Monthly Review

Cybersecurity news from around the world

ARTICLE

World economic forum at the heart of cybersecurity

Read article →

SECTRA

General cybersecurity news

1 MSB stresses need for a risk-based approach to cybersecurity

In January 2024, The Swedish Civil Contingencies Agency (MSB) released the report "Cyber attacks on societally important information systems – 25 recommendations for strengthening protection against cyber attacks" (In Swedish: Cyberangrepp mot samhällsviktiga informationssystem — 25 rekommendationer för stärkt skydd mot cyberangrepp). This report presents the threat landscape against government agencies and providers of critical services in Sweden, based on IT incidents reported to MSB from April 2019 to September 2023. The report highlights that the number of cyberattack attempts constitutes less than one-fifth of the total number of IT incidents reported to MSB up until 2022. The number of reported cyberattacks experienced an unusual peak in 2023 due to an increase in DDoS (Distributed Denial of Service) attacks. However, the analysis of cyberattack attempts shows that 53 percent of the IT incidents define a security incident that has resulted in an actual impact on an organization's operations.

Many of the cyberattacks that have resulted in impacts have been carried out using less sophisticated methods. This suggests that there are shortcomings in protection and procedures, and that security efforts within organizations need to be strengthened, but also that better security can be achieved through relatively limited improvements. MSB has identified six areas where organizations face significant cybersecurity challenges and has formulated 25 recommendations to address these issues. The report emphasizes the importance of a systematic, risk-based approach to cybersecurity in an increasingly uncertain security environment.

2 Malvertising is becoming more common

Online Malvertising, a blend of malware and advertising used to distribute harmful content, has become increasingly intrusive and challenging to detect. Recent large-scale cybercrime operations have employed malvertising instead of traditional phishing, with search engines like Google and Bing being widely abused in distributing malicious ads. While search engines try to prevent malware spread on their platforms, scammers know how to evade their detection mechanisms. This approach is often more effective than traditional phishing due to users' trust in self-entered search queries and AI-generated results. To protect oneself from malvertising, users should always check links before clicking, avoid clicking on ads out of curiosity, prioritize staff training on online safety, and exercise caution when using web applications or search engines.

3 Organizations' social media accounts are valuable

Social media accounts of credible organizations are valuable assets that can be targeted by cybercriminals for financial gain or spreading disinformation. Recent hijackings of Mandiant's and the US Securities and Exchange Commission's accounts on X, formerly Twitter, demonstrate the effectiveness of such attacks. These accounts are often trusted, so breaches can severely damage reputations.

Their value lies in the information they share. The social media accounts of reliable and significant organizations serve as primary news sources for organizations and individual citizens, and the information they convey may not be questioned. Misinformation published in hijacked accounts can be used for financial gain. In addition to financial gain, threat actors can also seek other effects. State threat actors may be interested in spreading disinformation or sabotage. If, for example, in the face of a national crisis, the social media accounts of the country's most popular news channel were to fall into the wrong hands, it could have significant consequences for society as a whole.

ARTICLE

Cyber risks of nuclear power

The safety of nuclear power plants has always been a hot topic. Recently, attention has been focused on cyber threats to them. Although nuclear power plants are not on the list of the most attacked targets, they are definitely not completely free of the threat. Most recently, there were examples of this in the UK, when the media reported on two cases of cyber influencing on a nuclear power related organization.

One of these came a couple of weeks ago, when Radioactive Waste Management, a British public organization focusing on nuclear waste management, announced that it had been the target of targeted and long-running phishing attempts. The incident itself was not serious and, according to the organization itself, the attacks were unsuccessful, but it illustrates the interest towards the field. The significance is increased by the fact that this has been apparently planned and targeted specifically at this organization. The second case relates directly to the nuclear power plant rather than to the treatment of nuclear waste. In December 2023, the British newspaper The Guardian reported that it had learned that the systems of one of the country's most important nuclear power plants, Sellafield, had been hacked years ago. Reportedly, it is likely that not all remnants of the malware have been removed and the plant's management has even tried to cover it up. According to anonymous sources, information about hackers' access to the plant's systems and sensitive data has been known, →

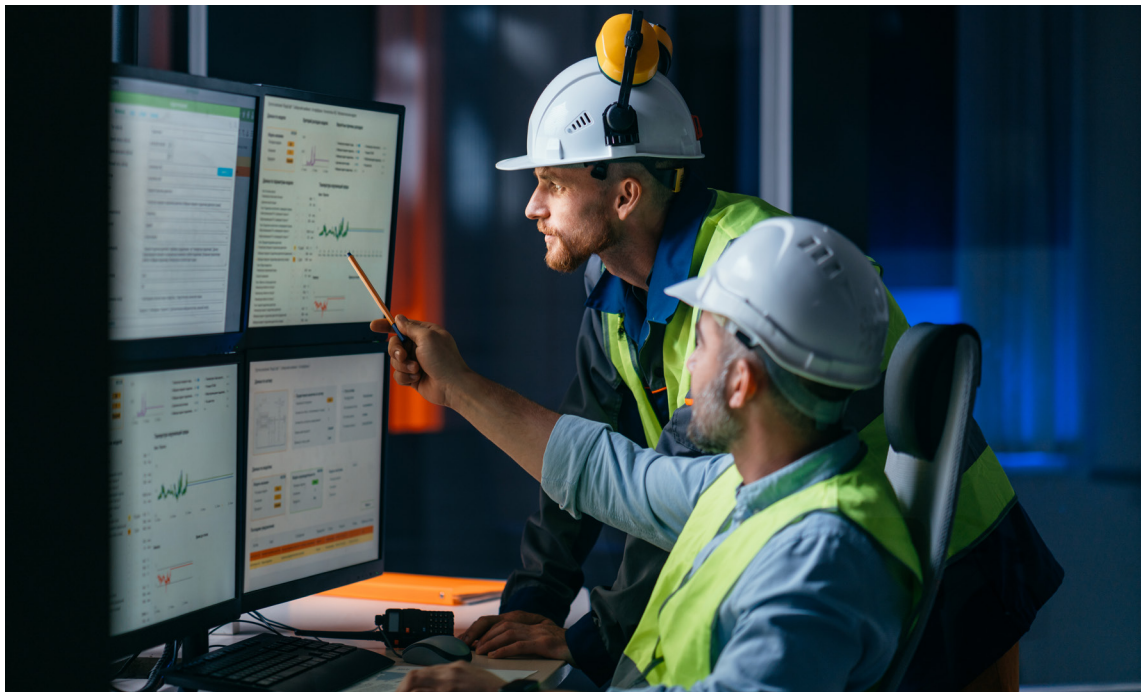
but very little has been done about it. In general, there have allegedly been many significant shortcomings in the plant's cybersecurity culture. Although anonymous journalism should be treated with caution, the fact that last week the Chief Cybersecurity Officer responsible for cybersecurity at this plant announced his resignation and the responsibility has been transferred to a different executive.

Energy sector faces growing cybersecurity concerns

In both cases, the motives behind the action are unclear. According to sources, both Chinese and Russian hackers have been involved in the Sellafield case, but there is no further information about the attackers' goals, at least not publicly. On one hand, it would be even quite worrying if high-risk targets had only been hit by a financially motivated operator who is not aware of or simply does not care about the risk that disruption of nuclear power plants may cause. On the other hand, however, it is perhaps more likely that behind the attacks exists a conscious and intended influence on specifically nuclear power plants by a nation-state directed hacker group.

"The informational effect of a cyber-attack on a nuclear power plant is also significant."

Power plants are attractive targets in many ways. Financially motivated crime is attracted by the industry's criticality, leading to a higher probability of paying ransoms. State influence is drawn by the significance of the activities to national energy production and the substantial information value associated with successful attacks The rise in electricity prices caused by outages is almost immediately felt in the everyday lives of ordinary citizens as well. The informational effect of a cyberattack on a nuclear power plant is also significant. In Britain, the debate on the safety of nuclear power has increased significantly in recent months. Although the attacks have not yet caused obvious or severe harm, concerns continue to grow. →



If the phenomenon is examined historically, it is clear that cyber influencing of nuclear power plants is not necessarily shy away. Over the past year, Russia, in particular, has demonstrated, in the form of military action against the Zaporizhzhia nuclear power plant, that it is prepared to use nuclear risks as a negotiating tool. The best-known cyberattack against nuclear power is also one of the most well-known cyberattacks in general and considered the best example of long-term high-level state cyber influencing. It is more than a decade old Stuxnet malware that targeted Iranian uranium enrichment plants and was likely a fact-finding and sabotage operation carried out jointly by the United States and Israel.

The digitalization of the nuclear power industry has increased cyber threats in recent years. Despite having strong cybersecurity measures, incidents like the Sellafield case demonstrate the risks. Enhanced security should encompass not just power plant operators but also subcontractors to protect critical infrastructure and maintain energy security. ■

ARTICLE

World economic forum at the heart of cybersecurity

The World Economic Forum (WEF) has recently profiled itself as a vocal advocate for cybersecurity. On January 10, the foundation published its Global Risk Report for 2024, which brings together leading insights from more than 1,200 experts around the world on short- and long-term risks.

According to the report, cyber threats are among the top ten threats by experts in both timeframes. A day later, the WEF released a report looking at the 2024 outlook for cybersecurity. Cybersecurity also featured prominently at the foundation's 54th annual meeting, which was again held in Davos, Switzerland on 15–19 January. In addition to having dedicated panels to the theme, including future scenarios for cybersecurity and tools for cyberdefenders, it was touched upon in several other speeches.

In order to understand the significance of WEF, its reports and the annual meeting, it is important to consider the background of the organization. The World Economic Forum is a foundation funded by large transnational corporations to promote globalization, free trade and public-private partnerships. The Annual Meeting, in particular, is an important discussion platform for topical issues. In Davos, business leaders and politicians meet every year. The value of WEF lies in its think-tank-like and unifying nature, where space is created for different ideas, expert speeches and futures thinking. →

In the WEF's report and at the cybersecurity discussions at the event, the most useful approach is to study future threats and their proposed solutions. For example, Ann Cleveland, executive director of the Center for Long Term Cybersecurity at the University of California, Berkeley, highlighted four looming future scenarios for cybersecurity. These include disruptions in microchip production and global production chains, constantly evolving deepfake materials and election interference, DNA data ending up in the wrong hands, and artificial intelligence. According to Cleveland, when responding to problems, it would be necessary to remember the principles of security by design in new applications. Also training and cybersecurity awareness play a significant role in responding to threats. Cleveland also pointed out that the future doesn't necessarily have to be negative. For instance, labor productivity may increase due to robotization and new technology, while active cyber cooperation could help tackle crime more effectively than before.

"When investigating a single cybercrime, many more are often revealed in the same case."

Although Cleveland also sought a positive approach in its introduction, the statistics and other speeches at the event indicate that the threat landscape is becoming more diverse, and the future looks rather bleak. For example, in a panel discussion on the possibilities of cyberdefenders, an Interpol representative said that the situation is challenging, because the more cybercrimes are investigated, the more they are uncovered. When investigating a single cybercrime, many more are often revealed in the same case. Also, the increasingly digitalized world increases the threat area to a significantly larger size. Increasing geopolitical tensions add their own spice to the mix. More than 70% of the respondents to the background material for WEF's cybersecurity outlook report say that the geopolitical situation has affected company's cybersecurity. In addition, less than one in ten respondents believe that AI will work to the benefit of cyberdefenders. →

Looking at the WEF data, it is obvious that cybersecurity is no longer a matter of its own in a vacuum. Cybersecurity has become an issue that has expanded to every area of life and is a key part of society's overall security and future solutions. The annual meeting discussed, among other things, climate change adaptation applications, biotechnology and the war in Ukraine. In all of these, there was also a place for the cyber element. From the perspective of ordinary citizens and organizations, the future can best be influenced by anticipating, preparing for and maintaining current cyber threat awareness. That way, even unpredictable events and future developments will not come as complete surprises. ■

Key takeaways

1. The Swedish Civil Contingencies Agency (MSB) provides actionable recommendations for enhancing cybersecurity through a newly released report.

2. Malvertising poses significant cyber threats by blending into legitimate ads and exploiting search engines, making it crucial for users to exercise caution.

3. Organizations should be aware of the value and effectiveness of their own social media accounts. They can be an attractive target for cybercriminals.

4. Nuclear power plants are an attractive target for both cybercriminals and nation-state supported hacker groups.

5. The World Economic Forum (WEF) has taken a prominent stand on cybersecurity. Future threats include unwanted election interference and artificial intelligence.

communications.sectra.com
communications@sectra.com

Sectra Communications is headquartered in Linköping, Sweden, and operates through offices in Sweden, the Netherlands and Finland.

SECTRA