[+] (IN)SECURE Magazine

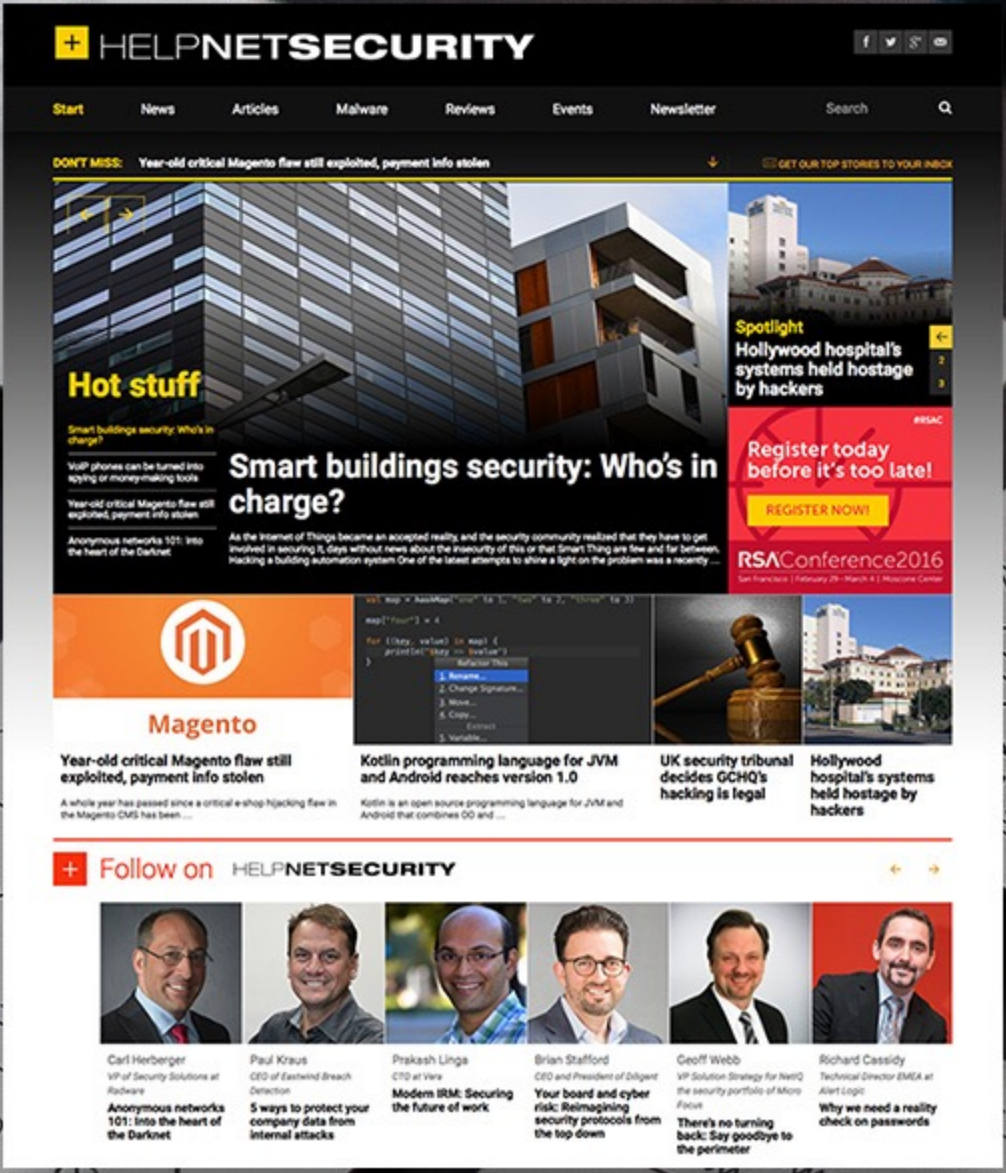
Issue 49, 02/2016

PRIVACY BY DESIGN: WHAT IT IS AND WHERE TO BUILD IT

BUILDING AND IMPLEMENTING AN INCIDENT RESPONSE PROGRAM FROM SCRATCH

CYBER SECURITY CONTROL MATURITY: WHAT IT IS, AND WHY YOU SHOULD CARE

THE SLINGS AND ARROWS OF ENCRYPTION TECHNOLOGY



DON'T MISS: Year-old critical Magento flaw still exploited, payment info stolen

Hollywood hospital's systems held hostage by hackers

Register today before it's too late!

RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Hot stuff

Smart buildings security: Who's in charge?

VoIP phones can be turned into spying or money-making tools

Year-old critical Magento flaw still exploited, payment info stolen

Anonymous networks 101: Into the heart of the Darknet

Smart buildings security: Who's in charge?

As the Internet of Things became an accepted reality, and the security community realized that they have to get involved in securing it, days without news about the insecurity of this or that Smart Thing are few and far between. Hacking a building automation system One of the latest attempts to shine a light on the problem was a recently ...

Year-old critical Magento flaw still exploited, payment info stolen

A whole year has passed since a critical e-shop hijacking flaw in the Magento CMS has been ...

Kotlin programming language for JVM and Android reaches version 1.0

Kotlin is an open source programming language for JVM and Android that combines OO and ...

UK security tribunal decides GCHQ's hacking is legal

Hollywood hospital's systems held hostage by hackers

Carl Herberger
VP of Security Solutions at Radware
Anonymous networks 101: Into the heart of the Darknet

Paul Kraus
CEO of Eastwind Breach Detection
5 ways to protect your company data from internal attacks

Prakash Linga
CTO at Vera
Modern IRM: Securing the future of work

Brian Stafford
CEO and President of Diligent
Your board and cyber risk: Reimagining security protocols from the top down

Geoff Webb
VP Solution Strategy for NetIQ the security portfolio of Micro Focus
There's no turning back: Say goodbye to the perimeter

Richard Cassidy
Technical Director EMEA at Alert Logic
Why we need a reality check on passwords

TABLE OF CONTENTS

(IN)SECURE Magazine 49
CONTRIBUTORS LIST

- **Ben Desjardins**, Director of Security Solutions at Radware
- **Wolfgang Kandek**, CTO at Qualys
- **Tom Kellermann**, Chief Cybersecurity Officer at Trend Micro
- **John Kuhn**, Senior Threat Researcher at IBM X-Force
- **Zoran Lalic**, Senior Security Engineer at a large corporation
- **Fan Lei**, Information Security Manager of Americas at Takeda Pharmaceuticals
- **John Smith**, Principal Solution Architect at Veracode
- **Shay Zandani**, Founder and CEO of Cytegic.

Visit the magazine website at www.insecuremag.com

Contact

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

Distribution

(IN)SECURE Magazine can be freely distributed in the form of the original, non-modified PDF document. Distribution of modified versions of (IN)SECURE Magazine content is prohibited without permission.

Security world

Hollywood hospital's systems held hostage by hackers

The Hollywood Presbyterian Medical Center, an "acute-care facility" located in Los Angeles, has had its computer systems compromised by hackers. The attackers are asking for 9,000 Bitcoin (approximately $3.6 million) in exchange for giving the hospital access to the systems again.

Not many details about the compromise have been shared, but it seems more than likely that computers and data storage devices have been infected with crypto ransomware.

News of the attack started appearing on February 11, but it apparently started a week before that. The hospital's website and social media accounts haven't mentioned any problems in an attempt to try and keep the situation under wraps.

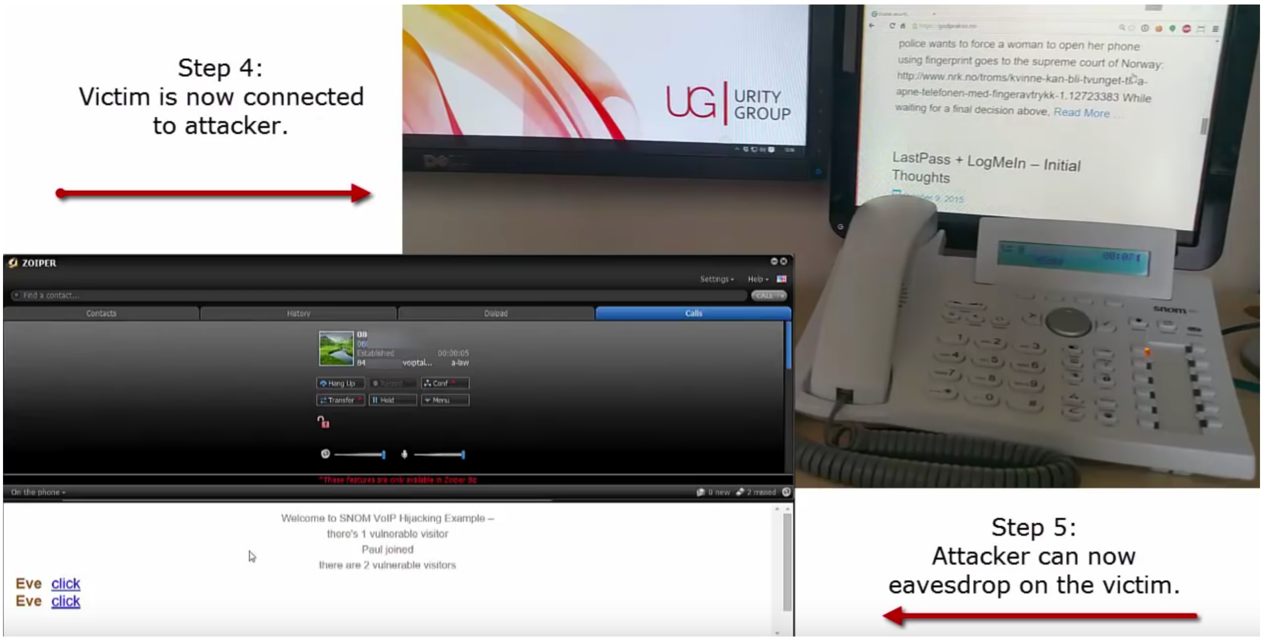
But the effect of the attack can definitely be felt. NBC Los Angeles reported that the hospital has taken down its entire network, and the staff and the departments are forced to communicate via fax.

Patients' medical records are inaccessible, and some of the hospital departments – namely Radiation and Oncology – have been temporarily shut down as they can't use their computers.

Emergency patients are being sent to other hospitals. Patients who have been examined and had medical tests done are forced to come to the hospital in person to pick up the results, as they can't be sent to them via email.

The only good news is that so far, there is no evidence that patients' medical records have been exfiltrated or accessed by the attackers.

But if this incident shows anything, it is how an organization's operations can be heavily disrupted by a cyber attack. In the healthcare industry this could, in certain situations, also lead to loss of life.


Step 4:
Victim is now connected
to attacker.

Step 5:
Attacker can now
eavesdrop on the victim.

police wants to force a woman to open her phone using fingerprint goes to the supreme court of Norway: http://www.nrk.no/troms/kvinne-kan-bli-tvunget-til-a-apne-telefonen-med-fingeravtrykk-1.12723383 While waiting for a final decision above, Read More ...

LastPass + LogMeIn – Initial Thoughts

Welcome to SNOM VoIP Hijacking Example –
thore's 1 vulnorablo visitor
Paul joined
there are 2 vulnerable visitors

Eve click
Eve click

VoIP phones can be turned into spying or money-making tools

A security vulnerability present in many enterprise-grade VoIP phones can easily be exploited by hackers to spy on employees and management, says security consultant Paul Moore.

In a less dangerous attack alternative, these compromised devices can also be made to covertly place calls to premium rate numbers operated by the attackers or their associates.

This vulnerability does not stem from a bug in the firmware, but from the fact that manufacturers of these phones often don't require authentication to be set in the default configuration.

When they do, they often provide an easily guessable default set of credentials, and when users set up new passwords, they often accept too short passwords.

Unfortunately, those who install these devices for companies frequently forget to harden them against attacks (by setting up authentication or changing the default passwords), believing them to be relatively safe as they are behind a strong firewall.

With the help of two colleagues, Moore has demonstrated how easy it is to compromise a company's VoIP phones, which are usually connected to same network that company computers are connected to.

The vulnerability is exploited via attack (JavaScript) code embedded in a site controlled by the attackers. Once the target visits the site using the company computer (e.g. is tricked into doing it through social engineering), the door is open for the attackers to take control of the VoIP phone located on the same network.

This allows the attackers to do anything they want with the phone: make, receive, and transfer calls, play recordings, upload new firmware, and turn the device into a covert spying tool.

Moore exploited the vulnerability on VoIP phones by German maker Snom, but says that they are by no means the only manufacturer whose devices are vulnerable to this kind of attack.

"If we look beyond the IP telephony sector to the industry as a whole, many companies ship devices which have no 'default' security… or permit the use of weak credentials which provide nothing more than a false sense of security," he noted, and urged vendors to disable all other functionality until a suitably-secure password is set to replace it if they are forced to supply devices with "default" credentials.

"A default configuration is rarely a secure configuration," he pointed out, and advised users and technicians tasked with setting up these devices to use strong passwords, network segregate the phones, restrict access to APIs, and regularly update firmware (and make sure to check whether the update forced a return to default settings).

Teenage admin of anonymous XMPP service arrested in connection to fake bomb threats

The teenage administrator of the Darkness.su XMPP service has been arrested by the French police, in connection to the wave of false bomb threats that were made against several French schools on January 26 and February 1, 2016, and later against educational institutions around the world.

The prosecutor wanted the 18-years-old Vincent L. to be indicted for conspiracy in the aforementioned events, but the high schooler has ultimately been indicted on only one count: refusal to provide the authorities with his computer encryption keys.

Darkness.su, when used by users who hide their IP address with the help of TOR or a VPN / proxy service, is considered to be completely anonymous. No IP addresses or communications are logged, and anyone can register an account without providing any personal information.

The youngster is not thought to be the author of the false bomb threats, but the ones who are – a group calling themselves Evacuation Squad – have possibly used his XMPP service to “phone” them in (the threats were made in the form of pre-recorded phone calls).

What they group definitely used the service for was to create an email account that has been tied to a Twitter account through which they took responsibility for the bomb alerts.

As reported by Numerama, the country’s penal code mandates a sentence of up 3 years in prison and a 45,000 Euros fine for anyone who is able to provide decryption keys for services that have been used to commit (or facilitate to commit) a crime but refuses to do so when asked by the judicial authorities.

That maximum sentence can be increased to 5 years in prison if that refusal results in the inability of the authorities to prevent further crimes or minimize their effect, which may be the case here if the Evacuation Squad still uses the service.

Still, that’s not what the youngster stands accused of. He has been temporarily released from custody, and is still unclear what the consequences of his refusal to hand over his computer keys to the authorities might be.

When it comes to cyber attack detection, IT pros are overconfident

A new study conducted by Dimensional Research evaluated the confidence of IT professionals regarding the efficacy of seven key security controls that must be in place to quickly detect a cyber attack in progress.

Study respondents included 763 IT professionals from retail, energy, financial services and public sector organizations in the U.S.

The majority of the respondents displayed high levels of confidence in their ability to detect a data breach even though they were unsure how long it would take automated tools to discover key indicators of compromise.

For example, when asked how long it would take automated tools to detect unauthorized configuration changes to an endpoint on their organizations’ networks, 67 percent only had a general idea, were unsure or did not use automated tools.

However, when asked how long it would take to detect a configuration change to an endpoint on their organizations’ networks, 71 percent believed it would happen within minutes or hours. Configuration changes are a hallmark of malicious covert activity.

“All of these results fall into the ‘we can do that, but I’m not sure how long it takes’ category,” said Tim Erlin, director of IT security and risk strategy for Tripwire. “It’s good news that most organizations are investing in basic security controls; however, IT managers and executives, who don’t have visibility into the time it takes to identify unauthorized changes and devices, are missing key information that’s necessary to defend themselves against cyber attacks.”

Government-mandated crypto backdoors are pointless, says report

If you needed another confirmation that government-mandated backdoors in US encryption products would only serve to damage US companies' competitiveness without actually bringing much benefit to the country's security, you only need to look at a recent report by security researchers Bruce Schneier, Kathleen Seidel, and Saranya Vijayakumar.

The report shows the results of a worldwide survey of encryption solutions and they are as follows:

- Of the 865 hardware or software products incorporating encryption, 546 (or two-thirds of the total) are from outside the US. Of these 546, 56% are available for sale and 44% are free, 66% are proprietary, and 34% are open source.
- 587 entities sell or give away encryption products. Of those, 374 (again, about two-thirds) are outside the US – at the top are Germany (112 products), the UK (54), Canada (47), France (41), and Sweden (33), but there is a considerable number of smaller countries like Algeria, Tanzania, Cyprus, etc. that produce at least one encryption product.

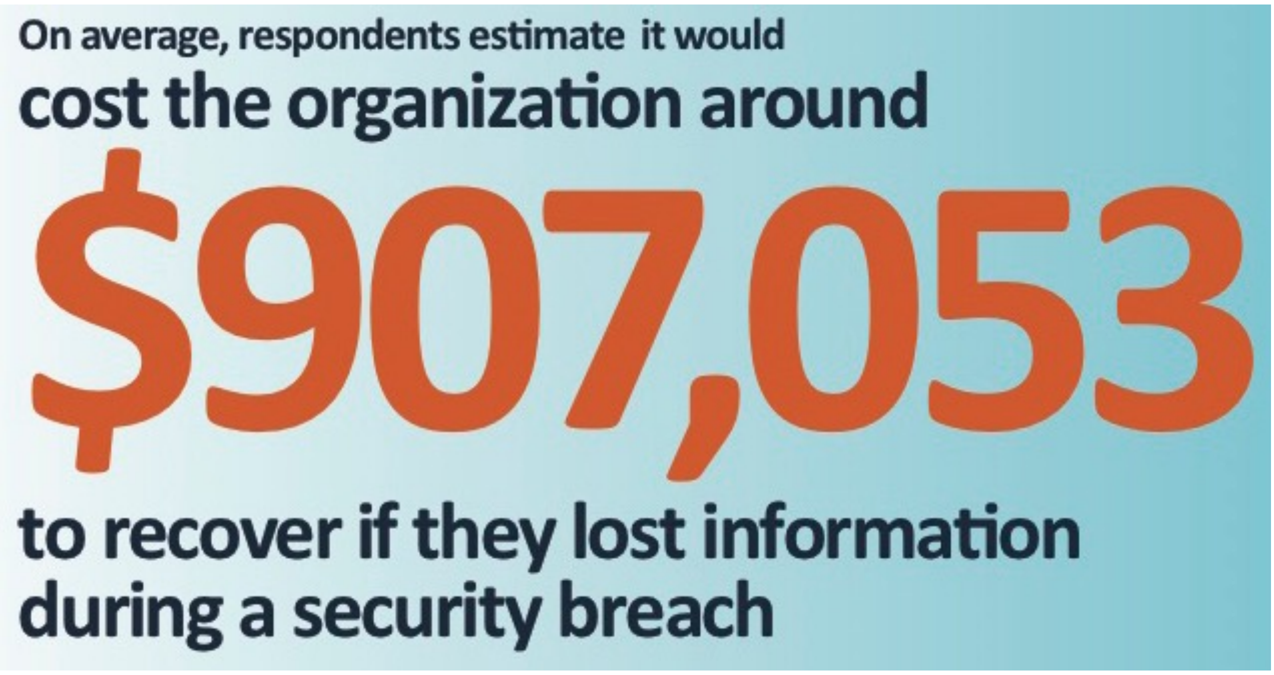
The quality of foreign encryption products is believed to be no better or worse than that of those created in the US, even though all are likely to have security vulnerabilities.

"With regard to backdoors, both Germany (with 113 products) and the Netherlands (with 20 products) have both publicly disavowed backdoors in encryption products. Another two countries—the United Kingdom (with 54 products) and France (with 41 encryption products) — seem very interested in legally mandating backdoors," the researchers noted.

"Some encryption products are jurisdictionally agile. They have source code stored in multiple jurisdictions simultaneously, or their services are offered from servers in multiple jurisdictions. Some organizations can change jurisdictions, effectively moving to countries with more favorable laws," they also pointed out.

With the "going dark" metaphor so loved by law enforcement already having been effectively discredited, the release of this report will hopefully add some much-needed insight into the "mandatory government backdoor" debate currently going on in the US, UK and several other countries.

This survey shows that criminals can easily switch to alternative encryption methods if they want to sidestep backdoors. "Any US law mandating backdoors will primarily affect people who are unconcerned about government surveillance, or at least unconcerned enough to make the switch. These people will be left vulnerable to abuse of those backdoors by cybercriminals and other governments," they concluded.



On average, respondents estimate it would cost the organization around

$907,053

to recover if they lost information during a security breach

What’s the real cost of a security breach?

The majority of business decision makers admit that their organization will suffer an information security breach and that the cost of recovery could start from around $1 million, according to NTT Com Security.

While 54% of those surveyed say information security is vital to their business and 18% agree that poor information security is the single greatest risk, 65% predict that their organs zation will suffer a data breach some time in the future. Respondents estimate a breach would take nine weeks to recover from and would cost $907,053, on average – even before the cost of any reputational damage, brand erosion and lost business are taken into consideration.

Decision makers estimate that 19% of their company’s remediation costs would be spent on legal fees, 18% on compensation to customers, 15% on third party resources and 15% on fines or compliance costs. The survey of 1,000 non-IT business decision makers in organizations in the UK, US, Germany, France, Sweden, Norway and Switzerland shows that recent high profile data breaches are hitting home.

According to the report, almost all respondents say they would suffer external and internal impacts if data was stolen in a security breach, including loss of customer confidence (69%) and damage to reputation (60%). One third of business decision makers also expects to resign or expects another senior colleague to resign as a result of a breach.

The report also shows that 41% of organizations have some kind of insurance to cover for the financial impact of data loss and a security breach, while 12% are not covered for either. However, 35% of respondents say they have a dedicated cyber security insurance policy, with 27% in the process of getting one. 52% have a formal information security policy in place, while 27% are in the process of implementing one.

Most IT pros have seen potentially embarrassing information about their colleagues

More than three-quarters of IT professionals have seen and kept secret potentially embarrassing information about their colleagues, according to new research conducted by AlienVault. The research, which surveyed the attitudes of more than 600 IT professionals into how they are treated, found that many are being called in to help get their colleagues out of embarrassing situations at the office.

Almost all the respondents (95%) said that they have fixed a user or executive’s personal computer issue during their work hours. In addition, over three-quarters (77%) said that they had seen and kept secret potentially embarrassing information relating to their colleagues’ or executives’ use of company-owned IT resources. The study highlights that very high levels of trust and responsibility are being placed on IT professionals over the course of their working lives.

Javvad Malik, security advocate at AlienVault, explains: “IT professionals are the superheroes of modern organizations. They are the people we call when things go wrong and who will drop everything to come and help us out if a problem occurs. But they are also the ones we trust with our secrets at work. If you click on a link that you shouldn’t have, or download a potentially dangerous file, then they are the people you’ll call. Some IT pros also have access to emails and data that has been quarantined due to its sensitive content. This gives them a clear vantage point into your private affairs, so it’s very important that you trust them.”

“Working in IT is a 24-hour-a-day career and the boundaries of the job often become blurred – be they the hours worked, or the actual work that needs to be done. Often working in isolation, IT teams are still considered to be supporting players in many workplaces, yet the responsibility being placed on them is huge. In the event of a cyber attack, network outage or other major issue, they will typically drop everything to fix the problem at hand.”

Government sector: largest revenue contributor for the global cyber security market

The cyber security market is predicted to reach close to $161 billion in revenue by 2020, according to Technavio.

“During the forecast period, the market share of North America is anticipated to witness a decline. Market shares of Europe, APAC, Latin America, and MEA are likely to increase during the same period. Stringent government regulations in Europe is likely to drive the adoption of cyber security solutions by enterprises until 2020. Increased penetration of internet in APAC countries such as India and China is also likely to increase the number of cyber-attacks over the next four years. The market is thus expected to witness a significant demand for security solutions until 2020,” said Amrita Choudhury, lead research analysts for IT security at Technavio.

“Rise in the use of mobile devices for personal and professional purposes is also expected to boost market revenues. Sectors such as retail, manufacturing, telecom, and BFSI will particularly witness higher adoption of cyber security solutions over the next four years,” added Choudhury.

Security flaws discovered in smart toys and kids’ watches

Rapid7 researchers have unearthed serious flaws in two Internet of Things devices:

- The Fisher-Price Smart Toy, a “stuffed animal” type of toy that can interact with children and can be monitored via a mobile app and WiFi connectivity
- The hereO GPS Platform, a smart GPS toy watch that allows parents to track their children’s physical location.

In both cases the problem was with the authentication process, i.e. in the platform’s web service (API) calls.

In the first instance, the API calls were not appropriately verified, so an attacker could have sent unauthorized requests and extract information such as customer details, children’s profiles, and more.

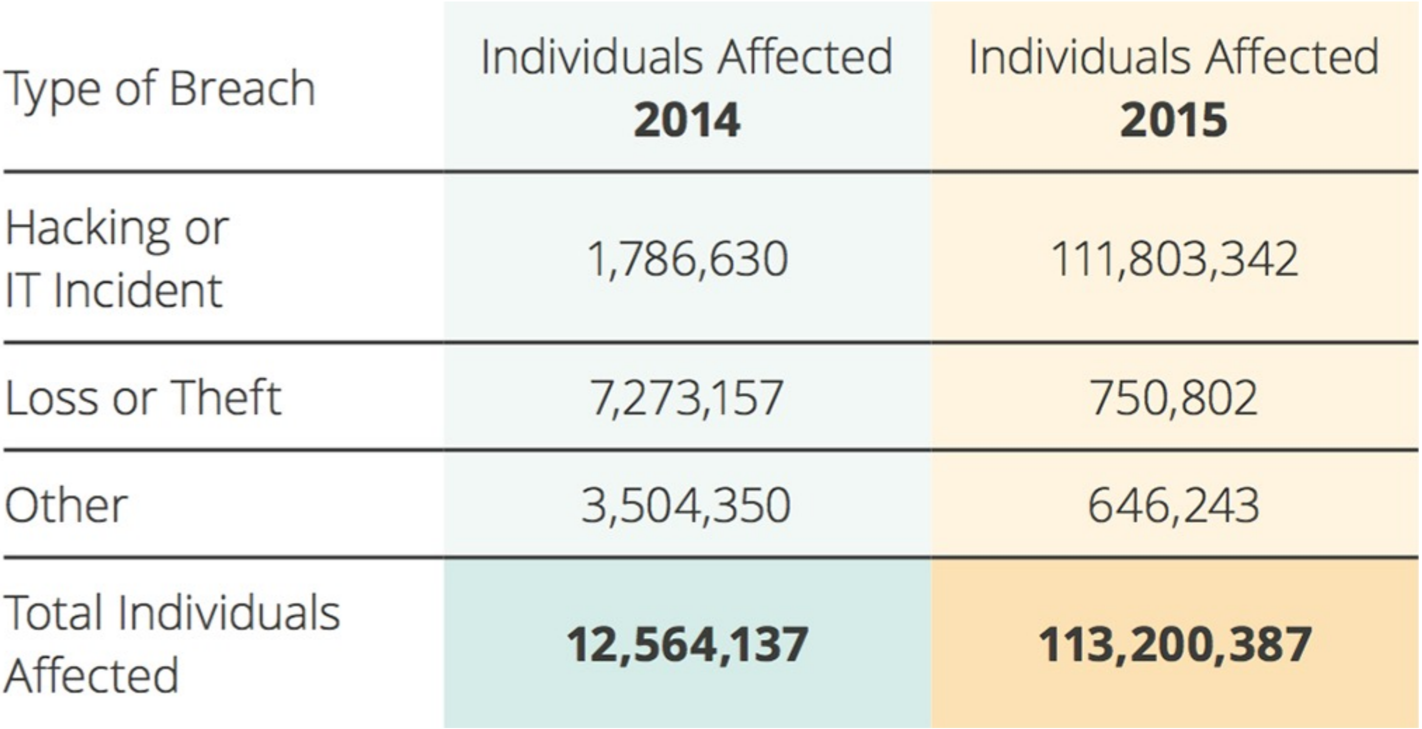
“Most clearly, the ability for an unauthorized person to gain even basic details about a child (e.g. their name, date of birth, gender, spoken language) is something most parents would be concerned about. While in the particular, names and birthdays are nominally non-secret pieces of data, these could be combined later with a more complete profile of the child in order to facilitate any number of social engineering or other malicious campaigns against either the child or the child’s caregivers.”

In the second instance, the flaw allowed attackers to gain access to the family’s group by adding an account to it, which would allow them to access the family member’s location, location history, etc.

“We have once again been able to work with vendors to resolve serious security issues impacting their platforms and hope that vendors considering related products are able to take note of these findings so that the overall market can improve beyond just these particular instances,” noted Mark Stanislav, manager of global services at Rapid7.

“This research helps to further underline the nascency of the Internet of Things with regard to information security. While many clever and useful ideas are constantly being innovated for market segments that may have never even existed before, this agility into consumers’s hands must be delicately weighed against the potential risks of the technology’s use,” he added.

“It’s great to see that Fisher Price has reacted so quickly to fix the security vulnerability found in its new Smart Toy. Just last year, the Vtech attack demonstrated how vulnerabilities found in connected toys not only pose a risk to children’s privacy, but also the information security of their parents who may use their details to buy add-ons for that toy or for related services,” commented Paul Farrington, senior solution architect at Veracode.



Type of Breach	Individuals Affected **2014**	Individuals Affected **2015**
Hacking or IT Incident	1,786,630	111,803,342
Loss or Theft	7,273,157	750,802
Other	3,504,350	646,243
Total Individuals Affected	**12,564,137**	**113,200,387**

Why cybercriminals target healthcare data

In 2015, one in three Americans were victims of healthcare data breaches, attributed to a series of large-scale attacks that each affected more than 10 million individuals.

The findings of the Bitglass 2016 Healthcare Breach Report come from analyzing data on the United States Department of Health and Human Services' "Wall of Shame," a database of breach disclosures required as part of HIPAA.

"The 80 percent increase in data breach hacks in 2015 makes it clear that hackers are targeting healthcare with large-scale attacks affecting one in three Americans," said Nat Kausik, CEO, Bitglass. "As the IoT revolution compounds the problem with real-time patient data, healthcare organizations must embrace innovative data security technologies to meet security and compliance requirements."

Among the most significant findings of the report was that in 2015, 98 percent of record leaks were due to large-scale breaches targeting the healthcare industry. These high-profile attacks were the largest source of healthcare data loss and indicate that cyber attackers are increasingly targeting medical data. Such breaches include the widely publicized Premera Blue Cross hack, involving 11 million customers, and the Anthem hack, which resulted in 78.8 million leaked customer records.

Why healthcare data?

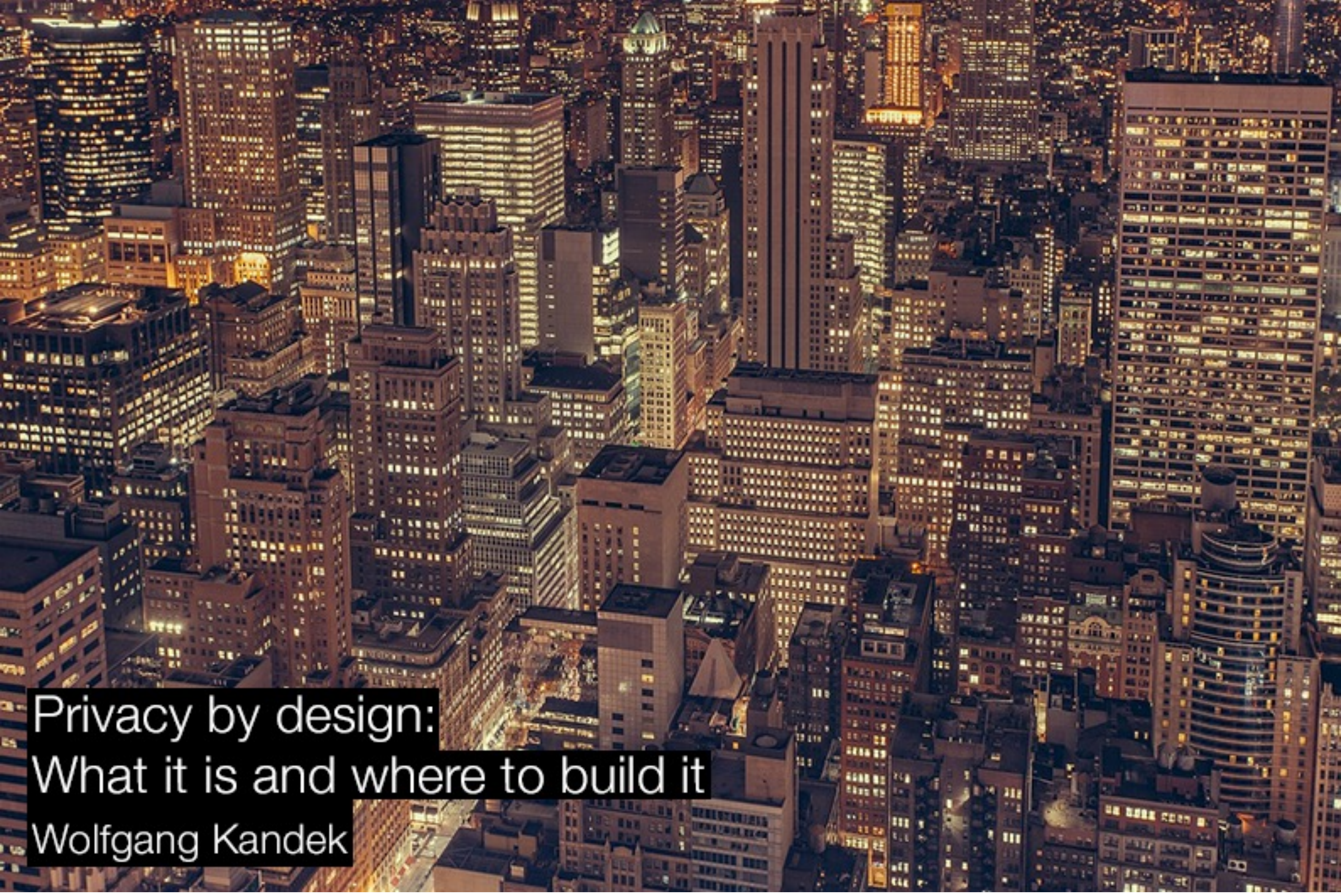
Protected health information (PHI) – which includes sensitive information such as Social Security numbers, medical record data, and date of birth — has incredible value on the black market.

A recent Ponemon Institute report on the cost of breaches found the average cost per lost or stolen record to be $154. That number skyrockets to $363 on average for healthcare organizations.

When credit card breaches occur, issuers can simply terminate all transactions and individuals benefit from laws that limit their liability.

However, victims have little recourse when subjected to identity theft via PHI leaks, and many are not promptly informed that their data has been compromised.

While criminals often leverage healthcare data for the purposes of identity theft, they can also leverage it to access medical care in the victim's name or to conduct corporate extortion.



Privacy by design: What it is and where to build it

Wolfgang Kandek

People tend to think about privacy in terms of the individual, but it is also critically important for the proper functioning of any business organization. This is being made increasingly relevant by the recent rise of personalization initiatives that rely on user data to recommend the right products or services to customers.

The failure to build privacy into these initiatives presents a major new data breach risk and thus an added risk to the company.

Organizations who wish to control this risk and take privacy seriously are adopting Privacy by Design principles, which were first developed in 2009 with the notion that privacy cannot be assured solely by compliance with regulatory standards.

IT security is, of course, the critical element here, and the great challenge is building security into different areas across the entire business. The three main areas to look at are:

Application development

Security's role within the development process has to become more prominent. Agile development – delivering software to the business faster and fixing problems as they arise – cannot be the inspiration for an organization's approach to security. Instead, an ethos of "measure twice, cut once" should guide security practices, with the added benefit that prioritizing app security quality will reduce the number of fixes that will be required later. This will improve the quality of the software and keep customer data private and secure.

Third party IT providers

When it comes to cloud services, the most important thing is ensuring that third parties are measuring up to their promises around security and data privacy. This should be outlined in any vendor contract, and it should be audited on a regular basis. Cloud security services can, of course, also be used to the organization's benefit, to help track devices and software updates to ensure that the organization's vulnerability management strategy is enforced.

IT asset management

Visibility into all IT assets has to be improved in order to help ensure security and build in more privacy controls. Monitoring mobile and other devices that are used for corporate tasks is generally an area in need of serious improvement, as is the need to make sure that security updates on these devices are routinely applied.

The number of patches for operating systems like Windows continues to grow. OS X had the highest number of CVE incidents published in 2015, and Adobe Flash, a popular attack target, frequently gets patches for zero-day vulnerabilities. When devices are outside the corporate network, keeping track of how patches have been applied becomes more difficult. Visibility is imperative.

If IT admins are able to continuously scan these assets – whether the devices are inside the corporate network or not – they can be sure that updates have been applied and that systems are as secure as possible. Mobile, PC and tablet devices can also have their security status checked to ensure that all the right steps have been taken. In the event of a lost device, data can be wiped.

There are well-known challenges affecting each of these areas. One is the sheer pace of change in the world of tech. The proliferation of cloud services, mobile computing and flexible working schedules means that companies have spread their IT assets much more widely.

VISIBILITY IS IMPERATIVE

Where data was once physically located on a desktop in a locked building and connected to servers sitting behind one big firewall, now it can be held on laptops that never see the inside of a company office. It may also never even be seen by IT teams to ensure that updates are implemented. This makes it much more difficult to enforce data security and data privacy across all the moving parts involved. Many companies are reliant on individuals "doing the right thing" as far as the business is concerned, which is never an adequate approach.

Meanwhile, the internal IT network is shrinking as more IT services get moved to the cloud. When this causes IT to lose some of the control over how data is managed and stored over time, it can make it more difficult to enforce the principles of Privacy by Design.

If a third party service provider makes a mistake or changes its approach to handling data without making this clear to the organization, then data privacy is jeopardized. Think of how many times Facebook, for example, has changed its privacy settings. Imagine this happening across multiple IT services for thousands of users and you can see the potential magnitude of the problem of losing control over the policies affecting sensitive information.

But the newest and perhaps greatest challenge is that all of these changes have coincided with an increasing public awareness of threats to customer privacy, driven in part by the rise of the personalization efforts mentioned earlier. Consumers are aware their information is being tracked and they want know that it's being protected and used responsibly. CIOs would be wise to listen to customer concerns and respond by employing Privacy by Design. All companies can do this by building security directly into their business processes, thereby showing that they genuinely respect data privacy.

Wolfgang Kandek is the CTO at Qualys (www.qualys.com), the leading provider of information security and compliance cloud solutions.

Harnessing artificial intelligence to build an army of virtual analysts

Zeljka Zorz

Enterprises of all types and sizes are continually probed and targeted by cyber attackers. It doesn't matter whether they are after the company's or their customers' information, or are trying to find ways in so that they can commit fraud, what matters is that many are succeeding.

So far, the security industry's attempts to stop them have not been enough, but maybe this situation will finally change.

An innovative combination

PatternEx, a startup that gathered a team of AI researchers from MIT CSAIL as well as security and distributed systems experts, is poised to shake up things in the user and entity behavior analytics market.

In early February, the company launched its Threat Prediction Platform, which combines the ability of machines to extract patterns from massive volumes of data with the capability of human analysts to understand the implications of these patterns.

Their goal was to make a system capable of mimicking the knowledge and intuition of human security analysts so that attacks can be detected in real time.

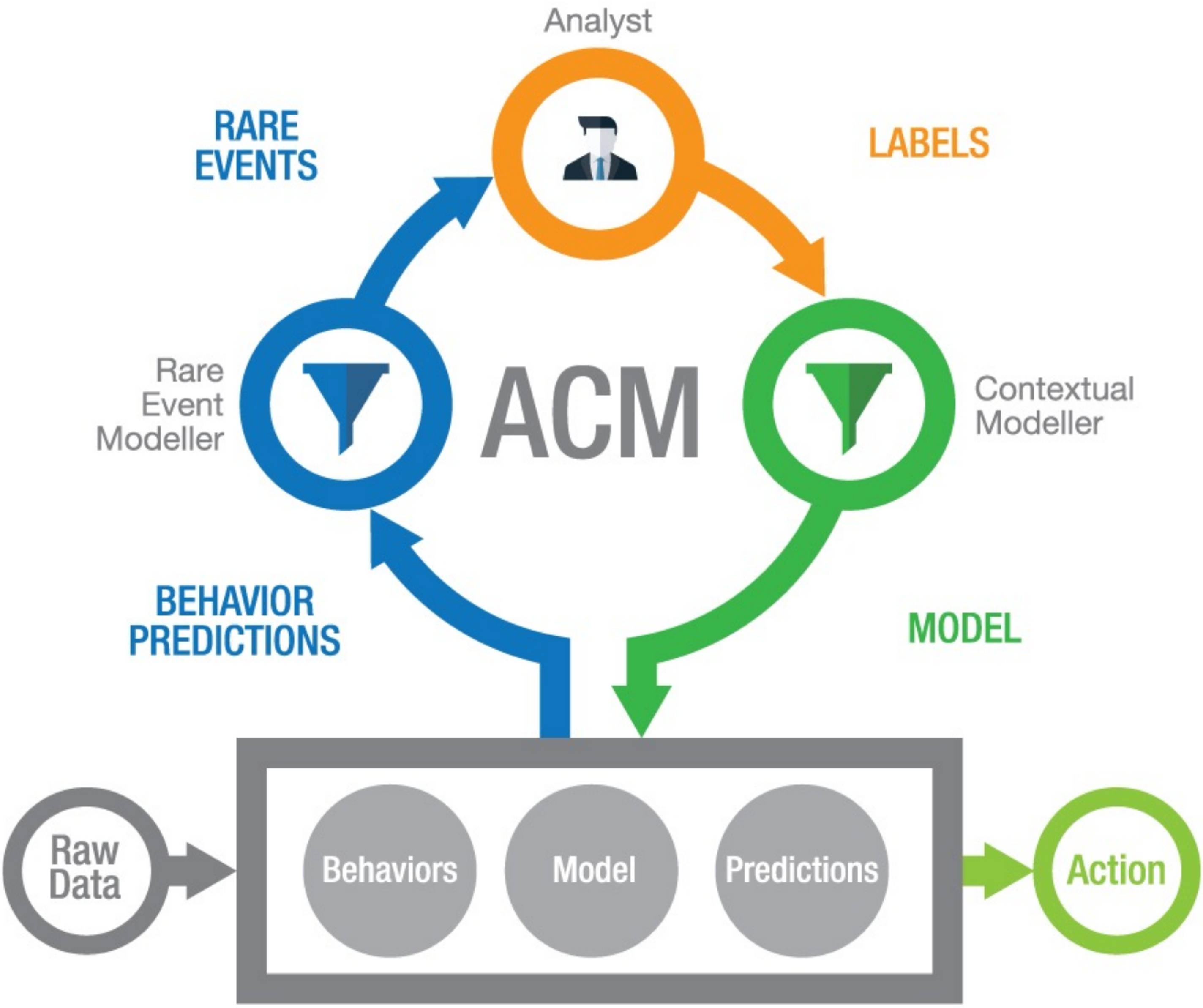
The platform can go through millions of events per day and can make an increasingly better evaluation of whether they are anomalous, malicious or benign. The company's human analysts aren't overwhelmed with an avalanche of unnecessary alerts and don't end up burned out.

A platform that never stops learning and adapting

Let's face it, most companies don't have the budget to employ an army of analysts - but this is just what PatternEx is offering.

"The whole purpose of this product is to make the analyst(s) you have super efficient," Uday Veeramachaneni, one of the co-founders and the current CEO of the company, told me.

The platform can effectively work with just one analyst at the helm. It "learns" how to mimic the analyst with the help of the analyst himself. The whole process, from start to end, looks like this:



The inputed raw data comes from the company's networking devices - firewalls, proxies, etc. The system's algorithms create behavior predictions, detect rare events (and unusual behaviors), and point them out to the analyst.

The analyst looks at the provided information and identifies malicious events. He labels them and this feedback is absorbed by the system. The algorithms then start creating models that will allow the platform to predict the very next day whether an anomalous new event is one (already labeled) attack or another, or whether it is benign.

On the second day, the analyst comes in and the platform shows that it has detected five attacks of one type. The analyst looks at the evidence and says: "These three are attacks of this type, the fourth one is benign, and the fifth one is an altogether new type of attack." He then labels the latter, that feedback is again inserted in the system and the models update themselves. As time goes by, they learn to discriminate between a great many types of attacks and benign events.

"The analyst is always training the system because there are always newer attacks," says Veeramachaneni. "At some point the system trains itself so well and becomes so very accurate that the analyst can get a bit more comfortable."

Unlike most other companies, PatternEx had to enter the market even before the product was finished, as they needed the data provided by customers to perfect it.

Additional help comes from the fact that once this solution is deployed by many companies, the models that are learned by the system at each of these can be aggregated and shared, creating a network effect.

"The more customers you have the more training you get, the more training you get, the more accurate you become, and the system starts detecting newer and newer attacks more speedily and more accurately," he pointed out, and made sure to note that no actual data about the customer or belonging to the customer is shared.

The training of the system doesn't have to begin on the first day of deployment. Most companies keep the needed logs for weeks if not months, and they can be fed into the models, as well as compared with the knowledge of past attacks in that period of time. This allows the system to start working initially and start identifying specific attacks from the very first day, and the training can continue from there.

"This is one approach we use with a lot of customers," says Veeramachaneni. "The other one is to install the software, extract the data and feed it into the system on the first day in real-time, and on the second day the system knows what's the 'normal' situation and what's abnormal behavior, and you can start screening through these events."

Real-time alerts of ongoing attacks allow the analyst to implement incident response if needed. Sometimes that means just picking up the phone and contacting an employee to see whether he or she is doing the thing that triggered the alert, and shutting the machine down if they aren't.

In large scale real-time environments, e.g. e-commerce, the reaction has to be even faster, and automated workflows have to be put in place so that they can be started immediately after the attack is detected in order to thwart it.

The platform is currently geared towards breach and fraud detection.

A tried and tested solution

It's interesting to note that, unlike most other companies, PatternEx had to enter the market even before the product was finished, as they needed the data provided by customers to perfect it.

They have been working on the platform for the last two years, and have deployed it at several Fortune 500 companies.

It proved to be extremely effective - it has 10 times better detection rates and 5 times fewer false positives than other user behavior analytics solutions.

“The most frustrating thing in infosec is that the data to detect malicious behavior often already exists in enterprise infrastructures today,” notes Veeramachaneni. “The human analysts can detect it, but analysts are difficult to hire and are not scalable."

He believes their technology is the right solution for the problem.

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

Building and implementing an incident response program from scratch

Zoran Lalic

Nowadays it is very unusual to read the news without some reference to a cybercrime and/or a data breach. The most recent high-profile breaches prove that even the most secure corporations are susceptible to being breached. Consequently, you should not ask yourself whether or not you are sufficiently secured to keep the bad guys out, but what to do when you discover them inside your network.

The new breed of cybercriminals use sophisticated and advanced evasion techniques to bypass detection tools and controls. Organizations must leave the “we are not on anyone’s radar” mentality in the past, and develop a plan to respond to security incidents. Typically, when we try to sell the value of incident response and security initiatives in general to executive management, we are always questioned. The two most popular questions that security professionals are asked:

1. Who would attack us being that we are not a big corporation?
2. Why would someone attack us when we don’t have any important data such as PII?

I used to work for a smaller organization and, at one point, I was asked the same two questions by our CEO. To prove a point, I decided to conduct an experiment and share the results with my CEO. I built a web server at home and exposed it directly to the Internet. Within 45 minutes, I started seeing different malicious attempts including brute-force and port scanning attacks. Within 72 hours, the server became very popular. I was seeing malicious attempts from all over the globe. I shared these results with my CEO and after that point on it became easier to get security initiatives approved.

If you are connected to the Internet, that is reason enough to be attacked. Your PC/server could be turned into a zombie (become part of a botnet) to be used to attack anyone else in the world. Attackers could also turn it into Bitcoin-mining machine.

Every organization, regardless of its size and the business they operate in, will experience a security incident. The sooner corporations accept this reality, the better. Once they do, they need to put a plan in place to detect and handle security incidents. The incident response components can vary, but the majority of programs consist of the following seven:

1. Executive management support

An incident response program requires executive management commitment and support. Without executive management leadership, buy-in and active approval and support, any effort to build and implement a successful incident response program will most likely fail.

Consider an example where an organization is building their incident response program and requires an IDS solution. The security team creates an implementation plan and goes to their CEO with this initiative. The CEO denies this request due to budget concerns.

2. Plan and prepare

Planning and preparing for the worst is extremely important. Without proper planning, the remaining pieces of the program are set up for failure.

"Give me six hours to chop down a tree and I will spend the first four sharpening the axe." – Abraham Lincoln

Include the following components in your planning and preparing for incident response:

Build the team

The foundation of an incident response program is a Computer Security Incident Response Team (CSIRT). Typically, there are two types of CSIRT teams that are found within an incident response program:

1. *Dedicated team* - Typically larger organizations can afford a dedicated team that is only responsible for incident response. They do not have other functions within the organization.

2. *SWAT team* - Smaller organizations cannot afford a luxury of a dedicated team and they build a SWAT team. The SWAT team members have their full time job responsibilities in addition to their incident response responsibilities.

The shape of a CSIRT team will depend on the organization, especially on the organization's budget, resources and size. It is extremely important to involve all business units within the organization in this team. Consider having a representative of the following business units (at least):

- Information technology
    - o Networking
    - o Systems
    - o Security
    - o Architecture
    - o Database
    - o Helpdesk
    - o SOC/NOC
- Human Resources
- Legal
- Marketing/Communication
- Compliance.

Identify roles and responsibilities

Now that you have identified the team, it is time to define roles and responsibilities for each member of the team. Ensure that each member has a clear understanding what their role, function and responsibility is within this team.

A CSIRT team with defined roles and responsibilities is capable to respond to an incident in a calm manner. Consider some of the following roles:

- Incident responder
- Incident handler
- Incident response lead
- Incident response manager

You might ask: "What is the difference between an incident responder and an incident handler?" Consider the example:

The DLP solution identified that PII has been leaving the network, is being exfiltrated to an unknown destination. The incident response plan has been executed and the CSIRT team responded to the incident. The incident responder started on the analysis to determine what was going on, but ten minutes into the analysis the CEO and executive management started emailing and calling the incident responder directly to learn more details.

Everyone is panicking and wanting to be in the loop. No one has the same updates. This is where the incident handler comes into play. He or she liaises with executive management and other business units. The major responsibilities of this role are the following:

- Keep executive management away from directly receiving updates from analysts
- Keep all business units in the loop of what is going on
- Resolve an incident in calm manner
- Be the only individual who provides updates

Look at incident response as a technical aspect and incident handling as a communication and coordination aspect of incident response. Incident responders will consist of computer, network and malware analysts.

Consider the example:

A smaller organization is in the process of building their incident response program. The decision has been made to build a SWAT team consisting of key members from all business units within the organization. One of the network engineers prior to joining this organization was employed as a network forensics analyst. This individual became a part of CSIRT team and his role became a network forensics analyst during an incident response execution.

Define the scope

Now that you have the team that has a clear understanding of their roles and responsibilities, it is time to define the scope of your incident response program. Define what types of incidents/events this team will respond to. You might consider that brute-force attack is not in scope and it is to be handled by the security team unless the malicious user gained access via this method.

Make sure to clearly identify when in the process of an incident will the plan be executed. You might make a decision that during a DDoS attack the incident response plan will not be executed unless there is a slowdown in website performance.

Additionally, consider assigning a severity level to each incident. For example, you might execute your incident response plan for all high and critical incidents immediately and not for medium and low incidents. Your plan should be documented and communicated to everyone involved.

Create an incident response policy

Policies are high-level statements and the incident response policy should be designed in the same fashion. The policy should make everyone within the organization aware of the incident response program and plan. It should contain sections such as perspective, scope, statements and enforcement.

Create a communication plan

The communication plan is an essential component of the incident response program and it should include both internal and external communication.

The internal communication procedures should include CSIRT team members, their backups, and management. Ensure their contact information is updated regularly. The external communication procedures should include law enforcement and external key stakeholders that must be notified in these situations.

Communication is key, especially if you have to comply with regulatory standards and have to communicate to external parties within certain period of time. It is extremely important to prepare and execute your communication plan the proper way – it will make a huge difference.

Provide training

All CSIRT members need to receive incident response training. Training should address:

- How to discover and recognize an incident
- How to communicate during an incident
- How to operate the tools used in incident response
- How to investigate and analyze an incident

- How to contain and eradicate an incident
- How to return to normal and more secure operations.

Tips

- Ensure SOC and/or security analysts receive the same training. In most organizations they are the front line of defense and responders to security alerts.
- Ensure your employees are aware of the incident response program. They also need to be trained on how to recognize threats such us phishing and social engineering.

3. Build incident response capability

Is your organization capable of detecting and analyzing an incident? Is your organization capable of containing an incident and recovering from it? You can have the best CSIRT team in the world, but without proper detection, it is as if you do not have a CSIRT team at all. The organization needs to identify and acquire tools that will help them detect an incident and respond to it. Organizations should consider the following tools:

- IDS/IPS
- SIEM
- DLP
- Traffic sniffers
- Dedicated forensics station and forensics software to collect and analyze data.

The tools must be well-tuned and monitored on regular basis. What good can a SIEM solution do for an organization, if no one is looking at the alerts?

4. Build an incident response plan

Every organization needs a plan in place on how to detect an incident and properly respond to it. To properly develop and implement this piece of the incident response puzzle, the organization must plan in detail for each stage of the incident response lifecycle and establish processes that have to be followed during the detection and response phases. This piece of the puzzle usually consists of six stages and each stage is equally important.

Detect

Requirement for this stage: Develop a plan to establish processes to be followed in order to discover potential incidents.

Detection is one of the greatest challenges that organizations face in the incident response lifecycle. The organization must detect a potential incident before they can properly respond to it. The sources of detection should be your employees, security assessments, audits, and alerts.

Several years ago my company at the time acquired a smaller organization and I was asked to audit their security controls and capabilities. I asked if they had an IDS solution in place and I was told that they did. Then I asked for the credentials to log in to their IDS solution and later that day they provided me with the credentials. Upon running the report showing activity for the prior 24 hours and learning the results, I was shocked. They had over 10,000 alerts in just one day! I asked them what was going on and I was told that they did not have resources to work on the IDS and that it was very chatty, but that they had to implement it to check the box in order to be compliant.

It is much more valuable to have an open source IDS well-calibrated and monitored, than several commercial and expensive IDS tools that are not.

Tip: If an organization is compliant with regulatory standards, it does not mean they are secured. In many high-profile breaches organizations were compliant with multiple standards, but they failed to follow their processes.

Investigate

Requirement for this stage: Develop a plan to establish processes to be followed once the incident has been detected.

You detected a potential incident, what do you do now? The next step is to investigate it to validate if this is a real incident or a false positive. Ensure that each step in the process is documented.

Collect and analyze

Requirement for this stage: Develop a plan to establish processes in order to gather forensics data and understand the nature of an incident.

Your investigation process determined this is a real incident. Now you have to analyze it. In this stage of incident response you need to collect evidence that must be analyzed in order to determine what happened. This stage will also discover if your organization is still under attack. Based on the analysis, the incident responders should be able to determine the scope, infected machines and/or applications, how the incident occurred, and attack vectors.

During the analysis phase is it extremely important to follow the proper forensics methodology in order for the evidence to be admissible in a legal cases. Consider the following:

- Make sure to collect evidence in a forensically sound manner.
- Maintain chain of custody
- Evidence has to be preserved properly
- Document, document, and document some more.

Contain

Requirement for this phase: Develop a plan to establish processes in order to stop the spread of an incident.

Armed with the knowledge from the analysis phase, the organization is now ready to take the proper steps to ensure that the incident does not spread to other parts of the network. This phase also ensures that the incident does not escalate in severity.

Eradicate

Requirement for this phase: Develop a plan to establish processes in order to eliminate an incident. After you successfully contained the incident, now it is time to resolve/eliminate it. This stage of incident response is very sensitive because you have to be 100% sure that the threat had been eliminated.

Consider the example where the organization executed their incident response plan and declared that an incident had been contained and then successfully eradicated. In less than 24 hours they had to re-execute their incident response plan because they did not initially discover a backdoor on the server that had been previously compromised. In most cases the best approach is to reimage the PC/server.

Recover

Requirement for this phase: Develop a plan to establish processes in order to return to normal and more secure operations. In this final stage of an incident response plan you bring the infected systems/applications back to operational state. Ensure that each system/application that was infected in the incident is now in a more secure state.

Post-mortem

Up to this point you have successfully detected, analyzed, contained and eradicated an incident. Your affected services had been recovered and are in operational state. What do you do next?

This is the aftermath of incident response. Schedule a meeting and involve everyone who was part of incident response execution. The members can effectively learn critical lessons during this meeting. Consider discussing following:

- What went well?
- What did not go well?
- Conduct root cause analysis
- What could you done differently?
- What needs to be changed in the incident response plan?

Armed with these details, you can go back to your incident response program and update it accordingly. All updates should be communicated to executive management.

5. Test the incident response plan

Building an incident response plan and leaving it on the shelf to collect dust is ineffective. It must be tested on regular basis. Consider testing your plan every six months through the use of tabletop exercises, every twelve months through the use of simulation tests, and every 24 months through the use of a full-scale test. Make sure to document results from each exercise and update your incident response plan. Upon updating it, distribute it to key stakeholders and train your CSIRT team on the new updates.

A tabletop exercise is the most common amongst all incident response exercises. It is an exercise of your incident response plan at a high level. Always choose a real-world scenario and make it as realistic as possible when you test your plan.

A period of calm is the best time to test and update your incident response plan. This is the time when you can discover flaws in your program and update it before a real incident happens.

Do not prevent your organization from discovering its mistakes and flaws through controlled failure via testing, as it will save you from headaches during a real incident.

6. Operate incident response capability

The incident response plan is a living thing. The success of your plan depends on this final piece of the puzzle. Cybercriminals are allowed to make as many mistakes as they want, we do not have that luxury and we must detect each and every potential threat.

Consider the following:

- Monitor systems/alerts for signs of incidents and compromise
- Tune your tools on a regular basis
- Leverage threat intelligence
- Categorize incidents according to established processes and standards
- Analyze all potential threats/incidents
- Fully document all aspects of the incident and incident response.

Now that we have put the incident response program puzzle together, it is time to execute it through a real-world scenario to see how each piece fits together.

Info about the organization in this scenario:

- Medium size (<500)
- 20 remote consultants
- Incident response program in place
- SWAT team
- 24/7/365 SOC (Security Operations Center).

1. The SIEM detects a suspicious activity and generated a critical alert.

2. All high and critical alerts are immediately sent to SOC team via email.

3. A SOC analyst investigates the alert and determines that someone has been conducting a port scan from the server in the DMZ.

4. All validated critical alerts are in scope of the incident response program.

5. The SOC team executes the incident response communication plan and calls the person that has a role of incident response manager immediately.

6. Upon learning of the finding, the incident response manager asks the SOC analyst to alert everyone on the CSIRT team per communication plan and authorizes the execution of the incident response plan.

7. Within 30 minutes, all CSIRT members are present in the conference room that is used as a war-room in case of an incident.

8. The incident responders started their analysis immediately. First, they collected live memory and cloned the server. Upon logging in to the server they learned that several suspicious tools have been installed.

9. This server is in the DMZ between the external and internal firewalls. The incident responders immediately add the firewall rules on both firewalls to completely shut down access that this server had to the outside world and the internal network.

10. Incident responders ensure that everything they do is documented. They also take many screenshots along the way.

11. The incident handler provides updates to executive management every 15 minutes.

12. The incident responders continue their forensics analysis by analyzing logs and determine that no attempts were conducted to get access to the internal network.

13. The incident responders delete a username that was created maliciously earlier that day. Passwords are reset for all legitimate users that had access to the server and each user ID is assigned a complex password.

14. The incident responders discover a database on the server. The analysis shows there is no data in this database and that it was not accessed for 3 weeks.

15. Upon further analysis, it is requested that this virtual server is shut down and a brand new one built.

16. The analysis uncovers that this server had port 3389 opened to the outside world and that a malicious user attempted a brute-force attack and guessed the correct password for administrator username and gained access to the server. Upon gaining access, they installed several malicious tools such as port scanners and several brute-force attack tools.

17. The new server is built and the old one replaced with it. Firewall rules are updated to allow access to port 3389 only once the users successfully authenticated to the VPN. No direct access from the Internet via port 3389 is allowed.

Up to this point we successfully conducted the following:

- Detected and investigated the incident
- Executed the incident response plan
- Contained and eradicated the incident
- Recovered the service in a more secure state.

Now we are ready to do a post-mortem. The incident response manager schedules a meeting for the next day.

In this meeting the following is determined:

What went well?
The response to the incident was very quick and efficient. The incident response plan was executed as planned.

What did not go well?
At the end of the analysis it was determined that there was a database on this server. Upon checking the database, it was determined that nothing was in this database. The team should have discovered this at the beginning of the analysis. If this was a real a database with sensitive data in it, it would be extremely important to discover it as soon as possible.

Conduct root cause analysis
It was determined that this server was used by several consultants to login and use reporting tools when on customer site. The remote desktop was wide open to the Internet.

What could you have done differently?
The incident response plan was executed as planned. However, the team should have checked the software inventory on the server first. That would have helped to discover the database at the beginning of the process instead of at the end.

What needs to be changed in incident response plan?
It was determined that every change to the external firewall must be analyzed and approved by the security team since the network team is in charge of firewalls. This change had been added to the incident response plan and it was communicated to all involved parties.

The modern cyber-crime landscape continues to evolve with lightning speed, and we must be prepared to combat the dangers. My years of experience with incident response programs allow me to offer you the following 17 tips:

1. Don’t panic.

2. Know all your facts before you make any announcements.

3. Know notification laws and who and when to notify.

4. Don’t use word the “breach” until you are 100% sure that is the case - in many cases that is when clock starts ticking.

5. Find out what can be shared about the incident, and with whom. You don’t want to hide

anything, but at the same time you don't want to share information that should not be shared.

6. Have a service agreement signed with a third party security/forensics firm in advance in case if you need to bring them in to conduct additional analysis.

7. Always consider the possibility that a malicious user might have your incident response program in front of them, providing them with the information required to strike where you are not looking.

8. Consider out-of-band communication during incident response.

9. Don't spend all your time and resources on just one stage of the plan. For example, don't spend millions of dollars on detection tools and consider this stage as the most important stage of the lifecycle. All stages of incident response lifecycle are equally important.

10. Ensure your incident response program is adaptable – there are too many variables.

11. Establish processes and guidelines for the most common scenarios. For example - virus outbreak process/guideline. This process would be followed in case of virus discovery within the network. Each stage in incident response plan lifecycle requires this (as noted in the "Build an incident response plan" section).

12. Documentation is key.

13. Create flow charts where necessary.

14. Change management. Ensure you don't introduce unnecessary vulnerabilities into your environment.

15. Choose an incident response sponsor. Typically the CISO or the CIO.

16. Upon discovery of the incident don't shut down the server immediately without any analysis. The most valuable data can be lost.

17. Test and update your plan.

You might ask: "Why tip 7 and 8?"

Several years ago I was conducting an internal penetration test which was supposed to execute an incident response plan upon a brute-force attack on a domain controller. During the penetration test I was able to gain access to the intranet site and then discovered a copy of the incident response plan along with processes and procedures.

It contained information about the CSIRT team members and their roles along with their contact info. In their plan they mentioned a conference bridge to be created for the remote CSIRT members to join in case of an incident.

My next objective was to learn the bridge info once they discover a malicious activity and execute their plan. I then sent a random email to all CSIRT members individually hoping to learn if any of them was out from the office and it was my lucky day - I got two out-of-office replies. I went back to their incident response plan and updated a contact number of the person out from the office to my mobile number.

Luckily, I was able to modify the document and save changes. Then I proceeded as planned and conducted a brute-force attack against the domain controller. I was hoping they did not have a separate copy of their incident response plan to be followed and executed in case of an incident.

Within 30 minutes I received a phone call from the SOC team informing me about the incident. I told the analyst that I am out from the office on a vacation without access to my email. I politely asked for the bridge information over the phone so that I can immediately join. He was very helpful and provided me with the number and meeting ID. I then successfully joined the conference bridge and listened to their incident response live.

Zoran Lalic is a Senior Security Engineer with extensive industry experience in information security program development, penetration testing, forensics analysis, vulnerability management, security architecture design and incident response. His experience spans environments of all sizes – small offices to global networks. Additionally, he helped companies become PCI DSS compliant. Zoran has been an active researcher of new techniques used to compromise networks.

Take it to the boardroom: Elevating the cybersecurity discussion

Tom Kellermann

As data breaches continue to rise, organizations, regardless of their size or the industry they are in, must take into consideration a new mindset. Despite the FBI's focus on cybercriminal activity, less than five percent of computer-related crimes are successfully prosecuted. Unfortunately, jail time and other penalties are rare, despite the pervasiveness of cybercrime and cyber espionage.

Corporate decision makers are faced with a shocking reality: from a cyber perspective, they are on their own when it comes to protecting their reputations, intellectual property, finances and consumers.

That having been said, it is no longer a good idea to consider the IT department solely responsible for the protection of important data. Instead, it should be assessed and managed at all levels throughout an organization. Each operating group within a company is vulnerable due to Internet-connected technology.

Taking a broader look at security can help mitigate daily threats that assail companies. When it comes to data breaches, the question is not "if," but "when" a company will be targeted. This should dictate a shift from the current security investment deficit.

Currently, only eight cents of every IT dollar is spent on security, which is inadequate for the majority of organizations, both large and small. At these levels, customer and corporate information is not sufficiently protected when facing the hostile cybercriminal community. Reputations are at stake and brands could be jeopardized due to lax measures.

Understanding that more than data is at stake, decision makers and board members must make data protection a top priority.

Rising to the challenge

Appointing a chief information security officer (CISO) to take the lead in keeping corporate data safe is a step taken by many forward-thinking companies. While this is a move in the right direction, the big question is to whom these individuals should report. In the past, the answer has been the chief information officer (CIO). While this seems logical, the problem lies in the competing priorities of a CIO and CISO. CIOs are typically only focused on technology infrastructure and resources, with the most concern for increasing efficiencies, access and resiliency.

Though important, these can be in opposition to the needs of a CISO, who aims to improve enterprise-wide security measures and risk management across all silos. When considering governance, placing the CISO within the purview of an executive with broader responsibilities, such as a CEO, is advisable.

Due to a myriad of overarching implications, today's enterprise leaders should be held accountable for cybersecurity, regardless of their role. A prime example is the chief marketing officers. The executives are typically more focused on how the Web is used, with email campaigns, mobile app development and website updates, but these promotional endeavors can leave the door open for malware or other attacks to be released on unsuspecting customers. At each operating level, the influence of technology demands an awareness of where security fits into everyday functionality.

Preventing the spread

An additional justification for broadening security responsibly across an organization is the propensity for threats to emerge as moving targets. Malware infections often migrate laterally within an enterprise, as well as from third-party vendors. When a network becomes compromised, attacks can be widespread in the entire IT framework and supply chain, in what is known as "island hopping."

The Target breach is a good example of island hopping at work. The investigation revealed that hackers had infiltrated a vendor's system in order to steal the retailer's credentials. As a result, criminals successfully gained access to information of approximately 40 million customer credit cards, potentially affecting more than 100 million consumers. The impact of this attack is still being felt across the retail sector today.

It can be easy to overlook third-party partnerships from a security perspective, but these potential gaps warrant the awareness of corporate leadership. Examining the policies of partner organizations is one way to strengthen internal security, particularly if the company is publicly traded. The fact that these partners often have access to sensitive information, making them attractive targets, cannot be ignored.

A holistic perspective to cybersecurity can help mitigate the risk of system-wide threats.

A new attitude

For the last 20 years, corporate focus has consistently been on cutting costs, improving access and increasing efficiencies. That level of commitment should now be given to customer, partner and investor information, and to making it secure as possible in the digital world. Physical safety is an expected convenience of in-store shopping, and online environments should offer information security. Therefore, enterprises should invest between 10 to 20 percent of their IT budget in cybersecurity as a function of brand protection.

Elevating cybersecurity to an operational and risk management priority will take effort and focus but can yield many dividends. For this practice to become a reality, boards of directors must educate themselves to improve governance and oversight. To stay ahead of the bad guys, a shift in investment strategy, as well as strong improvements to employee training and reporting structure are paramount.

Tom Kellermann is Chief Cybersecurity Officer of Trend Micro (www.trendmicro.com), follow him on Twitter - @takellermann.

Malware world

T9000 backdoor steals documents, records Skype conversations

A new backdoor Trojan with spyware capabilities is being used in targeted attacks. It has been dubbed T9000, since it's a newer, improved version of the T5000 backdoor. The attackers wielding it are believed to be of Chinese origin, as the T5000 has in the past been tied to the Admin@338 APT, a group that has, in the lat few years, been targeting APAC governments, US think tanks, and human rights activists. The T9000 is delivered via phishing emails containing a booby-trapped RTF file. This file contains exploits for two vulnerabilities (CVE-2012-1856 and CVE-2015-1641) present in a wide variety of software.

After exploiting one of these, it will go through a series of shellcode runs that will ultimately result in the loading of the backdoor's main module and three encrypted plugins. But not without first trying to show a decoy document, making sure that only one instance of the malware is running at a given time, and checking for installed security products.

"The malware goes to great lengths to identify a total of 24 potential security products that may be running on a system and customizes its installation mechanism to specifically evade those that are installed. It uses a multi-stage installation process with specific checks at each point to identify if it is undergoing analysis by a security researcher," Palo Alto Networks researchers discovered.

After the main module collects user, machine and software information and sends it to the C&C server, it downloads the three modules (tyeu.dat, vnkd.dat, and qhnj.dat) and loads them on the machine. Each of these has a different function. The first one is responsible for collecting information – recording video calls, audio calls, and chat messages – from Skype, and it does so by using the built-in Skype API.

"The victim must explicitly allow the malware to access Skype for this particular functionality to work. However, since a legitimate process is requesting access, the user may find him- or herself allowing this access without realizing what is actually happening," the researchers noted.

The second module searches for drives connected to the system, and through them for MS Office files, which it promptly copies and prepares for exfiltration. The third one records important actions taken by the victim – changes on the system – and this could come in handy if the attackers want to gain access to remote systems used by the victim. Finally, the main module can list drives and directories, execute commands, kill processes, download, upload and delete files, and so on.

Rooting malware lurking in third party Android app stores

Downloading Android apps from Google Play might not always be a safe proposition, but downloading them from third party app stores is definitely less safer.

According to Trend Micro mobile threats analyst Jordan Pan, the company has recently discovered in four third party app stores (Aptoide, Mobogenie, mobile9, and 9apps) over 1,163 malicious Trojanized APKs capable of rooting Android-running devices and opening them to additional dangers.

In just four days, the malicious apps were downloaded by users from 169 countries, mostly India, Indonesia and the Philippines.

All these apps are Trojanized versions of legitimate game, security, music streaming and other popular apps. “They even share the exact same package and certification with their Google Play counterpart,” Pan pointed out. But, they are repackaged to contain malware dubbed ANDROIDOS_ LIBSKIN.A, which is capable of rooting the phone, download additional malicious apps and install them, show ads, and collect user and device data and send it to a remote server controlled by the malware author(s).

The researchers have informed the aforementioned third party stores about these threats, but still haven’t heard back from them.

“Though we highly recommend to sticking to Google Play for Android users, downloading apps from third-party stores still has its set of merits,” says Pan.

Still, users should be careful – it’s always a good idea to check the reputation of the store and the app’s developer before downloading anything.

“For developers publishing their apps, make sure to partner with reputable stores. Secure coding also helps prevent cybercriminals from replicate or modify their work to include malware,” Pan advises.

Russian hackers used malware to manipulate the Dollar/Ruble exchange rate

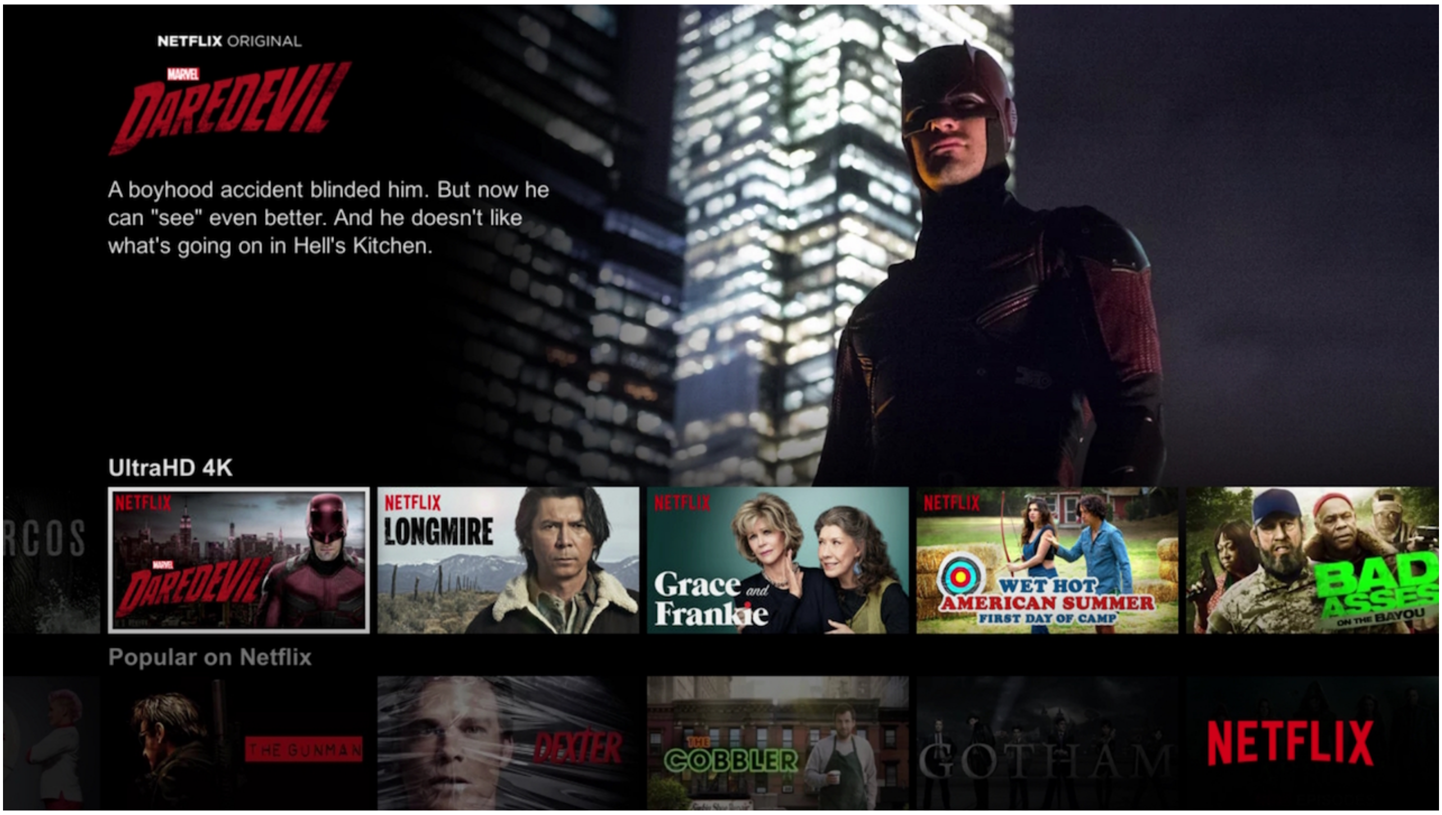
Russian-language hackers have managed to break into Russian regional bank Energobank, infect its systems, and gain unsanctioned access to its trading system terminals, which allowed them to manipulate the Dollar/Ruble exchange rate.

“The criminals made purchases and sales of US dollars in the Dollar/Ruble exchange program on behalf of a bank using malware. The attack itself lasted only 14 minutes, however, it managed to cause a high volatility in the exchange rate of between 55/62 (Buy/Sell) rubles per 1 dollar instead of the 60-62 stable range,” Russian security company Group-IB shared in a recently published whitepaper.

“To conduct the attack criminals used the Corkow malware, also known as Metel, containing specific modules designed to conduct thefts from trading systems (…) Corkow provided remote access to the ITS-Broker system terminal by ‘Platforma soft’ Ltd., which enabled the fraud to be committed.”

“As a result of the attack, the compromised bank which terminal was used for intrusion, suffered a huge financial and reputational damage, since many players on the market didn’t trust the hacking theory of the incident and tended to believe that a simple mistake had occurred,” noted Group-IB’s researchers, who were called in by Energobank to investigate the incident.

“Experts say that many companies that were trading at the time of the attack and successfully made profit while the attackers are believed to have received no money from the operation. This evidence leads us to believe that these hacker actions could be a test of the ability to influence the market and capitalize on future attacks.”



A boyhood accident blinded him. But now he can "see" even better. And he doesn't like what's going on in Hell's Kitchen.

Netflix-themed phishing, malware supply black market with stolen credentials

As the Netflix movie streaming service spreads all over the world, the number of users rises, as well as the number of those who wish to use it but don't want to pay for it or want to pay less than the set price.

With such a wide (and widening) pool of potential targets, it's no wonder that some cyber crooks are opting to concentrate on them.

Unsurprisingly, legitimate Netflix users are targeted with phishing emails impersonating the service, using one pretext or another to lure them to a fake Netflix site where they are directed to update their account, i.e. to enter their login credentials, personal info and credit card details.

"Netflix subscriptions allow between one and four users on the same account. This means that an attacker could piggyback on a user's subscription without their knowledge," Symantec researcher Lionel Payet explains.

Stolen Netflix login credentials are often sold on the black market, to users who wish to access Netflix for free or a reduced price.

"These accounts either provide a month of viewing or give full access to the premium service." Payet notes. "In most advertisements for these services, the seller asks the buyer not to change any information on the accounts, such as the password, as it may render them unusable. This is because a password change would alert the user who had their account stolen of the compromise."

A similar approach is taken by cyber criminals offering Netflix account generators. The software provides stolen login credentials or login credentials of accounts that have been created by using stolen payment card details.

That list is often updated, as some accounts are shut down either because the legitimate users stopped using them or because the compromise was detected.

Finally, potential users can be and sometimes are tricked into downloading malicious files posing as Netflix software.

In Brazil, for example, users have been tricked into downloading a banking Trojan masquerading as Netflix software, after clicking on fake ads offering free or cheaper access to the streaming service.

Unknown attackers are infecting home routers via dating sites

Damballa researchers have spotted an active campaign aimed at infecting as many home routers as possible with a worm.

A variant of the TheMoon worm, it works by taking advantage of a weakness in the Home Network Administration Protocol (HNAP), and is delivered to visitors of one of five one-night stand dating sites seemingly controlled by the same person (possibly a victim of identity theft).

If all of this seems familiar, it is because a similar campaign using the same malware was detected in early 2014 by SANS ISC.

Now, as then, the worm spreads but has no functional C&C server to control it, so effectively we can't really say the routers are roped into a botnet – but they could be at a later date.

The malware prevents users from using some of the router's ports and opens others so that it can spread to other routers, and currently goes undetected by popular AV solutions.

The initial infection is triggered when a user visits one of the aforementioned dating sites.

"The page loads an additional php file called remot.php from an iframe to run in the background. The file remot.php probes and accesses the router and other information. If criteria is met, the attack moves to Stage 2," the researchers explained.

The criteria is: the router is vulnerable to the aforementioned weakness, and it uses a default IP address (192.168.0.1 or 192.168.1.1) for the login page. Stage 2 includes a call for another URL, which launches a script and downloads the worm (a Linux executable ELF file).

"The criminals moved from scanning IP ranges for potential vulnerable home routers to embedding the attack on a website," noted Loucif Kharouni, senior threat researcher at Damballa. "In 2015 they released 3 versions of the file nttpd which is a main component of the attack. It feels like this conversion to a web-based attack is new and under construction. We are still looking for more information about the attack and the criminals."

Someone hijacked the Dridex botnet to deliver Avira AV's installer

After last September's arrest of an alleged member of the gang that has been developing and spreading the Dridex banking malware, and last October's temporary disruption of the Dridex botnet at the hands of UK and US law enforcement, the criminal group is experiencing problems again.

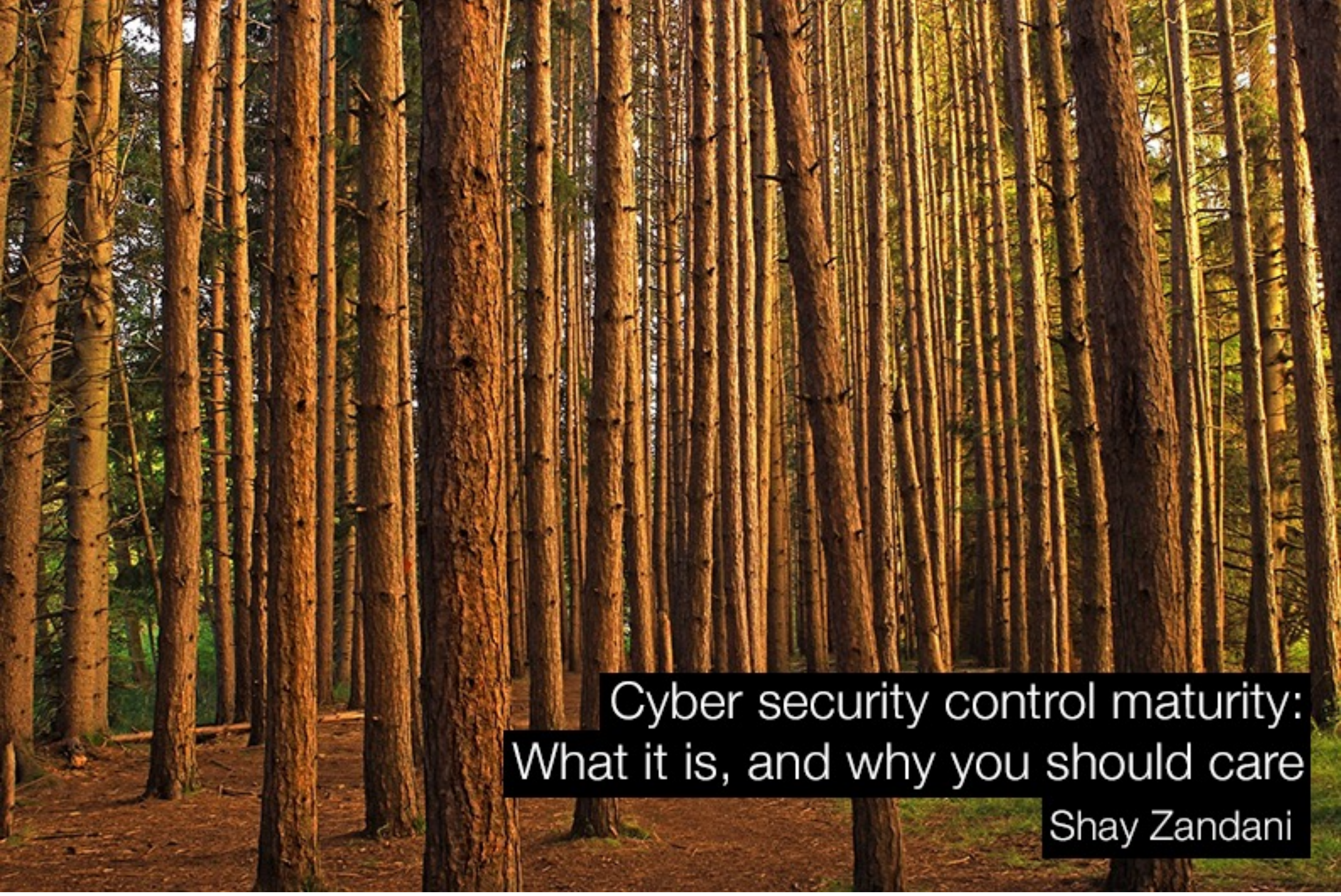
Someone – a white hat hacker, by the looks of it – has managed to compromise the server from which the malware is downloaded to the victims' computer, and swap the Dridex loader with an original, up-to-date Avira web installer.

So when the users open the spam email, download the attached Word document with malicious macros, and open it, instead of being hit with malware they get extra protection.

"We still don't know exactly who is doing this with our installer and why – but we have some theories," says Moritz Kroll, malware expert at Avira. "This is certainly not something we are doing ourselves."

Another possible theory is that the criminals did this themselves in an attempt to interfere with Avira's and other AV companies' detection process, but that seems very unlikely. Why would they want to increase the safety of potential targets' machines?

Interestingly enough, this is not the first time that the Avira installer has been added to malware. At one point in time, both the Cryptolocker and Tesla ransomware included the Avira installer. In both cases, the why of it remains unclear.



Cyber security control maturity: What it is, and why you should care

Shay Zandani

A popular belief circulating within the audit community is that it is both possible and desirable to create a shortlist of five to 10 security controls that are universally accepted to be the most important for cyber defense. The idea is that any organization that deployed them according to established best practices would be better protected against cyber-attacks than those that didn't.

While such a list might make a lot of auditors' lives easier, the business landscape we operate in doesn't allow for it. Cybercriminals run the gamut in their intent and motives, and their tradecraft evolves way too quickly for such a list to remain current for more than the blink of an eye. Not to mention, enterprises are constantly deploying new technologies and trying new models (i.e. cloud, mobile), which leads to the inevitable creation of new essential controls and/or the removal of others.

That's not to say that basic cyber security controls, such as network security, authentication and authorization, and others don't hold immense value to an organization when given the proper strategic focus - they absolutely do. But as IT environments continue to evolve, security and risk leaders need to ask themselves is that as things change, do they need new controls (i.e. invest in yet more point products), or can they improve their security posture by making better use of those already in place?

I believe they can. To that end, rather than spend more cycles creating a "master" shortlist of key controls, much more useful - and *achievable* - goal would be to work towards *control maturity*.

The problem with this metric is that it has traditionally been difficult to get an objective read on how mature a given control is, not to mention to have a level of comfort that it will mitigate the attack. For this metric to have any real meaning, organizations need to have a sustainable method for determining control maturity.

Back to basics: Setting the context and defining terms for control maturity

I spent more than a decade running PwC's Global Risk Management practice in Israel, which led me to become deeply involved with ISACA Israel, including more than seven years as the head of its professional committee and a three-year stint as its President.

What I've observed across organizations of all sizes and sectors is that most organizations frame their risk assessment efforts based on three major categories of controls, which result in a list of about 50 or so unique controls extracted from NIST, SANS20, CobiT, ISO and other leading standards and good practices. These categories are:

1. Administrative controls: These are "softer" metrics that are not inherently framed around technology, such as cyber security policy and procedures, training, awareness, etc.
2. Preventive controls: Such as network segmentation, web application firewalls, authentication, etc.
3. Detective controls: Such as SIEM/SOC, abnormal user behavior detection, network traffic anomalies detection, etc.

Next comes the process of determining control maturity. The model that I have found to work best consists of three basic components - high level metrics that can be reflected by a simple score, and determined by analyzing a set of indicators that determine how well (or not) the control is being used. They are:

1. Indicators of Maturity (IoMs): Objective facts from the device that indicate how it is configured. For example: Are there policies that define the minimum length/complexity for application and system passwords? How about for recommended/length complexity? What percentage of the organization adheres to the minimum length? What percentage follows organizational recommendations? IoMs need to be evaluated for:

- Management
- Functionality
- Coverage
- Up-to-dateness.

Additionally, organizations also need to make sure their Indicators of Maturity account for new or emerging parameters, such as relevant or new attack methods, industry specific considerations (for example, SCADA and banking have different security and risk concerns), compliance requirements, and can account for changing business requirements (e.g. as cyber insurance becomes increasingly mainstream, its significance as an IOM will increase).

2. The ability to translate high level, written corporate security policies into deployment best practices and measure how well they are being applied: Developing a set of measures that dictate how to score a given IoM based on best practices, company policy and industry standards. Criteria must be device-independent so that security readiness is not based on the need for a specific product or technology (e.g. password policies should be scored on a scale of 1-10 based on character length and complexity).
3. The ability to aggregate these scores at various levels through the organization and device hierarchy: Control -> Control Groups -> Business Environments.

Drilling down: Control maturity is inquiry-based, requires human input

For folks tasked with the day-to-day management of the organization's security controls (i.e. the various products, services, processes and involved in managing cyber security across the organization), "operationalizing" the data gleaned from each individual indicator is not always intuitive. This is due in great part because operations and audit functions in most organizations are siloed, when they should be working lockstep.

When you look up the word "assessment" on Dictonary.com, it is a noun - a thing. "To assess" is a verb. On the other hand, "audit" can be either a noun or a verb.

Risk managers and auditors approach audits as an active process, while an assessment is a tool that is used to measure progress along a continuum. However, security operations people perceive audits as a noun, a thing – and an unpleasant one at that, having been indoctrinated into the audit process during a period of intense regulatory clampdown due to the corporate malfeasance of Enron, WorldCom and Tyco.

Operations owned the day-to-day management of the controls being audited but had no input into what the audit requirements were, and found themselves under extreme pressure to implement controls they (rightly) felt held little (if any) intrinsic security value. To these folks, security audits were a huge, stressful waste of time that at best offered marginal improvements.

While mandates such as PCI DSS have closed the gap between compliance and security, and the process has become more automated and streamlined, the schism is far from gone. The only viable way to eliminate it completely is if control maturity becomes a primary operational objective, where audit results are continuously and expediently implemented into the environment.

Just imagine the cultural shift that can ensue if audits were less about adhering to externally mandated requirements and more about situational awareness, resource optimization and risk management. The process of determining control maturity can be intense – without a clear understanding of the business value it provides, the process will break down.

As I mentioned above, what seems to occur for most companies is that they rely 50 or so key controls. A single control can require some inquiry in order to determine its maturity.

Below are slivers of assessment parameters, but for the conversation's sake lets say a single control can have numerous IoMs depending on the nature and complexity of the control. With that being the case, these lists can appear to be way more daunting than they really are, especially if the viewer is apprehensive or apathetic towards the process.

IMAGINE THE CULTURAL SHIFT THAT CAN ENSUE IF AUDITS WERE LESS ABOUT ADHERING TO EXTERNALLY MANDATED REQUIREMENTS AND MORE ABOUT SITUATIONAL AWARENESS, RESOURCE OPTIMIZATION & RISK MANAGEMENT

For example – here are a few IoMs in the area of awareness and training, one of several key administrative-based controls:

1. Does the organization have an information security awareness and training program for employees? For customers? Vendors? Suppliers?
2. Does the organization provide basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial onboarding process? How often are users re-trained?
3. Does the organization document and monitor individual security training activities from basic security awareness training to specific information system security training?

For the second family of controls, preventative controls, let's use network device hardening as an example. Here's partial list of the IoMs that would come into play:

1. Is BOOTP service disabled?
2. Is CDP disabled on at least one interface?
3. Is the console session timeout defined?
4. Is the Network Time Protocol (NTP) defined on the router?

These are simple yes or no questions, but each control can have many attributes that are worth assessing. Many controls require a working technical knowledge of specific systems to know why some things are relevant IoMs and how they might be updated over time.

For the third family of controls, detective controls, let's use anomalous user behavior detection as an example. Anomaly detection technologies detect behavioral patterns that may signal an attack.

Once again, here is a partial list of Maturity Indicators:

1. Does the organization have processes and technologies in place to detect anomalous activities by users (clients and employees)?
2. Is statistical anomaly detection in use?
3. Is application, network, server and workstation usage examined to detect anomalies?

Keep in mind that these sample IoMs are just that – samples. Because what IoMs matter the most to an organization are often dictated by what IT systems and products are in use, they can become obsolete or shift in relevance over time. They need to be reviewed and/or updated regularly, which should happen naturally as companies start to focus on control maturity.

Finally, the kinds of external threats that they face are also a factor. For example, SCADA systems are primarily the domain of state-backed hackers, cyber terrorists and IP thieves – these attackers' motives are likely to be quite different than those of attackers targeting a large commercial banking organization.

Conclusion

Different controls are relevant to different organizations given (a) their internal risk profile, (b) the nature of the external cyber risks they face, and (c) their level of control maturity.

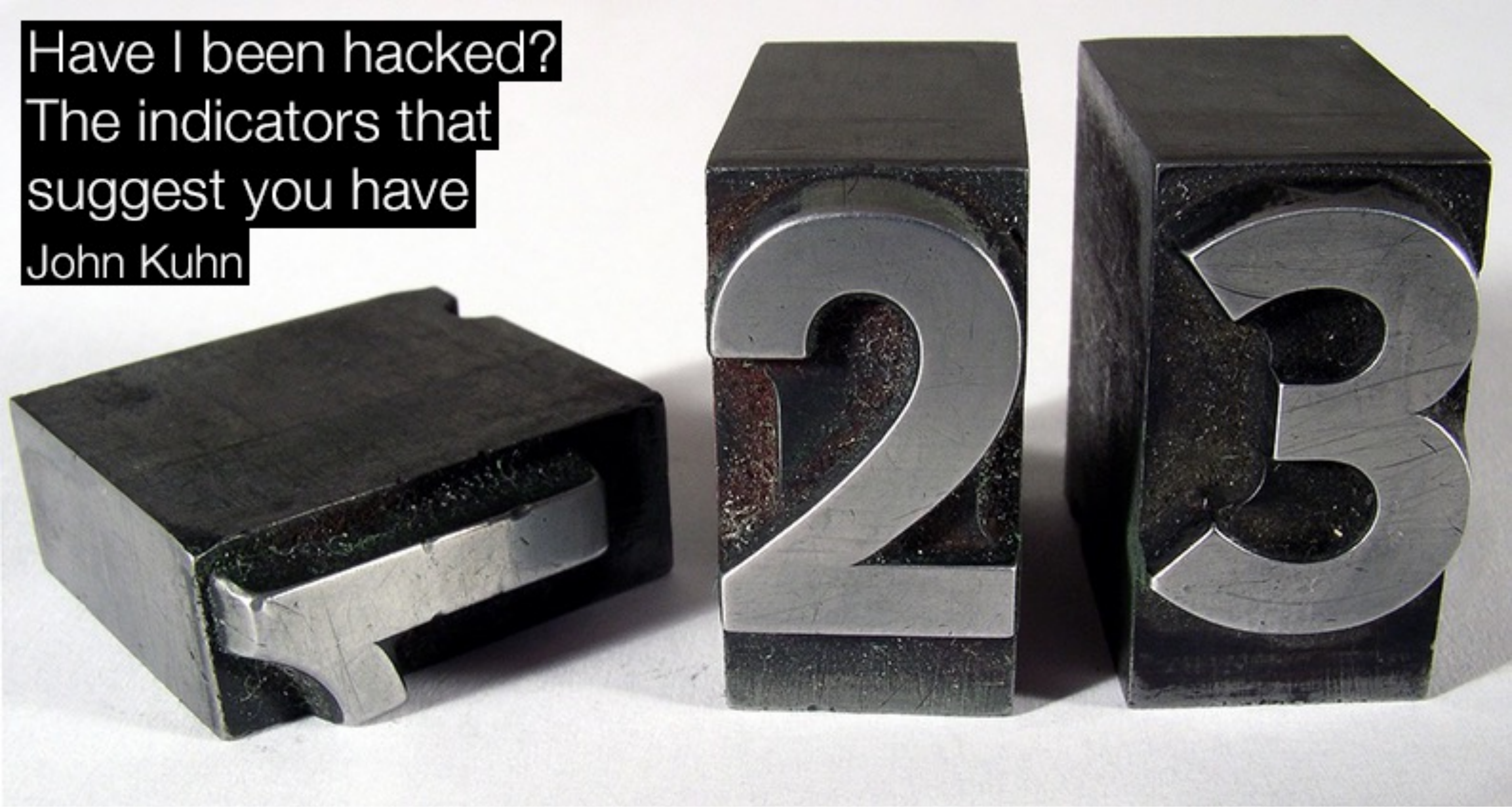
As IT security risk management practices mature, it will be the CISOs' job to create their own "Holy Grail" control shortlist, prioritize what controls are the most relevant and why, define what the key IoMs are for each control, and create an IoM revision process to account for change over time. For this process to have lasting value, the audit and operations functions need to be integrated. This is likely a cultural issue more than anything else, but if the two functions were to be merged, the outcome would be far greater than the sum of its individual parts.

The organization would not only have a clear vision and road map for cyber security maturity, it would also possess the ability to address and respond to cyber security issues in a much more agile, responsive and proactive manner.

Shay Zandani is the Founder and CEO of Cytegic (www.cytegic.com), a provider of an end-to-end solution for cyber security management.

Have I been hacked? The indicators that suggest you have

John Kuhn



Security professionals are constantly on the hunt for potential vulnerabilities and looking for ways to defend their networks. The term “indicator of compromise” (IOC) – first coined by governments and defense contractors trying to identify APTs – is something that all information security experts are familiar with.

Traditionally, investigators gather IOC data after they’ve been informed of a potential breach or discover a suspicious incident during a routine, scheduled scan. A recent IBM X-Force report looked at the top indicators of compromise so you can spot them before a hacker is able to do serious damage.

Let’s take a look at some of the top IOCs that your network has been breached by an attacker and how you can leverage them to detect irregularities in your system.

Unusual outbound network traffic: While it’s tough to keep hackers out of networks, outbound patterns are easily detectable and can be a sign of malicious activity. With visibility into this traffic, you can respond quickly before data is lost or major damage is caused.

Anomalies in privileged user account activity: Attackers often try to escalate privileges of a user account they’ve hacked. Monitoring privileged accounts for unusual activity not only opens a window on possible insider attacks, but can also reveal accounts that have been taken over by unauthorized sources. Keep an eye on systems accessed, type and volume of data accessed, and the time of the activity can give early warning of a possible breach.

Large numbers of requests for the same file: When a hacker finds a file they want – customer or employee information, credit card details, etc. – they will try to create multiple attacks focused it obtain it. Monitor for an amplified number of requests for a specific file.

Geographical irregularities: It may seem obvious, but it’s important to track the geographic location of where employees are logging in from. If you detect logins from locations where your organization does not have a presence, it’s worth investigating as it could mean you’ve been compromised.

Database extractions: Closely monitor and audit your databases to know where sensitive data resides, and to detect suspicious activity, unauthorized usage and unusual account activity. Watch closely for large amounts of data

PROFILE YOUR NETWORK TRAFFIC PATTERNS TO UNDERSTAND WHAT'S NORMAL

being extracted from databases, this can be a clear indicator that someone is attempting to obtain sensitive information.

Unexpected patching of systems: If one of your critical systems was patched without your initiation, it may be a sign of a compromise. While it seems strange that a hacker would repair a vulnerability, it's all about the value of the data to them, and keeping other interested criminals away from it. Once they get inside, they often try to add a patch to the vulnerability they used to gain access to the system so that other hackers cannot get in through the same vulnerability. If an unplanned patch appears, it's worth investigating for a potential attack.

Searching for indicators of compromise

These are just a handful of the different indicators of compromise that you should be on the lookout for, however, what are the steps to actually searching for them?

A good rule of thumb is to implement a defense-in-depth lifecycle – Document, Search, Investigate, Remediate, Repeat.

Document attack tools and methods: Profile your network traffic patterns to understand what's normal. Focus your attention on main protocols, especially the ones used by attackers such as DNS and HTTPS.

Collect and examine log file entries and leverage tools like log management and SIEM systems that can help automate and visualize these data patterns to detect suspicious activity. Subscribe to IOC data feeds, like IBM's X-Force Exchange, that share reported IOCs to help investigate potential incidents and speed time to action.

Use intelligence to search for malicious activity: By leveraging the data that you documented in step 1, you can configure your security systems to monitor and search for malicious activity. Your defenses can be configured to block activities or trigger alerts if activity is identified from a suspicious IT address or geographical location, if an attacker tries to use a known toolkit or tries to exploit a known vulnerability. You should also look out for new user names being created locally.

Investigate security incidents and assess compromise levels: If a security incident occurs, the next logical step is to investigate and assess the number of systems or applications that are affected. Start with system IP, DNS, user, and timestamps to first understand the scope of the breach and the degree of penetration the attacker may have gained in the system. Next, create a timeline to determine if any other events occurred. Examine all files with time stamps (logs, files, registry), the content of email communications and messages, information about system logon and logoff events, indications of access to specific Internet documents or sites, and the contents of communication with known individuals in chat rooms or other collaborative tools.

Check for evidence of document destruction and search for incident-specific IOCs including exhibiting patterns within working directories or using particular hosts and accounts.

Identify, remediate and repeat: Identify all compromised hosts, user accounts, points of exfiltration, and other access points. Next, move to reset passwords, remove points of exfiltration, patch vulnerable systems being exploited for access, activate your incident response team, and set trigger points to alarm if the attacker returns. After this is complete, it's important to continue searching for IOCs to ensure remediation tactics are successful and then to repeat the process, if necessary.

With this model in place, you can identify the breadcrumbs that attackers leave behind when they compromise security defenses, enabling you to react quickly and efficiently to security incidents.

John Kuhn is a Senior Threat Researcher at IBM X-Force (www.ibm.com/security/xforce).

HITBSECCONF2016 AMSTERDAM

MAY 23–27 @ NH KRASNAPOLSKY

TECHNICAL TRAINING SESSIONS

- The ARM Exploit Laboratory
- The Art of Escape
- Advanced LTE Security & Insecurity
- Mobile Application Hackers Handbook: Live Edition
- Hacking the IoT with Software Defined Radio
- Powershell for Penetration Testers
- Advanced Web Hacking
- Pentesting and Securing IPv6 Networks
- SAP Cyber Security

Keynote:
Morgan Marquis-Boire
Director of Security,
First Look Media

Keynote:
Chris Evans
Head, Tesla Motors
Security Team

http://conference.hitb.org

Demanding accountability: The need for cyber liability

John Smith

Key drivers for change in any market are regulation and incentivisation, whether by legal liability or insurance cover. But in the cybersecurity market these agents of change remain immature and we're seeing unnecessary, grave breaches as a result.

GCHQ director Robert Hannigan pulled no punches last month when he stated that the free market is failing cybersecurity. And with 90% of large organizations and 74% of small businesses reporting that they had suffered a breach in 2015, and high profile breaches constantly splashed across the headlines, his concern is well placed as he argued that cybersecurity standards are "not yet as high as they need to be".

Just recently both Talk Talk and VTech breached through a common application vulnerability. SQL Injection, as it is known, has been listed on the industry standard OWASP Top 10 – a ranking for critical web application vulnerabilities that should be remediated as a matter of priority – for more than a decade. With avoidable cases such as these, important questions are raised regarding accountability for the breach.

While it is evident that companies that suffer breaches do face negative consequences (the CEBR and Veracode report on the business and economic consequences of inadequate cybersecurity outlined how share prices decline on listed companies following an attack), it is still the consumers and clients who are left to deal with fraudulent payments and changing details. Cases have already been reported since the Talk Talk breach of social engineering attacks, where scammers armed with consumers' personal details were able to trick them into handing over their banking details.

Just as, since the introduction of health and safety legislation fatal injuries to employees have fallen by 86% due in part to organizations fearing liability for such an event, so legal accountability regarding appropriate levels of corporate cybersecurity could be key to reducing the number of breaches.

CYBER INSURANCE POLICIES AND GOVERNMENT REGULATIONS WILL NEVER PROVIDE A FIX-ALL SOLUTION TO CYBERCRIME

Clarity is key

While one might expect the business community to be resistant to the introduction of more legislation that might land them in hot water or with hefty fines and compensation payments, recent research that Veracode carried out with the New York Stock Exchange indicated otherwise. In fact, nine out of 10 board directors who responded to the survey believe that regulators should hold businesses liable if they don't make reasonable efforts to secure data.

This may sound counter-intuitive, but it actually demonstrates how businesses are crying out for benchmarks and greater clarity regarding what a sufficient and responsible level of cybersecurity is.

The case of Wyndham Hotels in the US demonstrated why clarification is sorely needed regarding this benchmark. Earlier this year the Federal Trade Commission (FTC) successfully sued Wyndham Hotels for having "unreasonably and unnecessarily exposed consumers' personal data to unauthorised access and theft", following three breaches in just two years.

With the appeals court ruling affirming the FTC's authority for requiring companies to securely store customer data and punishing them if they fail to do so, American companies are left with little information other than that they may be held liable following a breach.

This trend looks to be extending globally; the British government launched an inquiry into the Talk Talk breach and the Hong Kong Privacy Commissioner is initiating a compliance check to see if the company had sufficiently adhered to data privacy principles.

Insurance steering the trend

While legislation in this space may be a while off, cyber insurance will be a key driver in helping set the standards for responsible levels of cybersecurity. Many companies already have cybersecurity insurance, and this market is set to triple to about $7.5 billion in the next five years. Those companies paying into these insurance policies will want assurance that their cybersecurity processes meet the required level to receive a return after suffering a breach.

While the majority of companies are buying cyber insurance to mitigate financial losses brought forth by liability claims, it will ultimately play a far greater role in changing the business community's approach to cybersecurity. Just as the evolution of fire insurance drove the creation and enforcement of minimum standards in the way buildings are constructed and protected, cyber liability insurance will begin to create a new baseline for cybersecurity best practices.

Cyber insurance policies and government regulations will never provide a fix-all solution to cybercrime. No network is impenetrable, and regulations certainly don't prevent cyberattacks nor are they likely to even cover the full financial impact of a breach with regards to impact of brand damage and loss in shareholder value.

However, without clearly outlining what a reasonable level of cybersecurity is, we will continue to see organizations failing to addressing the basics and consequently suffering avoidable hacks. With the ongoing proliferation of cyberattacks, we can no longer assume that organisations are doing enough to ensure the privacy of customer data.

When teenagers are able to access millions of customers' details using off-the-shelf cybercrime products, it is clear that due diligence has not been done. It is time for organizations to be held to account over preventable cyberattacks, in order to incentivise all industries to ensure their cyber security is up to scratch.

John Smith is a Principal Solution Architect at Veracode (www.veracode.com).

Events around the world

RSA Conference 2016

www.rsaconference.com - San Francisco, USA / 29 February - 4 March 2016.

Celebrating its 25th anniversary, RSA Conference continues to drive the information security agenda forward. Connect with industry leaders at RSA Conference 2016.

HITBSecConf2016 Amsterdam

conference.hitb.org - Amsterdam, The Netherlands / 23-27 May 2016.

HITB2016AMS features 2 and 3 days of technical trainings followed by a 2-day conference with a Capture the Flag competition, a technology exhibition and mini Haxpo hacker-spaces village for hackers, makers, builders and breakers.

Infosecurity Europe 2016

www.infosecurityeurope.com - London, UK / 7-9 June 2016.

Infosecurity Europe is Europe's number one information security event featuring over 315 exhibitors showcasing the most diverse range of products and services to 12,000 visitors.

Adding the cloud to your rainy day plan

Fan Lei

A solid Disaster Recovery/Business Continuity (DR/BC) plan is critical to a business. It significantly increases the survivability of an organization in an emergency.

Traditional DR/BC plans focus more on the redundancy directly owned and managed by the business – the workforce, business operations, services, physical and virtual information assets. With enterprise cloud solutions gaining popularity, the traditional DR/BC plan is up for a major change. Cloud vendors should now play critical roles in the DR/BC planning.

Cloud vendor selection and placement should be contemplated and strategized. Vendor co-operation and coordination should be properly established early in the game.

Analysis

Consider this scenario: Your IT team just completed a critical project - they migrated your enterprise messaging system to a reputable hosted Exchange provider. All the outdated on-premise servers were properly retired. Hooray! Your team offloaded a major daily maintenance task (or burden) to the cloud, and they are ready to move on.

You are confident about the provider's reputation and services. They have given you a shiny five nines (99.999%) guaranteed service-level agreement (SLA). You will be fully refunded with that month's subscription if there is any downtime. This all sounded sweet, but yes, there will be downtimes. You also know, deep down in your heart, that the refund could not compensate for the loss of the service being unavailable for even an hour.

Something will go wrong, even at a world-class data center with full redundancy – there will be hacking activities (DDoS for example), natural disasters, and human errors (configuration errors, system bugs, maintenance issues, or an intern accidentally unplugging a network cable).

In a nutshell, clouds do not magically form and sustain themselves - they are systems designed, built and maintained by humans. You could convince yourself that by moving your IT infrastructure, applications and data into the cloud, you are a 100% safe, and that the cloud “up there” will never fail, but the truth is that, at certain point of time, for a couple hours or several days, they will, and in the worst of cases, they might never be restored again.

For our scenario, let’s say your business is located in the US. This provider’s two major US data centers have been under heavy DDoS attacks, but their European datacenter is fine. The redundancy kicked in, however performance is poor due to lower capacity at the EU datacenter.

The battle with the hackers lasts about 5 days, and during that time, you are pulled into the executives’ offices many times. You have to explain how the situation is now out of your local IT department’s hands, and wish you could fire this provider right away.

Halfway through these miserable five days, you have probably started to think about replacing this provider. You know it will be a lengthy process – from soliciting interviews, selecting vendors, checking references, reviewing, negotiating and signing the contracts, to eventually provisioning the services. The process will take at least a month, if not longer.

But what if you had a secondary cloud vendor already picked out and ready for providing the service since the very beginning? A vendor that you have on hand, with all the user accounts/mailboxes provisioned at the same time as the primary one, but inactive or synced with less frequency with the primary vendor? A warm or cold DR site/service in the cloud?

The outcome of the situation would be completely different. When the attacks start, and you notice that the EU datacenter can’t handle the load, you put your IT hero’s cape on, and initialize a well-planned sequence defined in your DR/BC plan:

- You tell the management about the hacking activities at the primary cloud provider and the associated business impact if you continue to use their poorly performing EU datacenter
- With the management’s approval, you send out an organization-wide notification about the upcoming change
- You inform the secondary provider that you will switch them from warm/cold to hot, and that they need to ensure all storage/processing/bandwidth are ready (these things need to be stated in the DR/BC plan, the secondary provider must be aware of these provisions, and the set up has to be regularly tested like it would be in a normal, physical DR site)
- You adjust MX records and the anti-spam solution to point to the secondary provider (this can be automated, of course)
- You help the high impact accounts switch to a new Outlook Profile or provide them a new OWA link, then gradually migrate the low impact accounts. These actions should all be pre-defined in your plan, and you could either provide user training on the new Profile setup during the DR test phase, or automate this process using tools like GPO or script.
- After the migration is completed and stabilized, you regularly check the capacity and performance of the secondary provider to ensure business continuity.
- After 5 days, when you are informed by the primary provider that the issue has been resolved, you can smile and take your time to rethink your company’s relationship with them going forward. It is up to you (and, of course, the management) to determine if you will continue using them as the primary provider, a secondary provider at a discounted rate, or completely terminate the contract.

The moral of this story is that, with more and more critical business and information technologies being moved into the cloud, you should start reevaluating your DR/BC strategy - a traditional one might be no longer sufficient to help your business continue its operation during a disaster.

Have you assessed your catalog of cloud vendors and asked yourself whether they are now your single points of failures? Do you have backup players if the primary ones cannot deliver what they promised during a disaster or if they go out of business? What would be the impact on your business if one of these cloud providers fails to deliver? And lastly: even if you have considered the cloud factor as part of your DR/BC plan, and you have contracts with other cloud providers as backup, are they aware of their roles, the processes they need to follow and the expectations they need to meet should the need arise? In other words, does the DR/BC plan go beyond the organization boundary and has it been properly communicated to the key stakeholders?

If this article makes you suddenly realize that you have a single cloud provider for critical business and IT functions, it is time to reevaluate your DR/BC plan

Business recommendations

Yes, it all sounds easy - just add another cloud provider as a backup at the beginning. But the reality is, there are a lot of things to consider.

Contract

Always make sure you draft your contracts properly with your primary and secondary providers. State clearly the responsibilities of both parties – what they offer and what they don't, how they coordinate with each other during a prolonged outage, what technology they will use to sync, what will be the service charge pre- and post- disaster (especially for secondary providers, as they might charge considerably lower when they are in standby mode, but expect a rate hike after they flip to being the primary provider).

A lot of cloud providers adopt a pay-as-you-go type of service agreement, but in case you need to use a long-term contract to get price advantage, make sure the contract can be terminated under conditions such as a severe outage, not just based on its duration. Involve your legal department for a thorough contract review and try your best to include all the possible conditions during operations.

Communication

You want to communicate with both providers, let them know your intentions and plans. By knowing you have a thorough DR/BC plan with a backup player, the primary provider will hopefully get motivated to continue improving, instead of providing an indifferent service after an over-the-top sales pitch.

From a business perspective, by reaching out to multiple vendors you will always have a better sense of the pricing. This will help you during the contract negotiation phase.

Plan

If this article makes you suddenly realize that you have a single cloud provider for critical business and IT functions, it is time to reevaluate your DR/BC plan. You should start with a list of cloud vendors, the services they provide, and the business impact associated with those services. You will need to prioritize.

Does every single cloud provider need a backup? Maybe not, it all depends on the business impact, your budget and your risk appetite. Once you have a list of priorities or, even better, a list that quantifies business impact and risk, you can start to engage different providers. And, after this round, you should incorporate this process for on-boarding new cloud providers for future projects.

You engage the potential secondary cloud provider like you would normally do with the primary, except with a different initiative and business requirement. You might not need all their services. Similar to what happens in a physical data center scenario, a virtual one can be cold or warm.

Let's continue to use the messaging system example. A secondary provider with all mailboxes provisioned but not fully synced can be considered a cold site. All the secondary provider needs to do is to ensure users and associated mailboxes get created either via automation or manual configuration (this also applies to the new user onboarding process).

In an emergency, when the company switches to this provider, users will see empty mailboxes. They can send and receive new emails from that moment on, but existing mails will start flowing in gradually from the primary provider once the issue is resolved, or they will simply not have them with the backup provider - it all depends on the expectations laid out in the DR/BC plan.

If the site is warm, that means there are some sync mechanisms in the back-end between the two providers (not real time, but maybe once a week). And when the users switch to a warm site, instead of completely blank mailboxes, they will see partial (if not complete) mailboxes with messages going up to the last sync.

This is all about setting up your plan and being up front with your expectations. You have to state everything accurately so that end users know exactly what will happen and what they can expect during and after a disaster.

You need to have extensive testing and training initially, then incorporate frequent tests and simulations afterwards

People and processes

You always want to include the right people – both internal and external stakeholders - during your planning phase. When it comes to the the latter, you want to make sure both the primary and secondary providers' dedicated account executives and technical contacts are invited to your meetings. Cooperation and coordination between the two providers is key to your DR/BC plan's success.

You have to ensure that, even though they are in a competing position, they consider each other friends instead of foes. Most of the time, prestigious providers will demonstrate their professionalism, but just in case, you should always enforce the terms in your separate contracts and build up protocols and procedures both parties will accept and follow.

After the plan and processes are shaped, you are now heading for the fun part. You need to have extensive testing and training initially, then incorporate frequent tests and simulations afterwards. Depending on your business requirements, you will need to test your DR/BC plan at least once a year – you need to provide proper training to key personnel, but you also need to make sure that the capacity of your secondary service provider follows your organization's growth.

Also, from the end-user experience perspective, a virtual DR/BC scenario differs from a traditional one, where all the infrastructure, systems, applications are mirrored and managed by the company's local IT folks, and during a disaster, when users switch to the backup environment, the user experience mostly remains the same.

In a cloud based DR/BC this is obviously not the case. Some solutions from a single software vendor such as Exchange, Sharepoint, or WordPress might look the same (except for different versions or provider specific administration portals), but other hosted applications or services, such as file sharing services, call centers, project management, content management, collaboration services might be significantly different from each other.

Even if the hosting providers host the exact same applications, you are still at the mercy of their software versioning and upgrade planning.

As IT professionals, you know what discrepancies software can present between different versions. And I am sure during a chaotic disaster, you will hate to receive help desk calls with questions like “Where is my round ribbon button? Why is it a square now?!” Thus, ongoing testing, user awareness training and process education is critical to your new plan’s success.

Always start with evaluating the technologies currently in use

Technology

A rule of thumb for many organizations, especially those without abundant IT budgets: always start with evaluating the technologies currently in use. Before you reach to a backup cloud provider, consider what you have in-house. If you let a hosting provider take over your messaging infrastructure, will it make sense to retire all the on-premise messaging servers? Maybe retire only half of them, and leave the rest as an on-premise DR/BC messaging site, a hybrid/co-located DR/BC plan.

If you have Rackspace host your website, do you really need to reach to Azure or Amazon for another array of virtual servers? Maybe utilize some retired servers as backup web servers, place them in your DMZ zone, fully synced with your Rackspace web hosting servers? Same thing for VDI - if you outsource VDI service to a cloud provider, consider using some on-premise servers to form a smaller scale farm just for emergencies.

You may say “No. This is not ideal - it will still consume manpower, space, electricity, licensing, etc., which defeats the purpose of cloud hosting.” But you can look into some alternatives. For messaging, consult your existing spam protection solution provider, see if they offer some sorts of mail spooling services in an emergency. For the web hosting, look into some CDN and web caching technologies instead of keep full web servers. And for VDI, look at some application delivery services just to focus on core line of business application delivery during a disaster, instead of full virtual desktops.

Some alternative solutions might just work fine without involving another fully managed cloud provider; some might work with limited capacities, features or durations, so it could cause troubles for a prolonged catastrophe. Then it is up to the business to determine if the alternatives serve its DR/BC requirements. At the end of the day, it all comes down to the risk acceptance at the business level.

The next thing you need to consider carefully is security. You need to make sure that the second provider meets the same security requirements as your primary one. Your security cannot be sacrificed because you are in an emergency.

This is the fundamental security principle you have to follow during a DR/BC scenario. If you use a cloud provider to send encrypted emails for highly classified communications, then the secondary encrypted email service provider needs to meet the same the encryption and authentication standards.

Another example would be if you have sensitive data that cannot go beyond the border: you have to make sure the primary cloud provider does not have any data center (or data communication) in other countries, and you have to go through the same evaluation for the second one.

Service provider recommendations

Before diving into the summary, I would like to add a comment from the cloud provider's angle. The entire article is trying to remind the corporate system/security professionals and management about the importance of weighing in the cloud factors while evolving their DR/BC plan.

I believe cloud computing will continue to proliferate and bring benefits to businesses, but will also increase their concerns from a security and continuity perspective. In my opinion, this will actually introduce more business opportunities for the cloud providers.

Virtual or cloud based DR/BC sites and services can be added to a provider's official service catalog as an offering. It provides more opportunities for newer and smaller cloud player to at least get their feet into the door of larger organizations. They might not be picked as a primary cloud provider for certain services due to many reasons such as size, reputation, and time in business, but they can prove themselves by starting with virtual DR/BC services at a lower risk.

Eventually this can become a standard process for smaller cloud players to get more market exposure, grow their revenues and client portfolios, and most importantly, build up their brand image.

The virtual or cloud based DR/BC concept also creates opportunities for CASB (Cloud Access Security Broker) vendors. With the increase of CASB vendors in the market, we could tell more businesses not only start to query how to use cloud efficiently, but also how to secure and provide governance of this technology.

As CASBs act more like a gateway or proxy between businesses and cloud providers, and a lot of mature cloud players have already provided APIs for CASB vendors to integrate with, it will not be surprising to see CASB appliances or services with added DR/BC features - such as proactive monitoring and seamless switching between primary and secondary cloud providers for particular services - in the near future.

Fan Lei is the Information Security Manager of Americas at Takeda Pharmaceuticals (www.takeda.us).

The slings and arrows of encryption technology

Ben Desjardins

A strong argument can be made for the claim that no technology has played a bigger role in the growth of the Internet as a platform for commerce than the core encryption technologies of Secure Sockets Layer (SSL) and Transport Layer Security (TLS). Each major milestone from these encryption technologies, from creation through commercialization and mass adoption, has triggered a subsequent rise of e-commerce.

Consider the growth rates of SSL certificate adoption and how closely it correlates with those of the Internet. From 1994 through 1995, the Internet grew at a rate of a little over 100% per year. However, from 1995 through 1997, that growth exploded to over 400% per year. Amid this growth Netscape Communications introduced SSL version 3.0, consistently cited as one of the major triggering events behind the growth of the World Wide Web, and e-commerce in particular.

The more recent history of encryption technologies, and SSL/TLS in particular, has not all been positive. A series of severe, high-profile vulnerabilities have caused the technology industry to push hard on replacing now insecure versions of the technology. Increasingly, those with malicious intent have used encryption to create additional challenges for security tools and professionals to detect attacks, both in the digital and physical world.

Encryption marches forward

Despite some high profile security issues, SSL and TLS remain the standard for ensuring secure communications and commerce across the Web. When SSL was conceived and introduced, a relatively small number of businesses had websites, and even fewer were managing commerce or critical aspects of their business operations online. Today, few businesses of reasonable size don't have an active website; at a minimum, they are driving consumer engagement with the intention of properly securing communication (if not transactions) through their website.

According to Netcraft, the use of SSL by the top one million websites has increased by 48% over the past two years. As more and more sites add SSL or TLS capabilities, user adoption will also increase.

The technology industry has actively been pushing broader adoption of SSL/TLS. The Let's Encrypt project has launched a new, free certificate authority in an effort to move more users over to encrypted online communication and commerce. The Electronic Frontier Foundation, in collaboration with the TOR Project, is pushing HTTPS Everywhere as a way to simplify the process of enabling encryption for both end users and web site owners.

A new challenge: The weaponization of SSL

Today, there is a new set of challenges facing organizations leveraging encryption technologies

Cyber attacks, including Distributed Denial of Service (DDoS) and advanced web application attacks, are increasingly leveraging encrypted traffic as an attack vector, further challenging many cyber-threat solutions that are currently in place. Most cyber attack mitigation technologies do not actually inspect SSL traffic, as it requires decrypting the encrypted traffic. According to Radware's 2014 Global Network and Application Security Report, as much as 25% of attack activity today is using SSL-based attack vectors.

SSL-based attacks take many forms, including:

- Encrypted SYN floods: These attacks are similar in nature to standard, non-encrypted SYN flood attacks in that they seek to exhaust the resources in place to complete the SYN-ACK handshake, only they further complicate the challenge by encrypting traffic and forcing the use of SSL handshake resources.
- SSL renegotiation: These attacks work by initiating a regular SSL handshake, and then immediately requesting for the renegotiation of the encryption key. The tool constantly repeats this renegotiation request until all server resources have been exhausted.
- HTTPS floods: These attacks generate floods of encrypted HTTP traffic, often as part of multi-vector attack campaigns. Compounding the impact of "normal" HTTP floods, encrypted HTTP attacks add several other challenges, such as the burden of encryption and decryption mechanisms.
- Encrypted web application attacks: Multi-vector attack campaigns also increasingly leverage non-DoS, web application logic attacks. By encrypting the traffic masking these advanced attacks, they often pass through both DDoS and web application protections undetected.

SSL and encryption protect the integrity of legitimate communications, but they also obfuscate many attributes of traffic that are used to determine if it is malicious or legitimate. Identifying attack traffic within encrypted traffic flows is akin to finding a needle in a haystack - in the dark.

Most anti-attack solutions struggle to identify potentially malicious traffic from encrypted traffic sources and to isolate that traffic for further analysis (and potential mitigation). In fact, in a 2013 report, Gartner Research noted that less than 20% of organizations using common security technologies (firewall, IPS) are inspecting inbound or outbound encrypted traffic.

The other major advantage that SSL attacks offer to attackers is the ability to put significant computing stress on network and application infrastructures they target. The process of decrypting and re-encrypting SSL traffic increases the requirements of processing the traffic, in many cases beyond the functional performance of devices used for attack mitigation.

Even for more attack-focused technologies, there are many gaps. Most are inline and stateful, and cannot handle SSL encrypted attacks, making them vulnerable to SSL flood attacks.

Even fewer of these solutions can be deployed out-of-path, which is a necessity for providing protection while limiting impact on legitimate users. Many solutions that can do some level of decryption tend to rely on the rate limiting the request, which results in dropped legitimate traffic and effectively completes the attack.

Finally, many solutions require the customer to share actual server certificates, which complicates implementation, certificate management and forces customers to share private keys for protection in the cloud.

Strategies for protection from a growing threat vector

The fact that many organizations are seeing an increase in encrypted traffic is, in general, a good thing. It is, however, a complicating factor when it comes to encrypted cyber-attacks.

The bottom line is that to provide effective protection, solutions need to delivery full attack vector coverage (including SSL), high scalability to meet the growing demands of the consumer, and innovative ways to minimize (if not eliminate) threats. They also need to handle management of encryption technologies (today predominantly SSL/TLS) in a manner that can be operationalized effectively and efficiently.

Here are some considerations you should keep in mind when looking at cyber attack protections if you want full coverage from encrypted attacks:

- Stateless mitigation: As previously mentioned, many security technologies are stateful in nature, meaning they maintain state throughout a session. This requires additional computing resources and poses the risk of filling session tables, at which point the device will fall over. Be sure the technologies you're depending on for encrypted attack protection are stateless in nature to ensure ability to scale to the higher demands of these attacks.

- Asymmetric deployment options: Most security technologies rely on a symmetric deployment model, meaning they are in the path for both inbound and outbound traffic. This has key benefits for some aspects of security, but in the case of encrypted attack mitigation, adds unnecessary computational strain on the solution. Look for technologies that can support an asymmetric deployment where only ingress encrypted traffic passes through the mitigation engine.

- Certificate management: Some security technologies that claim to cover encrypted attacks do so at the burden of operations teams that manage server certificates. Specifically, these technologies require the sharing of the actual web server certificates, meaning any change to these certificates have to be replicated in the security solution. Look for technologies that can manage the inspection of encrypted traffic through use of certificates legitimately issued to the organization but not tied specifically to the web server.

- Ensuring integrity of the trust model: One of the principles behind web site authentication through certificates is the confirmation to the end customer that they are engaged in a "private" communication with the intended organizations. Some service providers offer SSL capabilities that break this trust model and actually initiate a secure channel between the unknowing end user and themselves. In so doing, they essentially dupe the end user into trusting them with the shared information (as well as the service provider's certificate management).

- Optimizing legitimate user experience: As is so often the case, IT and security professionals are left to strike a balance between having lightweight security and creating such a locked-down user experience as to chase away customers. This balancing act plays out in encrypted attack mitigation as well, where some technologies employ something of an on/off switch for decrypting all encrypted traffic when a potential attack is detected. Look for technologies that can selectively apply challenge-and-response specifically to traffic identified as suspicious, thereby maintaining user experience for legitimate users sending through encrypted traffic.

The year ahead

With the strong push from industry and standards bodies to move off of SSL and earlier versions of TLS, combined with the drivers for dramatic expansion of encryption, it is safe to assume 2016 will be another eventful year when it comes to encryption. Statistics already show a troubling state of affairs with regard to encrypted attacks. Attack volumes from this vector are up (and increasingly complex) while many continue to lack the ability to inspect encrypted traffic. Given the inevitable expansion of encrypted traffic flows (legitimate and malicious) into organizations, now is the time to better understand the nuances of encrypted attack detection and mitigation and to start developing a strategy for protection.

Ben Desjardins is the Director of Security Solutions at Radware (www.radware.com). He focuses extensively on the competitive landscape for anti-DDoS, WAF and anti-scraping technologies.