ensure that your detection coverage is thorough across the vertical application stack, and expert-built.

Detection should take place as close to the business-critical applications and data as possible. Many of these are more commonly SaaS-based these days and likely not monitored by your organization at the moment.

Some gains in detection capabilities may extend to your Data Management solution. This is particularly relevant for monitoring hosted environments and applications that operate in areas outside of your control. Anomaly detection and machine learning tools may be helpful, but make sure the vendor's claims match the needs of your particular environments and data. The same goes for threat intelligence data feeds and alerts.

Data management

Objective: Consolidate as much information as possible about the environment in which threats and malicious activity have been discovered.

I could write volumes on what data should be collected for security monitoring. Outside of the usual suspects, like authentication, firewall, and proxy logs, think about where your critical data is stored, which applications manage that data, how access to that data is provisioned and controlled, the potential attack vectors against that data, and what type of information your incident response team needs in the event of a breach.

Ideally, activity data should be collected from every system, network, and application (the full stack) involved in managing your critical data assets. Monitoring prevention tools should be in scope as well. Your ability to understand the full context within which the preventive actions occur, as well as when preventive controls fail, is paramount to improving your security posture.

In the past, a lot of high-volume, low-value log data wasn't collected due to the performance impact and solution cost. Today, however, highly scalable, open source solutions make it possible to collect and analyze local workstation logs, database transaction logs, and application logs. In addition to these event data logs, you need contextual data, such as assets, application inventories, infrastructure configurations, etc. Script everything out or find a tool that manages the inventory well. Perform regular exports, store them in big data repositories, and correlate the data with other information in your logs.

The data you collect must be normalized and standardized. Normalization involves arranging semi-structured log data into uniform fields. The most typical candidates for field extraction are logs of certain Unix services. Fortunately, most solutions today are capable of producing log data in structured JSON or some other key/value format. The bigger concern is the standardization of data across multiple vendors and solutions. One way or another, the data must conform to the same standard.

The good news is, it doesn't matter which standard you use, so long as you use one. The Splunk "Common Information Model" (CIM) is a well-documented and viable option. There are also open standards that serve well as a reference.

The Open Data Model (ODM) from Apache Spot project is also at the top of my list. It has decent coverage of both event and contextual data structures, including contextual models for User, Endpoint, VPN, and Network. ODM provides a good foundation for open source-based security monitoring and analysis with all the benefits of big data scalability.

Analysis (including triage)

Objective: Provide security analysts with a robust environment to quickly identify false positives and conduct security incident investigations.

Alert triage requires contextual information to help reduce analysis fatigue and eliminate "zombie workflows." With an undoubtedly high volume of alerts reported by various detection tools, analysts' queues are overwhelming. Most teams only have the capacity to investigate 5-10% of daily alerts. The faster an analyst can identify a false positive, the sooner they can move on to something worthwhile.

Once analysts collect enough evidence to escalate an alert into an incident, the real work begins: reconstructing the full story of a compromise from the initial ingress point, to every lateral step, every involved system, credential, and successful data point access. The biggest challenge in this phase is ensuring sufficient interactive performance for distributed data platforms.

Analysts have a hard-enough time digging through volumes of cryptic system and application events - the last thing they should be doing is performance tuning the NoSQL backend. I can't emphasize enough the value of expert help to get your analysis environment moving blazing fast.

Other capabilities needed for the analysis phase are collaboration and knowledge retention. Every organization has "that guy" who knows everything. We need to make sure that the knowledge gleaned from analysis doesn't leave the organization when they leave. At the same time, findings should be shared with the team members.

Tips and tricks, knowledge of past incidents, indicators and attack vectors should be shared in a way that ties back to specific incidents and supplemental data to tell a complete story.

Finally, a robust security workflow framework is a must, but I'm sure you already know that.

Remediation/response

Objective: Once the first real findings of a security incident begin trickling in, close security gaps quickly and thoroughly.

For years, incident response teams have used remediation playbooks. More recently, security orchestration has become a hot market trend. Leveraging automation remediation tools is key to closing the gaps, especially during an active incident. As important as it is for response to be rapid, it's even more important that response is based on the results of a thorough investigation that completes the picture. Marking an incident as resolved while the hostile entity still has access to your network is not exactly ideal.

Conclusion

While SIEMs continue to have their place in information security monitoring environments, point solutions are proliferating almost as fast as data sources in the enterprise. But as much as our environments change due to big data and cloud services, following a capability-driven approach remains as important as ever. When you build your security monitoring program with a focus on fundamental capabilities first and technology second, your team will have everything it needs to identify, analyze, and remediate issues efficiently and effectively.

Anton Goncharov is the CTO of Gemini Data (www.geminidata.com).

AI for cybersecurity: Promises and limitations

By Kumar Saurabh

As organizations struggle with cybersecurity, one thing is clear: time is definitely on the side of the attackers. The median time for clicks across all phishing campaigns is 1 minute and 22 seconds, while the median time for breach detection is 229 days. It is simply too difficult for organizations to keep up.

High risks, complex analysis, and the need for split-second decision-making makes cybersecurity a perfect use case for Artificial Intelligence (AI).

Consider the progress AI platforms made in board and card games. In 1997, IBM Deep Blue beat reigning world chess master Garry Kasparov. More recently, Google's DeepMind beat a Go champion in Korea, and then an AI platform built at Carnegie-Mellon University beat Texas hold'em poker players. These examples demonstrate how AI capabilities increase at a rapid pace.

The promise of AI for threat detection

Can computers, enhanced with AI, detect and respond to cybersecurity threats more aptly than humans? For the moment, the answer is "not entirely."

If a human security analyst has time to study a security alert—a process that typically takes about 30 minutes—he or she will more accurately determine whether an alert has arisen from a genuine attack than an AI-powered computer will.

The challenge is that, in modern enterprises, security teams are forced to wade through thousands of alerts each day, and those alerts derive from literally billions of events recorded in Security Information and Event Management (SIEM) logs. There is no way for human analysts to keep up.

The promise of AI for cybersecurity is to scale the expertise, intelligence, and contextual understanding of an organization's top security analysts while using automation to make threat detection faster, cheaper, and more effective. Done right, this would be undoubtedly a huge boon for cybersecurity defenders.

THE NEXT BIG BREAKTHROUGH IN CYBERSECURITY AUTOMATION IS COGNITIVE AUTOMATION

This isn't a matter of AI replacing security analysts, but partnering the two so that security analysts can work more quickly and focus on incidents and situations that warrant their attention.

Making automation truly intelligent

To achieve this partnership, we may need to re-think our approach to AI.

Most AI today is heavily data-science driven and learns from processing large amounts of information. Data scientists "feed" a machine learning system with large volumes of labeled data, and this helps the system tell one thing from another (e.g., cats from dogs).

Over time, the system learns from these labels and can identify things without the labels being provided.

From a cybersecurity point of view, there are three limitations to this model.

Attacks are continuously evolving. There are no labels for zero-day powered attacks. Effective cybersecurity recognizes threats that have never been seen (or labeled) before. Furthermore, it is very difficult for organizations to produce such data sets.

The labeling approach ignores contextual information outside the data set. It's the contextual information that humans are so good at intuiting. Humans develop contextual understanding naturally, over time, through repetition - it is our everyday modus of learning. We receive an instruction, carry it out, receive feedback from a mentor or teacher, and thereby grow our understanding of the work we're doing. This contextual understanding is critical for detecting and characterizing an attack. For example, it's required for recognizing false positives and not pursuing random anomalies as though they were major threats to the enterprise.

"Black box" AI systems that develop autonomous understanding beyond simple labeling cannot explain why they are taking the actions they are taking. Without knowing why a system acted the way it did, it's nearly impossible to tune the system to make it more effective. AI cybersecurity systems need to be able to explain their actions, just as human security analysts do.

The way to address all these problems is to partner security analysts with AI platforms, so analysts can provide the feedback needed to tune and optimize platform performance. This "cognitive automation" from security analysts plays the role of a teacher or mentor by imparting their expertise to AI systems.

AI systems today can easily accelerate the rote, robotic functions of threat detection. The next big breakthrough in cybersecurity automation is cognitive automation, which helps AI systems better understand context. This way they can effectively reduce the workload of security analysts and improve the security of the enterprise overall.

Security analysts' tiers, roles in cognitive automation

In most large enterprises, there are several tiers of security analysts, playing different roles in training AI systems how to detect threats.

Tier 1 analysts perform fairly rote or robotic work and follow a playbook. They continuously monitor alert queues, monitor the health of security endpoints, and collect data for use in Tier 2 work when an alert seems serious enough to require an in-depth investigation. Automation can make them more productive, but they don't have a lot of expertise to offer the AI systems.

Tier 2 analysts perform deep-dive incident analysis by correlating data from various sources to determine whether critical systems or data sets were affected. They then advise other IT personnel on remediation and provide support for developing or implementing new analytic solutions to improve future threat detection. Unlike the mechanic work of Tier 1 analysts, Tier 2 functions require cognitive automation and the partnering of real analysts with machines to perform deep correlation of events, while also applying domain knowledge and instinct.

Most security automation systems today simply perform robotic automation, but with the increasing availability of new machine learning technologies, cognitive automation becomes more feasible. It's likely early successes with these technologies will be eagerly embraced by security analysts who feel overwhelmed with the workload of performing threat detection and attack remediation for a modern enterprise.

A Tier 3 analyst is a subject matter expert and more of a threat hunter than a threat sentry. Tier 3 analysts possess in-depth knowledge of networks, endpoints, threat intelligence, forensics and malware reverse engineering. They understand the functioning of specific applications as well as the underlying IT infrastructure. Rather than waiting for incidents to escalate, they proactively hunt for potential threats and develop, tune and implement threat detection analytics.

This type of work requires tremendous cognitive automation capabilities. No solution fully performs this type of automation today. Some vendors promise these capabilities, but their "black box" solutions don't truly replicate the contextual understanding and instinct of an expert analyst.

Looking ahead

Security threats aren't going away. Security analysts will continue to work long days, detecting and mitigating threats. Their work, however, can be streamlined and automated with the help of AI cybersecurity solutions whose analytical capabilities are refined by analysts in an ongoing educational feedback loop. By imparting contextual understanding and the wisdom of experience to these machines, security teams can scale their defensive and analytical capabilities to better withstand the security threats facing enterprises today and in the future.

Kumar Saurabh is the CEO of LogicHub (www.logichub.com).

Report: Black Hat USA 2017

By Mirko Zorz

The 20th Black Hat USA event welcomed 17,400 professionals across the InfoSec spectrum – from academics and world-class researchers to leaders in the public and private sectors. The event's record-breaking attendance signifies the growing importance of the information security sector as well as the community's need for rich and timely content.

The Black Hat Review Board, comprised of 24 security experts, evaluated more submissions this year than ever before – producing the largest program to date.

This year's conference welcomed more than 300 speakers and trainers across nearly 70 deeply technical Trainings and nearly 120 research-based Briefings on stage.

Show highlights

Alex Stamos, Facebook CSO and privacy advocate, presented "Stepping up our game: Re-focusing the security community on defense and making security work for everyone" to 7,300 attendees.

The CISO Summit welcomed 175 executives from top public and private organizations for an exclusive program intended to give CISOs and other InfoSec executives more practical insight into the latest security trends, technologies, and enterprise best practices.

The Arsenal returned for its eighth year, offering researchers and the open source community the ability to demonstrate the tools they develop and use in their daily professions. This year's event featured more than 90 tools – the largest lineup to-date.

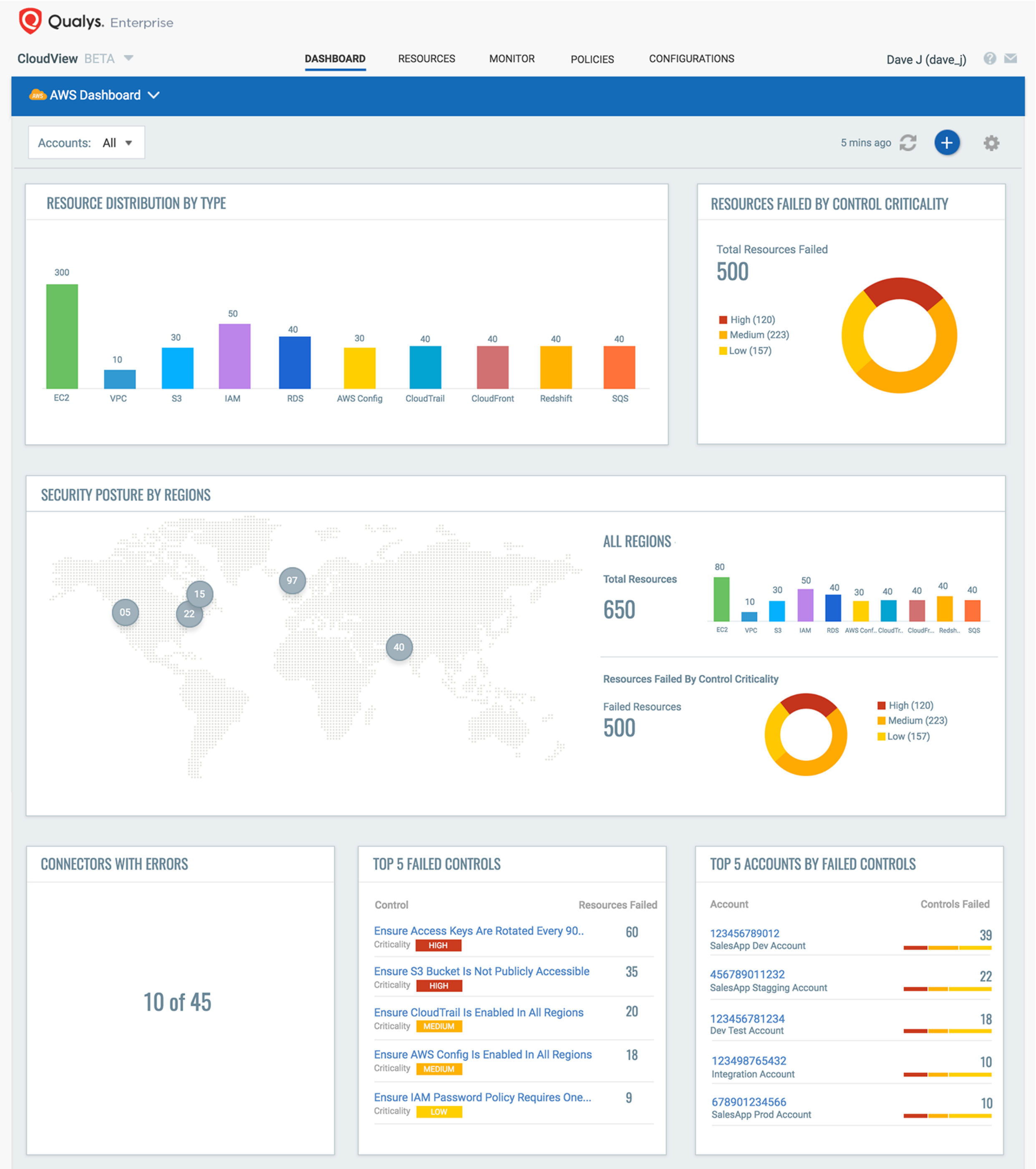
The Two-Level Business Hall was buzzing with more than 290 of the industry's leading companies showcasing their latest technologies, as well as a wide range of attendees eager to get a look at what innovations are taking the InfoSec space by storm. Both levels spanned hands on learning, education and demonstrations.

Qualys CloudView to deliver continuous security of public cloud infrastructure

Qualys announced CloudView, a new app framework in the Qualys Cloud Platform for comprehensive and continuous protection of cloud infrastructure, delivering InfoSec and DevSecOps teams a “single pane of glass” view of security and compliance across cloud infrastructures.

CloudView delivers to customers topological visibility and insight about the security and compliance posture of their complete public cloud infrastructure for major providers including Amazon Web Services (AWS), Microsoft Azure and Google Cloud. The first two apps in CloudView include Cloud Inventory (CI) and Cloud Security Assessment (CSA).

CloudView augments the existing Qualys view of host-related vulnerability, compliance and threat intelligence with a real-time inventory of all cloud services. This combination helps security teams monitor, assess and deliver reports from within the DevOps pipeline to ensure that cloud workloads throughout the Continuous Integration/Continuous Development (CI/CD) toolchain are configured in-line with Identity and Access Management, Network and Administrator access policies and regulations, thus drastically reducing exposure to attacks.

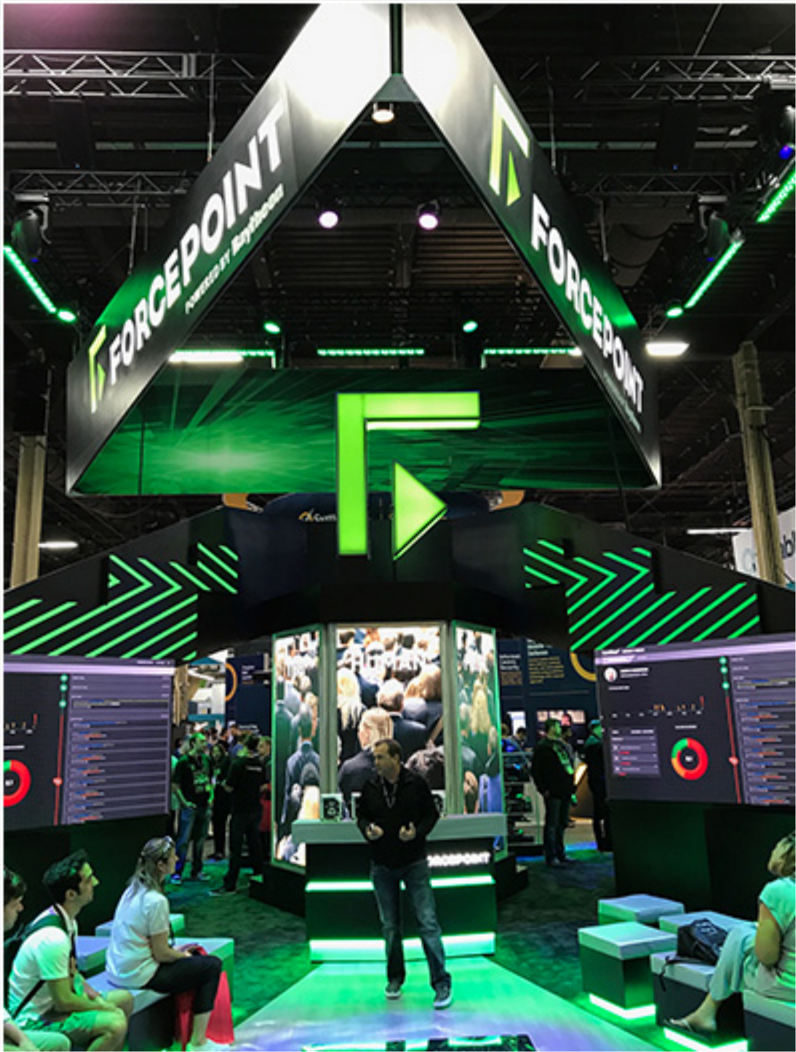


TOP 5 FAILED CONTROLS

Control	Resources Failed
Ensure Access Keys Are Rotated Every 90.. Criticality HIGH	60
Ensure S3 Bucket Is Not Publicly Accessible Criticality HIGH	35
Ensure CloudTrail Is Enabled In All Regions Criticality MEDIUM	20
Ensure AWS Config Is Enabled In All Regions Criticality MEDIUM	18
Ensure IAM Password Policy Requires One... Criticality LOW	9

TOP 5 ACCOUNTS BY FAILED CONTROLS

Account	Controls Failed
123456789012 SalesApp Dev Account	39
456789011232 SalesApp Stagging Account	22
123456781234 Dev Test Account	18
123498765432 Integration Account	10
678901234566 SalesApp Prod Account	10



You use more resource types than you account for..

In addition to the standard resources like instances, databases, and storage, you need to secure:

- IAM
- Network access
- Administrative access

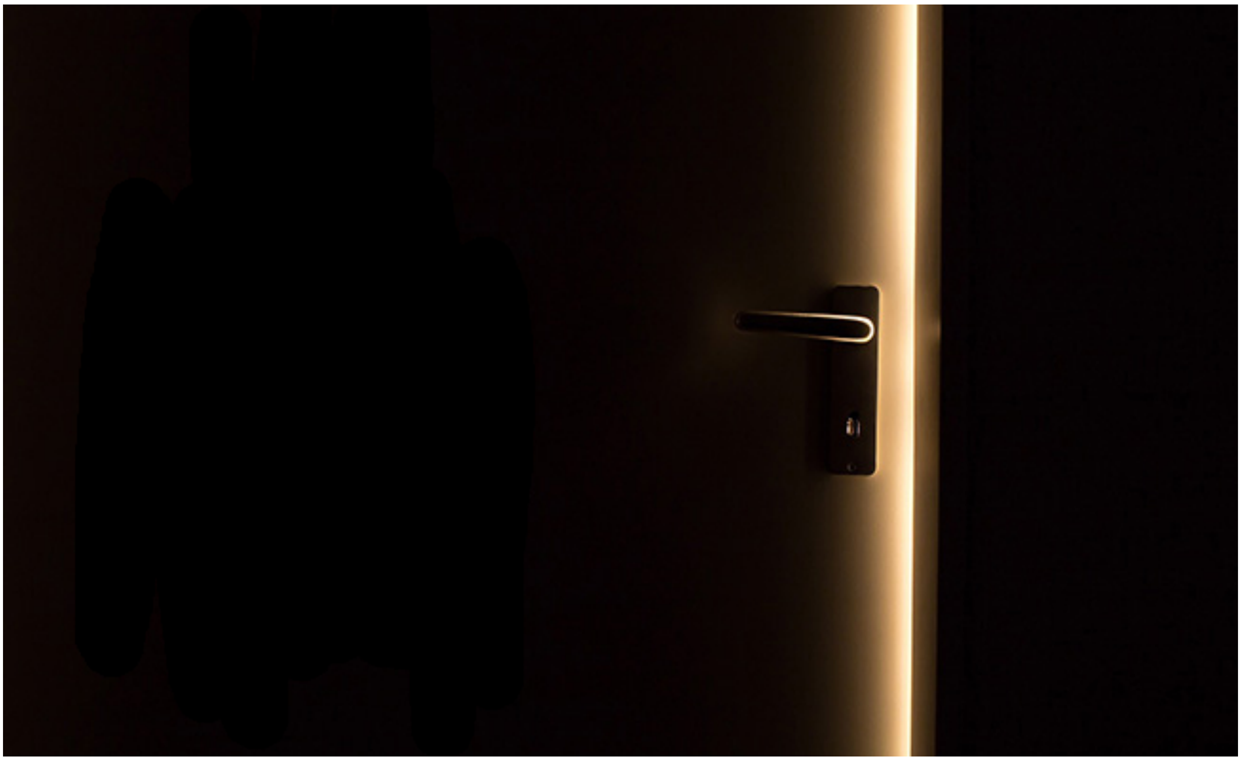
AI is key to speeding up threat detection and response

Time is the most important factor in detecting network breaches and, consequently, in containing cyber incidents and mitigating the cost of a breach.

Vectra Networks has polled 459 Black Hat attendees on the composition and effectiveness of their organizations' SOC teams. The group – a mix of security architects, researchers, network operations and data center operations specialists, CISOs and infosec VPs – were asked whether their SOCs are already using AI in some form for incident response, and 153 (33%) said Yes. The size of these teams, the time it takes them to detect and confirm a threat, and to remediate the incident and verify its containment varies. But, when comparing the time it takes SOC teams of over 10 analysts to do all those things with or without the help of AI, the former group is consistently more speedy.

"Security event investigations can last hours, and a full analysis of an advanced threat can take days, weeks or even months. Even large SOC teams with more than 10 skilled analysts find it difficult to detect, confirm, remediate, and verify security incidents in minutes and hours," says Chris Morales, Vectra Network's head of security analytics.

"However, the teams that are using AI to augment their security existing analysts and achieve greater levels automation are more effective than their peers and even SOC teams with more than 10 members who are not using AI."



How security pros look at encryption backdoors

The majority of IT security professionals believe encryption backdoors are ineffective and potentially dangerous, with 91 percent saying cybercriminals could take advantage of government-mandated encryption backdoors.

72 percent of the respondents do not believe encryption backdoors would make their nations safer from terrorists, according to a Venafi survey of 296 IT security pros, conducted at Black Hat USA 2017.

"Giving the government backdoors to encryption destroys our security and makes communications more vulnerable," said Kevin Bocek, chief security strategist for Venafi. "It's not surprising that so many security professionals are concerned about backdoors; the tech industry has been fighting against them ever since global governments first called for unrestricted access."

Hackable smart car wash systems can hurt people

Two years after researchers Billi Rios and Terry McCorkle first flagged serious vulnerabilities in automatic, smart car wash systems by US manufacturer PDQ, the company is finally acknowledging the danger.

Rios, founder of Whitescope, and researcher Jonathan Butts, founder of QED Secure Solutions, have managed to finally prove that the vulnerabilities can be exploited in a live setting (in their case, a car wash facility in Washington), and that they could lead to car damage and, more importantly, injury or loss of life of customers.

Also, their talk about the issues was accepted to Black Hat USA 2017, and the company obviously realized it could not afford to ignore them any longer.

The unearthed vulnerabilities could allow attackers to access the system's built-in web server either through the use of a rarely changed and easily guessable password, by sniffing login information as it is transmitted in unencrypted form, or by simply using an authentication bypass exploit.

Once inside, they can make the machine do all kind of nasty things: making the washing rig's doors close when it shouldn't, modifying the movements of the washing arm to hit the car or trap users inside it, and so on.

According to the researchers' findings via the Shodan IoT search engine, there are some 150 vulnerable PDQ systems online that can be fiddled with. PDQ's car wash systems are widely used in the US, but also in other countries.

Security vulnerabilities in radiation monitoring devices

IOActive researcher Ruben Santamarta has uncovered a number of cybersecurity vulnerabilities in widely deployed Radiation Monitoring Devices (RDMs), and has presented his research at Black Hat USA 2017.

RDMs are used to monitor the radiation found in critical infrastructure, such as nuclear power plants, seaports, borders, and even hospitals.

According to the researcher, if the vulnerabilities identified are exploited, an attacker could wreak havoc on these critical systems used for monitoring radiation levels, such as falsifying measurement readings to simulate a radiation leak, tricking authorities to give incorrect evacuation directions, or increasing the time an attack against a nuclear facility or an attack involving a radioactive material remains undetected by sending normal readings to deceive operators.

Santamarta's research focused on testing software and hardware, firmware reverse engineering and RF analysis. In doing so, he successfully uncovered security vulnerabilities in radiation monitoring devices from multiple vendors, including Ludlum and Mirion.

"Failed evacuations, concealed persistent attacks and stealth man-in-the-middle attacks are just a few of the risks I flagged in my research," he says. "Being able to properly and accurately detect radiation levels is imperative in preventing harm to those at or near nuclear plants and other critical facilities, as well as for ensuring radioactive materials are not smuggled across borders."

IOActive informed the impacted vendors of the findings through responsible disclosure. All vendors acknowledged receipt of the information and despite initial responses indicating the issues would not be addressed, more recent communications from some vendors have indicated work is being done to patch the critical vulnerabilities uncovered.

According to the researcher, the found issues are still not fixed, "so increasing awareness of the possibility of such attacks will help to mitigate the risks."

MANDALAY BAY
MANDALAY BAY

The Cybe
LOOKINGGLASS

The GES Servicenter
NTTSecurity
Security
Win a FREE Gap Assessment!
Register Now to Win!
Security

black hat USA 2017
JULY 22-27, 2017
MANDALAY BAY // LAS VEGAS
Death by a thousand abstracts
A quick ~~and easy~~ guide to become a Black Hat speaker
Stefano Zanero (Black Hat Review Board member)

Manage SSL/TLS certificates across IT environments with Qualys CertView

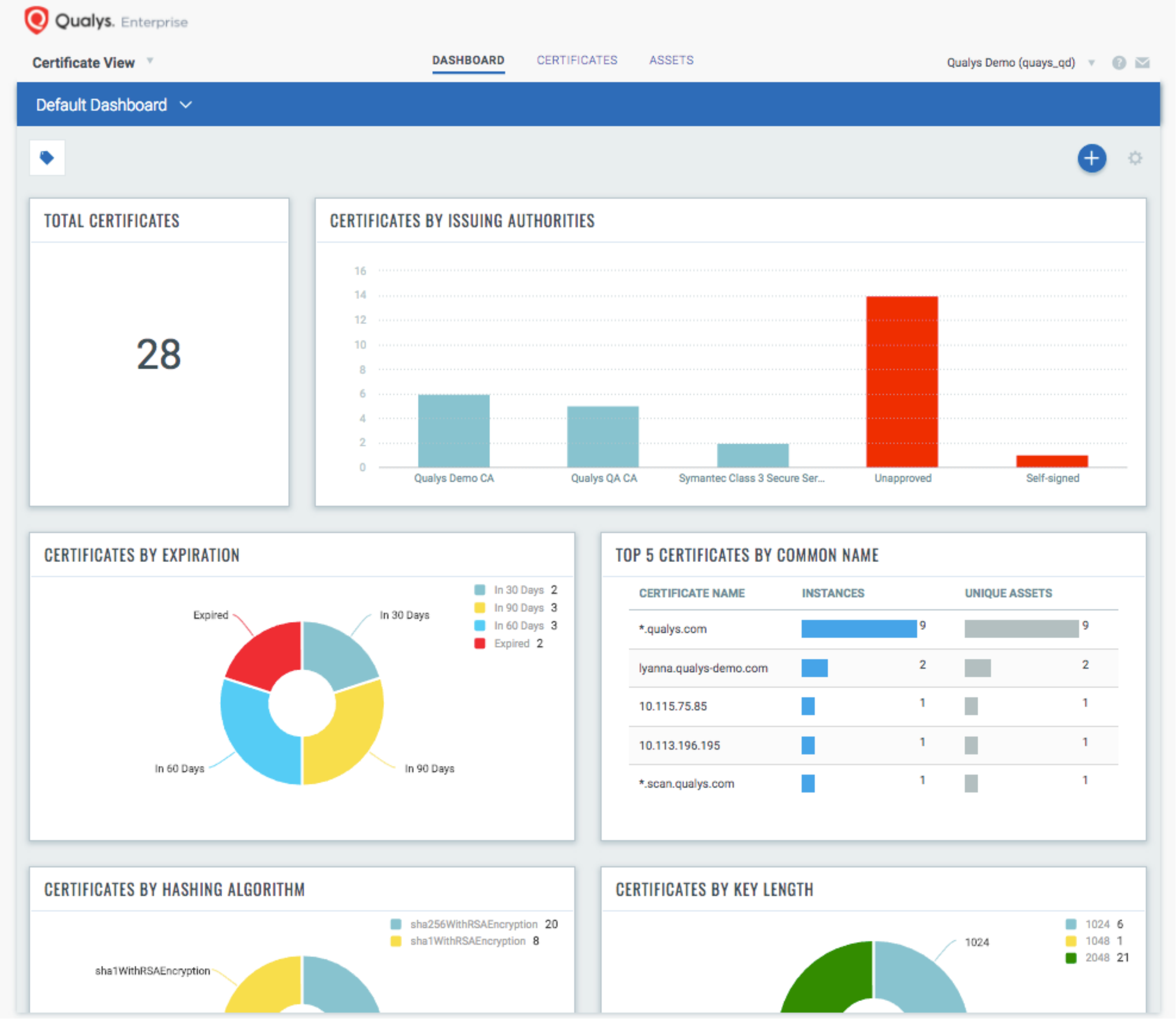
Qualys announced CertView, a new app framework in the Qualys Cloud Platform that enables customers to discover, assess and manage SSL/TLS certificates on a global scale, helping them prevent downtime and outages, audit and compliance failures, and mitigate risks associated with any expired and/or vulnerable SSL/TLS certificates on their business-critical systems.

The first two apps in CertView include Certificate Inventory (CRI) and Certificate Assessment (CRA).

Machines rely on X.509 certificates to communicate securely with each other both internally and externally, and this communication creates new attack surfaces — particularly amidst the rise of DevOps and public clouds. In order to stay ahead of this risk, organizations must automate visibility and tracking of their certificate deployments for DevSecOps.

Qualys CertView allows them to do so by centralizing visibility of certificate vulnerabilities into their overall continuous view of security and compliance state, and by enabling customers to rapidly see and remediate expired or vulnerable certificates.

“While several offerings exist to discover X. 509 certificates, most organizations rely on spreadsheet-based tracking methods and manual processes to keep track of certificates, resulting in many undocumented installations and increased exposure to risks,” said David Anthony Mahdi, Research Director, Gartner. “When using discovery tools, security leaders are often surprised by the amount of unknown certificates, from multiple certificate authorities (CAs) that exist in their environment.”



CERTIFICATE NAME	INSTANCES	UNIQUE ASSETS
*.qualys.com	9	9
lyanna.qualys-demo.com	2	2
10.115.75.85	1	1
10.113.196.195	1	1
*.scan.qualys.com	1	1

How to protect the power grid from low-budget cyberattacks

Cyberattacks against power grids and other critical infrastructure systems have long been considered a threat limited to nation-states due to the sophistication and resources necessary to mount them.

At Black Hat USA 2017, a team of New York University researchers challenged that notion by disclosing vulnerabilities in a component that, combined with publicly available information, provide sufficient information to model an advanced, persistent threat to the electrical grid.

Michail Maniatakos, a research professor at the NYU Tandon School of Engineering and an assistant professor of electrical and computer engineering at NYU Abu Dhabi, detailed the discovery of a security flaw in the authentication mechanism of a legacy protective relay — a component that responds to changes in flow across the grid to isolate electrical faults.

The vulnerability allows an attacker with local or remote access to extract and reverse-engineer the weakly encrypted and easily accessed passwords used to reprogram the relay's protective setpoints. Maniatakos and his collaborators demonstrated how information about network topology and grid components may allow adversaries to create a model of the power system — information that can be used to pinpoint the most critical nodes of the system.

Examples:

- Some local energy commission meetings, disclosing critical power usage information, are available on YouTube.
- Equipment suppliers market the sale of their critical equipment online, alerting potential adversaries to where their equipment is used.
- The researchers were able to use Google Earth to track power lines.
- The team was able to purchase the relay on eBay for about $1,000, and other equipment critical to the grid is also publicly available.

Most companies fail to measure cybersecurity effectiveness

Thycotic released its first annual 2017 State of Cybersecurity Metrics Report which analyzes key findings from a Security Measurement Index (SMI) benchmark survey of more than 400 global business and security executives around the world.

Based on internationally accepted standards for security embodied in ISO 27001, as well as best practices from industry experts and professional associations, the Security Measurement Index benchmark survey provides a way to define how well an organization is measuring the effectiveness of its IT security.

According to the findings, more than half of the 400 respondents in the survey scored an "F" or "D" grade when evaluating their efforts to measure their cybersecurity investments and performance against best practices.

"It's really astonishing to have the results come in and see just how many people are failing at measuring the effectiveness of their cybersecurity and performance against best practices," said Joe Carson, Chief Security Scientist at Thycotic. "This report needed to be conducted to bring to light the reality of what is truly taking place so that companies can remedy their errors and protect their businesses."

With global companies and governments spending more than $100 billion a year on cybersecurity defenses, a substantial number, 32 percent, of companies are making business decisions and purchasing cyber security technology blindly. Even more disturbing, more than 80 percent of respondents fail to include business users in making cyber security purchase decisions, nor have they established a steering committee to evaluate the business impact and risks associated with cybersecurity investments.

All photos by Black Hat and (IN)SECURE Magazine.

black hat
USA 2017

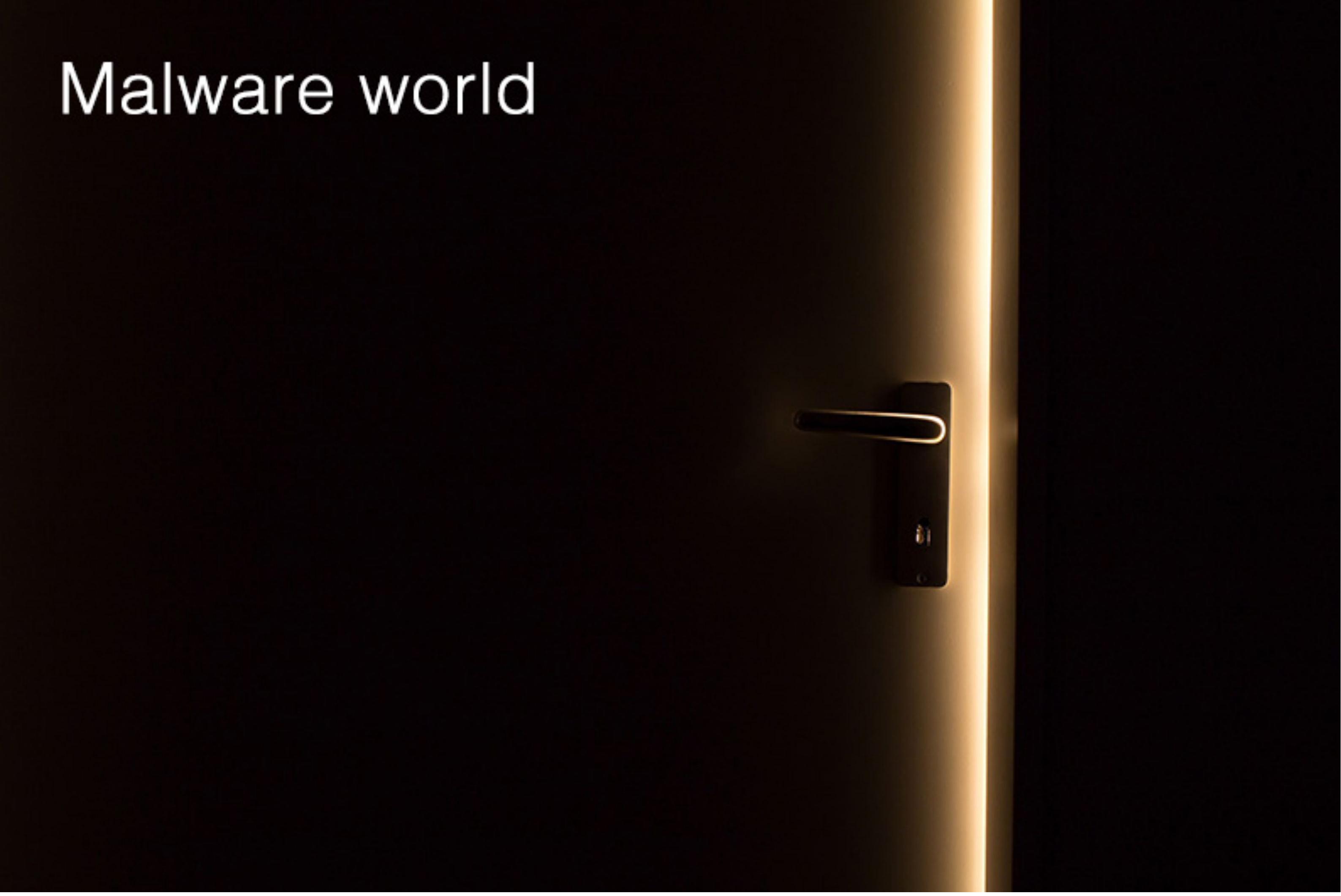
black hat

WOMEN IN SECURITY AND PRIVACY

black hat

black hat
USA 2017

Malware world

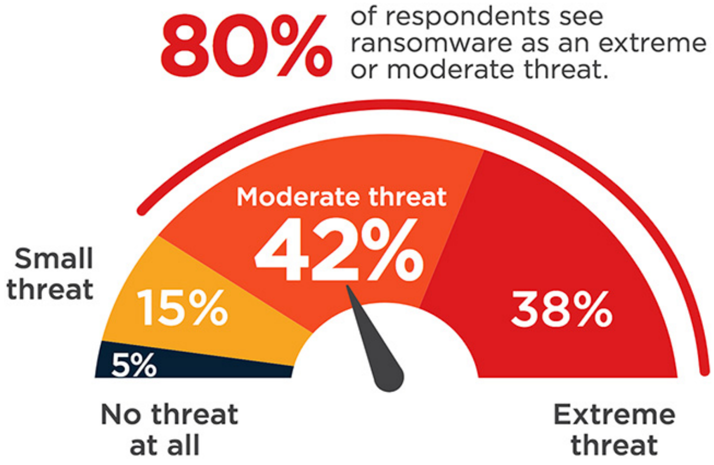


Shocker? Companies still unprepared to deal with ransomware

Companies and government agencies are overwhelmed by frequent, severe ransomware attacks, which have now become the #1 cyber threat to organizations, according to Crowd Research Partners.

Ransomware is the fastest growing security threat, perceived as a moderate or extreme threat by 80% of cybersecurity professionals. 75% of organizations affected by ransomware experienced up to 5 attacks in the last 12 months alone, 25% experienced 6 or more attacks. Only a small fraction of respondents say they would pay the ransom or negotiate with the attackers.

Email and web use represent the most common ransomware infection vectors with employees opening malicious email attachments (73%), responding to a phishing email (54%) or visiting a compromised website (28%). From a solution perspective, the majority of identified ransomware attacks were detected through endpoint security tools (83%), email and web gateways (64%), and intrusion detection systems (46%).



80% of respondents see ransomware as an extreme or moderate threat.

Stealthy backdoor used to spy on diplomats across Europe

A new, sophisticated backdoor Trojan has been used to spy on targets in embassies and consulates across Southeastern Europe and former Soviet Union republics.

ESET researchers have analyzed and documented the Trojan, which they dubbed Gazer, and are highly confident that it is being used by the Turla cyberespionage group.

The researchers have analyzed different Gazer samples and have identified four versions of the malware. Some of the samples were signed with legitimate certificates.

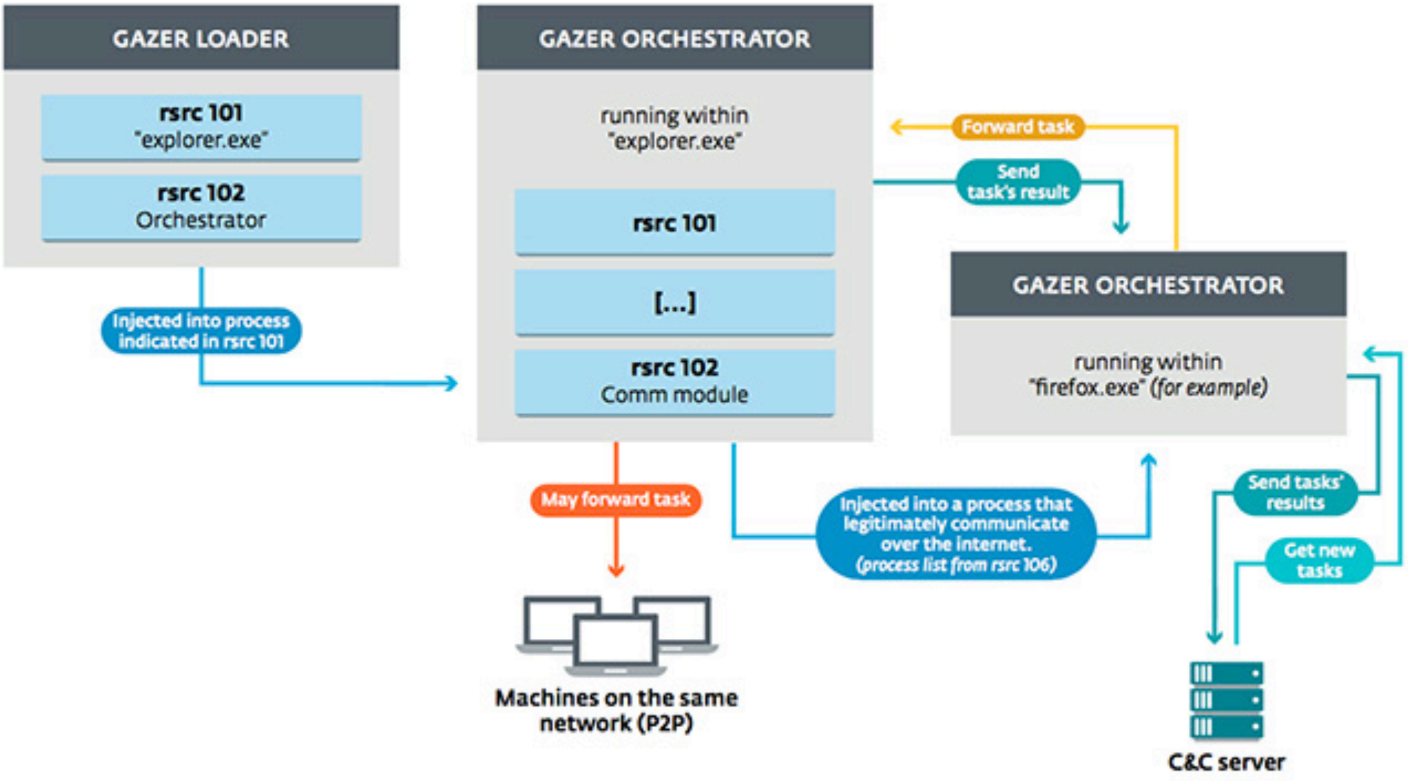
Gazer shares several similarities with other malware (Carbon, Kazuar) used by the Turla APT: it can receive encrypted tasks from a C&C server, uses an encrypted container to store its components and configuration, and logs its actions into encrypted logfiles.

The malware seems to have been in use since 2016, leveraged in targeted attacks against embassies and consulates (Turla's usual targets) but this is the first time that the malware has been documented.

Gazer flew under the security's industry radar for a some time. Part of the reason is that the authors used custom encryption (their own library for 3DES and RSA).

"As usual, the Turla APT group makes an extra effort to avoid detection by wiping files securely, changing the strings and randomizing what could be simple markers through the different backdoor versions. In the most recent version we have found, Gazer authors modified most of the strings and inserted 'videogame-related' sentences throughout the code," they noted.

"The witnessed techniques, tactics and procedures (TTPs) are in-line with what we usually see in Turla's operation: a first stage backdoor, such as Skipper, likely delivered through spearphishing followed by the appearance on the compromised system of a second stage backdoor, Gazer in this case."


GAZER LOADER
rsrc 101 "explorer.exe"
rsrc 102 Orchestrator
Injected into process indicated in rsrc 101
GAZER ORCHESTRATOR
running within "explorer.exe"
rsrc 101
[...]
rsrc 102 Comm module
May forward task
Machines on the same network (P2P)
Forward task
Send task's result
GAZER ORCHESTRATOR
running within "firefox.exe" (for example)
Injected into a process that legitimately communicate over the internet. (process list from rsrc 106)
Send tasks' results
Get new tasks
C&C server

Google pulls 500+ backdoored apps from Google Play

Security researchers have identified over 500 apps on Google Play containing an advertising software development kit (SDK) called Igexin, which allowed covert download of spying plugins. The apps in question represent a wide selection of photo editors, Internet radio and travel apps, educational, health and fitness apps, weather apps, and so on, and were downloaded over 100 million times across the Android ecosystem.

"Typically, mobile apps use advertising SDKs to make it easy for app developers to leverage advertising networks and deliver ads to customers. Like many ad networks, the Igexin service promotes its targeted advertising services that leverage data collected about people such as their interests, occupation, income, and location," Lookout researchers noted.

It should be standard procedure for app developers to analyze any third-party code they embed in their apps in order to discover and disclose any data collection capabilities it has in the app's privacy policy. Unfortunately, too many of them don't bother or don't know how to, and opt for trusting the developers of SDKs blindly.

The researchers pointed out that not all versions of the Igexin ad SDK deliver malicious functionality, but those that did implemented a plugin framework that allows the client to load arbitrary code, and requested instructions on what to download next.

Mostly, it was to exfiltrate call logs, which contain information such as time of call, calling number, and call state. But there were also instances where data about installed apps and GPS location was exfiltrated.

"Users and app developers have no control over what will be executed on a device after the remote API request is made. The only limitations on what could potentially be run are imposed by the Android permissions system," the researchers pointed out.

EV ransomware is targeting WordPress sites

WordPress security outfit Wordfence has flagged several attempts by attackers to upload ransomware that provides them with the ability to encrypt a WordPress website's files.

They dubbed the malware "EV ransomware", due to the .ev extension that is added to the encrypted files.

The ransomware is uploaded once the attacker manages to compromise a WordPress website. The attacker starts the encryption process from an interface, after choosing a complex key and pressing the "Submit" button.

EV ransomware encrypts most of the files but also leaves some unencrypted.

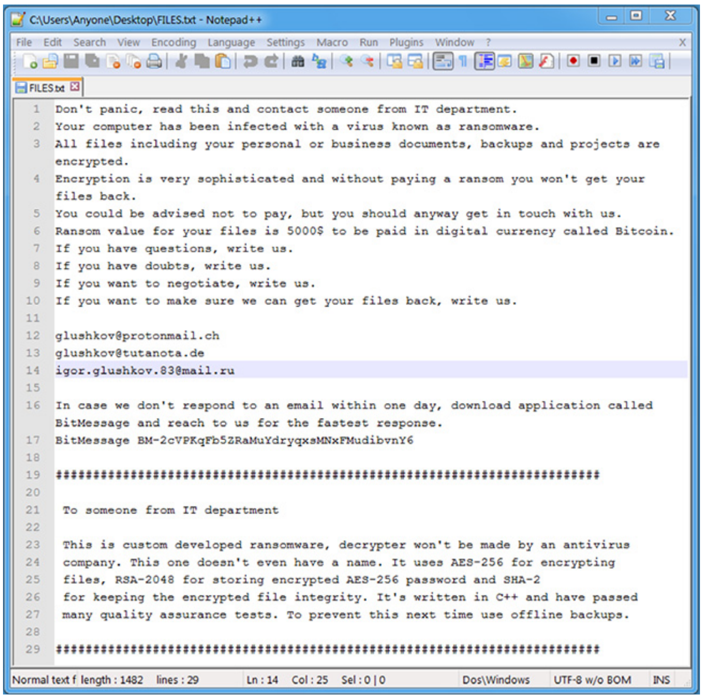
"The encryption process uses mcrypt's functionality, and the encryption algorithm used is Rijndael 128. The key used is a SHA-256 hash of the attacker-provided encryption key," the Wordfence team shared.

"Once the data is encrypted, the IV used to encrypt the file is prepended to the ciphertext, and the data is base64-encoded before it is written to the encrypted .EV file."

Another thing that's important for the victims to know is that even if they pay the ransom and receive the decryption key, decrypting the files will not be a simple process.

"This ransomware provides an attacker with the ability to encrypt your files, but it does not actually provide a working decryption mechanism," the team warns.

"If you are affected by this ransomware, do not pay the ransom, as it is unlikely the attacker will actually decrypt your files for you. If they provide you with a key, you will need an experienced PHP developer to help you fix their broken code in order to use the key and reverse the encryption."


C:\Users\Anyone\Desktop\FILES.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
FILES.txt
Normal text f length : 1482 lines : 29
Ln : 14 Col : 25 Sel : 0 | 0
Dos\Windows
UTF-8 w/o BOM
INS

```
Don't panic, read this and contact someone from IT department.
Your computer has been infected with a virus known as ransomware.
All files including your personal or business documents, backups and projects are encrypted.
Encryption is very sophisticated and without paying a ransom you won't get your files back.
You could be advised not to pay, but you should anyway get in touch with us.
Ransom value for your files is 5000$ to be paid in digital currency called Bitcoin.
If you have questions, write us.
If you have doubts, write us.
If you want to negotiate, write us.
If you want to make sure we can get your files back, write us.

glushkov@protonmail.ch
glushkov@tutanota.de
igor.glushkov.83@mail.ru

In case we don't respond to an email within one day, download application called BitMessage and reach to us for the fastest response.
BitMessage BM-2cVPKqFb5ZRaMuYdryqxsMNxFMudibvnY6

####################################################################

 To someone from IT department

 This is custom developed ransomware, decrypter won't be made by an antivirus
 company. This one doesn't even have a name. It uses AES-256 for encrypting
 files, RSA-2048 for storing encrypted AES-256 password and SHA-2
 for keeping the encrypted file integrity. It's written in C++ and have passed
 many quality assurance tests. To prevent this next time use offline backups.

####################################################################
```

New, custom ransomware delivered to orgs via extremely targeted emails

Ransomware campaigns are usually wide-flung affairs: the attackers send out as many malicious emails as possible and hope to hit a substantial number of targets. But more targeted campaigns are also becoming a trend.

Targeting different verticals

Take for example the latest ones spotted by Proofpoint researchers in August: one was primarily aimed at Healthcare and Education verticals, while the other targeted Manufacturing and Technology companies.

In both cases, the campaigns targeted UK and US organizations, and consisted of a few custom crafted emails, made to appeal to the intended set of potential victims and to carry a Word file booby-trapped with an embedded executable.

Healthcare orgs were hit with a file named “patient_report”, supposedly sent by the Director of Information Management & Technology at a UK hospital, while the emails aimed at Manufacturing and Technology verticals had “Order/Quote” in the subject line, and “presentation” as the booby-trapped Word file name.

Opening the file and double clicking the embedded executable resulted in the dropping of the ransomware on the target system.

The Defray ransomware

In the ransom note, the malware was not given a name. Proofpoint researchers named it Defray, based on the C&C server hostname.

If the attackers are to be believed, Defray “uses AES-256 for encrypting files, RSA-2048 fo storing encrypted AES-256 password and SHA-2 for keeping the encrypted file integrity.”

The researchers are yet to investigate the specifics of the encryption routine, but apparently the malware effectively encrypts a wide variety of file types, but does not add specific file extensions to them.

“After encryption is complete, Defray may cause other general havoc on the system by disabling startup recovery and deleting volume shadow copies,” they pointed out.

“On Windows 7 the ransomware monitors and kills running programs with a GUI, such as the task manager and browsers. We have not observed the same behavior on Windows XP.”

The attackers are asking for quite a bit of money to restore the encrypted files: $5,000. They’ve also provided contact email addresses and a BitMessage account for the victims to contact them and ask questions or even negotiate.

Designing security policies to fit your organization’s needs

By Mike Shultz

As private and public sector regulations are mounting and high-profile attacks continue to sweep the globe, adoption of the NIST Cybersecurity Framework is a rapidly accelerating trend. Built by drawing upon the wisdom of over 3,000 security experts and practitioners, the NIST CSF provides a comprehensive structure for designing and implementing a robust cybersecurity program.

While NIST CSF is comprehensive, it falls short of guiding execution for specific projects. Risk mitigation advice based on NIST CSF and delivered by security experts may be beneficial given an unlimited budget, but it’s safe to say very few of us enjoy that luxury. Structuring policies around known and potential vulnerabilities in the security chain can get complicated and costly, so how do we use the NIST CSF guidance to decide when and how to update or generate new policies?

"Although 80% of security spending is focused on the perimeter, only 20% of the breaches occur there.” - Zeus Kerravala, principal analyst at ZK

The vast majority of devastating breaches can be traced back to human error, the lack of adequate operational policies and processes, or both. Few organizations consistently apply the most basic techniques for protecting themselves, and addressing these internal concerns upfront is a prerequisite for implementing a comprehensive cyber risk management program.

“The Canadian Cyber Incident Response Centre (CCIRC) recommends that network administrators implement the following four mitigation strategies, which can prevent as much as 85% of targeted cyberattacks: application whitelisting, patch applications, patch operating system, restrict administrative privileges.”

Keeping vulnerability and risk factors in mind when considering organization-wide policies will allow executives and boards of directors to accurately address internal cyber defense needs. Implementing these risk mitigation policies is the most effective way to defend against the most devastating breaches:

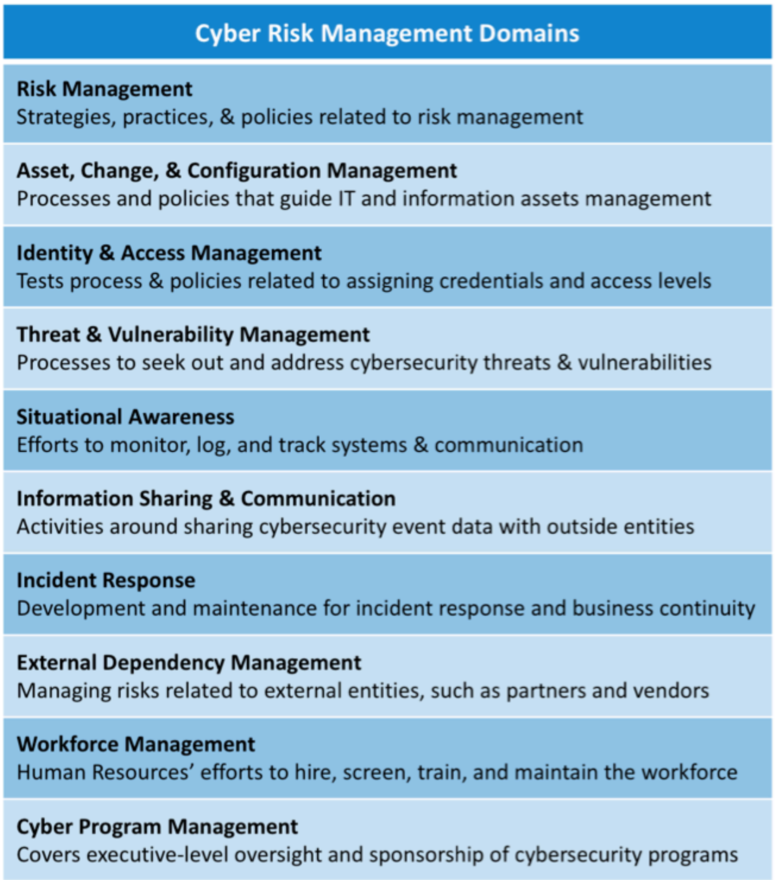
1. Keep up to date. Applying security patches as they are made available is a no-brainer that costs little. The same is true for keeping the latest anti-virus software up to date. In short, do what you already know are the right things, but in a timely and organized manner. With processes and audits in place encouraging speedy updates, it's easier to ensure they get done.

2. Restrict access to data. Employ the "least privilege" access model. Users and processes should only have access to the data and resources they need to conduct their work. A common error is enabling users to have administrative access when it's unneeded, thereby creating more targets for hackers and malware.

3. Maintain duplicate copies. Store data both locally and in the cloud. Major cloud vendors allow configuration that ensures multiple mirrored copies are kept in different locales. While adequate backup policies and processes are imperative, it's also important to note the need for knowledgeable staff to operate those cloud-based backups to keep data safe in both places.

4. Create a cyber-conscious culture. The cost for programs that educate employees about phishing attacks ranges from free to reasonable. Make sure every employee is retested on a regular basis. Use internal staff or hire an outside firm to run broad phishing tests and general cybersecurity awareness checks to track the organization's vulnerability.

Building a comprehensive program. Once these obvious gaps have been addressed, building a comprehensive cybersecurity program by applying NIST CSF is a rational move. Organize your efforts to identify and close gaps in ten different domains:



Cyber Risk Management Domains
Risk Management Strategies, practices, & policies related to risk management
Asset, Change, & Configuration Management Processes and policies that guide IT and information assets management
Identity & Access Management Tests process & policies related to assigning credentials and access levels
Threat & Vulnerability Management Processes to seek out and address cybersecurity threats & vulnerabilities
Situational Awareness Efforts to monitor, log, and track systems & communication
Information Sharing & Communication Activities around sharing cybersecurity event data with outside entities
Incident Response Development and maintenance for incident response and business continuity
External Dependency Management Managing risks related to external entities, such as partners and vendors
Workforce Management Human Resources' efforts to hire, screen, train, and maintain the workforce
Cyber Program Management Covers executive-level oversight and sponsorship of cybersecurity programs

Some domains don't fall under the responsibility of groups traditionally responsible for cybersecurity, like IT and security. In many organizations, Risk Management is a separate function. Responsibility for External Dependency Management usually rests with the purchasing or procurement department. Human resources (HR) manages the Workforce Management domain, often in collaboration with the security group. IT handles Asset, Change & Configuration, while Threat & Vulnerability Management and Situational Awareness are often managed by security. Information Sharing & Communication and Incident Response may be jointly managed by security and IT.

Overall responsibility for Cyber Program Management may fall to the CISO, but Internal Audit, General Counsel, and Risk Management often share this responsibility in larger organizations.

Creating a cyber-conscious culture

One thing that has become increasingly clear over the past few years is that cybersecurity is no longer solely an IT problem, it's a business problem. With so many moving parts in the cybersecurity chain and responsibilities divided across departments, it's important to instil cyber awareness throughout the organization and at all levels – from entry level to C-level. Keep in mind that cyber vulnerabilities have no boundaries, and significant risk can be introduced by normal business activities. As new vendors are added, the procurement department must learn to include security vetting of the vendors as part of their evaluations. Similarly, HR can introduce significant risk with the addition of new hires. When employees leave, it's critical that policies and processes are in place to ensure access to organizational resources is revoked immediately.

HR also plays a key role by ensuring all new employees receive cybersecurity training, and that existing employees receive regular refreshers to mitigate the likelihood of falling prey to phishing attacks and malware introduction. Surprisingly, those at the greatest risk for phishing attacks are C-level officers. They often aren't subjected to regular policy updates and training, and are therefore less aware of cyber risk. Because of their greater access to the organization and to valuable resources like financial records, they prove to be major (and unwitting) vulnerabilities for their companies.

Managing third party risk

Another source of risk derives from third-party relationships. Vendor management is a substantial risk many organizations fail to focus on until they experience a breach.
Some of the most egregious breaches over the last several years have occurred because of a breakdown in the management and oversight of external relationships that are supported by automated technical connections. One of the best known is the Target breach, which occurred through poor management of a vendor relationship with an HVAC vendor. Many others on the list of the worst breaches have been the result of lax policies and processes around supply chain partners.

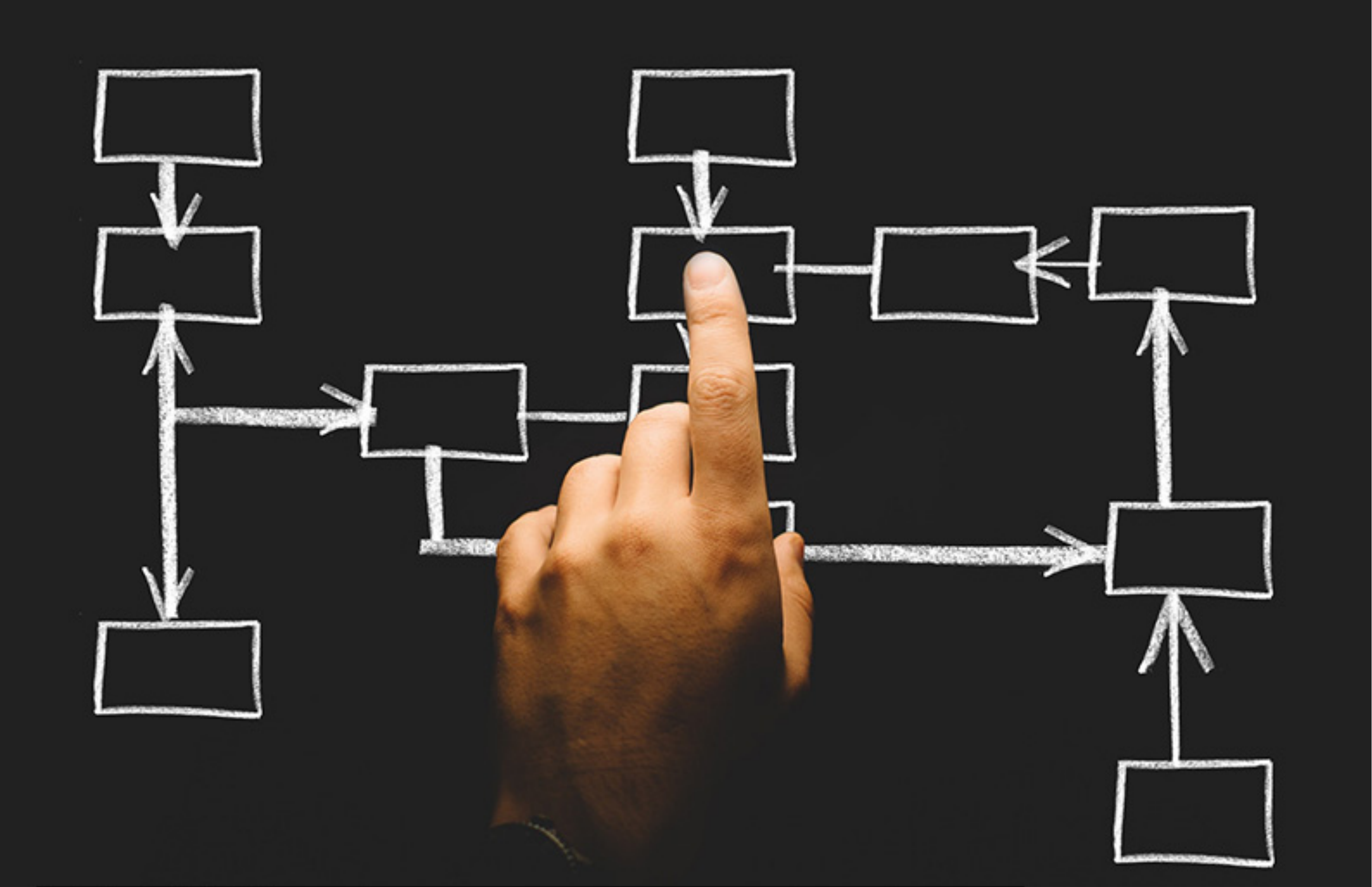
Implementing policies and processes

The recent presidential executive order and NY DFS regulations require specific policies to be set in place for government agencies and financial institutions. While these mandates are important in motivating change and pointing toward best practices, they are not a "one size fits all" solution. Policies will differ based on the unique business goals and risk factors an organization faces, which can be identified through traditional cyber reporting protocols (checklists and spreadsheets) and IT governance efforts and tools.

Once the organization's cyber policies are determined and accepted, processes must be defined, implemented, and monitored in order to ensure they adequately support the policies. These new processes and policies must be effectively integrated into current frameworks, and leadership must ensure the entire organization is properly trained to execute them.

Making it all work requires engagement from groups across an organization that play a role in other forms of enterprise risk, not just IT and security. Board members are concerned about shareholder suits and potential carve outs for cyber risk from D&O coverage. They also share the C-suite's concerns about maintaining the enterprise's valuation and reputation. Having a solid set of risk management policies in place provides the foresight about vulnerabilities needed for an organization's leadership to determine its resiliency in the event of a cyberattack. Company leadership, IT and security teams, and individual departments are responsible for working together to ensure cyber and business policies are in alignment with the organization's unique vulnerabilities to protect it from growing and evolving cyber risk.

Mike Shultz is the CEO at Cybernance (www.cybernance.com).



KPN CISO paints a greater security picture

By Zeljka Zorz

Being the CISO of such a huge and diverse company as KPN, the Netherlands' largest telecom and ISP provider, requires great determination, and the current holder of the position fits the bill on that score.

Jaya Baloo was brought in after the company was breached in 2012 by a teenage Dutch hacker, who managed to gain access to some 300 systems. Such a hack required nothing less than a thorough audit of the (failed) defenses, the will to realise and say: "It's our own fault," and a sincere determination to do better.

KPN's approach to security

It helped that Baloo was granted a lot of leeway to make the decisions she considered to be the right ones to improve security, and that she knew that a shift in perception was crucial: the security department needs to be always viewed as one that adds to the company's bottom line.

She achieved the latter by making sure that the impact for every vulnerability and incident is measured, and potential loss calculated (conservatively). This information makes extremely clear to the CEO and the board of directors the value of what they do, i.e. that they save the company much more money that they cost.

KPN has teams for each phase of the greater security plan. After a security strategy and policies are decided on, its red team is there to probe its networks and systems to expose the cracks open to attackers. The security operations center (SOC) does the reactive security monitoring (but also hunts for intruders), and the CERT manages incident response and resolution.

SECURITY AWARENESS, VISIBILITY AND RISK INTELLIGENCE, AND SECURITY CAPABILITY ARE CRUCIAL FOR ORGANIZATIONAL SECURITY

Each business sector has its own senior security officer, who reports directly to her and not to the head of that particular department, so that he or she does not have an incentive to make the situation seem better than it is.

Not getting hacked, ever, is an unrealistic expectation, she told the audience at this year's edition of the FSec security symposium, held earlier this month in Varazdin, Croatia. But, you have to be ready to minimize the impact of attacks that do succeed.

The only security metric that the CEO needs to know is how fast does it take for us to prevent a situation from turning into a problem, she added.

Another way to keep management appraised of the current security situation is to do a weekly status report that shows the current DEFCON state of the organization, current risks, problem areas and teams.

All for one, and one for all

One of KPN's informal mandates is to be a thought leader when it comes to security. Baloo fulfils that mandate by sharing the company's knowledge with infosec professionals attending security conferences around the world.

The company regularly calls in cyber security experts to share their knowledge with their employees, continuously educates management (through the aforementioned unfiltered risk reports), and provides security tools and open sources policies so that other organizations can use them to improve their security stance.

It also shares IOCs in trusted communities, and tries to keep pace with technological progress (e.g. they implemented end-to-end quantum key distribution in its network between KPN datacenters in The Hague and Rotterdam, and provided easy encryption tools through a partnership with Silent Circle).

She made sure to hammer the following messages home:

- We must learn from others (and encourage others to learn from us)
- We must know how to fail gracefully, and learn from it
- We should not blame attackers for our own failings, but work to fix them.

Security is a continuous process that doesn't have an end, she says. And you should not make the mistake of believing that if an incident does not affect you directly, it's not important. We're all in this together, and helping everybody helps us, she noted.

Some more tips for every CISO

She considers security awareness, visibility and risk intelligence, and security capability to be crucial for organizational security.

The former must be customized to each employee's position in the company, and the latter must be continually improved. And when it comes to visibility, you need to know how to get to the negatives and not drown in data.

All in all, she believes that all organizations should work on getting the trust of their customers – and just compliance won't do it. "If your CEO says that your security bar is set by legal requirements, you're in deep trouble," she pointed out.

Zeljka Zorz is the Managing Editor of (IN)SECURE and Help Net Security (www.helpnetsecurity.com)

Has healthcare misdiagnosed the cybersecurity problem?

By Kevin Magee

Take a cursory look at the US Department of Health and Human Services' "wall of data breach shame" and you might be scratching your head: Why does the healthcare sector seem so disproportionately victimized by hackers and cybercriminals? Why do its defenses seem so much weaker than those of other industries?

For the most part, the healthcare industry has misdiagnosed the cybersecurity problem.

Most senior leadership in healthcare is medically trained with a clinical background in an industry built on such noble concepts as "do no harm" and forward-thinking practices like evidence-based medicine. Through this lens, healthcare organizations regularly misinterpret the nature of the cybersecurity problem and, consequently, how to treat it.

This misdiagnosis has led to countless breaches over the past several years at healthcare organizations around the world as well as significant, often paralyzing ransomware attacks, including the WannaCry outbreak that crippled dozens of hospitals in the UK, effectively disabling the most basic of patient care.

Not only is IT subordinate to patient care in terms of attention, budgets and priorities, but cybersecurity is perceived as a problem that can be "fixed" rather than one best managed by means of a regular and ongoing health regime.

Acute care vs. sound overall health

When a patient arrives at the emergency room with a broken arm, there is a clear process: triage, treatment, discharge. This acute care model focuses on fixing problems as they occur. Preventing the broken arm, for example, is not a factor in the process, decision-making or treatment planning. In acute care, it's all about dealing efficiently and correctly with whatever problems walk through the ER door. However, unlike a broken arm, which can quickly heal with few lasting side effects, a ransomware attack like WannaCry can be interminable and even fatal to a healthcare organization.

Applying acute care to cyberattacks and security breaches doesn't work because it's entirely reactive in nature. No matter how well you define and refine the treatment process or in this case, mitigation and remediation, the outcome will never change. Simply put, more and more arms will continue to get broken regardless of how well the organization fixes them.

However, with cyberattacks and breaches, healthcare organizations do have the opportunity to change the outcome – if only they start to think differently about the problem.

Rx: A new security model that mimics the human immune system

To turn the corner and improve defenses, senior healthcare leadership must not think about cybersecurity in terms of patching problems and reacting to emergencies. By contrast, they need to look at the overall health of their networks and defenses, find ways to improve basic resiliency and apply a new security model – one that is based on pervasive visibility and mimics the human immune system, which:

1. Works proactively from within to prevent health problems from occurring or worsening.
2. Covers the entire body, not simply reactively focusing on problem areas.
3. Learns, adapts and remembers so it can fight off future infections more efficiently.
4. Responds immediately, independently and automatically.

In addition to pervasive visibility into all data flows – the lifeblood of all healthcare organizations – a new security model would include good hygiene (prevention), detection, prediction and action (containment).

Good hygiene

The benefits of good hygiene practices are clear in a healthcare setting. Simple measures, such as vigilance in adhering to handwashing, can drastically decrease the chances of contamination, spread of disease and hospital-acquired infection rates. A similar approach to cybersecurity can yield comparable results.

Examples of good security hygiene include patching, privileged credential protection, network segmentation, asset isolation and perimeter protection. These all help ensure that attackers cannot break in and infect organizations – or at least, limit an attacker's success. With good hygiene, organizations can protect themselves from being a target of opportunity by forcing attackers to take additional or unnatural steps to gain access and spread the threat.

Detection

Good security hygiene can help eliminate basic threats and prevent untargeted attacks, such as WannaCry, but it is unlikely enough to stop a focused attack by an experienced and determined adversary. In this case, forcing the attacker to take unnatural steps provides the organization an opportunity to detect anomalies – which are relative to normal behavior and consequently, their detection requires a baseline of what "good health" looks like.

This is the basis of many machine learning solutions in development today. With a baseline established, organizations can compare all activity and quickly detect anomalies. Machine learning technologies resemble the human immune system's ability to learn, remember and combat viruses and bacteria based on adaptation.

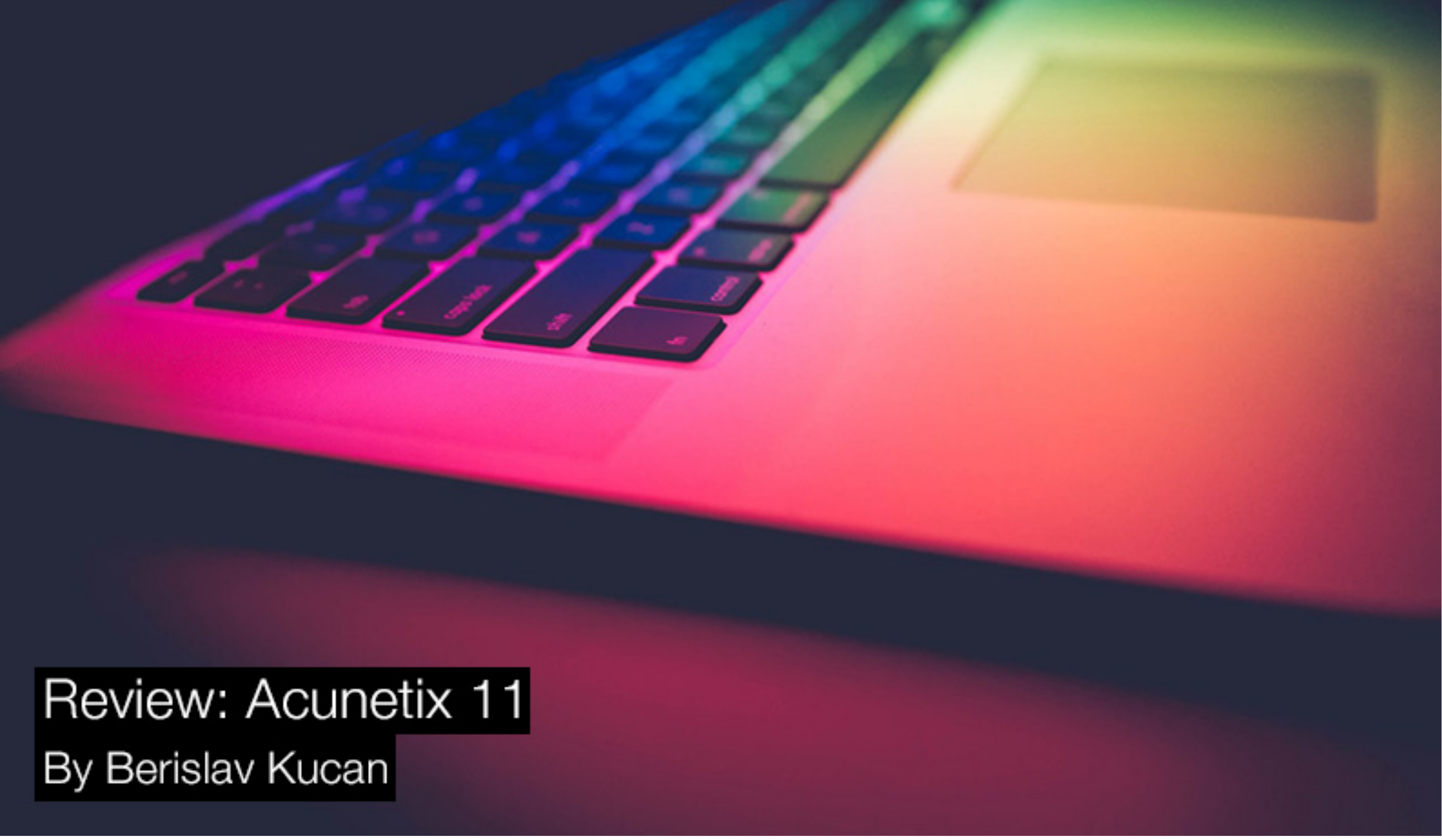
Prediction and action

Once anomalies are detected, the next step in a security immune system is to understand intent. For example, is what we're seeing normal or intentionally bad behavior? With intent uncovered, organizations can act to contain, remediate or even, allow contained detonation of the threat to better learn and understand the intent.

While much of this now happens manually and straddles organizational boundaries, there are many solutions, including artificial intelligence (AI) and security workflow orchestration, that can help automate the process.

Kevin Magee is the Global Security Strategist at Gigamon (www.gigamon.com).

77.232.53.14
SEE BEYOND THE SURFACE
LEVERAGE OUR 20+ YEARS OF CYBERSECURITY & INTELLIGENCE EXPERIENCE
Defend Your Network, Brand, Customers, and Employees
45.116.76.97
LOOKINGGLASS
Explore the Power of LookingGlass at LookingGlassCyber.com
Third Party Risk / Brand & Executive Protection / Malware & Phishing Protection



Review: Acunetix 11

By Berislav Kucan

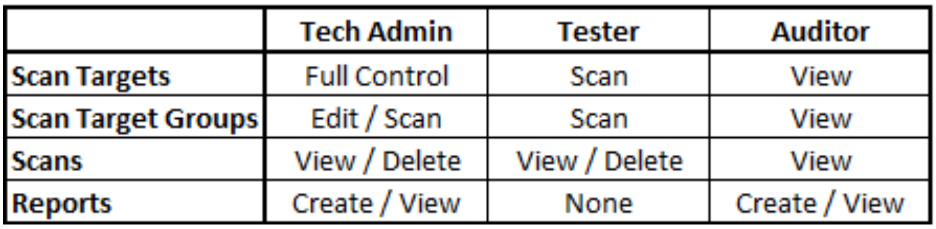
Acunetix is one of the biggest players in the web security arena. This European company released the first version of their product back in 2005, and thousands of clients around the globe use it to analyze the security of their web applications. They recently unveiled Acunetix version 11, so we've decided to take it for a spin.

Interface, users and roles

Before I start, it needs to be noted that I've tested the on-premise edition of Acunetix. The product is also available as an online system, and details on it can be found in the last part of the review.

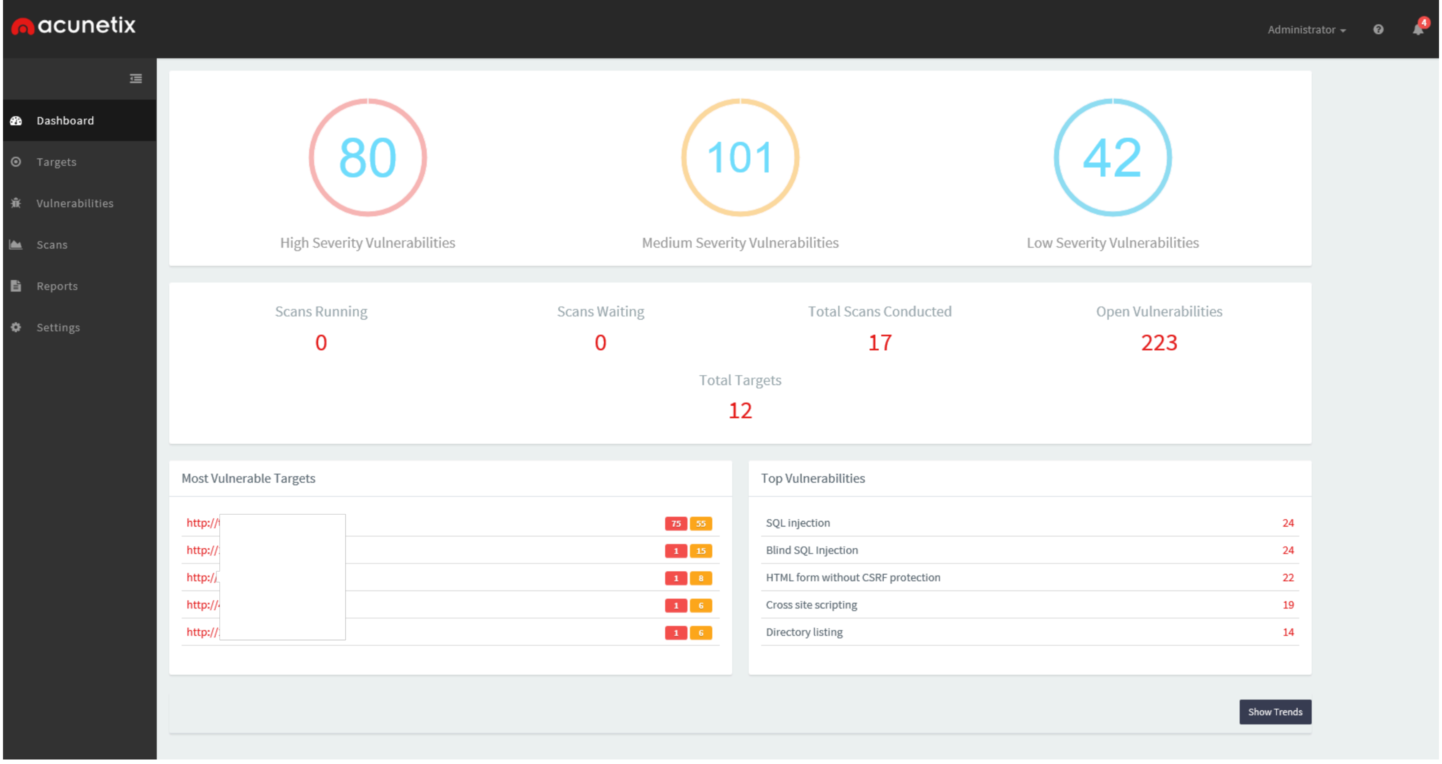
One of the major changes in this version is a new interface that has been engineered from the ground up. Up until now, Acunetix was a Windows application, but with this release the user interface was moved into the browser. You can now use Acunetix by accessing its UI running on localhost:3443.

This switch provides a multi-user and multi-role environment where different members of the organization can access Acunetix fully, or just in limited capacity. The latter depends on a system of user roles assigned to Acunetix users. The default roles are *Tech Admin*, *Tester*, and *Auditor*:



	Tech Admin	Tester	Auditor
Scan Targets	Full Control	Scan	View
Scan Target Groups	Edit / Scan	Scan	View
Scans	View / Delete	View / Delete	View
Reports	Create / View	None	Create / View

The interface is fast and responsive, with a strong focus on functionality. The data between the browser and the server, whether used directly on a computer running Acunetix or via the local network, is transferred via TLS/SSL. A unique certificate authority for your environment is generated during the installation procedure.



80 High Severity Vulnerabilities

101 Medium Severity Vulnerabilities

42 Low Severity Vulnerabilities

Scans Running	Scans Waiting	Total Scans Conducted	Open Vulnerabilities
0	0	17	223

Total Targets 12

Most Vulnerable Targets

http://[redacted]	75	55
http://[redacted]	1	15
http://[redacted]	1	8
http://[redacted]	1	6
http://[redacted]	1	6

Top Vulnerabilities

SQL injection	24
Blind SQL Injection	24
HTML form without CSRF protection	22
Cross site scripting	19
Directory listing	14

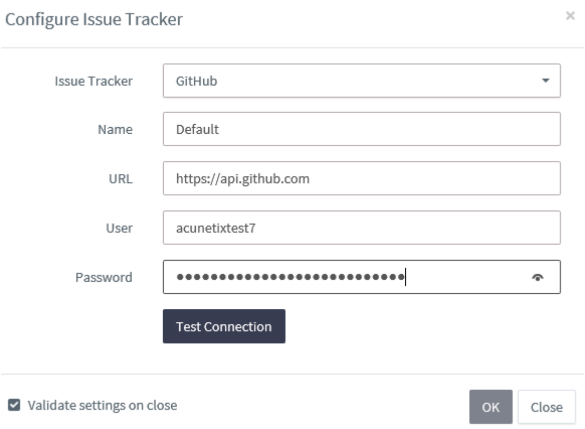
Target setup and scanning

Before starting the scanning process, you'll need to create one or multiple targets. Back in the days of the first web application security scanners, target setup was straightforward – you would add a target address and the port on which the httpd is running. Nowadays the process is more complex, and setting up the target can involve the customization of some 20 or so parameters. By default, Acunetix defaults work for most sites, so you can start the scan without any further customizing.

For starters, depending on the business criticality and performance of the target system, you can choose different impact levels and scan speeds. For sites with authentication, there are options covering both HTTP auth, as well as web app form logins. In the case of built-in form logins, the scanner will try to use the provided credentials to connect automatically. In some cases (e.g. custom applications) this won't work, but there is a nifty add-on called Login Sequence Recorder, which gives you the ability to record your manual login process and Acunetix will successfully recreate it when the scan is started.

The built-in crawler can be modified with predefined sets of user agent data, or you can create one that will fit your needs. You can also import different data into the crawler. Accepted formats include text files with a list of URLs, HTTP Sniffer (part of Acunetix's freeware pentest tools) logs, Fiddler .SAZ, BURP saved/state files and HAR (HTTP Archive) files. The "Advanced" tab of the target setup includes a couple of other options you can play with (e.g. writing your custom headers and/or cookies).

The issue tracking functionality is a nice addition and it currently supports Microsoft Team Foundation Server, Atlassian's JIRA, and GitHub.



Configure Issue Tracker

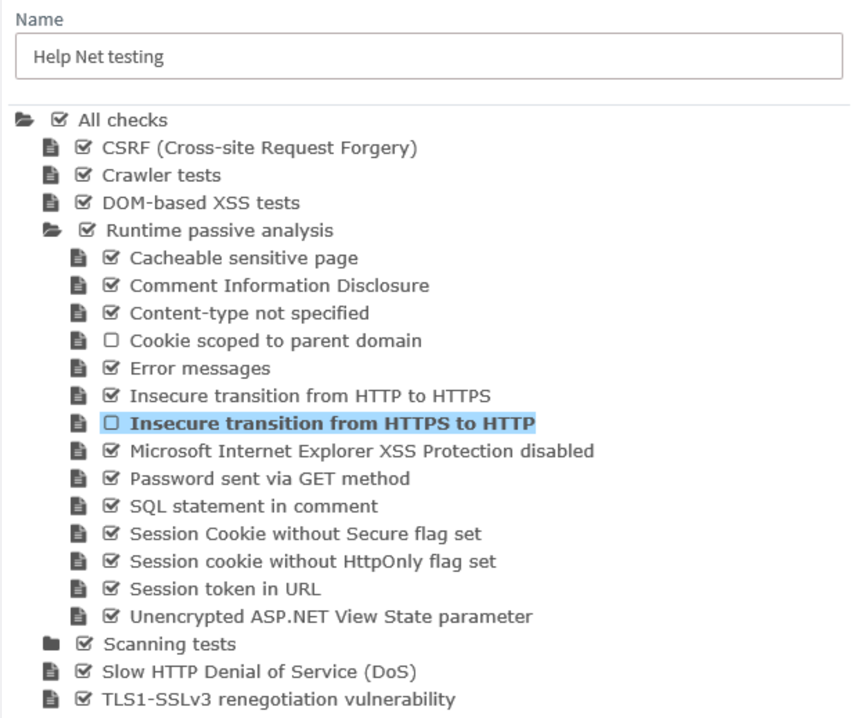
Issue Tracker	GitHub
Name	Default
URL	https://api.github.com
User	acunetixtest7
Password	••••••••••••••••••••••••••

☑ Validate settings on close

Every scan can be started immediately, be scheduled for a specific moment in the future, or set as a recurring task. By default, every scan is set as a *Full Scan*, but you can also choose one of the predefined options, including:

- High Risk Vulnerabilities
- Cross-Site Scripting Vulnerabilities
- SQL Injection Vulnerabilities
- Weak Passwords
- Crawl Only.

If you want to customize your scanning to an even greater degree, go into *Settings > Scan types*, and create a new preset by selecting items from a long list of vulnerability classes and sub-classes.



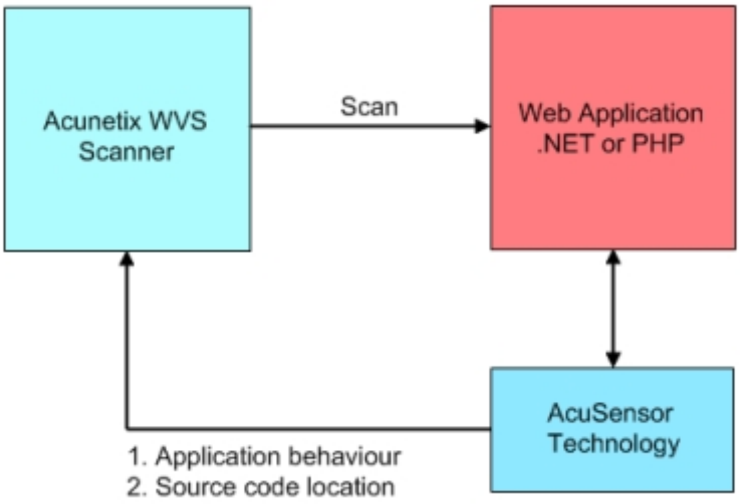
Name

Help Net testing

- ☑ All checks
  - ☑ CSRF (Cross-site Request Forgery)
  - ☑ Crawler tests
  - ☑ DOM-based XSS tests
  - ☑ Runtime passive analysis
    - ☑ Cacheable sensitive page
    - ☑ Comment Information Disclosure
    - ☑ Content-type not specified
    - □ Cookie scoped to parent domain
    - ☑ Error messages
    - ☑ Insecure transition from HTTP to HTTPS
    - □ **Insecure transition from HTTPS to HTTP**
    - ☑ Microsoft Internet Explorer XSS Protection disabled
    - ☑ Password sent via GET method
    - ☑ SQL statement in comment
    - ☑ Session Cookie without Secure flag set
    - ☑ Session cookie without HttpOnly flag set
    - ☑ Session token in URL
    - ☑ Unencrypted ASP.NET View State parameter
  - ☑ Scanning tests
  - ☑ Slow HTTP Denial of Service (DoS)
  - ☑ TLS1-SSLv3 renegotiation vulnerability

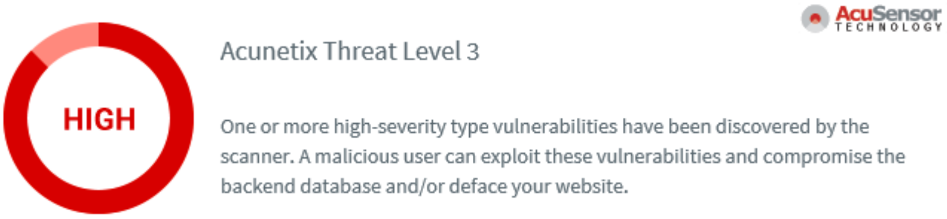
AcuSensor technology

Introduced in version 6 of Acunetix back in 2008 – and heavily improved since – AcuSensor technology extends the reach of the black box scanning with data collected from a custom sensor. For each target, Acunetix generates an AcuSensor file that should be uploaded to the web site being tested. Installing AcuSensor in an ASP.NET web application takes just a couple of clicks, while for PHP based sites you'll need to modify the *php.ini* or *.htaccess* file with the location of the AcuSensor file.



AcuSensor gives you the “inside job” functionality. There is much you can achieve by scanning a web site from the outside, but combining this with real-time feedback and analysis from the inside offers much greater visibility. When I did test scans with AcuSensor enabled, the number of detected issues (or different severity) was, on average, 45 percent greater than when AcuSensor was not used.

Web application scanners use a combination of crawled data (following links) and predefined lists of files (common locations for files being vulnerable or not) in different environments. As AcuSensor has access from the inside, it can deliver a third list of potential targets – those files that are invisible from the outside, but can have security issues (e.g. remote shells, backed-up files with sensitive data, or potentially vulnerable apps/plugins saved into non typical locations). Because of this scan structure (depicted above), AcuSensor can also report stack traces and affected SQL queries caused by the found vulnerabilities, as well as pinpoint the troublesome positions in the source code.



Acunetix Threat Level 3

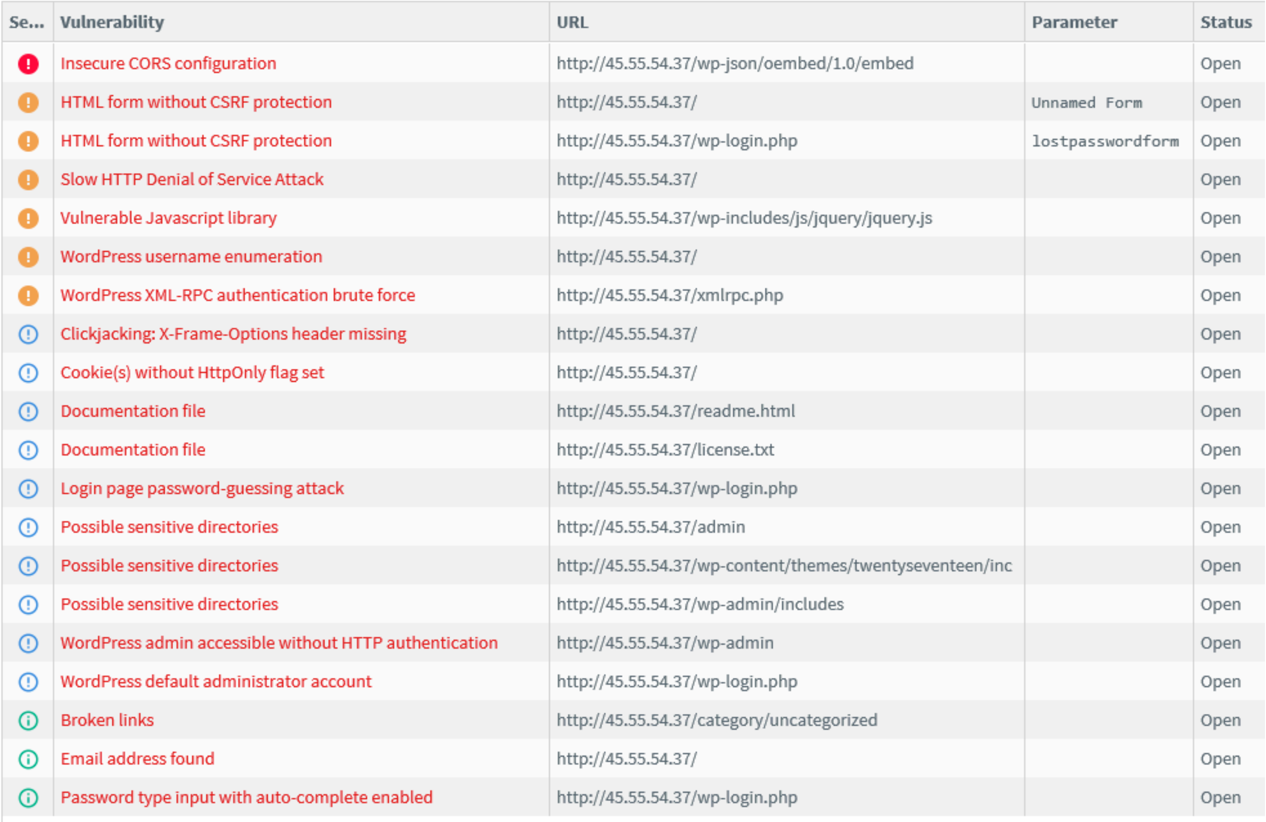
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Sample scan data

I tested Acunetix against a number of different websites running open source, commercial, and custom web applications. As expected, the scanning speeds and results differed.

For testing, I have set up a fresh instance of the latest Ubuntu server with the following specs: 8GB RAM, 4 CPU and 80 GB SSD disk. As a CMS of choice, I used WordPress 4.8 without the usual pre-installed plugins.

The scan ran for 1h 48m 30s, the average response time was 218ms and Acunetix generated 195,084 requests. From the payload perspective, the initially empty target systems’ access.log now showed a size of 44MB. Below is a screenshot of the issues discovered, ranked from high-risk to informational:



Se...	Vulnerability	URL	Parameter	Status
🔴	Insecure CORS configuration	http://45.55.54.37/wp-json/oembed/1.0/embed		Open
🟠	HTML form without CSRF protection	http://45.55.54.37/	Unnamed Form	Open
🟠	HTML form without CSRF protection	http://45.55.54.37/wp-login.php	lostpasswordform	Open
🟠	Slow HTTP Denial of Service Attack	http://45.55.54.37/		Open
🟠	Vulnerable Javascript library	http://45.55.54.37/wp-includes/js/jquery/jquery.js		Open
🟠	WordPress username enumeration	http://45.55.54.37/		Open
🟠	WordPress XML-RPC authentication brute force	http://45.55.54.37/xmlrpc.php		Open
🔵	Clickjacking: X-Frame-Options header missing	http://45.55.54.37/		Open
🔵	Cookie(s) without HttpOnly flag set	http://45.55.54.37/		Open
🔵	Documentation file	http://45.55.54.37/readme.html		Open
🔵	Documentation file	http://45.55.54.37/license.txt		Open
🔵	Login page password-guessing attack	http://45.55.54.37/wp-login.php		Open
🔵	Possible sensitive directories	http://45.55.54.37/admin		Open
🔵	Possible sensitive directories	http://45.55.54.37/wp-content/themes/twentyseventeen/inc		Open
🔵	Possible sensitive directories	http://45.55.54.37/wp-admin/includes		Open
🔵	WordPress admin accessible without HTTP authentication	http://45.55.54.37/wp-admin		Open
🔵	WordPress default administrator account	http://45.55.54.37/wp-login.php		Open
🟢	Broken links	http://45.55.54.37/category/uncategorized		Open
🟢	Email address found	http://45.55.54.37/		Open
🟢	Password type input with auto-complete enabled	http://45.55.54.37/wp-login.php		Open

As a comparison, I've tested the same WordPress setup but this time with AcuSensor enabled. This time the duration of the scan was 4 hours and 46 minutes, during which 397,545 requests were generated.

The scan found another potential high risk vulnerability (*allow_url_fopen*, which was on), 15 medium-risk vulnerabilities, 6 low-risk ones and 22 issues that were labeled as informational.

Reporting

Acunetix delivers reports in two sections. One focuses on standard reports such as quick, developer, executive summary and list of affected items, while the other contains compliance reports.

The latter are aimed for the following compliance bodies and standards:

- CWE/SANS Top 25 Most Dangerous Software Errors
- The Health Insurance Portability and Accountability Act (HIPAA)
- International Standard – ISO 27001
- NIST Special Publication 800-53
- OWASP Top 10 – 2013 (as a side note, OWASP announced that they plan to release the final OWASP Top 10 – 2017 in July/August this year)
- Payment Card Industry (PCI) DSS 3.2
- Sarbanes Oxley Act
- DISA STIG Web Security
- Web Application Security Consortium (WASC) Threat Classification

All reports can be downloaded in PDF and HTML formats, but the downloaded reports will always have the same generic name (e.g. Developer.pdf for a Developer report).

So, if you're downloading the same type of report for different targets, you'll have to make the effort to change the name, lest you end up with many files that you can't tell apart at first glance.

Documentation

Acunetix hosts all of its documentation online, and the product manual is extensive. I also suggest perusing the "Docs & FAQs" section located under the Blog menu of the Acunetix website. There you'll find some interesting posts on specific usage scenarios, third party product integrations, and more.

Pricing

Let's start with the on-premise edition. Acunetix is available as a one year or perpetual license in four different tiers, each depending on the number of concurrent scans and/or users.

One year licenses vary from $2,495/yr to $6,995/yr, while perpetual licenses are approximately double that price.

Yearly subscriptions for the online edition start from $345 for 1 target (web or network) + 3 free Network targets and the amount rises depending on the number of targets you need.

Final thoughts

I've used Acunetix a number of times over the last decade, and I like what I see in this latest version. The web-based interface makes it run smoother, and also unlocks the potential of offering role-based access to multiple users within the organization.

Every aspect of the product can be fully customized to optimize the scans. As far as I'm concerned, AcuSensor should be used by default, as it expands the reach of the analysis and can provide interesting and helpful findings.

Berislav Kucan is the Director of Operations at (IN)SECURE Magazine and Help Net Security (www.helpnetsecurity.com).

Events around the world

BruCON 2017

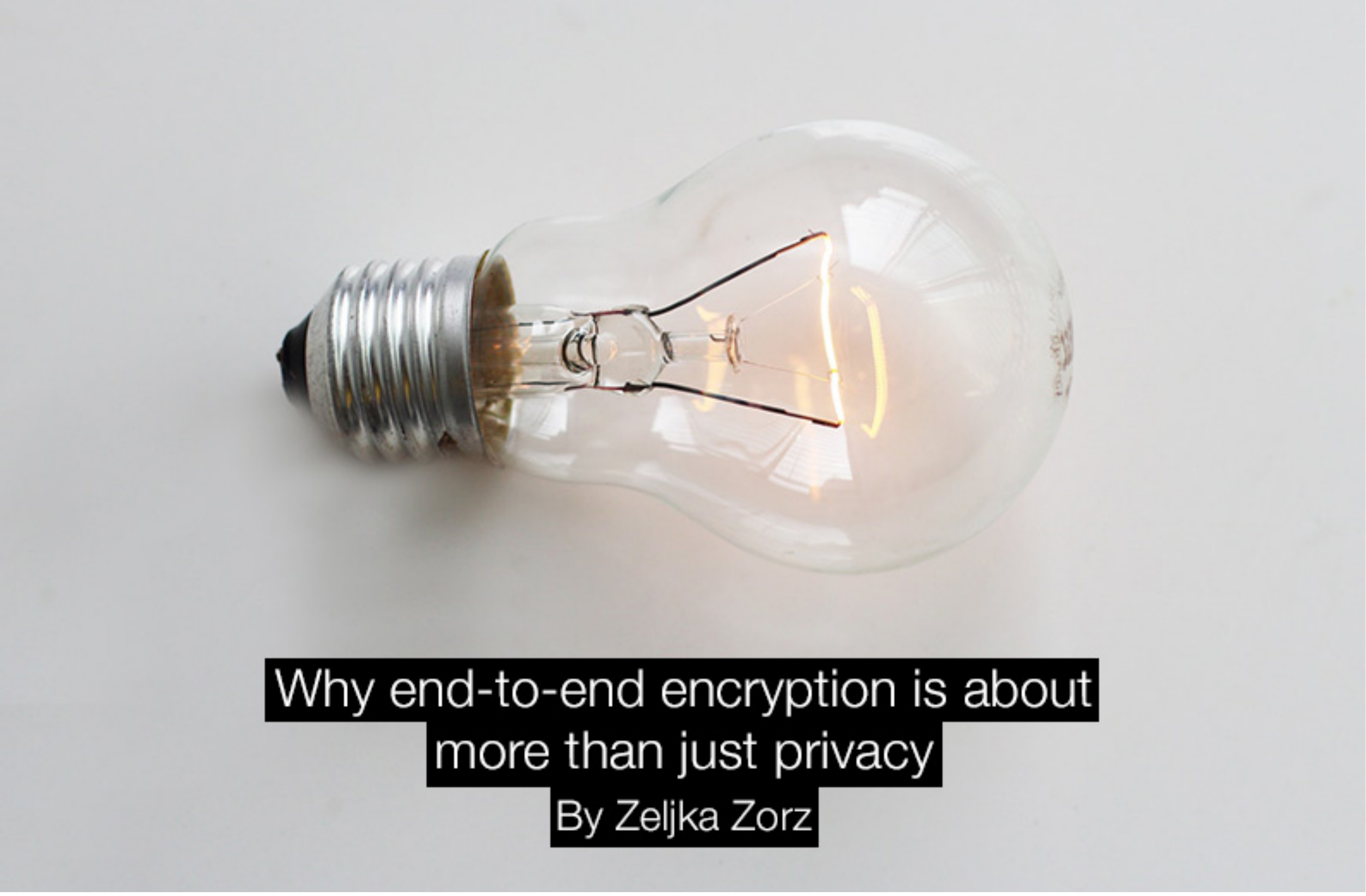
2017.brucon.org - Belgium / 5 - 6 October 2017

BruCON is an annual security and hacker conference providing two days of an interesting atmosphere for open discussions of critical infosec issues, privacy, information technology and its cultural/technical implications on society. Organized in Belgium, BruCON offers a high quality line up of speakers, security challenges and interesting workshops.

IFINSEC 2017

www.ifinsec.com - Turkey / 14 - 15 November 2017

IFINSEC Financial Sector IT Security Conference and Exhibition is one of the most important conferences in EMEA region on IT security, information security, network security, application security, database security, mobile security and cloud security technologies and solutions for the financial sector. IFINSEC presents a platform where speakers share their experience, knowledge, vision and future forecasts. The language of the conference speeches will be English or Turkish. Simultaneous translation to Turkish or English will be available.



Why end-to-end encryption is about more than just privacy

By Zeljka Zorz

The question of whether regular people need end-to-end encryption will surely be debated for quite some time. But for Alan Duric, CEO and co-founder of Wire, the question can only have a positive answer.

As he told the audience at the FSec security symposium in Varazdin, Croatia, end-to-end encryption is about more than just privacy – it is also critical for protecting business data, and our very lives and limbs as the Internet of Things becomes the norm.

With its eponymous open source, encrypted IM offering, Wire's (and Duric's) goal is to disrupt the privacy selling market headed by Google and Facebook, and offer secured communication to private users and organizations.

The latter have come to realize that they need to protect their intellectual property from industrial espionage, their own internal information (political parties, corporations involved in mergers and acquisitions, etc.), and their clients' information (lawyers, healthcare organizations). And, with the imminent advent of EU's General Data Protection Regulative (GDPR) and the heavy fines that will (finally!) be imposed on those who fail to protect their customers' information, companies should definitely be eyeing workable solutions for end-to-end encrypted communications.

Spreading the word about privacy

Duric says the information security community should work on raising awareness about the need for privacy among regular people/Internet users.

At the moment these efforts are being obstructed by Internet conglomerates, he notes, just as the tobacco industry hindered awareness raising about the dangers of smoking and passive smoking all those years ago.

But those who were fighting the good fight persevered, and today everybody knowns about those dangers, and can choose for themselves whether the option is worth the risk.

COMPANIES THAT SELL SECURITY NEED TO FIND GOOD WAYS TO DO IT

People need to be aware that the great power Internet giants have over us could lead to great abuses, and ask themselves what can go wrong if they choose not to protect their communications.

But also, companies that sell security need to find good ways to do it – adapt methods that have worked in the past for other vendors, both for physical and digital security. “We are working against human nature here,” he noted.

Finally, companies must not forget that the offered products must, above all, be usable, or the whole thing will not work in the long run.

Commitment to privacy and communication security

Ultimately, if E2E encryption technology is implemented well and regularly tested for security holes, even if the service provider or the cloud is compromised, the encryption keys are safely stored on your own devices.

Duric is aware that E2E encryption is not a silver bullet, but there’s no denying that it makes life harder for those who need to break it in order to get the data.

And from the vantage point of being included, in advisory capacity, into discussions by a number of non-governmental think tanks on the topic of encryption, he seems to believe that governments are slowly moving away from the idea of encryption backdoors, towards targeted compromise of suspects’ devices via exploits/malware.

Wire’s own commitment to privacy and communication security is backed by most of their choices:

- Open source code so that it can be independently audited
- Independent security reviews of the encryption protocol specification, implementation, and the complete solution, as well as regular code security audits for each major version of the solution
- Location of company (Switzerland) and servers (Germany, Ireland), meaning its users have the protection of Swiss and EU data protection laws
- Verifiable E2E encryption
- Minimal amount of collected data (and metadata) from users, short retention (72 hours) of the latter
- You can register an account with just your email address (and not reveal your phone number).

Wire has started by meeting the needs of the individual users, but have lately been concentrating on bringing end-to-end encrypted chats, file sharing and calls to businesses.

The company has released Teams – i.e. “Wire for work” – in beta this July, and Duric tells me there is a lot of interest in it, especially from European businesses and organizations, as the alternatives are mostly provided by companies outside of the EU.

What’s next?

As human-to-machine secured communication has been achieved, now is the time to start working on securing machine-to-machine communication, he says.

In machine-to-machine communication, integrity of the communication is what’s most important, especially when you consider the many nightmare scenarios that could happen as attackers get in the middle and can fiddle with connected devices, cars, etc.

“The stakes are definitely getting higher,” he concluded.

Zeljka Zorz is the Managing Editor of (IN)SECURE and Help Net Security (www.helpnetsecurity.com)

INTRODUCING
COGNITO™
AI that reduces SOC workloads by 29X, enabling you to stop in-progress attacks.
VECTRA
Security that thinks.
vectra.ai
Black Hat
Booth 1460

Indepth insights
into the
Human Factor
https://get.clt.re/report

Journey to the cloud: Automated, continuous, visible

By Aaron McKeown

A migration to a public cloud environment is a massive undertaking for any organization, no matter the scale. The journey rarely comes without challenges. However, doing it puts an organization in prime position to apply machine learning to its vast database - not only to keep it in check, but provide innovation for its customers.

Any migration journey requires an extensive planning phase beforehand, to determine how data transfer will occur without slowing down growth and the speed of innovation. Many modern product teams operate at a blistering pace, which requires the implementation of a culture shift for the security team, accelerating to keep up with product teams.

For many security teams, this cultural shift will necessitate working in cross-functional teams, building out product roadmaps, communicating effectively – essentially building and delivering “Security as a Service.” By defining a set of services, building clear lines of communication and setting expectations during this process, you can essentially operate as a supplier within your organization’s walls.

Security teams need to enable the organization as a whole to do what they need to do in a timely manner. The goal of many of these teams is to help their respective product teams improve their security posture, deliver faster and reduce cost. At the same time, it’s important to give product teams the autonomy to choose the technology, practices, tools and processes they use to build, deploy and operate their software. You can do so by providing a complete security framework and standard patterns for product teams to utilize. Standard patterns are important in order to remain automated, accelerated, and on-demand.

When growing environments at a rapid rate, keeping visibility across them is extremely important. An innovative hosting provider environment can be a double-edged sword, given that configuration drift and sprawl can quickly became an issue. You can offset this by building an account creation process, which is well understood by all, and implementing a logging service enabled across all accounts, without any exceptions.

Making operational visibility a design criteria is also instrumental in ensuring sprawl is kept in check. Again, instilling a mindset shift in your development teams, through assigning account owners and technical leaders for each account, is critical in order to get them invested.

You can ensure further buy-in by demonstrating how they can use the tools and how, with small changes, they can make the environments they own more secure.

As systems are constantly evolving at an ever-increasing rate, the amount of data flowing within an environment is increasing proportionally. Manual processing of security events is becoming increasingly difficult when organizations need to deal with ever-increasing data volumes and a growing number of data sources. There is a need to separate the useful from the useless information that is hidden inside log sources.

Acting quickly on this information is incredibly important in an agile environment. Without advancements in AI and machine learning it is not possible to keep all of this data in check.

During the migration process, many organizations will often find early on that they have exceeded the current limits of existing technologies, which are unable to deal with the substantial data transfer needed between the former and new hosting environments.

Subsequently, many will need to develop new methods for transferring large amounts of data. VPN as a structure is a good starting point, which can then be built on. When building a new transfer method, it is possible to maintain security while also facilitating high throughput traffic.

An encryption policy should center on two main principles: data needs to be encrypted in transit and at rest. Consider, too, the connectivity of both inbound and outbound traffic, how to protect your environment from cyber attacks including SQL injection, Cross Site Scripting and DDoS, whilst simultaneously creating an agile environment that can grow to scale. By collaborating with security vendors, you can establish first-rate practice environments – extending them to their limits.

SEEKING OUT PARTNERS THAT ARE ACTIVELY PURSUING DEVELOPMENT IN THE FIELDS OF AI AND MACHINE LEARNING FROM A SECURITY PERSPECTIVE IS BECOMING A BASELINE REQUIREMENT

That said, to create security services which are able to scale rapidly, you need to collaborate with security vendors so that, together, you can build an exceptional infrastructure. To achieve this, you need to find security vendors that will be your security partners.

Engage with these partners at all levels, from their global executives through to local account management and R&D teams. Seeking out partners that are actively pursuing development in the fields of AI and machine learning from a security perspective is becoming a baseline requirement. Ask them when they're going to build machine-learning capabilities into their management infrastructure.

By doing so, you can ensure a shared investment in and responsibility for security between your organization and your security partners.

At Xero, we followed our hosting provider's framework quite closely. One of its design principles was to apply security to all layers, meaning that rather than running security appliances at the edge of your infrastructure, you use firewalls and other security controls on all of the resources. When developing a defense-in-depth infrastructure, it's important to consider three layers: the first being system security. Starting with hardened machine images, deploy dynamic Host Based Security, and use best practice configuration for Identity and Access Management roles and credentials. Use a dedicated identity account in conjunction with well-defined cross account roles configured, ensuring multi-factor authentication is used by default within the hosting provider and all remote access systems.

Secondly, for the layer of data security, ensure all data is encrypted at rest, using a principle of least privilege and deploying a strong user authentication system. Use an encryption key management service as well as a dedicated, highly restricted account for both key management and logging services. For the network security layer, where you need to ensure encryption in transit, use security groups, and deploy a threat protection layer for ingress/egress filtering.

When communication uses HTTPS, use security groups and run a dedicated threat protection layer with proxy services for egress. An additional final layer is to monitor and alert, which is the aggregation and analysis of all component layers.

Leveraging the considerable investment a hosting provider makes in platform services will help your organization to build and deploy software with shorter delivery timeframes. This allows businesses to release new software faster, and to experiment with these features in new ways.

Businesses in general need to be more aware of security needs and prepare for the future of machine learning. Moving to AWS can be the technological enabler to help companies do all of these things. Keeping information secure is not the responsibility of a single person – it's a mindset that enables businesses to be both fast and secure.

Aaron McKeown is Head of Security Engineering and Architecture at Xero (www.xero.com), a cloud-based accounting software company with more than 1,000,000 subscribers globally. Aaron is driving the Xero Cloud Security strategy and is responsible for the implementation and management of technical security on the the Xero hosting platform inside Amazon Web Services. Aaron has more than 20 years experience in the architecture and management of complex solutions within the utilities and software industries.

How to catch a phish

By Rush Taggart

Of all the data breaches that occurred last year, two-thirds were enabled by compromised credentials. The most important asset for criminal hackers to obtain during a data breach is money, which generally comes in the form of credit card information, and compromised credentials will, in many cases, lead directly it. That's a big burden for the payment card industry.

With so much publicly available personal data, spear phishing emails, messages and phone calls match our expectations so closely that it's becoming more and more challenging to detect them. The emails can be incredibly deceptive and include content that is likely familiar to the recipient, e.g. company logo, the name of a colleague, information that may be timely to the events within a company, and so on.

It's easy to be fooled by a phishing email, especially if one hasn't been trained on the methods for spotting them. Unfortunately, we must be wary of every single email we receive. If you receive an unexpected email from a sender that may even be familiar to you, like a colleague or manager, you should still be suspicious.

To maintain this vigilance, slow down, become observant and never click on any link without checking its content for expected domain names. All it takes is one click on a malicious link to put your entire network in harm's way. In the 2015 Anthem breach, one malicious link was clicked on by one system administrator and it compromised 90 systems, leaking more than 78 million identities.

Data breaches will occur as long as there is information to steal. Organizations must monitor their systems every single day, for threats, for unexpected traffic in or out, and worse, active exfiltration of sensitive data. There are a handful of tactics every business and organization should be implementing as part of their data security plan.

Strip out spam

It's tough enough to monitor the volume of emails you receive from the people you do know, you might as well strip out the messages that aren't necessary to your day-to-day. Block incoming emails before they even get to your employees' inboxes with Domain-based Message Authentication, Reporting & Conformance (DMARC) standard. DMARC will help to automate the process, remove a level of human error and ease the obligation of having to evaluate the legitimacy of each email that does make it to your inbox, and can help instruct you on how to handle suspicious material.

Block phishing and malware where you can

Companies can protect their sensitive information by working with vendors like threat intelligence providers. They can provide real-time reports of malicious links, files and phishing emails. This will also help you and your security team keep on top of trending scam tactics, so you aren't caught off-guard by a new attempt that you haven't experienced yourself. Filter your email through a scanning vendor who is in the business of identifying and blocking malware before you receive it.

Monitor your systems daily

While companies may have a data breach impact reduction plan in place, a major responsibility that's overlooked is the need for teams to watch their systems every single day. How is it that major companies can go months without noticing irregular or malicious activity?

If you are watching your network every day and you happen to notice unusual activity, then you're only dealing with one day's worth of work. If you allow your system(s) to go unmonitored for long periods of time, then you may have to clean up the consequences of a much larger breach for years to come.

Teach your employees good practices for detecting phishing scams

Emails will get through your firewalls and into your network, and when they do, you can't expect your employees to identify every single one. But you can certainly help to better prepare them by providing the right defense knowledge. For example, teach your teams to recognize the obvious telltale signs like spelling errors (subtle or glaring) that can be present in phishing emails.

Case studies of recent phishing campaigns, successful or unsuccessful, make great timely examples of what your teams can look for, so over time make sure you're constantly communicating reminders to be defensive when it comes to their inboxes. It should become natural for your teams to be watchful of the attachments or links in emails.

Implement security solutions for when you are breached

Though the combination of the actions above is an effective one, sometimes this level of preparation still isn't enough. Say an email gets through your firewalls, through your malware detectors and into the hands of an employee who, while trained to identify the signs of a scam, opens and interacts with a creatively-crafted, malicious email. Your network has become vulnerable and your data accessible to criminals. Your data better be guarded.

For the data that's traveling through or sitting on your network, like credit card information, don't let it exist without protection. Give it a cloak of security with solutions like point-to-point encryption (P2PE) and tokenization.

Phishing scams are just one of many malicious methods used to get access to a network. Make sure you're maintaining awareness of scamming trends, monitoring your systems every day and teaching your teams about threats, then you'll be on your way to better protecting your business's information and your customers' credit card data.

Don't let your network become weakened by avoiding the obvious measures that help defend an organization.

Rush Taggart is the CSO at CardConnect (cardconnect.com).

NTT Security Strategic Consulting | Managed Secuirty | Technical Consulting Overview

The Cyber Skills Shortage

The Cyber Skills Shortage (also known as The Cyber Skills Gap) is a growing global problem and an important issue which organizations need to be made aware of in order for them to be able to deal with the issue by either investing in internal resources our outsourcing security services to a trusted security partner. Threats are not going away, and globally, the information security workforce shortfall is increasing – a combination of facts that continues to trouble CIOs and CISOs.

This lack of internal resource to keep pace with a growing problem means that it's no longer possible for many organizations to tackle all aspects of information security management in-house. And in addition to the growing frequency and complexity of threats, the regulatory landscape is also changing. For example, the European Union is set to impose tough new standards in 2018 (General Data Protection Regulation), along with punitive fines for failing to protect data.

Changing threats require a range of skills

Today's organizations are facing security challenges that didn't exist last year, let alone a decade ago. And with cybercrime now a serious business, organizations are discovering new issues to manage every day.

Stretched IT departments are struggling to keep on top of information security and the consequences can have a serious impact on the vulnerability of the business.

We need more resources to manage this. And we need the right resources – not IT generalists, but people with forensic skills, industry expertise, incident handling experience, an understanding of mobile security demands, up-to-date compliance knowledge, experts in cloud security and people with the analytical skills and experience to see what others might miss.

The threat landscape is evolving too quickly for organizations to keep up. And the broadening footprint of cloud based services, mobile devices, big data, and the Internet of Things is adding to the problem. There are simply not enough qualified information security experts entering the workforce and there's no silver bullet in terms of training internal resources or hiring new people to alleviate the problem.

Information security needs to be seen as a career choice and there must be greater awareness in schools and colleges globally in order to attract more people into the profession. Until then, organizations need to think carefully about a future that relies on getting by with existing resources versus outsourcing some or all of their security operations to a trusted advisor. There's never been a more important time to make that decision.

Outsourcing security services to a Managed Security Services Provider

A fully outsourced service is no longer just a case of managing complex networks from a 'lights on' perspective. It's about providing a fully managed solution which proactively protects your organization against multiple, complex security threats – around the clock – and providing added value such as insight and analytics, over and above managing your devices. Choosing a third party can mean gaining access to their collective global knowledge and systems as well as their highly-experienced people.

Security services providers keep their fingers on the pulse of current and next generation threats and vulnerabilities, ensuring they deliver effective security monitoring, detection and response capabilities to their clients. They should also have access to valuable regional and global threat intelligence all of which should help them deliver an added value service above and beyond what you may be able to achieve through your in house security team.

Enlisting an agile Managed Security Services provider such as NTT Security enables you to be proactive and keep one step ahead of the game, rather than simply reacting to what has already happened. NTT Security provides optimized managed security services to manage the most complex of infrastructures and diverse applications: on-premise, in the cloud or through a hybrid model.

For more information, download "Cyber Skills Shortage" today.
https://www.nttsecurity.com/-/media/nttsecurity/files/resource-center/what-we-think/global_thought_leadership_skills_shortage_uea_v4.pdf

About NTT Security

NTT Security is the specialized security company of NTT Group. With embedded security we enable Group companies (Dimension Data, NTT Communications and NTT DATA) to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of consulting and managed services for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more.