European Cyber Security Perspectives 2017

kpn
National Cyber Security Centre
Ministry of Security and Justice
POLITIE
BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN
EUROPOL
EUROPEAN LAW ENFORCEMENT AGENCY
Deloitte.
IDQ
PHILIPS
accenture
High performance. Delivered.
Check Point
SOFTWARE TECHNOLOGIES LTD.
GSMA
TNO innovation for life
pwc
ZIMPERIUM
KASPERSKY


Menu
Usage Now
Dual Fuel
HIGH
132 gm
Co2kg
47 kg

Preface

Dear Reader,

Greetings and a warm welcome to our fourth issue of the European Cyber Security Perspectives Report!

We could not be more excited to have made it to this point. We have never had a more stellar collection of articles or a wider selection of partners to work with.

Our articles range from topics like DDoS, Ransomware, Quantum Key Distribution, Baseband issues, so read on! This year, in addition to our very popular sticker and puzzle sheets, we have also included a centrefold which is meant to be used as a poster for developers. We have further enriched the timeline that you see at the footer of the ECSP with a collection of tweets that we thought were insightful and fun.

When we set out to create a magazine that would promote the collection of different views regarding information security, we tried to encourage a diversity of opinions that could also communicate at various levels rather than the monolithic, statistical reports that we all sometimes read. What you will find in the pages of the ECSP report is a collection of inspired and instructive articles written by real security folks who work hard in the trenches, but who are not afraid to admit the struggles we sometimes face. We believe that with open and inclusive collaboration we have a chance to improve the security odds in our favour.

We are honoured to share the work of so many committed and thoughtful people, you rock!

We appreciate your support through the years and are so happy to have you as a reader again for this year's European Cyber Security Perspectives Report.

With warmest thanks,
The Editors @KPN CISO

P.S. Let us know what you think on Twitter with @ECSP17 or e-mail ciso-ecsp@kpn.com

Contents

January

5 Dutch Government embraces encryption, denounces backdoors.

6 Destructive Disakil malware linked to Ukraine power outages.

New attack against HTTPS, "Bicycle attack".

Quotes contributing partners

Jaya Baloo

CISO, KPN

'Our challenges were never greater nor were the threats to confidentiality, integrity, and availability never sharper than today, where weaknesses in information security lead to geopolitical instability. In a world where old vulnerabilities show up in new technologies, and hardware and software vendors are not held to account, our capability to prevent, detect, and respond is minimal. We need to gather our forces and refocus our splintered security landscape. We need to embrace disruptive security innovation and reclaim our right to our own data. Progress of technology should be measured by the degree to which security and privacy are ensured at inception. The time is now.'

Hans de Vries

Head of the Dutch National Cyber Security Centre (NCSC)

'Over the past years we have seen the growth of connectivity. Connectivity can be comforting: smart thermostats automatically controlling heating, smart watches watching over your health. At the same time, the risks of these devices are often underestimated. This is not limited to the internet of things within one's personal environment. Incidents in other countries show us cyberattacks can cause great impact, for example when they are used to bring down power grids or when personal IoT devices are used to perform DDoS attacks on websites. Cyber threats are coming of age, affecting individuals, organisations and society. Digital attacks stress the need to take action. I actively embrace and encourage joint efforts: both the public and private sectors need to work together on improving our resilience.'

Gert Ras

Head of department THTC & TBKK, Nationale Politie

'Law Enforcement is a great asset within the realm of cyber security. It is the instance with legal powers to hold perpetrators accountable for high tech crime, and to obtain data through investigations. In our aim to keep the Netherlands cyber-safe we are connected to successfully cooperate with many partners to bring these perpetrators to court, but moreover to impinge on their criminal business models.'

Rejo Zenger

Policy Officer, Bits of Freedom

'Meaningful security is way more than just the development of another unbreakable encryption cypher. It's about making technology accessible to all users that need it. It's about making it both transparent and verifiable at the same time. Despite having pretty good solutions available, the implementation is too often too poor. It's about users being integral part of security design and fixing the lack of usable interfaces.'

Steven Wilson

Head of EC3, Europol

'Europol is fully committed to supporting the enlargement of the No More Ransom project within the EU and internationally to respond to ransomware in an effective and concerted manner," says Steven Wilson, head of the European Cybercrime Centre. "Despite the increasing challenges, the initiative has demonstrated that a coordinated approach by EU law enforcement that includes all relevant partners can result in significant successes in fighting this type of crime, focusing on the important areas of prevention and awareness. We are very pleased to see how the online portal has improved since it was launched. All police forces are warmly encouraged to join the fight.'

Dave Klingens

Director Cyber Risk Services, Deloitte

'Cyber risk models for quantifying risk are beginning to gain broader acceptance.'

Bruno Huttner

ID Quantique & Chairman of the Quantum-Safe Security Working Group, organized by the Cloud Security Alliance

'In order to protect our cyber security infrastructure from the threat of the quantum computer, we have to plan the transition to quantum-safe security right now.'

Cyber criminals abuse the free Let's Encrypt certificate system to smuggle malware onto computers.

January 7 11

Firefox rejection of SHA-1 leads to other security vulnerabilities.

Trend Micro anti-virus software gave any website command line access to Windows PCs.

Maarten Bodlaender

General Manager Philips Security Technologies

'Automatic exploit generation. High-speed hacking. New words for many of us. While many IoT vendors are still busy fixing simple blunders like hard-coded passwords, DARPA showed that the next few generations of exploits are already on their way. While we often distinguish between simple and sophisticated attacks, it doesn't really matter: once a sophisticated exploit has been automated and scripted, it works for everyone. Until the industry learns how to limit (the impact of) exploits, large-scale botnets like Mirai will continue to find a fertile ground in the Internet of Things. New building blocks, new security technologies are needed to build systems that withstand an increasingly sophisticated array of cyber attacks.'

Michael Teichmann

EALA Resources lead, Accenture

'The insider threat is as important to understand and mitigate as the external, given the deep knowledge an insider may have and the fact that an external actor may have compromised an actual user account, impersonating the 'insider' for malicious purposes.'

Gabi Reish

VP of Product Management at Check Point

'We are more connected than ever before, and innovations in cloud services, mobility and IoT are rapidly changing the way that we deploy and use technology. But we are also seeing dramatic increases in threats and attacks by criminals who are also trying to exploit these technologies. Cyber security is the business enabler that allows organizations to take full advantage of digital innovations and drive their business, by keeping them one step ahead of cyber threats and preventing attacks before they happen. Check Point is committed to staying focused on its customers' needs, and developing solutions that redefine the security landscape today and in the future.'

James Moran

Head of Security GSMA

'Like most industry sectors we now consider internal compromise to be one of the foremost threats facing us and we are striving to increase cognisance across our membership.'

Annemarie Zielstra

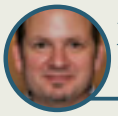
Director Cyber Security & Resilience, TNO

'People should become the strongest link when it comes to cyber security. Proper cyber behaviour should be in the DNA of any organisation. Awareness, education and culture play a role in this, but further applied research needs to show how the human factor can truly evolve towards the strongest force in combating cyber risk. TNO has the multidisciplinary knowledge to help organisations develop such DNA. To strengthen the human factor and enrich it with cutting-edge technologies that meet the specific needs of an organisation.'

Gerwin Naber

Partner Forensics, PWC

'Today, organisations want to hear about innovative new approaches to cyber security and privacy—not the same rehash of fear, uncertainty and doubt (FUD). They want to move beyond FUD and think more broadly about cyber security and privacy as both protectors and enablers of the business, hird party partners and customers.'



John Michelsen,

Chief Product Officer, Zimperium

'You are most vulnerable to cyberattacks on your mobile devices.'

Martijn van Lom

General Manager, Kaspersky Lab Benelux

'There is an alarming change in the nature of cyber attacks: from computer systems to politics. This affects people's daily lives significantly. Besides losing money, people are losing something that is even more precious: trust. Trust in things connected to the Internet, in having privacy, in the government protecting you and in information are a few examples. Especially trust in information is currently under pressure. With targeted misinformation - through often trustworthy channels – cyberattacks can influence and manipulate people and their thoughts, opinions and actions. It's becoming more and more challenging for people to understand what is true and what is fake with sometimes major consequences on national, regional and even global levels.

Another issue is that while cybercriminals are working together globally, nations are often not able to do the same because of politics. This allows cyber criminals to attack countries and get away with it. If we want to successfully fight cyber crime, private and public parties need to fight together, not only nationally but also internationally.'

January

12 Turkish carder scores record 332-year jail term.

15 SSH backdoors discovered in Fortinet firewalls.

18 Apple Gatekeeper vulnerable for security bypasses.

20 FDA Issues Guidelines on Medical Device Cyber security.

20 European Human Rights Court rules mass surveillance illegal.

Cyber threats coming of age

Wouter Oosterbaan, NCSC

Professional criminals and state actors are an ever greater danger to digital security in the Netherlands. Campaigns by professional criminals with the objective of monetary gain is a growing problem. This group has evolved into sophisticated actors and carry out long-lasting and high-quality operations. Foreign intelligence services on the one hand focus on economic espionage: companies in top sectors are being attacked, putting pressure on the competitive position of the Netherlands. On the other hand, political espionage in the digital domain is second to none: the Dutch government suffers regular digital attacks.

That is apparent from the Cyber Security Assessment Netherlands 2016 (CSAN 2016), published in September 2016 by the National Cyber Security Centre (NCSC). The CSAN is drawn up in close collaboration with a large number of partners, both from private and public sectors. It offers insight into the interests, threats and resilience, as well as the related developments, in the field of cyber security.

Professional criminals have evolved into sophisticated actors and carry out long-lasting and high-quality operations

Campaigns by professional criminals are becoming more and more sophisticated. In the past, the digital attacks and associated campaigns by criminals were often of short duration and focused on earning quick money by targeting a great number of parties. Criminals in the past year have, implemented a number of campaigns where huge investments have been made and which show a high degree of organisation. In addition, spear phishing by criminals is becoming ever more sophisticated and therefore more credible. Spear phishing is thus becoming increasingly difficult to fight with security awareness. Prolonged campaigns with large investments and advanced spear phishing were, in the past, the terrain of state actors.

Digital espionage by foreign intelligence services puts the competitiveness of the Netherlands under pressure and undermines political and governmental authority

The past year has seen many digital attacks on companies in the Netherlands in which the motive was economic espionage. Espionage for economic purposes is harmful to the position of the Netherlands. These attacks focused on acquiring technology that sometimes still has to prove its value. Two thirds of the affected companies were unaware of these attacks. Next to economic espionage, foreign intelligence services actively collect digital political information in the Netherlands. The Dutch government suffers regular digital attacks. Political espionage undermines political and governmental authority and is therefore a threat to the democratic legal order. Intelligence agencies find that state actors increasingly use digital tools to achieve their strategic objectives, to resolve (international) conflicts and to support, in some cases, an armed struggle.

Ransomware is commonplace and has become even more advanced

The use of ransomware by criminals in the past year has become common. Infections are everyday occurrences

Linux bug imperils tens of millions of PCs, servers, and Android phones.

January

20

Aeroplane parts manufacturer FACC Operations loses 54 million dollar to cyber fraud.

22

Attackers compromise over 3,500 public servers in possible reconnaissance drive for future attacks.

and affect the entire society. Whereas in the past the same price had to be paid per infection, the price is now determined on the basis of the type of affected organisation. In addition, the malware itself is more sophisticated: in addition to files on the local disk, nowadays databases, backups and files on network drives are encrypted. Various sectors indicate that the mode of infection with ransomware is changing. Previously, these were only random infections. Now, several vital sectors indicate that they are regularly confronted with person or organisation-targeted phishing e-mails by which attackers try to install ransomware. There are indications that criminals more often use ransomware to target organisations. Sometimes, they use an adjusted (higher) ransom demand for this and they focus on vulnerable targets where continuity is important, such as hospitals and care facilities.

Advertising networks have not yet shown the ability to cope with malvertising

The distribution of malware via ads on major websites is a problem. Advertising networks have not yet been able to find solutions to this problem. Malvertising through advertising networks remains an effective method for disseminating malware using exploit kits. In the past period, this also affected popular Dutch websites. The wide range of advertising networks provides, along with the large number of systems from which the latest updates are missing, a large attack surface. Operators of these websites and advertising networks themselves do not have full control over the ads. This makes it possible for malware to be spread. Complete ad blocking in the browser affects the business model of website owners. To protect users against malvertising without blocking all ads, fundamental changes are needed in the way these networks work.

Table 1 **Threat matrix**

	Targets		
Source of the threat	**Governments**	**Private organisations**	**Citizens**
Professional criminals	Theft and publication or selling of information	Theft and publication or selling of information	Theft and publication or selling of information
	Manipulation of information	Manipulation of information	Manipulation of information
	Disruption of IT	Disruption of IT	Disruption of IT
	IT takeover	IT takeover	IT takeover
State actors	Digital espionage	Digital espionage	Digital espionage
	Offensive cyber capabilities	Offensive cyber capabilities	
Terrorists	Disruption/takeover of IT	Disruption/takeover of IT	
Cyber vandals and script kiddies	Theft of information	Theft of information	Theft of information ↘
	Disruption of IT ↗	Disruption of IT ↗	
Hacktivists	Theft and publication of obtained information ↗	Theft and publication of obtained information ↗	
	Defacement	Defacement	
	Disruption of IT	Disruption of IT	
	IT takeover	IT takeover	
Internal actors	Theft and publication or selling of information ↘	Theft and publication or selling of information ↘	
	Disruption of IT	Disruption of IT	
Cyber researchers	Receiving and publishing information	Receiving and publishing information	
Private organisations		Information theft (industrial espionage)	Commercial use/abuse or 'resale' of information
No actor	IT failure	IT failure	IT failure

↘ ↗ *Change with respect to CSAN 2015.*

No new trends or phenomena are recognised that pose a threat. *OR* *(sufficient) measures are available to remove the threat.* *OR* *No appreciable manifestations of the threat occurred during the reporting period.*	*New trends and phenomena are observed that pose a threat.* *OR* *(limited) measures are available to remove the threat.* *OR* *Incidents have occurred outside the Netherlands and there have been several minor incidents in the Netherlands.*	*There are clear developments which make the threat expedient.* *OR* *Measures have a limited effect, so the threat remains substantial.* *OR* *Incidents have occurred in the Netherlands.*

SafeMail @ KPN

Getting a grip on some of the oldest internet protocols

Michel Zoetebier, Eva Kelder & Ruud Leurs, KPN

With ongoing phishing attacks, CEO/CFO fraud and fake invoices loaded with ransomware, e-mail remains a widely-used entry point for criminals.

If we do not take e-mail anti-spoofing measures, we invite attackers to simply send e-mail on behalf of legitimate company domains. The lack of these measures also removes the foundation to build a proper awareness program. Customers, employees and business relations are not able to visibly recognize a legitimate e-mail and are unable to distinguish phishing attempts from real corporate communications. As a result, trust in the official e-mail communications of a company deteriorates. In December 2016 it was announced[1] that the name of KPN is abused the most in fake emails.

Stop!

The decrease of trust in legitimate e-mail communication has to stop. By using open standards, KPN CISO has been given the chance to take back control of the usage of KPN's domains and to regain the trust in KPN's e-mail communication. The goal of this project (called SafeMail) is to make it visibly recognisable that a received e-mail is a legitimate message and to prohibit the rest of the internet to (ab)use KPN's domains.

Standards

To obtain absolute control of the domain being used in e-mail communications, and to implement an anti-spoofing mechanism, KPN has chosen to implement the standards: SPF[2], DKIM[3], DMARC[4] and S/MIME[5].

More visibility: DMARC RUA

For more visibility on the use of a domain in e-mail communications, it is not needed to have SPF and/or DKIM implemented. Based on DMARC alone a "none" policy can be published in DNS, including a mailbox to obtain so called Aggregate Data (RUA) reports from other networks. The DMARC "none" policy tells the receiving e-mail server not to reject any message in case the SPF and/or DKIM check fails. RUA reports are sent when an e-mail server receives an e-mail message containing the domain for which the DMARC records are published in DNS. These reports include the IP address that was used for sending out the e-mail. This will create an overview of IP addresses using the domain in e-mail communications.

When tagging the IP addresses of legitimate e-mail servers for a domain as valid (green) and all other

(1) www.emerce.nl/nieuws/naam-kpn-meest-misbruikt-nepmails

(2) SPF: Sender Policy Framework, an email anti-forgery system

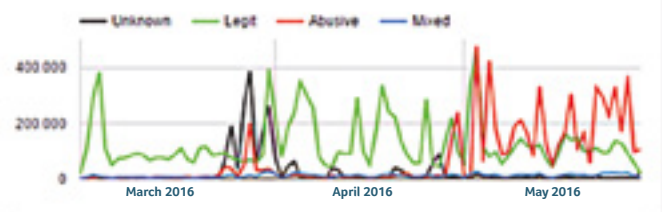
(3) DKIM: DomainKeys Identified Mail (DKIM) is an email authentication method designed to detect email spoofing.

(4) DMARC: Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email-validation system designed to detect and prevent email spoofing.

(5) S/MIME: S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data.

IP space as invalid (red) and plot the IP addresses onto a map, it will look like:

A graph based on the amount of e-mail received in time for a specific domain can also be created:



"Mixed" and "Unknown" data means hat, purely based on the RUA reporting, a message could not be marked as Legit/Abusive. This visualisation underlines the issue and the way the internet looks at the domain e-mail usage. Why are others using your domain? Mostly, because it's technically possible.

SPF

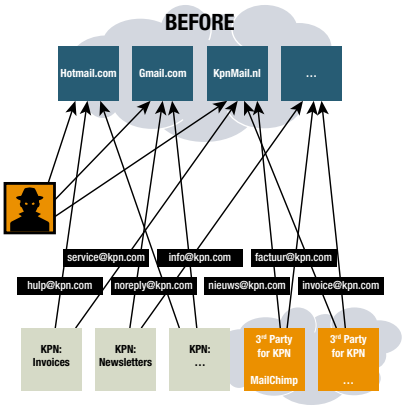
SPF is a good basis for DMARC. Its use without DMARC is seen in a lot of domains. Even though publishing the outbound SMTP servers for legitimate e-mails in a SPF record in DNS helps in the filtering and reputation with receiving e-mail servers, purely rejecting/accepting e-mail based on SPF records will lead to false positives. Because SPF is used widely on the internet many incorrect SPF records exist. Spammers and phishers have also been setting up domains with proper SPF records to circumnavigate filters for a long time.

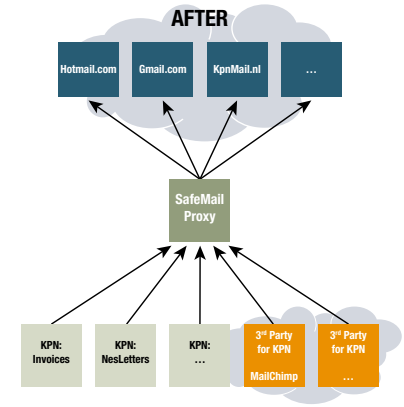
A common way to publish all legitimate e-mail servers in an SPF record is to include the IP addresses of external parties. This way little effort is needed to combine all e-mail communications in one policy. The SafeMail team received many requests to include external IP addresses in KPN's SPF record. In a company with the scale of KPN, this would result in an extremely big record. More importantly, to what extent is a company able and should it be willing to extend its trust towards external IP addresses? People can make mistakes, servers can be compromised and the simple process of keeping the list of IP addresses up to date is often forgotten.

To make sure none of these "mistakes" will lead to non-deliverability of important e-mail messages, and to prohibit blacklisting of the SafeMail SMTP servers, only the IP addresses of the SafeMail outbound SMTP servers will be included in the SPF record of KPN. This record will be the basis for a DMARC policy that will prohibit the rest of the internet to (ab)use the corporate domains of KPN.

Now what?

Instead of a big messy SPF setup, KPN has created one central e-mail platform that will proxy all e-mail communication from **all** internal **and** external applications. By doing this, only the SafeMail outbound SMTP servers should be allowed to send e-mail on behalf of KPN's domains. When you visualise the before and after situation it looks like this:





Technically this is not hard to implement, but a critical ingredient for this recipe is a complete overview of **all** internal and external applications and third party suppliers that send out e-mail using the domain you want to build the policy for.

American hamburger chain giant Wendy's hacked.

HSBC banking services offline due to DDoS attack.

The real challenge

Constructing this overview was done based on a three-way strategy:

- Internal communication campaign asking all to report e-mail communications
- Collecting all current e-mail relay server log files into one database
- Logging the internal network on port 25 to obtain sending IP addresses

Obviously, this will lead to a mismatch in what is known and what is actually seen on the network. Besides the recurring "who **is** the owner or administrator of this server?" question that will fly around for some time, the challenge is to create a best effort based overview of all e-mail sending applications and 3rd parties. Doing this also helps with testing and improving the accuracy of the CMDB.

Another outcome of this inventory of e-mail addresses is the realisation that the use of e-mail addresses has grown astonishingly. Should there really be hundreds of different no-reply addresses? Why are invoices being sent from dozens of e-mail addresses? Based on this discovered information, the rationalisations of e-mail addresses has been included in the project and the use of generic e-mail addresses has been added to the companies' security policy. Also, for the implementation of S/MIME a reduced set of e-mail addresses comes in handy to minimize the amount of certificates needed.

The external challenge

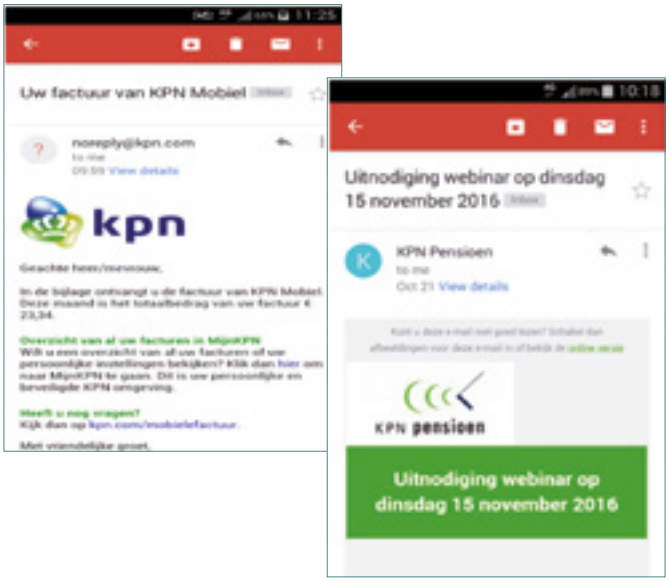
External parties need to be approached in a completely different way. KPN has outsourced most e-mail sending activities to specialised external parties. These parties have frequently implemented SPF, DKIM and sometimes DMARC. Companies outsource their e-mail sending activities to these specialized parties because this adds value in e-mail deliverability and reliability.

Normally such parties ask companies to include their IP addresses in the SPF record, as mentioned earlier. KPN now asks them to stop sending the e-mail directly, and to deliver the e-mail message to the SafeMail proxy of KPN. Applications that compose the e-mail messages, like invoices and customer satisfaction surveys, are often integrated to local SMTP platforms. Technical changes are needed in these environments to deliver the e-mails to the SafeMail proxy. Changing the way of sending out e-mails by these parties needs to be a joint effort to ensure the e-mail deliverability.

DKIM

While DKIM tells other servers a message originated from the announced server by signing the message with a private key, end users normally don't look at the headers of e-mail messages. Fortunately, the top mail providers are using DKIM to check if the messages originated from the announced domain and show this to their users. In apps, non-DKIM-signed e-mails are shown with a question mark. Online e-mail platform GUI's display the text "the origin of this e-mail message cannot be confirmed and might be harmful". When messages are DKIM signed, the question mark changes into a colored icon containing the first letter of the domain. The difference between non-signed and DKIM-signed messages are visualised in these screenshots:

S/MIME



By enclosing a S/MIME certificate with the e-mail, the sending server ensures the body of the e-mail has remained unchanged until received by the end user. This certificate also triggers most e-mail clients and online e-mail services to show a colored security symbol, which is visualised the same way HTTPS is for internet websites. When companies start using this in a consistent and transparent way, it creates a strong basis for e-mail security awareness programs.

Conclusion

Rolling out these standards can be a tough challenge, and has many dependencies. For the strongest and most effective implementation of this security design, many internal and external parties are required to actively change the way they are handling KPN e-mails, like checking on SPF, DKIM and DMARC policies before delivering e-mails to the end users. Regionally and/or nationally deploying these standards on both outbound and inbound e-mail communications improves e-mail security drastically and is definitiely worth the lengthy process of implementation.
However, attackers are already acting on the situation when networks will have implemented these e-mail standards. By registering look-a-like domains, hacking known legitimate websites and using the e-mail security standards as a weapon to avoid filtering, the cat and mouse game never ends...

Ransomware as a Threat

Steven Wilson, Europol

Ransomware is a type of malware that locks the victims' computer or encrypts their data, demanding them to pay a ransom in order to regain control over the affected device or files. Ransomware is often spread through malicious spam emails, which contain attachments or links to websites which then download the ransomware. Another way in which ransomware is spread is through compromised or hacked webpages, which contain scripts to download the ransomware on to the victim's device.

After ransomware has been downloaded and executed, victims find their personal files have been encrypted and they cannot run particular software, or their screen has been locked. Alongside this, a message from the malicious actor is displayed, informing the victim that their device has been locked and/or their files have been encrypted, and they must pay the attacker a particular amount of money, often in bitcoin, in order to have control restored.

The Internet Organised Crime Threat Assessment (IOCTA) 2016, the flagship strategic publication of the Europol's European Cybercrime Centre (EC3), identifies ransomware as a significant cyber threat: almost two-thirds of law enforcement in EU Member States are conducting investigations into this form of malware attack, and the number of victims is increasing. According to Kaspersky Lab, the number of users attacked by crypto-ransomware rose by 5.5 times, from 131,000 in 2014-15 to 718,000 in 2015-16. While the target is often individual users' devices, corporate and even government networks are affected as well.

The sale of variants of ransomware within criminal communities (Ransomware-as-a-Service) is also a significant issue, as individuals and groups have access to instantly distributable ransomware. After an encryption ransomware infected a substantial number of computer systems, German law enforcement began investigating the online network it originated from, named 'Avalanche.' This platform had been used by cybercriminals since 2009 to conduct malware, phishing and spam activities: more than 1 million e-mails with damaging attachments or links were being sent every week to unsuspecting victims. On 30 November 2016, after more than four years of investigation, the Public Prosecutor's Office Verden and the Lüneburg Police (Germany), in close cooperation with Europol, Eurojust, US agencies and global partners, dismantled this platform.

NO MORE RANSOM Initiative

On 25 July 2016, Europol, the Dutch National Police, Intel Security, and Kaspersky Lab joined forces to launch an initiative called No More Ransom, a new step in the cooperation between law enforcement and the private sector to fight ransomware together. The non-commercial initiative established an online portal – www.nomoreransom.org – to inform the public about the dangers of ransomware, how it works and how to protect themselves.

In order to better assist victims from all over the world, the online portal is available not only in English, but also in Dutch, French, Italian, Portuguese and Russian. Translations into yet more languages are currently

Only during the first two months, more than 2,500 visitors successfully managed to decrypt their devices without having to pay the criminals, using the main decryption tools on the platform.

ongoing, and their implementation will follow in the coming months.

Alongside prevention advice and the option to report a crime which is forwarded to relevant authorities, the portal contains more than 160,000 keys, with over twenty five decryption tools listed on the website. The initiative is always in the process of welcoming new public and private sector entities in an effort to step up the fight against this significant threat, with additional decryption tools being developed and made available to victims. Due to the constant evolution of ransomware, decryption tools must be developed regularly alongside the prevalence of new ransomware families.

Only during the first two months, more than 2,500 visitors successfully managed to decrypt their devices without having to pay the criminals, using the main decryption tools on the platform. This has deprived cyber criminals of an estimated EUR 1.35 million in ransom payments, an amount that keeps growing on a monthly basis. EC3 recommends that victims of ransomware do not pay the ransom. By doing so, they will be financing other forms of criminality, and there is no guarantee that victims will regain access to their files and computer.

The Future of Ransomware

A number of international threat intelligence and research organisations have identified the rapid development of ransomware campaigns, and the increasing targeting of public and private industry in more sophisticated means, as opposed to broad campaigns targeting unsuspecting individuals. It has been predicted that, despite the volume and effectiveness of ransomware decreasing, the number of successful attacks on Internet of Things (IOT) devices will increase greatly. This is particularly concerning for the healthcare industry, as hospitals have been frequently targeted by ransomware attacks such as Locky and Samsam, the latter being delivered through exploiting vulnerabilities in an organisation's networks and servers.

The recent developments in the sophistication of cyber threats including ransomware show that, whilst No More Ransom has undoubtedly been a success, prevention and victim support campaigns such as this must continue and develop in line with the tools used by cybercriminals. This can only be done with the continued cooperation and collaboration with private sector and industry.

Kaspersky Lab cracks digital walls of a Moscow hospital and finds an array of open doors on the network and weaknesses in medical devices and crucial applications.

February 9 10

Vulnerabilities identified in smart thermostats made by Trane allows malicious hackers to gain complete control of the devices.

Google warns Gmail users about unencrypted messages.

A game well played

Peter Zinn, Nationale Politie

The cyber security world sometimes seems to resemble a chess game. The red team makes bold moves and attacks wherever it can. The blue team plays slowly, carefully, and defensive. Red often wins.

Björn and Gijs

This particular game went a bit differently. It started in Sweden when a CISO, let's call him Björn, got hit with the Coinvault ransomware. Infected but by no means helpless, he followed the traces of the malware and identified a Dutch C2 (Command & Control) server it was connecting to. Good move. He then contacted the completely unaware owner of the server, let's call him Gijs, who traced the malware on his server and was able to extract the decryption key Björn needed. Then Gijs contacted the police. Another good move.

NHTCU

Gijs simply called the general police number. The days where you call the police for phishing and get sent to the water police are long gone - Gijs was directly connected to the Dutch National High Tech Crime Unit (NHTCU). Within an hour we started a preliminary investigation of the C2 database. It was a client database of sorts, with information on all the computers infected by the ransomware. Nice catch.

Strategy

To understand what happened next let's have a closer look at the strategy of the Dutch NHTCU.
In our investigations we try to follow these four steps - but not necessarily all of them:

1. Victim support
2. Damage mitigation
3. Disruption of the criminal business model
4. Attribution and bringing to justice

These steps show that police investigations are not solely aimed at attribution. Attribution is hard, costly, and not always most effective. Since law enforcement often has unique data and capabilities they can play a pivotal role in the first three steps. Which also fits in nicely with the police task of providing help to those in need.

Never alone

None of the four steps can be performed alone. Attribution in cybercrime almost always needs international police cooperation. For the first three steps public-private partnerships are a must. In this case, with the victim database in our hands, we wanted to create an opportunity for the victims to obtain the decryption key - for free. We reached out to our partners and found Kaspersky Lab willing to build a decryption website for Coinvault victims. Good move, especially since that meant they needed to work under the time pressure of a judicial investigation.

ENISA has weighed into the cryptography debate, warning that crimping cryptography will "create vulnerabilities that can in turn be used by criminals and terrorists".

Flaws in wireless mice and keyboards let hackers type on PC's.

February 14 16 23 24

PBX phone system hacking yields criminals $50 million over four years.

U.S. Federal Trade Commission and Asus settle router security case.

Sharing data

The data we needed to provide Kaspersky with, in order to build the cleaning tool for the victims, did not contain any personally identifiable information, which made sharing and caring a lot easier. While they were working, we found another Coinvault C2 server. We secured it (victim support, attribution) and took it offline (damage mitigation, disruption). Extra input for the Kaspersky tool.

Have your cake and eat it

Some people argue that victim support, damage mitigation and disruption harm your chances of successful attribution. After all, you are warning the suspects. But as far as we have seen, it might actually increase the chances of capture. In this case, both Kaspersky and us independently traced the suspects, in completely different fashions. Even though the criminals should have been warned by their databases being taken offline, they simply continued their actions. Game over.

So, with an unusual amount of blue players doing the right thing, we won. But hat is just one game. There is a match to worry about. There are it seems a gazillion different types of ransomware out there and every single day people and companies get hit. Would not it be possible to scale-up the cooperation with Kaspersky? With more law enforcement and more AV on board, more victims can be helped.

That is how the No More Ransom initiative was born. Good move.

March

1 Dutch company Vaulteq introduces physical password manager.

1 Apple wins ruling in New York iPhone hacking order.

7 The Cloud Security Alliance (CSA) released an important new research report about cloud computing threats.

7 French government wants legislation to force companies to cooperate with decryption or get fined.

Security and Safety, Plain and Simple

Rejo Zenger, Bits of Freedom

Even though there were a record 32 million departures of large aircraft in 2013, there were "only" 137 fatalities due to accidents. In the ten-year period before, there were 0.6 fatal accidents per one million flights. One of the reasons for this surprisingly low number of fatal incidents is the ability of the aviation industry to learn from mistakes. We should start doing the same with incidents in the digital world.

Whenever a plane has crashed, the first priority is to provide assistance to any survivors. Right after that, all efforts are put into the recovery of the two black boxes – which are often orange to increase the chance of finding them. One of the boxes records all the instructions sent to the electronic systems of the aircraft. The other records conversations in the cockpit, radio communications between the cockpit crew and others, as well as ambient sounds. These recorders are designed to capture all important data and can withstand great external impact. Black boxes are key tools in determining what has caused the crash.

The purpose of these investigations is plain and simple: finding out what we can do to prevent a similar accident from happening. Did the pilot misread the altitude on the cockpit panel? Was there some mechanical failure that caused the suspension to break upon touchdown? Was the collision of two planes caused by confusing taxiing procedures? In other words: Is there some mechanical part that needs preventive replacement in planes of the same make and model? Do we need to redesign the construction of the landing gear? Or do we need to revise the procedures when taxiing from the runway to the gate? These recommendations are then systematically shared in the industry, making traveling by plane safer for all of us.

Surprisingly, none of that happens when there is an incident in our digital environment. Of course, incidents are being investigated. However, those investigations are commissioned or done by the affected organisation and aim to limit the damage to its own interests – especially the damage to the image of the organisation. The results are kept secret or shared haphazardly with the most demanding customers. At best, the results are used to improve the internal monitoring system. Of course, this is somewhat exaggerated. Fact is: as a community, and as a society at large, we miss a great opportunity to learn and to improve the security of our digital infrastructure.

In the Netherlands, just like everywhere else, many agencies and institutions have a role to play in the aftermath of a plane crash. On the trail of the emergency services you'll see the public prosecutor, salvage businesses, insurance companies and many other organisations. They clean the site, chase after those who are responsible to try and get compensation and they prosecute the guilty. Perhaps the most important work is done by the Dutch Safety Board (DSB). They document every known detail that has led up to the crash and make recommendations for preventing a similar accident.

> The easiest way to improve the security of key IT systems for our society, is to start learning from our mistakes.

Accidents in the transportation sector have been examined on a fairly structured basis since the early 20th century, albeit never by a fully independent body. This only changed at the end of the century, together with the most pivotal improvement: blame was explicitly excluded from the investigation process in order to maximise the effectiveness. The DSB was established in early 2005 (after the fireworks disaster in Enschede and a devastating fire in a bar in Volendam). It is allowed to initiate investigations into accidents in the various transport sectors, as well as in the fields of defence, industry and commerce, health, nature and environment, crisis and emergency.

Strangely enough, the DSB focuses on situations where people are dependent on others for their safety, but doesn't investigate incidents in the digital domain - even when vulnerabilities in our industry can have an immense impact on the safety of large groups of people. And because of the architecture of these systems, people can't defend themselves against that impact.

These systems are entrusted with the data about millions of people. This can be sensitive data where people rely on the protective measures of companies and governments. It is not just the data users more or less knowingly share, the same goes for the data that is generated by all the devices in our homes. Soon everyone will have dozens of connected devices in their home, continuously sharing our private lives with the outside world. Vulnerabilities in those systems makes that sensitive data s accessible to criminals. Vulnerable IT systems lead to vulnerable societies.

We have become highly dependent on the availability of our IT systems. As a result, incidents may affect the supply chain to supermarkets, the correct functioning of our cars, access to emergency services, financial transactions or the navigation of planes. If any of those systems is prevented from operating for more than a couple of days, or maybe even just a few hours, it could derail our society considerably. When these kind of attacks cannot be contained, it will undermine the trust of citizens and may trigger societal unrest.

Given our reliance on those systems and the immense impact a disturbance of these systems may have, we need to do everything within our reach to eradicate vulnerabilities. We need to make sure that the software created is based on solid security practices and is audited frequently. We need to make sure that closed software developers are liable for the products they put out on the market. We need to make sure that the government doesn't introduce any new vulnerabilities in the form of backdoors. We need to make sure that all vulnerabilities we come across, are swiftly reported to those who are accountable and responsibly disclosed to the general public as soon as possible.

The easiest way to improve the security of key IT systems for our society, is to start learning from our mistakes. It would be fairly stupid to, after handling an incident, make the same mistake that led to that incident over and over again. The only way to prevent this from happening is by investigating security incidents transparently and thoroughly and create recommendations for preventive measures. Therefore, I propose the establishment of a new organisation with the sole purpose of investigating security incidents in the digital realm in order to prevent similar incidents from reoccurring. In other words, a cyber-incarnation of the Dutch Safety Board.
There are a number of vitally important requirements for such an investigative body. First and foremost, it needs to be fully independent. If it's not independent,

March

11 The discovery of a backdoor in a new EDA2-based ransomware allows 700 infected computers to be decrypted without paying.

14 Advertisements on msn.com and bbc.com are spreading ransomware.

16 Researchers find iOS-malware in the official Apple App Store that uses previously unknown ways to infect iPhones and iPads.

it won't be trusted. Without the trust, investigations will be obstructed and the reports not taken seriously. As the primary objective is to learn from mistakes, an environment of trust is necessary.

Secondly, these investigations may not be part of an investigation into guilt or liability. That should be explicitly ruled out. Only when investigators have full access to all relevant data, they will be able to make a factual, accurate and explanatory analysis. If the owner of the system, that has caused or discovered an incident, can't be sure that the information he shares is not used against him, he will be reluctant to cooperate. Information handed over to the investigative body can't be shared with insurance companies or law enforcement. If there is a need from law enforcement or others, those institutions should seek access to that information based on their own powers.

Because we need to learn from these incidents, this new organisation needs to be transparent and should extensively publish its findings. The reports should detail all the facts that led up to the incident, including the impact of the security breach. It needs to present readily applicable and relevant recommendations to enable others to prevent similar incidents. It should also provide suggestions for detecting early warnings and how to reduce the impact in case something goes wrong. Of course, this may mean that classified business information becomes public. The risk of disclosure can be decreased by reporting just facts in a timely manner. In any case the public interest should outweigh the interests of the individual company or government institution.

That does not mean the government has no role to play whatsoever. The opposite is true: the government needs to fund such an organisation as well as create the legal environment in which it can operate. When investigating security incidents in the digital realm, the investigators will need to have access to the systems in which a vulnerability has been abused. That requires investigatory powers to obtain access to documents and systems that are otherwise out of reach of an independent and non-law enforcement organisation. It needs to have the power to make copies of data carriers, audits and everything else that it deems relevant to the investigation. All of this requires a new bill that needs to be proposed and approved by the parliament.

The organisation should consist of a team of experts. While many of the incidents will have a root cause in a non-technical area, technical expertise will be required for a thorough examination in many other investigations. The organisation needs a number of forensic and security experts for all kinds of digital systems. Without losing its independence, the organisation may exchange experience and knowledge with experts from CSIRTs.

Finally, there will be way more incidents than any organisation is able to investigate. With the right set of priorities, the organisation should be able to make a selection that allows for a thorough investigation of a limited number of incidents while maximising the effectiveness of the outcomes. Without a doubt, the organisation should investigate high impact incidents in systems that are vitally important to our society. At the same time it should look into the low hanging fruit: incidents with small impact, hitting large groups of people. The latter could be done, for example, based on the notifications of data breaches that are made to the Dutch DPA. The organisation could investigate every 50th incident and publish a yearly summary of quick wins.

One unanswered question remains: What is the digital infrastructure equivalent of the black box?

March

22 When an external party offered a solution to decrypt the iPhone of one of the San Bernardino criminals, the FBI dropped their charges against Apple.

28 Kentucky Hospital Declares 'Internal State of Emergency' After Ransomware Infection.

PETYA Crypto-ransomware Overwrites MBR to Lock Users Out of Their Computers.

FBI Breaks into Terrorist's Encrypted iPhone.

cyber security is not a state that you can achieve, it's a journey. It is actually a lot like evolution: flexibility and adaptability are essential in order to survive.

Adapt or become extinct!
Cybersecurity requires flexibility to survive

Martijn van Lom, Kaspersky Lab Benelux

"It is not the strongest of the species that survives but the most adaptable to change", is a profound saying credited to Charles Darwin. While he didn't literally state it that way, his famous work 'On the origin of species' does shed light on the need to adapt in order to survive. The theory of evolution shows that the adaptation to changing circumstances is what gives a species better chances for survival than its competitors.

Darwinism

The same applies to cyber security. The current landscape of digital threats is quite different from that of just a few years ago. True, some cyber risks are old, well-known and seemingly survivable. Some of those older cyber risks still hurt and cause damage. In addition to those older risks, there are new and changing digital dangers on the horizon: the so-called 'evolving threats'.

Not the strong, not the smart and not even the secure are guaranteed to urvive, at least not in the long run. Those that are strong now probably have a weakness that will be exploited later. Those that are smart now can be foolish with new developments. Those that are secure now may just think that they are. It's a well-known saying in IT security that: "It is not a matter of *whether* you get hacked but *when*".

Assume the worst

A modern evolution of that saying is that you are probably already hacked, but you just don't know it yet. So it would be best to assume that your organization and its IT systems have already been breached. This may sound defeatist - or like a commercial pitch from a security vendor - but it's really sound advice. Advice to survive.

Cyber insecurity can lead to extinction. Not just virtual extinction but the out-of-business kind of extinction. The ongoing spate of big, sneaky, spectacular and even long-hidden security incidents has proven that cyber insecurity is a malady that plagues many 'species' in our modern world. We at Kaspersky Lab know that all too well. We have also been hacked, a painful fact that we did not hide but broadcast to the world, so that we, but also others, can adapt and survive.

Now, a lot of the companies and organizations that have been breached, are still standing. Do not interpret that as a debunking of Darwinism in cyber security. It took a long time for the dinosaurs to go extinct and some of them held out for quite a bit longer than others. In the end, lack of change is what killed off many species. Cyber insecurity will also take its toll.

Aim for the impossible

Cyber security is what we all want, or rather: it's what we all need. It's a goal that you need to keep striving for. However, it's not a set state that you can attain and then preserve. The 'you' in this statement is applicable to consumers, employees, executives and politicians, as well as companies, non-profits, NGO's, countries and broader entities such as the European Union. Perfect security, which gives you a hundred percent protection, is not possible.

This does not mean that we should give up. We, the security industry, telecommunications sector, the IT users and society at large, need to aim for perfection even when we know that this is unattainable. By striving for the impossible we will create an ever better security: in products, in systems, in processes, in skills and in mentality, even though every inch towards that impossible goal is exponentially more costly to reach, a bit like the high cost of the 'last mile' in the telecoms world.

The cost equation

Now, here's the good news: the problem of exponentially higher costs is something that can be turned against our adversaries. Just because a hundred percent perfect security is impossible to reach, this does not mean that ideal security is out of reach. Ideal protection is a level of security which is realistically attainable – meaning that it's feasible as well as affordable in relation to what's to be protected.

From the viewpoint of potential victims, ideal protection is achieved when the cost to hack your system is higher than the cost of the potential damage that could be caused by a hack. To put this in terms of the current cyber crime environment: ideal protection is achieved when the cost of a successful attack is greater than what an attacker could gain from a hack.

Two sides of the coin

Unfortunately, the huge strides we've made in information technology and telecommunications work both ways. The technical progress helps modern usage, facilitates new business models and enforces cyber security. At the same time it makes new cyber crimes and illegitimate business models possible, feasible and ultimately affordable for the bad guys. The shining coin of IT evolution has a dark other side.

Naturally, there are cases where the cost of a successful attack does not really matter. This applies to certain kinds of hack goals and certain kinds of attackers. Like state-backed hackers who are out to sabotage, steal, spy or even make cyber war. This is not scaremongering or just a theoretical possibility, this is stark reality.

Sabotage, spying, theft

Costly and complex cyber sabotage has already been done. A prime example is the sophisticated Stuxnet worm which disabled Iran's nuclear program, even before 2010. Costly and complex cyber theft has also been done. A recent example is the illicit money wiring through hack attacks on banks via the international SWIFT system (Society for Worldwide Interbank Financial Telecommunication).

A good, Darwinistic response to incidents like these is to study them, learn from them and then change in response. That change is not something to be done just in reaction to past incidents. Change should also be forward looking. Try to imagine the creative new ways in which adversaries could try to go after you, your assets and even your connections to others. Sometimes, a hacked organization is not the real goal, but just a mean to an end. Some of the more impactful hacks in recent history have been done through intermediaries, partners and other links.

Stop being static

In a sense it's good when a company or organization has been hacked, not too devastatingly, of course. It's good if the victim has survived the attack, learned from it and adapted. Like a home-schooled child that has never had the flu, the first infection will hit hard. And in the case of cyber attacks, that first hit will come, sooner or later, or it has maybe already happened, unnoticed.

Darwinism is the key to survive cyber insecurity. The trick to achieve Darwinesque adaptability is to stop being static. Don't just list and defend your assets. Realize that, over time, some assets devaluate and some protections erode. Make a graph of your assets and your security measures. Scale up your valuations and change your protections. Keep up! Beware of snake oil salesmen who peddle the marketing magic of so-called 'nextgen security'.

The bigger picture

Don't focus on specific security incidents. Instead, concentrate on potential attackers and correlate seemingly individual incidents to see patterns. Look at the bigger picture. Don't try to do all this by yourself, because nobody can. Sharing information, between businesses (yes, even your competitors!) and/or with law enforcement agencies equals learning, which in turn helps us all to adapt. We showed that it could be done: the 'No More Ransom' initiative[1] that consisted of Kaspersky Lab, Europol and competitor Intel Security, helped thousands of people in the Netherlands and Belgium last summer. This could not have been possible without working together.

Lastly, take Gartner's advice for adaptive security architecture to heart, and change retrospective security into a continuous cycle. That model delivers predictive and preventive security, whilst also giving you detective capabilities to respond quickly to threats. Evolve, or be a victim of 'natural cyber selection'!

(1) https://www.nomoreransom.org/

Remote SIM Provisioning

New standard adds new risks to the mobile domain

Daan Planqué, KPN

The world of mobile phones and their accompanying networks is one of constant high-speed innovation. The Netherlands hasn't even had a 4G network for 5 years and the trials for 5G have already started. On top of that there is a new standard in the works at the GSMA[1], a mobile industry standards body that will, change the concept of the SIM card as we know it. However, this new standard, as it currently stands, will introduce new security risks that make it increasingly easy for an attacker to listen-in or manipulate voice or data traffic. In the following paragraphs, I will explain why these risks exist, what they might mean for you or your company, and what you can do to reduce or remove them altogether.

First some background

Before explaining the risks of the new GSMA standard, some background knowledge on SIM cards and encryption is required. For a smartphone to work it needs to have a SIM card from an operator with whom t has a subscription for voice and/or data. The smartphone will create an encrypted connection with the mobile network once the SIM card is unlocked with a PIN code. This is possible because the mobile network and the SIM card both know a unique secret key called the Ki. This key is created during the production of the SIM card and is hardcoded in the chip, which means the key is programmed into the card in a manner that it cannot be changed or removed after the fact. After the production of a SIM card, a copy of the Ki is securely sent to the mobile operator, who then stores it in a database in the mobile network called the Authentication Center (AuC). Now that the mobile network and the SIM card both know the Ki, they can prove the others identity via a pre-defined algorithm[2]. This measure counters the possibility of an attacker impersonating (i.e. spoofing) a SIM card or mobile network. The Ki also allows for the creation of an encrypted connection between the smartphone and the radio network of the mobile operator preventing anyone from listening or manipulating phonecalls or data traffic. In other words, keeping the Ki secret is of paramount importance to guarantee the confidentiality or authenticity of the mobile connection.

Another benefit of a SIM card is the possibility to swap it if the trust in the security of the Ki or the connection is lost as a new SIM card means a new Ki. In the future, such a swap might not be possible anymore if a switch to embedded or integrated SIM cards is made. These new SIM cards, called eUICC or iUICC (embedded or integrated Universal Integrated Circuit Card), will either be soldered onto the motherboard of the phone (eUICC) or integrated into the processor (iUICC). The question then is: "How does the phone know what operator it wants to connect to?" and this is where the new GSMA standard comes into play.

Remote SIM provisioning

A cooperation of international telecom operators and vendors of mobile systems[3], who are all members of the GSMA, are developing the new standard called Remote

(1) GSMA (www.gsma.com)

(2) An example algorithm is Milenage specified by the 3GPP (www.3gpp.org)

(3) Examples of mobile system vendors are: Samsung and Apple who create smartphones, Vendors who produce SIM cards such as Gemalto and Morpho, and Cisco or Ericsson who create the IT systems used by mobile network operators.

Four hundred million vulnerable Androids are out there. There's still too many unpatched Android devices, Google reckons.

Viber is now end-to-end encrypting phone calls and messages.

SIM Provisioning (RSP). The RSP standard consists of multiple documents, some of which are still in draft, and describes how the systems that provide the provisioning functionality work together.
The RSP standard will bring many changes with it. The main difference will be that a SIM card has its subscription profile, which includes the secret Ki key, installed by a remote server. This remote server, called the SM-DP+ (Subscription Management – Data Protection), will store the subscription profiles of one or multiple telecom operators in its own Hardware Security Module (HSM). When a mobile device requests a profile, the SM-DP+ will ask the respective operator for approval and, if received, will send the complete subscription profile, including the Ki, over a TLS encrypted channel via the internet to the SIM card.

This encrypted channel is where another important part of the RSP infrastructure comes into play, namely the Public Key Infrastructure (PKI). The PKI is used to ensure that the authenticity of the systems in the RSP network can be verified. For RSP, the idea is to create a specialised Root Certificate Authority, 'owned' by the GSMA and trusted by all the members who use the system. The RSP Root CA signs the certificates of the systems, such as the SM-DP+, as well as the certificate for the SIM vendor (EUM) that allows it to create and sign the certificates for the SIM cards. This 'Chain of Trust' allows a SIM card to verify the identity of a SM-DP+, because it has been signed by the Root CA it knows and trusts. Likewise, the SM-DP+ knows and trusts the certificate of the SIM card because it knows and trusts the Root CA. When the identities have been verified the SM-DP+ and SIM card can create an encrypted channel and exchange the new subscription profile.

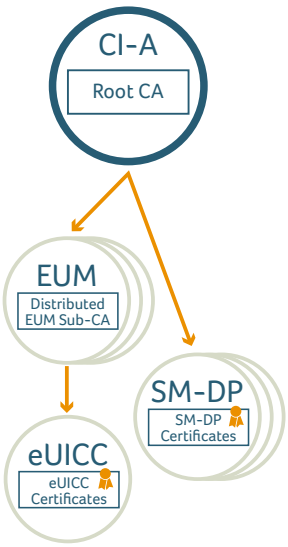


Figure 1 - PKI infrastructure of RSP

Soooo, why should I care?

With the outline of the basics of RSP in mind, lets consider the fact that the SM-DP+ stores all key material and is connected to the internet. Combine that with the fact that there is only one Root CA, which also must be connected to the internet in order to verify the identity of systems in the RSP infrastructure. On top of that, that the Ki, which is used to encrypt the phone call between a smartphone and the base station of a mobile network, is stored in the SM-DP+. So, when the SM-DP+ is hacked and the attacker can retrieve the Ki's, all traffic between mobile devices and base stations can be decrypted. This would allow a criminal to clone a SIM card and call expensive phone numbers for financial gain or prevent you from connecting to the mobile network. What if the only Root CA for mobile networks is compromised and all certificates need to be revoked? How can the SM-DP+ or a SIM card verify identity? And once this situation will occur, how can the 'chain of trust' be rebuilt and the Root CA certificate, that is stored on the SIM card, be replaced? How can the Root CA be replaced in a secure and trustworthy manner if the SIM card cannot verify the identity of the mobile network? The only solution then is to replace the processor or motherboard of the device. Also, don't forget the wonderful world of IoT devices with a mobile connection such as cars, sensors, fridges, or alarm installations. These will, as with the smartphone, all require their motherboard or processor to be replaced if the profile ever needs to be changed. For example, when wanting to switch to another provider or a new subscription. And what about all the embedded devices used for remote management of industrial devices such as cars, trains, or power plants? It would be an utter and complete nightmare.

Oh dear! Should I panic?

No, you should not panic. As I said before, these standards are still being developed and some are still in the draft phase. At KPN, we have expressed our concern and are working on improving the standard documents together with the GSMA and partners involved. You, as a user, can also prevent eavesdropping by adding another layer of encryption to your mobile traffic, for example by using HTTPS when browsing the web, using Silent Phone for voice calls, or by using Signal or Threema as messaging apps. If you want to go even further you can ask your telecom operator if they are aware of these security risks and ask them, if necessary, to act. In the end, it comes down to the importance of taking security into account right from the start when designing a new system or standard. This goes, not only for the systems of vital importance to modern society, but also the smallest and least-significant devices there are. Because even a simple DVR can, in large numbers, take down the internet.

Energy sector cyber security 2.0: Pro-active approach needed to tackle insider threats

Gisele Widdershoven, Accenture Security

Successful attacks and a potential for wide-scale disruption have made the oil & gas, chemicals and utilities industries prime targets for cyber attackers. Enterprises operating in these sectors are strongly advised to update their security practices to address insider threats.

While most of the current attention has been given on the threats to the electric grid worldwide, oil and gas have been almost forgotten in the media and research planning. The US Department of Homeland Security even states that the energy/oil-gas sector is the most attacked industry worldwide. Oil and gas production is part of nations' critical infrastructure, with many thousands of miles of exposed pipelines, making them vulnerable to both cyber and physical attacks. This makes them an attractive target for nation-states, hacktivists, splinter groups, lone actors and terrorists.
In 2016 the number of cyber attacks has increased beyond the 2015 count, and companies are reporting that they are losing confidence in the ability of their own organisations to detect and deter increasingly sophisticated cyber attacks.

Insider threats

Conventional Enterprise security mechanism are designed to keep the 'bad guys' out – and have tended to focus on perimeter defences. With the use of social engineering to bypass these defenses through fraudulent access to employee credentials, we need to extend our thinking to cover threats from the inside – where the attacker could be masquerading as an employee, or could also be a valid employee with a grudge. According to a 2015 survey performed by SANS[1], "insider threat" was regarded as one of the top security threats by 48% of the participants.

Social engineering is proving to be devastatingly effective in gaining access to secure systems by exploiting a lack of security awareness of employees. The economic necessity of converged IT/OT infrastructures has meant that the cyber attacker potentially has a wider attack surface to exploit. As the Ukrainian blackout proved, it is possible to gain access to and disrupt the OT domain by exploiting security weaknesses in the IT domain.

Risks are underestimated

Major oil and gas companies worldwide, such as Saudi Aramco and QatarGas[2] have experienced devastating insider cyber attacks, resulting in the shutdown of vast parts of their operations for pro-longed periods of time. It seems as if companies are underestimating the risks that energy production and production operations are facing. Although awareness of the need for effective security is growing, there is still a wide-scale lack of understanding

(1) SANS white paper "State of security in control systems today"

(2) Sources:
Insiders exploiting privileged accounts likely behind Saudi Aramco attack (infosecurity-magazine.com);
Insiders Implicated in Saudi Aramco Attack (securitywatch.pcmag.com);
Thinking about Security from the Inside Out (www.wired.com);
Natural gas giant RasGas targeted in cyber attack (www.scmagazine.com);
US officials: Cyberattacks on Aramco, RasGas may have come from Iran (dohanews.co).

the potential vulnerabilities present in industrial control systems, which is compounded by growing threat levels, and the potential for insider threats is largely overlooked.

Holistic approach

At a Society of Petroleum Engineers (SPE) conference, several speakers indicated that the responsibility for cyber security should not be the sole responsibility of the IT department. A more holistic approach is required to counter the growing cyber security threats linked to social engineering, human interference or insider threats, which are largely linked to human factors. The total organisation needs to become involved with security in a pro-active and consistent manner.

Looking at the overwhelmingly complex organizational structure of international oil and gas companies - which are not only financially and commercially integrated, but also in their technical operations - a lack of awareness in one department will constitute a threat to all.

The weakest link

At present, most energy or water companies are looking solely for their cyber security to their IT departments, and sometimes involving operational groups to support their efforts. However, looking at the insider threat parameters, several other groups should be involved at the same time to counter possibly increased threat opportunities. The underestimated role of human resources, HSE (Health, Safety and Environment) and even finance, is clear. Personnel is, at present, always the weakest link in any operational security approach. Personal issues will affect the effectiveness of any cyber security approach.

At the same time, based on growing integration and specialisation of oil and gas operators, but also power and water companies, engineering projects such as drilling, seismic, geophysics or construction, always involves third parties at the premises.

A risk to be addressed is the need for third party and contractor involvement in the normal day-to-day business of companies. This increases the potential risks of interference by contractors using insecure practices, or intent on causing cyber damage if they are not appropriately vetted.

Disgruntled employees

The range of potential insider threats is wide, but can range from disgruntled former employees with technical knowledge, to commercial spies or non-state/state actors. For normal employees to become insider threats is not an enormous leap.

Disgruntled employees, laid-off or misjudged personnel, can easily rationalise their actions when crossing ethical lines. Looking at these potential threats in your organisation, while bringing in new cyber security frameworks or workflows is not an easy task. The main difficulty is to bring in a purely technical approach into contact with the Alpha-world (emotions and personnel backgrounds), as shown in the attacks inside Aramco[3], which were all expedited by insiders.

Interaction on all levels

Eliminating insider threats necessitates interaction on all levels between HR, legal, HSE and IT departments, and necessitates increased vetting of personnel. This should be conducted on a continuous basis, perhaps supported by social media data mining or other legal assessments to be able to pro-actively approach possible breaches or outright theft, sabotage, ransomware or worse.
This approach will involve increasing the assessment of human behaviour through increased social media tools to keep an eye on out-of-area/over-the-horizon social media activities of employees or third parties.

The use of new tools to access and address official open source information will become a major new security tool to provide more actionable data to increase a company's own security environment but also will give it the tools to put in place a more pro-active approach to counter future threats. The inclusion of all departments, HR, IT-Security and operations, is a clear need. Addressing potential future threats inside your company, based on human factors, will need a more active HSE/Security awareness within the HR departments too.

Cyber security 2.0

Behavioural analysis is needed not only to keep your personnel out of risks but also to prevent future threats. Social engagement and behavior on the Internet, especially after working hours, could indicate a negative development that could lead to an insider threat opportunity. At the same time, social behaviour on the Internet/dark web or even grey web, needs to be addressed and taken into account. Networks of individuals indicate increasingly the possibility of threats. Data is available, but actionable data is hard to find. Cyber security 2.0 is needed, which should be a symbiosis between human or behavioural analysis (Alpha) and pure IT systems and algorithms (Beta). As long as algorithms and IT systems are not as smart as a human brain, human analysts will be needed to counter a potential insider threat which is developing outside of the company but will be targeting inside operations.

(3) Sources:
Insiders exploiting privileged accounts likely behind Saudi Aramco attack (www.infosecurity-magazine.com)
Insiders Implicated in Saudi Aramco Attack (securitywatch.pcmag.com);
Thinking about Security from the Inside Out (www.wired.com).

Breaking your band: one byte at a time over the air

Ömer Coşkun, KPN

Introduction

Modern computer systems – smartphones, PCs, embedded devices [1] – are comprised of multi-layered operating systems. This is unlike the conventional description from Computer Science books, which states that single monolithic pieces of software manage each piece of hardware, from CPU, the video card, and up to the wireless connectivity.

Let's take smartphones for instance, it actually runs two operating systems; the first layer (Android, iOS, Windows Mobile etc.) is the layer we, the end-user, interact with and the baseband operating system[2]. The baseband operating system lays in firmware that runs the baseband processor, which is relatively tiny and operating invisibly. Merely to responsibly process everything related to radio and cellular data.

Baseband (RTOS) Real-Time operating system

The functionality of baseband is time-critical, therefore a real time operating system (RTOS) is required on its architecture. For instance, the RTOS in Qualcomm Snapdragon's baseband processors' use a VLIW (very long instruction word), and a proprietary REX kernel, made of ~70 concurrent-threads which can handle signal and video processing, GPS, and mass storage (SD cards) etc.[3]

The following photo shows the internal structure of an iPhone 5/5s, utilized Qualcomm MDM9615 baseband mobile data modem (highlighted in blue)[4].

Figure 1: iPhone 5/5s internal circuit board structure

Baseband RTOS architecture

Hexagon is Qualcomm's digital signal processor used in the Snapdragon series on-the-system chip for supporting CPU and DSP functionality in deep embedded processing. The hardware utilizes VLIW architecture, variable instruction lengths and a very long instruction word processor architecture with hardware multi-threading.

(1) The second operating system hiding in every mobile phone (www.osnews.com)
(2) Baseband processor (wikipedia.org)
(3) Qualcomm Snapdragon 805 Processor (www.qualcomm.com)
(4) iPhone 5/5s internal structure (www.techinsights.com)

The hexagon is a 32-bit architecture, which operates with 32 bit registers over 32-bit addressing space. Instructions could be grouped together for parallel execution, with each group containing one to four instructions together. The following screenshots a sample disassembly of a hexagon binary using IDA Pro's Hexagon Plugin[5]:

Figure 2: Disassembly of a hexagon binary using IDA Pro

The main characteristics of hexagon's assembly analysis show that it's specifically intended for digital processing jobs with a fully-featured general purpose architecture, with a strong focus of computationally expensive operations such as vector and floating-point operations.

Interestingly enough, the hexagon architecture permits encoding of two instructions to one, in the sense of compound and duplex instructions. (E.g. two atomic instructions combined into one or two consecutive operations grouped together)

Analysis of a smartphone's DSP firmware

A smartphone's baseband firmware is not different than a standard Linux elf-executable (ELF), but it's compiled for hexagon's architecture. Therefore, it may be analysed by the GNU-Toolchain which consists of tools such as GCC, OBJDUMP etc.

The following screenshot shows that the smartphone's DSP firmware is correctly recognised by the GNU-Readelf.

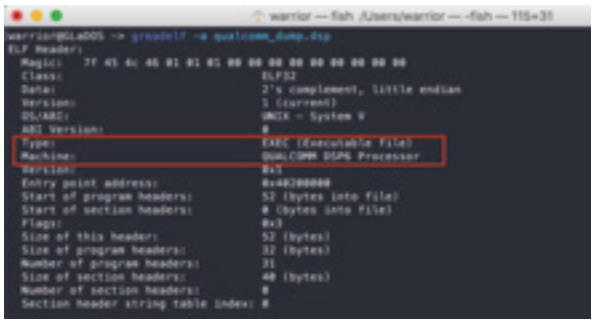


Figure 3: GNU-Readelf correctly recognises the DSP firmware

Despite the fact that the analysed firmware makes an attempt to prevent reverse engineers, from obtaining valuable information about its property. It still leaks a lot of useful information in the firmware, even when encrypting some of the binary sections.

The firmware, for instance, contained vendor related specific versioning and digital certificate information which were readable by a standard text editor.

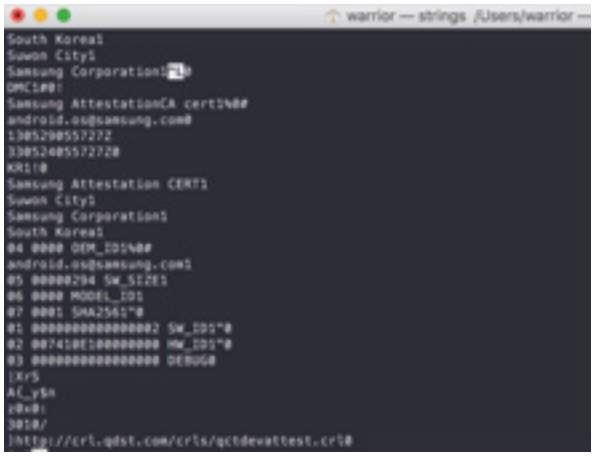


Figure 4: DSP Firmware containing vendor related information

Offensive exploitation scenarios on baseband RTOS

The DSP firmware binary is based on VLIW architecture with variable length instructions and multi-threading. This architecture exploits data, instruction and thread level parallelism with application specific instructions (compound instructions, e.g. 1 DWORD does 2 things in parallel) to achieve efficient data re-use and less power consumption.

According to disassembly analysis with a tool called IDA Pro and by reading the Qualcomm documentation[6]; it was found that the chipsets use the following security features: safe unlinking (heap), NX also known as non-executable(heap/stack), kernel/user-mode separation (a.k.a. SMEP), however, there is NO ASLR (Address Space Layout Randomisation) in place. This eases an attacker's work to achieve command execution on a victim's phone. Additionally, stack usage/allocation is similar to x86 with a little difference – stack frames are 8-byte aligned instead of 16 bytes on x86 systems.

(5) IDA Pro's Hexagon Plugin (github.com)

(6) Qualcomm developer reference manual (developer.qualcomm.com)

Having all this in mind, exploitation of multi-threaded applications is difficult. In general due to dealing with race conditions and difficulties with achieving Turing-completeness when it's required to have certain conditions to be met during exploitation. (i.e. tracing messages across multiple tasks, monitoring IPC etc.)

Specially, the exploitation in this (VLIW) architecture is harder, due to existence of compound/duplex instructions. This creates constraints for re-usable standard library code (a.k.a ROP gadgets). This can, however, be overcome by automating the constraint handling with help of memory sanitizers and constraint solvers. (i.e. LLVM[7], SMT solvers[8]). Manual gadget writing would require alternating in gadgets, and de-allocation of the frame (JMP R31) to achieve Turing completeness due to trampoline calls in hexagon instructions.

Conclusion

Achieving code execution on a baseband's RTOS would mean control over millions of phones, regardless of its brand, since they mostly use the same chipset. Therefore, attacking the baseband's RTOS has always been high profile and a well-compensated target for black-hat hackers and intelligence agencies alike.

It was actually hinted out by Edward Snowden in 2014, that NSA and other intelligence agencies could remotely turn on a phone and record everything by exploiting a vulnerability in the baseband's RTOS or sending their own modified firmware to a victim's phone through an innocuous looking firmware update[9].

(7) LLVM Compiler Framework (clang.llvm.org)

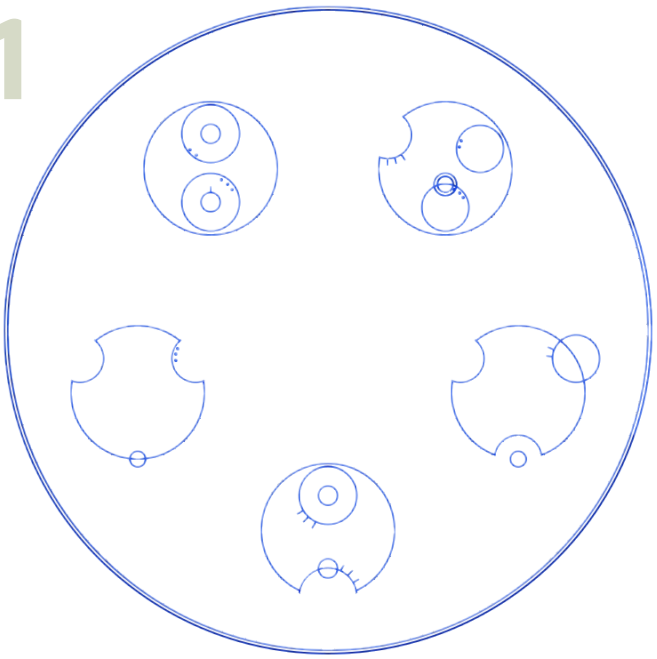
(8) Z3 Microsoft SMT Solver (github.com)

(9) How the NSA can'turn on' your phone remotely (money.cnn.com)

Puzzle time!

Can you crack these puzzles?

1



2

```
+++++[>+++++++++++++++++>++++++++++++++++
++++>++++++++++++++++++++>+++++++>++++
++++++++++++++++>++++++++++++++++++++
>++++++++++++++++++++<<<<<<<-]>-.>-.+.>-
----.>---.<+.<----.>++++.----.>.>-.<<<----
.>+++++.>.>+.+.<<-----.>.>---.<<-----.---
-.>.<+.---.++.<++++.>>.<<----.>>>>-.++.<<.
<<+.>>>>+.-.<<.<--.>>>.<<.<<++.>>>+++.<<<+
.>>>++++.<.<<-.>>>----.<.<<---.>>.<--.>>..
<<<+++.>>.<+++.+++++.<--.>>.>>>-----.<<<<-
.>.<--.+++..----.--.+++++.<+++++.>>.<.<--.
>+-++++.<-.>>>>+-+++++.<<<<<<+++++-++++++.
```

3

ilua dt slt reiia ttc ots bh oenhaoefp

Check page 63 for the correct answers

June

1 Criminals behind LURK malware arrested.

14 Democratic National Committee report that they have been hacked.

Stop Chasing Your Tail

John Michelsen, Zimperium

These days, the computers most vulnerable to a cyber threat in the enterprise are mobile phones and tablets. Security teams are totally blind to the risks these devices pose for the enterprise and are unable to deal with threats as they appear. Many enterprises manage device access to corporate resources, networks and identity, but they can't remediate a threat they can't identify. As more of our computing goes directly from mobile device to cloud services, network threat detection solutions are ineffective, since data often resides outside the corporate data center. There has to be a better way to remediate and identify mobile device attacks and risks in the enterprise.

In December of 2016, Ian Beer, from the Google Project Zero research team, released his local elevation of privileges exploit targeting Apple's iOS 10.1.1. iOS is the impenetrable operating system said to be secure with its "walled garden" approach, right? Well, we viewed this latest attempt as another opportunity to assess a new zero-day exploit against our machine-learning attack and exploit detection engine – z9.

After a test in our mobile research lab, z9 detected, once again, a previously unknown attack. Beer's 10.1.1 exploit allows remote shell access as root. z9 detected the attack without needing an update to see this threat. Since we didn't require an update, our customers were protected at a time when the vulnerability didn't have an official name, marketing campaign or disclosure.

Why is this important?

With iOS and Android platforms continuously evolving, it is crucial to detect attacks without having to update a detection engine. Having to update your detection engine to recognize a threat will continuously put you steps behind cyber attackers. Constantly updating your detection engine to protect yourself from an attack is only useful if you know of all of the attack methods, but you can't possibly know all of them. It is an impossible task since cyber criminals are constantly trying new techniques to avoid detection. Once an attack method has been publicly disclosed, a hacker or nation-state is less likely to use it. In essence, you are looking for attacks no longer being used.

Take for instance the Pegasus attack targeting human rights activist Ahmed Mansoor in September 2016. Pegasus is a device-level exploit identified in the wild after researching a link in an SMS sent to Ahmed. Having been targeted before, Ahmed is aware of the dangers of constantly being connected and would be considered an advanced smartphone user. After receiving a text he suspected was malicious, he sent it to a lab for investigation. After testing, the text proved to be an advanced kernel-level exploit, activated remotely by a group targeting Ahmed in order to take over his device and track his whereabouts and data. Our detection engine detected this attack without needing an update to recognize this vulnerability. Apple later fixed the vulnerability and pushed out an update.

June

15 Thousands of hacked Government and corporate servers sellling for $6 on black market.

24 Google Project Zero team releases report with multiple RCE vulnerabilities in Symantec and Norton products.

28 Researchers release a paper on transmitting data via pc fans.

Chrome makes it easy to pirate movies.

In July 2015, a similar, remotely executable exploit on Android, Stagefright, was disclosed. The Stagefright vulnerability allows an attacker to perform arbitrary operations on the victim's device through remote-code execution and privilege escalation. The attack can be delivered via MMS to the victim's device where it runs automatically, since the Stagefright library can execute a command without user interaction.

Pegasus and Stagefright are very similar. Both are remotely executable attacks and existed for years before they were identified. Pegasus was originally developed for iOS 7 and was identified 26 months later. Apple patched this vulnerability with the iOS 9.3.5 update, and if you are running iOS 9.3.5 or later on your device, it is no longer vulnerable. However, it is still vulnerable to the next Pegasus-like exploit or unknown vulnerability. The same scenario plays out with Stagefright, but on a larger scale. Google has updated the base Android OS, but the fragmented update process to get new versions to devices is tedious and slow. Approximately 800 million Android devices remain vulnerable and many will never receive security patches for the Stagefright bugs.

Protecting your workforce from these known attacks is well-documented and attainable. However, it is not possible to defend against these types of vulnerabilities before the research and documentation is provided, unless you are using an on-device, behavior-based detection method. Using a behavioral detection engine is the only way to defend against the unknown attacks lurking in the wild today.

Zimperium's research team has tested many other previously unknown attacks against z9 and found the same success. Dirty COW, Gooligan, Drammer and Dress Code were all exploits detected by monitoring the effects of the attack versus trying to identify the attacks via the cause or signature. A behavior-based detection software looks for the effect of an attack and can warn a user or security administrator of any new threats. If an app or process elevates privileges on the device, it is detected. If a process changes a file in the OS or any of the other thousands of parameters available, it is detected and classified based on the effect. Once an attack is detected it can then be remediated and locked down. This "on device behavioral detection" is how you detect "unknown" or "zero-day" attacks.

New and previously unknown threats are becoming more frequent. Targeted attacks on individuals' devices will continue to increase, as business users primarily use mobile devices not protected with a Mobile Threat Defense solution. Identifying these attacks via the cause or signature is an outdated method and is difficult to maintain, since mobile operating systems are updated several times a year.

In order protect yourself and your corporate data, I recommend using a future-proof, on-device mobile threat detection solution, rather than relying on a historic or signature-style method of detecting mobile threats.

With iOS and Android platforms continuously evolving, it is crucial to detect attacks without having to update a detection engine.

July

7 Google starts testing 'quantum-cryptoproof' proof crypto algorithm in Chrome browsers.

8 Fantom ransomware found to pose as Windows update to encrypt files in peace.

Facebook starts testing end-to-end encryption in Facebook messenger.

My First Golang Project

Bouke van Laethem, KPN

aiki.go

Aiki is a Japanese martial arts principle or tactic in which the defender blends (without clashing) with the attacker[...] One applies Aiki by understanding the rhythm and intent of the attacker to find the optimal position and timing to apply a counter-technique. In Japanese Aiki is formed from two kanji:

合 *: *ai - joining**

氣 *: *ki - spirit**

Down the rabbit hole

A while ago, a colleague noticed attempts by an "Administrator" to log in to one of his computers. His computer had the Remote Desktop Protocol (*RDP*) service open to the Internet. As the name suggests, the RDP service allows computer owners to remotely use their desktop. The attacker was trying all kinds of passwords to get into the machine. My colleague scanned the attacking computer. The only service open to the Internet was RDP.

Perhaps someone was consciously attacking others from his own computer, forgetting he/she had left RDP open. But more likely the system had been compromised through RDP, infected with malware and was now being used to attack others. The attacker was trying to log in through RDP and only had RDP open itself. Suddenly something dawned on me.

When a system mindlessly does whatever an attacker wants it to do, we call it a *bot*. A bot attacking other systems has usually been compromised using a list of common or standardized usernames and passwords, called a *dictionary*. I figured that eventually this bot would try to log in to RDP using the same username and password which was used to compromise itself. That seemed like a simple, provable and specific enough hypothesis.

One small problem: RDP is a complicated protocol to mimic for research purposes. Luckily Secure Shell (*SSH*), another protocol used to remotely manage devices and computers, is not. Just like countless system administrators all over the world, I use SSH to remotely manage my Internet facing servers. A quick look at the number of failed login attempts for SSH on one of my servers was enough: Password guessing attacks against SSH are happening on a very, very large scale.

Building the test case

"How do you know I am mad?" said Alice. "You must be," said the Cat, "or you wouldn't have come here."

How do you know I am mad?

I immediately started writing a program in Python that pretended to be a SSH service. The idea was simple:

- Pretend to be a SSH service.
- Bots will try to log in with a username and password.
- Automatically try to log in to the attacking system's SSH service using the same username and password.

In pseudo-code:

```
for connection in SSHD:
  try:
    SSH.connecttoattacker('connection.remoteIP',
'connection.username','connection.password')
    print('It worked!: ', connection.remoteIP, connection.
username, connection.password)
  except:
    print('The King said gravely: "Go on till you come to
the end: then stop"')
```

Sadly, my coding flow soon ground to a halt. I have this way of running into Python threading and performance issues. Things were getting ugly fast. That is when I decided to start my first Golang project. Because as some of you may know, the Golang programming language is right up there on the hipster scale with beards, soy lattes and fixies. This should be reason enough to choose it as a programming language, but it also performs great and has awesome threading functionality. So Golang it was!

In some pseudo-code, the program to fake a SSH service does this:

```
package main
import (
  //some libraries I need to make this work
)
// create a private key used by the SSHd to encrypt
communications
func buildkeys() (priv_pem []byte) {
}
// set up non-bruteforcable account details
func unguessable() (username string, password string) {
}
// ssh client that can reuse captured usernames and passwords
func aiki(ip string, username string, password string) {
}
func main() {
  // start fake SSHd server
  config := &ssh.ServerConfig{
    },
  // connect back to anyone connecting to the fake SSHd
server
  go aiki(ip, username, password)
  }
```

In the end the module turned out to require a few more nuts and bolts. You can find the aiki.go source on https://github.com/KPN-CISO.

I deployed aiki.go on one system, quickly followed by five others in different IP ranges around the world. And then, I waited. Would I catch anything? And if so, on how many different systems? Well...

```
Days aiki.go has been running: 183
Number of attacking systems: 8986
Number of successful "aiki": 742
Top 10 of usernames and passwords used in successful
"aiki":
  220 admin:admin
  132 root:admin
   53 pi:raspberry
   34 root:root
   33 root:123456
   29 ubnt:ubnt
   23 root:welc0me
   22 root:000000
   21 root:openelec
   14 root:1234
Top 10 of most successful days:
   33 2016/12/29
   28 2016/03/06
   24 2016/12/25
   18 2016/03/15
   14 2016/12/30
   14 2016/12/28
   14 2016/03/09
   14 2016/03/04
   14 2016/01/04
   13 2016/12/27
```

It was really nice to have my hypothesis proven, but now I had some hard questions to answer. Was what I was doing legal? And even if it was okay in the eyes of (international) law: how could I use all of this ethically?

Laws

"Now, I'll manage better this time," she said to herself, and began by taking the little golden key, and unlocking the door that led into the garden.

Now, I'll manage better this time...

In the Jabberwocky world of information technology it must be hard for lawmakers to decide what constitutes a crime. To make sense of intangible acts often the tangible world is taken as a guide. So, can we find a real-life example to explain what aiki.go does? And can we use it to decide if what we are doing is legal? I think we can do both, but first I have to give a little background on how SSH works.

When you use SSH (version 2), the acts of connecting, authenticating, and actually doing something on the remote system are strictly separated into transport, authentication and connection steps. A diagram might help to explain this.

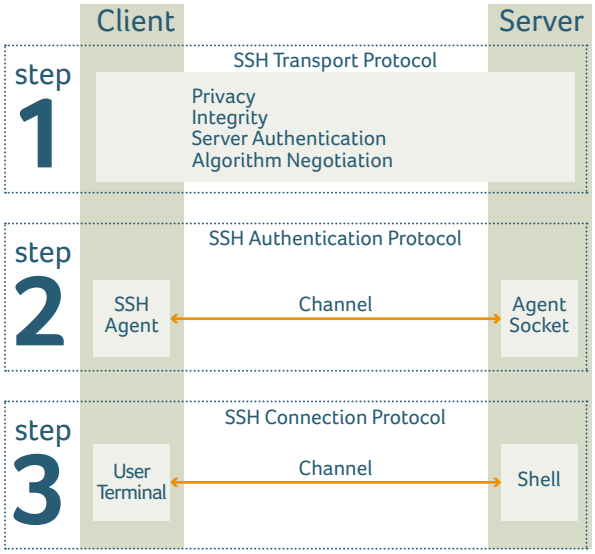


Figure 1: SSHv2 protocol

The aiki.go program works by taking the virtual key (username:password) the attacker used on us to try it on the attacking systems lock (SSH service). If the lock turns (Step 2: Authentication), aiki.go does not even bother with the digital equivalent of using the handle or pushing against the door (Step 3: Connection). aiki.go simply notes it found a working key and moves on.

I am not a lawyer but I think I am staying just on the (slightly bleeding) edge of what is legally allowed. I only try to authenticate (not log in!) with the exact username and password the attacker just tried against me. But I am not completely sure, so I sincerely hope you will let me know if you think differently. I am very much looking forward to some constructive feedback and expert opinions. But even if what I am doing is lawful, that does not necessarily make it right.

Ethics

The Queen turned crimson with fury, and, after glaring at her for a moment like a wild beast, screamed "Off with her head! Off--"

"Nonsense!" said Alice, very loudly and decidedly, and the Queen was silent.

Off with her head!

I am a hacker. I get a thrill from making things bend to my will. The buzz of getting my first positive results created a torrent of ideas. I could name and shame everyone attacking me on Twitter! I could log in to the attacking systems and remove the infection, or even destroy the remote system altogether! I could jump from system to system uprooting botnets! Off with their heads!

So I started with the first thing that came to mind and added functionality to put IP address, username and password of every successful "aiki" on Twitter. That would teach them!
Except it would not. Because there is nobody to teach. I had a look at a couple of attackers using a web browser. It quickly became clear these ruthless attackers were just cluelessly configured devices.

My sample of successful "aiki" is a collection of victims, not villains. People are usually completely unaware their devices are attacking others. Clearly they also do not know that anyone trying a couple of passwords can access their security cameras, baby monitors, backup devices, modems et cetera. If I started naming and shaming attackers on Twitter, I would just be giving access to these devices to all the Twitter trolls, violating the privacy of innocent bystanders.
As for the other ideas I had: logging in to devices to stop or attack botnets, besides being illegal, also felt wrong. Again, I would be further violating the privacy of the abused and that is not okay, ever.

Law enforcement agencies are likewise hampered in what they can do. They are usually allowed to request information about which person is behind a certain

IP address. Theoretically they could get into contact and secure digital forensic data. But that would be a lot of work and none of it would be done with the goal of helping those who have infected devices.

Conclusion

As far as aiki.go is concerned: in its current form it cannot do anything more without becoming unethical and unlawful. It has served to prove two things:

1. Most attackers out there are actually innocent victims with easily guessable passwords as their main weakness.
2. For anyone with some time and technical knowledge, it is possible take over large numbers of bots and botnets without actively attacking other systems. It would be illegal and unethical, but there are people out there who do not care about such "details". Someone might already be doing this, without us ever knowing.

In the mean time, the best response the international community has come up with is a technological arms race. Governmental and private sector defenders are out there fighting against the botnet herders. However, that fight focuses exclusively on trying to protect the (potential) victims *of* these botnets, not the victims *in* the botnets.

What I think we are lacking is the digital equivalent of the World Health Organisation (WHO) *Global Outbreak Alert and Response Network* (GOARN [1]). Perhaps Computer Security Incident Response Teams (CSIRTs [2]) could play a role in building a digital GOARN, with a focus and mandate to fight the disease by helping the victims.

> In the Jabberwocky world of information technology it must be hard for lawmakers to decide what constitutes a crime.

(1) GOARN (www.who.int)

(2) CSIRTs (www.cert.org)

IoT: next big thing or next big fear

Security and trust in the connected world

Vito Rallo & Bram van Tiel, PWC

I was 12 years old, young, passionate and excited about my recent expensive achievement: a white, thick plastic brick covered with brown keys called the Commodore 64. Framed blue screens, a big white square cursor blinking on my grandma's TV and a world made of sprites and numbered lines of BASIC were storing dreams in only 64 Kilobytes of RAM.

Not even 30 years later we are confronted, once again, with the next big thing; powerful processors and better operating systems capable of handling digital media contributed to the internet revolution. We brought the internet to our daily mobile life, imposed new needs and finally blended an ancient established human process called "communication".

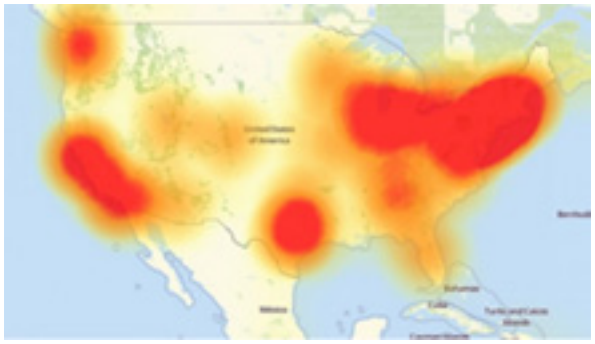
What is missing to meet the 70s vision of the future? Flying cars, jet packs, and droids!
Bruce Schneier defines the IoT as a robot. We are giving machines human senses; the Internet of Things can hear, see and smell, can feel cold and hot. The robot got arms to actuate commands in the physical world, even drive our cars. We are giving the IoT a brain to think through sophisticated analytics, sentiment analysis and machine learning and, finally, we are giving devices nearly real time communication powers, inter-connecting them in a way humans are certainly not to one other.

Say "hi" to the 21st-century robots.

The IoT revolution is not scary; it's just exciting in essence, from wearable technology and toys IoT to the Industry 4.0, it offers endless opportunities.

Security is still perceived as a barrier to the adoption of IoT solutions. Building a safer IoT means embedding security from the ground-up. "Billions" and "trillions" in market forecasts will not save the IoT from failing, badly, if the Droid does not meet one basic human requirement called "trust".

Security of the IoT is about trust and keeping control of the robot. Look at the recent facts: we clearly lost control facing one of those events whose possible occurrence cyber security experts, like prophets, had been discussing for years: an army of infected cameras in a botnet controlled by hackers, maybe just one, maybe a teenager, to exploit DNS (the internet's domain name system) vulnerabilities and bring down several sites and services.



The heat map shows the areas most affected by the Denial of Service attack of Friday, Oct. 21st.

A few days later, Mirai (the malware used in the attack) struck an entire country. The same malware was used to attack the heating systems of two house blocks in Finland, which is anything but a laugh when winter hits at -22 degrees Celsius. Hackers demonstrated how to hack medical devices, voting machines and critical infrastructures like power plants. What's next? Ransomware for washing machines to steal your expensive clothes or an armada of toasters to attack critical infrastructures? I wish connected things could stay far from influencing operational processes.

More than any abused parallel between humans' immunity and IT, the droid can get sick, can be infected by a virus, for instance exploiting wireless protocols like ZigBee. Recent research shows how to trigger a "chain reaction," spreading a worm infection by proximity to adjacent IoT devices. Keep your neighbour's drone away from connected light bulbs. The Droid could get infections like humans get the flu. The pandemic, comments the paper, could start with a single infected bulb being fitted in a city with a high density of vulnerable devices and trigger a catastrophic spread.

Should we fear the IoT?

The IoT is a compelling, unstoppable, big revolution that is already ongoing. I realize that many Security Experts bring negativity and fear about IoT and this article does not seem to be doing differently. On the contrary, in this article I want to bring a positive message and insist on how great the opportunities are and how amazing the technology behind it all is.

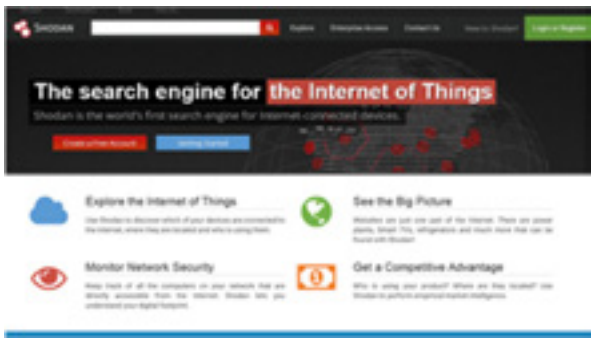
Security in the IoT will follow what I would coin "Cyber security Awareness Cycles". The same happened to web applications and mobile security. At the advent of every new disruptive innovation, we fall into a "total insecurity" phase. Risks and threats are completely "unknown". Slowly, by learning and researching, we move into a more conscious phase. Risk acceptance and threat modelling create security awareness but also generate fear. It is the process that pushes us to remediate, apply fixes and mitigate issues. Only by security awareness will we move into the "mitigated insecurity" phase, facing the uncertainty and learning how to deal with it.

Time is crucial while we're navigating the awareness cycles. We will certainly land in the IoT mitigated insecurity but how long will it take? Let's make sure it will be a short time, let's do it now as it might take longer than we're used to.

Tackling security for connected devices

For two years I have been speaking at events explaining how important "data" is. Data is the commodity business for the IoT. Information must be kept safe ensuring integrity, confidentiality and authenticity and protecting the intellectual property at all stages of the device lifecycle: at run-time, at rest, at boot, in communication. We are failing to bring the existing IT cyber security culture to the IoT and are making the same mistakes again. This time is hard, more than ever before. We face a scattered complex environment, a truly heterogeneous mix of different technologies, providers, and actors. Have a look at the IoT value delivery chain to sense this complexity.

How difficult is it to integrate security in this inherently unsafe design? The market has severely neglected security in favour of rapid development and cost efficiency. Out there, there are plenty of insecure (low-cost) devices. I am still an ethical hacker. In the past, the DarkWeb and Bitcoins were the ingredients to mount a real Denial of Service attack. Today, I could just go to the supermarket, buy a cheap camera, tear it apart, dump the firmware, search and exploit a vulnerability. By querying Shodan you can find thousands of similar devices - et voilà: yet another botnet!



Security for the IoT is a concept that has spread across the entire value delivery chain. Obviously, I do not have a magic wand solution. There are no industry-accepted guidelines yet. Many are working and struggling to produce good material. Online Trust Alliance, Cloud Security Alliance, GSMA and the Industrial Internet Consortium are doing great but the level of complexity is still too high.

GSMA suggests looking at security by type of ecosystem. It works like a charm as constraints and security requirements are different for each domain. We should consider:

1. Endpoint Ecosystem (devices, endpoints, sensors, etc),
2. Link Ecosystem (networking and communication), and
3. Service Ecosystem (back-end, APIs, data collectors and magic data processing services).

At PwC, we like the holistic approach and provide an ecosystem-aware framework based on:

- **Security by Design:** *it's about guidelines, secure design, validation and proper SDLC. It's also about the architecture, data security and many other properties of the final solution;*
- **Security by Assessment:** *we need to test and assess the security posture of our solutions, considering the threat model before hitting the market. Ethical hacking and white-box hybrid assessments are the way to go; and*
- **Security by Trust:** *trust and security are tightly linked. Extending machine trust to humans is the way to adoption of large-scale IoT solutions;*

three dimensions built on top of technology, modeling and crypto.

Trust as key factor for IoT success

Trust is the challenge and the key to the IoT success. Trust is more than security. It is a concept influenced by many properties in the IoT value system, tightly linked to security and inevitably related to privacy.

Identity, software integrity, and transaction integrity are all examples of trust issues. "Glitching", "side-channel analysis", "data tampering" and "identity theft" are some of the threats that could lead to corrupted data and/or broken privacy, and could wrongly influence decision-making processes in a failing trust design.

Get prepared; you will hear so much about it. In the upcoming years we will experience a tremendous growth and demand for solutions to establish machine trust. The answer is always an acronym: HSM, TPM, PKIs and TEE are just a few examples of great new or revamped solutions aiming to establish trust that are popping up in the IoT universe.

Trust is not entirely new to security folks. This time we're about to grant trust to machines that can interact with the physical world; that's the big deal! It's no longer about M2M. Humans must extend the trust circle to machines; that sounds scary, but again there's nothing new as we do it every day when driving our cars or submitting bank transactions on-line. We trust our bank and the technology behind the home-banking service.

IoT must learn to influence our "psychological safety", but it's not doing great for the time being! Such concepts are well known to economists and management experts. Psychological safety is what makes employees happy, creates trust in managers' leadership and builds winning teams. End-users must trust the IoT solution; data, privacy, efficiency and availability, it's all about trust.

Establishing trust

We need guidelines and mandatory regulations governing IoT security. Probably something will come soon from the US National Institute for Standards and Technology (NIST) or a similar entity. The US may be the first country to impose rules and liabilities. People trust institutions as safety regulators. That's one way to extend trust to the IoT but at the same time it forces companies to follow a proper secure development life cycle and consider security testing.

Humans establish trust *by head* and *by heart*. Machines can probably mimic head, learn to establish trust by means of technology, protocols and crypto. Establishing trust is a must in accomplishing the next big revolution. I just can't wait to understand more about this fascinating relation between people and machine trust. How far I am now from the Commodore 64, after not even 30 years… So far, yet not far enough. No, I'm not afraid of the IoT; despite Spielberg's vision, there is something that machines will never get. It's called **heart**.

Researchers find vulnerability in keyless entry system of 100 million cars.

(Ir)responsible Disclosure

A humorous look at dealing with Responsible Disclosures

Arnim Eijkhoudt & Wesley Post, KPN

Do you have a responsible disclosure policy and 'bug bounty' (reward) connected to it, or are you thinking of implementing one at your company? If you are: be prepared to attract interesting kinds of security researchers! Although responsible disclosure is a noble concept, it can attract less noble reporters as well. As soon as it became widely known that KPN-CERT rewarded valid responsible disclosures, security researchers from far and wide started approaching KPN-CERT with their vulnerability reports.

Only reporting vulnerabilities 'for profit'

Unfortunately, for many of those researchers the premise of a reward is their primary business model and motivation, rather than an overall concern about increasing security on the Internet. Because of their different goals, the communication could sometimes be classified as 'a bit different'. Here are some examples:

The most common thing we see is the researcher being upfront about his or her motivation by immediately asking for a reward as part of their initial report. That said, while the findings in their reports are generally less severe and insufficient to qualify for a reward, it obviously does not mean they will not be fixed. Additionally, while a reporter's perceived risk of some vulnerabilities can be high, they sometimes turn out to be harmless or a false positive. Due to the relative ease of finding certain types of vulnerabilities with automated scanning/crawling tools, we tend to frequently receive multiple reports of the same findings as well.

A second tendency by researchers is exaggerating the risk of their findings in order to increase their chances for a reward. We once received a responsible disclosure with the rather ominous title 'Remote Code Execution' – pretty serious sounding for any seasoned CERT. However, when reviewing and analysing the reported issue, it turned out to be a type of Cross-Site Scripting (XSS) which could only be performed within a user's own browsing session. This put the actual exploitability and risk of the vulnerability into a different category. Although the finding was insufficient to qualify for a reward, it was still a valid finding and it was fixed.

The third method is the researcher attempting to "brute force" our responsible disclosure and bug bounty policies. In this variant the researchers initially come up with a single, simple issue. After being informed that the report is invalid or insufficient for a reward, they subsequently switch to the method of employing a 'dragnet' and sending us as many different findings from their scanning tools as they can, in the hope of finding a legitimate vulnerability which might be eligible for a reward.

The Shadowbrokers group publicized multiple NSA vulnerabilities' moet worden 'The Shadowbrokers group announces an auction of an arsenal of NSA software, predominantly tools to covertly infect computers.

It can get worse: quantity over quality

And then there are the really bad disclosures… One of our most notorious reports had a security 'researcher' mail us to disclose more than 10 vulnerabilities.

Now, normally this would be a great report to receive, if it wasn't for the fact that he sent over 17 e-mails, with each e-mail containing carbon copy & pastes from an automated scanning tool, useless debugging output and annotations in poor English.
While we are in favour of employing automated vulnerability scanning tools, what made these reports particularly egregious was the clear lack of understanding on the reporter's part of the tools' output, the impact of the reported results and a complete lack of any proof of concept.

On top of that, all except one of the findings were either duplicates or false positives. A usual pattern of incessant e-mails by the sender requesting 'updates' and further reporting of false positives subsequently emerged.
After asking the sender to exercise more patience and informing the sender of the results of our vulnerability analyses, the e-mails then turned angry, practically accusing KPN-CERT of lying (quote: "surely these findings can't all have been reported before!").


Subject: About Swag
From: [redacted]@gmail.com>
Date: 07/27/2016 04:10 PM
To: KPN-CERT <cert@kpn-cert.nl>

Respected KPN,

Dear i reported many of the vulnerability many of the vulnerability i got duplicate as well as some accept but never ever i get swag from you… my all friends get swags from like t-shirt and stickers but i never ever get any of the swags so dear KPN from my heart i request you to send me swag..

Hope for swag i will get soon,

Postal address,

[redacted]
NSW Australia,

M : +61 [redacted]

Cheers,
[redacted]

Figure 1: "A typical 'quantity-over-quality'-style researcher's e-mail"

In all of these three variants, the initial goal of improving the security on the internet has long been forgotten; it has solely turned into the acquisition of 'swag' or 'credit' with the minimal amount of investment of time and effort possible. In fact, they sometimes even get aggressive when this reward is denied! Oh, and the three examples we've described above…? They all came from a single individual, trying all of the approaches!

You can find our Responsible Disclosure terms and submission form on https://www.kpn.com/algemeen/missie-en-privacy-statement/security-vulnerability.htm.

The upside

Fortunately, we also get top-quality responsible disclosures at KPN. A beautiful example was a new, worried customer that sent us a hand-written letter addressed to KPN's board of directors. The letter was internally rerouted to KPN-CERT.

The customer described her arduous journey of growing from a new computer user to figuring out what the mixed-content (HTTP / HTTPS) error in her browser meant on KPN's webmail portal. After realizing the security implications and learning more about security ethics, she then decided to report it. Her letter not only mentioned the actual finding, but also extensively described how to reproduce the issue on a step-by-step basis. This, of course, constitutes an example of a great responsible disclosure: it made it easy for us to check the validity of the finding. Consequently, it took less than 2 weeks to fully remediate the finding: from receiving the report to the internal routing/steering, communication with the external supplier, testing and finally implementing the solution into production.

As this was such an unusual report, both in the way it was communicated to us (via a **hand-written** letter) and due to the potential impact on our webmail environment, we also went the 'extra mile' ourselves, by sending a hand-written letter in return.

Conclusion

So, is "Responsible Disclosure" working for KPN? The answer is a resounding and definite "yes". We have received valuable reports we might not have gotten otherwise. However, it is important to be aware of the potential for side effects and have effective mechanisms, guidelines, policies and rules in place for dealing with the various types and qualities of reports you might (and probably will) receive.

And in case you were wondering: all examples and specific images in this article really did come from the (anonymized) actual real-world reports we've received over time.

Cyber Value at Risk
business value from cyber risk measurement

Maarten van Wieren & Vivian Jacobs, Deloitte

Managing cyber risk has clearly become a serious challenge, needing attention at all levels of the organisation. This requires communication in business terms to many (senior) stakeholders, dealing with change programs linked to large yet uncertain budgets and keeping up with the latest in cyber security while new developments require constant adjustments of the attention. On top of that, commonly used methods like red, amber, green reporting do not provide a solid base for decision making (1; 2).

Based on our work with the World Economic Forum and its partners, a Cyber Value at Risk (VaR) approach was developed to measure cyber risks in a single metric that translates into business value (3). In our experience, measurement of Cyber VaR makes a big difference in cyber risk management. Discussions become focused, projects get budget based on a business case, awareness of all stakeholders grows and most important of all, it becomes clear what steps to take next.
The easiest way to see the potential impact of Cyber VaR, is to think of protecting a building in the dark with employees, suppliers, customers and others constantly entering and exiting. You would have a hard time to start planning how to avoid pickpockets entering and stealing wallets, or worse, cracking the vault. By turning on the proverbial lights, a large part of the problem goes away because the situation becomes clear and as a consequence, it becomes evident what to do. Of course the key question is: how do I turn on the lights?

Cyber Value at Risk approach

The Cyber Value at Risk or Cyber VaR approach identifies a monetary amount that a given company may lose in a year through a "worst-case" cyber incident. It serves as a cyber risk management tool that identifies the strengths and weaknesses of the cyber defence capabilities linked to business value taking cyber threat levels into account. The key strength of the approach is that the uncertainty (that unavoidably is associated with measuring each of the elements) is accumulated into the overall risk. In this way the added value of more accurate measurements (shining a light) can also be determined.

The quick scan – a quantitative cyber risk assessment and strategic vantage point

A good starting point towards getting cyber risk measured is performing a quick scan. This initial analysis is about asking the right questions, identifying available information, setting initial assumptions where required, thus forming a comprehensive picture of the risk. For this, we employ a simple conceptual model containing four elements: an organization owns (1) "Information Assets" that need to be protected through (2) "Cyber Security Controls" from abuse by (3) "Cyber Threats". In case an Information Assets gets abused, a certain (4) "Business Value Impact" materializes (see figure 1).

Level-3 finds millions of IOT devices being compromised and added to botnets.

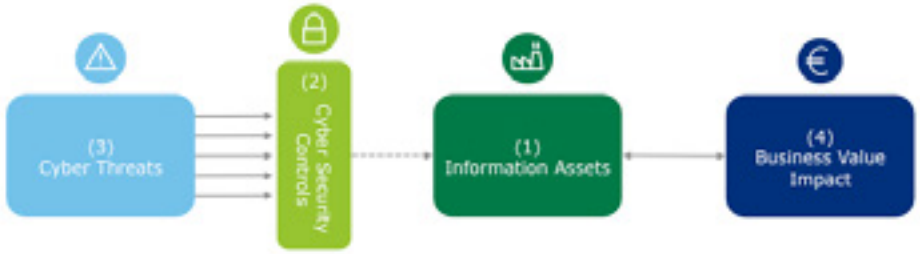


Figure 1: The four elements of the conceptual Cyber VaR model are the Information Assets an organisation owns, the Cyber Security Controls it has deployed, the Cyber Threats it faces and the Business Value Impact it incurs.

Step 1: Identifying key stakeholders

The first step in the quick scan is to identify the stakeholders associated to each of the four elements in the model. This is done by segmenting each of the four elements into more granular components until the high-level processes relevant for your business become clear. This identifies associated stakeholders. Through this segmentation, it also becomes clear what information is desired for each of the four model elements.

Example: Identifying key stakeholders

A simple example of stakeholder identification might look as follows: for the Cyber Security Controls and Cyber Threats we expect the CISO and perhaps a cyber threat intelligence officer. A slightly more challenging example is the Information Asset "Integrity", which may be segmented into "Integrity of Payments" and "Other Information Integrity", initially identifying Treasury and IT as key stakeholders.

Step 2: Collecting information and identifying information gaps

The second step in the quick scan is to identify for each model element which parts of the desired information is actually available. This often means that foremost the information gaps become clear. At least initially, it is unavoidable to use assumptions to close these gaps. These may initially be set on the basis of insights from multiple sources, including personal expertise, the many available cyber risk reports etc. For such assumptions, the uncertainty should typically be large, thus negatively impacting the overall risk.

Step 3: Engaging stakeholders and validating assumptions

After identification of stakeholders, information gaps and setting initial assumptions, follows engagement with the stakeholders to validate the assumptions. The order in this is important, to avoid miscommunication it's critical to come well-prepared, meaning that you need to translate the cyber risk concepts to concepts your stakeholder relate to. For example: involving legal means thinking through where cyber incidents may trigger litigation or fines. A valuable by-product of engaging stakeholders is that their cyber risk awareness will likely improve. Given the importance of the human factor in cyber risk management, this will help protect your organisation.

Uncertainty as risk

What's key to understand here is that measuring cyber risk is in fact measuring uncertainty. Some of this uncertainty is fundamentally unavoidable (e.g. it's unlikely you would be able to measure, let alone predict threat actor activity very accurately), while in other cases further measurement can at least partially remove uncertainty (e.g. through red-teaming exercises). This also means that you're adding value by performing a quick scan because this is expected to reduce uncertainty thus risk.

Strategic vantage point

As a result of the quick scan, you get a first snapshot of the cyber risk for the organization, a cyber-strategic vantage point so to speak. Where are the largest risks to be expected? Which capability improvements would have the biggest impact? What information is unexpectedly and critically missing? That is, you're turning on the first set of lights for the entire building, rather than for instance only in the security control room, as is often the case with most cyber dashboards we encounter.

Managing cyber risk from a business perspective

After the initial quick scan, the next step is to make further use of the newly gained insights. Strategically important activity with a large cyber risk component forms the best place to start with applying the quick scan results. This could be in support of budget approval for a cyber risk transformation program or an M&A deal, or impact assessments of new product launches. For a list of possible use cases see figure 2.

The Cyber VaR approach also adds value in regular risk management of the cyber security organisation. The principle is to continuously monitor the risk and performance levels of the organisation against the risk

68 Million dropbox accounts found to be compromised in 2012 leak.

Figure 2: Some of the many use cases of Cyber VaR categorized by four key organization objectives.

limits and performance norms on a cyber risk dashboard, so that management can intervene where needed. Structuring the cyber risk dashboard in line with the Cyber VaR approach allows for continuous monitoring and readjustment based on actual developments in cyber risk. In this way, cyber risk management can be optimised for efficiency and effectiveness.

From the perspective of the supervisory board, the situation also dramatically improves. Instead of a qualitative report on cyber risk, potentially filled with technical jargon and relying on multiple layers of interpretation, the Cyber VaR approach enables reporting on a clear metric with an unbiased root cause analysis to identify key challenges and obtain a strategic perspective on business implications.

Example: insight in return on investment of security program

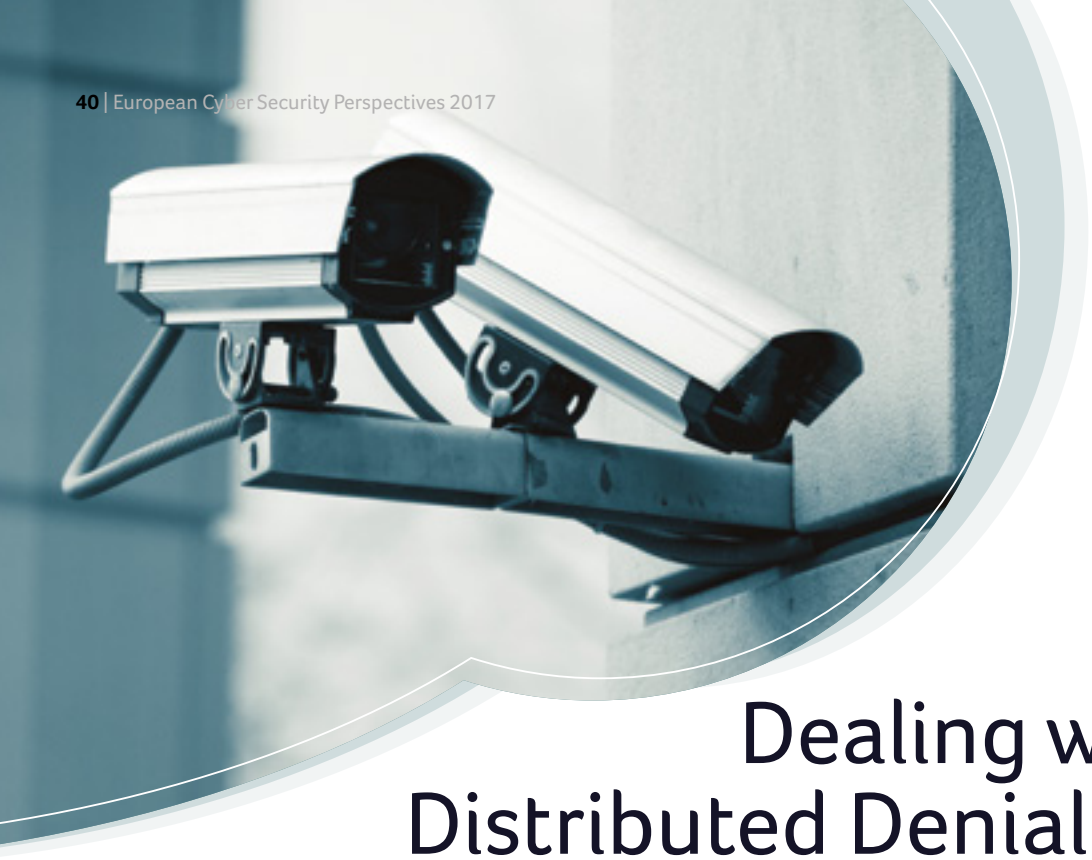
To see in more detail how Cyber Value at Risk may support strategic prioritisation and decision-making, we provide an example of an organisation plans a large cyber security transformation consisting of multiple security projects. By increasing security and reducing potential future losses, this cyber transformation will create business value. Initially, it may however not be immediately obvious how much each project will really contribute and thus which projects should receive priority. By including the investment required for each project, the Cyber VaR approach can be used determine a business case that assists in decision making. Furthermore, any changes to projects or threat landscape that will unavoidably occur can be quickly processed in the overview to enable program management to continuously steer the program towards optimal impact.

Making impact with measurements

In our experience, Cyber VaR has the potential to profoundly change cyber risk management in your organisation. It provides the tools to step away from a reactive way of dealing with cyber threats and incidents primarily based on expert intuition and focused on technological solutions and move towards a rational framework that incorporates the many relevant perspectives, enabling proactive and business oriented cyber risk management.
Although details of suitable next steps will vary by organisation given the wide range of possible applications, we are convinced that the “quick scan” approach presented in this article provides a universal starting point that works for any organization. It has the capacity to deliver a top-down, holistic perspective that captures the most relevant components of cyber risk by leveraging the perspective of all stakeholders. Most important of all, it shines a first light on the current state of your entire organisation and identifies how to make maximal business impact.

References

1. *What's Wrong with Risk Matrices.* **Jr., L. A. Cox.** 2008, Risk Analysis, pp. 497-512.
2. **Jr., L. A. Cox.** Improving Risk Analysis. Denver : Springer, 2012.
3. **World Economic Forum.** *Partnering for Cyber Resilience - Towards Quantification of Cyber Threats.* Davos : s.n., 2015.



Dealing with Global Distributed Denial of Service

Oded Gonda, Check Point Software Technologies

In October 2016 cyber security public awareness reached yet a new level, as the world learned that an army of bots hosted on Internet connected cameras was able to indirectly cause outage to well-known Internet services such as Twitter, Amazon, Spotify and Netflix. The unprecedented Global Distributed Denial of Service attack on DYN, a large DNS infrastructure company serving these well-known services, may not have shocked Internet security professionals, but it gave yet another demonstration of the fragility of the Internet grid. Fortunately, it was not as damaging as it could have been.

The Internet is a platform of innovation and inspiration. We can all invent, develop and publish our work without formal qualification or certification. Products and services are released, improved and updated constantly, often without physical contact between the manufacturer, reseller and consumer. This is very unusual in the engineering world and so far has worked fantastically well.

Security professionals realize that this unprecedented freedom to innovate comes with a risk. Many Internet connected products are not designed with security in mind and some of them contain very basic flaws that allow attacks such as the one on DYN. In the attack on DYN, Internet-connected cameras were easily accessed by hackers using hardcoded or default user credentials. Public awareness of these security oversights is rising, as cyber attacks targeting well-known services are becoming common.

As our lives are becoming so dependent on the Internet, it is time we thought about ways to protect the grid without hindering continuous innovation.

Securing the Grid

The most widespread grids in the world, alongside the Internet, are the electrical grid and the telephone grid. Both are designed for high resilience and require every devices connected to them to be certified and to meet various standards that ensure that it will not pollute the grid. Manufacturers are not allowed to sell electrical appliances or telephony equipment without the appropriate certification, and authorities of every country of the world enforce these certifications.

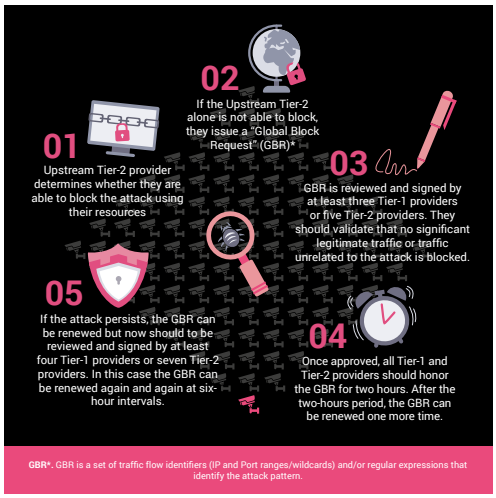
Some people suggest that a possible conclusion could be to require certification of any equipment that is connected to the Internet – ensuring that it will conform to basic security and other standards. This may end up being necessary and may develop over time, but would also be a very complicated process. It will take a very long time to agree on the standards and then implement them. But mostly it is likely to slow down the pace of innovation that we enjoy today.

A more practical solution would be for the grid to protect itself. It would require trust and entails some risks and yet it can be potentially done by co-operation of relatively small number of players, in a responsible and democratic way. Let's look at how this could be achieved.

Internet traffic control

The biggest challenge when dealing with Denial of Service attacks is how to separate malicious traffic from legitimate traffic coming from the same origin, even from the same IP address. Security vendors offer anomaly detection-based security solutions that solve this problem, often

Hackers leak records from world anti-doping agency.



very effectively. This is especially true when the attack is targeting the computing resources of the victim rather than just trying to fill their Internet link with traffic in order to slow down or prevent legitimate traffic.

And yet, if a link connecting a DDoS victim network to their Internet Service Provider (ISP) and moreover a link between the victim's ISP to an up-stream ISP is saturated with attack traffic, then it may be too late. The anomaly detection-based solution residing at the victim's end of the link or even at the ISP may not be effective, as the link is already saturated. This happens in a Global DDoS attack.

When Internet services or ISPs are not able to protect themselves using their own resources, they should be able to call for help to the companies that comprise the Internet backbone - the Tier-1 and Tier-2 Internet service providers.

Blocking attacks at source

The Internet is a mesh of networks owned by numerous companies at different tiers. Six large providers are known today to be Tier-1 (Level 3 Communications, Telia Carrier, NTT, Cogent, GTT, and Tata Communications) as due to their capacity and wide geographical reach they do not have to purchase transit agreements with other providers. Connected to them are about thirty Tier-2 providers. Within each country there are numerous other providers that are connected to these Tier-2 providers. Internet Service Providers (and sometime large Content Delivery Networks) interconnect to each other using Internet Exchange Points (IXP). The aggregated capacity of these providers is the maximum capacity of the Internet: no DDoS attack can exceed it.

As such, less than fifty Tier-1 and Tier-2 providers together have the technical capacity to stop most Global DDoS attacks (and in many cases country-level attacks) at the source. To do this, accurate attack patterns need to identified and agreed upon, but most importantly there is a need to define how this can be done in an effective and legitimate way, while maintaining data privacy.

Internet services should have internal means or cloud scrubbing service to deal with DDoS. However, if their protection is not effective because the connection to the up-stream provider is saturated with DDoS attack traffic, they should be able to approach their upstream Tier-2 provider (directly or through their local ISP), provide details about the attack and ask for help.
Upon an attack report from a downstream Internet service or ISP, a Tier-2 up-stream provider could work with the victim to identify an attack pattern. This may not always be easy, but security professionals can achieve this. Then, a scalable process with checks and balances could be implemented on these lines:

- Upstream Tier-2 provider determines whether they are able to block the attack using their resources.
- If the Tier-2 alone is not able to block, they issue a "Global Block Request" (GBR) - a set of traffic flow identifiers (IP and Ports ranges/wildcards) and/or regular expressions that identify the attack pattern. The GBR includes a ratio that indicates the desired blocking level – 1:1 for blocking all flows or 1:n for just easing the attack.
- GBR is reviewed and signed by at least three Tier-1 providers or five Tier-2 providers. They should validate that no significant legitimate traffic or traffic unrelated to the attack is blocked.
- Once approved, all Tier-1 and Tier-2 providers should honor the GBR for two hours. After the two-hours period, the GBR can be renewed one more time.
- If the attack persists, the GBR can be renewed but now should be reviewed and signed by at least four Tier-1 providers or seven Tier-2 providers. In this case the GBR can be renewed again and again at six-hour intervals.

GBRs can be enforced using a network/security device either at the Tier-1/Tier-2 providers upstream or downstream (or at the IXPs). The provider would also inform the ISPs downstream that a specific IP address is generating an attack so the IP owner could be informed. Check Point Software Technologies and some other vendors can provide today the technology required for handling GBRs.

Many attacks, such as the one on DYN, could be effectively mitigated using the above process. In case of attacks within encrypted channels (e.g. SSL), it will not be possible to isolate precise attack patterns using regular expressions within the encrypted traffic, but traffic from attacking IPs could be blocked or reduced using TCP/UDP traffic indicators that identify the communication pattern even without looking at encrypted traffic.

All too often, major policy changes only occur when a catastrophe has taken place; only then there is enough public demand, urgency and will to make concessions and drive real change. Solving Global Distributed Denial of Service of attacks can be achieved before such a catastrophe strikes. As described here, mitigating Global DDoS attacks is achievable through practical collaboration of just a few global parties. More importantly, it can be an exercise in solving a simple problem by working together, rather than standing alone.

From 01010100 01100101 01100011 01101000 T0 Talk

Mandy Mak, KPN

For some non-technical people an explanation of a computer security incident will sound like the title of this article read out loud. In this day and age almost everybody has daily interaction with connected machines, and connected machines are by definition susceptible to digital break-ins.
This article provides insights in technical security incidents by the main user of affected services, by describing some examples.

Digital crime hits the news more and more. DDoS attacks, phishing e-mails and ransomware are regular news items. But how does it work and what are the kind of computer security incidents we run into and resolve together with the colleagues 'behind the scenes' on a daily basis?

No matter what your job description is or what you like to do in your spare time, when you have e-mail, use online-banking or an ATM, surf to news pages, own a smartphone or use the internet in any other way you are a possible victim of cybercrime.

One of these standard and relatively easy attacks are phishing e-mails as they do not require someone to hack into the network. There are different ways of abuse possible when using this form of attack.
A phishing e-mail is an e-mail which is send by someone who tries to 'phish' for information. In the most common phishing e-mails the sender tries to make the e-mail look legit and does this by using logos of known companies. In the e-mail the user is being tempted to click on a link which leads him or her to a webpage (Image 1). This webpage could ask for credentials, which could be done in several ways. The attacker could have created an entire site with login or information fields.


Beste heer, mevrouw,

Zoals u misschien al weet, de online omgeving van KPN gaat veranderen Daarom stapt KPN over op nieuwe servers, om de snelheid van onze services te verbeteren.

Wat verandert er voor u als klant?
Wij blijven u dezelfde service aanbieden, die u van ons gewend bent. KPN Internet, Televisie en Bellen blijven aangeboden worden. Vo… lijke klanten. Indien u graag gebruik wilt blijven maken van… gevens voor betalingen bij te werken. KPN kan and… turen meer van uw rekening incasseren. Klik op onderstaa… verwezen naar onze website.

Click to follow link

inloggen

Let op: Wilt u uw huidige KPN producten behouden? Log dan binnen twee weken na ontvangst van deze e-mail in via bovenstaande button.

Met vriendelijke groet,

KPN Nederland
Afdeling klant communicatie

Figure 1: Phishing mails seem legitimate but point towards url's which are untrusted, like in this example where the button tricks users to go to the compromised website.

The attacker could also use clickjacking. This is only possible when the website the attacker uses is vulnerable to clickjacking, where the original website is loaded into a frame in the attackers website. The frame could be as big as the browsers screen so the user would not notice the difference. The attacker would have to use another web address (URL) in the address bar than the original URL but can use an URL which looks a lot like the original. By using the frame to load the webpage, the attacker can capture any user interaction with the original website through the frame.

Figure 2: Websites can be checked by Virustotal (virustotal.com)which uses a variety of different virus scanners.

More sophisticated phishers put more effort into it. They might send you an e-mail claiming to be from one company and after that send you one claiming to be from another.

An example of phishing is an e-mail from the telephone company stating that the banking records of the customers were compromised and that the bank would get in touch about this issue. Then they send another e-mail stating to be from a bank with the same story, an attachment asking to disclose some information and to send your ATM card to them for security checks.

Besides the often mentioned security loopholes, like phishing which is often in the news, there are more hacks relevant for users which are not as commonly known as the previous described issues.

One tab in the browser could affect the other. This could be a reason for one to choose to do sensitive tasks in a separate browser. An example of such an attack is called Cross Site Request Forgery (CSRF), where the attacker leads the victim to a webpage were certain settings are set by the attacker. The attacker has to make sure the victim is logged into the target site simultaneously. Then the attacker uses his own site to create a request on the page where the victim is legitimately logged in. By doing so the server of the legit website will think the request is made by the logged in user.

Image 3 Phishers try to steal personal data for financial gain.

You will also hear about data breaches and your data being published on the internet, this usually means you have to change your passwords.

Once a hacker gets access to a database with user records behind a web portal the hacker has access to the content of the databases and can read (and sometimes manipulate) the content. When the storage of passwords is done poorly the hacker could use these records in other attacks, because he could retrieve the plaintext passwords. Therefore the storage of passwords needs to be done securely. First off, you never want anyone to be able to read entries in databases that are not meant for their level of authorization. But even if this happens due to misconfiguration or an abused vulnerability, you would still want the data to be safe. This can be done by using hashing. Hashing is basically putting your readable text in a difficult mathematical equation and the output is not understandable. This data is saved in the database and cannot be reversed to readable text. Using strong and secure hashes it would take a super computer more years than a human life to break the hash for that password. This makes it strong enough for today's use.

You might wonder what you can do about these issues. The main thing you can do as a user is use different passwords for each account you have and be aware. If something seems off be extra cautious and check for example the web address you're browsing and search the address on the internet instead of following a link.
All of these issues can mostly be prevented by a secure server and environment. Which is why we support and enforce policies around secure coding and have every new product pentested to prevent such flaws from existing. During a pentest (which is short for penetration test) employed hackers will try to break in the product using different techniques. Every security flaw they find must be resolved to make the product more secure before providing it to customers. All network connected portals and products are tested by our hackers and everything they find has to be resolved before the product or portal can be connected for the user.

Cyber security today and tomorrow

Bruno Huttner & Kelly Richdale, ID Quantique

The need for Quantum-Safe security now

Over the last few years, the perceived threat of the quantum computer to the modern cryptographic standards in widespread use has increased dramatically. Governments and top companies world-wide are now investing in the development of a quantum computer using various technologies. This quantum computer will destroy all public-key cryptosystems, now at the core of our cyber security ecosystem. Although the arrival date for a practical quantum computer is still under debate, experts currently believe that we will see a cryptographically relevant quantum computer within 10-15 years. All our cyber security infrastructure has to be revamped and brought to a quantum-safe status. This means that , we will have to open our cryptographic toolbox and adapt our security infrastructure to new tools, yet to be defined. The transition to quantum-safe security has to begin now.

An important fact, which all security professionals have to realize, is that, although 10-15 years seems like a long-term threat, this is not truly the case. First, the transition to quantum-safe security means significantly changing our security ecosystems, which cannot be done overnight. The consensus is that at least 5 years may be required to adapt those systems to use new security algorithms and protocols. Second, most encrypted data has a long lifetime, often requiring secrecy for anywhere from a few years to ten years and above. With current progress in data storage technology, an almost unlimited amount of data can be downloaded now and stored for future decryption. This is known as the 'download now, decrypt later' or 'harvesting' type of attack. A quantum computer will be able to decrypt all the confidential information, which was previously encrypted using unsafe methods. Therefore, to prevent disruption in the long-term confidentiality of our cybersecurity systems, the time for action is right now. Finding new solutions that protect against quantum attacks should be a hot topic for everyone in the cybersecurity industry.

Current status of cyber security: an analogy

Most of our cyber security infrastructure relies on a few cryptographic primitives, such as AES, RSA and ECC for example. We can use the analogy of cybersecurity as a car (see Figure 1). The cryptographic primitives are the engine. All the other elements (transmission, brakes…) are needed to make the car run, and provide the required service: bring people from A to B in a safe, reliable and comfortable way. Some of these elements are compulsory, some other optional, to bring more comfort and ease. So far, we could consider that our engine was safe, and try to improve all the other elements, which were responsible for all the mishaps with our systems (mainly linked to implementation weaknesses). This is not the case anymore with the quantum computer, which will compel us to replace the engine itself. And we may now need different types of engines, to fit the different needs. Leaving the road and going back to cybersecurity, we now understand that we have to replace our current primitives by new quantum-safe ones.

Figure 1: Cyber security as a car The aim of cyber security is to provide a functioning secure service, in this analogy a functioning car. The cryptographic primitives are the engine. The remaining parts ensure a reliable, safe, comfortable ride. The Quantum Computer compels us to replace the engine- the crypto primitive itself.

Website of Brian Krebs hit with 620Gbps DDoS.

The new tools

Broadly speaking, we have two classes of tools at our disposal. The first class, commonly referred to as Quantum Resistant Algorithms (QRAs) or Post Quantum Algorithms (PQAs), aim to provide a drop-in replacement to existing ones, while keeping the same infrastructure as much as possible, and offering quantum-safe security. These algorithms can provide most of the cryptographic functions needed, such as signatures, authentication and encryption. However, they suffer from several difficulties. One is that, so far, the quantum-safe status of some of them is not clearly understood. We know that they do not succumb to the known quantum algorithms, which have been developed to break RSA and ECC for example. But what about new specific algorithms? Claims that these algorithms are quantum-safe forever are currently overblown. Another difficulty is that some of these algorithms are more complicated to implement, requiring for example longer keys, and more computing power. Therefore, the requirement of a simple drop-in replacement is probably not realistic. Different types of algorithms may be used for different types of applications. One could think for example of specific ones for IoT devices, which only have restricted memory and computing power. Others could be used for general applications, for transactions over the internet for example. However, doubts do remain about long-term encryption, where information has to remain secret for tens of year. This is where the second class of tools might be used.

The second class of tools is based on the physical layer, and is known as Quantum Key Distribution (QKD). QKD is based on the transmission of physical particles, typically photons, over a quantum channel. It provides a way to exchange a secret key between two users. The basic idea is that any attempt at eavesdropping on the channel, which represents a measurement of the particles, modifies their states. This change will be discovered by the legitimate users, who can then discard the exchange. Secrecy is not based on any mathematical assumption or result, but has been theoretically proven from the tenets of quantum mechanics. This key can later be used for any cryptographic purpose. QKD requires transmission of physical particles. Due to unavoidable loss in the channel, this brings up a limitation in the length of a QKD link. Commercial implementations of QKD utilize the widely available optical fibre infrastructure used in telecommunication. The typical length of a QKD channel is tens of kilometres, with a maximum about one hundred km. Free space implementations, which may lower the cost of a solution and/or increase the maximum length, are at the research stage. The length of a QKD network can also be increased by means of a trusted node infrastructure, where several QKD links are connected through safe locations, such as telecom exchanges. For example, a 2'000 km-long QKD backbone, linking Beijing to Shanghai is under construction. A world-wide QKD network can be envisaged with improved technology, as shown in Figure 2. As QKD is not based on computations, it is intrinsically quantum safe: the quantum computer has no influence on the security. QKD is already a realistic solution for long-term encryption over short distances. This distance limitation will be removed in the future, and increase the domain of application of this technology.

Figure 2: A world-wide QKD network based on satellites

The yellow dots represent the nodes. The ground nodes distribute the keys via an optical fiber network, over short to medium distances. Free-space distribution with satellites or high altitude platforms provides word-wide service.

One size does not fit all: a call for crypto agility

With the probable arrival of the quantum computer, we now realize that there is no universal primitive, which would provide perfect security for all applications. A future quantum-safe infrastructure requires different types of tools, adapted to the security target. Let us provide a few examples:

- If you are a software company, providing apps over the Internet, the first and foremost concerns are how to guarantee the authentication and integrity of your solutions. Your customers have to be sure that they are downloading and installing the right application on their device. You should plan the transition to new quantum-safe signatures, which are already well studied.
- If you are a private person, worried about Big Brother spying on your internet transactions, a so-called hybrid solution, relying on a mixture of standard solution and QRAs, would offer you better security at an acceptable extra level of constraints.
- If you are a hospital, transmitting patient medical records to a distant location, or a government office, dealing with highly confidential information, long term privacy is a major constraint. Here, adding a QKD component to your infrastructure should be envisaged.
- If you operate a large data centre, which requires daily backups of Terabytes of data from different companies between two locations, QKD is also a great alternative. In order to keep the necessary certifications you need for your customers, QKD should be implemented as an extra layer, complementing and enhancing your existing infrastructure.

The conclusion is that cryptographic tools have to be adapted to the type of data under consideration and the risk profile. The new tools, which have yet to be developed to answer the threat of the quantum computer, have to be tailored for the applications. It is also likely that the solutions of today will have to be revised in the future, once the threats are better identified. Cryptographic agility, where you can replace a given primitive by a more suitable one, will be a new requirement.

840.000 Cisco devices found vulnerable from the exploit BENIGNCERTAIN (an exploit from The Equation Group, leaked by The Shadowbrokers).

Combining tactics

The geek's lab to a better Internet

Rob Vercouteren, Stefan Zijlmans & Anne-Sophie Teunissen, KPN

Distributed Denial of Service (DDoS) attacks are increasing every day, in both size (volumetric attacks) and complexity (multi-vector). The largest attack in The Netherlands until now amounted to roughly 300Gb per second. Nowadays we regularly see attacks on our own network upwards of 250Gb per second. Due to the rapid evolution of attacks, anti-DDoS on its own is not always an effective solution. IT-Security professionals (CERTs / CSIRTs / SOCs) need to have an arsenal of tools at their disposal to counteract different types of DDoS attacks. They want to connect the dots, correlate all traffic analysis information into one single security platform, which can then be used to do a multitude of things. Good old Netflow, which has been around since the early 2000's, can help with that.

Netflow, what is it?

Netflow was invented by Cisco and introduced on their routers. It has three main advantages. These are the near real time research capacity of Netflow, the fact that Netflow is relatively easily obtainable, because it is a widely supported standard and Netflow can be used as an addition to existing services.' wijzigen in
These are:

- The near real time research capacity of Netflow
- The fact that Netflow is relatively easily obtainable, because it is a widely supported standard
- Netflow can be used as an addition to existing services

Besides this, Netflow can help with capacity management, troubleshooting, accounting, and security, but keep in mind that it cannot be used as a deep packet inspection (DPI) function, since there is only IP address- and port information in the Netflow data and because our netflow setup has a sample rate of 1 in 1000 packets for example.

Netflow is a feature and protocol that provides the ability to collect IP traffic as it enters or exits an interface. It collects metadata from IP traffic and can be used to determine the source and the destination of traffic, as well as class of service and cause of congestion. In this article we are focusing on Netflow version 5, the more easy and automatic version of the protocol. Higher versions like version 9 and IPFIX (which is based on version 9) are non automatic and need quite some configuration, based on templates which have to be pushed to the Netflow capable devices.
A standard v5 network flow is a unidirectional sequence of packets. To use Netflow you need to have control over your own routers and these need to be able to export Netflow. For collecting and analysing data you will need a powerful server with storage capacity depending on the amount of traffic transported through the network and the type of devices which will be exporting Netflow. Netflow is generally used with sampled packets, because sampled Netflow is not CPU intensive for routers and switches exporting the data. This makes the implementation less storage and compute intensive.

500 Million Yahoo accounts breached.

> Netflow is a feature and protocol that provides the ability to collect IP traffic as it enters or exits an interface.

Now we've explained what Netflow does, we will explain how it can contribute in traffic analysis.

How might Netflow help?

A nightmare for an ISP would be that its customer devices are contaminated and become part of networks of infected devices. So called botnets can be used to massively attack victims. If IT-security professionals can make use of Netflow data and correlate their findings they are able to determine which customers are affected and help them solve contaminations and malicious activity.

From a security perspective professionals can use Netflow to detect anomalies. IP address, ports and transport protocol information allows them to see what the origin and the destination of the traffic is. This way Netflow helps analysing DDoS attacks or other malicious data traffic. When it becomes clear where the data came from, IT-security professionals can inform abuse departments or in very urgent situations close the connection with the source to make sure malicious data traffic stops flooding the ISP's network.

Another advantage of Netflow analysis is that it amplifies the strengths of BGP Flowspec as a countermeasure for DDoS attacks. With the BGP Flowspec protocol it is possible to send a packet filter rule to a router via the routing protocol BGP.
BGP or Border Gateway Protocol is the default routing protocol which is used by ISPs everywhere on the internet to exchange routing information. While this is normally a manual action, propagating the packet filter can also be done automated. If the Netflow sensor is triggered by a raging torrent of packets, which is called a packet flood, it can alert the IT-security professional, who is then able to create an upstream filter to propagate to the edges of the network. With this methods the ISP's network is protected, since the flood is stopped at the edges.

Unfortunately Netflow analysis does have its limitations. An example of this is when the IP addresses of a DDoS or other malicious activity are spoofed. Spoofed traffic is especially being used for volumetric DDoS attacks. Most of these UDP based, volumetric attacks are of the amplification type: a small request is done, but the answer is huge. With spoofed traffic it is difficult to distinguish where traffic of requests came from. Essentially you will have to ask your upstream provider if they can see where the traffic came from.
Luckily there are forms of countermeasures against spoofed attacks. One of the ultimate goals would be that every ISP, upstream provider and / or peer will have anti-spoofing countermeasures in place. BCP38/84 is such a countermeasure. With BCP38/84 it is possible to filter outgoing IP traffic from within the own Autonomous System (AS). So, when traffic originates from an IP address which doesn't belong to the AS, traffic should be discarded. As an example, with these kinds of anti-spoofing countermeasures in place, the currently popular UDP based DDoS attacks from Internet of Things (IoT) devices will be less of a problem.

Future perspective

We have described how Netflow helps KPN and might help your organization with detecting and analyzing DDoS attacks and other kinds of malicious data traffic. However, Netflow offers more possibilities, like a feed to a threat intel solution. This aids IT-security professionals in the ability to correlate all kinds of data and information with Netflow. Examples could be honeypotdata, IDS / IPS, malware domains, spam domain and results of malware lab information that are all sent to a threat intel solution. Netflow data is relatively easy to parse, opening up possibilities for data exchange with others. With this approach security professionals are able to send and receive indicators of compromise and can create scripts for monitoring and alarming. Ét voilá!

What you need to know about research in 2016 on human factor in cyber security

Dianne van Hemert, Carlijn Broekman, Helma van den Berg & Tony van Vliet, TNO

Organizations are increasingly aware that cyber security is not just about technology; even in this technocratic domain the human factor maintains a crucial position. The human factor, however, is intricate. Campaigns designed to change behaviors such as weak password selection or opening e-mail attachments from unknown senders often do not have satisfying results [1]. How to realize proper cyber-behavior proves to be a challenge. On top of this, cyber criminals are creative and adapt their modus operandi to profit from weak spots in human behavior.

How does the scientific community deal with human factors in cyber security? We focus on a state-of-the-art in research on human factors of cybercrimes and victims of cyber-attacks. In order to prevent individuals and thus organizations from becoming victims of cyber threats, research needs to identify which (human) factors and particularly human behaviors foster becoming a victim of cyber criminality. This also includes circumstances in which they act.

This article shows the results of a recent literature review of scientific literature published in 2016[2]. This overview will not only provide insights on potential victim characteristics that should be further scrutinized, but also on relevant topics that deserve more attention in the (near) future.

Method

We searched for relevant articles in Scopus, a database for scientific literature. Articles were selected based on keywords[3] related to victimization in the cyber domain. The keywords were based on a discussion between domain experts and practical constraints such as the number of hits that could be processed. The search resulted in 748 articles published in (inter)national journals. Relevance of each of the articles was determined by a scan of title and abstract. Articles with a focus on human factors in cyber security were included for further analysis. This resulted in a subset of 107 articles.

The subset was examined in detail for information on human factors in cyber-attacks. During this examination 43 articles were considered less relevant, mainly because their focus was on technological issues, and in a few cases because the focus was on legislation. The remaining 64 articles were analyzed, using an a priori

(1) Mohebzada, J. G., El Zarka, A., Bhojani, A. H., & Darwish, A. (2012). Phishing in a university community: Two large scale phishing experiments. *In Innovations in Information Technology (IIT), 2012 International Conference on* (pp. 249-254). IEEE.

(2) Collecting articles was continued until October 13th 2016; articles published after October 16th are not included in this literature review.

(3) (Vulnerab* OR victim*) AND (cyber OR online) AND NOT bully*, all in title, abstract and key words

Trend Micro releases report of Dresscode malware which was found in 400 apps on Google Play.

designed coding scheme, that was slightly modified after having coded five articles.

Results

Despite carefully chosen keywords, our search resulted in 64 relevant articles, out of the initial set of 748 that focused on human factors in cyber security. The remaining articles were either fully technological oriented or generic, i.e., not focusing on human factors.

Perpetrators

Not all articles mentioned a specific attacker type. Of the 55 that did, we found different types of attacks. These include harassment (32%), phishing (20%), theft (16%), injection (7%), personal contact (5%) and other methods (20%).

The (human) focus of the attack(s) mentioned in the articles was mostly on end users (86%). Only 3% also focused on attackers targeting IT-specialists. In addition, 5% of the articles focused on attackers targeting organizations. The remainder (6%) did not describe a specific human focus.
Of the 48 articles that discuss whether the attacker is outside or inside the organization, most refer to attackers outside organizations (84%). Ten percent of these articles refer to an attacker inside the organization, and 6 % refer to both inside and outside the organization.

Victims

As for the location of the cyber-attack, the literature shows that most studies did not mention or did not focus on location (69%). Internet usage at home was the focus in 16%, and 12% focused on internet usage at the office. 3% specified internet usage in the public space.
Many vulnerabilities of individuals were found to be related to victimization of cyber-attacks. In total 85 unique vulnerabilities were mentioned. These were regrouped in 40 categories by combining related vulnerabilities (e.g. risk perception and perceived privacy belong to 'perception'). The word cloud in Figure 1 reflects the most predominant categories. Online activity is the prime studied vulnerability (21%), followed by perception (14%) and gender (6%).

Figure 1: Word cloud of categorized vulnerabilities

Mitigation

About half of all articles (53%) reported at least one way to mitigate the attack. Strategies mentioned vary from (awareness) training, to cyber hygiene, and from parental mediation to task design. The suggested mitigation strategies (21 unique suggestions) can be categorized in seven categories, by combining similar suggestions (e.g., training, cyber awareness training and cyber education are categorized to education). The categories were the result of a bottom-up process of grouping similar mitigation strategies. Figure 2 reflects these categories, and the proportion of times each category is mentioned.

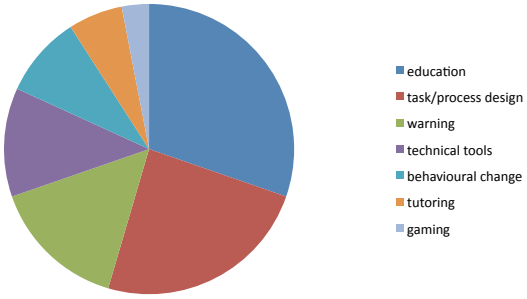


Figure 2: Pie chart of the different mitigation strategies found for human factors in cyber security

An interesting question is whether articles mention different strategies to mitigate cyber threat (for example, awareness training, technical interventions) depending on the vulnerability they find. Figure 3 shows the relations between vulnerabilities and mitigation strategies in a network visualization. Vulnerabilities are depicted in red, mitigation strategies are in green. Thicker arrows refer to more frequent relations. Many inferences can be drawn from this network representation. Not only is the most reported relation found between individual vulnerabilities and behavioural change, but also the lack of relations is notable, for example between personal characteristics and behavioural change. This implies that no articles in our database addressed both personality and behaviour change. Also the amount and strength of outgoing or incoming relations is of importance. For instance, contextual vulnerabilities are related to many mitigation strategies. And education is a mitigation strategy that is related to many vulnerabilities.

Figure 3: Network representation of vulnerabilities and proposed mitigation strategies, with vulnerabilities depicted in red, and mitigation strategies depicted in green.

Yahoo found to be scanning all 'customers' e-mail for US intelligence.

Discussion

We found that less than 10% of the articles, that surfaced as a function of keyword-based search, actually focused on human factors in cyber. This demonstrates that although the human factor in cyber is recognized as an important issue, it still deserves more directed attention. Our analysis of human factors of perpetrators show that in recent relevant studies there is an emphasis on harassment as attack, and that the studies largely focused on end users, as opposed to organizations and IT-specialists. Most attention goes to attacks having an attacker from outside the organization. However, a serious number of attacks is deployed by attackers that come from within the organization[4], and the FBI stated this number is growing[5]. These results demonstrate that in the near future more attention should go to attackers inside the organization.

Location of the attack (for example, at work, at home, in public) is often not included as a factor. However, location is relevant, not only because risks may differ in different locations, but the set of rules of behavior, among which internet usage, may differ at different locations. Future research can enrich the current literature by focusing on location.

Many victim vulnerabilities have been identified in the literature, with online activity and perception as the two most mentioned factors. However, when relating these to mitigation strategies in a network structure, we do not find a strong relation between these vulnerabilities and one or more mitigation strategies, indicating that more attention in future research should go to tailoring mitigation strategies to identified vulnerabilities.

Interestingly, none of the articles related attacker method to specific vulnerabilities. Different attacking methods may have different implications for different vulnerabilities. For example, extraversion might be a vulnerability when it comes to social engineering executed by a malicious attacker visiting an organization and having a chat with an employee, whereas impulsivity might be a more relevant vulnerability when it comes to clicking on a malicious link. Not specifying the modus operandi in a study might lead to missed results and hence to drawing incorrect conclusions. Following this line of thinking, it might be fruitful to match mitigation strategies to vulnerabilities. Future research should learn whether this is a more effective and efficient strategy to strengthen the human factor.

Finally, although many mitigation strategies are suggested or mentioned in the selected articles, these strategies are not often investigated. We suggest future research should focus on testing effectiveness of mitigation strategies, in combination with identifying vulnerabilities in specific contexts.

Our review showed that there is little attention for the human factor in scientific cyber security research. Characteristics of both perpetrators and victims are under exposed, as well as the assessment of effectiveness of mitigation strategies. In order to strengthen the human factor, aiming at the human factor to become the strongest force of the organization, more applied research focusing on the human factor is required.

(4) 2016 Cyber Security Intelligence Index

(5) Watkins, L., & Hurley, J. (2016, January). Enhancing Cybersecurity by Defeating the Attack Lifecycle. In 11th International Conference on Cyber Warfare and Security: ICCWS2016 (p. 320). Academic Conferences and publishing limited

REDteaming @ KPN

Mark de Groot & Sander Spierenburg, KPN

After three years of red teaming for KPN, we thought it would be a good time to evaluate what we have achieved, what we could have done better and, of course, to look ahead.

After the hack of 2012, KPN's new CISO put together the "REDteam" with two different tasks. Primarily, the team functions as an in-house penetration testing team. Additionally, the REDteam performs red team exercises, which are based on our assessment of current and realistic threats. The goal of red teaming is to continuously assess the readiness of KPN to withstand realistic scenario-based attacks. These scenarios can involve human, physical and technical elements. At the start of a red team exercise, we decide on whether we are going to simulate criminal activities, insider threats, state actors, activism and/or corporate espionage.

The REDteam consists of people with very different backgrounds and areas of expertise. Some are relatively new to the organization and some have a long working history at KPN. This mix of people ensures we know enough of the organization, while having a good supply of fresh ideas. The technical backgrounds of the members also vary, ranging from a development background to members that used to work in network and system engineering. Some have hardware hacking experience and others have social engineering experience.

When the REDteam started, red teaming was a fairly new concept in the telecommunications industry. Penetration testing was more common and most of the people we met, thought of us as a penetration testing team, somewhat similar to a quality assurance team.

Not exactly. There is a great website about red teaming at http://redteamjournal.com. It has a section with the "laws of red teaming" that is definitely worth checking out. Red teaming Law 15 perfectly reflects our experience over the past few years:

RTJ Red Teaming Law #15: The apprentice red teamer thinks like the attacker. The journeyman red teamer thinks like the attacker and the defender .The master red teamer thinks about the attacker and defender thinking about each other. Hire an apprentice to model an unsophisticated adversary. Hire a journeyman to model a sophisticated adversary. Hire a master to model the system.

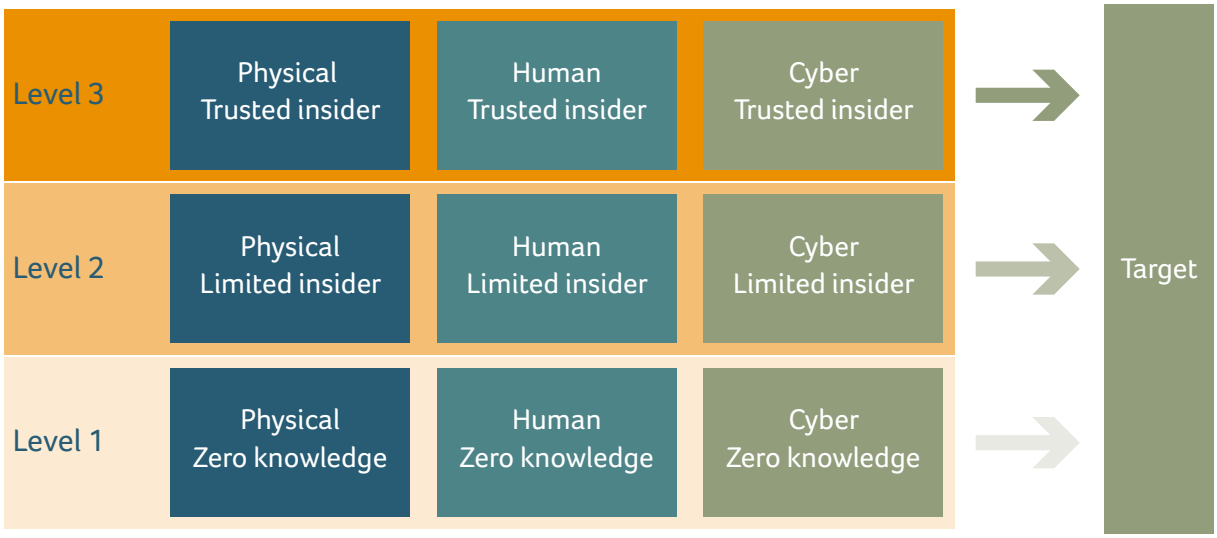
So in 2013 we were, roughly 7 guys of multiple disciplines in a team eager to "own all the things at KPN". We learned that not everybody was aligned with the definition and concepts of penetration testing and certainly not with red team exercises. In traditional penetration testing the scope and methods are mostly pre-defined, whereas a red team exercise exceeds those boundaries. Our adversaries don't abide by boundaries, so why should we? We are the friendly adversary. We hack you and then tell you about it. It's important to understand that red team exercises still however follow a detailed plan, stay within the law and are explicitly approved by our client, in this case our CISO.

The steps and rules of engagement

How can you fit red teaming in a model and where do you start with a redteam exercise? We suggest that it can start at various levels. The levels determine how much inside knowledge you need to have in order to perform

the exercise within a certain budget. Starting with zero knowledge is more expensive than starting form a trusted insider level.

These levels can be categorized into:
- Level 1: Zero knowledge about the organization/ target;
- Level 2: Limited knowledge about the organization/ target, the insider;
- Level 3: Full knowledge about the organization/target, the trusted insider.



(A red team exercise challenges a company on their physical, technical, and social defenses by simulating criminal activity, insiders, state actors, activism and/or corporate espionage.)

After the initial level is determined, the attack will be broken up into three stages.
- Stage 1 is Reconnaissance, Weaponization and Delivery.
- Stage 2 is Exploitation and Installation.
- Stage 3 Command and Control and Actions on the Target. The stages are based on Lockheed Martin's Kill Chain and the REDteam's "Dont's" during a red team exercise. The table below describes the actions from the Kill Chain with the methodology we use:

Stage	Action	Methodology
Stage 1	Reconnaissance	Harvesting Email Addresses, Social Networking, Passive Search, IP Port Scanning
	Weaponization	Developing Exploit with Payload Creation, Malware, Delivery systems, Decoys
	Delivery	Spear Phishing, Infected Website, Service Provider, USB
Stage 2	Exploitation	Activation, Execute Code, Establish Foothold, 3rd party Exploitation
	Installation	Trojan or Backdoor, Escalate Privileges, Root Kit, Establish Persistence
Stage 3	Command & Control	Command Channel, Lateral Movement, Internal Recon, Maintain Persistence
	Actions on Target	Expand Compromise, Consolidate Persistence, identify Targets, Data Ex-filtration

REDteam Don'ts

During a red team exercise there is a possibility of equipment or systems being damaged. For example, breaking in a door could permanently damage the lock. There are also types of damages that you would want to avoid, for example mentally traumatic experiences for any people involved. The minimum "don'ts" are, but not limited to:

- Harm people physically and/or mentally
- Steal laptops from employees;
- Activate fire alarms;
- Change valuable information on systems;
- Perform a (D)DOS on systems;
- Access out of scope systems without permission;Physically damage property/buildings;

Despite the defined scope of what the REDteam does and how, the role of the REDteam has changed over time. We dug around, found vulnerability after vulnerability and took over system after system. As we were the ones who found the vulnerabilities and reported them, people turned to us for guidance on how to fix them. The workload for our small team became very high, when on top of extensive red teaming we tried to help fix the issues.

KPN has a blue team too! For over 21 years, long before there even was a REDteam, KPN has had an incident response team called KPN CERT. This doesn't mean that offloading it to them is going to help solving these issues sooner. A commonly heard comment is "we know this already". It's our job to work together with them to solve these issues. Not to do this by ourselves. We need to teach each other on tactics and get better. It's important to remember that it's not about proving the vulnerability, it's about training the detection and response. A close interaction is needed between both the red and the blue team.

What we have learned and improved

From an organizational perspective:

- We need to be able to determine when something is simply out of the ordinary and when is it an incident
- Constantly ask ourselves: "Are we monitoring the right events?"
- We need to reevaluate our threat landscape from time to time and we need to have the right procedures in place to identify the attackers in case of an incident
- We constantly need to look for specific indicators of compromise instead of digging through haystacks
- Only when the REDteam and the blueteam are playing the game, the security maturity level of an organization will grow.

From a REDteam perspective:

- Use scenario's that reflect real life situations only
- Only do exercises that benefit the organization
- Determine our strengths and weaknesses and profile these for certain scenarios.
- Develop advanced training plans based on your weaknesses
- Make sure you have the right tools for the exercise and don't be scared to improvise

Our in-house REDteam is continuously finding new ways to hack the organization, like a persistent adversary. This is what we do every day. This can cause apathy and annoyance with management and operations alike. To the customer, a REDteam report often comes across negative - as criticism of how they do their work, as delay of a roll-out to fix blocking items, as extra costs that weren't budgeted. It is a challenge to create the mindset within an organization that REDteam findings are a service to the organization and its customers. With our model red teaming becomes more scalable for different types of organizations and budgets. The model gives clients the ability to choose a redteam exercise that fits within any budget.

After 3 years of red teaming we combined our knowledge and lessons learned into a red teaming model that fits many budgets and purposes. Since this year we can also perform commercial red team services. We encourage organizations to try red teaming instead of traditional pentesting to have another view on vulnerabilities within your organization.

DYN-DNS hit with DDoS forcing sites such as Netflix to go offline.

Managing Mayhem

Maarten Bodlaender, Philips

Mayhem is a computer AI specialized in fully autonomously hacking systems. Just let that sink in for a moment... At the 'Capture The Flag' hacking competition during DEFCON 24, a computer running Mayhem almost beat two of the world's top human hacking teams. The Malware-as-a-Service industry will love automatic exploit generation. Services, devices and software can be bombarded by tailored attacks created by autonomous robot software, almost immediately upon going live.

Hacking AIs are the natural evolution of pen testing tools, where binary analysis techniques like fuzzing and symbolic execution are used to detect software vulnerabilities. In the past years, white-box fuzzing tools like Sage have grown in sophistication, to the point where DARPA felt that AI-controlled, fully automatic hacking & patching might be in reach.

The DARPA Cyber Grand Challenge: hacking AIs

In 2016, DARPA organized the finals of the world's first all-machine, no human, hacking tournament: the Cyber Grand Challenge. Computer AIs were tasked to autonomously generate exploits and patches for provided binaries.

Seven AIs participated, including the AI called Mayhem from start-up For All Secure. Mayhem won the finals, gaining the right to participate in the prestigious DEFCON CTF tournament. This pitted Mayhem directly against fourteen of the world's best human hacking teams.

In Chess and Go, computer AIs got stronger over the years, eventually defeating all human world champions. A similar path can be expected for CTF tournaments, and indeed Mayhem finished last, hampered by last-minute compatibility issues. Even so, Mayhem proved competitive. It seems only a matter of time until hacking AIs are better & faster at hacking than human specialists (unless they have equally advanced tooling).

High speed hacking

The advantages of hacking AIs are their superior speed and tireless approach to finding and exploiting weaknesses. They can analyze more code in less time

Fuzzing & symbolic execution

Fuzzing is a way to test programs by feeding them random, often invalid inputs. The program is then monitored for exceptions such as crashes. Fuzzing usually only finds simple faults, but is fast and generic.

Symbolic execution uses symbolic formulas to describe all possible inputs. It transforms formulas with each program step, thus determining dependencies between inputs, program steps and conditional branches. Symbolic execution is theoretically very powerful, but in practice quickly overwhelmed by path explosion in large programs.

The first hacking AIs seem to alternate these approaches in an attempt to mitigate the individual limitations.

than humans can. Check out the following example from the contest:

15:04 binary released
15:34 first crash discovered by Mayhem
17:00 reliable full exploit generated

Imagine your organization releases a new app in the App store, and within 2 hours attackers have fully automatically generated an exploit! Mayhem may just be a proof-of-concept on a toy system, but it is a wake-up call that high-speed exploit generation is real.

Automated exploit detection tools

Equally powerful exploit detection needs to be part of the standard development cycle, to ensure that the code contains no vulnerabilities that hacking AIs can exploit. Automated analysis of software for vulnerabilities is computationally intensive. The state-space of large programs is too large to exhaustively search, and hacking AIs make heuristic choices to meet time constraints. Different hacking AIs make different choices, and thus find different vulnerabilities. Even with vulnerability detection included in the development cycle, a different AI or human expert can often still find vulnerabilities.

Revisiting Kerckhoffs's principle

According to Kerckhoffs's principles, a good cryptographic system remains secure even if the enemy has a copy. Unfortunately, once hacking AIs like Mayhem get a copy, it can take them less than two hours to find an exploit. As our ICT infrastructures are largely mono-cultures, we typically copy the same binary on many devices, making it easy to get a copy. Until vulnerability-free software can be created, most systems today are not meeting Kerckhoffs's principles.

One way to address this problem is to ensure that all binaries are different, in a way that analyzing one binary doesn't allow a hacking AI to create vulnerabilities for other binary. Experiences with diversification techniques like fine-grained address space layout randomization show that this complicates the work of attackers. However, many diversification techniques are defeated by exploits that manage to expose the run-time binary and/or find common aspects in the binaries.

Private Arithmetic

Philips' contribution to diversifying software at a fundamental level is to give each software instance its own private and secret number representation and corresponding calculation system. The software uses this secret number system for all calculations on sensitive data. The expectation is that symbolic execution on these systems will be impractical due to the complex data space. So-called Private Arithmetic generators are capable of generating a near infinite number of secret number systems, such that no two instances are alike.

The secret number systems generated by the Private Arithmetic generator are based on table driven arithmetic that replaces traditional ring operations like additions and multiplications by other basic primitives. These new operators use the underlying algebraic properties of the addition and multiplication in a ring to replace them by other operations in different algebraic structures. Addition and multiplication disappear. Therefore it is not possible for the attacker to study the arithmetical properties of these operators: they no longer exist in the code. They are replaced by new operators that can be customized to be no longer commutative or associative. Only the final result provides the correct solution to the sequence of operations.

Designed to be difficult to reverse engineer, the Private Arithmetic generator is ideal to hide confidential algorithms with their own number systems, and makes it hard to determine which secret number system was used by just scraping some data from memory. This gives hacking AIs a new challenge for every system they try to compromise, limiting the scale of their attacks.

Security by design

In summary, high speed hacking and high speed exploit generation by fully automated programs now exists. Binaries that are publicly released like in app stores will be automatically scanned for vulnerabilities. Organizations need to integrate security into their development processes and software designs, to avoid being hacked directly upon product release by a diligent AI. Philips is working on Private Arithmetic generators that deprive hacking AIs from an easy input to work on.

Internal Threat Management

Nick Mann, Nick Mann Associates Ltd & Chairman of GSMA Fraud and Security Advisory Panel

Introduction

History and recent surveys/statistics/cases teach us the unpalatable truth that a frightening percentage of our employees, managers, senior executives and even board members have the potential to go 'bad'. If one asks the question: Which of the crimes that could affect my business would be easier to commit from the inside? The answer unfortunately, is: *All of them!*
Belief and faith in those that work for you is vital and to be encouraged – unquestioning or blinkered trust is not. Knowing your loyal staff and protecting them from the disloyal will reinforce that trust and ensure it is returned.

Cyber security seminars and conferences abound but sadly the human aspect of internal threat rarely features very prominently on the agendas. The focus seems always to revolve around technical solutions when the issue is principally a people problem. We have yet to see a case involving theft or manipulation of data *perpetrated* by a machine.

In this article we will examine and recommend approaches to prevent, detect and deter this most insidious and serious business risk.

Note: There is a wide range of departmental structures within which the disciplines of fraud & investigations sit. The merits or otherwise of which functions sit with whom are not as important as the existence of a properly trained, resourced and equipped fraud, security & investigative function that has within its responsibilities all types of internal attack. For simplicity we will refer to this as the ***Fraud, Security & Investigations Function (FSIF)*** *throughout.*

Threat Assessment & Measurement

The starting point for improving the resilience of your organisation to internal attack is to establish where high threat potential exists. Thus it is essential to conduct a comprehensive Internal Threat Review encapsulating the exposure and management of all Fraud & Security issues across the business. Internal Threat Assessment & Measurement (ITAM) is a type of analytical measurement approach designed to clearly determine where high risk (Threat Quotient) posts exist within a business, thus enabling true implementation of targeted and proportional controls.

ITAM style exercises identify threat types by role and measure (in detail) their severity by examining all elements of **opportunity, ease/probability and impact**.

All role types (and role type families) across the organisation should be identified with the assistance of HR. A volunteer should be selected from each role type (or family) and they are then interviewed by experienced threat management professionals. It should be clearly explained to each interviewee that the interview is an objective examination of the threat potential of their role not about them personally. Once the interviewer has established exactly how their role is performed and how it relates to other roles and parts of the business and the controls to which it is subject, the interviewee is invited to explore with the interviewer how someone with malicious intent could pose a threat to the business.

The roles are scored during this examination using the following methodology:

Internal Threat Quotient Scoring Mechanism:

Role Opportunity

A. Level of Authority B. Ability to Supervise C. Level of Supervision Imposed
D. Access to Business Element (e.g. Systems, Network, Client Monies etc)
E. Ability to Change, Divert or Manipulate that Element

Threat Reality

A. Ease of Attack B. Detection Likelihood

Threat Impact

A. Financial Effect B. Business Element Impact C. Damage Limitation / Recovery Possibility
D. Client / Investor Confidence E. Market Reputation

Once the principle threat for that role has been determined* the above 12 elements should be scored individually within a designed range and a calculation algorithm applied to determine the Threat Quotient.

*External threats are included insofar as high internal collusion potential exists.

A simple ITAM type score sheet:

Role	Level of authority	Ability to supervise	Level of supervision imposed	Access to Business Element	Ability to change, divert or manipulate	Total Score		Results
Threat	Ease of Attack	Detection Possible				Totals	+	Results
Threat	Financial Effect	Business Element Impact	Damage Recovery / Limitation	Customer / Investor confidence	Market Reputation	Totals	X	Results
							Total	
							Threat Quotient	

These threat types having been identified and measured, the resilience of the organisation to such events and its ability to manage them is scrutinised. The resultant Threat Quotients give the principle threat and threat potential for each role type within the organisation and will determine exactly where and how you apply resource to the controls we will discuss later.

Resource levels will determine where the high threat criticality line is drawn in the Threat Quotient scores but it would be prudent to ensure that at least the top 10 or 15% roles attract most attention in terms of controls in particular pre-employment security screening (vetting). Equally important to the objective determination of where threat potential lies is to examine why it may manifest itself.

Motivation for Internal Attack

Motivation is never really considered when applying controls. This may be a mistake as there are certainly areas where understanding major attack causation could enhance objective prevention and detection as well as identify subjective predisposition to attack.

Studies that have examined the breadth or depth of motivations or their potential relevance in internal fraud/ crime management are very rare.

PoisonTap device (Raspberry PI + PoisonTap software), when plugged into a PC, siphons cookies, exposes internal router & installs web backdoor on password locked computers.

November 13 16

412 million accounts of 18+ dating sites from Friend Finder Network INC are found to be compromised.

Variant of Mirai botnet takes 900K routers of Deutsche Telekom offline.

Types of Motivation:
There are probably three major fields of motivation (with some cross over):

1. Greed
2. Need
   a. Debts (self inflicted)
   b. Debts (true necessity)
   c. Targets / Survival / Concealment of Error/ Deficit
   d. Coercion /Under Threat/ Blackmail/Kidnap
   e. Addictions: Alcohol, Drugs, Sex, Gambling
   f. Despair
3. Miscellaneous
   g. Malice / Revenge (Existing)
   h. Malice / Revenge (Responsive)
   i. Competitive Sabotage
   j. Peer (or Family) Pressure / Loyalty
   k. Psychological Problems
   l. Excitement / Entertainment / Self-Aggrandisement / Ego
   m. Idealism / Terrorism
   n. Stupid / Naive (i.e. no deliberate motive)
   o. Mole / Cell (i.e. only purpose to employment)
   p. Industrial Espionage
   q. Altruism – 'Robin Hood' syndrome

A lot of these are known to us and we will commonly see cases but it is worth recording some examples and explanations of the less obvious / common to illustrate that all are dangerous if ignored:

2d - a bank cashier helped thieves steal £150,000 after they threatened to uncover her as a bigamist

A finance director was convicted after stealing £85,000 by using the company credit card to fuel his sex addiction and pay for brothel visits and live internet sex shows. Thus falling into **2e** category.

2f is separated from other compulsion and debt categories where, for instance, desperation for urgent costly medical attention, has driven otherwise honest individuals to commit crime. The prime characteristic of this motivation is that the money needed is usually the limit of the proceeds of the crime. As with many of the categories stated, there will be cross over between **2b** & **2f** but the latter is often a long term situation linked to a debt cycle and there is not normally a definite correlation of proceeds to need. There is also a similarity to **2d**, the delineator is that in **2f** there is no malicious threat behind the need motivation.

3a, 3g, 3i are exemplified by the case where alleged terrorists were taped discussing 'targeting utility companies by using recruits with inside knowledge to cut off electricity, water and gas power supplies across the country'. **3i** has other recent public examples including employee/contractor placement to steal secrets from an electronics firm.

3d has a recent example of a mother who spent money stolen from her employers to "keep up with the Joneses"
An unusual example of **2a** and possibly **2e** is the case of the employee who admitted stealing £200,000 from her employers to fund her purchase of 18 show-jumping horses.
Probably the most famous examples of **2c** is the Barings case as well as the more
recent case of unauthorised trading by a French Bank trader, both with massive losses for their employers.

A personal assistant at an accountancy firm convicted of fraud after court heard that 'she was obsessed with being the centre of attention' and the judge said "You used the proceeds to buy friendship and affection". This would appear to fall into the self- aggrandisement category of **3f**.

3k is rare but there is a recent case where an individual gave part of the £370,000 proceeds defrauded from his employer, to charity.

Jill Stein asks for recount of votes in Wisconsin due to fear of manipulation by hacks.

Vulnerability in Realtek chip allows headsets connected to compromised devices to be used as microphones.

Motivation Linkage:
It is possible to link most motivations under 4 main Risk Factor Indicators (RFI's):
Financial – 1, 2a, 2b, 2e, 3c, 3j
Compulsion – 2c, 2e, 2f, 3a, 3b, 3d, 3e, 3g, 3h
Secret / Embarrassment – 2d
Illogical – 3f, 3i

There are opportunities to detect these RFI's in both subjective and objective controls before and after employment.

Making the connection between why employees attack us and applying controls respectively has to be more effective than simply having controls based on how attacks are perpetrated. That said, this is not something that is likely to provide easy wins in the short term but what is certainly evident from above is that it warrants further study.

Controls

Let's take the most difficult and most important of these first:

Vetting (Pre- employment Security Screening)

This is the principle tool in the internal threat prevention armoury. Sadly it is rarely applied sufficiently or correctly. Even those organisations that do apply vetting controls beyond asking for references usually do so in a very unscientific, costly and ineffective fashion where all roles are treated the same or checks levels are based on salary or seniority. Neither of the latter is particularly relevant in determining which are key risk roles.

To spot Risk factor Indicators (RFI's) will necessitate detailed 'checks' and realistically we can only conduct that level on a small percentage of roles. Thus it is necessary to decide which posts have high risk or criticality. The ITAM type process described earlier whereby we can measure attack opportunity, ease and impact for each role (or role family) is obviously perfect for this purpose. It enables proportional (most common legal/regulatory test for 'intrusive' vetting) and targeted vetting controls based on the Threat Quotient scores determined for each role.

Vetting is a huge subject in itself and it is important to understand the legalities within your jurisdiction. A hierarchical (related to criticality/Threat Quotient) system of vetting should be introduced for those roles which represent high internal threat potential and such roles should be subject to enhanced checks (see below). If there are high Threat Quotient roles requiring enhanced checks that have unmanageably high intake numbers (e.g. Customer Services), random sample candidates should be selected for such enhanced screening. A policy describing this commensurate approach is required.
It is paramount that any vetting scheme is within the law and based on 3 key principles:

- **Voluntary:** All applicants and potential applicants must be made aware of the level of screening from the stage of post advertisement onwards and their consent obtained either by inclusion in the Contract of Employment or a separate document. The subject may decline to offer such data or decline to obtain such data; in this case the future of the recruitment or promotion process in respect of this individual must be carefully considered

- **Open / Overt**: The subject is entitled to know of the existence and operation of the policy, the data sought and the sources used. Moreover, the subject must be given the opportunity to answer/explain any 'issues' discovered

- **Proportionate**: The level and intensity of the screening will be directly proportional to the criticality of the role concerned and be demonstrably proportionate i.e. by application of the appropriate Threat Quotient level accorded and/or application of role access levels as described in the Information Classification Treatment control below.

The type and extent of checks you conduct will be determined by the law in your country. There are some issues which should never form part of any screening e.g. ethnicity, sexuality.

In order to detect RFI's we discussed earlier, it is important to ensure the following points are covered in a vetting exercise:
- Is their application real?
- Are their qualifications (if true?) consistent with their career path to date
- Is what the subject does, or has done:
  - A Secret (e.g. criminal record, a habit or extra-marital affair)?
  - Expensive to them?
  - A risk because of how often or how much they do it?
  - Embarrassing if revealed / discovered?
  - A risk to them or anyone else?

It is not only possible to screen for motive presence but also feasible to discover any propensity or capability for fraudulent/criminal activity. **The Key is to look for the unusual or the inexplicable.** The analysis for RFI's must take into account all subjective as well as objective factors e.g. too much money can be as much an RFI as too little and one man's gambling addiction is another's hobby. An example:

- A £100 a week gambling habit may well pose a risk for a clerk who is only to earn £20k pa (possible addiction)
- It is not a risk for a Director who is to earn £100k pa (probably more a hobby) – unless…..
- He has kept it a secret from his wife?!!

NB. Such detailed (Gold Standard) Screenings must be conducted by experienced investigators. This is particularly important in the interviews and analysis of data e.g. bank accounts.

It is not feasible to spot some motivations prior to employment often because this is a first time offence and the employment is itself causal to the Motivation **(3a above**) and presents the opportunity and, if necessary to the miscreant, the rationalisation. Almost all motivations would become 'vettable' if we applied repeat vetting (on High Risk posts). Repeat vetting would be particularly successful if linked with Fraud Monitoring / Detection and other objective post employment controls. Whether the motivation or RFI is 'vettable' or not – all motivations and the resultant product, are controllable. Moreover, it should now be obvious that each control is better applied with knowledge of the range of Motivations and their RFIs.

Some other controls not mentioned elsewhere:
Education and Training – Security Awareness Programme
Communication and Intelligence
Audit Trails, Logs and Reconciliations
Access (Logical & Physical) Controls – particularly for High Risk Posts
Complete Range of ICT Security Policies
Information Classification & Treatment
Foster Good Industrial Relations
Realistic Target Programmes
Measurement, Reporting & Sharing
Segregation and Compartmentalisation

Reporting & Detection

We have examined the RFIs that may exist in the subjective sense related to an individual's motivation. Such indicators do, of course, also exist in the data we hold, produce or process.

There have been normal business fraud enquiry tools for internal fraud in existence for some time but it is only in the last few years that we have started to see the emergence of data engines that monitor for and detect such issues. Advances in accessible data warehousing and the emergence of 'big data' have opened up possibilities and exciting work is going on in development to use big data with prescriptive and descriptive analytics.

Nevertheless the fact remains that, unless controls are very mature, a large proportion of internal attack is detected by reports from other employees.
As such this route must be protected, nurtured and developed. There are a couple of simple actions that will dramatically enhance this invaluable intelligence / evidence source:

1. Duty to Report Policy & Process

This should make it **mandatory** for all staff to report suspicions of dishonesty, malpractice or security compromise to the FSIF. This is separate to any whistle-blowing process but can be made part of it. Thus whistle-blowing becomes mandatory not merely voluntary and the employee is encouraged to make the report to the FSIF (anonymously if they wish). The 'Duty to Report' should be included in induction training along with fraud & security awareness and all staff and newcomers should be made to sign as part of their Contract of Employment.

2. Investigative Engagement Policy & Process

The lines between evidence collection and disciplinary action are often confused within organisations. Thus only appointed and trained investigations staff (i.e. FSIF) should conduct internal investigations. There should be no line management or HR participation or interference in evidence collection or interview process. This is to ensure integrity of evidence collection, independence and to remove any possibility of conflict of interest. Moreover, it engenders trust in the staff that their concern will be handled by professionals who will provide protection for the 'whistleblower'. Similarly, investigators should not be involved in the disciplinary process (including disciplinary or exit interviews) or decision on punitive action. Investigators should only participate in any recommendations on likely success of prosecution or necessity for police involvement. It is imperative that the FSIF investigators are given this investigative mandate which should be endorsed by the Chief Executive / President / Chairman.

Note: The role of Internal Audit is sometimes given the role of investigator in 'normal business fraud.' This is not ideal and can be a source of confusion where a Fraud & Investigation function exists. Whoever is given the responsibility it should be clear what 'investigation' means i.e. the collection of admissible evidence, and the requisite training given and expertise recruited. Certainly the 2 functions are necessarily symbiotic.

Often staff state during reviews that they would have reported previous internal incidents had the above policies and facilitation been in place. Moreover, where such policies have been introduced there has been a significant rise in the number and quality of such reports.

Response, Investigations & Deterrent

- The objectives of any investigation should be:
- To provide a deterrent
- Collect admissible evidence & ensure the integrity of same
- To recover any lost assets, monies
- Inhibit or stem any further losses
- Minimise disruption to business
- Defend business reputation & retain customer and investor confidence
- Prevent/reduce harmful effect on staff morale
- Enact immediate operational damage limitation

Report Lines

Because of the possibility of investigation of Senior Management and the Executive / Board itself as well as other key directorates such as the Finance department, it is important to give some thought as to the report lines of the Fraud, Security & Investigation function (FSIF). The key objective here is autonomy (as well as the mandate/ authority discussed earlier).

As such it is important for the FSIF to have a non-functional (i.e. not one of the key business functions such as Finance, Technology, Customer Services) report line for the following reasons:

- Many aspects of its work are, of necessity, across all elements of the business. Thus being owned by any functional directorate is not beneficial in gaining cooperation and acceptance from any one of the main functional directorates, if part of another
- To enable objectivity of engagement across all units of the business and to be listened to, respected and trusted, it must be seen to have no alternative interest or agenda other than its own objectives
- Internal security and investigations can be centred on any function at any rank – investigating one's manager or colleague is neither practical nor desirable. This is more likely in a functional directorate such as Finance, Technology and Customer Services, as these are where the most opportunities for internal compromise exist
- Some functional directorates may be more problematic than others in terms of achieving the objectives with applicable and relevant KPI's: -
  - Finance:
    - Less understanding of the unquantifiable value of deterrent and prevention and reliance on fraud figures/percentage when low figures can mean either excellent Fraud Management or, as likely, failure to detect
    - Lack of understanding of non-financial threats, impacts or losses
    - Financial Reporting Fraud conflict
  - Technical:
    - Over reliance on technical solutions and defences
    - Lack of understanding of non-technical attacks

Hence there is a necessity for independence from these directorates. Options include: direct report to CEO / President / Chairman, Legal & Regulatory Director, Company Secretary or possibly even a Non-Executive Director or the Audit Committee.

It is also key to the success of any FSIF, that their direct report should be one who personally has empathy for the work in which they are engaged.

Future

Unquestionably the greater development of 'big data' internal fraud detection engines coupled with more focus on predictive behaviour linked to Risk Factor Indicators, will have a dramatic impact on early detection capability but we must have the resources, expertise, ability and desire to respond and manage the product.

This article is an abridged, updated and amended version of 'Internal Threat' a chapter contribution by Nick Mann to the book: 'Demystifying Communications Risk' – M Johnson - published by Gower Publishing.

Every CERT must continue to train

Wesley Post, KPN

Working in a Computer Emergency Response Team (CERT) requires a lot of skills and expertise. Some are technical like hacking techniques or forensic research. Some are more 'soft' skills like communication, or writing an article for an annual report. Often these skills are needed in different situations and stress levels.

It is important to be prepared for everything that needs to be handled by a CERT. Since this is quite a broad spectrum of activities the only way to keep the skills on the right level is to share knowledgeand perform exercises on a regular basis. Within KPN-CERT we use OTO for that.

Introduction

OTO is short for Opleiden, Trainen, Oefenen. Those are Dutch terms that roughly translate to Educate, Train and Exercise. OTO is a term which has its origins in public emergency organisations like the fire department or ambulance service. In those organisations OTO is used on a regular basis to exercise emergency situations as realistic as possible. In this way fireman or ambulance staff are prepared for a real-life emergency situation when it occurs and know what to do in these kind of situations. From KPN-CERT we see a large overlap between the public emergency services and the role of a CERT within a company. In both cases teams need to know what to do and need to make decisions in a stressful situation with little or no time having only their knowledge and experience as their guide since every situation is different.

Educate

Educate (Opleiden, the first O in OTO). The goal is to increase the knowledge level of the CERT members. To decide which education is needed we first determined a baseline of knowledge and skills required for CERT team members. Since each team member will have a different level to start with, individual choices are made to determine which trainings are required to grow to the desired level.

Examples of trainings are the SANS trainings like GIAC exams/certifications for incident handling and forensics or the python programming language.

Train

Training (the T in OTO) is used to share knowledge which is already available within the team. Since each team member has a different (professional) background we all bring our own specific knowledge. Of course it is useful to share this knowledge with the rest of the team and benefit from this. This is usually done in short sessions, generally an afternoon, where a team member tells about a subject and combines that with some hands-on practice.
Examples of knowledge sharing sessions we had so far: Malware analysis, hacking and in-depth networking.

> It's important to be prepared for everything that needs to be handled by a CERT. Since this is quite a broad spectrum of activities the only way to keep the skills on the right level is to share knowledge and perform excercises on a regular basis.

Exercises

Exercises (Oefenen, the second O in OTO) are used to actually practice common situations to make sure we are prepared for them when they happen in real life. The most common thing we do for practice are forensic challenges. The field of forensics is overwhelmingly huge. It is simply impossible to know everything. What we can do is practice situations where we want to build or maintain capabilities. In our case this includes disk, network and embedded device forensics.

Besides these technical subjects this can also include practicing a process with a tabletop or an actual simulation of an emergency situation. In time these types can vary from a few hours up to a few days.
Being a CERT we can not afford to have the team completely unavailable because of an OTO session, so any session lasting longer than a few hours will have to be done multiple times so the team can be split over de different sessions.

Since we have just started with OTO we did not have a exercise session yet but plans include Major Incident response and DDoS mitigation.

Two step planning

Actually planning the sessions turned out to be a two-step process. The first step is to have a generic year plan. In our case a month-by-month planning stating what type of OTO we want to do. This can be a forensics challenge, training, a tabletop exercise or a simulation. The specific contents are not yet defined at this stage.

Defining the specifics of each session is a continuous process throughout the year. This is where topics are chosen, challenges selected and the actual session is planned. This is usually done a few months ahead to allow the leader of the session to do preparations. These preparations range from creating a presentation to testing the challenge.

The tabletop and simulation practices need a bit more time to prepare, in these cases half a year should be considered as a minimum.

Example year plan

This is an example of a generic year plan. You can clearly see the focus on technical exercises (practice) and knowledge sharing (training).

Month	Activity
1	Technical exercise
2	Knowledge sharing
3	Technical exercise
4	Scenario exercise
5	Knowledge sharing
6	Technical exercise
7	No activity due to summer holidays
8	Knowledge sharing
9	Technical exercise
10	Knowledge sharing
11	Tabletop exercise
12	Technical exercise

Conclusion

In the end OTO takes a lot of time, from the whole team during the sessions, but also the time to prepare them. And is it worth it? Yes, I think it is. Keeping our knowledge and experience up-to-date is essential for a CERT and the OTO sessions are highly valued by the team members.

Answers puzzles

1) Some text looks like art

2) This text may not look like art but it does do a good job in looking nerdy

3) This is all about the art of deception

Overview contributing partners

KPN is the largest telecom and IT service provider in the Netherlands. Our network is Dutch to the core. We have a clear mission – to help the Netherlands move forward through that network.
We believe in a society in which communication technology makes life richer, easier and fuller. KPN wants to be the unifier of that society, for people and companies. At home, at work and on the move. We have the resources, and the technology and the reliable fixed and mobile networks.
We use our knowledge and experience to make our services and products accessible for everyone, anytime, anywhere. We fulfill people's expectations, but we also achieve the unexpected. KPN believes in technology, in the power of communication and in the power of connection. We are the network that enables the Netherlands to move forward.

National Cyber Security Centre
Ministry of Security and Justice

The National Cyber Security Centre (NCSC), in collaboration with the business community, government bodies and academics, is working to increase the ability of Dutch society to defend itself in the digital domain. The NCSC supports the central government and organisations with a vital function in society by providing them with expertise and advice, threat response and with actions to strengthen crisis management. In addition, the NCSC provides information and advice to citizens, the government and the business community relating to awareness and prevention. The NCSC thus constitutes the central reporting and information point for IT threats and security incidents. The NCSC is part of the Cyber Security Department of the National Coordinator for Security and Counterterrorism.

POLITIE

The Dutch National High Tech Crime Unit (NHTCU) was founded in 2007 as a response to the rise of organised and technically advanced online criminality. Since then the NHTCU has grown from a small pioneers team to a professional unit with 120 officers, maintaining its agility to adapt to technological and criminal developments. The mission of the unit is to use novel and collaborate investigation techniques in order to combat high-tech crime and new forms of cybercrime. The unit focuses on serious organised crime and crime targeting vital national infrastructure.
The NHTCU is embedded within the National Criminal Investigation Division of the Dutch National Police. It cooperates closely with other specialised teams within the National Police, with its foreign counterparts and with many public and private partners in order to be optimally equipped to help keeping the Netherlands cyber-safe.

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Bits of Freedom is the leading Dutch digital rights organisation, focusing on privacy and communications freedom in the digital age. Bits of Freedom strives to influence legislation and self-regulation, on a national and a European level. Bits of Freedom is one of the founders and a member of European Digital Rights (EDRi).

EUROPOL
EUROPEAN LAW ENFORCEMENT AGENCY

Europol is the European Union's law enforcement agency[1]. As such it acts as an information and criminal intelligence hub for the national law enforcement authorities in the 28 EU Member States and as a coordination platform for joint operations. Europol's main objective is to support and assist Member States in their efforts to prevent and combat organised crime, terrorism and other forms of serious crime.
The European Cybercrime Centre (EC3), officially established in January 2013 as one of Europol's operational centres[2], provides operational, analytical and strategic support to EU law enforcement in combatting cybercrime: committed by organised groups to generate large criminal profits such as online fraud; causing serious harm to the victim such as online child sexual exploitation; affecting critical infrastructure and information systems in the EU, including cyber-attacks. This includes support for large-scale, multi-national operations with international partners, leveraging and streamlining existing capacities through Europol's existing infrastructure and law enforcement network with EU and non-EU law enforcement agencies, industry, the financial sector and academia.

1. https://www.europol.europa.eu/
2. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Deloitte.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 200,000 professionals, all committed to becoming the standard of excellence.

IDQ

Founded in 2001 as a spin-off of the Group of Applied Physics of the University of Geneva, ID Quantique (IDQ) is the world leader in quantum-safe crypto solutions, designed to protect data for the future. The company provides quantum-safe network encryption, secure quantum key generation and Quantum Key Distribution solutions and services to the financial industry, enterprises and government organisations globally. IDQ's quantum random number generator has been validated according to global standards and independent agencies, and is the reference in highly regulated and mission critical industries - such as security, encryption and online gaming - where trust is paramount.
IDQ's products are used by government, enterprise and academic customers in more than 60 countries and on every continent. As a privately held Swiss company focused on sustainable growth, IDQ is proud of its independence and neutrality, and believes in establishing long-term and trusted relationships with its customers and partners. For more information, please visit http://www.idquantique.com/.

PHILIPS

Royal Philips (NYSE: PHG, AEX: PHIA) is a leading health technology company focused on improving people's health and enabling better outcomes across the health continuum from healthy living and prevention, to diagnosis, treatment and home care. Philips leverages advanced technology and deep clinical and consumer insights to deliver integrated solutions. Headquartered in the Netherlands, the company is a leader in diagnostic imaging, image-guided therapy, patient monitoring and health informatics, as well as in consumer health and home care. Philips' health technology portfolio generated 2016 sales of EUR 17.4 billion and employs approximately 71,000 employees with sales and services in more than 100 countries. News about Philips can be found at www.philips.com/newscenter.

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialised skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 384,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com

Check Point Software Technologies Ltd. (www.checkpoint.com) is the largest network cyber security vendor globally, providing industry-leading solutions and protecting customers from cyberattacks with an unmatched catch rate of malware and other types of threats. Check Point offers a complete security architecture defending enterprises – from networks to mobile devices – in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes.

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with almost 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series conferences.

TNO, The Netherlands Organisation for Applied Scientific Research, is one of Europe's leading independent R&D organisations. TNO is not for profit and operates independently and objectively. Its unique position is attributable to its versatility and the capacity to integrate knowledge across specialist disciplines.
TNO innovates for a secure cyberspace and provides cyber security research, development, engineering and consultancy services to government and industry. Customers include Dutch government departments and private sector companies across Europe, including many providers of national critical infrastructure (a.o. in telecoms, finance and energy).
TNO is an active member of numerous cyber security partnerships, including the European Network for Cyber Security (ENCS), the Hague Security Delta (HSD) and the EU NIS platform. TNO was part of the core team that formulated the Dutch National Cyber Security Strategy (NCSS) II and was one of the lead authors of the Dutch National Cyber Security Research Agenda (NCSRA) II.
www.tno.nl

At PwC, we see cyber security and privacy differently. We don't just protect business value; we create it—using cyber security and privacy as a tool to transform businesses. By bringing together capabilities from across PwC, we seek to understand senior leaders' perspectives on cyber security and privacy in the context of strategic priorities so they can play a central role in business strategy. By incorporating tactical knowledge gathered from decades of projects across industries, geographies, programs and technologies, PwC can create and execute holistic start-to-finish plans.

Zimperium® is the industry leader in Mobile Threat Defense, providing enterprise class protection for mobile devices against the next generation of advanced mobile cyberattacks and malware. Zimperium is the first and only company to provide a complete on-device Mobile Threat Defense system providing visibility, security and management for iOS, Android and Windows devices. With its unique behavior-based non-intrusive approach, mobile user privacy is protected at all times. Zimperium's MTD solution protects mobile devices for any size enterprise (B2B), or large-scale consumer uses (B2C).

Kaspersky Lab is a global cyber security company founded in 1997. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialised security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them.
Learn more at www.kaspersky.nl

Nick Mann Associates Ltd is a specialist Threat Management Advisory Service. Nick himself has spent over 40 years in Fraud & Security including senior roles in The Stock Exchange and Vodafone (Global Director). He is now Chairman of the GSMA Fraud & Security Advisory Panel.
The length and depth of Nick's experience gives him unparallelled access to a large range of consultants within the complete range of Security & Fraud disciplines and the expertise to match those Associates to the exact client needs.
www.nickmannassociates.com