TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

February 2020

#cyberweather 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

Cyber weather February 2020

Data breaches and leaks

- The number of reported Office 365 data breaches continues to increase.
- An Exchange server vulnerability that emerged in February is exploited in data breaches.

Scams and phishing

- Hundreds of thousands of phishing calls claiming to be from technical support were made to Finns.
- Phishing for Office 365 credentials continues and leads to almost daily data breaches.

Malware and vulnerabilities

- Neglecting critical updates puts the continuity of business operations at risk.
- Laptop mobile connectivity a blind spot for businesses?

Automation

- EKANS ransomware detected globally. A possible connection to MEGACORTEX ransomware previously in circulation identified.

Network performance

- A large number of DoS attacks was reported, however with no significant impacts on service functionality.
- Six significant disruptions in February.
- An extensive incident in Microsoft Teams; Microsoft forgot to renew a certificate.

Spying

- The standard of log management is usually not sufficiently high for investigating data breaches.

Top 5 cyber threats - significant longer-term phenomena

1

Vulnerabilities are exploited more rapidly, necessitating speedy updates. Devices and services whose information security has not been addressed and whose security measures and maintenance are inadequate are left connected to the network.

2

Phishing is very common, and detecting the fraud may be difficult for the phishing message recipient. This is also exploited in targeted attacks and spying.

3

Ransomware attacks with extensive impacts put business continuity at risk. The damage caused has amounted to tens of millions of euros in individual cases.

4

Unclear division of responsibilities between the service provider, subcontractors and customer undermines information security management. Shortcomings in log monitoring make detecting threats difficult.

5

Organisations are unable to manage their cyber risks. Risks are underestimated as organisations are unable to anticipate the impacts of the threats on their operations. Shortcomings in recovery plans.