Cyberwatch Finland

WEEKLY REVIEW

16/2024

Cybersecurity is Built by Small Actions and Management of Large Concepts

CONTENT

16/2024

MICROSOFT AND LACKING CYBERSECURITY

Last week, the Cybersecurity and Infrastructure Security Agency (CISA), the U.S. cyber and information security agency, issued a warning to government organizations about potential Russian cyber intruders. The warning is based on concerns that attackers may have managed to infiltrate systems by exploiting data stolen from Microsoft earlier this year. Microsoft announced in January that it had experienced a data breach in which an attacker gained access to emails from the US government and Microsoft's own source code, among other things. The hacker group known as Midnight Blizzard, Cozy Bear and APT29 was found to be behind the attack. This group is widely associated with the Russian Foreign Intelligence Agency (SVR) and is considered one of Russia's most powerful state-owned hacker groups. CISA urged all government organizations to inspect their systems for intrusion that has already occurred and to be particularly vigilant in the near future. It says it is likely that the hacker group is trying to continue its attack on some part of the government or an agency working for it. Neither Microsoft nor CISA has exactly disclosed what information Midnight Blizzard has obtained. However, it seems that the threat is real. Indeed, CISA said the leaked data posed a "grave and unacceptable threat." The warning applies to all entities under the U.S. government.

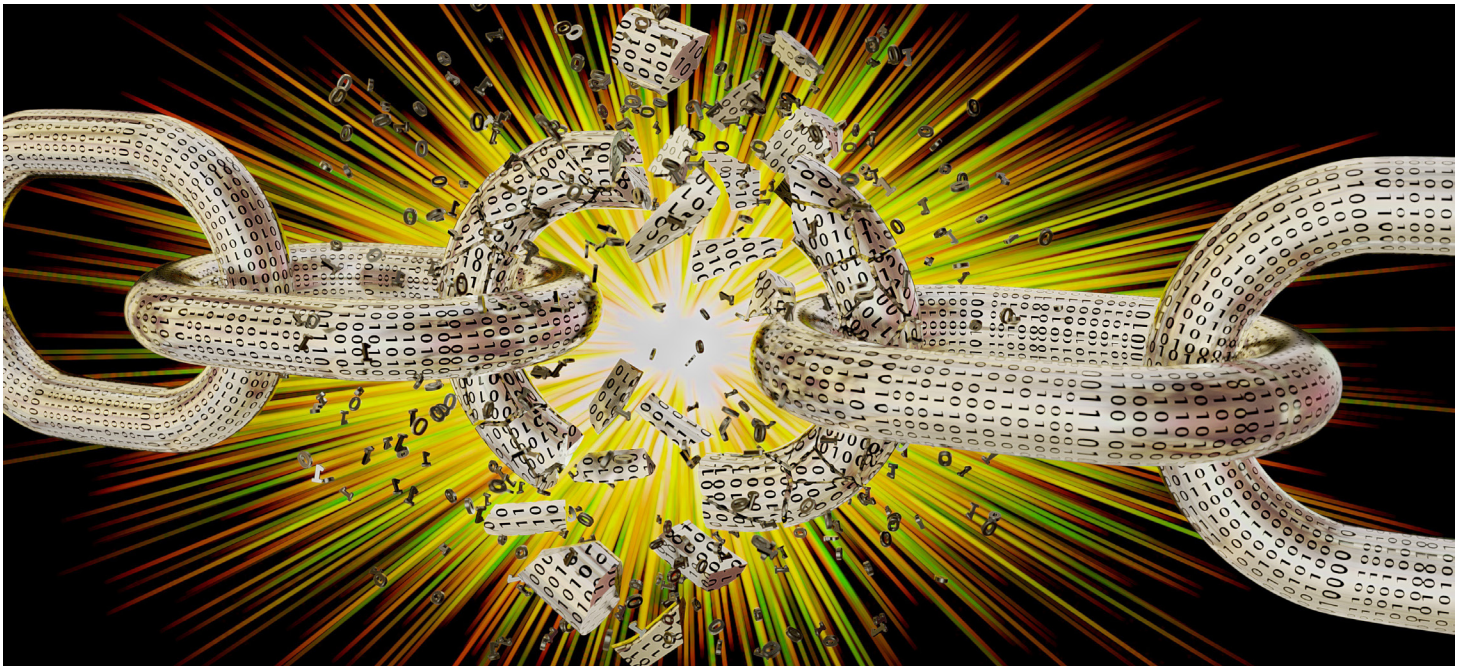
This is an embarrassing event for Microsoft, as it is not the first time that information about the US government has been stolen from its systems. Last summer, an operation that lasted several weeks was uncovered in which the Chinese APT group had managed to hack into dozens of mailboxes, including accounts of key US government officials. This attack had also been carried out by exploiting weaknesses in Microsoft's systems. The timing of this attack is also embarrassing because at the turn of the month, CISA's Cyber Safety Review Board (CSRB) published a report on the summer attack. According to the report, the attack could have been completely avoided, but Microsoft's lazily implemented security made it possible. The report also included major criticism of Microsoft's cyber security culture, and the trend that has been going on in the organization for years, where investments in security and risk management have been sidelined.

The reputational damage caused by the attacks and the critical report is only to a limited to an extent by the fact that Microsoft has made every effort to investigate the incidents and openly shared information about them together with the US government. The shortcomings in Microsoft's operating culture that have now been revealed in information security circles have been received with disappointment, but not as surprising discoveries. The digital giant has long been the subject of similar criticism, and recently many accusations – previously based on assumptions and conclusions – have been backed by evidence.

EXPLOITATION OF ZERO-DAY VULNERABILITIES ON THE RISE

Microsoft isn't the only digital giant to have been criticized for neglecting security. However, the threat posed by its poor security level is in a completely different league with, for example, Meta's unclear data collection practices or Google's privacy concerns. The use of Microsoft's products is virtually unavoidable, and security gaps pose a global and universal threat. Although so far attacks have only been carried out by state actors targeting the secrets of other states (or mainly the United States), nothing excludes, for example, a larger data breach in which business secrets would also be revealed. Successful attacks also have the potential for effective information influencing. Whatever Microsoft's reputation in security circles, it is still generally considered a reliable player. Successful attacks on this Western digital giant can therefore serve as an inspiring example for other criminals as well.

The relevant question at the moment is whether this debate will actually affect Microsoft's practices. Although the company has made statements that concerns are being taken seriously and measures have already been taken, it is unclear how much and how quickly it will manage to change course and whether the security culture will improve permanently. However, while waiting for this question to be answered, it is also good to consider what information and functionality organizations provide to Microsoft, and what would happen if this information were revealed. It may also be essential to consider how to prepare for the event that Microsoft services become unusable, either due to a lack of trust or a long-term disruption. It is worth considering in advance whether there are backup systems for the services, to what extent and how long it would take to implement them. It is good to remember that regardless of size or position, any actor is vulnerable to cyberattacks, and threats realised through value chains may also affect global data giants.



WEAK CYBERSECURITY OF SMALL BUSINESSES

At the beginning of April, the UK published an annual report on the level of cyber security of companies in the UK. The study was produced by the Department of Science Innovation and Technology (DSIT), and its figures do not flatter companies. According to the results, only about 22% of companies in the country have a cyber incident plan. In addition, only about 20-30% of deviations were reported to the authorities, and the figure for customers or partners was even lower, only 5%. The statistics are pulled down especially by small companies, which were by far the worst in all areas.

Companies' preparedness for cyber threats and risks has also been studied elsewhere. The findings are similar: based on several sources, small businesses appear to be inadequately prepared for and resilient to cyberattacks. One of the root causes has been considered not only the naturally limited resources and competence capacity of small companies, but also the gap in safety culture in cyber security and a lack of situational awareness. Contrary to popular belief, there is a significant cyber threat towards small businesses. For example, the financial magazine Forbes reported in 2022 that small companies face relatively more cyberattacks than their large peers. For these reasons, small companies should also be able to secure their own operating environment against cyber risks. In Finland, for example, small and medium-sized enterprises account for the majority of private sector jobs and a significant part of the entire national economy.

Cyber risks for small businesses are differ from those for larger organizations. It is less likely that a threat actor will carry out a long-lasting and prepared attack on a smaller organization. Instead, threats can be automated or the result of poor security levels that expose them to "easy" attacks. For example, unsecured network infrastructure, a lagging pace of vulnerability updates and poor cyber hygiene pose threats that criminals can easily and effortlessly exploit. So, from a criminal's perspective, smaller targets can be attractive simply because they are easy to hit. For example, malware extortion may be more effective for a small organization because it may have a significantly lower chance of surviving the attack other than paying the ransom.

Evolving legislation also sets increasingly tighter requirements for the cyber security of smaller companies. For example, the NIS2 Directive extends cyber security risk management to the supply chains of organisations within its scope and thus indirectly imposes obligations on smaller operators in the chain, even if the regulation does not directly apply to them. Therefore, NIS2 and the resulting national law will serve as an excellent basis and guideline for cyber risk management for all, regardless of size and sector. The guidelines and recommendations of the authorities also provide means for smaller operators to develop and maintain a good level of cyber security within the limits of their financial capabilities. For example, acquiring entire security certificates by random can be inappropriate and an unreasonable investment. Forming a situational picture of one's own organisation and its operating environment are at the heart of everything. Increasing the awareness of management and the entire personnel and taking measures based on risk-based consideration goes a long way. These include, for example, up-to-date information security guidelines, an appropriate update rhythm of devices and systems, and good cyber hygiene. If the significance of cyber security is understood as essential for the continuity of operations, investing in it does not feel like a burden. Ensuring sufficient cyber security in advance is always cheaper than cleaning up after the risk has materialised.

AUKUS DEFENCE COOPERATION MAY EXPAND IN ASIA

Aukus defence cooperation between Australia, the United Kingdom and the United States has become topical when rumours of Japan joining the trio gained momentum at the beginning of April. The defence ministers of the Aukus countries released a joint statement in which they said that the countries were considering cooperation with Japan under the second pillar of defence cooperation. What is Aukus all about, and what significance could it have from a broader cyber security perspective?

Aukus was born in 2021, when these aforementioned countries agreed to intensify defence cooperation. Cooperation is based on two objectives, so-called pillars. The first, in many respects more concrete and important, pillar is cooperation in the field of nuclear submarine technology. The aim is to help Australia build its own nuclear submarine fleet. The second pillar, within which cooperation with Japan has now also been initiated, is so-called advanced technologies, which refers to cooperation in areas such as cyber capabilities, artificial intelligence, quantum technology and electronic warfare.

Cooperation can be viewed from several different perspectives. The United States has said it is a way of increasing cooperation with its closest strategic partners, although economic reasons certainly weigh as well, as the supply of nuclear submarines to Australia is an economically significant investment for the country. In the UK, the benefits have been calculated to come from technological cooperation, it has also been estimated by international experts, that cooperation also plays a role in building the country's post-Brexit foreign policy and position. Immediately after the announcement of the cooperation agreement, the proposal raised objections in China. Many Western estimates also thought it was one of many ways to try to limit China's growing influence in Asia and the Pacific. With Japan's involvement, talk of directing defence cooperation against China has gained even more resonance. China expressed deep concern about Japan's possible accession to Aukus cooperation.

Japan's entry to coalition would certainly make a difference. The country is known for its high-tech expertise, which is why the alliance believes that Japan can bring something new and mutually beneficial to the table. At the same time, closer defence cooperation, especially in the cyber environment, is certainly of interest to Japan as well. Despite its merits, the country has not been successful in various comparisons or indexes measuring cybersecurity. For example, in the cyber index comparison of the Estonian e-Governance Academy, the country ranks 52nd between Argentina and Peru. On the other hand, the usefulness of Western indices and comparisons, in particular, can be reduced by the language barrier – it is not always clear how well Western researchers or analysts can obtain information about a country where many things are still published only in the local language. However, Japan has taken cybersecurity into account at the national level, for example in the 2022 National Security Strategy and the National Cybersecurity Strategy published in 2021. Still, Japanese companies have faced significant cyberattacks, in many cases traces lead to countries such as China and North Korea. For example, country's largest port fell victim to a ransomware attack in July 2023, even though in that case the attacker was the well-known Russian ransomware actor LockBit. Therefore, cyber cooperation, in particular, within the framework of Aukus would certainly have something to offer Japan.

For the time being, cooperation seems to be only taking its first steps. For example, with regard to cyber security, the UK Parliament's website so far states that under Akus cyber cooperation "we are focusing our efforts on strengthening cyber capabilities, including protecting critical communications and operations system". In the field of artificial intelligence technology, Aukus has already organised joint trials, and in quantum technology, the countries have signed an agreement (The AUKUS Quantum Arrangement, AQuA) to increase investments. The development and possible expansion of Aukus cooperation should be monitored. It is still too early to say what cooperation on the cyber environment will ultimately take. Although cooperation with Japan has not yet been definitively confirmed, speculation has already raised the possibility of extending it to Canada, New Zealand and South Korea. It is probably no coincidence that the current Aukus countries, as well as Canada and New Zealand, already cooperate in areas such as Five Eyes intelligence cooperation. It would be logical to continue the tried and tested cooperation with familiar partners in other security sectors as well. At best, closer cyber defence cooperation between the countries could provide models and development paths for other countries and lead to innovations in both cyber security and artificial intelligence.

REFERENCES:

MICROSOFT AND LACKING CYBERSECURITY

https://www.cisa.gov/news-events/directives/ed-24-02-mitigating-significant-risk-nation-state-compromise-microsoft-corporate-email-system

https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf

https://www.securityweek.com/microsofts-security-chickens-have-come-home-to-roost/

https://www.securityweek.com/us-government-on-high-alert-as-russian-hackers-steal-critical-correspondence-from-microsoft/

https://www.securityweek.com/microsoft-says-russian-gov-hackers-stole-source-code-after-spying-on-executive-emails/

https://www.techtarget.com/searchsecurity/news/366577765/Cyber-Safety-Review-Board-slams-Microsoft-security-failures

https://arstechnica.com/security/2023/08/microsoft-cloud-security-blasted-for-its-culture-of-toxic-obfuscation/

WEAK CYBERSECURITY OF SMALL BUSINESSES

https://www.theregister.com/2024/04/09/uk_biz_response_to_cybercrime/

https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024#summary

https://www.huoltovarmuuskeskus.fi/files/29b11d0af56a115126ad490af444f1c4fd7885af/hvk-toimialojen-kyberkypsyyden-selvitys-2022.pdf

AUKUS DEFENCE COOPERATION MAY EXPAND IN ASIA

https://www.gov.uk/government/news/world-first-as-uk-hosts-inaugural-aukus-ai-and-autonomy-trial

https://www.gov.uk/government/publications/implementation-of-the-australia-united-kingdom-united-states-partnership-aukus-fact-sheet/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus

https://commonslibrary.parliament.uk/research-briefings/cbp-9842/

https://edition.cnn.com/2023/07/06/tech/japan-port-ransomware-attack/index.html

https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1

https://www.nisc.go.jp/eng/index.html

https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf

https://www.scmp.com/news/china/diplomacy/article/3258265/china-gravely-concerned-about-reports-japan-could-join-aukus-security-pact

https://www.defense.gov/News/Releases/Release/Article/3733790/aukus-defense-ministers-joint-statement/

https://sciencebusiness.net/news/international-news/aukus-defence-technology-pact-welcomes-japan-eu-excluded-now

Cyberwatch Weekly

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
Pixabay
Unsplash

A PASSION FOR A SAFE CYBER WORLD

Contact

Cyberwatch Oy
Nuijamiestentie 5C
00400 Helsinki Finland

aapo@cyberwatchfinland.fi
ake@cyberwatchfinland.fi
myynti@cyberwatchfinland.fi