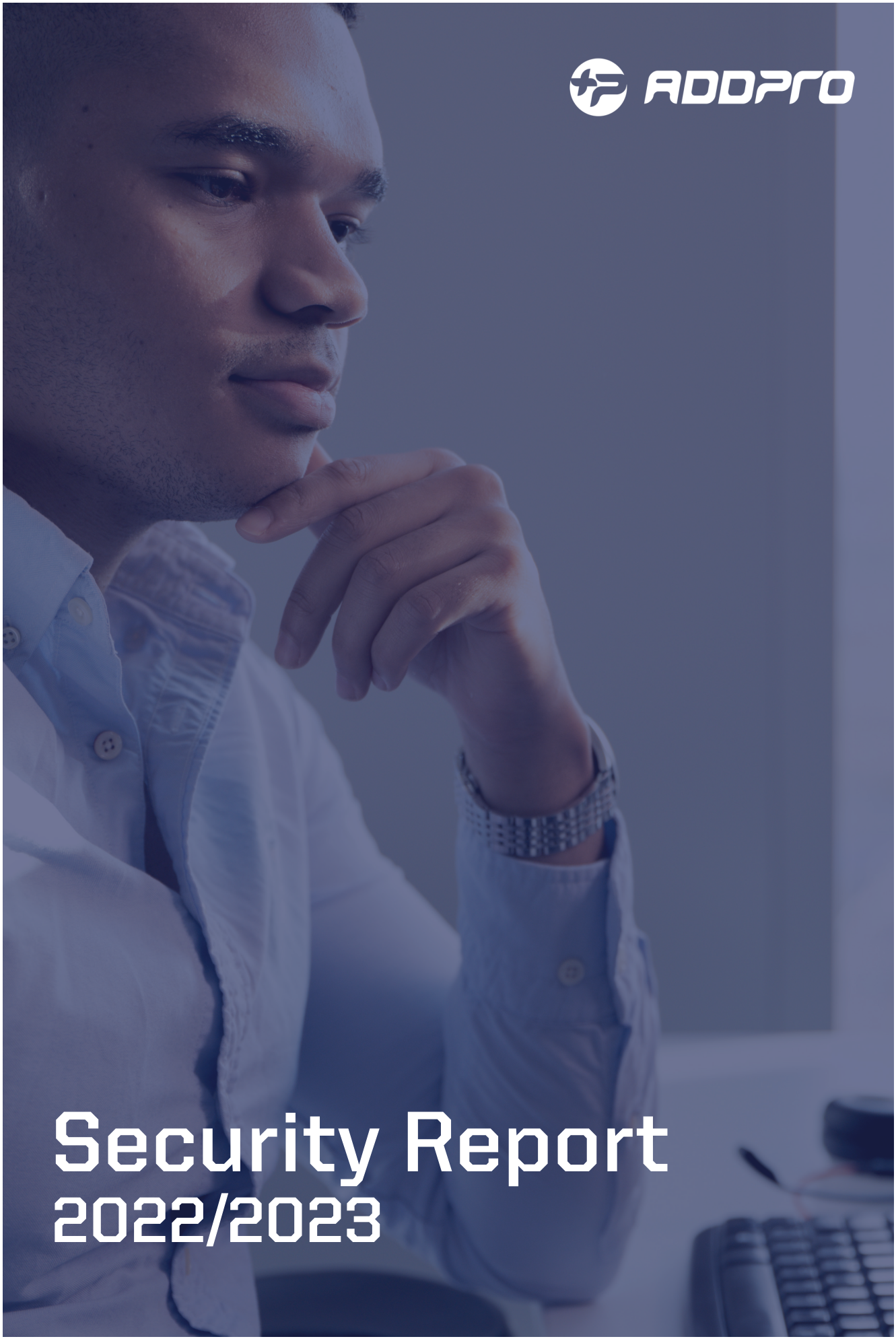


Security Report
2022/2023

Contributors

This edition of the Security Report has been made possible with the contribution from the following individuals.

AddPro

Nicklas Persson, CEO
Niclas Szieger, CFO
Thomas Öberg, Competence Area Manager
Jens Johansson, Management Consultant
Rikard Burman, Lead Architect
Kent Ekensteen, Lead Architect
Daniel Olsson, Lead Architect
Marcus Landgren, SOC Manager
Josefine Olsson, Marketing & Sales Coordinator
Sara Ferhm, Digital Marketing Specialist

Improsec

Thomas Wong, Director of Technical Cyber Risk Advisory

Norelid Advokatbyrå

Marcus Appeltofft, Lawyer | Senior Associate

A word from the CEO

2022 has been an eventful year from a security perspective. When we finally could state that the Covid pandemic was coming to an end, the world was hit by several decisive events with a global impact and consequences for both people, countries, politics, economy and societies for a long time ahead. In short, the world has become more insecure and dangerous, and we must relate to and act accordingly, both as individuals, companies, organizations, politicians and countries.

The overall world events affect us all politically, economically and security-wise. Russia's war of invasion against Ukraine has been the single biggest cause of the challenges we have to deal with today. Strongly rising inflation, weakened economy, energy prices reaching new highs almost daily causing everyone to make new risk assessments both from a private and professional perspective. This is also accelerated by North Korea's and China's aggressions against their closest neighbors, South Korea and Taiwan.

All these activities triggers a number of political and economic sanctions. The decisions are made from a currently united world preferably consisting of democracies that in unison support the Ukrainian people's fight for their freedom and perhaps even partly fight for Europe as we know it today.

There is also a cyberwar going on in parallel with the conventional war. Cybercrime is increasing worldwide and in Sweden we have seen several examples of this when large Swedish companies, organizations and service providers have suffered with major consequences for the businesses, society and private individuals.

In this security report for 2022/2023, we have tried to gather the major and overall events and trends. With this background, we hope that you can prevent many security risks both for your business and for you as a private person during 2023 and beyond.

Never trust, always verify!

Nicklas Persson, CEO

Editor’s notes

One thing we´ve changed in this year’s edition is the addition of perspectives from a wide range of roles and competences. Several individuals from AddPro have shared their thoughts about the past year as well as some insightful predictions, all from the perspective of their unique position in cybersecurity.

We are also happy to introduce the participation of two new partners; Improsec and Norelid Advokatbyrå. Improsec is a leading cybersecurity firm in Denmark and is not only a partner but also share the same owner as AddPro; ITM8. Norelid Advokatbyrå is a law firm specializing in cybersecurity that we think will be very valuable to our customers in the coming years as the legal landscape is becoming more and more difficult to navigate.

As always, we try not to get too technical in the articles while still providing value in an easily digestible format.

Thomas Öberg,
Competence Area Manager

Content

World politics

What has become more evident during the year is the two-sided polarization in the geo-political arena. The ongoing war in Ukraine more or less forces countries to chose an alliance. On one side, the Western governments with the United States, EU and United Kingdom representing the current dominant political and financial force in the world along with the military alliance NATO. On the other side, the emerging economies joined together in a group known as BRICS. Representing interests from Brazil, Russia, India, China and South Africa, this group is not only growing financially and geographically but is also dominating global production and transportation. With Egypt, Iran, Saudi Arabia, Turkey, Argentina and other countries in some process of joining the group, the dependency to the US dollar and the world banking institutions is gradually declining. The impact of economic punishments, such as sanctions is therefore becoming less effective to a noticeable degree.

Cybersecurity has not been spared in this division of alliances as the nation state activities in this regard are steadily increasing with multiple attacks to critical infrastructure. With less focus on stealth and more on effectiveness, the threat actors backed by nation states are increasing the cyber warfare to a global scale which reminds us of the cold war.

Could it be that the year 2023 marks the beginning of the end of Pax Americana?

Thomas Öberg, Competence Area Manager

Economy, energy and war

In 2022, the pressure on energy supply turned into an energy crisis with a shortfall in supply, leading to prices we´d never seen before. Politicians all over Europe have had this issue as one of their top priorities for a while now and investment in sustainable energy will for sure continue and accelerate. Even though we expect to see improvements in 2023 there will still be challenges, and prices will continue to be high. The energy crisis has contributed to the accelerated inflation during 2022, with an inflation above 10%, which we haven´t experienced in decades. Central banks have acted well synchronized with front-loaded rate increases and we will likely see a stabilization in near time.

Inflation, war, and energy crisis together with a challenging supply of semiconductors puts enormous pressure on the economy. The future will undoubtfully be uncertain and challenging, and a recession is almost certain. We can expect many businesses to be shut down during 2023, however, there are also tremendously many opportunities for the ones that can transform, increase efficiency and digitalize to continue to be competitive.

Niclas Szieger, CFO

Laws and regulations

The current global situation is reflected in organizations' prioritization of security issues. IT and information security are now one of the top priorities and we notice an increased demand for support regarding compliance from organizations. They demand not only competence related to technical security but also organizational security. In general, we see that our customers are faced with increased demands, in terms of compliance, from external stakeholders, e.g. laws, industry requirements and customers.

NIS 2
During autumn 2022, the Directive on security of network and information systems (NIS 2) was voted through in EU, and the member states must implement the directive. The biggest changes are; that more organizations will be covered by the directive and the focus of the directive will be capabilities regarding risk management and incident reporting. However, in Sweden we have to wait for the ratification process and a clarification of what the implementation exactly entails.

Whistleblowing
During 2022, legislation regarding whistleblowing came into force in Sweden. Organizations need to ensure reporting routes and awareness regarding whistleblowing. During the year, organizations with more than 250 employees should comply with the law. The technology company Insight, points out that approx. 60-70% of affected companies have taken initiatives to comply with the law. At the end of 2023, the number of organizations covered will increase as the threshold will be lowered to 50 employees.

Data transfer EU-US

During the year, an executive order was carried out by the President of the United States with the aim of equating the protection in the United States for personal data to be leveled equivalent to the EU. Negotiations still remain between the US and EU as well as precedents from courts in the EU. The outcome of the judgment will affect many of our customers and provide them with guidance in future strategies.

GDPR

In 2022, an increased demand from organizations to review their work with personal data management and the introduction of appropriate protection measures has been noticed. Since 2017/2018 when data protection regulation took place, many organizations have lived with the work they did then. In 2022 they where more matured on the subject and seriously wished to work with issues connected to GDPR.

Jens Johansson, Managment Consultant

Readiness

Vulnerabilities have increased to a large extent in recent years and the threat to our daily work is something that everyone needs to take seriously. Today, it's not good enough to apply OS updates and believe that everything is fine. Drivers, BIOS and applications must all be in your patch management process. During 2022, we have seen firmware vulnerabilities being actively exploited to gain a foothold in customer environments.

The lack of labor with competence in cybersecurity has been a contributing factor to the breaches during 2022. Organizations are willing to invest in security but haven´t been able to recruit new employees or hire consultants which has slowed down the implementation of security functions.

The cybersecurity firm Cyble has detected that over 8.000 VNC instances are exposed to the internet without authentication requirements. This shows that security is not only for the IT department to consider but for the entire organization. When new systems are bought, security must be one of the requirements in the procurement process.

During 2023 we expect that boards get more involved with cybersecurity, especially with NIS 2 being implemented in Europe.

Business e-mail compromise

The latest years ransomware attacks have been a big threat to companies and organizations of all sizes around the world. But lurking in the shadows is Business Email Compromise (BEC) that's five times as large as ransomware when looking at the money transactions being performed.

With cleaver and sophisticated social engineering attacks or by exploiting vulnerabilities in email systems in order to gain access to e-mail accounts and conversations, the threat actors get the tools to create new or manipulate ongoing conversations with customers. One of the most common one is when they get the target to acquire a gift certificate for an upcoming birthday of someone in the targeted organization and send the gift certificate to the threat actor.

A more sophisticated attack is when accounts of suppliers have been breached and instead of the supplier sending an invoice of the ordered wares to the customer it's the threat actor sending the invoice from a known associate with the bank details altered to the threat actor instead.

In 2023, it´s likely that BEC attacks will continue to evolve and become more sophisticated. Attackers may use artificial intelligence like ChatGPT to make their emails and websites more convincing and may also target specific individuals or industries in order to increase the chances of success. It will be important for businesses to stay vigilant and continuously update their security measures in order to protect organizations against these threats. End user training of all employees starting with the finance team is in high demand.

Identity security

During 2022, companies and organizations have worked hard to strengthen the most targeted asset in the world, the user identity.

It used to be that the user identity was protected behind firewalls and in most cases not accessible from internet. Today, it's the other way around. Instead of the identity being something that's protected in our on-premises environment, it's now available from anywhere and from any device. To protect user identities the most common way is to use multifactor authentication, but even this turns out not to be strong enough.

With multifactor authentication being implemented on everything, uses are requested multiple times a day to approve sign-ins. This has led to MFA fatigue, where users are approving sign-ins without considering "Did I really just sign in?".

In order to protect user identities, MFA is no longer good enough in today's threat landscape. This was something the ride-sharing giant Uber got to experience in September 2022. By gaining access to an employee's credentials, the user account was overloaded with MFA requests. By using social engineering posing as the IT department, the employee finally approved the MFA request, giving the threat actor inside access to Uber systems via a VPN system.

To protect organizations against MFA fatigue, one of the solutions available now is number matching. Instead of just approving a sign-in request, there are 2 digits shown on the screen that must be entered in the authenticator app on your phone. Even if it seems insignificant, this strengthens the MFA process while using the same app the end users are already used to.

But relying on one layer of protection is not enough. Security is like an onion, filled with layers. Although security shouldn't make the end user cry when using it. It should instead make the threat actors cry when cutting into it. If MFA fails to stop a threat actor, a safety net of identity protection technologies should be in place to allow for investigation and capabilities to challenge or block the sign-in.

Identity protection will continue to be of major concern for all organizations during 2023. A key trend is the usage of biometric authentication methods such as facial recognition or fingerprint scanning, which will provide stronger security for online accounts.

.

"Trust no one, question everything and suspect everyone"

Rikard Burman, Lead Architect

Azure security

It's still very easy to create a SaaS service in Azure such as a database or storage account. The problem we've experienced is that some organizations have no control of the information flow. SaaS-services are often published directly to the Internet by default, and the simplicity and agility as well as lack of knowledge of Azure have been contributing factors as to why many companies have exposed sensitive data without knowing it. In Azure, it´s no longer a team of collaborating people who set up the services, such as application specialists, firewall gurus and infrastructure teams where each instance filters doubtful configurations. The responsibility for all security is now placed on the individual who creates the resource in Azure. This person should not only think about function, but also the security linked to the information classification of the data in the service. This demands that we consume Azure on a secure and correct way.

Identity theft
Another alarming trend we're noticing is the identity theft of user accounts that has rights to create resources in Azure. Once the threat actors have hijacked an identity, they create resources in Azure that can be used for illegal activities, and at the end of the month when the invoice arrives the damage has already been done. This can be prevented by consuming Azure properly.

A change in mindset
Despite all the challenges, everything in 2022 was not bad. On a positive note, we saw the focus shift from previously connecting Azure to the datacenter, to now connecting the datacenter to Azure. An important change in attitude.

With products like Azure Arc and Defender for Cloud, we now experience that:

1. The on-premises datacenter becomes a part of Azure's security mindset even for those organizations who consume nothing at all in Azure, which allows the datacenter to be monitored and managed as if they were in Azure.

2. Azure Arc in combination with Defender for Cloud is an important piece of the puzzle that many organizations need to work with.

In 2023, we will continue our proactive work to secure how information is published in Azure and how to consume Azure correctly to avoid information leakage. We do this with workshops to get an understanding of what simple Azure delegation means. Information must be secured with frameworks and instruments so that Azure can be consumed and delegated in a secure way.

Kent Ekensteen, Lead Architect

Endpoint security

”Plan for the best but prepare for the worst”

The year 2022 was a security wakeup call for a lot of customers. The old focus was to maintain the platform and only react to security related incidents when they already had occurred. The mindset has now started to shift to a more proactive way of thinking regarding security in general and device management. Now the customer gets in the driver's seat and takes control of the security related concerns. No one can fix all the security issues on the endpoints but with the right focus, we can mitigate the largest ones in a higher velocity than ever before. The security focus has changed with the help of Microsoft Defender for Endpoint and similar products that visualize and prioritize security related activities and needs.

We´ve seen a rapid increase in both BIOS and driver related hacking to gain control over computers during 2022/2023 and there will probably be even more situations with the rise of AI-based malware incidents. The black market will increase with companies where remote access can be bought to a lower cost than before. If 2022 was the wakeup call to focus on security with sensor-based knowledge on the endpoint, 2023 will be the year when we actively mitigate against those issues.

”Get-Secure or die trying“

In 2023, many organizations will require security-based endpoint services. In combination with a Security Operations Center for 24/7 monitoring and incident response, the endpoint security will be taken to the next level. This will also increase the need of even stronger authentication methods, such as passwordless sign-in.

We still don´t have a bulletproof endpoint with zero security issues. With the financial situation in 2023 we´ll probably add more requirements for digital transformation and all of us must work in that direction together as a team. "Work smarter not harder" to create a more user friendly and secure endpoint experience in the end.

Daniel Olsson, Lead Architect

Security Operations Center

A year of growth
2022 has been a busy year for AddPro SOC. We have doubled our number of customers and expanded our protected user base by a factor of ten. We have responded to a wide array of incidents which has both tested and confirmed that our SOC service is well worth the investment.

Security awareness - "Full stack"
The IT department has always somewhat acknowledged the importance of security, but we are finally experiencing security being taken seriously from a C-level perspective. Security services, tools and licenses being included in the IT budget and the demand for security workshops, end user security awareness trainings and compliance workshops has increased rapidly during the year.

Every organization is unique, but basic IT security remains the same. Fundamental security measures such as enabling multifactor authentication, segmenting privileged accounts and servers and isolating the backup systems, goes a long way. While it´s not possible to change the IT environment overnight, efforts can be made to make an inventory and start securing and monitoring the company's most exposed and critical assets.

Preparation is key
We strongly advise every organization to have an incident response plan in place for 2023. A plan that covers how to act and who to involve in the event of an IT security related incident. Questions such as 'what regulatory requirements do we have?'

Or 'how do we perform a partial lockdown?' Should be answered, pre-approved, and up to date. Having these processes in place will be of great assistance when disaster strikes.

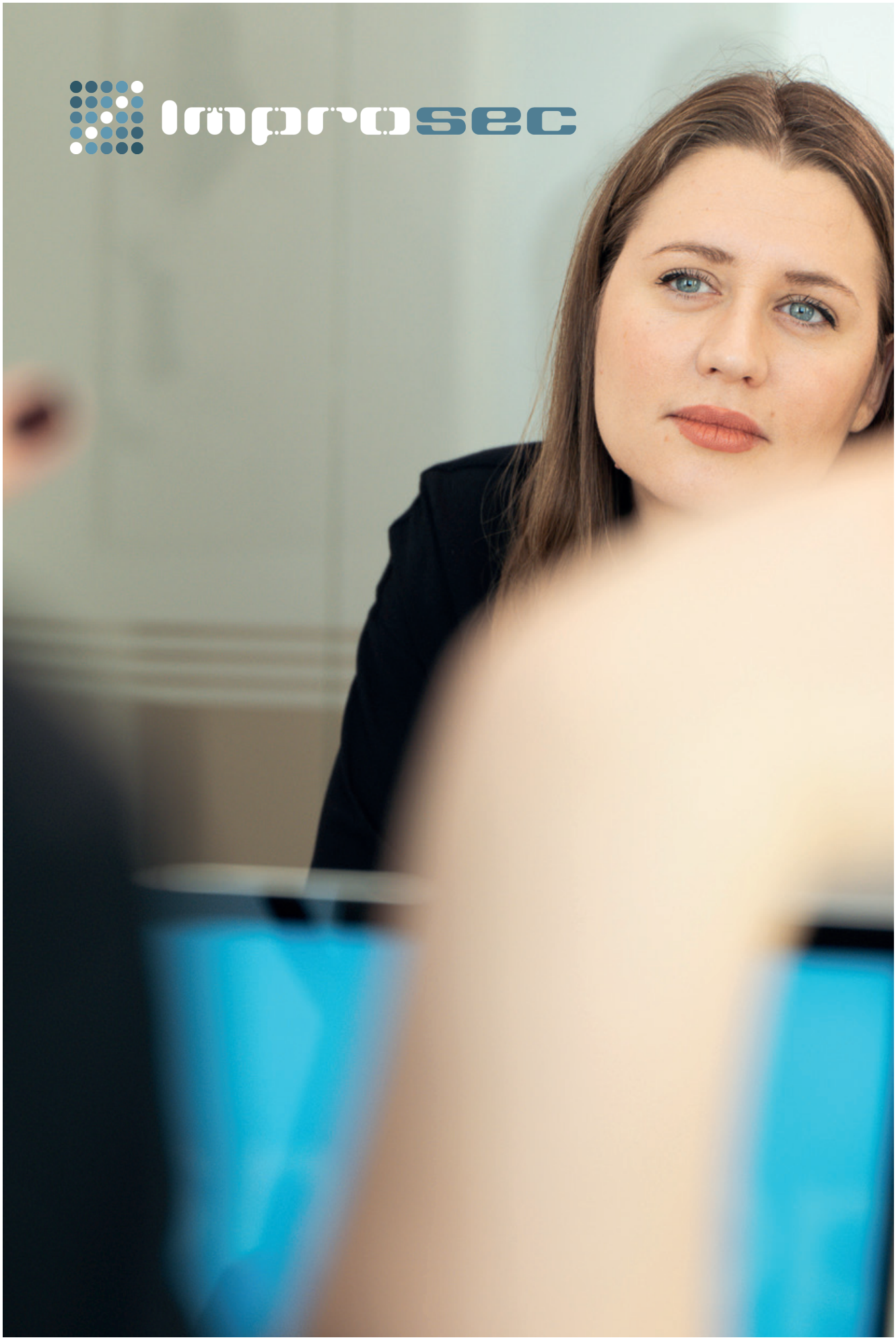
Tools that help

AddPro SOC is based on Microsoft's security, and we are confident in our choice. Microsoft Sentinel, a relatively young SIEM solution, is already being placed as a leader both in Gartner's and Foresters' reviews. Microsoft has a strong focus on security and is constantly adding new features, services, and integrations with vendors, but what really stands out is the community. Security personnel worldwide are sharing their knowledge and keep adding content to the tools.

Final words

Our service is built on the relationship between AddPro and our customers and we are looking forward to a 2023 with a continuous collaborative effort to evolve the SOC service, and to keep securing organizations.

Marcus Landgren, SOC Manager


Improsec

Out with the old, in with the new

In the world of cybersecurity, a year is an incredibly long time. In 2023, cybersecurity threats are expected to continue to evolve at an astounding rate. It´s inevitable that the novelty and inventiveness of cyberattack methods will keep pace. Cyber criminals will continue to develop new ways of attacking businesses. In December 2021, a zero-day vulnerability was exposed involving arbitrary code execution in the wide-spread component Log4j which was completely unknown one year earlier. It quickly caused major damage. The United States CISA chief, Jen Easterly described it as one of the most serious flaws out there. In 2022, Log4j was still unmediated in many companies which means that this threat is likely to continue to haunt us for many years to come.

Regardless of how much we try or wish we could, we can´t predict threats like Log4j. Novelty and creativity are by definition unpredictable. However, that doesn't mean that threat analysis is futile. Despite the creativity of cyber criminals, and the impossibility of predicting the future, it´s imperative to learn as much as possible about potential cybersecurity threats.

What we can predict, is that malicious actors are bound to try to use the same strategies again in the future with the hope that their target is not updated on all the latest exploits and vulnerabilities. Cybercriminals know that a significant number of enterprise networks remain vulnerable to security flaws despite the fact that solutions for these flaws have been available for quite some time now.

When we anticipate the biggest threats for 2023, they are often the same threats presented in 2022. Therefore, it´s worthwhile to review the threats and events of 2022. Looking back, we have experienced a global pandemic, the death of a queen, and a regional war that has highlighted the darkest sides of human nature. There is no question that the stakes are rising in terms of the risk of cyberattacks on digital assets and critical infrastructure.

When we reflect on 2022's threat landscape we also must account for how these world-changing events affect cyber security. The threats that haunted us in 2022 are not just going to repeat, the nature of their threat is known, or they are poised to become more acute. For example, ransomware has been a major cybersecurity issue for years, and it doesn't look like it's going away anytime soon. Threats like ransomware is increasingly becoming more targeted, with the attackers going for larger companies that they believe have the capacity to pay. They are also more patient, avoiding detection for years before they begin to deploy their malware. Another example is the talent shortage. The demand for qualified employees will most likely grow in 2023 and further intensifying the gap between the need for and the availability of experienced IT personnel.

On the following pages we'll share our top predictions for 2023, along with a peek into the key emerging trends we predict will take hold over the next decade.

Targeted ransomware

Skilled criminals are moving towards targeted ransomware techniques to make larger payments. In addition to using specialized strategies, approaches, and processes, these attackers can target specific companies in a specific way based on their capacity to pay a significant ransom. This is commonly referred to as "big game hunting".

These attackers are often very innovative, as they go to considerable lengths to find and exploit weaknesses within a victim's technology stack. They also select the most valuable data in order to encrypt and hold it as a ransom. In addition to that, they are extremely patient, raising privileges to bypass security measures and avoid detection for months, if not years, before they begin installing malware.

A recent example of this long-tail, targeted technique can be seen in the Hades ransomware attacks. According to ZDNet, ransomware operators are targeting huge multinational corporations with yearly sales of over $1 billion and have successfully targeted at least three enterprises in the transportation, retail, and industrial industries. There has been a fundamental shift in the security industry since ransomware first made headlines.

OT/SCADA

OT is a term that refers to the systems that are used to monitor and manage the assets of an organization that are involved in manufacturing, or manufacturing processes related to industrial processes.

As OT is closely related to both ICS (industrial control systems) and SCADA (supervisory control and data acquisition systems), it´s a term used to distinguish it from IT, which represent the information technology assets of an organization.

Vulnerabilities and risks associated with SCADA systems
It´s primarily due to the lack of monitoring that SCADA systems are so vulnerable to vulnerabilities. As most SCADA systems lack an active monitoring system, they often fail to detect suspicious activities or to provide a proper reaction when a cyberattack happens. The more sophisticated systems become, the more vulnerabilities they develop. It can be challenging to keep everything under control, if there´s no proper system in place, for maintaining the hardware and software that needs to be updated consistently. Unfortunately, there is often an absence of knowledge about the devices that are connected to SCADA systems and updates are also often overlooked. It isn't uncommon for SCADA systems to evolve over time, which can result in finding new technologies paired together with old technologies.

As a final reason for SCADA vulnerabilities, authentication holes can also be found in the software, because even though they were designed to keep SCADA systems safe from unauthorized access, they are usually defeated, either due to poor passwords, weak authentication, or the sharing of usernames between users.

Where do we think the risks will be higher next year?

- **Increased Malware Attacks**
  Malware is constantly evolving, and SCADA systems are not immune to attacks.
- **Data Loss**
  SCADA systems are increasingly being used to collect and store large amounts of data. If this data is compromised, it could cause significant damage.
- **Regulatory Compliance**
  SCADA systems must comply with various regulations, such as those related to safety and privacy. If these regulations are not followed, organizations could face serious penalties.
- **Network Vulnerabilities**
  As SCADA systems are typically connected to large networks, there are a variety of vulnerabilities that could be exploited.
- **Outdated Software**
  SCADA systems often rely on older, outdated software, making them vulnerable to known security flaws.
- **Physical Access**
  If an attacker can gain physical access to a SCADA system, they can bypass all security measures in place.

Thomas Wong,
Director of Technical Cyber Risk Advisory

2022 from a legal point of view

The biggest issue over the last couple of years regarding the safety and protection of personal data has arguably been the question of under what circumstances transfers of personal data to the US are allowed. Following an executive order signed by President Joe Biden, the European Commission on December 13, 2022, published a "draft adequacy decision" regarding the US. Although this is far from a final adequacy decision, we are steadily moving closer to a Privacy Shield 2.0 which might finally provide some clarity regarding compliant EU-US data transfers.

On the 10th of November 2022, the European Parliament adopted the NIS 2 Directive which will replace and repeal the NIS Directive. The NIS 2 Directive means that a significantly increasing number of businesses and industry sectors are covered by the Directive's security requirements and aims to further strengthen the cybersecurity for critical infrastructure.

The budget for the Swedish Authority for Privacy Protection, the authority responsible for enforcing the GDPR, will increase with approx. 40 % for 2023. This increased budget will enable the authority to employ more personnel and conduct more oversight to further enforce compliance with the GDPR.

Marcus Appeltofft,
Lawyer | Senior Associate

During 2022 we´ve also learned, through statistics published by the Swedish Authority for Privacy Protection, that:

- Personal data breaches have increased with 26 % in 2021 compared with the year before.
- The most common reason for of personal data breaches is the human factor, i.e., it´s extremely important to ensure that an organization's entire staff is educated and trained in the organization's responsibilities according to GDPR.
- The number of data breaches affecting Swedish data controllers appear to be severely under-reported when compared with statistics for other EU member states, something that is likely to be on the radar for the authority in 2023 and the coming years.

AddPro Cybersecurity

Phone: 040-59 24 00

E-mail: info@addpro.se

addpro.se