Cyber Risk GmbH
Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341,
Rebackerstrasse 7, 8810 Horgen
Phone: +41 43 810 43 61, Web: www.cyber-risk-gmbh.com

Top cyber risk and compliance related news stories and world events, that (for better or for worse) shaped the month's agenda, and what is next

June 2017, cyber risk and compliance in Switzerland

We have an interesting paper from MELANI, the Reporting and Analysis Centre for Information Assurance in Switzerland (published on 2017-05-15 by GovCERT.ch).

We read: "On Friday, May 12th, 2017, a ransomware called WannaCry hit the cyber space.

Among the victims are hospitals in UK, the national telecom provider in Spain and U.S delivery service FedEx.

But WannaCry did not only hit the internet, the ransomware was also very present in newspapers worldwide.

It also kept us and our partners from abroad very busy during the last weekend, analyzing the malware, reevaluating the current situation in Switzerland and world-wide, communicating with National Critical Infrastructure, and talking to the press."

They added: "So far, we are aware of 183 potential victims in Switzerland (State on Sunday Evening).

Those have been either notified by us directly or the ISP."

To read more:
https://www.govcert.admin.ch/blog/31/wannacry-it-is-not-worth-it

https://www.melani.admin.ch/melani/en/home/themen/Ransomware.html

One year ago, we had a great effort from MELANI, the Swiss Ransomware Awareness Day.

We read: "19.05.16 - Together with partners, the Reporting and Analysis Centre for Information Assurance MELANI is organising an awareness day for ransomware today.

The participants include organisations from various sectors, software manufacturers, federal offices and a range of Swiss associations and consumer protection organisations."

To read more:
https://www.melani.admin.ch/melani/en/home/dokumentation/newsletter/ransomwareday.html

Another interesting development - After each major cyber-attack, we have a second wave: The attack using the fake 'fixes' and 'support services' for the previous attack.

Where people are ignorant, only the imagination of the criminals is the limit. For example, they offer (fake) protection for Android devices, to avoid the WannaCry ransomware. But Android devices cannot be affected by WannaCry, because this threat exploits a vulnerability in Microsoft Windows that cannot harm mobile systems.

Cybercriminals don't just send fraudulent email messages. They might call you on the telephone and claim to be working in a hardware or software vendor, for example Microsoft.

They might also setup websites with pop-ups displaying fake warning messages and a phone number to call and get the "issue" fixed.

They might offer to help solve your computer problems or sell you a software license.

Microsoft and vendors do not make unsolicited phone calls to help us fix our problems. It is the other way around.

Perpetrators often use pay phones, disposable cellular phones, or stolen cellular phone numbers.

Treat all unsolicited phone calls with scepticism. Do not provide any personal information.

In an excellent report, the UK National Cyber Security Centre explains the risk:

"WannaCry ransomware may not have generated the wealth the scammers responsible were hoping for but since the attack enterprising criminals have been attempting to cash in on the heightened public awareness of WannaCry.

Targeting concerned users, scammers have been offering a range of fake 'fixes' and 'support services'.

This type of social engineering is a common methodology for cybercriminals. Whether viral social media posts, malicious pop-ups or well-crafted phishing campaigns, high profile events such as the WannaCry attack offer cyber criminals a hook to spread malware or to solicit funds.

It's not only online incidents that criminals seek to take advantage of.

Following news of high profile disasters such as hurricane Catrina in 2005, the 2014 Ebola outbreak and the 2015 Nepal earthquake, scammers set up fake charity websites and sent phishing emails in attempts to steal funds donated to the victims.

Recent examples of scams piggybacking on the WannaCry incident include:

- Alerts circulating of social media directing users to fake WannaCry patches which deliver malware;

- A phishing email posing as a BT customer service email which informs the user they are locked out of their BT account and directs them to a malicious link to obtain a 'security upgrade' to re-establish full access;

- Third party app stores offering 'patches' for mobile users - despite the fact no mobile operating systems are believed to be vulnerable to WannaCry."

According to US-CERT (part of the Department of Homeland Security), good security measures are:

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate in-bound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching the end users.

- Ensure anti-virus and anti-malware solutions are set to automatically conduct regular scans.

- Manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary.

- Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.

- Develop, institute, and practice employee education programs for identifying scams, malicious links, and attempted social engineering.

This month, we want to discuss also this: Malvertising (malicious advertising) is a delivery method for malware.

A simple form of malicious advertising: You see the ad, it is interesting, you click on that, you are redirected to websites that will infect you with malware or install some other software. Malvertising is such a dangerous threat because it can be easily spread across many legitimate websites without directly compromising those websites.

Users running out-of-date operating systems and browsers are more vulnerable to this and other forms of malware infection.

More sophisticated forms of malicious advertising: Malware-infected ads can be inserted into popular, legitimate websites, and often do not require

user action to be effective - simply visiting an infected site can be enough to get infected.

Internet users make a dangerous assumption: If we do not click on a URL or an ad, nothing is going to happen.

There is pre-click malware embedded in main scripts of a web page. Malware can auto-run, as in the case of auto redirects, where the user is automatically taken to a different site, which is malicious.

A post-click malvertisement works really well. Users expect a redirection to happen when clicking on an advertisement. A redirection only needs to be co-opted to lead to infection of a computer.

Welcome to our monthly newsletter.

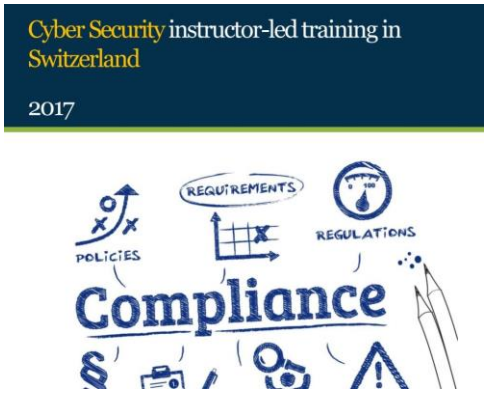
Best Regards,

George Lekatis

George Lekatis
General Manager, Cyber Risk GmbH
Rebackerstrasse 7, 8810 Horgen
Phone: +41 43 810 43 61
Mobile: +41 79 505 89 60
Email: george.lekatis@cyber-risk-gmbh.com
Web: www.cyber-risk-gmbh.com

Cyber Risk GmbH, Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341

Our Catalog - Instructor-led training in Switzerland:
http://www.cyber-risk-gmbh.com/Cyber_Risk_GmbH_Catalog_2017.pdf



Number 1 (Page 9)

Disinformation operations in cyber-space

In parallel to cyber-attacks that impact technological assets, threat actors have been conducting an increasing number of multi-faceted disinformation operations.

Alleged objectives of these attacks are to infiltrate dependable information sources and influence and distract public opinion, (social) media and the press.

Number 2 (Page 13)

Information Operations and Facebook

Facebook understands that it has become a battleground for governments seeking to manipulate public opinion in other countries. This is a paper you must read.

It covers "information operations" and very interesting response plans. Facebook speaks about well-funded efforts by nations and other organizations to spread misleading information.

Number 3 (Page 14)

Fourth Money Laundering Directive and Fund Transfer Regulation Implementation (DEPP and EG)

The Fourth Money Laundering Directive (4MLD) and the Fund Transfer Regulation (FTR) update the European Union's (EU) anti-money laundering (AML) framework to meet new international standards issued by the Financial Action Taskforce.

Number 4 (Page 15)

ENISA works together with European semiconductor industry on key cybersecurity areas

The uptake of connected devices and services demands baseline requirements for security and privacy and the efficient application of EU standards.

The paper focuses on four main areas actively debated at the EU level: standardisation and certification, security processes and services, security requirements and implementation, and the economic dimensions.

Number 5 (Page 18)

Android app malware

According to IT security company Check Point, as many as 36 million Android devices may have been infected with ad-click malware.

The malware, dubbed Judy, is reported to have been present in approximately 50 apps in Google's play store, but the total number of infections cannot be accurately determined as it is not known for how long the apps have been malicious.

Those responsible generate money through ad-clicks – in this instance Judy silently imitated a browser and clicked on banners from Google's ad infrastructure to generate revenue for the malware author.

Number 6 (Page 20)

NISTIR 8170 DRAFT
The Cybersecurity Framework: Implementation Guidance for Federal Agencies

Draft NISTIR 8170 provides guidance on how the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) can be used in the U.S. Federal Government in conjunction with the current and planned suite of NIST security and privacy risk management publications.

Number 1

Disinformation operations in cyber-space

Introduction

In parallel to cyber-attacks that impact technological assets, threat actors have been conducting an increasing number of multi-faceted disinformation operations.

Alleged objectives of these attacks are to infiltrate dependable information sources and influence and distract public opinion, (social) media and the press.

This is attempted by seeding distrust, undermining widely accepted societal and democratic values, and potentially influencing the outcome of important events such as elections.

Such attacks can be perfectly disguised beneath the vast amount of publicly available information (often tailored to individual or group profiles) that people "consume" on a daily basis.

This renders those attacks difficult to detect and mitigate.

Disinformation operations are a clear reminder that cyber-space is a term that not only incorporates networks and computing devices but also the human element.

This note outlines disinformation campaigns and provides an overview of the trending threat of "tainted leaks".

Disinformation campaigns

Disinformation operations in cyber-space became evident after the revelation of the Democratic National Committee (DNC) hack in 2016, where according to the US government agencies a foreign state attempted to covertly interfere (additional overt channels were possibly used as recently disclosed) with the US presidential elections.

Following this attack, US government agencies assessed that similar attempts of influencing elections would be seen across Europe.

During March-May 2017 there were attacks against Emmanuel Macron's election campaign in France.

The attacks involved spear-phishing campaigns, controversial leaks aiming to discredit Macron, and a massive data leak ("Macron leaks").

The leak allegedly included e-mails between Macron, his team, other officials, politicians, as well as original documents and photos.

A recent report, which focused on disinformation campaigns and tactics, introduced the term "tainted leaks" to describe "the deliberate seeding of false information within a larger set of authentically stolen data".

The tactic behind tainted leaks is not new. Intelligence services have used them in the past for disinformation and psychological warfare.

Nowadays, tainted leaks use cyber-space to gain more traction.

Tainted leaks move a step forward from the dissemination of fake news, by further blurring the lines of what is true and what is a fallacy.

A large volume of stolen data is a good candidate for tainting before publicly leaked.

As stated in the aforementioned report, a carefully constructed tainted leak contains a series of legitimate data/information -as a proof of authenticity, while they are surrounded by well-tailored fake information.

The mixture of legitimate and fake information is quite challenging to be detected and hence it can be overlooked by the press.

The combination of the dissemination of tainted leaks together with the launch of well-orchestrated social-media campaigns that focus on spreading the falsified elements of these leaks, highlights how serious -and non-trivial to solve- the problem of tainted leaks is.

Tainted leaks usually have a twofold goal.

On the one hand, they aim at propagating false information and discrediting the party affected by the falsehoods.

On the other hand, and perhaps most importantly, they aim at cultivating distrust among citizens and inducing them to question the integrity, reliability and trustworthiness of the media - which often fall in the trap of relaying fake news.

Citizens usually do not have the ability to verify the integrity of data leaks and in the case of tainted leaks the media may have a difficult time performing proper fact checking in a timely manner.

In the meantime, false information spread like wildfire fulfilling their goal.

Examples of mitigation approaches

One interesting aspect in Emmanuel Macron's case was the "counter offensive" tactic that Macron's digital team employed against the frequent phishing attacks it faced during the election campaign.

The head of Macron's digital team revealed that his team "replied" to the several phishing attempts by feeding them with decoy data (referred to credentials of fake accounts containing fake data/information e.g. documents) and hence rendering the validation of the authenticity of those data a non-trivial as well as time-consuming task for the attackers.

The head of Macron's digital team also noted that the "Macron leaks" included both authentic and fake documents (created by the attacker/s), stolen documents from various companies, and fake e-mails created by Macron's team.

He did not comment on whether fake documents created by Macron's team were part of the leak.

In the context of tainted leaks, an interesting point in this case is that Macron's team attempted to use the tainted leaks in its favor by trying to influence them -prior to their revelation- and hence limit their impact.

Therefore, Macron's case suggests that not all tainted leaks work the same or cause the same damage.

In case the already shared information regarding this "counter offensive" operation is correct, a few remarks can be made: "counter offensive" operations are controversial and are still a grey area in cyber security.

They might have worked in Macron's case but they may not have the same impact and consequences when applied in different sectors.

Having said that, as highlighted in a previous note, there are some considerations that need to be taken into account prior to employing "counter offensive" operations.

Europe has raised concerns about fake news while warning that there are no easy solutions to this issue.

After pressure from European bodies, social networks (which are heavily leveraged for spreading fake news) seem to be taking steps in the fight against fake news campaigns.

For example, Facebook, recently acknowledged the issue and published a report about it, describing its approach against fake news.

It is expected that similar actions will be initiated by various stakeholders whose businesses heavily depend on information.

Conclusion

Disinformation campaigns and tainted leaks, are becoming a serious issue both in the cyber and physical world.

Due to their nature, they are difficult both to identify and counter.

Societies will have to develop defences against such attacks, particularly the ones that aim to potentially affect democratic processes such as elections, legislative procedures, law enforcement and justice.

In the context of cyber security, disinformation campaigns should be closely monitored and thoroughly analysed in order to counter similar attacks in the future.

Number 2

Information Operations and Facebook

Facebook understands that it has become a battleground for governments seeking to manipulate public opinion in other countries. This is a paper you must read.

It covers "information operations" and very interesting response plans.

Facebook speaks about well-funded efforts by nations and other organizations to spread misleading information.

To read more:
https://www.facebook.com/notes/facebook-security/making-facebook-safe-and-secure-for-authentic-communication/10154362152760766/

https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf

Number 3

Fourth Money Laundering Directive and Fund Transfer Regulation Implementation (DEPP and EG)

The Fourth Money Laundering Directive (4MLD) and the Fund Transfer Regulation (FTR) update the European Union's (EU) anti-money laundering (AML) framework to meet new international standards issued by the Financial Action Taskforce.

On 15 September 2016, the Treasury published its consultation paper (CP) on the transposition of the 4MLD and FTR. On 15 March 2017, it published a further consultation together with the draft implementing regulations, the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR2017).

MLR2017 is stated to come into force on 26 June 2017 and will replace the Money Laundering Regulations 2007 (MLR2007) and the Transfer of Funds (Information on the Payer) Regulations 2007 (TFR2007).

The overall objective of these new regulations is to ensure the UK's AML and counter terrorist financing (CTF) regime is up to date, effective and proportionate.

MLR2017 require firms subject to AML obligations to ensure that measures they take in meeting customer due diligence and ongoing monitoring obligations are based on an overall assessment of the money laundering/terrorist financing risks that a firm faces, including taking account of guidelines published by the European supervisory authorities (ESA), UK supervisory authorities and the UK Government's national risk assessment.

To read it: https://www.fca.org.uk/publication/consultation/cp17-13.pdf

Number 4

ENISA works together with European semiconductor industry on key cybersecurity areas

The uptake of connected devices and services demands baseline requirements for security and privacy and the efficient application of EU standards.

The EU Agency for Network and Information security – ENISA – together with industry recently reached a common position on cybersecurity, that reflects the concerns of industry and provides a set of suggestions for policy makers.

The paper focuses on four main areas actively debated at the EU level: standardisation and certification, security processes and services, security requirements and implementation, and the economic dimensions.

The paper identifies key challenges and recommendations identified for the European Commission to:

- define a policy framework for ensuring minimal security requirements for connected devices. The development of European security standards needs to become more efficient and/or adapted to new circumstances related to Internet of Things (IoT). Based on those requirements, a European scheme for certification and the development of an associated trust label should be evaluated.

- ensure that reliable security processes and services are being developed to support industry in implementing security features in their products (e.g. through providing information and training about state-of-the art security solutions).

- encourage the development of mandatory staged requirements for security and privacy in the IoT, including some minimal requirements. These common principles should be considered in future revisions and new legislative initiatives.

- create a level playing field for cybersecurity and look into incentives similar to the Digital Security Bonus in order to reward the use of good security practices.

ENISA's Executive Director Udo Helmbrecht said: "Trusted solutions and a common defined level for the security and privacy of connected and smart devices is both recommended and needed, to allow Europe to reap the benefits of soon to become ubiquitous technologies.

As such, standardisation and certification have been identified as a priority, to accelerate the level playing field for the entire industry and reflect the trust of citizens, consumers and businesses in the connected environment".

"Pervasive connectivity over the Internet of Things means that security is becoming an important issue for just about all citizens – whether they be using a computing device, TV or washing machine.

The European policy framework is set to define easy-to-use measures that will give industry the guidance it requires and consumers the transparency they need," said Dr. Stefan Hofschen, Division President Chip Card & Security at Infineon Technologies.

"On the product side, security solutions based on certified, hardware security trust anchors are already available today to serve the increasing security requirements."

"The growth in IoT and connected devices creates a tremendous amount of opportunity for businesses and consumers. How the industry comes together, agrees on common principles to address complex concerns like security, can break down the barriers of adoption and is key to fostering this market," said Rüdiger Stroh, Executive Vice President & General Manager of Security and Connectivity at NXP® Semiconductors.

"Security and privacy by design, a proven approach that grew business streams for mobile phones, cars and wearable manufacturers, help build trust between businesses and consumers. Our vision is to help grow the IoT market and bring this quality of security to other IoT applications."

"This initiative will increase the much-needed awareness for security in IoT devices and organize a collective effort to establish important standards to help deliver it, which will ultimately bring big benefits to consumers and

businesses," said Marie-France Florentin Group Vice President & General Manager of Secure Microcontroller Division at STMicroelectronics.

"With its long history and valuable expertise in embedded security, ST is in a strong position to make vital contributions to this key framework."

The common position was developed by Infineon, NXP, and STMicroelectronics, supported by ENISA. The Agency aims at working further with industry and seeks the support of more actors in the semi-conductor and chip-product manufacturer field, application and service providers.

Furthermore, ENISA is working alongside the Commission and cooperates with the recently formed cPPP (contractual Public-Private Partnership) in order to define a roadmap on NIS Certification, and looks forward to supporting the Commission in the NIS Certification policy area.

To read more:
https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity

Number 5

Android app malware

National Cyber Security Centre
a part of GCHQ

According to IT security company Check Point, as many as 36 million Android devices may have been infected with ad-click malware.

The malware, dubbed Judy, is reported to have been present in approximately 50 apps in Google's play store, but the total number of infections cannot be accurately determined as it is not known for how long the apps have been malicious.

Those responsible generate money through ad-clicks – in this instance Judy silently imitated a browser and clicked on banners from Google's ad infrastructure to generate revenue for the malware author.

The malware has had little real impact upon the end user, though it does equate to an illegitimate use of a device, and could potentially be exploited for more sophisticated attacks, including: gaining control of devices for additional malware download, conducting DDoS attacks or gaining access to private networks.

Google's protection system did not immediately identify the problem because the apps themselves did not contain any malicious code.

Rather, once downloaded from the play store, the affected apps are designed to call out to a remote server which then delivers malicious ad-click software to devices.

This type of two-stage delivery is increasingly common. Last month, FalseGuide malware was discovered hidden inside apps and games on the play store.

Following download, these compromised apps allow malicious actors to install additional malicious software.

App stores may come under increased pressure to enhance their scrutiny of apps before permitting them to feature, particularly if the number of instances of adware infections increases.

The NCSC recommends that users only install apps from the official application store for your device.

Malicious apps in official stores are more likely to be discovered, and subsequently removed from the store and the device.

Number 6

NISTIR 8170 DRAFT
The Cybersecurity Framework: Implementation Guidance for Federal Agencies

Draft NISTIR 8170 provides guidance on how the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) can be used in the U.S. Federal Government in conjunction with the current and planned suite of NIST security and privacy risk management publications.

The specific guidance was derived from current Cybersecurity Framework use. To provide federal agencies with examples of how the Cybersecurity Framework can augment the current versions of NIST security and privacy risk management publications, this guidance uses common federal information security vocabulary and processes.

NIST will engage with agencies to add content based on agency implementation, refine current guidance and identify additional guidance to provide the information that is most helpful to agencies.

Feedback will also help to determine which Cybersecurity Framework concepts are incorporated into future versions of the suite of NIST security and privacy risk management publications.

NIST would like feedback that addresses the following questions:

- How can agencies use the Cybersecurity Framework, and what are the potential opportunities and challenges?

- How does the guidance presented in this draft report benefit federal agency cybersecurity risk management?

- How does the draft report help stakeholders to better understand federal agency use of the Cybersecurity Framework?

- How does the draft report inform potential updates to the suite of NIST security and privacy risk management publications to promote an integrated approach to risk management?

- Which documents among the suite of NIST security and privacy risk management publications should incorporate Cybersecurity Framework concepts, and where?

- How can this report be improved to provide better guidance to federal agencies?

To read the paper:
http://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf

Special Publication 800-39			Cybersecurity Framework Components
Level 1 Organization	**Integrate enterprise and cybersecurity risk management** by communicating with universally understood risk terms.	Core	
Level 2 Mission/ Business Processes	**Manage cybersecurity requirements** using a construct that enables integration and prioritization of *all* requirements.	Profile(s)	
	Integrate and align cybersecurity and acquisition processes by relaying cybersecurity requirements and priorities in a common and concise language	Profile(s)	
	Evaluate organizational cybersecurity using a standardized and straightforward measurement scale and set of self-assessment criteria.	Implementation Tiers	
	Manage the cybersecurity program by determining which cybersecurity outcomes necessitate common controls, and apportioning work and responsibility for those cybersecurity outcomes (supports RMF Implement & Monitor).	Profile(s)	
	Maintain a comprehensive understanding of cybersecurity risk using a standardized organizing structure (supports RMF Authorize).	Core	
	Report cybersecurity risks using a universal and understandable reporting structure.	Core	
Level 3 System	**Inform the tailoring process** using a comprehensive reconciliation of *all* cybersecurity requirements (supports RMF Implement).	Profile(s)	

Figure 1: Federal Cybersecurity Uses

Disclaimer

Cyber Risk GmbH enhances public access to information about cyber risk and compliance in Switzerland.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which Cyber Risk GmbH has no control and for which Cyber Risk GmbH assumes no responsibility;

- is not professional or legal advice);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.