TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

September 2022

#cyberweather

Cyber weather gives you an update on the key information security incidents and phenomena of the month. We want to give our readers an overview of what has happened in the field of cyber security during the past month. The situation can be:

calm worrying serious

TRAFICOM

17.10.2022

Cyber weather, September 2022

Data breaches and leaks

- In September, a few M365 breaches evolved into a wide-spread M365 phishing campaign employing a secure email theme.
- Brute force attacks trying to bypass multi-factor authentication have been observed also in Finland.

Scams and phishing

- Thousands received police-themed extortion messages in September.
- Finnish consumers have once again received scam calls from foreign numbers.

Malware and vulnerabilities

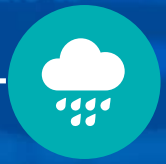
- Malware have been spread by email in September.
- A vulnerability that could allow for remote code execution discovered in Microsoft Exchange. Exploitation requires authentication.

Automation and IoT

- The EU published on 15 September 2022 a proposal for a new Cyber Resilience Act on the cyber security of smart products. The Act introduces requirements for manufacturers, retailers and importers.

Network performance

- Four major disruptions.
- The disruptions were mainly short and only had a local effect on the availability of communications services.
- Denial-of-service attacks have increased after the summer and have also had some effects.



Spying

- Russia is expected to increase its cyber espionage activities in the coming winter. Espionage may also concern information related to product development to make up for the technology deficit.
- A group associated with the Iranian government has once again targeted Albania.

TRAFICOM

13 October 2022

TOP 5 cyber threats – near future (6–24 months)

1

Economic and political phenomena are reflected in cyber security.

Digitality cuts across all activities of organisations, and changes in the international security situation have a major impact on continuity and risk management in organisations.

2

Cyber threat level in Finland has increased.

The increase in malicious traffic and the rise in the threat level make preparedness even more important in organisations.

3

Weaknesses in ordinary control measures still cause the majority of information security incidents.

For example, access rights management, keeping software up to date and good information security cultre are at the core of cyber security.

Symbols

New

Updated

4

Insufficient exchange of information leads to poorer situational awareness of cyber security.

A cyber threat encountered by one organisation today may be encountered by others tomorrow. Efficient sharing of information improves cyber security for all.

5

Cyber security depends on experts, and cyber security skills are important for all of us!

Increasingly diversified cyber security expertise is needed: there is a growing need for experts as new regulation is adopted and cyber security becomes an integral part of daily operations in businesses and organisations.

TRAFICOM

17.10.2022