Special media of strategic cyber security

Cyberwatch Finland

MAGAZINE 2/2024

IDENTITY ACCESS MANAGEMENT IS A CRUCIAL PART OF CYBERSECURITY

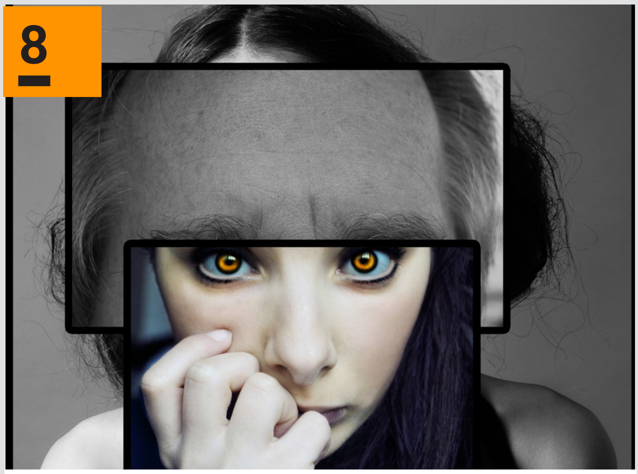
IDENTITY SECURITY IS AT THE FOREFRONT OF MODERN CYBERSECURITY

WHAT KIND OF CYBER-DIGITAL WORLD WILL WE LIVE IN 2024?

Cybersecurity is built by small actions and management of large concepts

CONTENT

2/2024



Cyberwatch Magazine

Special media of
strategic cyber security

PUBLISHER
Cyberwatch Finland
Nuijamiestentie 5 C
04400 Helsinki
www.cyberwatchfinland.fi

THE EDITORIAL TEAM
Editor-in-Chief
Aapo Cederberg
aapo@cyberwatchfinland.fi

Subeditor
Elina Turunen
elina@cyberwatchfinland.fi

LAYOUT
Elina Turunen
elina@cyberwatchfinland.fi

ILLUSTRATIONS
Gencraft
Pixabay
Shutterstock

ISSN 2490-0753 (print)
ISSN 2490-0761 (web)

PRINT HOUSE
Scanseri Oy, Finland

Editorial

IDENTITY ACCESS MANAGEMENT IS A CRUCIAL PART OF CYBERSECURITY

// Aapo Cederberg

Our global security environment is increasingly unstable and anticipating the future is becoming increasingly challenging. We must consider our preparedness and capacity to cope crisis situations, as well as our mental resilience. Various sabotage operations target critical infrastructure and vital services in our society. The threats come from both our physical and digital operating environment. Cyberattacks exploit vulnerabilities caused by the humans as well as technical vulnerabilities in critical systems. The threat has traditionally been assessed through the capacity and the motivation of the threat actors. Assessing a cyber threat is difficult while state actors, cybercriminals and hackers work more closely together. Therefore, motivational factors are also increasingly complex. The dividing lines between politically motivated operations and economically motivated attacks are hard to be detected. This is certainly what many state actors are aiming at, as they are maximising the deterrent effects of deception and the uncertainty it creates. Cyber operations are arguably the most useful spearhead of Russia's hybrid warfare, and attacks are widely targeted at Western civilization.

The hallmark of the great powers has been considered to be nuclear weapons capability and the deterrent effect it causes. Russia says it is waging a hybrid war against Western civilization. In this war, cyber potential has become even more important. It seems that the deterrent effect of nuclear weapons alone is not enough, because they cannot and will not be used. In hybrid warfare, the importance of operational capabilities is emphasised, especially their wide range of means and usability, without crossing the threshold of conventional war. Therefore, the focus of hybrid power is on developing cyber weapons, information warfare methods and cognitive warfare capabilities.

In Ukraine, a physical war is being waged using traditional methods of warfare, the destructive effects of which are much more effective, in crippling critical infrastructure. Many cyber weapons can be used only once and may not be wanted to be revealed as part of this war of annihilation. They are saved for hybrid operations against Western civilization. Therefore, our future scenarios highlight both cyber sabotage and traditional sabotage operations. The most insidious effect of hybrid operations is the psychological pressure exerted on citizens in order to change public opinion and thereby influence political decision-making. This was visible, for example, in the activities and communications of various extremist movements during the European election campaign. The policy of Putin's Russia was supported, even quite openly.

In cybersecurity, there is a task for everyone. The importance of international cooperation is emphasised, national strategies and cyber policy objectives need to be updated, companies need to improve their level of cyber security to meet the requirements of the NIS2 directive. Perhaps the most important thing, however, is each citizen's own competence and behaviour in the digital domain. The main reasons for the successful cyberattacks are still slow update rhythm for technical vulnerabilities and weak passwords, i.e. carelessness in taking care of digital identity management. If these two areas could be improved, it would be much more difficult to carry out successful cyberattacks.

Cyberwatch Finland wants to do its share in this area as well, which is why we are delighted to publish our cooperation arrangement with ID-North. They are specialized in IAM (Identity Access Management) processes, which is easily forgotten as one of the most critical areas of cybersecurity. An identity-driven cyber strategy reduces the attack surface and improves the ability to detect data breaches targeting your organization. The responsibilities and tasks of corporate management are increasing. Through the requirements of the ISO 27001 information security standard and the NIS2 directive regulations, companies need qualified ID security. ID security is part of responsible cyber security policies and functional cyber hygiene. Two-factor authentication should already be self-evident for everyone. Cyberwatch's network analysis effectively reveals cybersecurity gaps and risks, which is a robust basis to improve the level of cyber resilience. Therefore, it is also a good basis for clarifying and improving the level of identity management.

It's time to get the basics of cyber hygiene in good shape and to remember the management's growing responsibility for cyber security as a whole. Let's take care of each other and remember the importance of the crucial actions of cybersecurity. ■

AAPO CEDERBERG

- Managing Director and Founder
- **Cyberwatch Finland**

CYBER OPERATIONS IN UKRAINE

// Alex Crowther

The unprovoked Russian invasion of Ukraine has been one of the most reported-on conflicts in history. Open-source intelligence (OSINT) specialists discuss events on and off the battlefield immediately after they occur. One area that is under-reported, however, is cyber operations. Given that the Russians have aggressively used cyber operations in the past including 2007 against Estonia, 2008 against Georgia, 2014 against Ukraine, and 2016 in the United States, the seeming lack of Russian cyber operations is surprising. The Russians are clearly conducting cyber operations, so why are these operations under-reported? The answer seems to be more that cyber operations are not creating major effects rather than not happening or being overly classified.

There are several lessons learned when examining cyber operations in the Russian invasion of Ukraine. First, cyber operations are not decisive. Second, modern combat moves too fast for inflexible forces such as the Russian to adapt. Finally, cyber resilience works.

CYBER OPERATIONS ARE NOT DECISIVE

Although a number of what could be called “cyber charlatans” promise that they can achieve almost any result using cyber operations, reality is different. Cyber operations in Ukraine demonstrate that decisive cyber operations are rare and that during combat cyber operations are another enabler. To be clear, they can be very helpful in modern combat but as a force multiplier, not as a main effect creator. Although national cyber forces can and do create major effects, these usually take place in the gray zone during notional peacetime, where states seek to stay below the threshold of an armed attack as mentioned in the United Nations Charter. Although there are a lot of tactical-level cyber operations happening, they are integrated into other operations, so we are hearing about the operations in toto, but not the capabilities at use. We could call these "cyber-enabled conventional operations" and "cyber-enabled special operations", where cyber is integrated as an enabler like electronic warfare or information operations. Cyber intelligence has also been successful, such as finding Russian military leaders so they can be eliminated, an example of a cyber-enabled special operation.

This has at least two implications: first, we must treat cyber during combat as part of an overall menu of enablers, where the commander uses all available enablers to improve the quality and effect that combat operations are creating. The second implication is we must teach our combat leaders about the utility of all available enablers including cyber operations. Many leaders do not understand the use of enablers in general and cyber in particular. This means that we need to integrate cyber and other enablers fully into professional military education so that planners and commanders both seek to integrate cyber into their kinetic or maneuver operations from the very beginning.

Since Ukraine shows cyber to be another enabler, US allies and partners should consider grouping several different enablers under the category called something like “information”. This might mitigate the current issue of ‘silos of excellence’ which plagues several military and civilian organizations, where there is no cross-cutting function to force collaboration between the different information capabilities.

RUSSIAN FAILURES

Their cyber operations prior to the unprovoked invasion of Ukraine showed that Russians can be good at set-piece operations, where they have the time to plan and resource and operation. This is particularly important with cyber operations, as the initial penetration of a network can require months of work even in a static environment. This is not so in Ukraine. Although Russians are doing well at cyber enabled information operations, commentators have pointed out in 2022 and 2023 that the Russians were failing at offensive cyber operations. The fluidity of combat in Ukraine, where weapons systems can be deployed and replaced within a matter of weeks or months, does not allow the Russians time to properly plan or prepare for operations, which would significantly degrade the effectiveness of their cyber operations.

A POTENTIAL IMPACT

When states no longer have to stay in the gray zone, it is often more effective to just perform a kinetic operation rather than a cyber operation. If you do not care if a power station survives, why take it off the grid with a cyber attack when a missile is faster, easier, and provides more of an effect? The Russians are seeking to create different effects that their previous successful cyber operations in places like Estonia and Georgia and are not motivated to stay in the shadows. As cyber effects have not yet developed enough to create the kinetic effects of an operations like 9/11, and the Russians have literally everything short of nuclear weapons their disposal, there are few effects they can create via cyber (someday) that they can't do (today) with some other, typically more kinetic, capability, so the Russians just take the easy way and deliver a kinetic effect.

Focusing on kinetic effects in Ukraine also allows the Russians to realign cyber forces to an area where they have excelled in the past: political warfare in Europe and the Americas. Political warfare is not only still very dangerous, but also the only tool Putin has left in the toolbox other than threatening the use of nuclear weapons.

RESILIENCE

Russia had moderate success in cyber operations against Ukraine prior to 2022. Once they recognized the nature of Russian cyber operations, the Ukrainians asked for assistance, which several states provided. Additionally, Ukraine embarked on a program of cyber resilience.

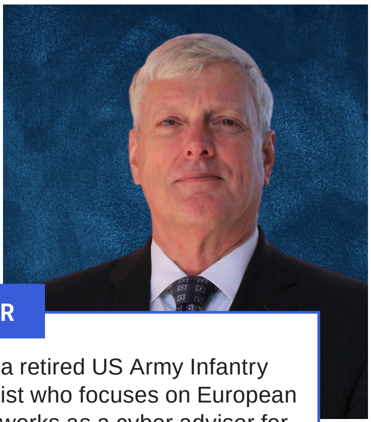
Resilience works; Estonia provides an example. It is one of the most informationized societies on earth but have overcome their cyber problems with the Russians. That is because they swore after 2007 that they would never let that happen again and integrated cyber resilience into their national security architecture. Ukraine has also achieved a degree of resilience. Unfortunately, because it is hard to prove a negative, and because successful cyber resilience is boring as "nothing is happening", resilience is not discussed in detail except amongst cyber security specialists.

The key to resilience is awareness. Just like improvements in the Ukrainian NCO corps, their cyber resilience has worked very well so there are not as many opportunities for the Russians. Ukrainians systems are better defended and are better at mitigation during and recovery after Russian cyber operations.

CONCLUSION

Although Russians are not very flexible and have a hard time adapting to the speed of modern warfare, they are still there and still conducting cyber operations. They will continue to plan and execute set-piece operations with a certain amount of success and will continue to try to conduct cyber operations at speed, with limited success. Understanding that cyber is more of an enabler in combat situations, combined with an emphasis on information related enablers, can ensure that commanders at all levels integrate effects into their planning and operations to improve the results of their maneuver and kinetic operations.

Modern states should embrace resilience as a major goal as we now have several examples of successful resilience-building. This is particularly important as we remember that outside of combat, which should remain fairly rare, cyber will remain a powerful part of political warfare and, given time and capabilities, can create major effects for a state. Because Russia, China, Iran, and North Korea use large amounts of cyber operations during notional peacetime, anyone who is their target can improve their situation and diminish their effects by properly integrating cyber resilience into their national security approach. ■



ALEX CROWTHER

Dr Alex Crowther is a retired US Army Infantry Colonel and Strategist who focuses on European security issues and works as a cyber advisor for friendly governments in Europe, Latin America, and Asia.

IDENTITY SECURITY IS AT THE FOREFRONT OF MODERN CYBERSECURITY

// Sami Mäkelä

The importance of identity security is growing in the digital economy and as the use of artificial intelligence becomes more common. Work is done regardless of time, place, and network. Enterprise data and applications are spread across the cloud and on-premises data centers.

All stages of cyberattacks, i.e. breaking into the network and critical target systems, as well as the actual attack, use identity data. It's even baffling that people's credulity, vulnerabilities, credentials, and identity information were misused in as many as 71% of cyberattacks[1]. Malware was exploited in less than a third (29%) of attacks.

The capabilities of identity security, which is at the forefront of cyber security, must be improved in companies. Organizations need the ability to control who has the right to access and what. Reliable access control of persons, devices, and applications requires well-managed identities and access rights. In identity security, a kind of protective bubble is created around the user's identity. Protection around data has been built long and hard, but in the modern world, this is not enough.

LOGIN CREDENTIALS ON THE DARK WEB ARE A BIG RISK

Login credentials, e.g. usernames and passwords purchased from the dark web, i.e. the anonymous internet, are a good example of a big risk. Anyone can buy login credentials for people's work emails or even admin credentials for information systems and databases. A hacker can use an email account to gain access to other systems by using, for example, password reset functionality. With an email account, a hacker can start phishing for information and ask for access to various applications. The situation is more serious if a hacker gets hold of admin credentials intended for application administrators. Additional user accounts that can be exploited for criminal purposes may be found in databases.

Cybercriminals no longer need special technical skills, unlike 10 years ago, as tools used for attacks can be purchased online. Cyberattacks were carried out in an average of 84 minutes after the hacker had obtained the credentials for access[2]. At its fastest, it only took three minutes.

Management must be aware of the dangers and risks found in the dark and deep web. There are competent tools for identifying risks. For example, Cyberwatch's solution can be used to map what information is available about a company and its personnel on the dark web. The report provides valuable information for making high-quality cybersecurity strategies or action plans. The data can be used by companies to take measures to strengthen cyber and identity security, such as removing compromised user accounts and credentials.

OVERLY BROAD ACCESS RIGHTS ARE A COMMON PROBLEM

The management is responsible for ensuring that the organization's cyber security strategy is up-to-date and covers various threats as comprehensively as possible. With identity-based cybersecurity, management effectively protects its organization and fulfills its legal obligations. This is necessary because identities are at the absolute forefront of cyberattacks.

Detecting a data breach is difficult if a hacker gains access to an employee's email or company information systems with the usernames and credentials they have acquired. The behavior of a cybercriminal may look just like that of a real employee of a company. Employees often have overly broad access to the company's data and information systems, which makes it significantly easier to carry out data breaches. The risk is especially high when talking about administrators. Managing admin accounts requires special care.

IoT devices with network connections which are connected to applications can create a major attack surface. During installation, devices have been given administrator-level access rights, which have not been reduced since. The management of device identities and access rights is often inadequate. By 2025, IDC estimates that there will be an estimated 41 billion internet-connected devices.

In the 'Identity-First Security' model, employees, devices, and applications have identities. Identity security must be in place for an organization to operate according to the Zero Trust model. After all, the basic principle of Zero Trust is that no device, user, or other individual actor is trusted by default. This requires reliable identification of the user and the device and a secure connection before access to the application is allowed. Identity security measures, such as updating passwords and removing unused accounts, throughout the lifecycle of identities, are needed. Access rights shall be kept up to date.

NORTH

MORE RESILIENCE AGAINST CYBER SECURITY THREATS

In our view, identity security covers three different areas. The first is related to the everyday life of employees. How is logging in to information systems done and how are people and devices identified? The second area covers the administration of identities and access rights, as well as how identities can be integrated into an HR system and how to automate administration based on HR data. The third dimension relates to governance, guidance, and approval processes. It is important to define principles on how and by whom access rights can be granted to different systems. Good governance also means continuous monitoring of the given access rights and compliance with the 'Least Privilege Principle'.

The 'Least Privilege Principle' is also at the heart of the Zero Trust model. This means that all employees have the least number of privileges they need at work. No more, no less. Broad and deep privileges are exploited to carry out attacks, and hackers can do a lot of harm by using these. Access rights providing high privileges must be admitted and controlled very carefully.

Effective identity security means highly digitalized processes and continuous maintenance of identity data. Accounts and access rights must be granted and removed at the right time to make sure that, for example, people who have left the company no longer have active access to the systems. Ensuring this in practice is very difficult without purpose built digital tools. Artificial intelligence can be used to monitor and analyze large amounts of data in identity security and to identify anomalies that humans are not capable of.

BASIC ID HYGIENE IS IMPORTANT

An identity-driven cyber strategy reduces the attack surface and improves the ability to detect data breaches targeting a company. It helps to get rid of unnecessary licenses and access rights and leads to potential cost savings. Efficiency is improved if access rights can be delivered quickly to employees. Identity security is needed to comply with regulations such as GDPR, NIS2, and CRA. Applicable from October 2024, NIS2 calls for enhanced identity security in many ways. Companies operating according to the ISO 27001 standard require competent identity security.

Basic ID hygiene must be in order. It means two-factor authentication when logging in to all applications, which prevents criminals from exploiting the credentials they have acquired. All identities, people, and devices need right-level access rights and good control. The importance of identities is also demonstrated by new Identity Threat Detection and Response (ITDR) solutions, which help identify and respond to threats related to identities and identity infrastructure. The solutions detect suspicious activities and protect identities, as well as improve the company's cyber security.

Are you familiar with the present status and vulnerabilities of your organization's identity security? An agile survey to identify risky identities and analysis of the maturity of an organization's identity security provide clear steps to improve your company's cyber security. ■

[1], [2] CrowdStrike 2023 Global Threat Report

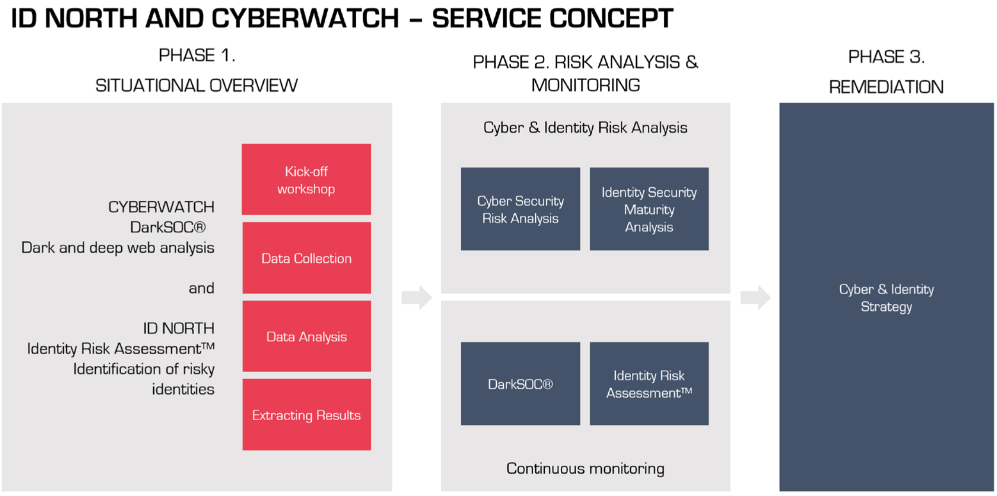
SAMI MÄKELÄ

ID North, Chief Technology Officer

I began my career as a system developer and transitioned into information security in the late nineties. Since then, I have worked both practically and strategically as a consultant and co-founded companies in leadership roles. My primary focus is on Identity Security, encompassing IT, business, security, governance, risk, and compliance.

ID NORTH AND CYBERWATCH JOINT CYBERSECURITY SERVICE

ID North and Cyberwatch Finland have jointly developed a service that helps organizations in a rational way to become aware of their current cybersecurity maturity and risk posture. It presents customers with intelligence both on unmanaged and risky identities within the organization's environment and discovers what information about the organization and its personnel can be found on the dark web. The resulting analysis report provides valuable information and recommendations for enhancing the cybersecurity posture.


ID NORTH AND CYBERWATCH – SERVICE CONCEPT
PHASE 1.
SITUATIONAL OVERVIEW
CYBERWATCH
DarkSOC®
Dark and deep web analysis
and
ID NORTH
Identity Risk Assessment™
Identification of risky identities
Kick-off workshop
Data Collection
Data Analysis
Extracting Results
PHASE 2. RISK ANALYSIS & MONITORING
Cyber & Identity Risk Analysis
Cyber Security Risk Analysis
Identity Security Maturity Analysis
DarkSOC®
Identity Risk Assessment™
Continuous monitoring
PHASE 3.
REMEDIATION
Cyber & Identity Strategy

ID NORTH AND CYBERWATCH SERVICE CONCEPT

Our service concept is divided into phases. The outcome is a roadmap and strategy conception for improving the customers' cybersecurity posture.

The service concept is based on an up-to-date situational overview of cybersecurity and identity management within the customer's environment. The first phase covers the two most forefront areas for a customer to understand their current cybersecurity risk posture: Cyberwatch's darkSOC® review and ID North's Identity Risk Assessment™ risky identities discovery.

Cyberwatch's darkSOC®: focuses on dark and deep web analysis, helping organizations identify and respond to hidden cyber threats. DarkSOC® analysis is used to create a situational picture of an organization's cyber security status and to identify and assess risks that may impact the organization's operations.

ID North's Identity Risk Assessment™: focuses on examining an organization's user accounts and identities and identifying risk identities such as unused accounts, shared accounts, and admin accounts. This provides a rational observation from an internal perspective on the organization's identity risk posture.

In the first phase we perform following steps:

1. **Kick-off workshop:** Define the objectives of the work and plan the practical implementation.
2. **Data Collection:** Collect data from agreed-upon sources and dark web searches to identify risks and vulnerabilities.
3. **Analysis and Reporting:** Analyze the collected data and prepare a comprehensive report on the results.
4. **Results Review:** In a joint meeting with the customer, discuss the results and agree on further measures and development targets.

This new service concept provides a fast and efficient approach for improving an organization's cybersecurity! The complete service is always tailored together with customers. ■

TIINA HENTUNEN-VANNINEN

- More information: Tiina Hentunen-Vanninen
- email: tiina.hentunen@id-north.com
- **Sales manager at ID North Finland**

MACHINE IDENTITY MANAGEMENT IN THE MODERN BUSINESS WORLD

// Matti Särkisilta

In today's digital environment, machine identity management has become a significant part of cybersecurity. Machine identity refers to a digital identity that is used by an automated system. These can be, for example, robots that perform automation tasks, IoT devices or industrial machines that retrieve updates or production instructions over a data network.
Each device or robot can have one or more machine identities, such as user accounts, that allow them to identify themselves in the services they use. Artificial intelligence identity management is also part of machine identity management.

MEANING, CHALLENGES, AND RISKS

Machine identities are used in many different situations, such as RPA (Robotic Process Automation) tasks, where robots perform repetitive processes, or IoT devices that communicate with each other and with cloud services. The number of machine identities is growing exponentially; The Digital Strategy Department of the European Commission estimates that there will be 41 billion IoT devices in use in 2025 (1).

Managing these identities is critical to preventing misconduct and protecting company resources. The biggest challenge in managing machine identities is ensuring that the identity management system has information about what these identities have access to and who manages those accounts. For example, if a machine identity service account falls into the wrong hands, it could give an attacker extensive access to critical company resources.

It should also be remembered to separate accounts in different environments. It is still very common to notice in production that some account (created during development) has too broad permissions, sometimes even admin-level rights.

BEST PRACTICES

Creating and managing secure machine identities starts with using separate accounts and minimizing permissions. Every machine identity should have a clearly defined purpose and limited rights limited to the functions that are necessary. Each machine identity should be controlled by a designated person. After all, employees also have a supervisor who is responsible for their access rights.

For example, Financial Manager Pekka owns a robot RPA_TalHa_maksut that automatically pays invoices. The robot uses the provided system IDs and makes payments according to predefined rules. This robot does not need the rights of an ordinary employee, such as access to the intranet or other general company resources.

Secure authentication methods, such as passwords, keys, and certificates, are essential for protecting machine identities. Role-Based Access Control (RBAC) ensures that each identity can only access the resources to which it is entitled. It is important that the rights related to the machine identities owned by Bob are strictly controlled and that their access rights are clearly defined.

Continuous monitoring and auditing are essential for managing machine identities. It is important to monitor how these identities are used and detect anomalies that may indicate abuse. Tools and methods such as log analytics and behavioral analytics can be utilized to ensure effective monitoring.

It is also important to remember and take into account the deletion of rights at the end of the machine identity's life cycle so that unnecessary rights or user IDs are not left in different systems. User IDs and user rights must also be regularly checked at the end of the system to ensure that no unnecessary unused IDs have been left hanging.

TECHNOLOGIES AND TOOLS

Managing machine identities manually is challenging and virtually impossible in organizations due to the number of machine identities and their user rights. In one of its analyses, CyberArk estimated that there are 45 times more machine identities than real human identities (2).

Modern identity security solutions offer ways to manage machine identities efficiently, such as IAM (Identity and Access Management) and PAM (Privileged Access Management) products. These tools help create, manage and enforce identities and ensure that access is granted only to legitimate actors. Other cyber security solutions, such as Security Information and Event Management (SIEM) systems and behavior analysis tools, can also be used to monitor machine identities.

FUTURE TRENDS AND CHALLENGES

Artificial intelligence and machine learning can also provide aids in managing machine identities. These technologies can improve predictive analytics and automated threat response. Potential challenges in the future are particularly related to the growing number of devices and more complex attack vectors. Organizations need to remember to constantly update their strategies and software to stay secure and keep up with developments. The latest cautionary example is a data breach by the City of Helsinki, where the main cause was an unupdated remote connection server (3).

SUMMARY AND FIVE TIPS FOR THE FUTURE

Machine identity management is a key part of modern cyber security and identity security, but many organizations could improve this. Organizations need to adopt best practices, leverage powerful tools, and stay up-to-date with the latest developments. This ensures that all identities, both human and non-human, are properly protected and managed.

FIVE TIPS FOR MANAGING MACHINE IDENTITIES

1 Machine identities should have as few and limited access rights as possible

2 Access rights to machine identities should be centrally controlled only by the owner

3 In connection with the removal of old robots, the removal of rights and IDs must also be added to RPA processes

4 All tools should have password or key encryption enabled or certificate-based authentication

5 Be aware of the risks and try to prevent misuse by other means if you cannot influence the above-mentioned matters

> **Do you know the maturity of your organization in the area of machine identity management?**
>
> **Agile mapping of machine identity access rights provides a concrete understanding of the current state of your organization.**

References:

1) https://digital-strategy.ec.europa.eu/en/policies/next-generation-internet-things
2) https://www.cyberark.com/resources/blog/why-machine-identities-are-essential-strands-in-your-zero-trust-strategy
3) https://www.hel.fi/fi/paatoksenteko-ja-hallinto/tietomurto

MATTI SÄRKISILTA

Identity Architect, ID North

I started my career as a full-stack programmer and in the beginning of 2010, I transitioned into technical architect in a cybersecurity project. Since that I've worked as a consultant mostly as an architect in information security. I've worked long in digital identity management and most of my projects have been in the area of telecommunications, insurance, and financial services, where the main challenges have been legal regulation especially in the area of cybersecurity and compliance.

WHAT KIND OF CYBER-DIGITAL WORLD WILL WE LIVE IN 2024?

// Kimmo Rousku

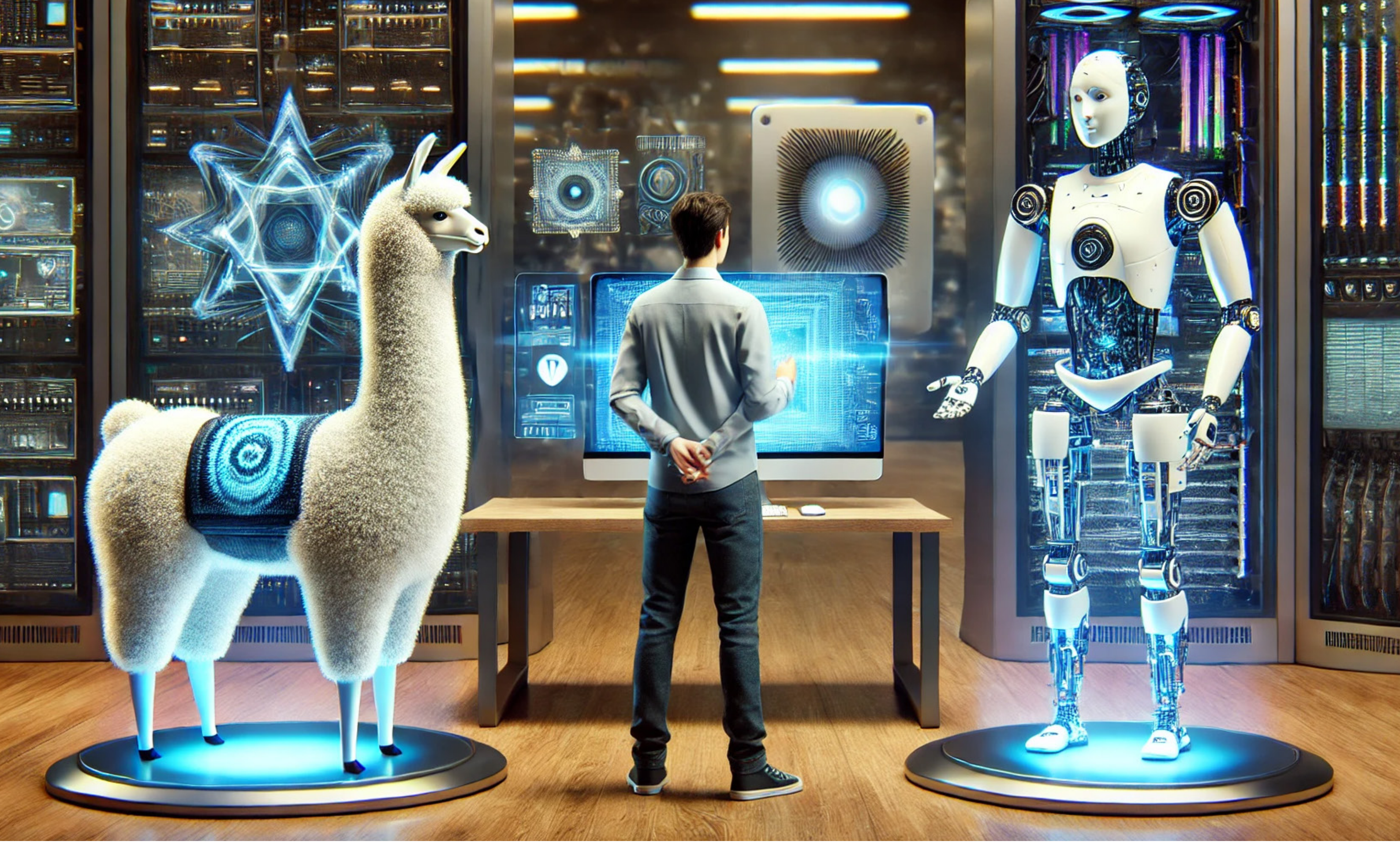
PHYSICAL WORLD VS. DIGITAL WORLD

How many of you have had a break-in at home or in your holiday home in the last year or three? As a novice mentalist, I sense that some of you will recall an unpleasant moment when such a burglary was discovered. When do you remember reading about a traditional bank robbery in Finland? I think our society has become safer in this respect. Similarly, our security in the physical world has been improved by joining NATO.

And when was the last time you received a contact or message on your digital device or service that you recognised as some kind of digital fraud? As a mentalist, I dare say some of you even within the last hour. If crime is declining in the physical world, it is growing exponentially in the digital world. You can see this from the fact that every few days we read in the media about warnings or experiences of successful digital fraud, or know someone who has lost their data and/or money in recent years.

The previous intro looked at the digital world from the point of view of ordinary users or citizens. What about businesses and other organisations? The same exponential increase in attacks and other malicious phenomena can be seen there. Ten years ago, news of a cyber attack or data breach against a Finnish company (which became public) was a rare exception indeed. Now, such news is no longer alarming and, unfortunately, the same exponential growth is taking place with a slight delay in volume compared to attacks on citizens. So we can continue to expect bad news.

The entry into force of the NIS2 Directive/Cyber Security Act and the obligations it brings, e.g. "Article 14 Notification of incidents and cyber threat to a non-authority", i.e. "An operator shall promptly notify the recipients of its services of a significant incident if the significant incident is likely to adversely affect the provision of the operator's services", is likely to raise the profile of incidents against these operators even further. Not all anomalies are due to cyber-attacks, some are simply traditional technical failures.



WE ARE AFFECTED BY CYBERCRIMINALS, BY PEOPLE THEMSELVES AND BY STATE ACTORS

In a perfect world, nothing bad would ever happen to us in the digital world. In practice, we face at least three distinct threats: cybercrime, our own mostly human, accidental mistakes, and state actors.

Cybercrime is growing significantly, as shown by data from the authorities (the National Cyber Security Centre, the Office of the Data Protection Ombudsman, the police, the Finance Finland) and international reports. The most visible cybercrime is directed at citizens, who are bombarded with ever-changing methods on all digital services and devices, trying to get us to click on a link, install a program, open an attachment, or add someone to our social network. And let's not forget the traditional phone call, which seems to be on the rise again this year. In addition to citizens, various forms of ransomware attacks against companies and organisations have become more common since we first warned about them in 2018-2019.

Based on last year's data, my personal estimate is that we lose <€200 million> in criminal proceeds to cybercriminals every year. The amount could be significantly higher, as individual companies in Finland may have lost as much as €20 million. The official statistics are only the tip of the iceberg, as many organizations, not to mention individuals, do not report the loss of money, for reasons such as embarrassment (I was so stupid to get scammed) or damage to reputation (customers disappear).

HUMAN ERROR

Another threat directly related to us human activity is human error. Who wouldn't have accidentally sent e-mail to the wrong recipient or discussed matters in a public space that should not have been discussed there? Or where can you find an ICT professional who hasn't inadvertently forgotten to follow a procedure by the book, or forgotten to turn on a critical setting in a hurry? Or where do you find an application developer who always produces code that is 100% bug and vulnerability free, or that is always tested before release so that bugs don't make it into production?

In addition to cybercrime, we are also exposed to various attacks, data breaches, security breaches and vulnerabilities due to our own activities. Who can we blame but ourselves? No, you can't blame #AI, but that day will come, until then we humans are still effectively responsible for the information and services provided by AI, we will probably never be able to take responsibility or shift responsibility to AI for anything. Of course, I'm waiting for a clickbait news story that blames AI for causing significant damage, etc.

STATE ACTORS INCREASINGLY IN THE PUBLIC EYE

If cybercriminals attacking an organization want to operate in secrecy, hiding long enough to take over the position and be ready to launch their criminal operation, state actors mostly want to do the opposite. That is, they want to stay hidden for years (decades), or they want to get the necessary information and leave without a trace so that their visit is never discovered. Here, a separate activity of state actors is to do the opposite in a very visible way, such as state-sponsored denial of service attacks or other cyber influence operations, which they want to be visible and prefer to be reported in the media. As with the above approaches, state actors have also become much more active in the digital world, with the coronavirus pandemic forcing them to make greater use of the cyber world and Russia's war of aggression in Ukraine ushering in a whole new era of hybrid, cyber and information influence.

INFORMATION INFLUENCE - THEY ALSO WANT TO INFLUENCE OUR FEELINGS, THOUGHTS AND DECISIONS

All the above methods also influence our feelings, thoughts and, indirectly, our actions. And not only us, but also our organizations and society. If you are scammed once in the digital world, you will remember it for a long time. If you lose personal data and/or money as a result of a data breach of a service, it will certainly make you more cautious or suspicious for a while, maybe even stop using that service.

In addition to these explicit events, we are also influenced more or less directly by information interference. We have been exposed to information manipulation practically all our lives, including those of us born in the 20th century. Advertising is information interference, not as negative as negative or harmful, let alone damaging, information interference, which has become much easier in the 2010s with the proliferation of social media services. Once again we see how new technologies have created new threats for us, albeit with a more real-time ability to communicate and monitor globally what is happening in the world or with our friends.

State-sponsored information influence can be seen, for example, in the form of bot and troll networks on social media channels, individual influencers, or in the form of 'news channels' or other media found on the Internet that even appear to be very genuine. We Finns have been praised for being quite good at recognising and tolerating information influence (resilience) against us, and, for example, there were extremely few attempts to influence our elections in 2024.

On the other hand, both in Finland and globally, the TikTok service, which is used mainly by young people and unfortunately also by minors, has been in the spotlight, especially because of the harmful effects it has on young users. It has also raised concerns about the data it collects. As one colleague said, this new form of "digital drug" is a phenomenon that has taken us completely by surprise and we are still far from realizing the damage that such phenomena are doing to us.

NEW TECHNOLOGIES ARE BRINGING US A WHOLE NEW SET OF THREATS - ARTIFICIAL INTELLIGENCE, QUANTUM COMPUTING AND SERVICE ROBOTS

We live in an era of increasingly rapid exponential development of digital devices and digital services. If it could take a year (decades) for a service developed in the last millennium to become widespread, it can now happen in months. A prime example is the rapid adoption of artificial intelligence services based on large language models (LLMs) in the last two years or less. Like any new technology, it offers enormous potential to process and produce data and other material, but it also offers unprecedented opportunities for cybercriminals and state actors to automate their operations or attacks on a 24/7/365 basis. Similarly, we, the good guys, need to be able to simultaneously develop countermeasures to identify them, also taking advantage of the opportunities presented by AI services.

Another example is quantum computing and quantum computers. Here we may already be irreversibly late, because if future quantum computers can be used to decrypt the encryption we have now, there will certainly be *a lot* of that traffic already stored by certain actors.

What about when service robots with advanced artificial (general) intelligence, also physically very capable, start running around us, moving with agility, and possessing lifting and other abilities significantly more advanced than our human capabilities (muscles)? Personally, I dare say that this will be the greatest opportunity for humanity, but also the greatest threat, and we should start preparing for it now at a global societal level.

HOW DO WE COUNTER THESE THREATS?

1 Cybercrime must be brought into the open - there is no shame in being scammed or cyber attacked. We all need to do more to report and warn about what we see also in our neighborhoods.

2 We need better technical solutions to protect us and prevent these attacks on us across different digital devices and services.

3 Organizations need to ensure that the security solutions they buy to protect their devices and services work as they are supposed to, and that when they fail, they are clearly identified and reported to the *human* resources that may be needed to fix them.

4 All of the above is supported by the NIS2/Cybersecurity Act, which will now come into force in the autumn. While it does not apply to all companies or public sector operators, it provides the building blocks for every organization to ensure that we in Finland are better than average prepared for the threat posed by cybercriminals. Cybercriminals are looking for easy and quick money, and if they cannot break into something easily, they will move on to the next target.

5 Change the way we work. Since there is not and never will be 100% security, a very cost-effective way to increase those percentages is to influence the way we humans behave. I have calculated from various studies that we may have as many as 1,2 million digital users in Finland who do not know, do not dare or do not know how to behave safely in the digital world.

6 International cooperation - we face the same problems everywhere, and by working together more closely we can react faster and hopefully find better solutions together. ■

KIMMO ROUSKU

- Kimmo Rousku is a recognised expert, non-fiction author and lecturer in the field of cyber and digital security and digital transformation. In his spare time, Kimmo Rousku also serves as Vice-Chairman of the Board of Finnish Information Security Association, which reinforces his commitment to information security issues outside his professional career.
- At the forefront of Rousku's work is the societal importance of cyber and digital security and its integration into the everyday life and culture of organisations and people. With four decades of experience as an educator and speaker, his diverse expertise and experience in leadership positions make him a respected speaker and expert in the areas of security communication and culture.
- He plays a significant role as VAHTI General Secretary and Chief Senior Specialist at the Finnish Digital Agency, with a particular focus on leading the activities of the Public Security Digital Security Steering Group.

DATA PROTECTION: A GROWING CONCEPT

// Eneken Tikk & Mika Kerttunen

Data protection is a known notion – confidentiality, integrity and availability of data are a preoccupation of information and cybersecurity efforts. The European Union General Data Protection Regulation (GDPR) makes these features mandatory for personal data processing. Security and privacy are the leading narratives of what it means to protect data. However, data now fuels the transformation of the economy and societies thrive on data-driven innovation and benefits like personalized medicine, new mobility and the convergence of digital and green transitions. Increasingly, welfare and progress rest on non-personal data, and even the ability to de-personalize data for better decision-making. Commodification of non-personal data as high-quality and interoperable data from different domains is expected to increase competitiveness and innovation, thus contributing to sustainable economic growth.

As digitalization has advanced, data has increasingly become a key to value and the value itself. The vault line between data and the phenomenon has been diluted. Follow the money: we have alongside bills and metal coins bitcoins and other forms of de facto digital currency. To a great extent, data about our monetary assets is/are our monetary assets. Similarly, sensitive information from ethnic categorization to individual health to national security has been turned into, transferred to, machine manageable data. Whole new discoveries and synthetic data are made with the help of advanced data analytics and new forms of creation emerge in the virtual worlds. No wonder digital data has become an object of interest and a target of action, both protective and threatening. For the latter, digital data in particular is subjected to theft, destruction and manipulation. For the former, data is being protected by physical, logical and procedural measures but increasingly also legally.

In other words, traditionally the relationship between data and its point of reference has been purely representational; e.g. statistical data provides the values of artefacts or phenomenon but das Ding an sich is elsewhere. This distinction is rather obvious with the traditional formats of data, from carved stones to written papers. Today, however, data witnesses of the intrinsic or instrumental value of the body of data (e.g. statistics; databases) or its individual datapoints. The value data has is highly contextual and relative. For example, [the schoolbook statistic example of] population shoe size data, and changes within, is of financial importance for shoe manufacturers and sellers but an individual data point [43] can be ignored in the very act of purchasing a shoe, it is the shoe that fits. Moreover, data acquires (and builds) value through interrelationships and integration, combination of multiple sources and availability through layered services. As a transformative commodity, data holds strategic value to consumers, businesses and governments alike, both due to its volumes and quality.

The more strategic opportunities embedded in data, the more challenges need to be overcome – domestically, within collective settings, like the EU, and globally, where technologies and content from different jurisdictions blend and compete. While data protection as a notion seems universal, its scope and contents can vary significantly: the legal landscape of data protection is a patchwork of regimes and jurisdictions, some much more efficient than others.

For example, in the EU, any personal data sharing will be subject to full compliance with the EU's strict data protection rules under the GDPR. Globally, it is impossible to pinpoint any particular standard of personal data protection – data breaches mostly fall under domestic privacy laws. Also, while the integrity of information is an increasing issue as tensions between major powers are channeled to information interference and manipulation, there is hardly any global understanding of basic data and information integrity standards. Political priority on commodification of non-personal data expands the surface of potential harmful action against data for criminal and politico-military purposes as well as commercial opportunism. As pointed out above, the EU stands out for its privacy guarantees, while the US has recently made a strong statement against foreign espionage targeting industry and private sector information. Meanwhile, traditional cyber espionage remains a point of contestation and, consequently, largely to be resolved under domestic legislation. Where international law exists that could be applied to abuses of data, notable differences surround its application and implementation. Meanwhile, residing in computer systems and networks, data is a frequent target (or collateral) of cyber-attacks. Prominent politico-militarily motivated attacks on databases include the January 2022 attacks on International Committee of the Red Cross servers hosting personal data belonging to more than 515,000 people worldwide and Ukraine's offensive against Russia's tax database in December 2023. Informationisbeautiful.net lists over 16 billion affected records between 2004 and 2024. Non-personal data breaches are expected to increase with the political drive towards making non-personal data available to all – whether public or private, big or small, start-up or giant.

Importantly, protecting data is no longer about locking it away but making it available, visible, accessible, making sense of it and finding ways to make it work. To gain full value of data, it needs to be in motion, share and scrutinized. It needs to cross borders, break fears and test conventions. It is timely, therefore, to think of what internationally agreed standards of data protection exist or are feasible in the current strategic climate. From the pitch of freedom of information in the early phases of the information society building to privacy to data and network security concerns, the current focus is on data's transformative economic and welfare potential. Accordingly, new issues are emerging regarding transparency and access to data, its quality and integrity as well as ways to balance between privacy and prosperity interests.

THE EU LEADING (ITS OWN) WAY

The European Union's Data Strategy sets the goal of the EU as a society empowered by data. In an advanced information society and data economy, data is key to making better decisions – in business and the public sector. Digital Europe should reflect the best of Europe - open, fair, diverse, democratic, and confident. Consequently, the EU has adopted several legal and policy instruments to support the Digital Decade and the Data Strategy. These are to address the issues identified on the way to an even fuller digital transformation. Data holders tend to withhold data and are reluctant to share it with users, let alone third parties, creating bottlenecks and access imbalances. The lack of technical interfaces and procedures increases the cost of data access and sharing. Absent standards for semantic and technical interoperability, data remains siloed and poorly categorized. Further compounding the issue are the lack of data analytics skills and the lack of interoperability between data and data services.

To facilitate the availability and mobility of data, the Data Governance Act (2022) consolidates the conditions for the re-use data held by public sector bodies, establishes a framework for data intermediation services and promotes the processing of data in public interest. It creates the notion of data intermediation services for wider, more functional, better coordinated and predictable uses of data. The data governance act further establishes data altruism as voluntary sharing of personal data for objectives of general interest, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research.

The Data Act of 2023 obliges data holders to make data in their possession available to a range of recipients, including businesses, individuals as well as the EU bodies. It also seeks to create a fair balance between different actors about the use of non-personal data and related benefits. Its expected outcomes include increased transparency about connected products and related service data to the user and access to a wider pool of data for better decision-making. Other regulatory effects include easier terms for switching between data processing services, conditions for non-personal data security and increased interoperability.

WILL THE WORLD FOLLOW?

The EU's ambitious and thorough approach to data remains largely unmatched. Agile ICT adopters may be headed to a similar direction but for the majority of countries, high standards of especially non-personal data protection and security to function as data-centric societies are a new theme. The effect of this is that data will remain target of attacks and offensive that can be routed through less prepared and capable territories, which renders relevant investigations and remedies problematic. Against the values and goals of the EU and other data economies, this also means a fragmented world where data can be localized, stopped at national borders, controlled and manipulated. Indeed, states have been able to create a framework for technical cross-border data flows and agreed on certain crisis and distress communication protocols as well as basic principles of sharing scientific and technological process data. However, personal data protection and freedom of information remain subject to different domestic requirements and standards of implementation. Non-personal data and its role in economic and societal well-being, in turn, is a rather new issue for the international community.

There are several reasons for this situation to change in the coming years. The best proof of concept will be the EU's ability to demonstrate that transformation through data brings the expected benefits and that an autonomous approach, even among allies, can be fruitful. A second reason derives from the reality of data being targeted for various purposes, which cases risks and harms to states regardless of their political regimes as well as international organizations and the industry. Thirdly, the longer states keep remediating data breaches and other risks on their own, the more issues of information sharing and interoperability persist. Another reason for the liberal democracies will be to try and convince more countries to consider the adverse effect of restrained information flows.

There will be many hurdles to overcome, which also underscores the potential benefit of an open and inclusive talks over the role of data in the contemporary society and ways to protect it. Privacy and security have long been the leading considerations of data protection. However, without proper balancing with access to information and the value embedded in data for societal and economic progress, approaches to data will remain narrow and prejudiced. As the Data Governance Act notes, privacy is just one element in the hierarchy of interests and values for individuals. As the Digital Decade strategy emphasizes, security will need to serve the fundamental values and goals, not the other way around.

Coming to an understanding of the data's many facets and functions will require thorough administrative and societal awareness as the formula will be unique for each society and organization. Making use of data globally will also require breaking paradigms and reconciling a multitude of views – for instance, in the context of international law, the discussion of data as an object or not provides an example of how deep and far different arguments can go and how much depends on their outcome. Few would contest the lucrativeness of data as a military objective – a legitimate target if its nature, location, purpose or use make an effective contribution to military action. However, as some scholars have posited that data cannot be considered an object within the meaning of Article 52 in the Geneva (I) Protocol that creates the legal framework for protecting civilian objects, it remains unclear what, if any, guarantees exist against targeting civilian data such as national databases or social media platforms in conflict. Along come issues of private (sector) data and ways in which industry perspectives could inform not only better security or cyber operations but better processes and decisions.

To use another example, there are very different ways in which states may choose to prevent and combat information influence. In domestic legislation, the approaches to combatting foreign influence and interference include:

- Restrictions to foreign investment, ownership and operational control of strategic industries, critical infrastructure or resources;
- Restrictions to foreign funding of or transactions with parties, political processes, election campaigns and candidates, certain civil society organizations and/or research entities;
- Content and publicity restrictions, e.g., hate speech, violent extremist and terrorist content, manipulated or misrepresented information;
- Integrity of public processes and services, such as broadcasting and news, elections and public decision-making.

Further examples of legally moderating unwanted foreign influence at domestic level include restrictions on technology transfers and restricting other types of interference, for instance radio. In addition to investment and ownership screening, and value or fact limitations on transactions, online content moderation and foreign agent registration constitute frequently applied regulatory mechanisms to address the issue. The more diverse the approaches, the more difficult it becomes to coordinate and prevent harmful and malicious activities targeting or taking advantage of data.

In sum, data protection is more than meets the eye. Instead of hiding data, contemporary European data protection efforts seek to create a safe environment where inevitably aggregated data can be used safely and effectively. Instead of providing only security-from (threats), the EU has moved towards a security-to (be and act) approach which aligns with and expands the four freedoms of the EU. Eventually, to protect data is to protect people. The contemporary information society is an extremely sophisticated and complex formation of stakeholders, interests, technologies and issues that make data protection a balancing act between not just privacy and security but also access to data, data's economic potential and data as property. Where an appropriate point of balance lies, requires thorough understanding of the multifaceted nature of data and representative political domestic and international debate. ■

[1] Data Governance Act (2022/868), EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868, recital 1; European Commission, European Data Strategy. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en; Fair access to and use of data (2023/2854), Eur-Lex, https://eur-lex.europa.eu/eli/reg/2023/2854, recital 1. (All accessed 10 June 2024).

[2] ICRC, "Cyber attack on ICRC: What we know." (16 February 2022; update 24 June 2022) https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know (accessed 10 June 2024).

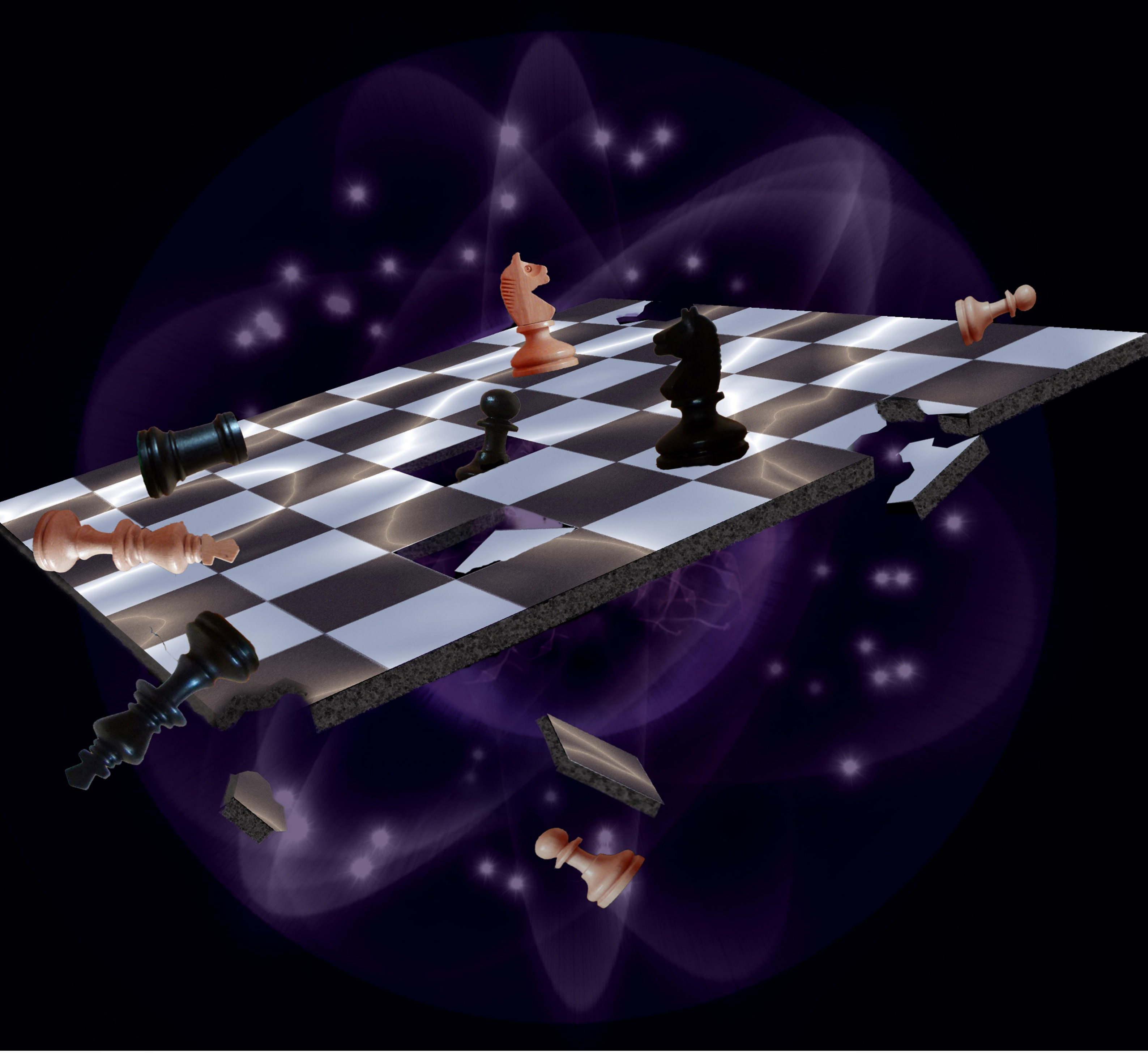
[3] Ukrainska Pravda, "Ukrainian intelligence attacks and paralyses Russia's tax system – photo." (12 December 2023) https://www.pravda.com.ua/eng/news/2023/12/12/7432737/ (accessed 10 June 2024).

[4] A European strategy for data (COM/2020/66 final), EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066 (accessed 10 June 2024).

[5] ibid.

ENEKEN TIKK AND MIKA KERTTUNEN

’ D.Jur Eneken Tikk and D.Soc.Sc Mika Kerttunen are independent experts focused in cyber diplomacy, regional capacity-building and national policy and law questions.



POLISH DEFENCE AGAINST RUSSIAN OPERATIONS IN CYBERSPACE

// Andrzej Kozłowski

Poland has been the target of Russian cyber operations and cyber enabled information operations for years, but after the large scale invasion on Ukraine, Russian activity in cyberspace has significantly increased. Till now, it seems that Russian cyber forces have not achieved any meaningful success in penetrating IT systems in Poland.

WHY HAS POLAND BEEN TARGETED?

Poland has been the main logistical hub for military and humanitarian aid to Ukraine. It has been a key to early success on battlefield as well as the survivor of the Ukrainian statehood. The disruption of this logistical chain or getting detailed knowledge about it via using digital espionage could negatively impact the Ukrainian Armed Forces and give Russian troops advance on battlefield. Not only was it a reason of Russian significant cyberattacks, but also Poland has been on spearheaded Western countries toward imposing stronger sanctions on Russia and therefore Moscow intended to punish Poland for this decisive stance. Last but not least Poland also accepted the largest number of Ukrainian refugees and through using cybermeans Russians aimed at creating mutual factions between Ukrainian and Polish population. All these reasons with treating Poland as the eternal, historical and ideological foe contributed to the significant increase in volume of cyberattacks.

THE EXAMPLES OF CYBERATTACKS AGAINST POLAND

A few days before the Russian large scale invasion there was a ransomware attack against air ambulance service, which led to problems with websites, communications and emails box. Poland was also touched by the cyberattack on Viasat satellite network, which followed the Russian conventional invasions on 22nd of February 2022 but the Polish networks were significantly less affected than Ukrainian ones.

Furthermore, Polish email addresses were flooded with phishing attempts throughout February and March both addressed to mass receivers but also directed to the selected entities to gather credentials to get an authorized access to the resource of the attacked subjects. The attacks tried also distribute malware Service RedLine Stealer used to steal data and users credentials.

The most significant disruption in the critical infrastructure happened in March 2022, when 80% of the Polish train network was inoperable for over a day. Initially media reported about a possible cyberattack, but the investigation showed that it was an incident of IT equipment. The similar situation happened in August 2023, when more than 20 Polish trains were stopped. Again, it was a malfunction of the system than the cyberattacks, but these two incidents showed the worrying flaws in the security of this critical infrastructure in Poland.

Not only were the entities in Poland attacked but also the Polish embassies abroad. The ATP-29 prepared massive phishing campaigns using emails, which should encourage embassies staff to open an attachment or click on hyperlink to the staged website. The attackers used hijacked email accounts and fabricated phishing emails using content that might attract people who work in embassies. It included invitations for banquets, meetings with ambassadors of other diplomatic missions and offers of selling different commodities such as cars with the discounts for diplomats. The aims of this campaign was to penetrate networks of the Ministry of Foreign Affairs.

The salvo of the most advanced malware in Russian arsenal launched at the beginning of the large-scale invasion caused that Russian cyberforces needed time to redesign and redevelop their "cybertools". It caused the lack of meaningful actions till the end of 2022. Then in November, Microsoft revealed that Sandworm, a hacking group tied to the GRU, Russia's military intelligence service, was targeting Ukrainian and Polish logistical networks with new ransomware, known as Prestige. These attacks are among the first Russian state-sponsored attacks that intentionally target NATO members with destructive malware since the large scale invasion against Ukraine began. However, Microsoft and Polish authorities did not reveal who was targeted and the results of Russian attack. Generally in 2022 Polish CSIRT GOV responsible for protection of the governmental networks and systems reported 1 234 040 notifications of the possible incidents in comparison to 762 175 in 2021. The growth was naturally linked with the outbreak of war in Ukraine. A similar situation was detected in military systems and networks. The Head of the Polish Cyberspace Defense Forces general Karol Molenda said that number of attempts to penetrate military networks increased significantly. He added that the number of cyberattack attempts on IT systems and networks in the first quarter of 2022 surpassing the whole total number of 2021.

THE DDOS ATTACKS WAVE

One of the daunting challenge for the Polish systems was the number of Denial Distributed of Service attacks, which doubled in 2022. The character, correlation and the selected targets confirmed the high level of coordination and preplanning. The attacks were realized by Killnet group, which officially declared war on Poland, Noname057(16), Cyber People Army. The attacks were targeted against the domains of the public administration and the crucial entities from energy and transportation sector. Especially vulnerable were airport's websites. The websites of President Office, Polish Parliament, Supreme Court, National Central Bank and the telecommunication operators were among attacked domains. The most spectacular attack happened when the Polish High Chamber of Parliament–the Senate declared Russia a state sponsor of terrorism. The website of the Senate was temporarily unavailable. However, these attacks were not particularly successful as the websites survived DDoS attacks. It is also important to mention using DDoS attacks in information operations as the Telegram channels of groups conducting such an activity very often advertise success of their operations against particular websites. But in reality the websites were not shut down. Alongside with the DDoS attacks there were several attempts to breach the CMS of the websites and defaced them by adding anti-Ukrainian slogans.

THE REACTION OF POLISH GOVERNMENT

Polish government after the ransomware attack against air ambulance and massive DDOS attack against Ukrainian website decided to introduce the ALFA CRP alert. These alert was the lowest in the 4th scale grade introduced by the Polish antiterrorism bill. It means the increasing monitoring of security of ICT systems of the public administration and critical infrastructure, checking and modifying access to the ICT services, informing staff about the threat and instruct them about the necessity to behave more responsibly. However, the ALFPA CRP lasted only for 5 days and was levelled up to CHARLIE CRP just three days before the Russian large scale invasion. It is the highest level before the incident appeared, the last one – DELTA is introduced only to mitigate the impact of the incident. CHARLIE-CRP level introduced 24 hours every day shifts of cybersecurity stuff in the selected entities of the public administration. The public administration and critical infrastructure were also responsible for preparing continuity plans and preparations for limiting operations on servers. It is worth mentioning that these measures were not mandatory to ordinary citizens or private business. However, it seems that introduction of CHARLIE CRP on the very early stage of the conflict was a good decision. According to Microsoft Russians achieved a low success rate of cyberattacks against Poland, which stands to 29% only.

Polish Ministry of Digital Affairs tried also to reach out private sectors through the Cybersecurity Cooperation Program, which was based on cooperation of the private companies and entities from government sectors. More than 30 companies from technological sector joined till the outbreak of largescale invasion. This program facilitates the exchange of information about threats and increases the coordination of the action on domestic level through providing the necessary tools and raising situational awareness.

It was not the only action the Polish government conducted. It also engaged in proactive campaign to disrupt Russian operations and burry their capabilities. The Military Counterintelligence Service and the CERT Polska team (CERT.PL) observed a widespread espionage campaign linked to Russian intelligence services, aimed at collecting information from foreign ministries and diplomatic entities and decided to reveal the Techniques, Tactics and Procedures (TTPs) of adversary to disrupt the ongoing campaign, impose additional cost of operations against allied nations and enable the detection, analysis and tracking of the activity by affected parties and the wider cyber security industry.

CONCLUSION

Poland has faced the significant risk of threats as the consequence of its key role in helping Ukraine attacked by aggressive Russia. The constant threat for the services available in the internet and the attempt of exploiting the well known exploits but also the 0-day caused that it is important to conduct a analyse of the networks and IT systems of public administration institutions and critical infrastructure operators to find weak points and eliminate them. Considering the fact that Russia is trying to find new ways, methods and technologies to breach the cyberdefence every incident should be analysed and the results of this analysis should be disseminated and used to change the ICT tools and used procedures. Last but not the least, the users of systems must be continuously educated and their awareness must rise in the field of actual threats especially in the sector of critical infrastructure and public administration. ■

ANDRZEJ KOZŁOWSKI

Cybersecurity and disinformation expert. Political Science PhD. Assistant professor at the University of Lodz

CYBER ADVOCACY CONTINUES TO BE ACTIVE IN FINLAND AND EUROPE

// Peter Sund / Risto Rajala

Finnish Information Security Cluster – Kyberala ry is an industry advocacy association and an ecosystem for cyber security companies and organisations established in Finland. The purpose of the association is to promote cybersecurity and shape digital risk policies in Finland and the EU in a wide-ranging and goal-oriented manner, as well as the cyber security of public administration, companies and civil society.

With the accelerating digitalisation of society, cyber security has risen even more strongly to the agenda of political decision-making. For this reason, the role of advocacy and policy shaping in the cybersecurity sector is constantly emphasized. This spring and during the rest of the year, political guidelines will be made both nationally and especially at the EU level, which will have a significant impact on the operating conditions of the cyber security industry operating in Finland far into the future. The growing and internationally expanding cybersecurity industry is the cornerstone of our digital security and security of supply, hence its viability must be systematically secured through policy measures.

TIMES OF AUSTERITY IN PUBLIC FINANCES THREATENS THE DEVELOPMENT OF CYBERSECURITY

In its Government Programme, Orpo's Government (2023-) set ambitious goals for the current parliamentary term to promote the data economy, digitalisation and digital security in Finland and the European Union. The achievement of the objectives depends on the implementation of the entries in the Government Programme and the methods of implementation. The policies of the Government Programme and, partly based on it, of Finland's Digital Compass implementation plan guiding the digitalisation development and policy of public administration on the development of cyber security are, for the most part, very good. However, there is a real risk that ambitious policy guidelines will be overtaken by fiscal austerity pressures.

The Government published the General Government Fiscal Plan for 2025–2028 on Thursday 25th April. The General Government Fiscal Plan decided on additional measures that will strengthen general government economy by approximately EUR 3 billion, in addition to the EUR 6 billion previously agreed in the Government Programme. Savings will be targeted at all administrative branches.

Despite the difficult situation in public finances and savings, the Government is committed to maintaining the additional investment of EUR 1 billion in research and development by 2027 in accordance with the new R&D Funding Act. Investments will be made in increasing business-driven research, development and innovation (RDI) investments, for example, by increasing Business Finland's RDI funding authorisations annually. In addition, the Government proposes a fixed-term tax incentive for large industrial investments and is preparing to replace the supercomputer EuroHPC LUMI with a new supercomputer.

There were no additions for new undergraduate places in higher education in the fields of technology (incl. ICT, cybersecurity, etc.), as was anticipated. However, most higher education institutions will maintain high level of undergraduate places (although insufficient) and/or increase graduation rates. Higher education institutions should be encouraged to cooperate even more with companies at the end of their student's degree programns, so that experts who have already ended up working or otherwise working during their studies graduate and higher education institutions receive the funding intended for them. This is essential for the functioning of the education system. In the coming years, therefore, it will be increasingly emphasised that the productivity of training measures aimed at professional-level competence in cybersecurity will increase in terms of increasing the number of new experts. In addition, attention should be partly focused on increasing externally funded development activities in the form of projects and on strengthening cooperation between actors engaged in competence development.

The fate of budgetary commitments in cybersecurity remained unclear in the government discussion on spending limits. It seems that the dimension of cybersecurity as part of society's comprehensive security has still not become sufficiently clear when decisions are made on the allocation of financial resources. In the upcoming government budget negotiations, it must be ensured that the effectiveness and multiplier benefits of digital and cybersecurity measures can be levered for nation's benefit. This requires that funding from the Ministry of Finance, Transport and Communications Agency (Traficom) and Business Finland for the development of the ecosystem in the sector is implemented in accordance with the Digital Compass implementation plan. In addition, where applicable, the entity should be strengthened with private funding, e.g. with the help of business angels and venture capitalists. At the same time, it must be ensured that the measures outlined in the Government Programme and the Digital Compass, such as acquiring cryptographic technology capabilities for the quantum age and increasing resources for cryptographic product certification activities, are implemented in order to bring domestic cyber security technology to international export markets more efficiently.

The use of public funds must prioritise activities that strengthen the ability of industries and public entities to manage their digital risks and for the latter, refrain from delivering services that are available on the market. The vibrant cybersecurity industry operating in Finland produces the products, services and solutions required for society's digital security and security of supply. These will also secure a resilient digital infrastructure and services covering the whole of society, both private and public.

EUROPE AT A CRITICAL TURNING POINT

European Parliament elections were held in June in all European Union (EU) Member States for the 2024-2029 parliamentary term. The European Parliament and the new Commission will play a key role in promoting the EU's economy, safety, environmental sustainability and competitiveness. Strengthening the security of the digital environment both at European and global level must be at the core of all cybersecurity-related policy measures at EU level during the next parliamentary term 2024–2029.

Fundamental rights must be ensured also online throughout the European Union, including privacy for businesses and a high level of data protection for citizens. The jurisdiction of the authorities must be strictly limited, transparent and strictly purpose-bound. Digital risks must be managed front-loaded and based on information systems and data. The development of cybersecurity in Europe must not only be the work of public authorities but must be based on rule-of-law and respect private ownership and thus be based on strong cooperation between the private and public sectors. On a practical level, this means developing the EU's cybersecurity architecture and tackling data breaches, industrial espionage, sabotage, data breaches and property crime on a broad scale in the digital environment.

The EU must support industry-led policy measures to strengthen quantum-secure encryption in Member States. In supporting the development and deployment of quantum-secure encryption solutions, preference should be given to the most reliable post-quantum cryptography (PQC) algorithms over QKD (Quantum Key Distribution) technology. The EU should rely on the PQC standards developed by the US National Institute for Technology and Standards (NIST) and refrain from developing its own competing standards. The EU must promote and support the hybrid use of classical and quantum-secure encryption methods.

Significant regulatory initiatives, such as the Cyber Resilience Act, the NIS2 Directive and the Artificial Intelligence Regulation, will be completed during this parliamentary term. With the entry into force of these comprehensive horizontal legislative initiatives, we will see that the European regulatory environment for cybersecurity is well advanced. In the coming European parliamentary term, it is time to focus on Europe-wide efforts to ensure the successful and uniform implementation of fresh legislation and to develop the necessary European standards in the market. Enforcement of legislation is an opportunity to prevent regulatory fragmentation and promote a single market for cybersecurity in

Europe by removing unnecessary barriers and bureaucracy. Regulatory needs need to be reviewed again, if in the digital environment are development paths that run counter to European values and cannot be resolved by the market.

With its large single market and ambitious regulatory framework, the European Union is well positioned to promote sustainable, responsible and secure digitalisation globally. However, in order to succeed, the EU must engage in genuine cooperation with third countries, rather than unilateralism or 'data imperialism'. The EU must work with its allies to promote digital trust and strengthen international good practices and standards that enable the successful global uptake of digital products and services. Promoting safe and reliable data transfers with like-minded third countries is a prerequisite for successful economic activity. Technical or administrative cybersecurity requirements should not be used to further national trade policy objectives. At the same time, it is essential that the EU invests in combating illegal influence, espionage, data leaks and sabotage in the digital environment.

The talent shortage is one of the biggest challenges facing the European cybersecurity industries. The EU should carefully assess how best to support Member States in training and mobility projects that foster a dynamic and vibrant European labour market for cybersecurity professionals from diverse backgrounds. One of the most urgently needed actions is to support the upskilling of those who are already part of the labour market through reskilling and upskilling activities. It would be beneficial for the Finnish cybersecurity industry to allocate more European funds and resources to the European Cybersecurity Competence Centre (ECCC), which can support Member States' efforts to strengthen their cybersecurity ecosystems through national coordination centres.

CYBERSECURITY ADVOCACY WORK CONTINUES ACTIVELY

Advocacy work in the cybersecurity sector continues to be active both at the Finnish and EU level. The operating environment is both favorable and challenging for the work, and we naturally strive to seize opportunities both through cooperation at the official level and through advodacy at a higher political level. Close and integrated cooperation in content and structures with Technology Industries of Finland provides the industry the opportunity to create impact beyond our size and bring the perspectives of the cybersecurity industry as part of the advocacy work of the entire technology sector. We will benefit from wider shoulders, especially in broader EU and other issues on requiring deeper and wider investigation and research.

Members of the Finnish Information Security Cluster can follow the association's advocacy work via weekly member notification messages informing about past and future actions and activities. One can participate in advocacy work in many ways through our activities or structures, or simply by reacting to a member notification on a matter that is found relevant at the time. ■

> ❞
>
> **Digital risks must be managed front-loaded and based on information systems and data. The development of cybersecurity in Europe must not only be the work of public authorities but must be based on rule-of-law and respect private ownership and thus be based on strong cooperation between the private and public sectors.**

PETER SUND

CEO
Finnish Information Security Cluster (FISC)
Technology Industries of Finland

RISTO RAJALA

Advisor
Finnish Information Security Cluster (FISC)
Technology Industries of Finland

FINLAND'S COMPLICATED PATH TO NATO – FASCINATING DOCUMENTARY COMING SOON

// Michael Franck

In his upcoming documentary, documentarist Michael Franck delves deeply into Finland's recent history and describes Finland's decades-long dance between East and West in a personal way. The dance has led to this moment and Finnish NATO membership.

Franck started working on the documentary immediately after Finland joined NATO, even though it had been maturing for a long time. As a theme related to the security of the Baltic Sea region, it offered a natural continuation of his previous documentary Åland - The Finnish Bridge to the West, which dealt with the history of Åland and its exceptional peace project. In it, he goes back several centuries, reflecting on what started to happen in Russia already after the Viking Age.

In the document now under work, the focus is on post-Cold War processes that have led Finland towards ever closer Western cooperation.

"The film opens up the decisions that have been considered and made behind the closed doors of various parties in Finland, mainly the President of Finland, the Ministry for Foreign Affairs and the Defence Administration – as well as the structures of our country's public security policy, civil and state administration," Franck says.

The backbone of the documentary consists of numerous interviews with key personnel. Among other things, several people who have worked and operated at the state level have been interviewed, which sheds light on the very challenging "westernisation" that Finland has gone through for decades. In part, therefore, there are also actions taken behind the scenes.

"In my opinion, it is essential that the people who have been involved in this process - here now, with their own faces and voices, open up our country, from a Western perspective to an exceptionally challenging process of Westernization: This through our young history - without provoking the constantly threatening expansionist Eastern Neighbour", Franck continues. As a documentarist, he says that he also brings his own experiences with him when he visits the palaces of power of the Soviet Union in the 70s and 80s as throughout the 90s and 2000s. His last interview in Russia was conducted in the Kremlin just before the outbreak of war in late 2022.

Franck has also wanted to address the topic from the perspective of security of supply, both in relation to the ongoing hybrid challenges and the possible deepening of the crisis. "For the next generations, it is now very important to be able to open up the tasks of civil administration and the private sector – in other words, how to secure the maintenance of food, energy and electricity as well as telecommunications and material logistics across the Baltic Sea, he explains.

The aim is to examine Finland's path to becoming part of Western NATO cooperation - both from the perspective of history and the future. Comprehensively and interestingly. The release of the film has already been agreed with the main broadcasting company of Finland (YLE)). Also international distribution is currently being negotiated. There is plenty of interest. And like Franck's previous historical and social documentaries, it will also be available in schools to support the teaching of history and social studies. ■

Photo: Thomas Whitehouse

MICHAEL FRANCK

- Michael Franck is an internationally awarded documentarist, who has directed and produced more than 150 documentaries shown both on Finnish television and internationally. He has lived and worked in both the Middle East, Central Asia and in the United States. During this period he also participated in Rand Corporation´s Middle East and Central Asia Studies group. His films main focus is on independent Finlands challenged Nordic history, about entrepreneurship as a base for future living conditions - as well as the long and history of the Middle East and central Asia (prime Iran), where his family has been working and living for three generations.
- Recent films include the story of the legendary Finnish Student Union, that came to be a base for the building up off this Nordic independent country and Michael Franck´s documentary portrait "My Godfather and Kekkonen", featuring the controversial Finnish cold war time pro western parliamentarian Georg C. Ehrnrooth, the documentarist´s own godfather, whom Michael as a young politician in the 1970's decided to disagree with.
- Currently his and his teams main documentary project is Finlands Road Into Nato, set to be tv - published also internationally. Like many Franck documentary films since the 1980-ies.
- Michaels both older sons; awarded documentarist Arthur Franck and producer Edvin Franck, also work with their fathers documentary projects.

SAMPLES FROM CYBERWATCH FINLAND WEEKLY REVIEWS

// Cyberwatch Finland Analyst Team

THIS COMPILATION INCLUDES FOLLOWING ARTICLES

WEEK 18:

- Passwords and brute force attacks

WEEK 19:

- Facial recognition cyber threats

WEEK 21:

- Leakage of personal identity code exposes to identity theft

WEEK 22:

- Credential stuffing attack is a common threat that endangers the entire organization

PASSWORDS AND BRUTE FORCE ATTACKS

When talking about password security, the discussion usually focuses only on what constitutes a secure password. Sometimes one can see references to times, on how long it takes to crack different passwords, or how password length increases the security factor. A longer and more complex password, i.e. one that uses several character types (lowercase, uppercase, numbers, special characters), is secure because it provides better protection against brute force attacks on passwords. In these attacks, the malicious actor tries to guess the password associated with the username simply by trying all possible combinations using automation. Naturally, brute force attacks cannot be used on the login windows themselves, which passwords are intended to penetrate, as these usually limit the number of login attempts allowed to a particular account. Carrying out a brute force attack often requires, for example, the hash value of the password obtained through a data breach. This value is also known as an encrypted password, and simply put, it refers to a password that has been unreadable using an encryption algorithm. A common example of password encryption goes as follows: when a user first registers for a service, a hash value corresponding to their password is created and stored in the service's database. Since the encryption algorithm always produces the same hash value for the same password, there is no need to store the password itself in the service. In the future, when the user returns to the service, the login can be verified by comparing the hash value of the entered password with the value stored in the database. The natural advantage here is that the service provider never gets hold of the actual easy-to-read passwords, which reduces the risk of both internal misuse and data breaches. Done this way, the attacker has the potential to gain access to hash values alone.

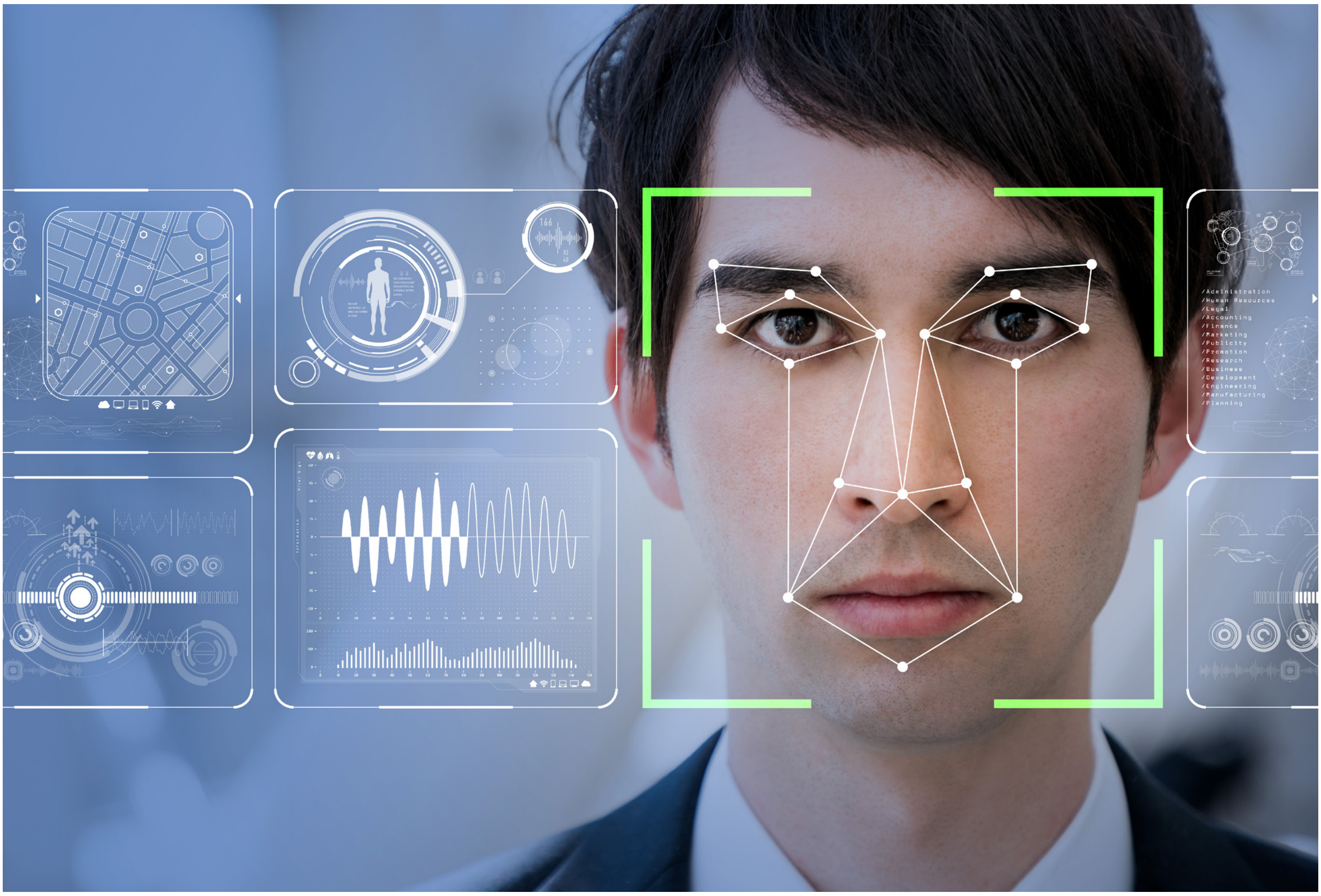
There are several different cryptographic algorithms, and there are differences between them, among other features, but also in how well they withstand brute force attacks. At the moment, the popular and well-liked encryption algorithm is called bcrypt, but to some extent the older and much less secure MD5 algorithm is also used. Typically, the user cannot notice or distinguish which or what kind of password protection method is in use, as even the highest level of security algorithms only take a few seconds to change the password to an encrypted form, so the differences in the login process are practically imperceptible. In any case, no matter how high-level the algorithm is, a brute force attack is always theoretically possible if the threat actor gains unlimited access to the hash value. In theory, because passwords encrypted with bcrypt, for example, can take tens, hundreds or thousands of years to crack with modern technology, depending on the characteristics of the password. Most recently, these times have been mapped by US security firm Hive Systems, which measured theoretical times how long it would take

References on page 41

to crack various bcrypt-protected passwords. The attack used twelve high-quality graphics cards as computing power. The power was deliberately chosen so that it could match the computing power held by a mid-level threat actor, either through physical components or a botnet. According to the results of the test, the critical limit would go to eight characters if both numbers and lowercase and uppercase letters are used. It would take about three years to crack a password of this level, and the times increase exponentially as passwords become longer or more complex.

However, neither this chapter nor any other guidance on how long a password is secure should be relied on too much. Tests usually only measure the durability of randomly generated passwords, and since extremely few people actually use completely random passwords, cracking is often easier than what with only a brute force attack. Some of the most common password cracking techniques include a dictionary attack i.e. trying commonly used passwords, phrases or variations of them. It is also common to try passwords stolen from elsewhere by the same user or modifications of these. Nowadays, brute force attacks are more often accompanied by one of these techniques. For example, if it is known what types of passwords a particular person usually uses, the time it takes to carry out a brute force attack will be significantly reduced. To illustrate, if it can be seen from the hijacked passwords that a person usually uses a passphrase consisting of two words, the first letter of which is always uppercase and there are two numbers and a special character at the end a this knowledge can significantly enhance the effectiveness of a brute force attack, as it the amount of possible passwords the attacker has to go through. This can make a long and complex password vulnerable to brute force attacks when supported by other methods of cracking.

Therefore, when creating a good password, one shouldn't just focus on character count and complexity. Of course, they are important factors in improving security, but equally critical are the difficult guess ability and uniqueness of the password. The use of whole plain text words should be avoided, and the same password should under no circumstances be used in multiple places. When talking about passwords, it is important to remember that in many respects it is already considered an outdated solution for authentication, from which the aim is to move away. As a verification method, passwords have a lot of downsides, and their crackability is just one of them. Various biometric authentication methods as well as multi-factor authentication are gradually replacing or at least rising alongside passwords. However, most likely, they will not be completely gone anywhere in the near future, so the protection of passwords is an acute issue, at least for the time being.



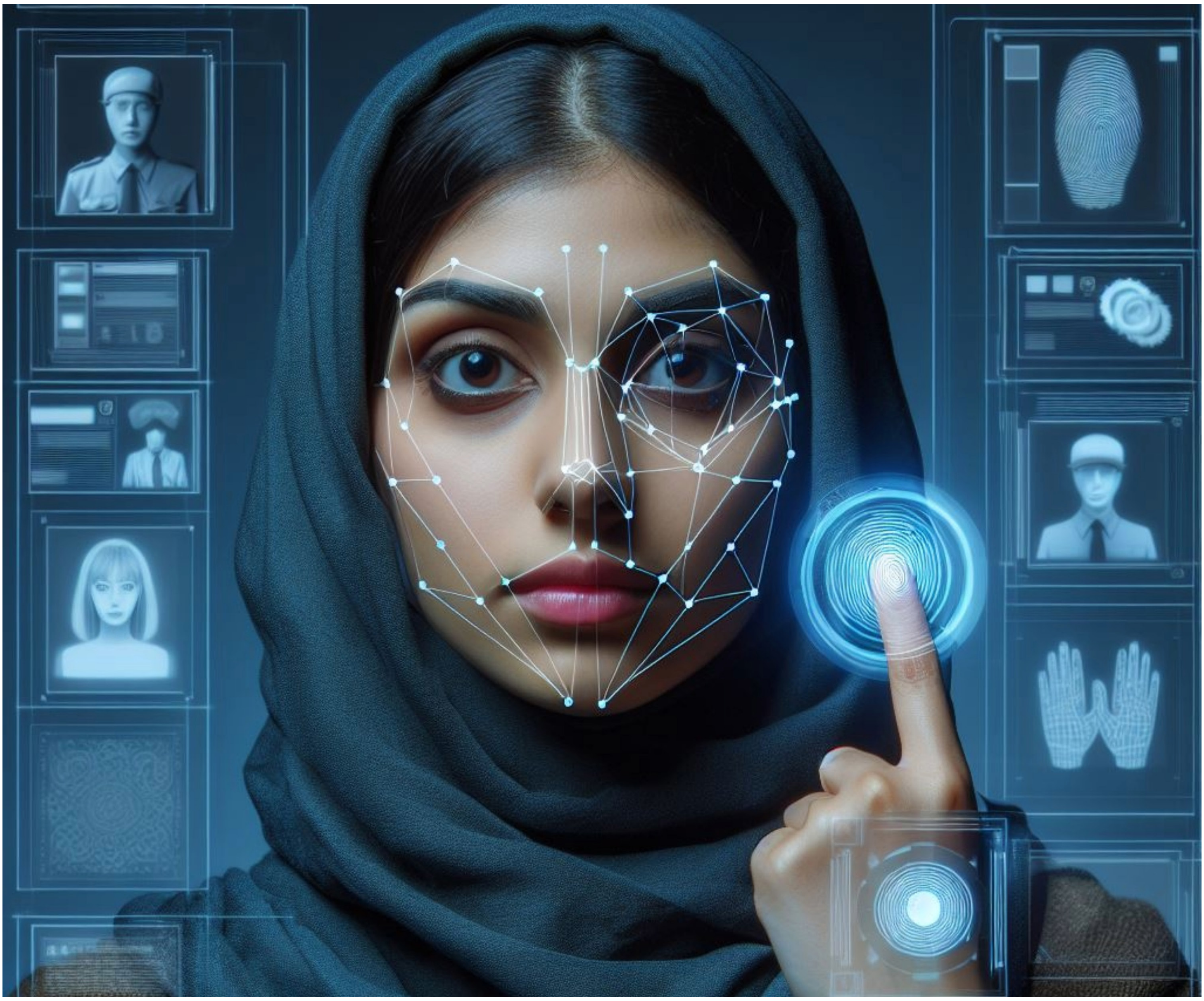
FACIAL RECOGNITION CYBER THREATS

Like artificial intelligence, biometric identification, i.e. the use of people's physical characteristics for identification, is spreading, albeit at a slightly slower pace and without a corresponding boom, to different sectors of society. The most common use case where biometrics is encountered in everyday life is logging in to mobile devices. In many ways, it is more convenient and better than the previous option, passwords. However, biometrics are also used elsewhere, and as the technology becomes more common and new uses are developed, new kinds of risks also arise. The use of biometrics for mass surveillance, especially when combined with artificial intelligence algorithms, has recently generated the most debate. The issue has been raised in particular in connection with the security measures related to the 2024 Summer Olympics in France. For more than a year, France has been developing a system that combines artificial intelligence and camera surveillance with real-time threat detection. This functionality intended for the Olympics has been tested this spring at concerts and other mass events. When the plan to implement this type of monitoring first came up, it was met with considerable criticism regarding privacy and data security.

However, in accordance with EU regulations and France's own laws, the technology will not be used for biometric identification, in this case facial identification, but will only monitor anomalies, such as fires, weapons, abandoned objects or fallen persons. However, many voices, including representatives of Amnesty International France, have criticised the introduction of the technology, describing it as just one step away from "Orwellian" mass surveillance based on faces. According to critics, modifying the same system would make it possible, and even easy, to include biometric surveillance. Developers of the system have responded with arguments that the system is not designed to this purpose and that modifying it to do so would not be as simple as proposed. However, it is not difficult to imagine that if AI is trained to recognize things or objects from a live feed that the same system could also be trained to recognize and classify human faces. Natural concern that arises is that if such a technology existed it would be hard to not to adopt it to usage in the name of national security.

Within the EU, however, laws are somewhat effective in preventing mass biometric surveillance. The EU's AI Act, which entered into force at the end of 2023, also includes a mention of restricting facial recognition. In practice, facial recognition from a live image is prohibited, even though identification based on a recorded feed, for example, remained within the scope of the law. Critics say that this functions as a

References on page 41



loophole in the law that actually allows for surveillance.

In any case, there is considerably more control within the EU than in other parts of the world. Outside the EU, China, for example, uses massive biometric surveillance, especially in Uyghur regions, and the Moscow metro has been using the FacePay payment system using facial recognition for years. In Australia, for example, facial recognition has also been used in the systems of both public authorities and private companies. The activity was at its most intense during the coronavirus pandemic, and although monitoring and legislation have been increased since then, the collection of biometric data is still legal for private companies.

Regarding biometric data a new threat first materialised at the beginning of May, when Outabox, a company that produced facial recognition systems for bars, clubs and restaurants, suffered a data breach. At the turn of the month a database containing personal data of more than a million Australians reportedly originated from the company appeared on the dark web. The database was allegedly leaked by a disgruntled Outabox subcontractor and contained not only biometric identification data, but also other sensitive personal data such as addresses, dates of birth, scanned driver's licenses and copies of signatures. The natural concern is what criminal actors can exploit such data for. In addition to this, it has also been questioned how the data in question has been stored and how it is possible that the subcontractor has had access to the entire database.

The widespread collection of biometric data therefore poses significant threats. Although the idea of facial recognition makes many everyday things easier, its risks are hard to ignore. The threat of misuse or data breaches is real and concerns that its introduction will lead down a path of mass surveillance are also justified. The case of Australia and the debate in France illustrate these risks. However, since the technology also offers many opportunities and opens up new markets, both governments and companies producing applications have an interest in expanding its use. It seems that, unlike in the case of artificial intelligence, the threats currently outweigh the opportunities when it comes to the mass adoption of biometrics, but we should keep an eye on the developments.

LEAKAGE OF PERSONAL IDENTITY CODE EXPOSES TO IDENTITY THEFT

In several recent security incidents, concerns have been raised about the leakage of victims' unique ID ́s or social security numbers (SSN). There are several examples of re-cent security incidents where personal identity details have been exposed. Most recent-ly, in Finland, the personal details of more than 100,000 residents of the City of Helsinki are feared to have been leaked as a result of a data breach into the information system of the City's Education Division. In the United States, telecom giant AT&T announced in early April that it had found the social security numbers of more than 70 million of its customers on the dark web. Leaks containing data such as this also garner big headlines in the media, but it is rarely reported what kind of threats a leak can pose in concrete terms. As a whole, a leak of a personal identity code exposes one to several different threats, the most significant of which are different forms of identity theft.

Identity theft refers to situations in which the identity of another person is imper-sonated. The intention is to mislead a third party, this may mean, for example, making online purchases or appearing on social media under someone else's name. There are different forms of identity theft. For example, synthetic identity theft refers to a situation where criminals build a new identity by combining true and false information. Synthetic identity theft is more advanced than regular one and may be going on for years before it is revealed. In some cases, criminals have favoured children's personal data when constructing fake identities, as it is even more likely that the activity may continue for a long time before it is detected. Of-ten this happens only when the child reaches the age of majority, and at worst, a young adult may immediately when reaching this breakpoint in life have to wres-tle with the consequences of identity theft.

Internationally, practices and everything that can be done with a personal security num-ber vary. In the United States, for example, social security number and basic personal data alone can be used to take up loans, open mobile subscriptions or obtain forged documents such as passports or other certificates. In Finland and other Western coun-tries, personal identity codes and other basic information can in some cases be used to take instant loans or order products from online stores with an invoice (that is sent to the victim of the identity theft), or to change address information to direct products to crimi-nals. Although in Finland, for example, the law obliges to use strong authentication when taking out instant loans, for example through a bank connection, not all instant loan companies offering their services in Finland comply with this. In addition, around the world, it is usually possible to obtain additional

References on page 41

information about an individual with the help of a personal identity code. Knowing it and saying it out loud on the phone is often enough to identify yourself, for example, at the customer service of operators or at a hospital when asking for your own medical information. For operators, this may enable, for example, the hijacking of a phone subscription through a SIM-swapping attack. This is unfortunate, as the personal identity code itself is not intended as a means of identifi-cation, but its purpose is to help identify persons from each other.

There is very little an individual can do to protect themselves from leakage of their per-sonal identity code. The only way a person can leak their ID is by entering it on a scam site, for example, or otherwise giving it directly to a criminal. This is much rarer than ex-posure these details through other means. These are almost always data breaches, where thousands of people's data ends up in the hands of criminals, and protection against this should have been the responsibility of the party managing the data. One can reduce their own risk of becoming a victim of this type of data breach by trying to limit the use of your personal identity code. In all services where a personal identity code is requested, it may not be mandatory or relevant to the use of the service. Espe-cially in the case of children's personal identity codes, it is possible that they are asked for unjustifiably, for example, when concluding a rental agreement.

The victim of a leaked personal identity code has few means. In some parts of the world, for example in the United States, it is possible to change your personal identity code if certain conditions are met, but even this is not without its problems. At worst, it can lead to even greater challenges in proving one's identity or using one's ID for other purpos-es. For example, a complete emptiness of credit information or payment history related to a new number may make it difficult to take out a loan, even if the payment default entries attached to the old ID have been eliminated. However, in many countries it is not even possible to change your personal identity code, and in Finland it can only be done in extremely rare situations. The preferred option is to impose a personal credit ban (Oma luottokielto) or some similar restriction. However, a credit ban is a drastic meas-ure, and it restricts and hinders the performance of many everyday activities. However, it is often the only viable solution for the victim of identity theft.

CREDENTIAL STUFFING ATTACK IS A COMMON CYBER THREAT THAT ENDANGERS THE ENTIRE ORGANIZATION

Credential Stuffing attacks are common and easy-to-implement cyberattacks. The attack exploits previously leaked or hijacked credentials. In attacks, the criminal automatically enters previously hijacked username-password pairs into several different online platforms. The goal of the attackers is to find a platform where users have the same username-password pair as the original leaked platform. Subsequently, in one way or another, the attacker seeks to financially profit from the information obtained through credentials. The idea behind the attack is to rely on the fact that most people still use the same passwords on multiple platforms. The same email address is often used as a username for different platforms, so together with the reused password, they form an easy target for attackers to exploit this in their criminal activities. In various data breaches or leaks, leaked credentials remain circulating on dark web platforms in the form of Credential Stuffing lists. These lists collect credentials leaked in various data breaches, which criminals use, among other things, for these credential exploitation attacks. These lists are updated approximately once a month, so that credentials that have already ended up on the list are not removed, but new credentials are added to the list. Such lists are traded on the black market, but they are also available for free.

The attack method differs from a brute force attack in that in a brute force attack, the attacker tries to guess a password using random words or combinations of letters and numbers, whereas in a credential stuffing attack, the attacker tries to guess where all the pages are registered with existing credentials.

References on page 41

But how to protect from the threat? There is no one-size-fits-all protection against this threat. Protection against credential stuffing attacks requires versatile and wide-ranging precaution. Creation of various preventive methods, such as system detection indicators and their alarm system, password management systems, CAPTCHA tests, multi-factor authentication (MFA) and adaptive authentication (geolocation, IP address, browser and device status, etc.) plays an important role in protecting against this threat. Scanning the dark and deep web and threat intelligence monitoring also helps the organization to identify and monitor the realization of these threats, as well as the development of the cyber environment. Following identification and observation, any infringement shall be immediately reacted to, relevant stakeholders shall be informed immediately, and any remedial measures shall be taken to mitigate the impact and protect sensitive data.

The most effective practices for protecting against credential exploitation attacks are to use unique and strong passwords, as well as to indicate the organization's systems for high number of login attempts and, if necessary, block IP addresses from which a large number of login attempts target the organization's systems. Along with these, organizations can minimize the likelihood of successful credential stuffing attacks. It is also good to note that even a single compromised or reused credential can endanger the systems of the entire organization and, at worst, the systems of stakeholders outside the organization. ■

REFERENCES

PASSWORDS AND BRUTE FORCE ATTACKS:

https://www.proofpoint.com/us/blog/information-protection/password-cracking-techniques-used-in-cyber-attacks
https://www.hivesystems.com/blog/are-your-passwords-in-the-green
https://www.securityweek.com/new-password-cracking-analysis-targets-bcrypt/
https://guptadeepak.com/password-hashing-algorithms-101/

FACIAL RECOGNITION CYBER THREATS:

https://www.reuters.com/sports/olympics-how-france-plans-use-ai-keep-paris-2024-safe-2024-03-08/
https://www.france24.com/en/tv-shows/tech-24/20230324-france-passes-controversial-ai-surveillance-bill-ahead-of-2024-olympics
https://thebulletin.org/2022/10/chinas-high-tech-surveillance-drives-oppression-of-uyghurs/
https://www.biometricupdate.com/202301/moscow-metro-to-expand-face-pay-biometric-service-as-customer-base-grows
https://www.edpb.europa.eu/news/news/2023/edpb-adopts-final-version-guidelines-facial-recognition-technology-area-law_en
https://www.politico.eu/article/eu-ai-facial-recognition-tech-act-late-tweaks-attack-civil-rights-key-lawmaker-hahn-warns/
https://www.wired.com/story/outabox-facial-recognition-breach/

LEAKAGE OF SOCIAL SECURITY NUMBER CAN EXPOSE TO IDENTITY THEFT:

https://dvv.fi/-/kysymyksia-ja-vastauksia-identiteettivarkauden-ja-tietovuodon-uhreille
https://www.ssa.gov/pubs/EN-05-10064.pdf
https://fortune.com/2024/04/01/att-70-million-users-social-security-numbers-dark-web-you-affected/
https://tietosuoja.fi/-/kho-lasten-henkilotietojen-saannonmukainen-keraaminen-vuokraustoiminnassa-oli-tietosuoja-asetuksen-tarpeellisuusvaatimuksen-vastaista
https://onfido.com/blog/what-is-synthetic-identity-fraud/

CREDENTIAL STUFFING ATTACK IS A COMMON CYBER THREAT THAT ENDANGERS THE ENTIRE ORGANIZATION:

https://www.ncsc.gov.uk/news/use-credential-stuffing-tools
https://securityboulevard.com/2024/05/how-to-mitigating-credential-stuffing-attacks/
https://www.enzoic.com/blog/2023-verizon-dbir/
https://www.enzoic.com/blog/what-is-credential-stuffing/
https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/

MONTHLY REVIEW JULY 2024

// Cyberwatch Finland Analyst Team

CONTENT:

IN THIS REVIEW

In this monthly review, we examine the most significant cyber phenomena of the previous month and tie them into larger entities. The review is divided into three perspectives: the most significant events in the cyber world during the month, phenomena that we want to highlight especially from the previous one, and entities whose development is worth monitoring.

In June, one of the most visible incidents in the cyber world was the data breach in the UK against the healthcare subcontractor Synnovis.

In June, special attention was paid to events related to the European elections and how small and valuable information can play a role in cyber security. As we move into July, we want to highlight the cyber threats accelerating during the holiday seasons and the cyber threat scenarios related to the Paris Summer Olympics.

1. EVENTS IN THE CYBERLANDSCAPE

In June, the cyber environment was relatively quiet compared to the other months of the current year. In fact, there was only one significant cyber event that crossed the international news threshold, but it illustrates many of the prevailing cyber threat trends. This is a data breach against a company called Synnovis in the UK at the beginning of the month. Synnovis is a subcontractor to the country's health services. The Russian Qiling ransomware group carried out an cyberattack, and ended up with a significant amount of personal and health data of British patients. The attack also encrypted and disabled several Synovis systems, which has led to service disruptions throughout the month and, in particular, an increase in queues for blood tests.

The organization was also required to pay a ransom as a condition for the recovery of the systems and the stolen data. It has not been made public what amount of money the criminals are demanding, but at the end of the month it became clear that Synnovis has either directly refused to pay, or at least the negotiations have not proceeded in a way that pleases the criminals. This was revealed when Qiling shared a database of about 400 gigabits on its dark web leak site, which includes some or all of the data stolen from Synnovis. This includes personal data of British patients, such as dates of birth and names, as well as medical records relating to blood samples and their contents. Criminal groups have also occasionally published partially or fully falsified databases in an attempt to pressure victims into agreeing to ransom demands. Although verification of the authenticity of the information published is still ongoing and likely to take time, many experts have made an early assessment that it appears to be correct information.

The case highlights several details that fit the cyber threat picture of today. Firstly, it is a financially motivated attack on the health service, which has been a threat that has existed for years but is still growing. Secondly, the impact on the desired target was achieved through a single subcontractor, which is common in almost all cyberattacks, regardless of the target or motive. Thirdly, it illustrates how ransomware actors carry out their operations: the victim is pressured to pay the ransom for several reasons (restoring systems, avoiding reputational damage by restoring stolen data, and protecting patient security) and if agreement is not reached, the stolen data is made public as a warning example to others. The case also illustrates the individual's powerlessness over many cyber threats. There is no way that British patients who have used Synnovis services could have prevented their own data from ending up in the hands of criminals, and there are probably just few alternatives to using the services of a public healthcare subcontractor. While the target, Synnovis, will certainly suffer reputational damage and possible financial outcomes, especially if the attack was made possible by poorly managed information security, the worst sufferers will still be individual citizens who had nothing to do with the attack itself.

It is worth noting that the situation would not have been different if Synnovis had agreed to the ransom, but probably even worse. In addition to receiving a direct monetary reward for their operations, the extortion would likely have continued, or the stolen data would have been both shared and sold. The database would hardly have been made openly available as it is now, as this kind of activity could weaken the next victim's willingness to pay, but it is likely that the group itself could have started blackmailing individual victims or sold the data to another threat actor for the same purpose.

In many ways, the Synnovis case is a horror example of a modern cyberattack. It describes well the evolving threat, which is directed especially at health care, but can also hit any other actor in the sector. On the other hand, on the positive side, both the organisation itself and the NHS, the health authority, have communicated about the incident very openly and offered all possible assistance to victims who have lost their data. However, only the future will tell how significant the incident will ultimately be, while it is already thought to be the most devastating cyberattack ever carried out in the UK.

2. IN THE SPOTLIGHT

2.1. Less cyber interference than expected in the European elections

At the beginning of June, an active election year in Europe continued in the form of European parliament elections. It was anticipated in advance that exceptionally active cyber interference or even serious cyberattacks from Russia, would be experienced in connection with or during the elections. The concern was justified in the sense that Russian hacker groups at various levels have been attacking various European targets in waves for several years now, and disturbances at the time of the elections certainly provide information value for the attacks. However, the election came and went without a significant wave of attacks. Russian hacktivist groups on their own social media channels did repost denial-of-service attacks on organizations in different states during polling days, but in the majority of cases, these attacks were never even noticed by ordinary voters. Most of the attacks were probably prevented and only minor malfunctions occurred. These malfunctions were minor enough that they might as well have been the result of a slightly slower internet connection. Only in the Netherlands were actual service interruptions of a few hours reported as a result of the activities of Russian hacktivists, but even there the damage was repaired relatively quickly.

However, the limited achievements did not prevent the groups that carried out the attacks from boasting about the harm they had caused on their own channels. The images of the pages momentarily down seem plausible, but in many cases, it is either that the organization has identified where the DDoS attacks are coming from and blocked access to these actors. It is also possible that the pages have only been down for a few minutes, during which time the screenshot pictures were taken. However, this is of little relevance to the activities of hacktivist groups. The aim of posts on Telegram channels and other social media channels is to maintain the image of a continuous and effective campaign of aggression against Europe and to increase unity among one's own followers. They are therefore intended as a communication for pro-Russian actors, who are unlikely to independently verify what the impact of the attacks was, and do not believe the information about their effectiveness from European sources.

The reasons why the expected cyberattack front was not seen can be many. One is certainly that all over Europe we are already used to DDoS attacks by hacktivists, and the ability to counter them has developed considerably. Another possible reason is that Russia did not feel that it could significantly advance its objectives by interfering with the elections, and slowing down the pan-European process would have required considerable effort. In addition, it should not be forgotten that Russia, both in elections and in general, is constantly exerting information influence across Europe. Influencing political decision-making is likely to be more effective by supporting hidden opinion influencing and sources of internal conflicts than direct cyberattacks. Therefore, the only visible phenomenon remained the scattered attacks of the hactivists, which were weak in success.

References on page 49

2.2 All information matters in the cyber world

In the cyber world, every piece of information counts. The loss or contamination of even small or non-critical data can put large amounts of data at risk. This risk applies not only to the information resources and systems of the organization that has lost data, but also to the various stakeholders of the organization. This is due to the fact that the information systems also contain information on partners and forms of cooperation.

One example of a data category that is considered minor or non-critical is log data. Log data is historical data produced by information devices or systems. This information tells you what has been done with the device or system, when and by whom. The log data can be used to investigate various misuses, attacks and fault states, among other things. However, in the hands of an attacker, log data can be a very critical factor. With the help of log data, an attacker can easily get an idea of the organization's network structure and collaborations. With this information, the attacker can navigate in the desired direction and actual goal.

Another example where leaking of a small amount of data can harm and risk a large amount of data are phishing operations. Fishing can be done with a large sample, i.e. by sending a large number of contaminated e-mails to various addresses. Fishing can also be done in a more targeted way. An individual member of an individual organisation can be targeted. This can be approached subtly through social engineering, or through a simple infected email. There are countless ways. In any case, when a member of an individual organization falls victim to phishing, an attacker can gain access to, for example, user IDs for the organization's internal systems. In this case, the negligence or ignorance of an individual can backfire at the expense of the entire organization. From public sources, attackers are able to collect even trivial-sounding information about the organization and its members. From the bits of information found on various social media platforms and other internet platforms, it is possible to compile for the attacker, for example, an image of the target's organizational structure, managerial relationships or functions included in the job description. With this information, attackers can find out, for example, who is responsible for paying the organization's bills and thus target them directly.

In the cyber world, there are no free tickets for anyone. Even if an organization handles its part of information security in an exemplary manner, each member of organization must also be familiar with basic cyber hygiene and be able to think critically about incoming inputs. The contribution of each member of the organisation to collective safety is important and crucial. In cybersecurity, the old saying really applies: 'A chain is as strong as its weakest link'.

3. FOLLOW THESE

3.1. Olympics attract cyber threats

In July, one of the most unifying events in the world begins, when representatives of more than two hundred different countries gather at the Paris Olympics to represent their home country. However, the preparations for the sports festival have been accompanied by heightened concerns about potential cyber threats, and there is good reason for this, as this would not be the first time that cyber operations have been used to disrupt the Games. When the opening ceremony begins, the attention of the whole world will be caricatured in Paris, and this will provide an attractive platform for hostile forces to arouse fear and uncertainty if the operations are visibly disrupted. In addition, millions of visitors and hundreds of millions of remote attendees are potential victims of various scams or frauds related to the event.

Cyber risks to the Olympics have been discussed for a long time, and the French information security authority ANSSI, together with its partners, has been preparing for an increased cyber threat level for years. There is particular concern about Russia's attempts to exert influence, as relations between Russia and France are poor. Russia also has a high interest in disrupting the Games that unite the rest of the world, from which it is itself excluded.

So, there are a lot of threats, and even though we have invested in preparedness, only time will tell how well the risks can be prevented. It has been speculated that not only Russia will be able to use the attention received by the Games to push its own agenda. For example, there have been fears that the conflict between Israel and Hamas could encourage visibility-seeking hacktivist operations, and the possibility of cyberterrorism has also been mooted. However, individuals following the Games should be prepared for possible disruptions and be extremely attentive to Olympics-related websites or applications. Criminals' scam products are becoming increasingly credible and can rise to the top of search results with paid advertising space. Organisations directly participating in or sending employees to the event should also remind their staff of cyber risks.

References on page 49

3.2. During the holiday season, scams are on the rise

July is the most popular holiday time for Finns. This also brings with it an unpleasant side effect, as various scams and phishing attempts increase. There are many factors behind this phenomenon: When employees are on holiday, only part of the staff stays in the office to work. In this case, communication and chains of command are different from those in everyday situations. You no longer get an answer or confirmation from a colleague or supervisor on every issue. In addition, organisations transfer tasks within the organisation so that critical tasks can be carried out through various substitute arrangements. This may cause challenges in some tasks for which the substitute does not feel that his or her competence is sufficient in every situation. In addition, organisations often hire summer substitutes or take on trainees whose work input is intended to help fill the labour shortage during the holiday season. All these factors related to resourcing contribute to attracting cybercriminals to various scam campaigns that take advantage of these unusual situations.

In their operations, cybercriminals try to create a fake sense of urgency for the chosen victim. In a hurry, the victim is more likely to make hasty and unconfirmed decisions. Such attacks may include, for example, various phishing attacks, fake IT support requests, CEO fraud and the like. Common to these actions is often an unexpected message from a bank, authority or other authority. The attackers may appeal to the victim's feelings, reputation, use of a position of authority, or even blackmail the victim.

Fortunately, it is possible to protect against this threat as well. Always verifying who you are really dealing with goes a long way. By always being careful and ensuring the origin, purpose and safety of links sent to your email before clicking on them, you can avoid many threats. By not sharing your own or your organization's critical information, you can avoid it ending up with criminals. Employees who process and pay invoices must always ensure the authenticity of the invoice, and it is a good idea for another person to double-check the correctness of the invoicing. In addition to these, actively maintaining and developing traditional cyber hygiene saves most scams, whether it is the holiday season or not. In addition, it is the task and responsibility of the management to ensure that the instructions are up-to-date and that people have received sufficiently good training. ■

REFERENCES

EVENTS IN THE CYBERLANDSCAPE:

https://www.ncsc.gov.uk/news/ncsc-statement-following-reports-of-a-synnovis-data-breach
https://www.hayesconnor.co.uk/news-resources/news/highly-sensitive-patient-information-exposed-in-london-nhs-hospitals-data-breach/
https://www.england.nhs.uk/synnovis-cyber-incident/

LESS CYBER INTERFERENCE THAN EXPECTED IN THE EUROPEAN ELECTIONS:

https://www.euronews.com/my-europe/2024/06/07/dutch-cyberattacks-latest-in-eu-election-campaign-marred-by-disruption-violence
https://www.bleepingcomputer.com/news/security/ddos-attacks-target-eu-political-parties-as-elections-begin/
https://blog.cloudflare.com/exploring-the-2024-eu-election-internet-traffic-trends-and-cybersecurity-insights
https://www.radware.com/blog/security/2024/06/uncovering-the-hacktivist-cyberattacks-targeting-the-eu-election/

ALL INFORMATION MATTERS IN THE CYBER WORLD:

Cyberwatch's previous weekly reviews

OLYMPICS ATTRACT CYBER THREATS:

Cyberwatch’s weekly review 25

DURING THE HOLIDAY SEASON, SCAMS ARE ON THE RISE:

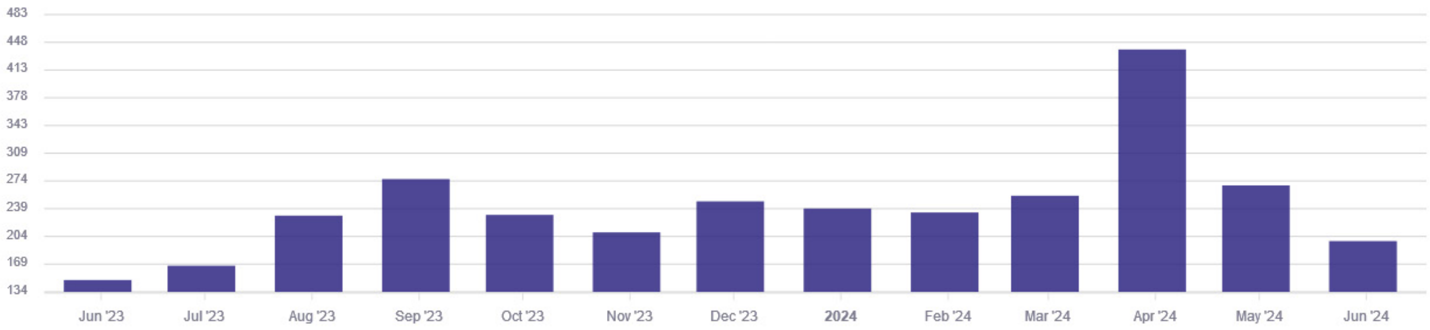
Cyberwatch's previous weekly reviews
https://www.omasp.fi/ajankohtaista/omastoori/verkkohuijarit-eivat-lomaile-kesakuukausinakaan

Cyberwatch Finland

THREAT INTELLIGENCE REVIEW

Cyberwatch Finland publishes threat intelligence monitoring that collects the most significant cyberattacks of the past month and information on the most active threat actors around the world. Cyberwatch analysts monitor activity not only on the surface network, but also on the deep and dark web. The sources also include publications by international information security actors and extensive monitoring of the Finnish and international media field.

DATA BREACHES BY MONTH FROM LAST TWELVE MONTHS.



Source: Cyber Intelligence House

MAJOR CYBERATTACKS AND CAMPAIGNS

SYNNOVIS

DATE: 03.06.2024

DESCRIPTION: Synnovis, a subcontractor to the UK's NHS, which provides state health services, was hit by ransomware in early June. In particular, patient data was stolen from a company specialising in the collection and processing of blood samples, and the use of several systems was prevented by encrypting files. At the end of the month, the company publicly admitted that British medical records had been leaked to hackers and a file of about 400 gigabytes appeared on the attackers' page for download. Synnovis has not disclosed what ransom has been demanded from it, let alone whether the data now published is the entire stolen database or only part of it. In addition to data successes, the attack has caused delays in blood sampling across the UK.

ACTOR: Russian Qilin ransomware

MOTIVE: Economic

IMPACT: It is likely that thousands of British people's personal and medical records have ended up first in the hands of an attacker and later shared for free on the dark web. The data includes information such as names, dates of birth and blood samples. In addition, longer queues have been experienced in several thousand hospitals or laboratories across the UK.

MAJOR CYBERATTACKS AND CAMPAIGNS

INDONESIA NATIONAL DATA CENTER

DATE: June 2024
DESCRIPTION: Indonesia's national data center faced a ransomware attack. The latest LockBit 3.0 malware from RaaS operator LockBit was used in the attack.
ACTOR: LockBit or an unknown subcontractor
MOTIVE: Economic
IMPACT Various government services, especially airport operations, were most affected by the attack. The attacker has demanded a ransom of USD 8 million.

INDIAN NATIONAL TELECOMMUNICATIONS COMPANY BSNL

TIME: June 2024
DESCRIPTION: India's state-owned telecommunications company suffered a data breach that resulted in 278 gigabits of sensitive data ending up in the hands of criminals.
ACTOR: kiberphant0m
MOTIVE: Economic
IMPACT: There is a risk that the SIM card of millions of the company's customers could be cloned, identity stolen, and financial information exploited. Stolen data is sold on the dark web for $5,000.

CYBER-PHYSICAL ATTACKS AGAINST CRITICAL INFRASTRUCTURE IN FINLAND

DATE: June 2024
DESCRIPTION: The Southern Finland Preparedness Centre reported physical breaches of water supply infrastructure in its area. In addition, the emergency response centre reported that the "fake doctor" had attempted to connect his computer to the fixed network of at least two different health centres.
ACTOR: Unknown
MOTIVE: Unknown
IMPACT: So far, there have been no reports of any actual disruptions due to these events. At the moment, it seems that the potential attacker has not achieved his objectives and the effects of the attacks have been avoided. As a result of these events, preparedness of the critical infrastructure has been further enhanced.

ACTIVE THREAT ACTORS

LOCKBIT 3.0

DESCRIPTION: One of the best known and largest Ransomware as a Service (RaaS) actors. Sells the ransomware it develops to its subcontractors who carry out the actual ransomware attacks.

RECENT ACTIVITY: Recovered from the official operation at the beginning of the year almost to its previous level. The most active threat actor in June.

METHDOS AND TACTICS: This ransomware is used for precisely targeted attacks that prevent the target from accessing the computer system in exchange for a ransom.

8-BASE/8BASE

DESCRIPTION: An extortion operator that started already in 2022 but actually became active in April 2023. It is believed to be a rebranding of a group called RansomHouse, as the operating methods and outward communication correspond almost perfectly to this defunct group. Links and similar operating models can also be found to a threat actor called Phobos.

RECENT ACTIVITY: During 2023, the group emerged from nothing as one of the threat actors carrying out the most attacks. Activity has continued throughout 2024, and every month the group carries out dozens of attacks around the world.

METHODS AND TACTICS: Targets mainly small and medium-sized enterprises and, instead of the large size of ransom demands, seeks income from a large number of crimes. It has been observed to both carry out intrusion into systems themselves and obtain this access from outsourced IAB (Initial Acces Broker) operators. In a typical attack, the target's files are encrypted, not hijacked, and a ransom is demanded both to restore the data and to threaten to publish it.

SENSAYQ RANSOMWARE

DESCRIPTION: A group of hackers first spotted in the second week of June 2024. This is most likely a new Lockbit subcontractor, i.e. a group that has rented or purchased their malware from a larger operator.

RECENT ACTIVITY: During June, the group announced on its dark web site that it had struck two targets. One of the targets was from Italy and the other was from Lebanese. Both sites were private sector operators.

METHODS AND TACTICS: Acts like a typical ransomware operator. After hacking into the systems, the files are encrypted with the LockBit3.0 malware and a ransom demand message is left to read. At the same time, victims are pressured by announcing on their own sites which targets have been attacked and that their data will soon be available for download if the ransom is not paid.

A PASSION FOR A SAFE CYBER WORLD

CWF
Cyberwatch Finland

Cyberwatch Finland is a strategic cybersecurity consultancy house that provides professional services for companies and other organisations by strengthening and developing their capabilities to protect and defend their most significant assets.

Our Mission: Make Cybersecurity a Business Opportunity

Cyberwatch Finland serves companies and other organisations by strengthening and developing their cybersecurity culture.

Increasing regulation improves cybersecurity in all organisations, but compliance with the minimum requirements is not enough in the ever-tightening competition. A high-class cybersecurity culture is a competitive advantage and creates new business opportunities.

Our strength is a unique combination of profound know-how and extensive experience.

Our team of experts consists of versatile competence in strategic cybersecurity, complemented by extensive experience in management, comprehensive security and operations in an international business environment.

Our experts know how to interpret and present complex phenomena and trends in the cyber world in an easy-to-understand format. Our work is supported by advanced technology platforms as well as modern analysis tools.

”We help our clients stay up-to-date and consistently develop a cybersecurity culture. At the same time, we are building a more sustainable and safer world together”

Aapo Cederberg, CEO and Founder, Cyberwatch Finland

OUR SERVICES

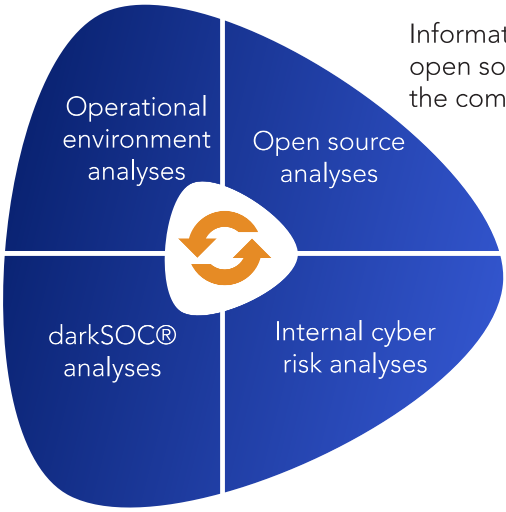
Management Advisory Services

We are experienced and trusted experts and management advisors. We give support in comprehensive security, cybersecurity, internal security, and third party risk management. Our working methods include, for example, theme presentations, background memorandums, workshops, and scenario work.

A Comprehensive Situational Picture

A comprehensive situational picture of cybersecurity is created with the help of the modular service developed by Cyberwatch Finland, for which the necessary data is collected using numerous different methods.

By analysing the operational environment from different perspectives, an overall insight is formed about the events, phenomena, and trends affecting the organisation.


Operational environment analyses
Open source analyses
darkSOC® analyses
Internal cyber risk analyses

Information collected from open sources complements the comprehensive picture.

The dark and deep web data is collected non-stop at 9 Gb per second, from servers located all around the world.

With the help of internal cyber risk analysis, a comprehensive picture of the organisation's insider threats, and other risk factors are formed.

OUR SERVICES

Reviews

Cyberwatch's analysis team constantly monitors the cybersecurity operational environment by collecting and analyzing information about events, phenomena and changes in the cyber world. The situational picture is produced by regular situational reviews.

Cyberwatch Finland
WEEKLY REVIEW
27/2024
THEMEREVIEW:
CYBERTHREATS AND HOW TO PROTECT AGAINST THEM
Cyberwatch Finland
MONTHLY REVIEW
JULY/2024
Cyberwatch Finland
MAGAZINE 2/2024
IDENTITY ACCESS MANAGEMENT IS A CRUCIAL PART OF CYBERSECURITY
IDENTITY SECURITY IS AT THE FOREFRONT OF MODERN CYBERSECURITY
WHAT KIND OF CYBER-DIGITAL WORLD WILL WE LIVE IN 2024?
Cyberwatch Finland
THEME REVIEW

Weekly Review

Weekly reviews introduce the current events of the cyber world and are declarative in nature.
The focus of the weekly review is identifying phenomena and trends and placing them in a relevant framework.
The weekly reviews serve as the basis for the monthly and quarterly reviews and the annual forecasts that are based on this data.
With the help of the weekly reviews, it is possible to get an up-to-date understanding of the significant events in the cyber world to support decision-making.
The weekly reviews are published 52 times a year in Finnish and English.

Monthly Review

The monthly review sums up, expands, and puts into context the themes and phenomena discussed in the weekly reviews.
The monthly review describes of the development of phenomena, focusing on different perspectives of hybrid influencing.
With the help of the monthly review, it is possible to get a deeper insight into how the events of the cyber world affect society and the operational environment.
The monthly reviews are published 12 times a year in Finnish and English.

Cyberwatch Magazine

Cyberwatch magazine is a digital and printed publication, in which experts from both inside our organisation and from our professional network explain about the current events of the cyber world, the development of technology and legislation, and their impacts on society, organisations and individuals.

Special reports

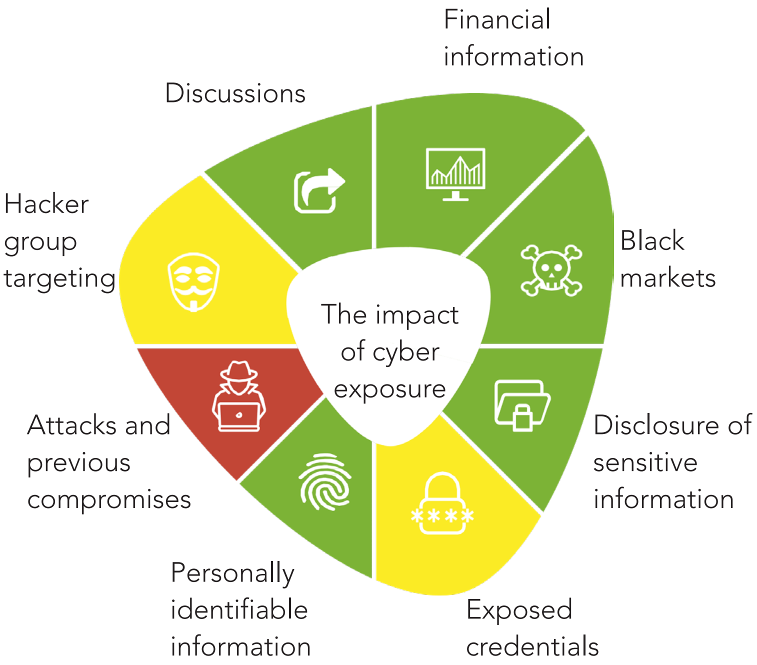
We produce reports and overviews on customised themes, for example from a specific industry or target market: assessments of the current state, threat assessments, analyses of the operational environments, and forecasts.

OUR SERVICES

darkSOC® – the Dark and Deep Web Analysis

With darkSOC® -analysis, we examine and report your organisation’s profile and level of exposure in the dark and deep web. Data is collected non-stop at 9 Gb per second, from servers located all around the world. The analysis reveals organisation’s cybersecurity deficiencies, data breaches, and other potential vulnerabilities. With the help of analysis, you get an overview of what the organisation looks like from the cybercriminal’s perspective.

We prepare a written report from the analysis, in which we highlight key findings to support management's decision-making. The report also includes a more detailed presentation of the findings. We also give recommendations on immediate corrective actions and strategic-level development targets.


Financial information
Discussions
Hacker group targeting
Black markets
The impact of cyber exposure
Attacks and previous compromises
Disclosure of sensitive information
Personally identifiable information
Exposed credentials

The Benefits of darkSOC®

Increases cyber intelligence capabilities

Anticipipates constantly changing cyberworld

Complements company's cybermaturity

Serves as a forensic investigation tool

Supports organisational strategic decision-making

Complements strategic cyber situational picture

Discovers vulnerabilities and weaknesses

Fasilitates cyber strategy process

OUR SERVICES

Analysis

The Surface Web Analysis

We form an external view of your level of cybersecurity in the surface network and compare your position with other organisations in the same industry. Our analysis is based on the platform of our global partner SecurityScorecard, whose data is based on a trusted, transparent classification method and data collected from millions of organisations. Based on our analysis, we make recommendations on corrective measures and draft a road map for their practical implementation in your organisation.

Powered by

Security Scorecard

The Open Source Analysis

We produce analyzes based on open sources on the topics you choose. We use advanced digital tools with which we search for information from public free and commercial sources as well as from various media and social media platforms. We refine the data into a form relevant to the goals of the analysis.

Internal Cyber Risk Analysis

With the help of an internal cyber risk analysis, it is possible to form an overall picture of insider threats and other risk factors related to your organisation's cybersecurity.

We analyse the up-to-dateness and comprehensiveness of your organisation's cybersecurity policies, guidelines, instructions and other documentation. In addition, we interview the selected management members and other key personnel.

As a result of the analysis, you will have an image of the balance between your organisation's operation and the internal guidelines and external regulations that guide it, as well as a road map for developing the operation.

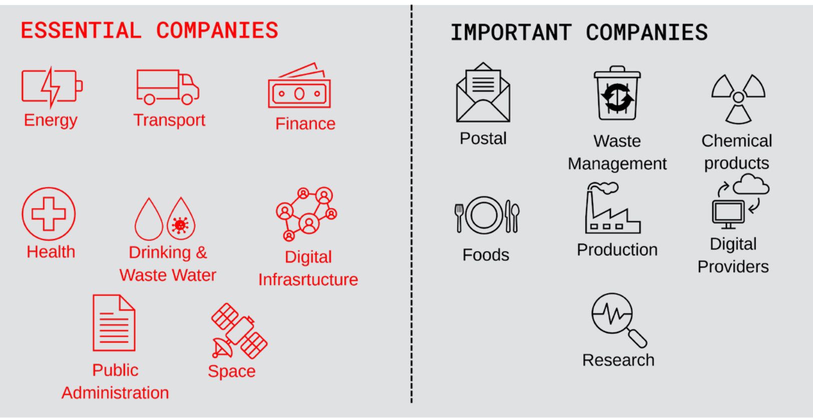
OUR SERVICES

Analysis

NIS2 Gap analysis

The aim of the NIS2 Cybersecurity Directive is to improve the basic level of cybersecurity in the EU and to ensure the continuity of operations of critical entities
The directive entered into force on 17.1.2023, with member states having time to put things in order by 17.10.2024.

NIS2 cyber security directive concerns the following fields:



ESSENTIAL COMPANIES

Energy
Transport
Finance
Health
Drinking & Waste Water
Digital Infrasrtucture
Public Administration
Space

IMPORTANT COMPANIES

Postal
Waste Management
Chemical products
Foods
Production
Digital Providers
Research

The minimum requirements of the NIS2 Cybersecurity Directive are:

1. Policies on risk analysis and information system security
2. Incident management
3. Business continuity, such as backup management and recovery, and crisis management
4. Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
5. Security in network and information systems acquisition, development and maintenance, including vulnerability management and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
7. Basic cyber hygiene practices and cybersecurity training
8. Policies and procedures regarding the use of cryptography, and appropriate encryption means
9. Human resources security, access control policies and asset management
10. The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Preparing the equivalency of current state of your organisation with the minimum requirements should be started well in advance. Cyberwatch's NIS2 gap analysis is a risk-based approach to the minimum requirements, using not only the directive but also the ISO 27001 standard and related management measures as a framework. With the help of the analysis, the organisation can direct development activities to the right targets.

OUR SERVICES

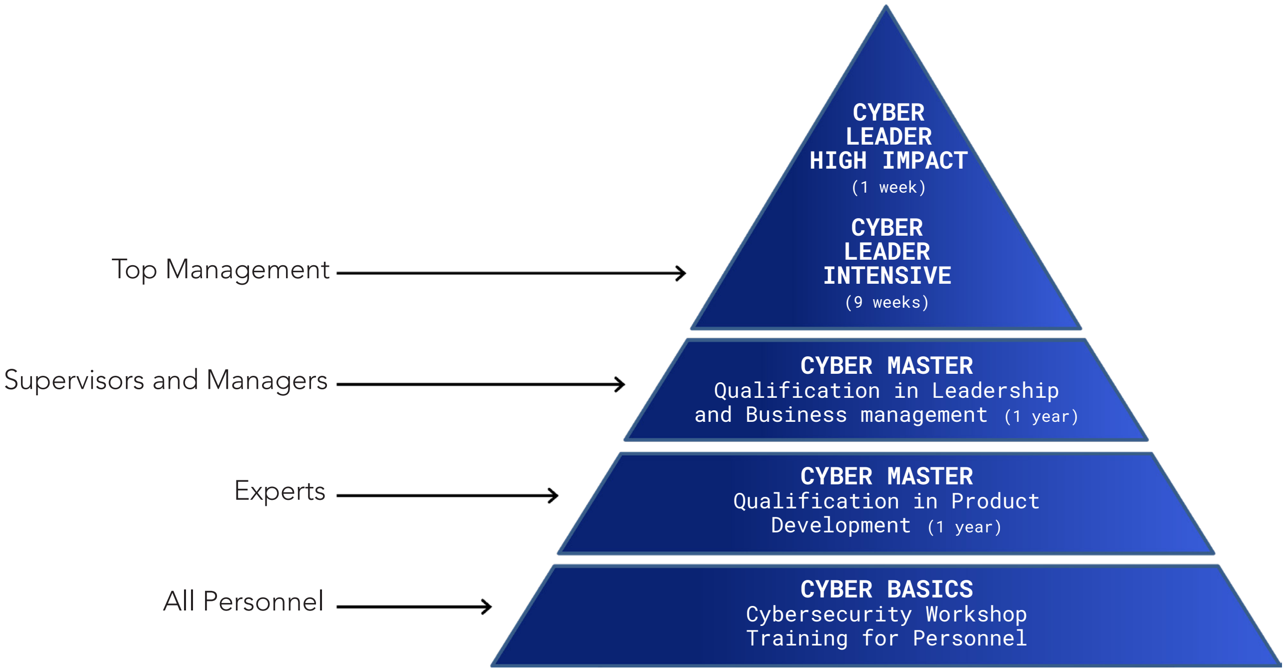
Training and Competency Development

We produce training for the Cyber Master specialist vocational qualification in co-operation with the Management Institute of Finland MIF Oy.

Currently, in the programs, it is possible to complete the Cyber Master qualification in leadership and business management as well as in product development.

We also provide tailored training for your organisation, which helps to strengthen your organisation's cybersecurity skills and helps you to be better prepared for the challenges of the digital operating environment.

Our all training offering consists of modules, from which student or organisation can choose the options according to their needs.



Top Management → **CYBER LEADER HIGH IMPACT** (1 week) / **CYBER LEADER INTENSIVE** (9 weeks)

Supervisors and Managers → **CYBER MASTER** Qualification in Leadership and Business management (1 year)

Experts → **CYBER MASTER** Qualification in Product Development (1 year)

All Personnel → **CYBER BASICS** Cybersecurity Workshop Training for Personnel

CWF

Cyberwatch Finland

A PASSION FOR A SAFE CYBER WORLD

Contact

Cyberwatch Oy
Nuijamiestentie 5C
00400 Helsinki Finland

aapo@cyberwatchfinland.fi
myynti@cyberwatchfinland.fi

secapp

PREPARE | ALERT | COMMUNICATE | DOCUMENT

"Coordinating a large-scale disruption and starting operations has sped up enormously. One push of a button, and things start rolling."
- Tomas Lång, DNA

Every second matters

Helps secure daily operations, manage crises and save lives.

Improves preparedness for and response to unexpected situations.

Ensures secure communication and sharing of real-time information both in everyday and critical situations.

Do you want to know more?

sales@secapp.fi
secapp.fi

identityday.se | identityday.fi

Event
Identity
Security

Identity Day 2024

Stockholm, October 3rd | Helsinki, October 24th

Get inspired!

Identity Day is the event where leading experts gather to share insights, knowledge, and tools to protect your organisation against data breaches and modern IT threats.

The event is free of charge, but the seats are limited. Make sure to secure your seat today!