

INFOSEC TIPS I LEARNED FROM GAME OF THRONES



CLOSING SSL IMPLEMENTATION GAPS
DISSECTING THE NEWLY-DISCOVERED
DESIRE FOR CONTROL AND PRIVACY

THE IMPACT OF
SECURITY BREACHES
ON AUTHENTICATION

THECUS N5550
NAS SERVER
INSIDE & OUT

WHAT INSPIRED YOU
TO START HACKING?

People spend
over 700 billion
minutes per month
on Facebook.

Research by Facebook



The Internet is full of temptations. Can your users resist them?

The Internet is one of the most useful resources in the office – but only if you can manage the potential issues:

- » Productivity losses due to employees spending time on sites with little work-related content
- » Security risks: from unsecure sites and from legitimate sites that have been compromised
- » Bandwidth losses from people downloading large files or watching streaming media.

Run the 30-day trial of GFI WebMonitor to find out exactly how your Internet connection and remote machines are being used and what security risks you are exposed to.

Quality web filter

Comprehensive web security

Highly competitive pricing

Thousands of customers

Download your free trial from <http://www.gfi.com/webmon>



GFI WebMonitor™

Web security, monitoring and Internet access control

TABLE OF CONTENTS

Page 05 - Security world

Page 12 - Six infosec tips I learned from Game of Thrones

**Page 16 - Dissecting the newly-discovered desire for control
and privacy**

Page 21 - Incident response and failure of the "Just Fix It" attitude

Page 25 - How to learn information security

**Page 27 - Who are you? The impact of security breaches on
authentication**

Page 31 - Malware world

Page 35 - Thecus N5550 NAS Server inside and out

Page 41 - Report: Hack In The Box Amsterdam 2014

Page 43 - Ensuring the integrity of Rostelecom's Wi-Fi network

Page 46 - What inspired you to start hacking?

Page 49 - Events around the world

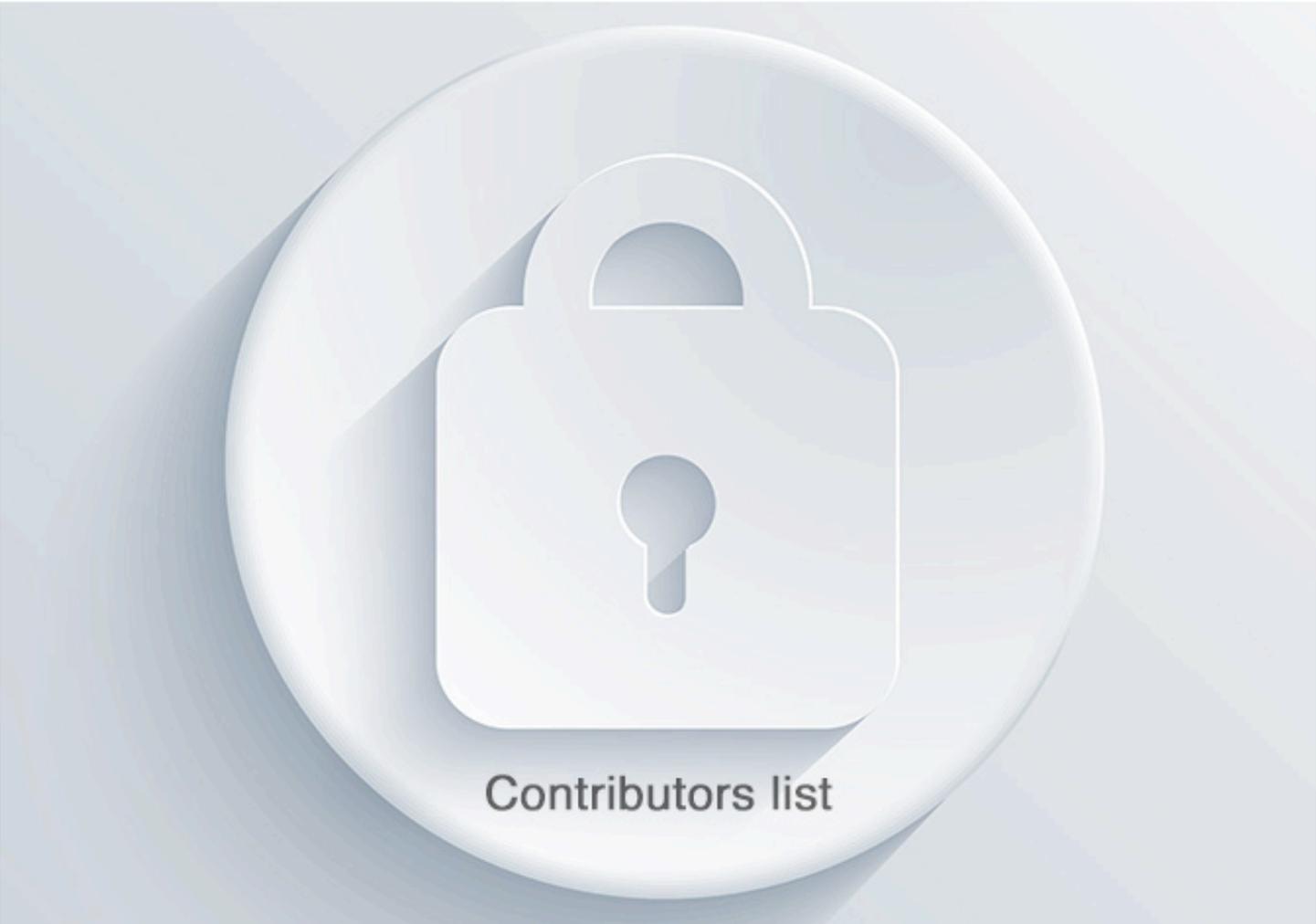
**Page 50 - Beyond Heartbleed: Closing SSL implementation gaps
within our own networks**

Page 55 - Ironclad incident response

Page 59 - Hands-on fun at HacKid 2014

Page 61 - Are you ready for the day when prevention fails?

Page 65 - Why privacy engineering is needed



Contributors list

- **Chuck Archer**, CEO and Executive Chairman of Covata USA.
- **Christiaan Brand**, co-founder and CTO of Entersekt.
- **Tom Cross**, Director of Security Research at Lancope.
- **Chris Hoff**, VP, Strategic Planning - Security Business Unit at Juniper Networks.
- **Mike Horn**, Vice President of Threat and Response Products at Proofpoint.
- **Corey Nachreiner**, Director of Security Strategy and Research at WatchGuard Technologies.
- **Kai Roer**, Senior Partner at The Roer Group.
- **Jason Sabin**, VP of Research & Development at DigiCert.
- **Ramil Yafizov**, Systems Engineer at Nominum.

Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

Feedback and contributions: **Mirko Zorz**, Editor in Chief - mzorz@net-security.org

News: **Zeljka Zorz**, Managing Editor - zzorz@net-security.org

Marketing: **Berislav Kucan**, Director of Operations - bkucan@net-security.org

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 the explicit permission from the editor.



DARPA's Cyber Grand Challenge offers \$3.75 million in prizes



Computer security experts from academia, industry and the larger security community have organized themselves into more than 30 teams to compete in DARPA's Cyber Grand

Challenge, a tournament designed to speed the development of automated security systems able to defend against cyberattacks as fast as they are launched.

The CGC is the first computer security tournament designed to test the wits of machines, not experts. The final competition is scheduled to co-locate with the DEF CON Conference in Las Vegas in 2016.

At the event, computers that have made it through a series of qualifying events over the next two years would compete head-to-head in a final tournament. Custom data visualization technology is under development to make it easy for spectators—both a live

audience at the conference and anyone watching the event's video stream worldwide—to follow the action.

35 teams from around the world have registered with DARPA to construct and program high-performance computers capable of competing in the Cyber Grand Challenge. Most competitors have entered on the "open track" available to self-funded teams.

A parallel "proposal track" consists of teams invited and partially supported by DARPA to develop automated network defense technology. Those teams represent a mix of participants from industry and academia and will receive seed funding from DARPA until their performance is tested in open competition involving all teams at a major qualification event scheduled for June 2015. Additional teams may register to participate through November 2, 2014.

The winning team from the CGC finals stands to receive a cash prize of \$2 million. Second place can earn \$1 million and third place \$750,000.

Google unveils source code for Chrome encryption extension



Google has made publicly available the source code for a new Chrome extension that helps users encrypt, decrypt, digitally sign, and verify signed messages within the browser using OpenPGP.

The extension, dubbed End-To-End, has not yet been released in the Chrome Web Store. "We're just sharing the code so that the community can test and evaluate it, helping us make sure that it's as secure as it needs to be before people start relying on it," Stephan Somogyi, Product Manager, Security and Privacy at Google noted.

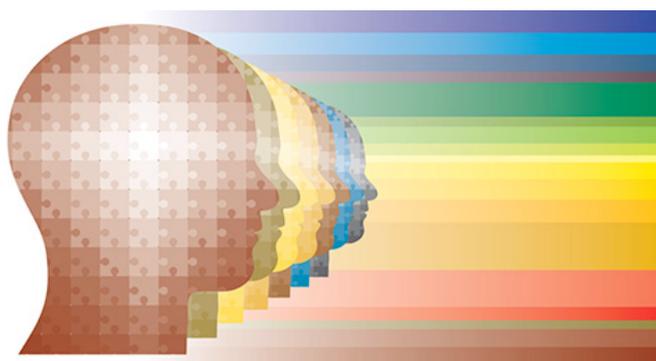
The alpha release of the extension is built upon a newly developed, custom JavaScript-based crypto library, and implements the OpenPGP standard for key generation, encryption, decryption, digital signing, and signature verification.

With the extension, the body of the message (but not the email subject line and list of recipients) is encrypted and decrypted locally in the browser. For those worried that their private key might not be safe, the company advises users to choose a passphrase for their keyring, so that private keys are stored encrypted in localStorage. While in memory, the key is protected by the Chrome sandbox.

The company has asked users not to use the code to build an extension and submit it to the Chrome Web Store before they do. "The End-To-End team takes its responsibility to provide solid crypto very seriously, and we don't want at-risk groups that may not be technically sophisticated — journalists, human-rights workers, et al — to rely on End-To-End until we feel it's ready," they said. "Prematurely making End-To-End available could have very serious real world ramifications."

The release of the code has piqued the curiosity of many cryptographers and security researchers, and Google is offering an added incentive for them to poke around: any security bug they find can be submitted to the company's Vulnerability Reward Program and is eligible for a monetary prize.

Most people have done nothing to protect their privacy



Over 260 million people have been victims of data breaches and increased risk of identity theft since the Target revelations, yet nearly 80 percent have done nothing to protect their privacy or to guard their financial accounts from fraud, according to idRADAR.

The poll showed that most people don't even take the time to change their passwords. Less

than 10 percent adopt new passwords monthly and about 58 percent said they would only do it when forced to by a website or vendor.

Roughly 93 percent of the adults surveyed think that after a breach, they would want the company involved with the breach to offer them free credit monitoring. Further, 70 percent of consumers say they still use their debit cards, despite the warnings by retailers of the increased risk of debit over credit cards.

"Clearly, consumers do not want to take responsibility for protecting themselves before or after a serious breach. They want someone else to worry about it," said Tom Feige, CEO of idRADAR.

According to the survey, 55 percent are more concerned about the threat of data breaches than about the government monitoring their private phone conversations or their email.

Some governments have direct access to Vodafone networks



Telecommunications giant Vodafone has released its first-ever Law Enforcement Disclosure Report, and among the things revealed in it is the scary fact that some countries have direct and permanent access to the company's

servers and to customer communications via their own direct link.

"In most countries, governments have powers to order communications operators to allow the interception of customers' communications," they noted. "Lawful interception is one of the most intrusive forms of law enforcement assistance, and in a number of countries agencies and authorities must obtain a specific lawful interception

warrant in order to demand assistance from an operator."

"In most countries, Vodafone maintains full operational control over the technical infrastructure used to enable lawful interception upon receipt of an agency or authority demand," they shared.

"However, in a small number of countries the law dictates that specific agencies and authorities must have direct access to an operator's network, bypassing any form of operational control over lawful interception on the part of the operator. In those countries, Vodafone will not receive any form of demand for lawful interception access as the relevant agencies and authorities already have permanent access to customer communications via their own direct link."

The company has not revealed which particular countries these are, as the local law also prohibits them to share that information.

Security at higher education institutions



SANS announced the results of its inaugural survey of security in institutions of higher education, in which nearly 300 higher education IT professionals answered questions about the challenges

of making their environments secure while maintaining the openness needed by faculty, staff, students and benefactors in traditional educational models.

The majority of respondents represented IT staff working predominately at US institutions: 48% at public universities, 19% at private universities, 10% at private colleges and 7% at two-year public/community college institutions. They represent a good blend of security management and technical security roles.

"IT staff at colleges and universities always feel as if they are isolated—that no one else faces the same challenges, but this isn't the case," says survey author Randy Marchany.

"Our message from this survey is that you're not alone. All of us share the same problems in creating and maintaining a secure campus." Of the organizations represented in the survey, only 45% have formal risk assessment and remediation policies in place. The situation is worse in smaller institutions, where only 31% have such policies. Yet all respondents say their organizations are required to secure a variety of personally identifying information across different types of networks, with often competing privacy requirements.

Yet, only 57% classify their sensitive data and provide guidelines for safe data handling, and even fewer (55%) define appropriate owner, user, and administrative roles.

Staffing and budgeting for institutional security are key reasons why organizations are failing to protect their confidential data, according to the survey. While 64% believe they need 1–5 FTEs of additional staff, 43% believe they cannot pay premium rates for skills needed. Lack of budget, selected by 73% of respondents, is deemed a cause of not being able to maintain or increase IT staffing.

Cyber Security EXPO comes to London



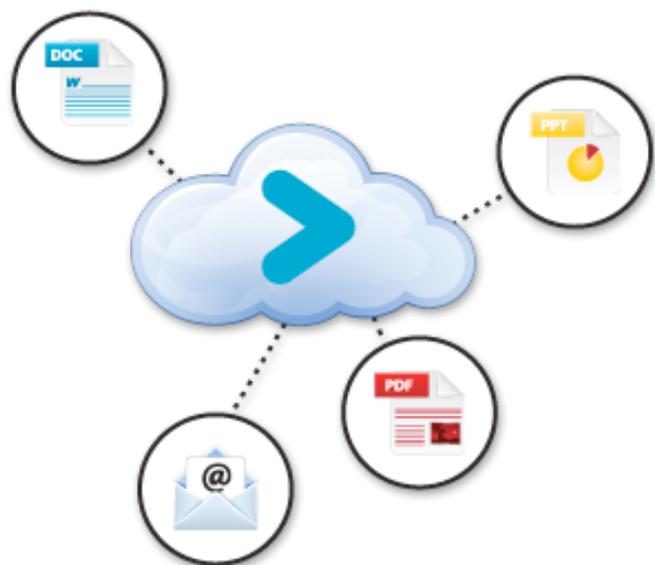
Brand new for 2014, Cyber Security EXPO (www.cybersec-expo.com) is the new place to be for everybody wanting to protect their organization from the increasing commercial threat of cyber attacks. The event has been designed to provide CISOs and IT security

staff the tools, new thinking and policies to meet the 21st century business cyber security challenges. At Cyber Security EXPO, discover how to build trust across the enterprise to securely manage disruptive technologies such as:

- Cloud computing
- BYOD
- Social media
- Identity and access
- Encryption
- GRC
- Analytics
- Data.

The event delves into business issues beyond traditional enterprise security products, providing exclusive content on behavior trends and business continuity. Cyber Security EXPO will host the first Hack Den, a live open source security lab. In the Den, you'll be able to share ideas with White Hat hackers, security gurus, speakers and fellow professionals.

Proofpoint launches Proofpoint Content Control



Proofpoint (www.proofpoint.com) launched a new cloud-based solution for control of confidential, private, and regulated data. Proofpoint Content Control, in an easy-to-deploy and user-friendly addition to the industry-leading Proofpoint Enterprise Privacy suite, provides complete visibility and control

over sensitive content such as customer records, patient information or credit card data across the enterprise.

In the last year, it is estimated that nearly 100 million records were exposed via data breaches, including health records, passwords, and even the personal information of executives at the Federal Reserve. Even well-known and secure high-tech and defense organizations have lost significant intellectual property and personally identifiable information. Yet at the same time, employees must work remotely often or in shared workflow environments such as Sharepoint, so enterprises must have more information stored in more places than ever before – and thus are more exposed to an attacker in a breach.

Proofpoint Content Control enables enterprises to rapidly identify and pinpoint the location of data that poses a risk for theft, loss or breach of regulatory compliance, and automates the remediation of these risks by moving or deleting the offending content, minimizing the attack surface and risk exposure.

Microsoft battles US search warrant requesting customer emails stored abroad



Late last year, a federal magistrate judge in New York has granted prosecutors a search warrant in a drug case that would force Microsoft to hand over to the feds a customer's email stored in their Dublin data center.

Microsoft is contesting the decision, arguing that if that part of the order is allowed to stand, the warrant "would violate international law and treaties, and reduce the privacy protection of everyone on the planet."

Microsoft maintains that "the Government cannot seek and a court cannot issue a warrant allowing federal agents to break down the doors of Microsoft's Dublin facility.

Likewise, the Government cannot conscript Microsoft to do what it has no authority itself to do - i.e. execute a warranted search abroad."

They claim that if the initial court decision is confirmed, it will negatively impact on Microsoft's business and the competitiveness

of US cloud providers, as it will erode the trust of foreign governments and companies.

Arguing for the government's side, Preet Bharara, United States attorney for the Southern District of New York, says that Microsoft is wrong in equating physical and digital search warrants, and that simply saying that the wanted data is stored abroad should not enable the company to avoid complying with the court order.

He also says that Microsoft does not check whether the location information provided by users is correct.

"A person planning or committing crimes in or affecting the US could easily reduce the risk of detection by providing false information about his place of residence, causing Microsoft to store responsive records outside the US and beyond law enforcement's ability to obtain the records in a timely manner, if at all," he noted.

Privacy-minded users and advocates are following the case closely, as it could decide the future of privacy laws around the globe.

Oral arguments before the judge are scheduled for July 31, and it's still difficult to say when a decision will be made (and whether the losing side will appeal).

Safari to include privacy-protecting search engine



Apple announced the inclusion of DuckDuckGo, the search engine that doesn't track its users, in the future versions of Safari on iOS and OS X. This makes DuckDuckGo the first private search engine to be added to a major browser.

DuckDuckGo recently launched a reimagined and redesigned version that showcases a more powerful way to interact with their "instant answers"—information that appears above links and ads for recipes, videos, and hundreds of other topics.

DuckDuckGo's instant answers are open source, allowing anyone to contribute ideas and code to them.

In 2013, DuckDuckGo received over one billion searches as people flocked to services that make privacy a primary focus. "A significant percentage of people prefer our search experience and we're delighted to welcome Safari users," said Gabriel Weinberg, DuckDuckGo's CEO and founder.

Life after TrueCrypt



While speculation continues around the fate of popular disk encryption software TrueCrypt, Sophos conducted a survey of over 100 IT professionals regarding their use of encryption, including TrueCrypt.

Key findings:

- One-third of IT professionals that use cryptography use TrueCrypt in some fashion
- 68% of TrueCrypt users have used the software for business
- One-third of survey respondents use encryption provided by operating system

vendors such as Microsoft's BitLocker or Apple's FileVault

- One third of survey respondents are using a commercial solution or are not sure what is being used
- The news surrounding TrueCrypt has made 64% of respondents think critically about encryption.

"Many TrueCrypt users appear to have been unaware of its unclear pedigree, and considering that 68% of TrueCrypt users use it in a business environment, it appears this situation has been a bit of a wake-up call," said Chester Wisniewski, senior security advisor at Sophos.

"Apple, Microsoft and other commercial players are unlikely to stop supporting integrated encryption moving forward, in fact they will likely double-down on their investment after the allegations being made by Edward Snowden. Thinking critically about not just your laptops, but servers, desktops, cloud and mobile devices could result in organizations making changes that strengthen their security stance resulting in a positive outcome from this whole incident."

Automatic updating of Android apps becomes riskier



Google has made unwelcome changes to the way new app permissions are disclosed to users: no warnings will be shown if a new permission is in the same category as an old one that has previously been accepted.

The change has been introduced with the recently released new version of the Play store app, and has apparently made to streamline the installing of updates and to avoid confusing users.

With this update, a user who has previously permitted an app to access the device's coarse GPS location will not be notified when the new version of the app starts collecting information about the device's fine location, as

both permissions belong to the same category. Similarly, an app that initially only had the permission to read the call log could now be updated to initiate phone calls without the user's knowledge. Or if it originally was permitted to read the contents of the SD card, it can be updated to write to it. Find out more about the different permission groups here.

"Unfortunately, most groups contain at least one 'innocent' or common permission that many apps on the Store use next to some more nasty ones," noted a software developer that goes by the online handle "Tubeman," who created an app named Permission Tester to test for this "latest Google security screw up."

If you are not comfortable with this new change, you can prevent it by turning off auto-updates for specific apps by opening the Play Store app, touching the app's icon, selecting "My Apps", selecting the app, and unchecking the box next to "Auto-update" in the Menu.

GFI Software expands GFI Cloud Suite



GFI Software (www.gfisoftware.com) announced the addition of remote control and remote access capabilities as part of a major update to GFI Cloud, the company's IT platform for SMBs. GFI Cloud enables IT administrators to easily manage and secure servers, workstations, laptops and mobile devices from a single, intuitive, Web-based user interface.

Based on the technology used in the popular TeamViewer remote access utility, Remote

Control in GFI Cloud enables admins to connect, take control and screen share with a user's client computer with just one click of the mouse – launching a secure connection within the GFI Cloud web console and allowing the admin to have immediate access to the rest of the security and network management modules they have also purchased.

Remote Control gives IT admins full audio and video access to a client computer, as well as file transfer, cut, copy and paste capabilities between remote client and host. Multiple remote connections can be launched within GFI Cloud and sessions can be recorded for training, compliance and diagnostic review.

The ability to remotely manage and control individual clients is an increasingly important tool for IT departments as modern workforces are frequently located across disparate working locations including home and field workers as well as multiple office and branch locations. GFI Cloud simplifies this process, and enables IT admins to deploy and monitor a variety of tools including antivirus, web filtering and network monitoring to users regardless of their location.

Scan of Google Play apps reveals thousands of secret keys



A team of researchers from Columbia University has downloaded and decompiled over 880,000 applications found on Google Play, and has discovered that app developers often embed their secret authentication keys in the apps, which can lead to attackers stealing server resources or user data available through services such as Amazon Web Services or Facebook.

“Google Play has more than one million apps and over 50 billion app downloads, but no one reviews what gets put into Google Play— anyone can get a \$25 account and upload whatever they want. Very little is known about what's there at an aggregate level,” pointed out Jason Nieh, professor of computer science at Columbia Engineering.

You would think that Google would be able to prevent such a large-scale and automated scanning and downloading of its Android app market, but the researchers managed to circumvent Google's defenses via a specially crafted crawler tool called PlayDrone, which randomly generates valid IMEI and MAC addresses to prevent device blacklisting by Google, and by using some 500 different Google accounts and reverse-engineering the various Google Play store APIs in order to implement them.



Six infosec tips I learned from Game of Thrones

by Corey Nachreiner

In Westeros—the land of dark knights, backstabbing royals, dragons, wildlings, wargs, red witches, and White Walkers—even the youngest ones have to learn basic self-defense if they’re to have any hope of surviving the cruel fictional world imagined by A Game of Thrones (GOT) author, George R. R. Martin. And so, too, must every CISO and security pro learn the latest information security best practices if they’re to survive today’s Internet threat landscape.

1. The sturdiest wall may conceal a hidden passage. In Game of Thrones, The Wall is a colossal fortification that protects the Seven Kingdoms from the mysterious and malignant beings (the Others), who live in the far north. Made entirely of ice, it runs more than 300 miles in length and stands 700 feet tall. Even from the defender’s side, riding the rickety lift to the top seems like a petrifying proposition, let alone trying to breach it from the outside. On the surface, The Wall offers an impressive, seemingly impenetrable defense.

So how does this relate to infosec? I could go the obvious route and talk about how your network needs a “wall” to defend its perimeter, or maybe mention the importance of manning

your network wall the way the Night’s Watch guards the gates of the North. However, though those tips ring true, I’m going a more unconventional direction by reminding you there are cracks or holes hiding in every wall.

As impassable as The Wall seems, many groups were able to breach it throughout Martin’s narrative. For instance, a group of wildlings and Jon Snow simply climb over it at one point. Even Bran and his ragtag group of kids, with help from Samwell, find a secret passage called The Black Gate.

The point here is that no defense is perfect. Every defense can fail under the right pressure, or miss certain types of attacks.

This is why infosec experts have long relied on the basic concept of defense in depth.

Here's a concrete example. If you manage a network, you need a firewall. However, firewalls—especially traditional ones—will miss many types of attacks. Today, most network attacks originate from the inside (your users clicking a link), and occur over ports you must allow through your firewall (80, 443). Most legacy firewalls miss these. In fact, no techni-

cal security control, no matter how advanced, can prevent every type of attack. This is why you need to layer multiple defenses together, so others can catch what the first layers miss.

While the final battle between the White Walkers and The Wall has yet to begin, I feel safe in predicting that if Westeros relies on The Wall alone for defense, they have a lot to fear!

In network security, our ravens come in the form of log messages and reports. We deploy various network and security controls that monitor our computers and networks.

2. Heed the warnings of ravens. In the Game of Thrones universe, maesters (and by extension the kings they serve) send important messages to one another through ravens; in the same way we used carrier pigeons in the past. However, over time these raven messengers developed an unfavorable reputation, likely since they often delivered bad news. “Dark wings, dark words,” as the in-world saying goes. Nonetheless, bad or not, these messages usually contain important news, and ignoring the news carries consequences.

In one such example, Aemon (maester to the Night's Watch) bade Samwell to ready Castle Black's forty-four ravens to send messages warning the Seven Kingdoms of the return of the White Walkers, and the impending threat on Castle Black. However, most of the kings ignored these messages, not believing the threat really existed. Ultimately, this would have ended in tragedy if not for one king. Eventually, Davos convinced King Stannis to heed the warning, and ride to Castle Black's rescue. If not for this, the Seven Kingdoms may have fallen.

In network security, our ravens come in the form of log messages and reports. We deploy various network and security controls that monitor our computers and networks. They record logs of interesting or unusual activity,

probable malicious activity, and even prevented attacks. However, if you don't regularly inspect these logs and heed their potential warnings, you may miss the opportunity to take actions that could prevent an impending breach.

The recent Neiman Marcus and Target breaches are great examples of not heeding warnings. In both cases, forensic investigations uncovered that these organizations had security logs that identified malicious activity related to the breaches. Neiman Marcus' systems apparently logged over 60,000 security events, and Target had an advanced threat protection solution that identified the POS malware in their systems. However, Target and Neiman Marcus either didn't registers these warnings, or ignored them outright, and thus missed the opportunity to take actions that may have prevented the data theft.

In short, watch for ravens and heed their warnings. They may deliver the intelligence you need to withstand an attack.

3. Words carry more power than weapons. Game of Thrones likely enjoys a wider mass appeal than most fantasy since it spends more time exploring political intrigue and human sociology than it does swords and sorcery.

Many of the fictional world's conflicts are fought in council chambers, at dinner tables, and in gardens, not on battlefields. Lies and manipulations are the weapons of choice. In fact, many of the physically weakest characters, who don't carry positions of authority, often wield much more influence and power than is first apparent.

Lord Varys (The Spider), Lord Baelish (Littlefinger), and Tyrion Lannister (The Imp), are all perfect examples of this type of smart, manipulative character and savvy politician. They use well-placed words and subtle suggestions to manipulate events to their liking, rather than armies or direct power.

Often, their victims don't even realize they are targets of attack, until it's too late. When you see a sword being swung at you, it's obvious to defend with your shield and counter attack, but how do you defend against malicious

whispers and rumors that you may not even hear yourself?

In the security industry, we call this sort of threat actor a social engineer. Social engineers prey on weaknesses in human behavior to trick unsuspecting users into doing things they shouldn't, rather than exploiting technological flaws to break into networks.

Unfortunately, our industry spends more time defending against technological threats than human ones. Social engineering attacks don't rely on technical flaws, so the best mechanical defenses do little to stop them. While you should certainly bolster your technical defenses, don't forget to spend time educating your users to make them aware of the tricks social engineers exploit. You may have erected a castle wall, but that won't prevent an attacker from tricking an untrained guard into opening your gates.

Unfortunately, our industry spends more time defending against technological threats than human ones.

4. Beware the insider threat. While you're considering the manipulative characters in Game of Thrones, don't forget that these characters often attack people in their own group. If, say, the Lannisters used every shady, backhanded, manipulative trick in their book to defeat an obviously evil enemy such as the White Walkers, you'd probably forgive them. However, the manipulators in GOT target members of their own kingdom, council, and even family, for personal gain. In other words, they are insiders carrying out insider attacks.

Perceptive viewers just saw a perfect example of an insider attack during episode two of the fourth season, when King Joffery dies under mysterious circumstances (hurrah!). If you've read the books, or noticed some of the subtle visual cues in the episode, you may have already guessed the culprit. But even if you have no clue whodunit, you probably still suspect poison, and realize that Joffrey's attacker

must have been close. One second he was drinking a cup of wine without issue, the next second a sip of wine resulted in swift death; a classic insider job.

The take-away here is obvious, but still quite important. Inside attackers are not fiction. Malicious insiders have carried out many real-world security breaches and data leaks. It's easy to overlook the insider threat, since malicious insiders are harder to identify and do anything about (they already have elevated access), but you need to remain wary of the threat.

Some basic defensive advice includes vetting your employees and partners carefully, implementing internal segmentation and access control to enforce least privilege principles, and leveraging data loss prevention technology to identify leaks, even when they come from within.

5. The best training makes the best defenders. One of the things I like most about A Game of Thrones is its strong female characters. Unlike in stereotypical, outdated fantasy tropes, most women in this story aren't princesses in need of saving. One of my favorite female characters is Arya Stark. When we first meet Arya, she's a small, nine-year-old girl. Initially, most would not suspect her to be a character of much consequence in an epic tale about battles with medieval knights, wicked sorcerers, mystical zombies, and dragons. Yet, Arya develops into one fierce warrior.

What makes the difference? Well, Arya's heart and attitude have much to do with it, but ultimately, I would argue training is what makes her the accomplished fighter she becomes. Arya hones her skills every chance she gets.

Early in the series, the girl strives to receive bow training that the menfolk typically reserve for boys. In King's Landing, she trains in a graceful style of swordplay called Water Dancing, chasing cats to improve her balance.

Finally, for those who read the books, she joins the guild of Faceless Men, where she receives even more specialized training from the Kindly Man. Through this training Arya becomes a formidable character, and as a result, I'm sure we'll see great things from her.

Like the best warriors out there, the best network defenders are those who train the most. The more you immerse yourself in information security knowledge, news, and practices, the better you'll be at defending your organization. While every pundit has a different view of the various certifications out there, all of them require some study, which means you are training in your field. If you are passionate about protecting your network, continue to learn all you can about infosec. Play with attacker tools (many are freely available in Kali linux), not just security controls. Read the latest research from the smartest whitehat hackers. Simply put, the more you train in your field, the better you'll get at it.

6. Winter is coming (or stay vigilant). Even if you've not caught a single episode of Game of Thrones, or cracked any of the books, if you follow Internet pop culture you've probably seen references to the phrase "Winter is coming."

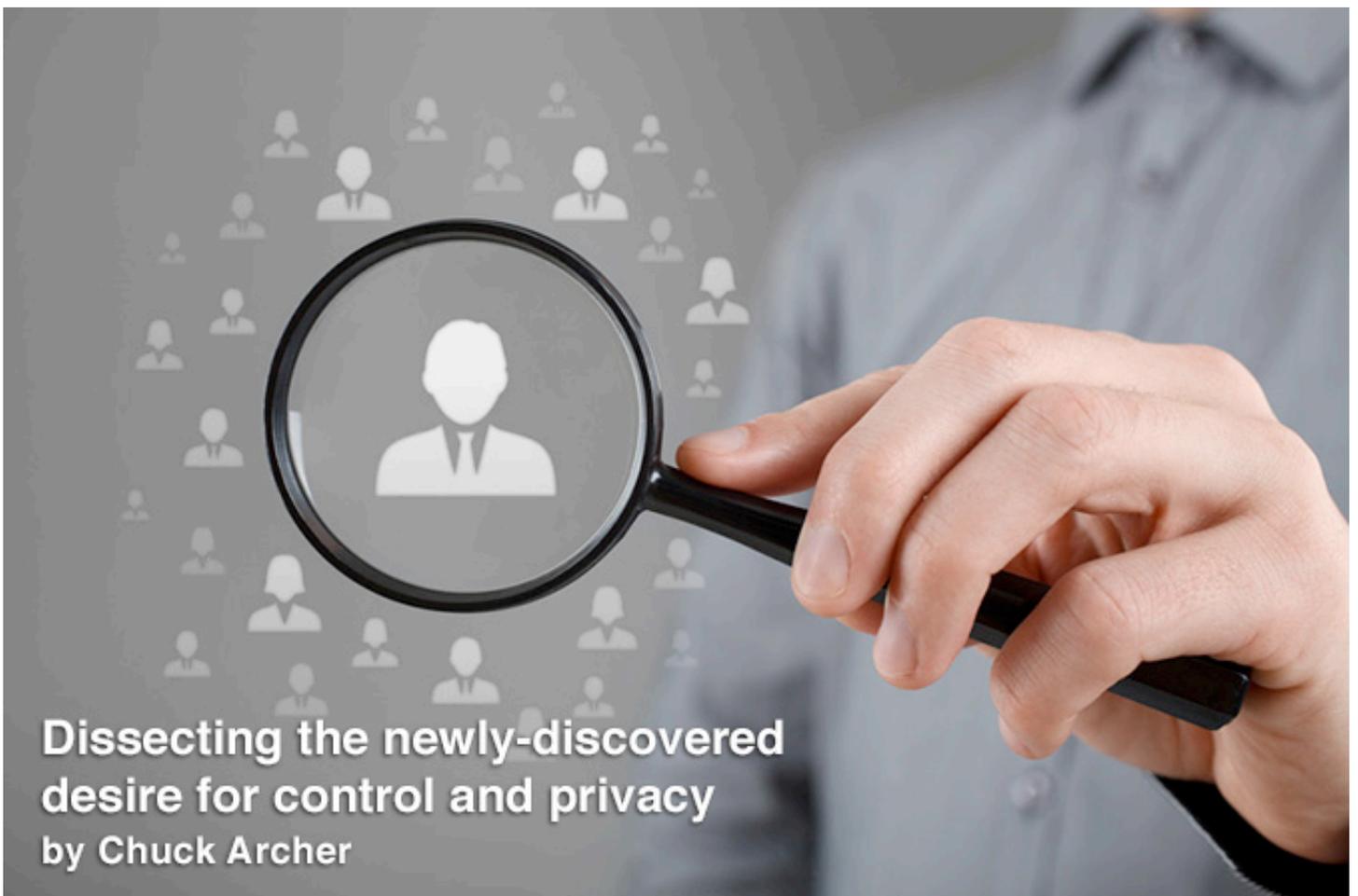
"Winter is coming" is the motto of House Stark, one of the main GOT protagonist families. As a family of the North, the Starks' forefathers were directly affected and closely involved in "The Long Night," which was the first time the White Walkers invaded the lands of Westeros. As a result, the Starks better remember the atrocities and sufferings of that time, whereas other citizens dismiss it all as legend. The motto "Winter is coming" is the Starks' way of reminding their descendants to stay vigilant against future strife and attacks.

The advice to "stay vigilant" directly applies to information security. In fact, if I could only give one piece of security advice, it would be to stay vigilant. The techniques blackhat hackers exploit to breach our networks will continue to change, our defenses depreciate over time and need updating, but one thing remains constant: there is a threat actor somewhere on the Internet who wants your digital information. Constant vigilance means you accept that the threat is real, and remain continually cognizant of potential new attacks. Even if you don't have the latest, high-tech security gadget or largest team of crack security experts, your vigilance will allow you to recognize and react to real digital attacks much quicker than the apathetic administrators who ignore the threat entirely.

There is a second part to the Starks' motto, which is left unsaid. Winter is coming... prepare for it.

The Game of Thrones world often seems like an overly dark universe, where our beloved characters perish and the perceived "good guys" lose as many battles as they win. However, you can learn from their mistakes. Follow these six security tips and perhaps you'll prevail when the digital White Walkers storm your network gates.

Corey Nachreiner is the Director of Security Strategy and Research at WatchGuard Technologies (www.watchguard.com).



Dissecting the newly-discovered desire for control and privacy

by Chuck Archer

Now is the time for businesses to change their approach to privacy needs and build the best defense against both malicious insiders and external threats. Truly innovative, alternative approaches must be found for protecting sensitive information. Through the combination of a zero-trust strategy and a data-centric approach, organizations will be able to share sensitive information without ceding control, enabling businesses to reap the benefits of data sharing while diminishing risk.

Until recently, people have taken advantage of all the connectivity this digitized world has to offer with blissful ignorance. They have been sharing photos, videos and public messages through mediums like Facebook, Twitter and Instagram without regard for their permanence or accessibility. Baby Boomers have hopped on the social media train, excited over the ability to share pictures of their grandkids and to connect with old friends.

More digitally-sophisticated Gen-Xers and Millennials have mastered these social mediums without much thought as to how the posted content will impact their reputations or careers later in life.

There has been a noticeable and wide-spread shift away from this carefree attitude. In a

post-Snowden world, people are realizing that the lines between public and private data have become blurred. The simple fact that technologies like Snapchat exist indicates a newly-discovered desire for control and privacy. People are realizing that once distributed, information can end up in places they did not anticipate and certainly do not control.

There is a surprising parallel with business data. Much as a Millennial would like to trust a Snapchat recipient, many employees operate under the assumption they can trust those with whom they share corporate data. This includes data attached to e-mails or shared through solutions such as Box, Dropbox or SugarSync. Unfortunately, the stakes are much higher than social embarrassment – the employee may be putting sensitive data or

intellectual property at risk. Employers understand that they cannot stop information sharing, so they must move decisively to put processes and controls in place to protect organizational information.

The everyday mobile workforce and C-suite executives alike yearn for more control over the information they share. For example, ripcord access for those times when regret kicks in after a confidential document has been sent office-wide or to an outside partner.

Data acquires value when it is appropriately shared, indicating a critical need for a way to effectively collaborate without risk or regret. The injection of cloud and mobility into business processes means that those processes are increasingly being conducted on untrusted networks and devices. Sensitive information may go places you do not know nor control.

Businesses must therefore rely on the security of the device, network or application where the data resides and must trust recipients not to forward shared data to others without the originator's knowledge or consent.

The simple, everyday act of sending a data object to multiple recipients via e-mail is much more complicated than users realize. The attached data object is replicated by Exchange Server storage, multiple devices, mobile carriers and cloud backups.

It cascades rapidly when the recipients are outside of the original domain or when a recipient forwards the object. Frequently, the originator has no idea that half of these copies exist, much less where they reside. This is not a problem specific to e-mail; using cloud storage creates a very similar scenario. The results, and the challenges, are the same.

The simple, everyday act of sending a data object to multiple recipients via e-mail is much more complicated than users realize.

What can we learn from the Millennials' passion for Snapchat? We must create a method for sharing information without ceding ownership or relying on the trust of associated networks, devices and recipients.

The idea is simple: enable a data owner to share data with a defined set of recipients without actually distributing the data. Enable the originator to assign access controls that determine the criteria for granting access (provide a key) and define the trust level of how the recipient can interact with the data.

For example, a recipient might be limited to view-only capabilities (ad hoc recipient), limited to annotation and change privileges (collaborator), or given full ownership of the data (trusted collaborator). Regardless, data protection must be independent and ubiquitous, able to secure the data within and beyond the enterprise perimeter, to any storage provider, and on any device.

There are certain must-haves to any "zero-trust" strategy:

- Settle on a corporate standard and set policy for its use. Don't just dictate – sell the virtues and features internally. File sharing will be used in your organization whether it is a corporate standard or a grassroots user-by-user choice.
- Choose a file sharing solution that provides a virtual tether to the data so it can be revoked if the need arises.
- Pay attention to auditability and visibility. Not every file sharing tool is created equal in this regard, and these functions are critical.
- Don't get hemmed in by a solution that won't extend protection, control and visibility beyond the perimeter. Remember that sharing will include partners and customers.

Businesses must take ownership of their data as it moves away from the center of the organization at lightning speed into the cloud and onto mobile devices. There is an established consensus that the cloud provides much more value than any business could

generate in-house. However, this transition doesn't mean organizations must abdicate control to the provider.

Decision-makers must own their originator controls to protect information at rest, on the move, in use and on any platform or device. They must proactively avoid potential remorse from giving someone access to critical business information by taking a data-centric approach to security.

There are three critical truths for such data-centric security that point the way for implementing effective security:

1. Data will go places you do not know, cannot control and increasingly cannot trust. This happens in the normal course of processing, through user error or complacency, or through malicious activity. Because the places your data goes may be untrusted, you cannot rely on the security of the network, device or application to protect that data.

2. Encryption alone is not sufficient to protect data. Encryption must be combined with persistent, adaptable access controls that enable the originator to define the conditions under which a key will be granted, and change those controls as circumstances dictate.

3. There should be comprehensive, detailed visibility into who accesses the protected data, when, and how many times. This detailed visibility ensures auditability for regulatory requirements and powers analytics for broader insight into usage patterns and potential issues, which in turn improves control.

Starting with the first truth, there is an obvious conclusion: For data-centric security to be effective, the data must be protected at the point of origin. If the data is encrypted as the very first step in the process, it is secure no matter where it goes, on which network it travels and where it eventually resides.

Doing otherwise means you must trust every computer, every network connection and every person from the point that the information leaves the originator's care and for as long as it or any copies exist.

Protecting data at the point of origin makes a big assumption: Your data-centric security solution must be able to protect the data wherever it goes. As the first truth tells us, the data and its many naturally created copies will go to a lot of places, including mobile devices, personal devices and the cloud.

An effective solution secures data regardless of the device, application or network. It also must secure that data regardless of its format or location and whether it is at rest, in motion or in use. It must readily extend past the perimeter boundary and be capable of protecting ad hoc dialogues.

This is where it is good to consider the many point and function specific data-centric security solutions available on the market. By their very nature, these solutions create silos of protection because, as the first truth dictates, data will reside somewhere outside of their span of operation. Because these solutions lack the ubiquitous protection necessary, agencies and businesses are compelled to erect multiple silos.

Yet despite the best efforts of these multiple silos, the results are predictable: Data will still fall between the gaps. And these gaps are precisely where outside adversaries and malicious insiders lie in wait to exploit vulnerabilities and steal data. Furthermore, each silo represents real costs in acquiring, implementing and supporting the associated solution, and the operational burden of managing multiple solutions.

The second truth states that encryption on its own is not sufficient—it must be combined with granular and persistent controls. Sharing content effectively surrenders control over it, essentially making the recipient the co-owner of the data.

Controls enable the originator to set the conditions under which the recipient is granted a key to access the file and enable the option to dictate what the recipient can do once the data is accessed. This includes the option of providing view-only capability where the recipient cannot save the file, copy/paste content or print the file.

The term “persistent” is a critical characteristic of the access controls necessary for effective data-centric security. The data remains virtually tethered to the originator, who can respond to changing requirements or threats by revoking access or altering the conditions of access at any time.

These changes must be instantly applied to all copies of the data, wherever they reside. Remember that the first truth states that the data may be in places the originator does not know or where they cannot exert control over it. Therefore, the originator cannot assume prior knowledge of where the data resides and physical access to the associated devices.

Persistent control has the added bonus of addressing revocation of data on lost or stolen devices that likely will never be in contact with the network again.

Adaptability is critical to differentiate competing solutions and support the case for a unified, ubiquitous approach. Not all data-centric security solutions are created equal, as some use encryption methods invented before mobility, the cloud and broad adoption of the Internet.

With these methods, the access controls are set at the moment the data is encrypted; yet they lack the benefits that come with persistent control.

Adaptability is critical to differentiate competing solutions and support the case for a unified, ubiquitous approach.

The third truth of effective data-centric security is that an organization needs comprehensive visibility and auditability. This includes visibility into all access activity for each data object, authorized and unauthorized. It also includes visibility into any data type, inside and outside the perimeter boundaries.

Comprehensive audit data and non-repudiation enables an organization to know who is using data, when and how often. Visibility empowers control, giving organizations the information to make rapid and well-informed responses to the relentless attempts to exfiltrate information.

This visibility should extend to the organization’s broader security ecosystem, providing

the data to Security Information and Event Management (SIEM) tools and operational analytics. In turn, the correlation and analysis can yield insights and even identify possible malicious insiders.

In today’s quickly changing and highly complex computing environment, organizations must turn to alternative approaches to protect their valuable information. Trends like mobility, BYOD and the cloud have changed the game. Businesses must advance their security strategies. Through the adoption of a zero-trust model and a data-centric approach, businesses can take the next step in security’s evolution.

Chuck Archer, CEO and Executive Chairman of Covata USA (www.covata.com), is a senior executive with Government and Industry experience of exceptional breadth. Chuck culminated his 28 years of Federal Government service as Assistant Director of the FBI in charge of the FBI’s Criminal Justice Information Services Division (CJIS). While at the FBI, Chuck was appointed by the US Attorney General to SES-6, the highest civil-service rank in the US Government.

Chuck is one of the few FBI “alumni” to have held a broad range of positions in the FBI throughout his career, giving him a unique perspective on the real-world challenges of law enforcement and national security. Since leaving the FBI, Chuck has held various leadership positions with system integrators and leading manufacturers. Chuck’s experiences in law enforcement, intelligence and business strategy have made him a highly valued contributor and provide him with valuable insights into the needs of Federal customers.

ARE WEAK OR MISCONFIGURED CERTIFICATES ENDANGERING YOUR NETWORK?

Find and **fix** vulnerable SSL certificates
and termination endpoints **now** using



**Certificate
Inspector**

Certificate Inspector works for you, the security professional, to discover forgotten or misconfigured certificates, and identify potential vulnerabilities, such as weak keys, problematic ciphers and expiring certificates. Certificate Inspector not only presents all of your internal and external SSL certificates and endpoints in one intuitive dashboard, but also provides remediation activities specific to each vulnerability found.

Gain peace of mind and run your first report today. Get your complimentary access at [digicert.com/cert-inspector](https://www.digicert.com/cert-inspector)



Incident response and failure of the “Just Fix It” attitude

by Mike Horn

Incident response is a hot button for CISOs, security analysts and IT administrators and no wonder: with recent headlines reporting disastrous high-profile data breaches, both consumers and enterprises from A to Z are scrambling to put in place an effective and rapid response process. Incident response needs to happen, with or without enough staff in place. The basic question is "how long will it take to contain the threat?"

There is no standard answer, as most companies have a response process that's manual and often inconsistent, with many delays exacerbated by manual human labor tasked with sorting out and managing even the most mundane iterative phases of the crisis. At the same time, most companies are understaffed when it comes to incident response. The problem is compounded by the industry-wide shortage of skilled cyber security professionals.

Without a strong combination of automation and skilled staff, companies are in for a long, arduous, and a possibly devastating scenario. If there is a staff shortage and lack of automa-

tion, a breach can shut down critical functions of a company – until they can find, hire, and insert short-term resources to get through the crisis. In the meantime, the damage can put the company in the headlines.

In this article we look at which incident response steps are at the breaking point, how we got there, and the steep pressure this puts on incident response teams. We'll also include tips and suggestions for improvement along the way.

The basic incident response process is typically covered in 5 steps: Detect – Investigate – Prioritize – Contain – Remediate.

On the surface, this looks simple, however, those steps assume that certain important parallel functions occur. These functions include communication, information sharing, auditing, and ticket management. These “other functions” just need to happen, just like a detected threat simply needs to be stopped. This mindset is called the “just fix it” approach, and it assumes that layers of required actions can be executed with a simple platitude or business directive.

The reason for this mindset goes back to the days of when IT budgets started freezing or shrinking. Companies used simple models based on hardware depreciation schedules and IT staffing ratio relative to their entire head count.

This started to break down when network security issues started to increase. IT staff initially increased workloads to deal with the added security remediation, AV tools, new firewall requirements, and IDS tools. As that came under control, it became clear that managing detection and prevention tools be-

came more cost-effective than hiring staff to manually prevent or detect new cyber attacks. After IT departments wrapped their heads around the requirements for the new systems, security budgets and proactive thinking in security fell into a period of standstill.

Most companies are still stuck in this “wait and see” mindset, getting by with processes developed over 5 years ago and hoping things don’t get any worse. When the systems for prevention are bypassed and a breach occurs, organizations face the breach with the tools, staff, and processes designed around outdated ratios created during the last operational break down - and it’s a mad scramble.

With already loaded staff on hand, the time consuming, arduous manual incident response process is applied to a threat that requires immediate response. As incidents, alerts, and attacks increase, this forces staff to take longer and longer to respond, or dramatically cut corners to get things done “fast enough”.

Most companies are still stuck in this “wait and see” mindset, getting by with processes developed over 5 years ago and hoping things don’t get any worse.

Every minute that unhampered malware is loose on your network represents lost data, lost goodwill, and lost customers. The fear of those losses has led to an eruption of detection technology that firms have been snapping up. The resulting implementation of detection tools has reduced both some fears and the need for manual detection, but it also increased the noise of automatic detection.

Detection is faster and from multiple angles, but it brought volumes of reports that include duplicates of the same threats and overly cautious false positives.

Rapid detection has created new problems that increasingly lead to missed prioritization and wasted time. Before the new detection tools, a small security operations team might have seen 50 to 200 alerts a day, but with the addition of new tools, that might spike to 100 to 1000 alerts a day or more. The same team

that once processed 100 alerts a day could now easily face 500 alerts a day. If the team is allowed to continue processing only 100 alerts a day, problems start to arise. In two days, there would be 200 alerts processed but 1000 alerts delivered. In four days that would mean 400 alerts processed but 2000 alerts delivered.

If you change the “processing requirements” to match the number of alerts in a day, you have other problems. In the “fast enough” daily load scenario, processing the 500 alerts a day would be the target, but to do that, the team would need to grow 5X in size or process 5X more alerts. It’s unlikely that the team could find, vet, and hire 5X more staff, so instead, the analyst have to work longer and spend less time per alert to weed out the false positives, prioritize, then contain the biggest threats.

Since threats are getting more sophisticated and evasive, is it really a good idea to reduce the time analyzing the threats or pile on “variable” human judgement? More complex threats need smarter analysis, but at the same time, the volume of threats still demands faster processing. The conundrum is how to combat more, evasive threats in the same time with the same staff.

Cost of failure

The cost of failure still rings in the headlines, as the Wall Street Journal estimated the costs of the Target breach topping \$1.4B (online.wsj.com/news/articles/SB10001424052702304834704579405342143588098). In spite of many of the things that may have been wrong at Target, they appeared to have automated detection tools that did identify the attack. Analysts and others seem to agree that the break down occurred in the incident response process. It may have been a lack of skilled staff, an overload of alerts, or even a poor communication process to update firewalls and proxies that led to the extended breach. The end result has been splashed

across the headlines, including data loss, customer loss, and a drop in earnings.

Addressing the conundrum

While automated detection appears to be working, the problem is bigger than how to update hundreds of enforcement devices from multiple vendors – it also includes the steps to investigate and prioritize the threat. The key in the investigative phase is to collect and connect incident intelligence to understand the who, what, and where of the incident. Understanding domain and IP reputation as well as the country of the threat source or communication target can aid in increasing the confidence in the threat.

Files used in the attack and indicators of compromise such as registry and process changes and other fingerprinting on the targeted systems can boost the urgency and confidence in an attack as real threats are scored and presented to security team members. This, in turn, can drive threat scorecards, which can escalate priority or enable an alert to be tossed in the “false positive” waste bin.

Automated systems can double check the incident intelligence and the scorecard and allow analysts to make a “go or no go” decision.

This process of collection and connection is necessary for successful investigation and priority, but the time-cost for this effort can be steep unless automation is introduced. Automation can increase the speed and consistency of investigative analysis by leveraging continuous incident intelligence that is placed at the security team’s fingertips as they receive each threat for analysis. The best security operations teams spend time reviewing scorecards, not running around collecting information to create report cards. If time is of the essence, manual processes will be costly.

The scorecards for each threat are reviewed, with the highest scoring and confirmed threats being pushed to the top of the “required containment list”. Threats that are flagged as “requiring containment” may also go through another review. Again, manual review takes time and will be limited by the number of analyst

and the threats that they have to review. Automated systems can double check the incident intelligence and the scorecard and allow analysts to make a “go or no go” decision. In high confidence situations, automation can also be used to contain reported threats in real-time.

The containment step can be automated, locking down reported threats as they are detected. In reality, this rarely happens, as the usual process involves a security analyst filing a ticket for an update and sending that to the network team.

This is another opportunity for human error or debate about the threat that can further delay protections. If the network team is busy, accidentally misses the ticket, or simply does not believe that the changes recommended by the security analyst are valid, the containment

may be delayed, or may not happen at all. Lastly, the remediation step should occur after containment. If the threat is locked down and the damage mitigated, remediation to reimage or restore affected systems follows. Another delay point can occur here, as remediation may be withheld if the network teams encounters a delay or does not act to contain the reported threat. It's not uncommon for ticketing system workflows to leave a ticket in a pending state. In this case, remediation actions could be held up pending threat containment, as a check and balance against reimaging non-compromised systems. Any delays here

can allow an infection to spread or more data to be exfiltrated.

This strain on incident response teams can easily land a company in the headlines, but it doesn't have to be that way. With a good combination of structured manual and automated processes, companies would have a much better chance of stopping an attack as it happens and responding without delay. This would also keep companies from overloading staff that is already stretched too thin and reduce the chance of catastrophic data or IP loss.

Mike Horn is the Vice President of Threat and Response Products at Proofpoint (www.proofpoint.com).

Want to reach a large audience of security pros by writing for (IN)SECURE?



Send your idea to mzorcz@net-security.org



How to learn information security by Kai Roer

Learning is a skill. A skill that can be, well, learned. I am often approached by young people who ask me what does it take to move into the information security field, what certifications are required, what training should be done, and so forth. In my opinion, the most important skill in infosec, and many other areas too, is the ability to learn.

Twenty years ago, security was a very different and much narrower field than it is today. As technology evolves, so do the threats, and with new threats come new protection requirements. In order to be able to do a great job in the infosec field, you need to constantly up your game, and learn as much as you can every single day.

Here are some methods I use to learn, and I apply these not only when I study for a psychology class at the university, but also when I need to learn a new skill, or when I discover an new area of interest that I want to know more of.

1. Take interest in the new

The most important thing in life is to realize that there are always new things happening. Evolving technology, evolving threats, evol-

ing business context - everything is in constant change. Accepting this fact will help you set out to discover changes before they become evident to others, and thus prepare yourself and your organization. Being on the lookout for new information and allowing yourself to be curious is very important when you set out to learn.

2. Mix sources

People are different, and so are our learning preferences. Some prefer reading, some prefer doing. Some need practice, others need time to reflect. For most of us, a mix of methods and sources yields the best results.

As a learner in 2014, you can easily mix sources. From university classes to certification trainings, from reading books to watching YouTube videos, and attending Massive Open

Online Course (MOOC) classes - you have so many options when it comes to learning today that not learning should be no longer an option. And if you are one of those who prefer practice, well, go on then! Set up a virtual environment at your home, in your office, or even on AWS, and hack your heart out!

3. Always question common beliefs

As stated above, change is inevitable. Questioning common beliefs should be a habit for any individual working in the infosec field, but not many have acquired it. Ask yourself "Is this really what it seems?" and "How can this be?" and also "What other interpretations could explain this?". Apply some of that scientific method you learned at the university (or learn some if you did not). Question everything, and you will learn more. You may even stumble across a bug, a new way of doing things, and even a blind spot no-one has ever even considered!

4. Challenge yourself

We incorporate a large amount of mental models, behaviors and habits on an individual level. Most of these can be changed if you want it bad enough. The way you do your job, the way you think, the way you learn are social constructs, meaning they are methods created through interaction with social groups.

You are in charge of your learning, so you also need to take control and challenge your own status quo. If you think that you are "too old for this" or that "this is way too hard" for you, apply cognitive psychology, and change your thoughts into: "With my age comes experience I can use to learn more, faster and better," and "This is a challenge I will rise to".

5. Never stop learning

Some people seem to think that when school is out they don't need to ever learn again. This is a wrong assumption - especially in infosec, where you need to be constantly on the alert. If you ever want to be good at anything, even if you are highly skilled by birth, you cannot stop learning - either by attending classes, re-

searching new topics or just by doing something new. There are a number of ways to learn, and the topics are limitless, so why limit yourself?

You may think that in order to learn more about infosec, you should only learn things that are of relevance to infosec. But I disagree. Learning new things - no matter what they are - keeps you sharp. Set out to learn something new every week - it can be a simple thing like cooking a new dish, or something more advanced (for some) like building a robot.

Connecting cooking to infosec is not that difficult: food security (cleanliness, ingredients, treatment, etc.), applying a method/best practice (using a recipe, tools, etc.), creativity (experimentation, figuring out what works best) are all easily "translated" to both learning and to infosec!

6. Apply the learning process that works best for you

Studies shows that the best students are those who adopt a good structure for their learning. There are a number of best practices out there, so I will only cover the main ones:

- A strict schedule: reserve time to study, and follow the made schedule!
- Work with the materials: read, write, answer questions, do the tasks, practice.
- Practice tests: Spend time learning how to work the test. If it's a written exam, do mock exams. If it's a multiple choice test, run a demo.
- Motivate yourself: Write down a personal goal, a reason for your learning, and put it in a prominent place to remind yourself. Also reward yourself when you reach milestones.

As long as you keep on pushing yourself towards more knowledge, more understanding, more learning, you are helping the infosec community to evolve and grow.



Who are you? The impact of security breaches on authentication

by Christiaan Brand

As businesses that rely on the Internet continue reeling from the recent Heartbleed bug incident, the question remains *when*, not *if*, another SSL bug will emerge and wreak havoc on Internet users.

With weekly announcements of new security issues, the weaknesses of today's security solutions and techniques are on full display. Rather than continue to sit back and wait for the next attack to happen, organizations need to consider revisiting their security protocols in order to adequately protect themselves and their customers.

In addition to the widespread impact these breaches have on online portals, mobile applications are also being targeted by hackers, which can bring about disastrous results as more and more consumers store valuable personal information on their smartphones and tablets.

While Heartbleed has become one of the most widely publicized security bugs in recent history, it was not the first and will certainly not be the last. In the wake of Heartbleed and the

continued increase in the frequency and sophistication of today's security breaches, organizations are scrambling to get themselves and their customers back on track and better protected for the future.

By abandoning reliance on a single, standard SSL channel to manage security in exchange for a multi-factor approach to authentication, organizations can ensure that as the next big security bug emerges, their business and customers will escape unscathed.

While multi-factor authentication has become a frequently adopted security technique among many organizations in a variety of industries, the key to successfully thwarting the efforts of today's fraudsters requires more robust techniques that take communication out-of-band.

Another SSL vulnerability? Now what?

More than a month after the Heartbleed bug was first discovered, businesses and customers are still feeling the effects. As one of the most widespread SSL libraries in use today, a bug inside the OpenSSL system spells disaster for maintaining secure communications online for some of today's most popular websites.

While many experts have focused on the attackers' ability to steal usernames and passwords from a given organization's server, the bug can also leak the unique private key that corresponds to the server's digital certificate. Once this information has been compromised, it is virtually impossible to accurately confirm the identity of an online portal. This makes Man-in-the-Middle attacks, even on web sites protected with SSL, trivial.

Should a given organization suspect their system has been infiltrated, they will need to rekey their SSL certificate immediately and have

that reissued by the certificate authority. In addition, all open sessions should be discontinued and all passwords should be changed if the system solely relies on usernames and passwords. Finally, the organization should have its certificate authority revoke the current SSL certificate that has been potentially compromised.

Aside from leveraging commonly used SSL certificates that are more easily hacked, the common weakness shared by many organizations impacted by Heartbleed is the reliance on passwords as the sole means for authenticating the identity of a user. By instead requiring users to go a step further and provide login credentials (something they know) and a second authentication factor (something they have in their possession), the risk factor of inadvertently having a hacker infiltrate accounts could be significantly lower. However, just as there are varying methods of SSL communication, some stronger than others, the same goes for multifactor authentication.

SHOULD A GIVEN ORGANIZATION SUSPECT THEIR SYSTEM HAS BEEN INFILTRATED, THEY WILL NEED TO REKEY THEIR SSL CERTIFICATE IMMEDIATELY AND HAVE THAT REISSUED BY THE CERTIFICATE AUTHORITY

Taking multifactor authentication to the next level

As businesses and their customers gain greater capabilities and opportunities with the continued introduction of more advanced online and mobile technology, fraudsters are able to leverage these exact same offerings to easily launch increasingly sophisticated attacks. With the war on fraud showing no signs of slowing down, many organizations have turned to multifactor authentication as a means for beefing up security for their customers.

Widely used within the financial services industry, multifactor authentication requires customers to generate a one-time-password (OTP) issued to them through their mobile devices, a key fob or chip card in their possession in addition to their usual login credentials. Recently introduced methods of multifactor authentication go as far as utilizing voice rec-

ognition and biometrics to ensure the user is in fact who he or she claims to be.

While these methods of authentication were once a viable option for protecting businesses and their customers from even the most advanced fraud attacks, the introduction of newer technology has given fraudsters more robust capabilities to easily compromise tokens and one-time-passwords. How?

Each of these methods of multifactor authentication shares the same vulnerability as a result of their continued reliance on browser-based communications between the customer and the organization they do business with.

Today's fraudsters have the ability to easily create a phishing site that mimics a company's online business portal or even attack the browser itself. From there, they have immediate access to the customer's unique information and the newly generated one-time

password, which means they have full access to the customer's account.

With instances of account takeover increasing at an alarming rate, authentication through browser-based communications is simply no longer a wise option.

Rather than remain a sitting duck for fraudsters to easily pounce on, two-way out-of-band authentication presents the ideal alternative to more obsolete methods of authentication and provides the added convenience of allowing customers to leverage their own mobile device as the second factor.

The future of authentication in the palm of your hand

Beyond the need for greater security and peace of mind, today's consumers demand the ability to carry out daily tasks, such as

managing their bank account and paying bills, as quickly and easily as possible. Out-of-band multifactor authentication through the consumer's mobile device is the perfect solution to satisfy both needs.

Through this means of authentication, highly secure private keys are deployed to the online user's mobile phone, essentially transforming the smartphone into a personal authentication device. Independent from the device's own operating system, this additional channel creates a secure, out-of-band communication channel between the customer and the organization they are doing business with based on both parties authenticating their identity.

In addition, all communication between the customer and the organization is encrypted end-to-end and cannot be intercepted by outside parties, eliminating the risk of Man-in-the-Middle and Man-in-the-Browser attacks.

WHEN DISASTER STRIKES, IT LEAVES ORGANIZATIONS AND USERS VULNERABLE TO DATA THEFT, IDENTITY THEFT AND EVEN THE LOSS OF FINANCIAL ASSETS

As the customer completes a task, such as transferring funds from their bank account to a friend's account, they are required to respond to a one-touch verification prompt of "Accept" or "Reject" on their mobile device before the transaction is completed.

This simple verification process requires little to no education before being deployed to customers and fully eliminates the need for expensive hardware tokens or cumbersome OTPs.

The premise of using a diverse authentication channel to augment the encryption schemes supplied by the phone's own operating system has been suggested for years, but most mobile applications still rely solely on the encrypted channel managed by the phone itself.

When disaster strikes, it leaves organizations and users vulnerable to data theft, identity theft and even the loss of financial assets.

When the next Heartbleed-style SSL bug comes about, those organizations continuing to rely on a standard single encrypted channel will once again be scrambling to fix the problem before their customers jump ship and leave their business with nothing.

On the other end of the spectrum, businesses leveraging digital certificates and customers' mobile phones for multifactor authentication and channel diversity will emerge unscathed and will have done so without further complicating the authentication process for themselves or their customers. The choice is clear.

Christiaan Brand is co-founder and CTO of Entersekt (www.entersekt.com), a pioneer in transaction authentication. Brand oversees Entersekt's information technology services, mobile processing platforms and enterprise applications, playing a key role in application development, infrastructure and operations. Additionally, Brand leads the delivery of Entersekt's cloud and mobile strategies, ensuring that the company is well positioned to address the introduction of new business models and payment types.



Malware world

Angler exploit kit starts wielding Silverlight exploits



"Silverlight exploits are the drive-by flavor of the month," claim Cisco researchers. "Exploit Kit owners are adding Silverlight to their update releases, and since April 23rd we have observed substantial traffic (often from malvertising) being driven to Angler instances partially using Silverlight exploits."

Vulnerabilities in Adobe Flash and Oracle Java have long been preferred targets of exploit kit developers, but as those two firms have been increasingly improving their patching efforts, malware developers have realized that Silverlight users also make good potential targets.

Silverlight, the framework for writing and running rich Internet applications that Microsoft created as an alternative to Adobe's Flash, has not, so far, surpassed the latter when it comes to user numbers. Still, it has been used to provide video streaming for many high profile events and is currently used by popular video streaming service Netflix.

Exploit packs bring a lot of money to their owners, whether they are bought or simply rented by attackers. In the wake of the arrest of the creator of the infamous Blackhole exploit kit, other exploit kit makers are eager to keep the market share they have gained with Blackhole's downfall.

They can be expected to diversify the exploits used, and add some for Silverlight vulnerabilities.

"Silverlight exploits are also ideal because Silverlight continues to gain rich Internet application market share, perhaps surpassing Java, and Microsoft's life cycle schedule suggests Silverlight 5 will be supported through October, 2021," says Cisco threat researcher Levi Gundert.

Hybrid Zberp Trojan targets bank users around the world



A new threat created by the amalgamation of the publicly available code of two of the most (in)famous malware families around is targeting users of over 450 financial institutions around the world, warn Trusteer researchers. The creators of Zberp - as the researchers dubbed the threat - have used the leaked source code of both the Zeus/Zbot and Carberp banking Trojans.

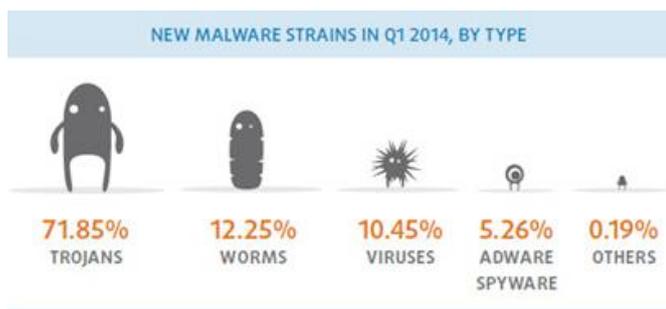
The Zeus/Zbot malware needs no introduction, as it's been the top banking Trojan for a few years now. The Carberp Trojan is a complex piece of malware that is capable not only of stealing sensitive information, but also of modifying a computer's hard drive's master boot record (MBR) in order to avoid being detected by antivirus software present on the targeted machine.

This new "hybrid beast" allows those who wield it to collect basic system information, take screenshots, steal data submitted in HTTP forms, user SSL certificates, and FTP and POP account credentials. And the malware is apparently also capable of performing Web injections, MITM and MITB attacks, and initiating remote desktop connections.

Its hybrid nature is best witnessed in the way it evades detection: by deleting and rewriting the registry key that allows it to persist on the system so that it wouldn't be spotted by AV solutions after the system is booted; by hiding its configuration code in an image file; by "hooking" into the browser to get control of it, but also to evade AV software; and by securing the communication channel through which it contacts its C&C.

This is not the first time that malware developers used Carberp's code to create a new threat - the first ever information-stealing Trojan targeting SAP enterprise software was also partly based on it.

Malware creation breaks all records! 160,000 new samples every day



Malware creation has broken all records during this period, with a figure of more than 15 million new samples, and more than 160,000 new samples appearing every day, according to Panda Security.

Trojans are still the most abundant type of new malware, accounting for 71.85% of new samples created during Q1. Similarly, infections by Trojans were once again the

most common type of infection over this period, representing 79.90% of all cases.

Trojans also top the ranking of newly created malware, accounting for 71.85% of the total, followed by worms, at 12.25%, and viruses at 10.45%.

In the area of mobile devices, there have been increasing attacks on Android environments. Many of these involve subscribing users to premium-rate SMS services without their knowledge, both through Google Play as well as ads on Facebook, using WhatsApp as bait.

Along these lines, social networks are still a favorite stalking ground for cyber-criminals.

China is once again the country with most infections, with a rate of 52.36%, followed by Turkey (43.59%) and Peru (42.14%). European countries ranked high among the least infected countries, with the best figures coming from Sweden (21.03%), Norway (21.14%), Germany (24.18%).

ESET analyzes first Android file-encrypting, TOR-enabled ransomware



One year ago, Android Defender, a hybrid comprising characteristics of a rogue AV and ransomware (the lockscreen type, not a file-encryptor) was discovered. In May we saw a report about a police ransomware for Android by the Reveton team. The malware did not encrypt any files on the infected device.

But this Trojan, detected by ESET as Android/Simplocker, scans the SD card for files with image, document or video extensions and encrypts them using AES, then demands a ransom in order to decrypt the files.

The ransom message is written in Russian and the payment demanded in Ukrainian Hryvnias, so it's fair to assume that the threat is targeted against this region. This is not surprising, the very first Android SMS Trojans (including Android/Fakeplayer) back in 2010 also originated from Russia and Ukraine. The malware directs the victim to pay using the MoneXy service for obvious reasons, as it is not as easily traceable as using a regular credit card.

It will also contact its C&C server and send identifiable information from the device (like IMEI, et cetera). Interestingly, the C&C server is hosted on a TOR .onion domain for purposes of protection and anonymity. ESET's analysis of the Android/Simplocker.A sample revealed that we are most likely dealing with a proof-of-concept or a work in progress.

There's a new banking Trojan in town



A new piece of banking malware is being delivered via tax- and invoice-themed phishing campaigns, Danish security company CSIS is warning. Dubbed "Dyreza," the malware targets users of a number of major online banking services in the US and the UK: Bank of America, Natwest, Citibank, RBS, and Ulsterbank.

"The code is designed to work similar to Zeus and as most online banking threats it supports

browser hooking for Internet Explorer, Chrome and Firefox and harvests data at any point an infected user connects to the targets specified in the malware," shared CSIS researcher Peter Kruse.

The malware also allows attackers control browser traffic and perform Man-in-the-Middle attacks. By having this opportunity to read all the encrypted traffic between the victims' browser and the financial institutions' servers, they can also try to circumvent 2-factor authentication.

"We believe this is a new banker trojan family and not yet another offspring from the Zeus source code," says Kruse. "Still it's unclear if this is provided as a "Crime as a Service" or if it's a full circle criminal outfit."

Kruse also warns users to be wary of future spam campaigns delivering the Trojan, as there are indications that the crooks will try to push it onto users by masquerading it as a Flash Player update.

International action against Gameover Zeus botnet and CyptoLocker ransomware



On Friday, 30 May 2014, law enforcement agencies from across the world, supported by the European Cybercrime Centre (EC3) at Europol, joined forces in a coordinated action led by the FBI which ensured the

disruption of the Gameover Zeus botnet and the seizure of computer servers crucial to the malicious software known as CryptoLocker.

US authorities identified a 30 year old suspect from Anapa, Russian Federation, as a leader of the cyber criminals behind Gameover Zeus.

Gameover Zeus is an extremely sophisticated type of malware designed to steal banking

and other credentials from the computers it infects. It then uses those credentials to initiate or re-direct wire transfers to accounts controlled by cyber criminals. It is the latest version of a malware family which appeared already in 2007 and security researchers estimate that between 500,000 and one million computers worldwide are infected. Known losses caused by the malware are estimated to be around EUR 75 million.

The Gameover Zeus network of infected computers also distributes the ransomware known as CryptoLocker. Security researchers estimate that, as of April 2014, CryptoLocker had infected more than 234 000 computers. Furthermore, the FBI estimates that over USD 27 million in ransom payments were made in just the first two months since it emerged.

Besides US authorities, investigators from Canada, France, Italy, Japan, Luxembourg, Germany, New Zealand, the Netherlands, Ukraine and the United Kingdom participated in the operation.

Android smartphones pre-installed with malware hit the market



Cheap Android-based smartphones pre-installed with spyware are being distributed to European users, say G Data experts. The malware is disguised as the Google Play Store app, and cannot be removed as it is integrated into the firmware. It's also undetectable by users.

"The affected model 'N9500' is produced by the Chinese manufacturer Star and looks very similar to a smartphone from a well-known manufacturer," they shared. "Large online

retailers are still selling the Android device at prices ranging from 130 to 165 euros and distributing it across Europe."

The app allows criminals behind this scheme to have full access to the smartphone. It collects personal data and sends it to a server located in China, and prevents the installation of security updates. "The spy program enables criminals to secretly install apps, which enables the whole spectrum of abuse: localization, interception and recording, purchases, banking fraud such as theft of mobile TANs, and sending of premium SMSs."

The researchers believe that the cheap price at which the device is sold is made possible by the subsequent selling of data records stolen from the smartphone owner.

Users who have bought such a device are advised to use a security solution see whether the malware is there, and if it is, to return the device to the online shop from which they bought it and ask for the money back as it's impossible to remove the malware from the phone.



Thecus N5550 NAS Server inside and out
by Mirko Zorz

While just a decade ago having a DVD burner for your home storage needs was quite sufficient for most users, today's multimedia-hungry consumers require terabytes of space.

Once an obscure term used mainly by IT geeks, backup has become part of everyday language. You can blame inadequate computer maintenance, faulty hardware, as well as a massive increase in high resolution digital photography and HD video.

Having a backup drive has become essential. Those serious about their storage needs turn to Network Attached Storage (NAS) devices. Like most tech available today, those range from introductory models with a modest set of features, to complex powerhouses with a myriad of options.

Thecus N5550 at-a-glance

What I'm taking a look is a fairly complex device whose feature list is anything but basic. The Thecus N5550 is a five-bay NAS powered by an Intel Atom Processor D2550 (1.86GHz Dual Core) and 2 GB of DDR3 RAM. There are two RAM slots, which makes memory upgrades a breeze.

This appliance is well made, and its robust (mostly) metal construction ensures that, once the drives are installed, you won't be able to knock it over accidentally.

The NAS has a variety of ports: USB 2.0, USB 3.0, HDMI, VGA, eSATA, LAN2, WAN/LAN1, MIC input, line input and audio output. The front is equipped with an LCD display for accessible monitoring, below are two examples of information it can display:





You don't even need a computer to administer this NAS. Thecus has made available a module that allows you to manage it by using a keyboard and a screen connected via HDMI. The VGA output allows you to attach traditional monitors, projectors and televisions. If you want to play audio files, you can also attach speakers.

If you want to backup data directly from the N5550, you can use an external network or optical drive via the Data Burn module. This can come in handy if you need your data burned to a CD, DVD or Blu-ray disc.

Installing the drives



The HDD enclosures can hold 3.5" or 2.5" disks and are quite sturdy, with rubber pads

For the purpose of this review, I used two WD Red 3TB HDDs, designed specifically for use with NAS devices.

Using a decibel meter app for iOS, I measured the noise coming from the NAS while working at around 55 dB, which is fine, unless you're used to working in a very quiet environment.



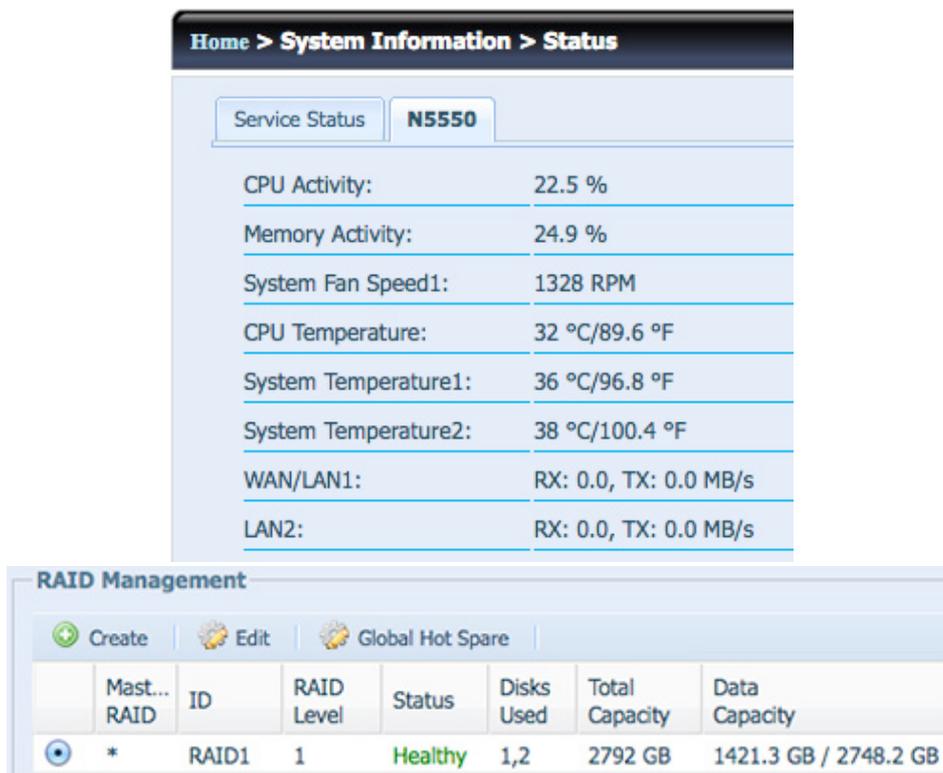
Administrative interface

The device I tested was running the latest firmware (2.04.05). Just like I expected, the administration GUI is rich with options.

Although its design takes you back to the days of Windows XP, don't let that fool you, as it's well laid-out and easy to use.



It's always a good idea to keep an eye on the status of your NAS device and here's the information at-a-glance:



The System Monitor can be setup to monitor network throughput, fan/temperature status, CPU/memory utilization, and on-line user list in various protocols:



If you enable the History function, System Monitor will allow you to select different periods for each selection. This is particularly convenient if you want to pinpoint certain issues.

The installation of modules is straightforward so you can get to work instantly, and the N5550 also comes with built-in Dynamic DNS (DDNS) support.

Backup and apps

Chances of data corruption exist even if you use multiple drives in a RAID configuration. If you're interested in this device, you're probably passionate about backup and storage, so

you'll be pleased to learn that you have the option of making backups to another remote or local NAS, as well as Amazon S3 right out of the box. Those looking beyond storage/backup can also use this device for numerous purposes, such as a mail or IP camera server.



The N5550 can run apps which you can install using the administration GUI. At the time of writing, the Thecus App Center featured an impressive number of nearly 400 apps spanning several categories. Just to mention a few

that (IN)SECURE Magazine readers will find particularly interesting: Nagios, McAfee Antivirus, TrueCrypt, xCloud, Dropbox, Syncrify, WebMin, Splunk, Ruby on Rails, Apache and MySQL.



Thecus made sure you can access your NAS even when on the move by using an iOS or Android device and apps. T-OnTheGo allows you to access and manage files, as well as play videos directly from your Thecus NAS. T-Dashboard enables you to view the status of the device and control some administrative functions.

Conclusion

The Thecus N5550 is feature-rich, robust, simple to setup and use. It's a versatile device with wide appeal, a good fit for anyone storing and managing terabytes of data with security in mind.

DDOS PROTECTION

DDOS ATTACKS ARE NOT A QUESTION OF
'IF' BUT 'WHEN'



ARE YOU PREPARED?

**AUTOMATED SERVER
PROTECTION AUTOMATED**

24X7 MONITORING

**PREVENTS SERVICE
DISRUPTION**

**SAFEGUARDS YOU
BUSINESS**

**PROVIDER LEVEL
NETWORK PROTECTION**

**ISP & DATACENTER
PROTECTION**

**CONTROL OVER YOUR
ENTIRE NETOWRK**

**PREVENT COLLATERAL
DAMAGE**

**PROXYSHIELD
WEBSITE PROTECTION**

**NO CONTRACTS OR
HARDWARE NEEDED**

**STOPS ATTACKS
UNDERWAY**

**KEEP YOUR
HOSTING PROVIDER**

ORDER NOW

**VISIT GIGENET.COM
1-800-561-2656**



SALES@GIGENET.COM



Report: Hack In The Box Amsterdam 2014

by Zeljka Zorz



I always look forward to the Hack in the Box conference in Amsterdam, and I'm never disappointed. This year, though, my expectations were more than just met - they were exceeded.

This year's edition was different than previous ones in a few aspects. First: the venue. The conference has moved to the imposing and conveniently centrally located De Beurs van Berlage, the former building of Amsterdam's Stock Exchange.

Apart from being an impressively beautiful building, it offered great spaces for the presentations. Phil Zimmerman delivered his talk about pushing back on pervasive surveillance in a chapel-like space, which certainly added to the seriousness of the topic. One of the presentation auditoriums was a futuristic-looking glass box, and happenings at the Haxpo could also be observed from upper floor balconies as the expo was placed in an internal courtyard. Finally, all the spaces were easily and quickly accessible, which is important when you're running from one presentation to another.

As usual, the Haxpo hosted hackerspaces, but also a "lab" where you could learn to solder and create a TV-B-Gone keychain, a sleep mask for inducing lucid dreaming, and more. There was a lock-picking corner, and a num-

ber of booths where the researchers were displaying and explaining their projects. It was also the place where the Capture the Flag (CTF) battle took place and, it's good to note, this year two of the participating teams consisted of women.

I'm mentioning this because this year's edition of the conference also had an all-women keynote lineup that included (among others) Katie Moussouris, former Senior Security Strategist Lead at Microsoft Security Response Center and current Chief Policy Officer of HackerOne, IOActive CEO Jennifer Steffens, and Jaya Baloo, the energetic CISO of KPN, the biggest Dutch telecom operator and owner of several ISPs.

Unfortunately for me, I only got to witness the first two. Moussouris talked about the need for hackers to start hacking (and fixing) things for the greater good, and Steffens delivered an stirring tribute to her colleagues - researchers / hackers that inspire other people and herself. More on Steffens' talk on page 46 of this issue.

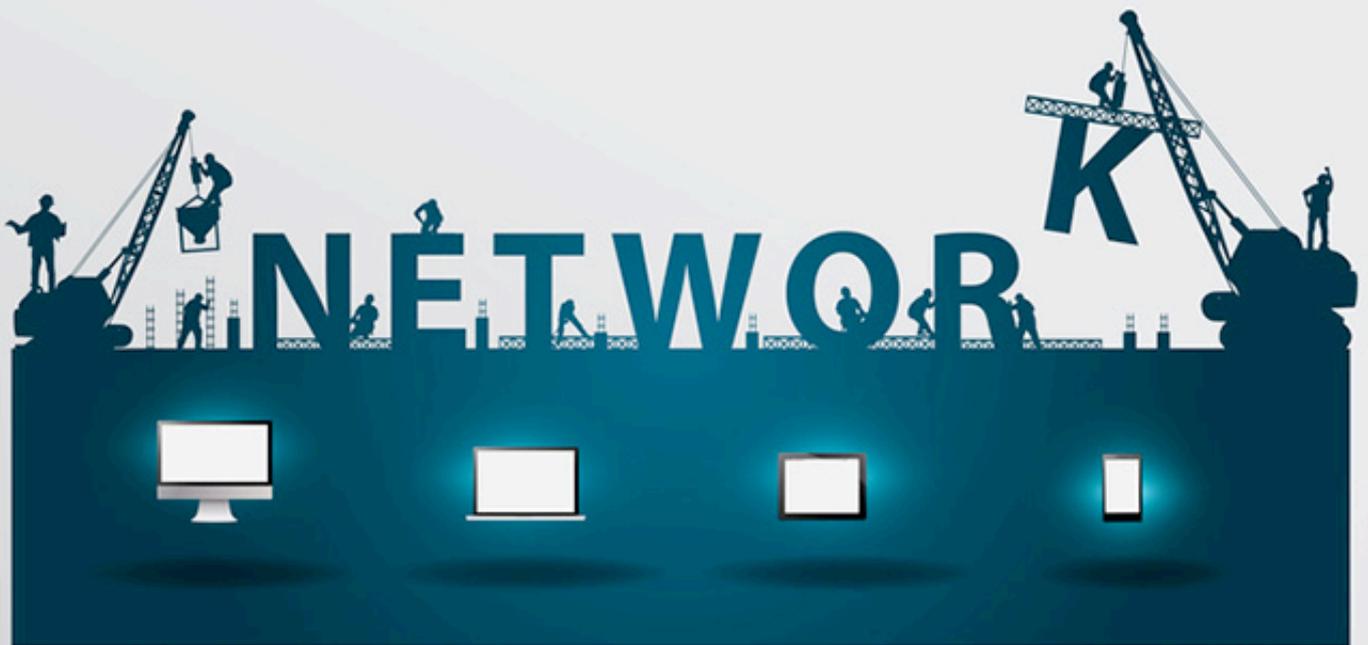
Another great decision by the conference team was to make the entrance to the Haxpo free, so you could see groups and individuals coming in from the street and be amazed. It was particularly heartwarming seeing groups of children asking a hundred and one questions at the booths. This was a good move in more ways than one, as conference presenters and "working" visitors felt free bring their children along for the trip and to the conference.

Aside from the usual two presentation tracks, this year there was a third one - the HITB Haxpo Track - where hackers, makers, builders and breakers took turns to deliver 30-minute-long presentations open to the general public. This track was also arguably the most interesting one for less technical visitors, and hackers could hear about legal issues they might encounter, security awareness, and more (haxpo.nl/hitb2014ams-haxpo).



Zeljka Zorz is the Managing Editor of (IN)SECURE Magazine and Help Net Security (www.net-security.org).

www.insecuremag.com



Ensuring the integrity of Rostelecom's Wi-Fi network by Ramil Yafizov

Large-scale sporting and entertainment events can put a huge strain on wireless infrastructure with a whole host of unsecured devices flooding onto the network. Leading Russian communication service provider Rostelecom needed a secure and robust security system to protect itself and the influx of new users utilizing its network during February 2014.

Earlier this year, Rostelecom rolled-out one of the largest deployments of free Wi-Fi hotspots seen in Russia, to accommodate the tens of thousands of visitors set to descend onto the city of Sochi.

The city is the 52nd most populous city in the Russian Federation with only 350,000 residents. Although the cellular capacity was adequate to support its residents, the sudden addition of tens of thousands of smart-phone carrying visitors onto the network would have strained capacity to breaking point.

Recognizing this potential issue, Rostelecom took the decision to deploy free Wi-Fi hotspots throughout the area to alleviate network pressure and supply high quality levels of coverage to visitors. Hotspots were deployed with sufficient bandwidth to cope with the streaming of ultra-high definition TV from hundreds of

users simultaneously. Over 1,100 optical wires were used, supplying speeds of up to 140 Gbps.

This level of robust infrastructure was required as it was difficult to predict the number of users who would be accessing the network at any one time, and how many of these would be using high bandwidth applications. Sudden spikes in demand create peaks and troughs in network usage, meaning Rostelecom had to deploy a network capable of excelling even in "worst case" scenarios.

One of the main concerns when deploying such a large network to cater for a wave of users with unknown and potentially unsecured devices is security. There are a vast number of potential security risks in deploying a large hotspot network, and not just for the users themselves.

The whole infrastructure needs to be protected from the increasingly common threat of DDoS.

The level of international attention on the city in February meant the network would suddenly become a very prestigious target for potential hackers, who often look to cause the highest level of disruption and create the largest number of newspaper column inches by attacking the most noteworthy targets. One of the largest recorded and notorious DDoS attacks – on Spamhaus, a body formed to track spam email activity and expose the main per-

petrators – exposed the website to 300 gigabits per second of useless traffic, forcing the website offline.

With these attacks increasing in regularity, notoriety and scale, Rostelecom sought to deploy a solution that would protect users and simultaneously protect the operator's infrastructure from attacks perpetrated from inside of the network. These types of attacks could render this expensive infrastructure useless and open the network to further security threats, as well as damaging its reputation with existing customers and partners.

AS DNS IS THE FIRST TOUCH POINT IN ANY INTERNET TRANSACTION, USING IT TO IDENTIFY INFECTED CUSTOMERS IS BOTH LIGHTWEIGHT AND COST EFFECTIVE, SINCE IT ONLY HAS TO DEAL WITH RELATIVELY SMALL DNS PACKETS

Network users infected with botnet-based malware serve as a pertinent example of an inside threat. Users' devices can be infected with malware and once the infected devices are connected to the network, they can then be controlled by a "bot master" who can consume network resources and wreak havoc. Many cyber criminals employ botnets as their instrument of choice to execute malicious activities.

For example, they might rent their botnet out to perform DDoS attacks against websites or they are tasked with penetrating network defenses and looking for valuable data. Bot masters control botnets by providing the agents that infect devices with instructions dictating the malicious activities. They do so by providing these instructions via a command and control (C&C) server.

One major risk is data exfiltration, which can have serious consequences: loss of valuable intellectual property and unauthorized disclosure of personal and confidential information. Most perimeter-style defenses only protect from threats emanating from outside of the network ("outside-in" attacks) – they are powerless to defend against DDoS attacks emanating from inside of the network infrastructure. Bots can lie dormant for long periods of time within the network before being activated

and used to attack resources such as DNS servers, gateways and mobile evolved packet core resources. These inside-out attacks can also affect external resources such as websites, network assets, enterprises and end users.

In order to limit this risk, Rostelecom employed DNS-based security intelligence techniques. DNS-based security intelligence makes use of a network's caching DNS server to monitor and block DNS queries to known botnet domains.

These domains are the addresses of servers that are in the control of cyber criminals for purposes of botnet command and control. Bots will perform a DNS query for one or more of these domains in an attempt to connect to these servers in order to receive their instructions. By monitoring queries to these domains, all infected clients can be identified on the network. Moreover, by subsequently blocking access to the domains, malware responsible for the bot infection is denied the critical instructions it needs to function.

As DNS is the first touch point in any Internet transaction, using it to identify infected customers is both lightweight and cost effective since it only has to deal with relatively small DNS packets.

If, as a network operator, you have a list of known botnet C&C domains, you can determine which clients are infected on your network by comparing that list to your DNS logs. The network operator can also use this information to configure its DNS servers to block any queries to these domains, which denies the bots the instructions needed in order to conduct malicious activity.

The system installed for Rostelecom included direct and instant access to a list of malicious domain names accessible for both its cellular and network of Wi-Fi hotspots. This database is updated in real-time and provides a comprehensive list of suspicious websites that can be used to signal the launch of attacks from bots already present in the network. The sheer number of unsecured devices could provide an open gateway to bots entering the infrastructure, therefore, this element was a vital layer of protection.

The solution deployed to protect the hotspots included an in-built ability to isolate any attempted DDoS attack and allow other customers to continue to access the network and minimize any disruption. This was a vital aspect of the deployment as this would enable Rostelecom to continue to offer an uninterrupted service and maintain network integrity to its 100m customers across Russia, even in the event of a large DDoS attack.

Using precision policy capabilities, a system was installed with the ability to segment, identify and enforce policies by users or traffic types, providing a level of policy granularity that is capable of throttling attacks using rate-limiting technology. Preventative throttling of attacks works alongside the proactive prevention of attacks by blocking access to addresses known to be related to malware and botnets.

Rostelecom was able to enforce DNS precision policies based on specific and adaptable criteria including by type of query, client IP or response size.

Two Vantio CacheServe servers from Nominum were installed on dedicated servers with 3GHz of multicore CPUs and 64GB of RAM, running a RedHat EL6 operating system.

In order to offer a robust level of protection for customers during their time in the city and also to protect its own resources, Rostelecom deployed a Defense in Depth strategy. The DNS is a vital part of this proven layered approach. It represents an essential link in the chain to plug up potential holes in the broader strategy while providing redundancy to multiple other security solutions.

Any Defense in Depth strategy is made up of a series of layers that are designed with the same principles in mind. It must:

- Fill gaps in the security position
- Provide redundancy for layers where a single strategy is not always enough.

The DNS should be considered as one of the Defense in Depth layers to address these needs because, just as end users rely on the DNS for connectivity, so do bot-infected machines to reach their command and control servers for instructions, code, and other forms of payload. DNS can be utilized to control this traffic right at the source, the DNS query.

As mentioned earlier, the DNS server can be adapted to block malicious (e.g. botnet command and control) domains. There is no need for additional investment in costly DPI components to do the job the DNS was designed for.

By carefully considering the security implications of its Wi-Fi deployment, Rostelecom was able to ensure the influx of visitors in the early part of the year were able to utilize the network safely without negatively affecting the rest of the carrier's infrastructure.

Events passed without security incident and the system remains in place to ensure its domestic customers are able to utilize its network resources safely while also protecting the integrity of the network.

Ramil Yafizov is a Systems Engineer at Nominum (www.nominum.com). He has over 10 years' experience working with security technologies, and has held senior level sales and sales management positions at several early stage companies in network infrastructure, software applications, and wireless technologies.



This is a question that Jennifer Steffens, IOActive CEO, often asks hackers she meets on conferences around the world. More often than not, the answer is movies: *War Games*, *Hackers*, *The Matrix*, and so on. But today, it is the real life hacking that is inspiring the movies of tomorrow.

"Hackers are doing epic stuff," she says, and they are now inspiring movies and comics, she pointed out in her keynote at the Hack In The Box conference in Amsterdam.

People are coming up with crazy new technologies every day, and that technology is getting to the larger public at an ever increasing pace. With it come new ways to exploit the technologies in unexpected and often malicious ways, and there is an increasing need for people who will research the security of these new technologies.

As CEO of IOActive, Steffens has the opportunity to work every day with some of the brightest in this field, and she says that they are a daily inspiration.

So, what makes a good researcher and a good hacker? For one thing, to break something you first need to know how it's made, you need to understand the technology.

Case in point: Mike Davis, IOActive's principal research scientist and head of the embedded devices department, got interested in testing the security of the computers operating nuclear bombs. Needless to say, this is the kind

of technology that a government is unlikely to share with anyone from the "outside," so he decided to try to recreate the tech by himself, taking for inspiration a device from the movie *The Manhattan Project*.

Another thing that you need to have to be a good hacker is seemingly inexhaustible curiosity, and to know how to look at problems from angles that no-one has contemplated yet. Also, be persistent - despite many failures - and work hard. And when the game doesn't give you satisfactory results, you have to know how to change it and keep playing.

Take for example IOActive's researcher Ruben Santamarta. After he discovered many design and security flaws in satellite communication systems, and being practically ignored by the vendors when he shared his research with them (only one responded), he wrote a report and released the research to the public. One hour later, the industry took notice - all because he knew how to change the game, change the language, reframe the question and bring to the fore what mattered: how the exploitation of these flaws could impact people.

SOME HACKERS AND RESEARCHERS ARE MOTIVATED BY MONEY, BUT MOST OF THEM ARE MORE INTERESTED IN "PLAYING WITH TOYS."

He is not the only one that knows how to play the public attention angle. As Steffens says, sometimes a good researcher means also to be a good showman. When researchers Charlie Miller and Chris Valasek (the latter is the Director of Security Intelligence at IOActive) researched and discovered flaws that can be exploited to hijack car computers and, consequently, cars, they went public in a spectacular way, giving journalists a terrifying real-life demonstration.

The public took notice. Now when some people go buy a new car, they ask about the secu-

rity of the on-board computer system, says Steffens. The game has changed - manufacturers are beginning to see why the issue is important to their bottom line, and some of them have moved to employ researchers who will aim to keep the systems safe.

Some hackers and researchers are motivated by money, but most of them are more interested in "playing with toys." Most of them are also interested in helping with things that affect people directly, and want their research to really matter.

ASK QUESTIONS, START BREAKING THINGS, GET TO KNOW THE COMMUNITY, DISCLOSE RESPONSIBLY AND, FINALLY, BE INSPIRED!

One such researcher was the late Barnaby Jack. His first claim to (wider) fame was the famous ATM hacking, but he later turned to researching the security of medical devices, mainly pacemakers. One of the ways he approached the research was by interviewing Steffens' father, who had one inserted following serious heart problems. Jack wanted to know how was it like to have a pacemaker and how it affected him, in order to know on what attacks to concentrate on.

Another thing that Steffens deems important for a good hacker: "No excuses." Determination and dedication are crucial.

"If you want to change the InfoSec scene, get involved in InfoSec," she says. "At IOActive, we're looking for bright minds, cool ideas, passionate and hardworking people." They want the people who want to do research whether they were paid to do it or not.

She finished with some advice for hackers: Ask questions, start breaking things, get to know the community, disclose responsibly and, finally, be inspired!

Zeljka Zorz is the Managing Editor of (IN)SECURE Magazine and Help Net Security (www.net-security.org).



SECURITY NEWS & INDUSTRY INSIGHT. WWW.NET-SECURITY.ORG

Automated Security Incident Response and Containment Capabilities



THREAT RESPONSE

Respond to advanced threats in minutes instead of hours or days

Learn about Threat Response www.proofpoint.com/ThreatResponse
Contact us at: 877-634-7660 or on the web at sales@proofpoint.com



Events around the world

Black Hat USA 2014

www.blackhat.com/us-14/

Mandalay Bay, Las Vegas, USA / 2 August - 7 August 2014

PasswordsCon 2014 Las Vegas

www.passwordscon.org

Tuscany Suites & Casino, Las Vegas, USA / 5 August - 6 August 2014

BsidesLV 2014

www.bsideslv.org

Tuscany Suites & Casino, Las Vegas, USA / 5 August - 6 August 2014

Cyber Security Expo 2014

www.cybersec-expo.com

ExCel London, UK / 8 October - 9 October 2014

HITBSecConf2014 - Malaysia: Past, Present & Future conference.hitb.org

InterContinental Kuala Lumpur, Malaysia / 15 October - 16 October 2014

Beyond Heartbleed: Closing SSL implementation gaps within our own networks

by Jason Sabin



As security professionals put in place the final patches to fix the Heartbleed bug, I think network administrators have a unique opportunity to look beyond Heartbleed to close the unintentionally self-inflicted SSL implementation vulnerabilities within their control.

The ubiquitous authentication and encryption transport layer security protocol (TLS), more commonly referred to as secure socket layer (SSL) remains the backbone of internet transactions and the primary method of secure communication. Heartbleed did not reveal a flaw in the SSL protocol itself, but was the result of poor coding and implementation of the Heartbeat functionality within OpenSSL. It reminds us that implementation matters.

Unfortunately, SSL is not always enabled where it is needed or always deployed correctly. A key to defending against active attacks and surveillance efforts of unwanted intruders is using the tools we have today to correctly implement SSL.

Whether it's Heartbleed or NSA snooping, we've learned some valuable lessons in recent months:

- By protecting our information, SSL done right provides enormous, intrinsic value to our world economies, intellectual property, personal freedom, and entrepreneurial initiative.
- Attacks are on the rise, and we (organizations) need to do more to protect our most valuable assets and assure that our own networks are properly using SSL.
- Encryption works and is our friend. "Trust the math," as Bruce Schneier has told us. We need to encrypt more data.
- It's about the implementation. If we properly deploy and configure SSL, we can make surveillance and attacks expensive, difficult and unattractive to intruders.

As SSL usage increases, some common practices leave organizations vulnerable

As an industry, we're moving well beyond the standard practice of only using SSL for e-commerce. As a minimum, leading organizations today, deploy HTTPS on any server

hosting dynamic content where data is exchanged. Leading brands such as PayPal and Google are taking it one step further and applying HTTPS to their entire site to prevent side-channel attacks and other methods of stripping user information as they move from protected to non-protected pages within a website architecture.

Surprisingly, many organizations still do not use any SSL at all on critical servers. Of course, this exposes users to Man-in-the-Middle (MitM) attacks, and with today's increasing awareness among consumers, may also act as a deterrent for people to conduct e-business via their site.

Let's look at some common problem areas and see how they can be addressed:

Intranet and mail servers

No matter how many locks someone might have on the windows and doors in their house, it is still a good idea to place valuable possessions in a safe deposit box, in case intruders gain access to their house. The same theory can apply to data security within your internal network.

Network administrators assume that internal servers behind a firewall are safe enough, and that they do not need to use SSL certificates for servers that are not public-facing. Yet, we have seen in recent events such as the infamous Target breach that many pathways exist for attackers to get behind the firewall – some that could be hidden from IT.

If organizations are not using multiple layers of security, administrators may be leaving their networks vulnerable to the first hacker or malware that slips in. Once inside, the attacker has ample time to sniff networks without detection.

Mandiant's fourth annual M-Trends report, released in 2013, showed that advanced attackers typically are on a network 243 days before being discovered. That's more than enough time to launch Man-in-the-Middle attacks that intercept or compromise server data.

In a worst-case scenario, an attacker could access company e-mail, proprietary code and

databases – leaving lasting damage and an enduring negative impression on a company's brand that is difficult and expensive to overcome.

The best fool-proof method to protect against these types of scenarios is to deploy SSL certificates on every server, internal or external, regardless of the sensitivity or volume of data that the server manages. With each certificate deployed, proper implementation and configuration becomes a must.

FTP

FTP remains one of the most common ways to transfer large files across the Internet, and is used by 51 percent of organizations, according to a recent Harris Interactive poll of 1,000 IT decision makers.

The problem is that with today's threats many of these FTP servers in use fail to use encryption. Administrators need to convert improperly clear text FTP services with SFTP or another secure file transfer protocol.

APIs

In today's era of cloud computing and expanded connectivity, business-to-business communication is growing. With this trend, it becomes increasingly important for these data connections to be protected via SSL. The use of APIs is rapidly providing efficiencies as organizations move more of their data to the cloud. REST APIs have become especially popular in recent years, due to their ease-of-use. However, with so much data being transferred to and from an organization's network via APIs, it can be an attractive target for attackers.

That's why organizations need to take efforts to make sure that they are encrypting all API connections with SSL, and that their vendors and cloud providers can offer similar assurances about their security practices.

Popular internet sites, including Twitter and Google, use HTTPS to protect API connections and so should you. This is a simple step that can prevent leaky data connections in a cost-effective manner.

Connections to and from the cloud

With the advent of cloud computing, organizations are finding some efficiencies in managing their bandwidth and associated costs, as well as benefiting from the reduced need to manage inventory. Similarly, single sign-on functions are growing, thanks to the use of federation protocols, which sign and encrypt every user communication.

At the same time, we've seen how the NSA and other agencies gathering intelligence have taken advantage of a lack of SSL encryption of data flowing on cables to and from the cloud of some of the Internet's largest companies. The use of publicly trusted certificates can put a halt to the usefulness of such large-scale data collection.

To protect their critical data from plaintext interception, organizations need to apply SSL on all outbound and inbound data. They also need to receive assurances from their cloud providers that they also follow these basic security measures.

Self-signed certificates

At no time has the value of public trust in the SSL ecosystem been made more needful than in the wake of the NSA revelations. As noted cryptographer Bruce Schneier pointed out when discussing revelations of NSA surveillance, "Try to use public-domain encryption that has to be compatible with other implementations. For example, it's harder for the NSA to backdoor TLS than BitLocker, because any vendor's TLS has to be compatible with every other vendor's TLS, while BitLocker only has to be compatible with itself, giving the NSA a lot more freedom to make changes. And because BitLocker is proprietary, it's far less likely those changes will be discovered."

Self-signed certificates present the same problem when trying to identify and counter attacks. Because self-signed certificates do not rely on third-parties for trust, they make MITM attacks easier to pull off. Since no identity vetting has been done by a trusted, audited third-party, users have no way of telling if the certificate has been tampered with, and there is no early-warning system of trouble. Though they are often free, these certificates do not earn trust in the browsers, and

many times end up costing administrators more than they saved in lost business and trust.

Using all the tools we have

Amid today's heightened threat model, some existing technologies are gaining new attention for their ability to protect valuable data. These include: Perfect Forward Secrecy, HTTP Strict Security, Secure Flag, and TLS 1.2. So, why don't more users / organizations use them? In many cases, it's a matter of a lack of awareness of how their own SSL is configured, or they may not yet be an expert on how HTTPS works. But, that can be solved with the education that many administrators seek out.

Perfect Forward Secrecy (PFS) uses a distinct method to encrypt data without using the certificate's private key, meaning there is no link between the server's private key and each session key. In its simplest explanation, PFS makes every session unique, so if a hacker did obtain a key, they would be limited to only the information contained in that specific session.

All past or future session data would still be safely encrypted. While it remains very unlikely that an attacker can access and decrypt any encrypted session initiated on a secure server, PFS makes the attempt much less fruitful and difficult to achieve as well as protects future session decryption. PFS is available in nearly all major browsers and web servers and can be enabled by using the right Diffie-Hellman cipher suite configuration.

HTTPS Strict Transport Security (HSTS) is another technology that can protect web operators and users by allowing a site to request via a HTTP header of "Strict-Transport-Security" that it always be contacted over HTTPS. Frequently, users will omit the HTTPS when typing the secure site web address. This can create an insecure connection that an attacker can seize and manipulate. Only the most trained users might notice that an attacker might have redirected the connection to a similar but different domain intended to capture their personal information. From that point, the attacker controls the user's session and can mine passwords and other sensitive data at her discretion.

HSTS is simple to enable and is available in nearly all browsers and web servers.

TLS 1.2 is the latest version of the TLS/SSL protocol suite. It incorporates all the latest cryptographic protocol advancements in pseudorandom functions, authenticated encryption ciphers, and additional TLS extensions. If your infrastructure can support it, I highly recommend disabling all previous versions of TLS/SSL and moving everything to the TLS 1.2 protocol.

Using HttpOnly and secure cookies will help mitigate risk and protect your browser sessions from leaking or allowing MITM attacks, XSS injection, XSRF, and numerous other exploits. By utilizing these two options on your

web server, you will protect your SSL communication from being hijacked by common web based attacks. This is typically a common configuration within your web server implementation.

Using key lengths of 2048 or above is a must in your RSA certificates. Key sizes smaller than 2048 are quickly becoming vulnerable to brute force attack and are no longer considered strong enough. Most publicly trusted certificates have been converted to 2048 key sizes, but there are still a large number of internal certificates running on internal networks with 1024 bit key sizes or even 512. These are a risk within your network and should be converted to a higher key strength, if possible.

Key sizes smaller than 2048 are becoming vulnerable to brute force attack and are no longer considered strong enough.

Even with all of these settings configured correctly, you are still at risk unless you have the needed ciphersuite configuration. Nearly every SSL server is configured with a default set of ciphersuites that are typically not the most secure set. Commonly, you will find that anonymous and null ciphersuites are enabled within your server's configuration. Low ciphers—which include weak protocols, hashing, and other problems—could be enabled. Additionally, the ordering of the list is important. Experts recommend always including Perfect Forward Secrecy algorithms first and then only including the ciphersuites that are needed to support backwards compatibility.

As recent cases have shown, current encryption protocols work, and we just need to implement them thoroughly. We can all benefit from an approach that seeks to understand common implementation errors and apply simple ways to fix them.

The role of business intelligence

Recent research shows a key reason why many administrators' systems may not be up-to-date. According to Cisco's 2014 Annual Se-

curity Report, professionals lack the resources, skills and time to fully manage all the demands of optimum data security in an age of big data and increasing attacks. They often wear many hats, and web security is just one of those.

Consequently, as the attackers are getting smarter about their techniques, sometimes organizations are getting behind. They're struggling to get by with limited resources, leaving them stuck deploying archaic techniques to manage their SSL certificates and endpoints.

Frequently, due to a lack of other options, organizations use manual tracking processes, which introduce human error and result in significant downtime when a certificate unknowingly expires. In addition to incomplete certificate inventories, it can also lead to neglected servers that use outdated TLS versions or ciphers vulnerable to BEAST, BREACH, CRIME or other published attack theories.

In other cases, departments outside of IT might bypass standard corporate policies to order, install and deploy their own certificates.

When done outside of IT security's knowledge, a lack of expertise and a push for expediency over all else might lead to hidden configuration problems that downgrade the effectiveness of these SSL certificates. In a worst-case scenario, rogue employees may purposely set up malicious servers that can escape IT's watchful eye.

Perhaps, this can help explain why, according to Ponemon Institute, 51 percent of enterprises do not know about all of the keys and

certificates on their network. Meanwhile, as many as two in three certificates are enabled with ciphers vulnerable to the BEAST attack. In some cases, these might exist because web administrators do not know what they should be looking for. Alternatively, administrators might have thought that SSL was properly enabled on a server only later to find out that it was not installed correctly or at all, and the employee that purchased the certificate no longer works for the organization.

Unfortunately, security professionals cannot rely upon large budget increases to save the day.

Where to start?

Unfortunately, security professionals cannot rely upon large budget increases to save the day. Many more may not have the time or interest to become an expert in SSL or to stay up to speed on the latest RFC standard. At the same time, these security professionals are held accountable if a major security incident happens on their watch.

Fortunately, a heightened interest in SSL and security had led to the development of a number of automated tools that help provide relevant business intelligence in real-time for an administrator's certificate landscape. Budget-conscious organizations do not need to spend tens of thousands of dollars on certificate management systems that might include a lot of bells and whistles but might also be more than they need. My company and others have affordable solutions that can help.

In today's security model, it's important for administrators to have the knowledge of their

entire certificate landscape. Fortunately, administrators do not need to be PKI experts, but can take advantage of available tools and automation to gain real-time intelligence. By knowing what's happening across their SSL certificate and endpoint architecture and having a proven way to identify potential misconfiguration, the industry can take a major step forward, one server at a time.

It's a new era that requires new vigilance

Today's web offers exciting opportunities for enhancing life and connecting global economies and communities as never before. Our connected lifestyle also presents an attractive attack vector for criminals and nation-states. While events like the discovery of the Heartbleed bug cause considerable headache and concern and must be addressed promptly, administrators also may have a tangible impact on their day-to-day network security by focusing on the immediate, controllable, and unintentionally self-inflicted threats that may be lurking in their own networks.

Jason Sabin is the VP of Research & Development at DigiCert (www.digicert.com), where has helped expand the company's products and tools to a growing roster of customers, since joining the company in February 2012.

A lifelong tinkerer with a penchant for Thinking Maliciously, Sabin has been breaking down hardware and software since he was 13-years-old. Today, Sabin applies his deep knowledge of security and trust systems to enable DigiCert's customers to efficiently and effectively deploy SSL certificates and related authentication and encryption technologies.



Ironclad incident response Interview by Mirko Zorz

Mike Horn is the Vice President of Threat and Response Products at Proofpoint. In this interview he talks about the challenges related to incident response.

What are the most significant challenges involved in setting up and maintaining a well-rounded incident response process in a large organization?

A well-rounded incident response process addresses several key areas. At the highest level, consider the following:

- What needs be done and how fast?
- Who will do it?
- What tools will make sure it can be done effectively and efficiently?

The list of tasks and timing seems like it should be a simple checklist – have a list, do everything on it, and do it as quickly as possible. The problem with such an oversimplification is that this puts time and security quality at odds.

The security quality vs. time challenge represents the dilemma that we face everyday. If we spend more time, we can do a better job on each step of the incident response process. Unfortunately, we live under time constraints, and incident response teams can

come under pressure to review hundreds or even thousands of alerts in a short time window. If you face 50 alerts in 24 hours and the load increases to 200 alerts in 24 hours, the time allocated for reviewing alerts actually decreases while the chance of a real attack increases.

This is a real challenge in maintaining a strong incident response process, as the skill(s) of the security analyst can play heavily in the speed and quality of the analysis.

Another hidden aspect of the “what needs to be done” checklist is properly understanding the order of the checklist. One of the easiest steps that is often ignored is what type and depth of forensics to apply – and more importantly, when to do it.

This is a challenge since the news tends to focus on forensic analysis of breaches. Unfortunately, deep forensics about malware lifecycles, human errors, and network configurations can take weeks or months depending on the complexity of the infection and the skill of

the analyst. Focusing on deep forensics while the breach is still active means that confidential information could be bleeding out of your network for those weeks or months. Deep forensics should be done after an infection has been locked down and the threat contained.

It's a huge mistake for companies to skip the "containment" phase of active security and jump into the post-mortem security steps of deep forensics and remediation. Companies often make this mistake as many product and services vendors push their forensic and remediation solutions without advocating the obvious containment requirement of incident response.

When you consider the available manpower and the rapid response that's required in security, hiring X people for Y incidents may seem prudent. The risk is that what you want is not necessarily what you can hire. Skills in security operations span an understanding of multiple OS platforms, networking, command-line scripting, and programming languages as a starting point.

Add to that knowledge and experience that comes from analyzing and fighting off years of attacks or malware infections. And let's not forget the ability to communicate and document analysis, actions, and code.

There are many steps in incident response, but at the core we're dealing with the attack or infection. One important step is verifying if a security alert is true or false, as time wasted on false positives is time that could be better spent elsewhere. There are third party automated tools to eliminate false positives and confirm and prioritize threats, but many firms have handcrafted scripts to do one or more of these steps. Both third party and homegrown tools can be useful time savers. However, it's a challenge for IT security teams to be in the software development business. As organizations and teams scale, building and maintaining custom security tools becomes too costly and inefficient.

When it comes to incident response, intelligence and context are essential. How does a security team make sure they have the right information at all times?

The term "Threat Intelligence" refers to the up-to-date information about threats "in the wild." In an ideal situation, a firm will work with best-of-breed threat feeds to constantly provide information on new malware, command and control servers, hostile domains, compromised domains, and more.

These would be seamlessly integrated into the team's tools to apply the threat intelligence against reported breaches or infections in the incident response process.

Contextual information is necessary to effectively combat these sophisticated threats. External threat intelligence is just one type of context, but there's more. Once an attack reaches your network, it's prudent to understand which systems are infected, which network systems are compromised, and even if a targeted system has indeed been infected in the way the detection tool reported. For example, internal context can tell you that both the CFO's PC and the financial systems database were targeted by malware launched from North Korea. If your context and intelligence were coupled together, you would move to act immediately.

In order to connect these dots, security teams often use third party software, or code their own integrations to a number of threat intelligence and context providing services. As we discussed earlier, since the security team's focus should be on security and not software development, it's advisable to use third party software. Specifically, a solution that provides continuous context and intelligence and can automatically assemble, integrate, and analyze information from these sources before any human intervention is required.

What are the traits of an experienced incident response analyst?

The old saying "good help is hard find" definitely applies to finding good incident response team members. We hear it from customers and partners as they struggle to find qualified people to join their teams.

This problem is apparent when you look at the job boards. We found an interesting job posting that highlights the skills necessary and the difficulty of finding this person:

EXPERIENCE / SKILLS

8+ years experience in Incident Response

- Must: familiar with the Attack Kill Chain framework
- Must: in depth understanding of Windows Unix systems
- Must: practical experience with Linux CLI and scripting/programming (Perl, regex, etc.)
- Must have a demonstrated practical knowledge of networking
- Must have demonstrated practical experience with log analysis, for example:
- Event Logs (Windows, Unix, DNS, DHCP, Antivirus Logs)
- Certifications are a plus but not required, depending on experience: GCIH, GREM

4+ years Experience in Forensic Investigations

- Evidence Acquisition – volatile and static
- Remote & Local Evidence Analysis
- Practical tool experience (Encase / Sleuthkit / Autopsy / FTK / Etc)
- Creating and analyzing timelines
- Data carving extraction
- Windows Unix forensic analysis & Reporting
- Certifications are a plus but not required, depending on experience: GCFA, ACE, EnCE

Experience working in a collaborative team environment performing the following functions:

- Technical mentoring
- Problem solving
 - Driving organizational change through innovation
- Tactical development: Python, Perl, etc
- Reverse Engineering

That's a robust skillset. Even if you found the perfect candidate, how much are you willing to pay? How much will your competition pay?

What are the benefits of automated incident response?

The core benefits of automated incident response are five-fold: Replacing manual tedious task with automatic context collection, providing regular and consistent analysis on context data, delivering incident prioritization with automatic elimination of false positives, automatic triggered mitigation and enforcement, and a general increase in speed while reducing human errors.

1. Automate repetitive tasks: Collecting whois data, domain freshness information, IP reputation, command and control server identification, and indicator of compromise data collection are frequent tasks and time consuming. This work should be done with automated incident response tools.

2. Provide regular data collection, connection, and analysis: Drawing insight and un-

derstanding from collected data is greatly enhanced via automated analysis and comparison capabilities.

3. Incident prioritization and elimination of false positives: Applying threat context, verification logic, and automatic analysis can eliminate false positives and elevate the true priority of a detected threat.

4. Automatic triggered mitigation and enforcement: Automatic analysis can be used to escalate visibility of a threat, automatically fire off mitigation tasks such as revoking Windows AD privileges, or blacklisting certain domains or IPs, thereby locking down the suspected threat.

5. General increase in speed while reducing human errors: Automatic "all the above" or parts of the above will no doubt increase the speed of response, but more than that, machine algorithms that compare, verify, and analyze threats can do it with fewer errors while considering more variables. The result is an overall increase in security.

Mirko Zorz is the Editor in Chief of (IN)SECURE Magazine and Help Net Security (www.net-security.org).

remember when
the internet and technology
were going to save the world?
SO DO WE.

At Geeks Without Bounds, we believe that technology can be the great equalizer. Our mission is to create social justice through mutual aid. We do this by:

- Hosting global hackathons,
- Accelerating humanitarian projects
- Connecting NGOs and technologists (you)

Interested? Here's how you can plug in.

donate to our cause: GWOB.ORG/SPONSORSHIP/

apply to our accelerator program: GWOB.ORG/APPLY/

join the conversation: GWOB.ORG/GET-INVOLVED/

**GEEKS
WITHOUT
BOUNDS**

GWOB.ORG



Hands-on fun at HackKid 2014

by Chris Hoff

In April, families and tech industry leaders descended on The Tech Museum of Innovation in San Jose, California, for HackKid 2014.

We had a great turnout for the event – reaching capacity through advanced ticket sales with over 200 attendees, including parents with children ages 5-17.

We were thrilled to see again such great cultural and gender diversity: nearly 50% of the attendees and 40% of our presenters were women.

We had families travel all the way from Hawaii, Tennessee, Ottawa, Toronto, Utah, Chicago and New York to participate!

We started HackKid in 2010 in Boston to provide kids and their parents with hands-on workshops and activities to raise awareness, excitement and understanding of technology, gaming, mathematics, safety, privacy, networking, security and engineering and their impact on society and culture.

Continuing our commitment to bring technology to everyone, we offered numerous educational scholarships for those who would

otherwise not be able to attend.

It's been exciting to work with colleagues and volunteers to organize events like HackKid because it's a way to give back and demonstrate how the security and technology community is a close-knit group, and we have a blast putting together educational programs to stimulate young, bright minds.

It also illustrates the spirit of hacking: finding innovative ways to make, break and use things to create a better world.

While the attendees may not have realized it, many of the sessions were lead by notable luminaries, industry experts and researchers. We also had some amazing kids leading sessions as they taught other kids their skills.

The agenda included nearly 30 multidisciplinary sessions each day with a mix of both interactive talks as well as hands-on labs.

Popular sessions included “Bring your son or your daughter – it’s time to learn to solder,” “Fun with Crypto(graphy),” “The Science of Locks – improving security by learning how to break it,” “How-to R2D2 – An intro to robotics,” and “If Harry Potter Could Code – Advanced programming in Python the Slytherin Way,” as well as squishy circuit electronics, Raspberry Pi and Minecraft, food hacking, 3D printing, robotics, trebuchet building, and a computer controlled Lego Derby competition.

We also covered Internet safety, staying safe online, dealing with cyber bullies, physical self defense, online gaming safety and a session on how the Internet works, helping parents communicate and interact with their kids, especially as parents (even the most tech or security savvy) come to the realization that their kids will soon surpass their knowledge, if they haven't already.



It was thrilling to see the event come together, and we had a ton of fun interacting with the kids and families.

I'd like to give a quick shoutout and thanks to our corporate sponsors, Juniper Networks, Kaspersky Labs, Wickr and No Starch Press, and our many private donors. Most impor-

tantly, I'd like to recognize the many individual and family volunteers who gave their time to setup, proctor and mentor the kids and parents across the two days.

The future is bright – and we look forward to organizing more of these events.

Chris Hoff is the organizer of HackKid and VP, Strategic Planning - Security Business Unit, at Juniper Networks (www.juniper.net).

Are you ready for the day when prevention fails?

by Tom Cross



According to a recent study by the Ponemon Institute, most security professionals agree that the best thing their organizations could do to mitigate future breaches is to improve their incident response capabilities.

For years, IT security teams have been focused on preventative measures that often involve systems that sit at the network perimeter and keep the bad stuff out. However, no matter how much effort is spent on prevention, there will come a day when your defenses are going to break, and the question becomes: Is your organization prepared for that day?

Many organizations aren't. Respondents to the same Ponemon Institute study also indicated that investment in incident response within their organization had remained static or decreased over the past 24 months.

Why is this the case? Often, it's because management underestimates the value of incident response preparedness. Many organizations have an incident response plan on paper, but it has never been tested, and when real incidents occur, it isn't followed.

Breaches happen to major organizations on a regular basis. There is a constant drumbeat of news stories about significant security com-

promises. While it isn't realistic for organizations to expect that it will never happen to them, a rapid and professional response when incidents do occur can limit their scope and their reputational impact. However, you can only respond effectively if you are properly prepared.

Creating an effective incident response program

Creating and maintaining an effective incident response program requires constant effort. Organizations cannot just set up a team of experts and call it a day. This team needs to be continuously trained, its success regularly measured, and its skills periodically assessed and improved. Otherwise, the team won't really be ready when an incident occurs.

Additionally, threat indicators uncovered during incident response procedures should be continuously fed back into an organization's security strategy to remediate ongoing issues and help prevent similar attacks in the future.

The incident response team should not be relegated just to the IT department. Those responsible for cyber security must regularly communicate with and involve other departments within their organization, including C-level executives, and make security the responsibility of everyone in the business.

The fact is that executives are often personally targeted by attackers, so it's important to ensure that the entire organization has basic security training. Furthermore, a security breach can have an impact on the whole company, so it is best to involve professionals from departments such as legal and public relations up front before a crisis occurs so everyone is prepared to handle it if necessary.

A successful incident response effort must involve the right mix of people, processes and technology.

People: Building a solid incident response team

The first step in planning for incident response should be the creation of appropriate security incident response teams. These should include both an operational computer security incident response team (CSIRT) and a multi-disciplinary threat management group.

The CSIRT

The CSIRT consists of the technical staff that conducts the tactical response to a security incident. CSIRTs typically include technical functions such as:

- **Security analysts** – who figure out what happened, extract relevant indicators, and determine necessary remediation. Roles can include:

- o Network Forensics Analyst
- o System/Hard Drive Forensics Analyst
- o Malware Analyst
- o Threat Intelligence Analyst

- **Security engineers** – who monitor the network for incidents and keep detection and log collection systems running, up-to-date with intelligence, and automated where possible.

These roles can include:

- o Security Operations Engineer
- o Security Systems Engineer

In large organizations, it is important that many of these team members be solely dedicated to incident response, as opposed to CSIRT duties being just one of their many functions. Although most organizations have some part-time CSIRT members, this can be challenging if the need to react to an incident competes with day-to-day job responsibilities.

It's important to make sure that team member priorities are clear in the event of an incident, both to the team members themselves, as well as to their managers and other colleagues.

It goes without saying that CSIRT team members should also consist of your best and brightest security professionals – often those with many years of experience who carry relevant certifications.

Threat management group

The threat management group is also typically chaired by the information security team, but consists of leaders from throughout the organization.

It should include as a minimum:

- ✓ Information security team leaders with responsibilities related to the incident response function
- ✓ Operations leaders responsible for critical functions of the business
- ✓ Technical leaders representing the major technology functions expected to be involved in incident response
- ✓ Legal representation to advise the team on compliance obligations related to security incidents
- ✓ Public relations staff to handle media inquiries, press releases and news conferences when applicable
- ✓ Human resources team members to advise on appropriate steps if disciplinary action against staff members results from the incident.

Some organizations will also choose to supplement both their CSIRT and threat management group with third-party consultants if needed during an incident.

Processes: Empowering the CSIRT to perform at its peak

Training the CSIRT

CSIRT team members should be seasoned IT professionals who come to the job with much of the expertise that they need. However, incident response related skills can always be developed, and they need to be kept fresh, particularly if they aren't being exercised constantly. It's important to provide CSIRT team members with access to opportunities for continuing education that are relevant to their area of expertise.

Additionally, it is important to assess CSIRT readiness through regularly scheduled exercises to provide constant feedback to the team regarding its responsiveness.

Measuring response times

The most mature organizations not only have a CSIRT in place, but also have meaningful operational metrics they can use to assess whether the CSIRT is able to respond to incidents effectively. The time and effort required to identify, respond to and resolve each incident are important components of the overall cost of the incident to the organization.

Therefore, without a quantifiable understanding of incident response, it is impossible to accurately measure the return on investment of any information security project.

Defining rules of engagement

It is critical for incident response teams to have defined rules of engagement. For example, is your CSIRT permitted to interact with malicious hosts for the purpose of intelligence gathering? And in the event of an incident, can the CSIRT autonomously decide to pull infected systems off the network? What if it's a production server?

These types of policies need to be clearly defined in advance so that unnecessary roadblocks do not get in the way of fast incident remediation. While building these policies, keep in mind that complex approval requirements can significantly delay incident re-

sponse and increase the overall cost of an incident to the business.

Communicating with others

The C-suite

While many security teams may not want to report bad news to the executive management team, sharing information can be extremely valuable for strengthening management support for incident response efforts. If the C-suite has no sense of its organization's security posture, then obtaining the right investments for incident response will be nearly impossible.

The public

One of the most significant negative consequences associated with security breaches is the impact they can have on the victim's reputation. In the event of a material exposure of customer data, it may be necessary for the organization to disclose facts about the breach to the general public. Having a pre-defined plan in place for exactly how and what to communicate is the key to success in this arena.

Industry peers

A thorough incident investigation should result in intelligence surrounding Indicators of Compromise (IoCs) for a specific attack. Putting this intelligence to work internally can help detect future attacks by the same adversary. Sharing it amongst industry peers can create tremendous value when it comes to our collective ability to fend off future attacks. Organizations not already doing so should assess ways that they can share threat intelligence back and forth with third parties to both improve their own incident response procedures and assist other security teams in fighting off the "bad guys."

Technology: Equipping the CSIRT with the right tools to get the job done

Effective incident response requires audit trails of the activity that occurred on the systems and networks that the attacker accessed. The specific tools needed within your organization will vary based on your resources and business needs, but you should consider

implementing:

1. Syslog collection with a SIEM
2. NetFlow collection
3. Collection of full packet captures.

These technologies provide incident responders with a record of activity that enables real-time threat detection and may also contain key pieces of evidence and indicators that can be used to detect future breaches.

SIEM

Security Information and Event Management (SIEM) systems are capable of collating logs from a wide variety of sources. They allow security professionals to analyze and correlate disparate information sources in order to identify and/or investigate security incidents.

However, a SIEM is only as good as the information feeding it. For that reason, organizations must also dedicate sufficient time to the log configuration of each monitored component. This ensures that, in the event of an incident, the necessary information will be stored in the SIEM's database and ready for analysis.

NetFlow

NetFlow is a family of standard protocols spoken by a wide variety of popular network equipment. It provides a record of each connection that occurs over a network, including the "to" and "from" addresses, port numbers and the amount of data transferred.

Because NetFlow is supported natively by so many different kinds of equipment, it provides an easy way to obtain an audit trail of activity throughout a network without having to deploy special sensors or probes. NetFlow records should be forwarded to a collector that is capable of retaining them for an extended period of time.

Packet capture

Analysis of packet payloads can be an important investigative tool. It can help identify malware command-and-control protocols or the

type of data that was stolen, as long as the content hasn't been encrypted by the attacker. Of course, storage of full packet captures can be expensive, but the value can outweigh the expense, particularly at key network egress points.

Each of these technologies has its place in an incident responder's toolset. Each creates an audit trail that provides different pieces of the puzzle of what was happening while the network was infected. One other incredibly important tool that every incident response team needs is backups.

Backups

Ultimately, effective incident response is about business continuity. You want to understand what happened, fix it, and get things back to business as usual as quickly as possible. Regular system and server backups are a critical part of this equation. They provide a way to rapidly roll back the environment to a state prior to the compromise, and often they can capture evidence of the attack as well.

Quick tips for a strong CSIRT

A properly equipped and trained incident response team can contain breaches more rapidly, reduce their impact on the organization, and apply its findings to protect the organization against future attacks. As a recap, it is recommended that organizations:

- Build an incident response team consisting of experienced, dedicated security professionals
- Create a multidisciplinary team, including the C-suite, Legal and Public Relations
- Train and assess the readiness of incident response team members on an ongoing basis
- Establish meaningful operational metrics to gauge the overall effectiveness of incident response
- Define clear rules of engagement for the CSIRT
- Consider sharing threat indicators with third parties to foster a more collaborative approach to threat defense
- Invest in technologies that support the collection and analysis of key information needed to support the incident response process.



Why privacy engineering is needed

by Michelle Dennedy, Jonathan Fox
and Thomas Finneran

The Information Age is constantly evolving. The current stage is about people, devices, and systems seamlessly making handshakes, connecting, processing information, and providing services based on personal information that are designed to improve the quality of life and are tailored to our needs.

This stage is the dawn of the Personal Information Service Economy and we call it the Intelligence Stage. It is driven by increased bandwidth, throughput, processing power, analytic skills, data-reading abilities, and the desire to provide value.

Some early examples of the computing in the Intelligence Stage are:

- Smart grid technologies recording and optimizing energy use in homes within communities
- Mapping apps that provide real-time traffic updates and suggest course corrections
- Connected appliances such as mini-bar refrigerators that automatically inventory themselves
- Augmented reality and gaming as a tool as well as recreation
- Localized shopping applications that give real-time pricing comparisons.

These applications take in user-provided information, observed information or behavior,

and output results that can be life improving, labor saving, and time efficient. These applications and the applications yet to be imagined will require new engineering roles and responsibilities – namely that of privacy engineering - and a greater and more granular understanding of privacy (or as it is known in the European Union, Data Protection).

Privacy defined

- Substantive privacy describes the right and ability of an individual to define and live their life in a self-determined fashion. Other forms of privacy - such as decisional, behavioral, physical, and data - all attempt to describe and define this basic human fact.
- Decisional privacy is really about being able to make decisions and choices without third party inspection or intrusion.
- Behavioral privacy is about being able to act as one wants, free from unwanted third-party intrusion or observation (assuming no harm to others is incurred or laws broken).

- Physical privacy is privacy about one's body or person. Modesty is another word for it.
- Data privacy is about the processing of personal information.

Data privacy may be defined as the authorized, fair, and legitimate processing of personal information.

Although this operational definition may seem deceptively simple, we can break it down into its components to start to see this definition as the beginnings of a pragmatic framework for not only defining data privacy, but also for beginning to build it from the following foundations:

Personal information: Any data that identifies an individual or from which identity or contact information of an individual can be derived (this may include such things as IP address or device ID that can be reasonably linked to a person).

Processing: Data is processed upon any action or inaction that can be performed in relation to that data or dataset. Processing personal information includes, but is not limited to, collection, storage, use, sharing, organization, display, recording, alignment, combination, disclosure by transmission, copying, consultation, erasure, destruction, and alteration of personally identifiable information and any data related to it.

Fair and legitimate: The processing of personal information is considered fair and legitimate when it is processed according to the notions of Fair Information Practice Principles (FIPPs), OECD Privacy Guidelines, or the Generally Accepted Privacy Principles (GAPP) such as notice, consent, transparency, purpose specification, limitation, openness, security, quality, onward transfer.

Authorized: This means with permission. The type of data, the nature of the processing, as well as local laws and regulations will determine the nature and level of permission that may be required. The four primary protocols for permission gathering are:

- Opt-out/Opt-in
- Implied consent
- Informed consent

- Express consent

The tension between privacy and technology

Throughout history, one can correlate innovation and the use of information technologies to pivotal moments in the history of privacy. In fact, there are many examples where technology either directly or indirectly impacts the sharing of personal details.

Take as an example the Gutenberg press and the invention of movable type. The development of the printing press and movable type not only directly led to the emergence of inexpensive and easily transportable books but also contributed to the development of the notion of personal space, privacy, and individual rights, as noted in Karmak's "History of Print" (http://karmak.org/archive/2002/08/history_of_print.html):

"[Print] encouraged the pursuit of personal privacy. Less expensive and more portable books lent themselves to solitary and silent reading. This orientation to privacy was part of an emphasis on individual rights and freedoms that print helped to develop."

Another example (also in the late 1800s) of innovation of information technology that resulted in a pivotal privacy moment was the invention of the camera—or more precisely, rolled film. In 1888, George Eastman invented film that could be put on a spool, preloaded in easy-to-handle cameras, and sold much like today's disposable cameras. The technical innovation of this new film and packaging allowed for cameras to become more portable (or mobile) and thus allowed more people access to becoming "Kodakers" or photographers. These technical advances widened the range of subject matter available to the photographers to include people who did not necessarily desire their behavior to be captured on film.

Two years later, prominently citing the example of photography as technology capable of intrusion upon individual space and publicity, Warren and Brandeis wrote an article that first articulated the right to privacy as a matter of U.S. jurisprudence.

In the late 1960s, there were many concerns that governments had access to massive stores of personal information in easily accessible formats. The U.S. government's use of databases in what was then the Department

of Health, Education, and Welfare, in particular, led to the first articulation of the Fair Information Practice Principles (FIPPs). The FIPPs are widely considered the foundation of most data privacy laws and regulations.

The intent of privacy engineering is to close the gap between privacy policy and the reality of systems or technologies or processes.

Enter the privacy engineer

We are at another pivotal privacy moment given the ongoing and ever accelerating pace of information technology innovation and consumerization. This acceleration is being driven by market demand—individuals who want new and different functionality from technology and uses of information—and market creation—enterprises and governments attempting to capitalize on new and expanded business models.

The time for privacy engineering as a necessary component to constructing systems, products, processes, and applications that involve personal information has arrived. In today's world, systems' products, processes, and applications that involve personal information must be thought of as personal information or privacy "ecosystems" and like any ecosystem, they must be treated in a certain way to not only exist, but also to grow and thrive.

Privacy engineering, as a discrete discipline or field of inquiry and innovation, may be defined as using engineering principles and processes to build controls and measures into processes, systems, components, and products that enable the authorized, fair, and legitimate processing of personal information.

Privacy engineering may also be applied to the creative innovation process to manage increasingly more complex data streams and datasets that describe individual humans. Privacy engineering can be considered the gathering and application of privacy requirements with the same primacy as other traditional feature or process requirements and then incorporating, prioritizing, and addressing them at

each stage of the development lifecycle, whether its for a process, project, product, system, application, or other.

The intent of privacy engineering is to close the gap between privacy policy and the reality of systems or technologies or processes. The greater the mismatch between the two, the greater the opportunity for needless inefficiencies, risk, or both.

The importance of privacy engineering

Privacy engineering in the Intelligence Stage is crucial because information provided by or gathered about individuals often determines:

- What we build
- How we build it
- How it works
- How our customers use it
- How well it protects our customer or other persons involved
- The risks it may pose to our business and to future markets.

Privacy engineering uses engineering principles and processes to build privacy controls and measures throughout system and data life-cycles (development, production, and retirement).

The privacy engineer recognizes privacy policies not as something that is linked to web-pages because of a regulatory need, but as meta-use case requirement documents for how personal information should be processed – and uses it as such. The FIPPs, or GAPP, or the OECD guidelines mentioned earlier become QA documents for validating the proper controls and measures have been implemented.

Privacy is important to people impacted by the systems; privacy protection encourages trustworthiness and other factors that people expect when working with an enterprise or with its systems. Privacy engineering will further assist in:

- Protection of customers and other people impacted by our systems and their data
- Improving trust by the people impacted by enterprises and their systems
- Developing secure and respectful computing that may encourage more data sharing and engagement
- Gathering better information that will help create better tools
- Greater innovation and opportunity in the marketplace.

Poor system design, poor policy requirement gathering, or poor communication (which are the hallmarks of design without privacy engineering techniques) may cause risk or harm to the developers of such systems, the owners of them, and the individuals described or impacted by the data, or all of the above. Further, the monetary, reputational, organizational, or even criminal risks or harms will only increase for those who fail to recognize a privacy engineering approach as systems become more complex and personal data more valued and/or valuable.

Privacy engineering is not merely a call for mindful engineering where personal information is involved. The call for privacy engineering use and study is a call for leadership, innovation, and even a good measure of courage to change the status quo for design and information management.

Once every system owner, designer, and user expects and understands privacy engineering principles, we expect that privacy engineering will become so integrated into standard innovation cycles that there will be no need for reference to a discrete practice. Rather, the principles of privacy engineering will be an obvious and necessary part of engineering of any kind when personal information is involved or potentially involved.

When privacy engineering becomes ubiquitous, individuals will not be treated as “inventory,” and data about them will be viewed as a special asset, important, sometimes profitable, and always one with a fundamental ethical value. When this happens, systems that use personal information will be designed, implemented, and decommissioned accordingly.

We propose that privacy engineers take responsibility for:

- Designing and constructing processes, products, and systems with privacy in mind that appropriately collect or use personal information
- Supporting the development, implementation, and measurement of privacy policies, standards, guidelines, and rules
- Analyzing software and hardware designs and implementation from a privacy and user experience perspective
- Supporting privacy audits
- Working with other stakeholders to ensure privacy requirements are met outside as well as inside the engineering space.

We propose that privacy engineers, in addition to better protecting and ensuring the proper use of personal information in the things they design, build, and implement, will provide the following benefits to individuals, as well as government and business enterprises:

- Protection for customers, users, or citizens
- A more objective basis for a trusted data platform
- A foundation to drive more thoughtful and higher-quality personal information services, sharing, and engagement

These benefits can lead to better and more information from users, which in turn help to build and inspire better user experiences, better applications, better services, better products, and greater innovation.

SECURITY AWARENESS FOR THE 21st CENTURY

Go beyond compliance and focus on changing behaviors.

Create your own program by choosing from 30 different training modules.

Meets requirements of the Data Protection Act and PCI DSS.

Training is mapped against the 20 Critical Control framework.

For more information visit us at www.securingthehuman.eu



www.securingthehuman.eu