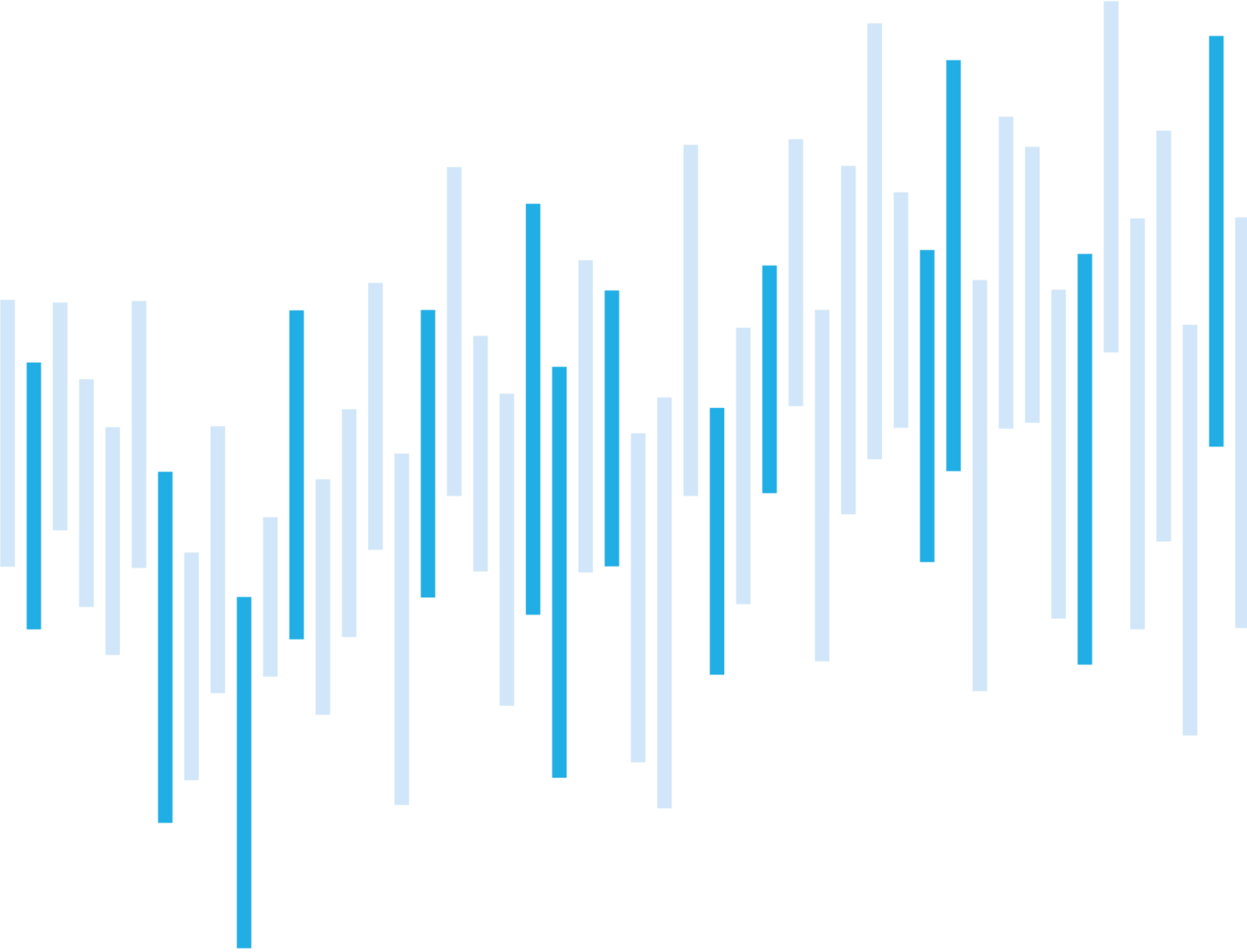
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

JULY 2024



National Cyber
and Information
Security Agency

Summary of the month

July brought a significant increase in recorded incidents, a significant number of which were caused by the CrowdStrike outage. The Czech Republic was not spared the impact of this global incident, but overall its implications in the Czech Republic were rather low. DDoS attacks were also recorded.

The total number of incidents reached 32, of which 27 were classified as less important. The remaining 5 incidents are recorded by the NÚKIB as important.

In the Focus on an event chapter, we summarize the causes and impacts of the CrowdStrike incident that was due to a faulty update of their Falcon EDR (Endpoint Detection and Response) software. This led to the so-called Blue screen of death (BSOD) on devices using Falcon EDR and Windows OS. Overall, the incident affected approximately one percent of all Windows devices, making it the largest IT outage in history with damages so far estimated in the billions of dollars.

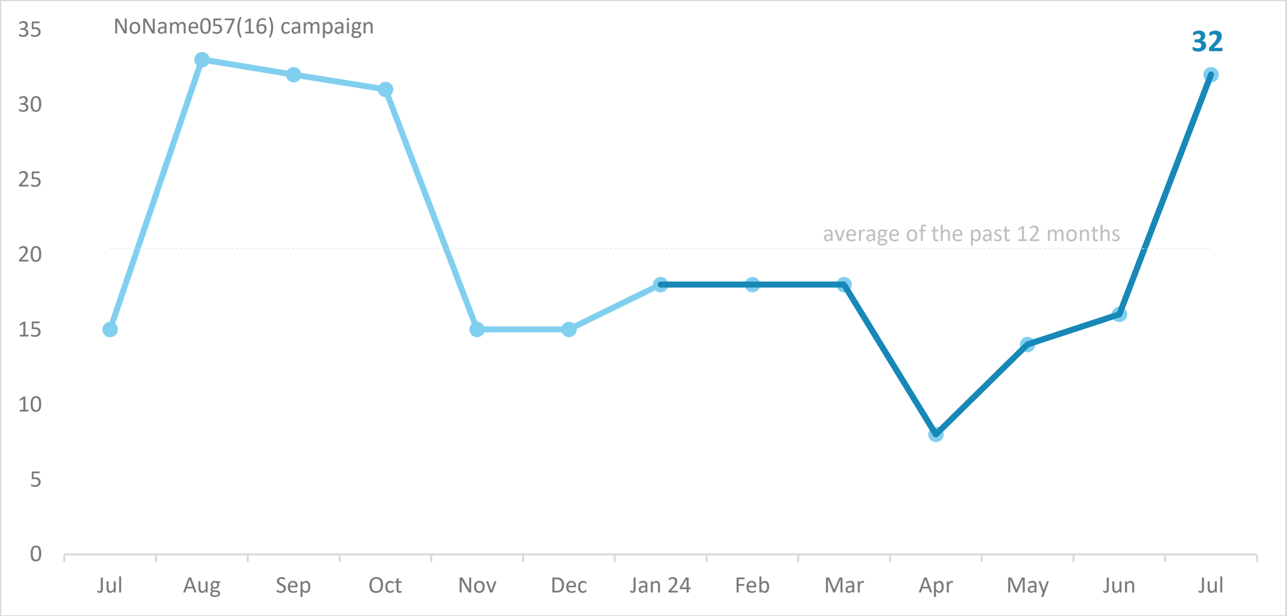
Table of content

The following report summarises the events of the month. The data, information and conclusions contained herein are primarily based on cyber incidents reported to NÚKIB. If the report contains information from open sources in some sections, the origin of this information is always stated.

You can send comments and suggestions for improving the report to the address komunikace@nukib.gov.cz.

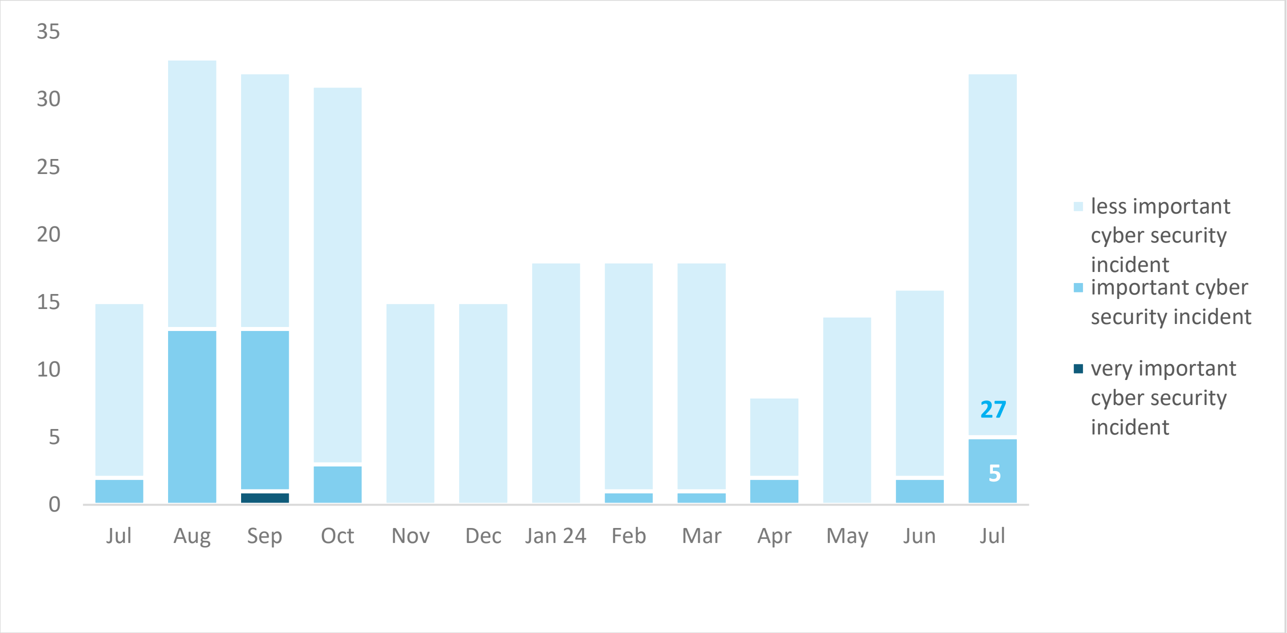
Number of cyber security incidents reported to NÚKIB

During July, NÚKIB recorded 32 incidents, which represents a significant increase compared to previous months. This is mainly due to incidents related to the outage of CrowdStrike EDR software and the continued occurrence of DDoS attacks.



Severity of the handled cyber security incidents[1]

There has also been an increase in the number of more severe incidents recorded by NÚKIB. Two of these relate to the CrowdStrike outage, while the remaining three to various other compromises, in one case involving significant financial damage as a result of successful spear-phishing.



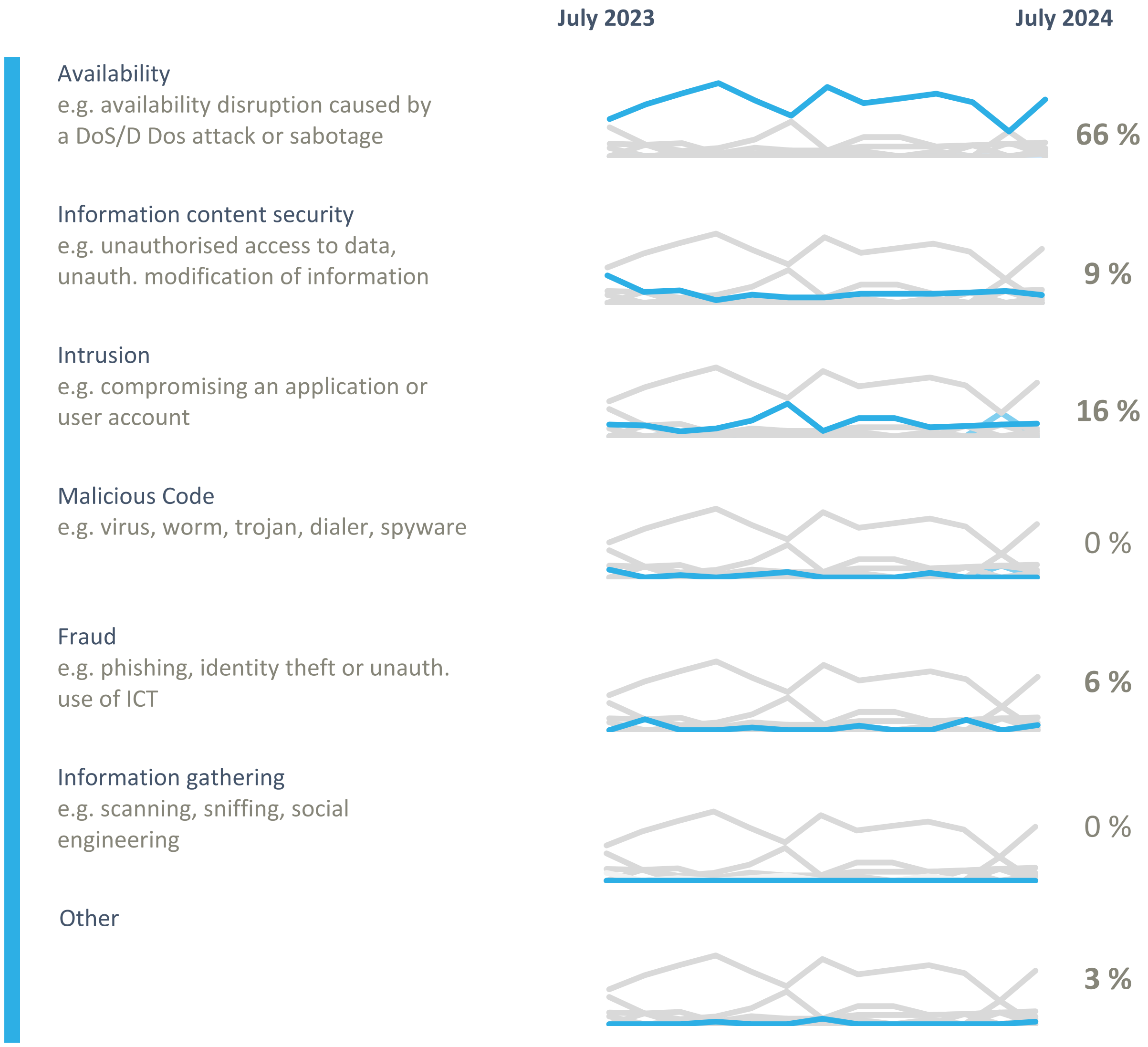
[1] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB [2]

The largest category of incidents during July is Availability, in which NÚKIB recorded ten incidents in the context of the CrowdStrike outage, ten DDoS attacks and one outage caused by a technical failure. The Russian-speaking hacktivist group NoName057(16) is responsible for four DDoS attacks.

NÚKIB also addressed incidents in these three categories:

- Five incidents fell into the category of Intrusion, four cases involved compromised email inboxes and subsequent phishing or spamming, and in the last case the system of a Czech state institution was compromised by an unknown attacker.
- In two incidents in the Fraud category, attackers used spear-phishing, in both cases successfully convincing the victim to authorise a fraudulent payment.
- Within the Information Security category, NÚKIB recorded two successful ransomware attacks using DragonForce and Qilin ransomware, and one data leak incident.



[2] The cyber incident classification is based on the ENISA taxonomy: Reference Incident Classification Taxonomy — ENISA (europa.eu)

July trends in cyber security from the NÚKIB's perspective[3]

Phishing, spear-phishing and social engineering

↗

In July, NÚKIB recorded two cases of spear-phishing. In both cases, the awareness of the attackers of the compromised organisation led to the successful authorisation of fraudulent payments by the victims.

Malware

→

In July, as in the previous months, there were continuous activities in the area of malware analysis in connection with some previously recorded incidents.

Vulnerabilities

→

During July, NÚKIB did not issue any vulnerability alerts. However, the government CERT continues to share information on current vulnerabilities on the X platform. For example, CVE-2024-37085 within WMware ESXi was disclosed to be actively exploited by ransomware gangs even after it was patched. Malicious activity by various threat actors exploiting the themes of CrowdStrike's EDR software outage was also mentioned.

Ransomware

→

In July, two ransomware related incidents were recorded. One of them was caused by the DragonForce Ransomware group, while the second incident involved the Qilin ransomware, which is offered as a service (RaaS).

Attacks on availability

↗

In July, NÚKIB recorded 10 DDoS attacks, at least four of which were carried out by the Russian-speaking hacktivist group NoName057(16). All of them targeted state and financial sector institutions.

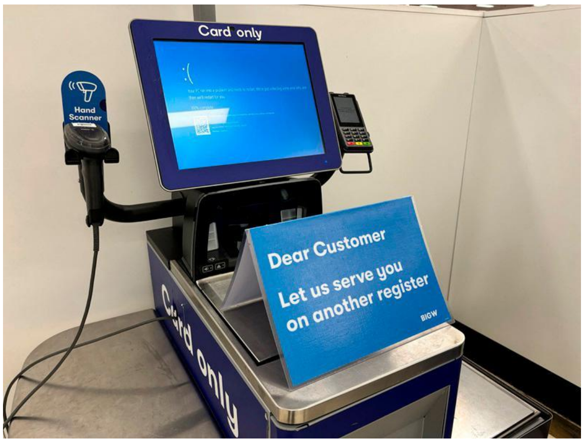
[3] The development illustrated by the arrow is evaluated in relation to the previous month.

Focus on an event Faulty update knocked millions of devices out of service around the world, but the impact in the Czech Republic was mild

On Friday, July 19th, a wide range of Microsoft Windows devices around the world were affected by a problem causing these devices to malfunction, specifically the collapse of the operating system into a so-called "blue screen of death" and subsequent inability to boot. The issue was caused by a bug in the Endpoint Detection and Response (EDR) update to the CrowdStrike Falcon platform. Within hours, CrowdStrike issued a patch and instructions that included locating and removing the problematic file. Although the fix was simple in principle, affected computers had to be manually booted in safe mode. This meant that each affected device had to be repaired individually, which significantly increased the time and the impact of the outage.

Only users of the Falcon platform running Windows OS were affected. According to Microsoft, over eight and a half million devices were affected by the outage, which is less than one percent of all Windows OS devices. **Despite that, it was the largest IT outage in history to date.** The impact of the incident has affected almost every sector, with airlines facing perhaps the most significant impact. Television stations, medical appointment systems, self-service terminals, banking services and railways were also affected. **Within the Czech Republic, NÚKIB records ten affected entities, two of which were assessed as having severe impacts.**

Figure 1: Affected self-service terminal



Source: thesun.com

Shortly after the event, the attackers began to exploit the situation for other malicious cyber activities. These included fraudulent emails or phone calls in which the fraudsters posing as CrowdStrike employees or independent researchers offering technical assistance. **The main goal of the scammers was to convince the victim to install malware that they provided under the pretext that it was a fixing tool or script to help resolve the outage or its possible effects.**

CrowdStrike has warned directly of a wave of such phishing activity, and its findings are consistent with publicly available sources and information from NÚKIB partners. According to the information available, the outage was exploited by both cybercriminal and state-sponsored actors.

Probability terms used

Probability terms and expressions of their percentage values:

Term	Probability
Almost certain	90–100 %
Highly likely	75–85 %
Likely	55–70 %
Realistic probability	40–50 %
Unlikely	20–35 %
Highly unlikely	0–15 %

Traffic Light Protocol

The information provided shall be used in accordance with the Traffic Light Protocol methodology (available at the website https://www.first.org/tlp/). The information is marked with a flag, which sets out conditions for the use of the information. The following flags are specified that indicate the nature of the information and the conditions for its use:

Colour	Conditions of use
TLP:RED	For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.
TLP:AMBER+STRICT	Restricts sharing to the organization only.
TLP:AMBER	Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP:GREEN	Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defence community.
TLP:CLEAR	Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.