February 2019, cyber risk and compliance in Switzerland

Top cyber risk and compliance related local news stories and world events

Dear readers,

Swiss Post is making its future e-voting system available for a public intrusion test from 25 February to 24 March 2019.

The e-voting system is the first Swiss system that can be completely verified. The complete verifiability makes e-voting available to a broader public, and ensures that systematic malfunction resulting from software errors, human errors or attempted manipulations is detected.

In accordance with the requirements of federal law, the system must be certified before first use and the source code must be disclosed. In addition, the Confederation and the cantons have decided that completely verifiable e-voting systems must undergo an intrusion test before they are used for the first time.

Intrusion tests stage attacks to verify a system's security. An intrusion test is already being carried out by an accredited body as part of the certification process. The public intrusion test has the added benefit of including a large number of people to test the security of a system.

According to the media release of the Federal Chancellery of 7 February 2019, the Confederation and the cantons have adopted common requirements for the public intrusion test, requiring system providers to make their systems available for testing for a period of four weeks.

The hacker community should try to manipulate votes, read votes cast and disable or circumvent the security measures that protect votes and security-related data. The system documentation and source code must be published before testing.

SCRT, a company specialising in intrusion tests, registers participants on behalf of the Confederation and the cantons, and evaluates feedback.

According to the decision taken by the Steering Committee Vote électronique on 29th October 2018, the following requirements apply to public intrusion tests:

1. The system providers will allow a public intrusion test to be conducted on their system.

2. The test will cover a minimum of 4 weeks (duration of the voting process).

3. Participants from anywhere in the world can test the system.

4. The participants must be permitted to attack the system. It should be possible to attempt the following: to manipulate votes, to read votes that have been cast, to breach voting secrecy, to disable or circumvent security measures that protect votes and data relevant to security.

5. Participants are permitted to publish their test findings.

6. The system documentation and the source code must be published beforehand on the internet (the provisions of Ordinance on Electronic Voting Art. 7a f. apply). The participants will be given a sufficient number of polling cards as test material. These can be sent out electronically.

7. The feedback from the testers goes to a service company appointed by the Confederation and the cantons. This company will evaluate the feedback and provide its assessment as quickly as possible. The system providers will support the service company in doing this.

8. As a requirement for taking part in the test, the system providers may require persons interested in participation to adhere to a code of conduct. This could include the following obligations:

a. to refrain from making attacks that are excluded from the test;

b. to report any deficiencies found immediately;

c. to postpone publication of any description of deficiencies found until the system providers have decided how to deal with the deficiencies.

9. The following are excluded from the test:

a. load-based attacks that are intended to make voting impossible (distributed denial of service);

b. attacks using fake messages that are intended to distract voters from the required processes (social engineering);

c. attacks that are intended to manipulate votes where the attack can be recognised with the aid of individual verifiability;

d. attacks that are intended to read votes by infecting the devices used for voting with malware;

e. attacks on the system providers' services that are not connected with e-voting;

f. attacks on the system for sending out polling cards online.

10. Once the system providers have given their consent to the test, the participants are protected from prosecution, unless their attacks are excluded from the test.

Q&A regarding the public intrusion test

Is the federal government allowed to pay for hacker attacks?

Swiss Post is responsible for paying people who report security breaches. Swiss Post decides how much is paid. The federal government and the cantons are contributing CHF 250,000 towards the public intrusion test via eGovernment Switzerland's priority plan.

Does the public intrusion test aim to prove that E-Voting cannot be hacked?
No. The aim of the intrusion test is to reveal weaknesses and eliminate them if necessary.

Furthermore, it is in the interest of transparency that as many independent experts as possible are familiar with e-voting security issues. The public intrusion test could provide them with the opportunity to find out more about e-voting.

Is it the responsibility of independent experts to make sure that all weaknesses are revealed?

No. The public intrusion test is one security measure among many. Every IT system has weaknesses, and this will remain the case with e-voting even after the public intrusion test. The decisive factor is that no weakness gives rise to a serious risk. Weaknesses must be countered by security measures that are sufficiently effective.

With full verifiability, e-voting has a comprehensive and particularly effective security measure that is not available for other services. In addition, the systems are regularly audited and certified by an accredited body.

Computers are necessary for full verifiability. Are these computers free of vulnerabilities?

Full verifiability essentially means that manipulating a single component is not enough to falsify votes unnoticed. If a single component is manipulated, other components are available that can be used to uncover the attempted voting fraud.

How serious does the weakness need to be before people are paid for reporting it?

The seriousness of the weakness is not decisive. Rather, what is important is that participants play by the rules when testing the system. We are essentially encouraging participants to make attacks that will provide new findings that help increase security against voter fraud.

No payment will be made for attacks that simply highlight known weaknesses. Some attacks are even forbidden, even though they are linked to a relevant risk. To keep these risks under control, however, more effective means are available than the public Intrusion test.

What attacks are excluded?

A payment will be made for any successful attacks on Swiss Post's e-voting infrastructure, provided the attack is permitted for the purposes of the test. Other organisations (cantons, printing companies and other Swiss Post services) will not be taking part in the intrusion test, and therefore must not be attacked.

In addition, distributed denial-of-service attacks are prohibited as they do not provide new findings in a public intrusion test, can be tested elsewhere and would also disrupt the testing process.

No payment will be made for attacks on voters' platforms, or for any attacks using fake messages to persuade the actors to deviate from the planned processes (social engineering). Successful attacks take advantage of errors by the actors which cannot be realistically simulated in a public intrusion test. Nevertheless, a payment will be made for breaking individual verifiability (a 'yes' is cast and a 'no' is displayed), where voters are completely unaware that their vote has been manipulated.

Won't the public intrusion test also help malicious hackers understand how to hack the e-voting system?

A weakness could be reported to a potential attacker instead of to the organisers. This is not a problem as long as the organisers are also informed about the weakness and fix it if necessary. The payments offered by Swiss Post provide an incentive to report weaknesses to the organisers.

Illegal attempts to find weaknesses could be made at any time, not just during the public intrusion test. On the other hand, the public intrusion test provides well-meaning participants with the opportunity to examine the system thoroughly for weak points.

Why is e-voting already being used if the system has not yet been subjected to an intrusion test?

The system that is now available for public intrusion testing is the first system to be fully verifiable. The systems in use today offer individual verifiability, but not yet full verifiability.

Given that full verifiability allows the wider use of e-voting, such a system must meet even higher security requirements, including certification and source code disclosures. In addition, the federal government and the cantons have decided that fully verifiable systems must undergo a public intrusion test before they can be used for the first time.

Another interesting development - The Federal Council approved the 2018 foreign policy report at its meeting on 30 January 2019.

In 2018, global events were marked by increasing competition between the world's superpowers and a weakening of the commonly accepted rules underpinning the international system. This created a challenging situation for Switzerland to find solutions and compromise.

Nevertheless, Switzerland's role as a mediator and bridge-builder gained in importance against this backdrop. In addition to its existing protecting power mandates, Switzerland made a key contribution by hosting peace talks and participating in selected negotiations throughout the world.

Bilateral relations are central to the safeguarding of Swiss interests. In 2018, relations with neighbouring Germany, Italy and France were close and friendly, although several aspects concerning cooperation remain pending. Switzerland also maintained wide-ranging bilateral ties with major global powers such as China and the US, including human rights dialogues that allow Switzerland to raise concerns that are at the core of its values.

To read the report (German language):
https://www.newsd.admin.ch/newsd/message/attachments/55499.pdf

---

The *Threat Landscape Report 2018* from the European Union Agency for Network and Information Security (ENISA) is very interesting. There are several developments that must be well understood by all organizations and companies of the public and the private sector.

According to the report, State-sponsored activities have led to the assumption that there is a shift towards reducing the use of complex malicious software and infrastructures and going towards low profile social engineering attacks.

The W2 scam starts by spoofing an executive member of finance or HR department for employees' records. These records are then used for identity theft. The scam is named after the US W2 tax form used to report employee's wages. This social engineering scam, although not new (first reported in 2016 by IRS), is resurfacing with an increase of 10% more incidents than last year

In 2018, attack tactics have shifted to malware-less attacks with email and impersonation attacks being the main infection vector.

In the enhanced threat agent capabilities belong time related attack tactics (e.g. kind of phishing according to week days), selective phishing via refined social engineering tactics, payload installed via remote access tools (e.g. Remote Desktop Protocol (RPD) interfaces), targeted attacks tailored to sectors, etc.

Another clear trend in cybercrime attacks in 2018 has been the refinement of phishing by using social engineering techniques. Remarkable are the trends towards attacking Software-as-a-Service (SaaS), the rates of phishing using social engineering (tripled in 2018) and the continuous innovation towards persuading users for the originality of phishing scams.

Attack vectors taxonomy for this year's threat landscape

The list below provides a categorization of the most predominant and noteworthy attack vectors observed by ENISA throughout the year. A full knowledge base of cyber adversary behaviour and taxonomy for adversarial actions maintained by MITRE is available at ATT&CK website[629].

- **Attacking the human element**
  - Social engineering
  - Phishing/spear-phishing/business email compromise(BEC)/whaling/spam through email/social media/online services
    - Malicious attachments in emails
    - Malicious URLs in emails and social media
    - Microsoft office attack vectors (macros etc)
    - Social media messaging services
  - Scams
    - Customer/tech support scams
    - Phone scams (Vishing)
    - SMS scams (Smishing)
- **Web and browser based attack vectors**
  - Drive-by downloads
  - Drive-by mining (cryptojacking)
  - Malicious scripts/URLs

During the reporting period, various reports from global security research organisations revealed that cyber espionage ("nation-state-sponsored") is becoming increasingly popular among certain nation states.

This threat typically targets industrial sectors, critical and strategic infrastructures across the world including government entities, railways, telecommunication providers, energy companies, hospitals and banks.

Cyberespionage focuses on driving geopolitics, stealing state and trade secrets, intellectual property rights and proprietary information in strategic fields.

It also mobilises actors from the economy, industry, foreign intelligence services, as well as actors who work on their behalf.

In a recent report, threat intelligence analysts were not surprised to learn that 71% of the organizations are treating cyber espionage and other threats as a "black box" and are still growing and expanding their knowledge over them.

During the reporting period, the number of nation-state-sponsored cyberattacks that focused primarily on the economy has grown, and is likely to continue this way.

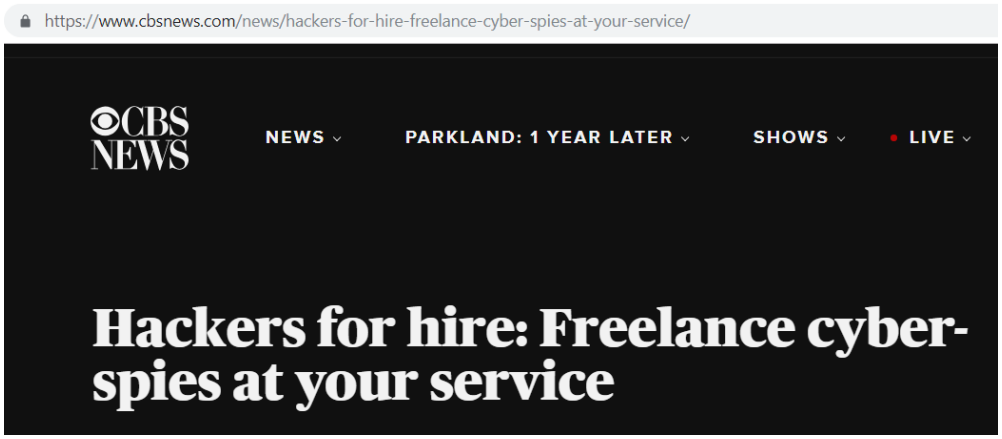
In detail, nation-state-sponsored and other adversary-driven attacks on Industrial Internet of Things (IIoT) are increasing in the utilities, oil and natural gas (ONG), and manufacturing sectors.

Furthermore, advanced persistent threat (APT) cyberattacks indicate that many financial attacks are motivated by espionage.

The term "crowdsourcing" is used to describe how businesses can use the Internet to outsource work to the crowd. Crowdsourcing can also be used in espionage - the process of obtaining information that is not normally publicly available, using human sources (agents, for example) or technical means (hacking, for example), to influence decision makers and opinion formers, and to benefit the interests of a country.

With "Hacking-as-a-service (HaaS)" hackers become contractors, offering services ranging from "white" penetration testing to "black" services like earning market share by hacking the competitors. With "Ransomware- as-a-service (RaaS)" malware developers become vendors of malware, without the need to distribute their products. Criminals and State- sponsored groups purchase the products and use them for their own purposes.

"Espionage-as-a-service (EaaS)" is any intelligent mix of the above tools, that is used by experts employed directly or indirectly by a nation state.



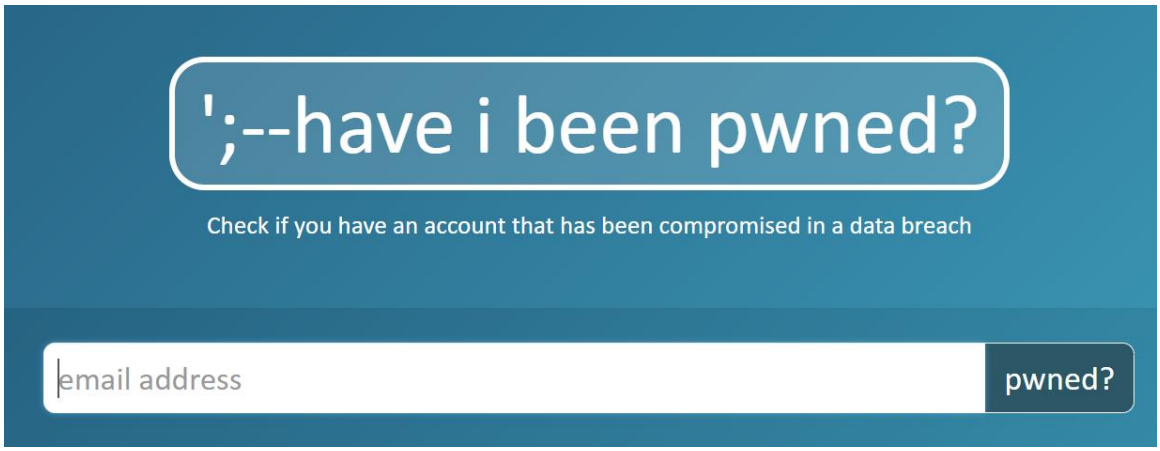
According to a recent alert from the NCSC in UK, details stolen from almost 620 million accounts following website hacks have appeared for sale on the dark web.

16 websites including the likes of MyFitnessPal, MyHeritage and Dubsmash suffered hacks mostly during 2018 with the hacker explaining that they were able to exploit security vulnerabilities within web apps.

Some of the websites including MyHeritage and MyFitnessPal have previously notified customers of the breach, although a number had not admitted to the breach until it had become public knowledge.

The types of detail stolen includes names, passwords, email addresses and other personal information but no payment or banking details have yet to appear for sale.

If bought, this kind of information can be used to hack into other online accounts but there are a number of ways you can help to defend yourselves against these risks.



Haveibeenpwned.com allows you to check whether you have an account that has been compromised in a data breach.

If you find that you have been affected then changing your passwords on key accounts is a good first step, whilst ensuring you have unique passwords for those important accounts also.

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, *in-house* instructor-led training in Switzerland, Liechtenstein and Germany:
https://www.cyber-risk-gmbh.com/Cyber_Risk_GmbH_Catalog_2019.pdf

Number 1 (Page 14)

INTERPOL and UN join forces to counter exploitation of Internet for terrorist activities

INTERPOL and the United Nations Counter-Terrorism Centre (UNCCT), the capacity building arm of the United Nations Office of Counter - Terrorism (UNOCT), jointly conducted a workshop on “Enhancing Member State Capacities to use Social Media to Prevent and Counter the Foreign Terrorist Fighters Phenomenon”.

Number 2 (Page 16)

IoT Security Standards Gap Analysis, from ENISA

Mapping of existing standards against requirements on security and privacy in the area of IoT

ENISA conducts a preliminary analysis of the IoT-related landscape of standards, which indicates that there is no significant gap in standards to bring secure IoT to the market.

This does not mean that the security of the IoT ecosystem as a whole has been addressed by means of standards.

Elements of a holistic approach towards IoT security can be found in a series of standards, however to achieve an overarching approach that protects the entire IoT ecosystem further work is needed.

Number 3 (Page 18)

NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals'

The field has narrowed in the race to protect sensitive electronic information from the threat of quantum computers, which one day could render many of our current encryption methods obsolete.

Number 4 (Page 21)

ENISA Threat Landscape Report 2018

2018 was a year that has brought significant changes in the cyberthreat landscape. Those changes had as source discrete developments in motives and tactics of the most important threat agent groups, namely cyber-criminals and state-sponsored actors.

Monetization motives have contributed to the appearance of crypto-miners in the top 15 threats. State-sponsored activities have led to the assumption that there is a shift towards reducing the use of complex malicious software and infrastructures and going towards low profile social engineering attacks.

Number 5 (Page 24)

Experts from financial supervision, politics and industry took part in the discussions in Bonn

BaFin's first symposium on combating money laundering and terrorist financing

500 representatives of banks, insurance companies, public authorities, and associations attended Dr Pötzsch's opening speech, in which he pointed out

that combating money laundering and terrorist financing has significantly grown in importance both in terms of regulation and in terms of public perception.

Number 6 (Page 26)

International hacker-for-hire jailed for cyberattacks on Liberian telecommunications provider

National Cyber Security Centre
a part of GCHQ

A British cyber criminal has been jailed for conducting attacks that disrupted a Liberian telecommunications provider, resulting in losses estimated at tens of millions of US dollars.

Daniel Kaye pleaded guilty in December 2018 to creating and using a botnet and possessing criminal property. He was sentenced to 2 years and 8 months following an investigation led by the NCA's National Cyber Crime Unit.

Number 7 (Page 27)

NASA employee data left exposed due to misconfigured app

National Cyber Security Centre
a part of GCHQ

According to security researcher Avinash Jain, a system administrator may have misunderstood the definition of "all users" and "everyone" when assigning permissions to newly-created dashboards within the app, interpreting these terms to mean everyone within the organisation.

Number 8 (Page 28)

Building Trusted Human-Machine Partnerships

Autonomous systems to assess their own competence and communicate it to human teammates

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

A key ingredient in effective teams – whether athletic, business, or military – is trust, which is based in part on mutual understanding of team members' competence to fulfill assigned roles.

Number 9 (Page 30)

Securing Office 365 with better configuration

We believe that anyone with an Office 365 account would benefit from acting on the security recommendations in this advisory. From small businesses through to large enterprises, implementing measures such as Multi-factor Authentication (MFA) should be a high priority.

Number 1

INTERPOL and UN join forces to counter exploitation of Internet for terrorist activities

INTERPOL and the United Nations Counter-Terrorism Centre (UNCCT), the capacity building arm of the United Nations Office of Counter - Terrorism (UNOCT), jointly conducted a workshop on "Enhancing Member State Capacities to use Social Media to Prevent and Counter the Foreign Terrorist Fighters Phenomenon".

The three-day (14 – 16 January) workshop brought together law enforcement officers and investigators from Iraq, Jordan, Lebanon, Morocco, Tunisia, the United Arab Emirates and Pakistan.

The objective was to raise the understanding of the Foreign Terrorist Fighters (FTF) phenomenon, including the gender dimension and the importance of respecting human rights and fundamental freedoms while countering and preventing the phenomenon through the use of social media.

The joint INTERPOL-UNOCT/UNCCT workshop included practical exercises aimed at developing the ability of Member States to use information on the Internet and social media to counter the FTF threat.

It focused on the role of law enforcement agencies to collect, analyse and share information found online, particularly on social media platforms, to assist in detecting, preventing, investigating and prosecuting terrorism-related crimes.

Participants were trained in four main areas:

- detecting terrorist-related activities online;
- collecting e-evidence;
- requesting e-evidence across borders; and
- engaging with the private sector to advance investigations by law enforcement agencies.

The 14 participants benefited from the expertise provided by INTERPOL's Counter-Terrorism Directorate, UNOCT/UNCCT, national law enforcement agencies, as well as from partners organizations such as the

UN Counter-Terrorism Committee Executive Directorate (CTED), the UN Office on Drugs and Crimes (UNODC) and the private sector, including Facebook.

The workshop is part of a broader project on preventing and combating terrorism in the Middle East and North Africa (MENA), Southeast Asia and South Asia regions, which is funded from the Trust Fund on Counter-Terrorism managed by UNOCT, by the Government of Japan and the Government of the United Arab Emirates.

INTERPOL's global role in combating terrorism has been widely recognized. In 2017, the United Nations Security Council unanimously adopted Resolution 2396 recognizing the efforts of INTERPOL against the threat posed by foreign terrorist fighters, including through global law enforcement information sharing.

As part of its global counter-terrorism strategy, INTERPOL seeks to counter terrorist threats on digital platforms by reinforcing the social media analysis capabilities of its member countries in the MENA region and Pakistan.

UNCCT provides capacity-building assistance to Member States, upon their request, at the global, regional and national levels. Mandated by the General Assembly, UNOCT was established in June 2017 to provide leadership to the implementation of General Assembly counter-terrorism mandates, to enhance coordination and coherence, and to strengthen the delivery of UN counter-terrorism capacity building assistance to Member States.

Number 2

IoT Security Standards Gap Analysis, from ENISA

Mapping of existing standards against requirements on security and privacy in the area of IoT

ENISA conducts a preliminary analysis of the IoT-related landscape of standards, which indicates that there is no significant gap in standards to bring secure IoT to the market.

This does not mean that the security of the IoT ecosystem as a whole has been addressed by means of standards.

Elements of a holistic approach towards IoT security can be found in a series of standards, however to achieve an overarching approach that protects the entire IoT ecosystem further work is needed.

Accordingly, given the particularity of the IoT ecosystem (e.g. very high scalability, context of use, short time to market and cost drivers), this study does not intend to promote a specific solution for the entire IoT.

Conversely, by identifying and mapping the existing standards landscape for IoT security, the study aims at pinpointing potential areas of improvement and additional efforts in securing the IoT.

In general, there is an identifiable gap in process by which a vendor can assert that their IoT product or service is secure.

On the assertion that standards enable interoperability, the lack of cohesion on the use and application of standards for secure IoT mean that interoperability is not guaranteed even if all devices were to be placed on the market with security features enabled.
The primary argument of the present document is that standards are essential but not sufficient to ensure open access to markets.

In the particular case of security, a large number of processes as well as technical standards have to be in place to ensure that any device placed on the market is assuredly secure.

In this case the present document proposes, in Annex B, a theoretical approach towards a certification and assurance and validation scheme to identify what is sufficient, as a precursor to allow for market access through device, service and process certification.

It should be noted that this approach is inherently theoretical, since it does not take into account relevant concerns such as economic considerations that might affect the viability of applying standards.

The process recommended in this document is intended in part to engender a change in attitude towards device security by making secure IoT the only form of IoT that reaches the market and to give confidence to the market through a mélange of certification, assurance testing & validation, and market surveillance.

The bulk of the material in the present report is contained in Annex A, the mapping of requirements to available standards, and in Annex B, a proposal for the technical basis of market certification.

To read the paper:
https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis

Number 3

NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals'

NIST
National Institute of Standards and Technology

The field has narrowed in the race to protect sensitive electronic information from the threat of quantum computers, which one day could render many of our current encryption methods obsolete.

As the latest step in its program to develop effective defenses, the National Institute of Standards and Technology (NIST) has winnowed the group of potential encryption tools—known as cryptographic algorithms—down to a bracket of 26.

These algorithms are the ones NIST mathematicians and computer scientists consider to be the strongest candidates submitted to its Post-Quantum Cryptography Standardization project, whose goal is to create a set of standards for protecting electronic information from attack by the computers of both tomorrow and today.

"These 26 algorithms are the ones we are considering for potential standardization, and for the next 12 months we are requesting that the cryptography community focus on analyzing their performance," said NIST mathematician Dustin Moody. "We want to get better data on how they will perform in the real world."

Currently, the security of some cryptographic algorithms—which protect everything from online banking transactions to people's online identities and private email messages—relies on the difficulty conventional computers have with factoring large numbers.

Quantum computers are still in their infancy, but their design—which draws upon very different scientific concepts than conventional computers—may eventually enable them to factor these large numbers relatively quickly, revealing our secrets. So post-quantum algorithms must be based on different mathematical tools that can resist both quantum and conventional attacks.

This winnowing of candidates advances NIST's effort to develop these tools. After releasing a report on the status of quantum-resistant cryptography in April 2016, NIST followed up in December 2016 with a call to the public to submit post-quantum algorithms that potentially could resist a quantum computer's onslaught.

The agency spent one year collecting the submissions and another working with the larger cryptography community on a first round of review to focus on the most promising algorithms. Of the 69 submissions NIST received, these 26 algorithms made the cut.

This second round will focus more heavily on evaluating the submissions' performance across a wide variety of systems, Moody said, because so many different devices will need effective encryption.

"We want to look at how these algorithms work not only in big computers and smartphones, but also in devices that have limited processor power," he said. "Smart cards, tiny devices for use in the Internet of Things, and individual microchips all need protection too. We want quantum-resistant algorithms that can perform this sort of lightweight cryptography."

In addition to considering the multitude of potential device types that could use the algorithms, the NIST team is focusing on a variety of approaches to protection. Because no one knows for sure what a working quantum computer's capabilities will be, Moody said, the 26 candidates are a diverse bunch.

"A wide range of mathematical ideas are represented by these algorithms," Moody said. "Most fall into three large families—lattice, code-based, multivariate—together with a few miscellaneous types. That's to hedge against the possibility that if someone breaks one, we could still use another."

The three families rely on different, promising sources of mathematical difficulty. Lattice cryptosystems are built using geometric structures known as lattices and are represented using mathematical arrays known as matrices.

Code-based systems use error-correcting codes, which have been used in information security for decades. Multivariate systems depend on the difficulty of solving a system of quadratic polynomial equations over a finite field.

Once this second round of review is finished, it is possible there will be a third before NIST announces the post-quantum algorithms that will supplement or replace three standards considered to be most vulnerable to a quantum attack: FIPS 186-4 (which specifies how to use digital signatures), NIST SP 800-56A and NIST SP 800-56B (both of which specify how to establish the keys used in public-key cryptography).

Factoring into this decision will be the state of quantum computer development as the months go by. Quantum computers may still be years

away, said Moody's colleague Gorjan Alagic, but many designers are focused on developing them.

"There's no indication that the technological leap to a practical quantum computer will happen soon, but people are spending a lot of effort on it," said Alagic, a mathematician and computer scientist at the University of Maryland and a NIST guest researcher. "It's reasonable to assume it might happen faster, so we want to develop these algorithms quickly and responsibly."

For more information, see the NIST Computer Security Resource Center's announcement of the 26 candidates at:

https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates

https://csrc.nist.gov/publications/detail/nistir/8240/final

Number 4

ENISA Threat Landscape Report 2018

2018 was a year that has brought significant changes in the cyberthreat landscape.

Those changes had as source discrete developments in motives and tactics of the most important threat agent groups, namely cyber-criminals and state-sponsored actors.

Monetization motives have contributed to the appearance of crypto-miners in the top 15 threats.

State-sponsored activities have led to the assumption that there is a shift towards reducing the use of complex malicious software and infrastructures and going towards low profile social engineering attacks.

These developments are the subject of this threat landscape report.

Developments have been achieved from the side of defenders too. Through the emergence of active defence, threat agent profiling has led to a more efficient identification of attack practices and malicious artefacts, leading thus to more efficient defence techniques and attribution rates.

Initial successes through the combination of cyberthreat intelligence (CTI) and traditional intelligence have been achieved.

This is a clear indication about the need to open cyberthreat intelligence to other related disciplines with the aim to increase quality of assessments and attribution.

Finally, defenders have increased the levels of training to compensate skill shortage in the area of cyberthreat intelligence.
The vivid interest of stakeholders in such trainings is a clear indicator for their appetite in building capabilities and skills.

Recent political activities have underlined the emergence of various, quite novel developments in the perceived role of cyberspace for society and national security.

Cyber-diplomacy, cyber-defence and cyberwar regulation have dominated the headlines.

These developments, when transposed to actions, are expected to bring new requirements and new use cases for cyberthreat intelligence.

Equally, through these developments, existing structures and processes in the area of cyberspace governance will undergo a considerable revision.

These changes will affect international, European and Member States bodies.

It is expected that threat actors are going to adapt their activities towards these changes, affecting thus the cyberthreat landscape in the years to come.

In summary, the main trends in the 2018's cyberthreat landscape are:

- Mail and phishing messages have become the primary malware infection vector.

- Exploit Kits have lost their importance in the cyberthreat landscape.

- Cryptominers have become an important monetization vector for cyber-criminals.

- State-sponsored agents increasingly target banks by using attack-vectors utilised in cyber-crime.

- Skill and capability building are the main focus of defenders. Public organisations struggle with staff retention due to strong competition with industry in attracting cybersecurity talents.

- The technical orientation of most cyberthreat intelligence produced is considered an obstacle towards awareness raising at the level of security and executive management.

- Cyberthreat intelligence needs to respond to increasingly automated attacks through novel approaches to utilization of automated tools and skills.

- The emergence of IoT environments will remain a concern due to missing protection mechanisms in low-end IoT devices and services. The need for generic IoT protection architectures/good practices will remain pressing.

- The absence of cyberthreat intelligence solutions for low-capability organisations/end-users needs to be addressed by vendors and governments.

To read the report:
https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

Number 5

Experts from financial supervision, politics and industry took part in the discussions in Bonn

BaFin's first symposium on combating money laundering and terrorist financing

BaFin Federal Financial Supervisory Authority

"If anyone in the private sector still believes that combating money laundering is unimportant, they clearly aren't up-to-date." With this message, BaFin Chief Executive Director Dr Thorsten Pötzsch opened the first BaFin symposium on combating money laundering and terrorist financing, held in Bonn on 12 December.

500 representatives of banks, insurance companies, public authorities, and associations attended Dr Pötzsch's opening speech, in which he pointed out that combating money laundering and terrorist financing has significantly grown in importance both in terms of regulation and in terms of public perception.

Dr Jens Fürhoff, Director-General of the Prevention of Money Laundering Directorate at BaFin, and Bettina Volprecht, Head of the Internal Communications, Internet and Central Event Management Division at BaFin, acted as hosts for the event, which took place in the German Bundestag's former plenary chamber at the World Conference Center in Bonn. Dr Jan-Gerrit Iken (Commerzbank AG), Thorsten Höche (Association of German Banks – Bundesverband deutscher Banken), Daniel Thelesklaf (Moneyval – the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism), and Dr Fürhoff took part in the panel discussion on the future direction of money laundering prevention.

One interesting observation was that banks are already using artificial intelligence to detect money laundering. BaFin's new guidelines for the interpretation and application of the German Money Laundering Act were received positively.

Interpretation and application guidelines

The presentation by Tatjana Leonhardt and Golo Trauzettel (BaFin) focused on the guidelines and the new Money Laundering Act. They began by putting the provisions within a national and an international legal context and highlighted the dynamic nature of the guidelines – which are not static but continuously changing.

They also looked into the regulatory content of the guidelines in detail. For instance, all obliged entities are required to draw up a risk analysis as part of risk management.

Money laundering reporting officers, who play a key role, cannot be linked to any other organisational departments or units reporting directly to senior management.

In addition, BaFin rigorously scrutinises applications for an exemption from the obligation to appoint a money laundering reporting officer and the appointment of senior management members as money laundering reporting officers.

Leonhardt and Trauzettel went on to outline internal safeguards and customer due diligence and record-keeping obligations.

Leonhardt concluded by stressing the magnitude of the challenge of finding the right balance between a risk-based approach and the principle of binding provisions while drawing up the interpretation guidelines.

Olaf Rachstein (Federal Ministry of Finance – Bundesministerium der Finanzen) described the key points of the 5th Anti-Money Laundering Directive, which EU Member States are required to transpose into national law by 10 January 2020.

To read more:
https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2018/fa_bj_1812_Fachtagung_Geldwaeschebekaempfung_en.html

Number 6

International hacker-for-hire jailed for cyberattacks on Liberian telecommunications provider

National Cyber Security Centre
a part of GCHQ

A British cyber criminal has been jailed for conducting attacks that disrupted a Liberian telecommunications provider, resulting in losses estimated at tens of millions of US dollars.

Daniel Kaye pleaded guilty in December 2018 to creating and using a botnet and possessing criminal property.

He was sentenced to 2 years and 8 months following an investigation led by the NCA's National Cyber Crime Unit.

Kaye began carrying out intermittent DDoS on the Liberian telecommunications provider Lonestar MTN in October 2015 using rented botnets and stressor.

He was hired by a senior official at Cellcom, a rival Liberian network provider, and paid a monthly retainer.

From September 2016, Kaye used his own Mirai botnet, made up of a network of infected Dahua security cameras, to carry out consistent attacks on Lonestar. In November 2016, the traffic from Kaye's botnet was so high in volume that it disabled internet access across Liberia.

The attacks had a direct and significant impact on Lonestar's ability to provide services to its customers, resulting in revenue loss of tens of millions in US dollars as customers left the network.

A European Arrest Warrant was issued for Kaye and when he returned to the UK in February 2017, he was arrested by NCA officers.

Number 7

NASA employee data left exposed due to misconfigured app

National Cyber Security Centre
a part of GCHQ

A misconfigured app has exposed NASA employees' personal details including their names and email address, as well as details about ongoing projects, according to a security researcher.

The data was exposed for three weeks in 2018 after an administrator set permissions in Jira incorrectly.

A filter misconfiguration was also found exposing how NASA tasks and categorises projects and who oversees them.

According to security researcher Avinash Jain, a system administrator may have misunderstood the definition of "all users" and "everyone" when assigning permissions to newly-created dashboards within the app, interpreting these terms to mean everyone within the organisation.

Jain added that such access can "give an attacker an idea of what kind of information may be housed within the application and what projects team is working upon along with showing features of different projects."

He reportedly notified the NASA Security Operations Centre and US-CERT on 3rd September 2018, and was informed the issue had been resolved three weeks later, on 25th September.

Many cloud services are intentionally designed to promote collaboration and data sharing, however accidental data breaches can occur when organisations using cloud services fail to apply the security settings needed to keep information private.

Under old models of information security, making some data available to 'everyone' meant 'everyone within the organisation, but no-one else'.

In the cloud it can mean that same thing, or by design it can mean that 'everyone on the Internet can see it'.

The NCSC has published measures which organisations can take to make such incidents less likely, such as setting sharing to be 'off' by default at: https://www.ncsc.gov.uk/guidance/cloud-security-collection

Number 8

Building Trusted Human-Machine Partnerships

Autonomous systems to assess their own competence and communicate it to human teammates

A key ingredient in effective teams – whether athletic, business, or military – is trust, which is based in part on mutual understanding of team members' competence to fulfill assigned roles.

When it comes to forming effective teams of humans and autonomous systems, humans need timely and accurate insights about their machine partners' skills, experience, and reliability to trust them in dynamic environments.

At present, autonomous systems cannot provide real-time feedback when changing conditions such as weather or lighting cause their competency to fluctuate.

The machines' lack of awareness of their own competence and their inability to communicate it to their human partners reduces trust and undermines team effectiveness.

To help transform machines from simple tools to trusted partners, DARPA today announced the Competency-Aware Machine Learning (CAML) program.

CAML aims to develop machine learning systems that continuously assess their own performance in time-critical, dynamic situations and communicate that information to human team-members in an easily understood format.

"If the machine can say, 'I do well in these conditions, but I don't have a lot of experience in those conditions,' that will allow a better human-machine teaming," said Jiangying Zhou, a program manager in DARPA's Defense Sciences Office. "The partner then can make a more informed choice."

That dynamic would support a force-multiplying effect, since the human would know the capabilities of his or her machine partners at all times and could employ them efficiently and effectively.

In contrast, Zhou noted the challenge with state-of-the-art autonomous systems, which cannot assess or communicate their competence in rapidly changing situations.

"Under what conditions do you let the machine do its job? Under what conditions should you put supervision on it? Which assets, or combination of assets, are best for your task? These are the kinds of questions CAML systems would be able to answer," she said.

Using a simplified example involving autonomous car technology, Zhou described how valuable CAML technology could be to a rider trying to decide which of two self-driving vehicles would be better suited for driving at night in the rain.

The first vehicle might communicate that at night in the rain it knows if it is seeing a person or an inanimate object with 90 percent accuracy, and that it has completed the task more than 1,000 times.

The second vehicle might communicate that it can distinguish between a person and an inanimate object at night in the rain with 99 percent accuracy, but has performed the task less than 100 times. Equipped with this information, the rider could make an informed decision about which vehicle to use.

DARPA has scheduled a pre-recorded webcast CAML Proposers Day for potential proposers on February 20, 2019. Details are available at: https://go.usa.gov/xE9aQ

The CAML program seeks expertise in machine learning, artificial intelligence, pattern recognition, knowledge representation and reasoning, autonomous system modeling, human-machine interface, and cognitive computing.

To maximize the pool of innovative proposal concepts, DARPA strongly encourages participation by non-traditional proposers, including small businesses, academic and research institutions, and first-time Government contractors.

DARPA anticipates posting a CAML Broad Agency Announcement solicitation to the Federal Business Opportunities website in mid-February 2019. You may visit: https://www.fbo.gov/index?s=agency&mode=form&tab=notices&id=048f413b4c64abc6c0afbc36b09f099d

Number 9

Securing Office 365 with better configuration

National Cyber Security Centre
a part of GCHQ

In December last year we published an advisory detailing how to protect Office 365 accounts against the kind of credential stealing attacks that we had been seeing (https://www.ncsc.gov.uk/alerts/rise-microsoft-office-365-compromise).

We believe that anyone with an Office 365 account would benefit from acting on the security recommendations in this advisory. From small businesses through to large enterprises, implementing measures such as Multi-factor Authentication (MFA) should be a high priority.

This blog post gives you a little background on some of these recommendations and introduces important new security guidance published by Microsoft (https://news.microsoft.com/en-gb/2019/01/07/government-backs-office-365-cloud-move-after-microsoft-guidance/).

More cloudy by the day

Business adoption of cloud computing continues to grow rapidly. To put this in perspective - EuroStat noted that 42% of UK enterprises depended on cloud computing services in 2018, compared with 24% in 2014 (https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises).

Regular readers will not be surprised to learn that cyber attackers are also following this trend, shifting their focus to the cloud.

They're also using tried and tested techniques, such as password guessing and phishing campaigns, to spearhead their attacks.

Rapid adoption across organisations of all sizes, has made Office 365 a particularly juicy target.

Our advisory, and Microsoft's own guidance aim to address the increased level of unwanted attention which this popularity is generating.

Use Multi-factor Authentication (MFA)

Before going on to look at Microsoft's security advice, I want to make a plea for Multi-factor Authentication. You should be using some sort of MFA to access their cloud services.

Sometimes called 2-factor authentication, two-step authentication or 2FA, this is your account's first line of defence, and it's a good one. If you're not already doing this, you should get onto it right away.

The single-use codes generated by authenticator apps can be a tough sell in larger organisations.

However, as our MFA guidance explains, the same level of security can be achieved in other, more user-friendly, ways (https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services).

Logging in from a trusted IP address or from a device that has been pre-registered in Azure AD are two examples.

Enterprises can use Conditional Access to enforce the use of MFA. Smaller organisations and individuals should manually check that each of their accounts has enabled a second factor (https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview).

New Office 365 guidance from Microsoft

Microsoft's new security guidance (https://news.microsoft.com/en-gb/2019/01/07/government-backs-office-365-cloud-move-after-microsoft-guidance/) provides up to date advice on how to implement Office 365 installations so that they meet the NCSC's cloud security principles and recommended configurations.

We recommend this advice to enterprises in both the public and private sectors, though it was conceived to explain how UK public sector bodies can configure and use Office 365 to meet the threat at OFFICIAL (https://www.gov.uk/government/publications/government-security-classifications).

The guidance covers all Office 365 services. So, the measures it suggests will give you confidence that you are safely using newer, cloud-only features, and familiar staples such as SharePoint and Exchange.

There are two parts to Microsoft's guidance:

The first document is a response to the NCSC's 14 cloud security principles (https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2MCCr) It also explains how certain configurations map to those security principles.

The second document describes the recommended configurations for an Office 365 service, including step-by-step implementation instructions (https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2MHP5)

In the second document, Microsoft has divided the recommendations into three categories: good, better and best.

The NCSC recommends that enterprises should aim to implement all the recommendations in the good category. And, ideally, the ones in the better category which are included in the Office 365 E3 license.

Moving to cloud-native authentication

This new guidance includes one major change which some may find a little controversial.

We now recommend that hybrid environments – i.e. those that use Active Directory as well as Azure AD – should prefer native authentication against Azure AD rather than ADFS.

In Microsoft-speak this is 'Seamless SSO with Password Hash Sync', configured to use either per-user or Conditional Access MFA.

Password synchronisation with the cloud can feel like a scary thing to do, but we think that organisations using Azure AD as their primary authentication source will actually lower their risk compared with ADFS.

This is because:

- It's actually the hashes of your password hashes that are sent to Azure AD, and not the reusable NTLM hashes commonly discussed in "pass the hash" attacks. (Microsoft explains further in their Azure AD Connect documentation). This means that the credentials sent to Azure AD can't be used to authenticate to any of your on-premise infrastructure that relies on Active Directory.

- We are already relying on Azure AD to make access control decisions regulating who can see which data, hosted in Office 365. So we already need to trust that it's built and operated securely. Storing password hashes doesn't change that security requirement.

- The availability of Office 365 will no longer be affected by any outages or downtime suffered by your on-premise ADFS or Active Directory infrastructure.

- The full set of Microsoft's credential protection technologies only work on accounts that are fully synchronised with the cloud. Benefits include the service identifying users with passwords that are easily guessed, and flagging accounts whose reused passwords have been leaked through data breaches from other services.

- Extensions to Conditional Access that include an assessment of the health of a device will, in the future, probably only be available for users that are authenticating directly to Azure AD.

The guidance goes into more detail about some of the relevant authentication options and associated services, including how to implement them.

Acting on the new guidance

We recommend that organisations already using Office 365 review their deployments against the NCSC advisory and the new guidance published by Microsoft, treating their recommendations as the minimum you should put in place.

Smaller organisations will find the mitigations in the advisory more relevant, larger organisations and the public sector should also use the more detailed guidance.

If you aren't already protecting against the risk of password guessing and leaked credentials using something like MFA or Conditional Access, it's worth repeating - you should get started, right now!

What next?

Cloud products and the way we use them will continue to change and develop over the next few years.

It's therefore worth planning to periodically review the configuration of all the SaaS instances used by your organisation, including a check to see whether the vendor has updated their recommendations.

If you have any questions for us about the recommendations in the guidance, or have any comments, please leave a comment below, or use the Contact us form to get in touch directly.

We'd also love to hear from other vendors whose services are popular with the UK public sector if you're writing guidance about how you meet our 14 security principles and/or how you'd recommend configuring a service to meet the threat at OFFICIAL.

To read more:
https://www.ncsc.gov.uk/blog-post/securing-office-365-better-configuration

Disclaimer

Despite the great care taken to prepare this newsletter, we cannot guarantee that all information is current or accurate. If errors are brought to our attention, we will try to correct them, and we will publish the correct information to the LinkedIn and Facebook pages of Cyber Risk GmbH.

Readers will make their own determination of how suitable the information is for their usage and intent. Cyber Risk GmbH expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

Cyber Risk GmbH and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided on this newsletter, or our web sites.

We are not responsible for opinions and information posted by others. The inclusion of links to other web sites does not necessarily imply a recommendation or endorsement of the views expressed within them. Links to other web sites are presented as a convenience to users. Cyber Risk GmbH does not accept any responsibility for the content, accuracy, reliability, or currency found on external web sites.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular 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 the association has no control and for which the association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of interpretative;

- 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.

Readers that are interested in a specific topic covered in the newsletter, must download the official papers, must find more information, and must ask for legal and technical advice, before making any business decisions.