TLP:GREEN

Emerging Cyber Threat Landscape Healthcare: which incidents must be reported?

COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

ZCERT

My name is

Wim Hafkamp

HTTPS//www.linkedin.com/in/wimhafkamp/

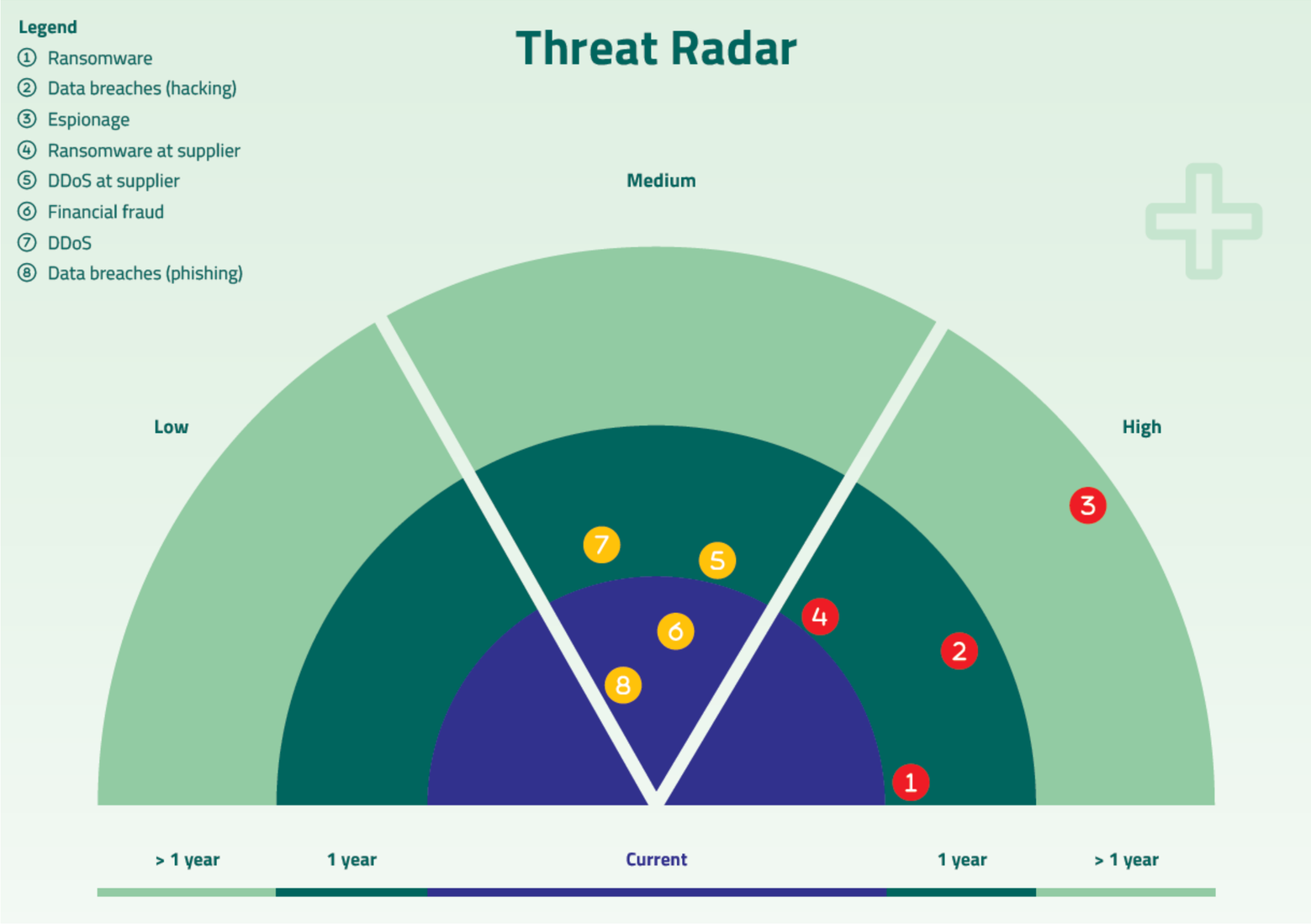
- Managing Director Z-CERT
- Chair EH-ISAC

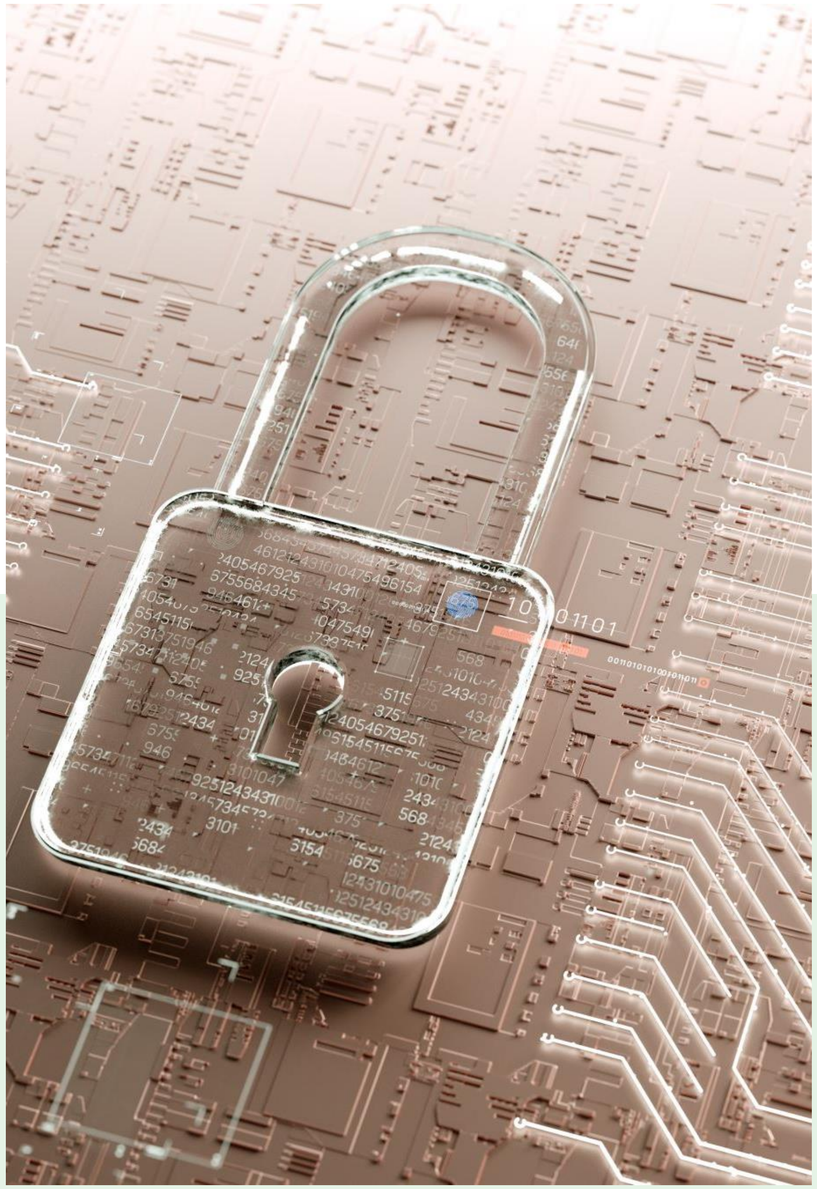
Our mission

Dutch Healthcare digitally secure

Content

Cybersecurity Threat Landscape for the Healthcare sector 2023



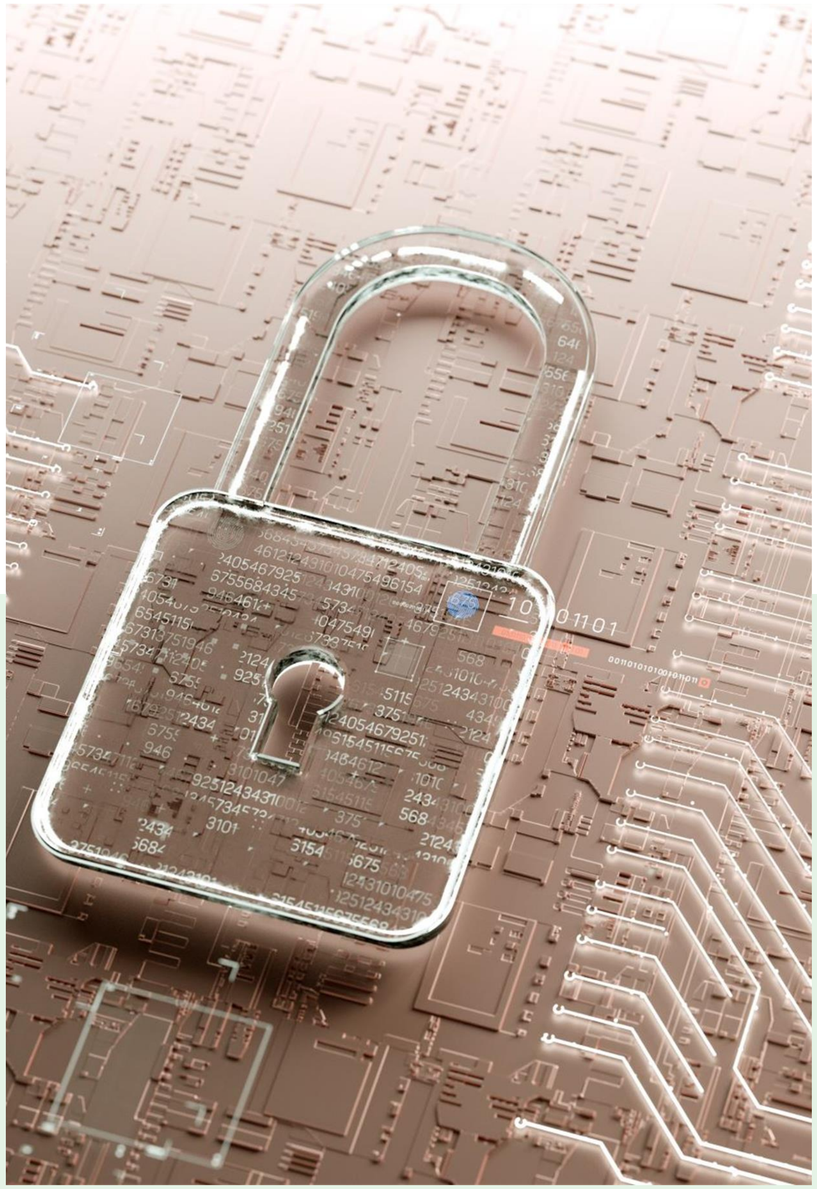


Ransomware

Threat level: **High**

Ransomware sector is evolving

New techniques leave the healthcare sector more vulnerable



Ransomware *at suppliers*

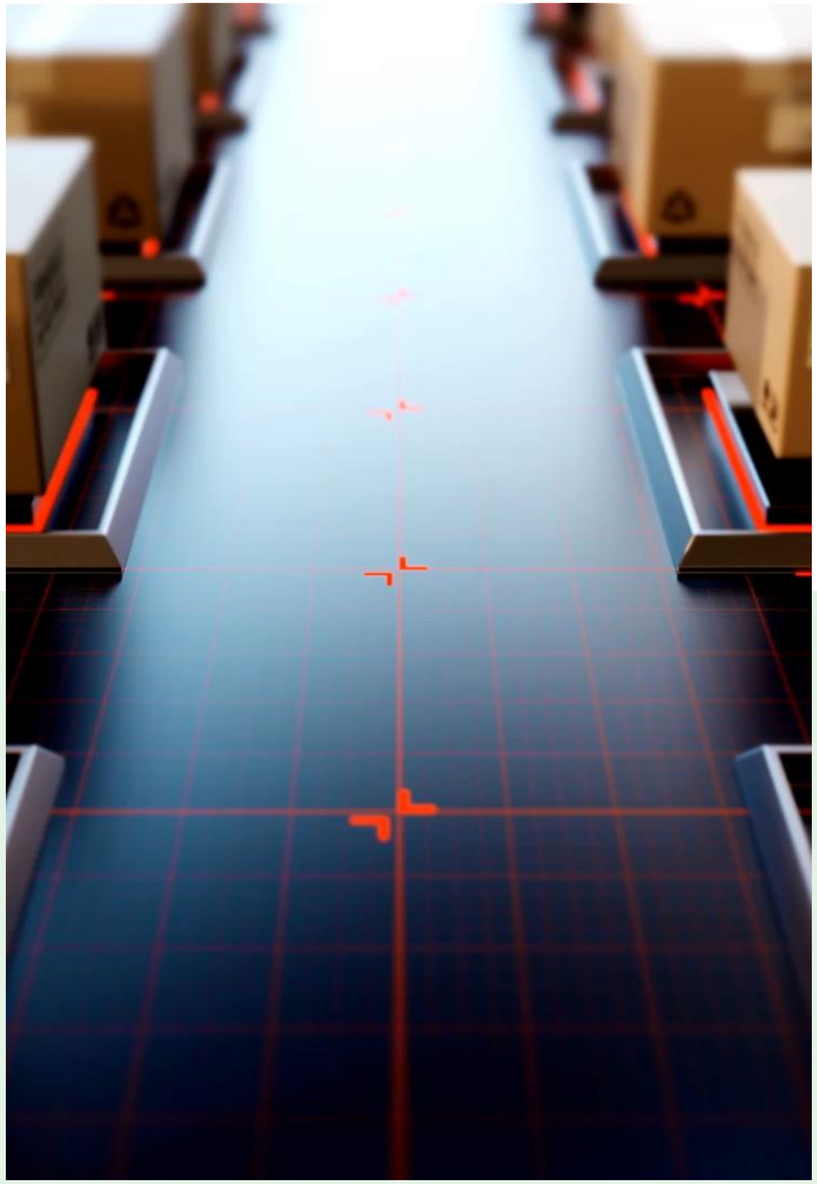
Threat level: **High**

More ransomware attacks on IT service providers

Healthcare sector impacted when making use of these providers

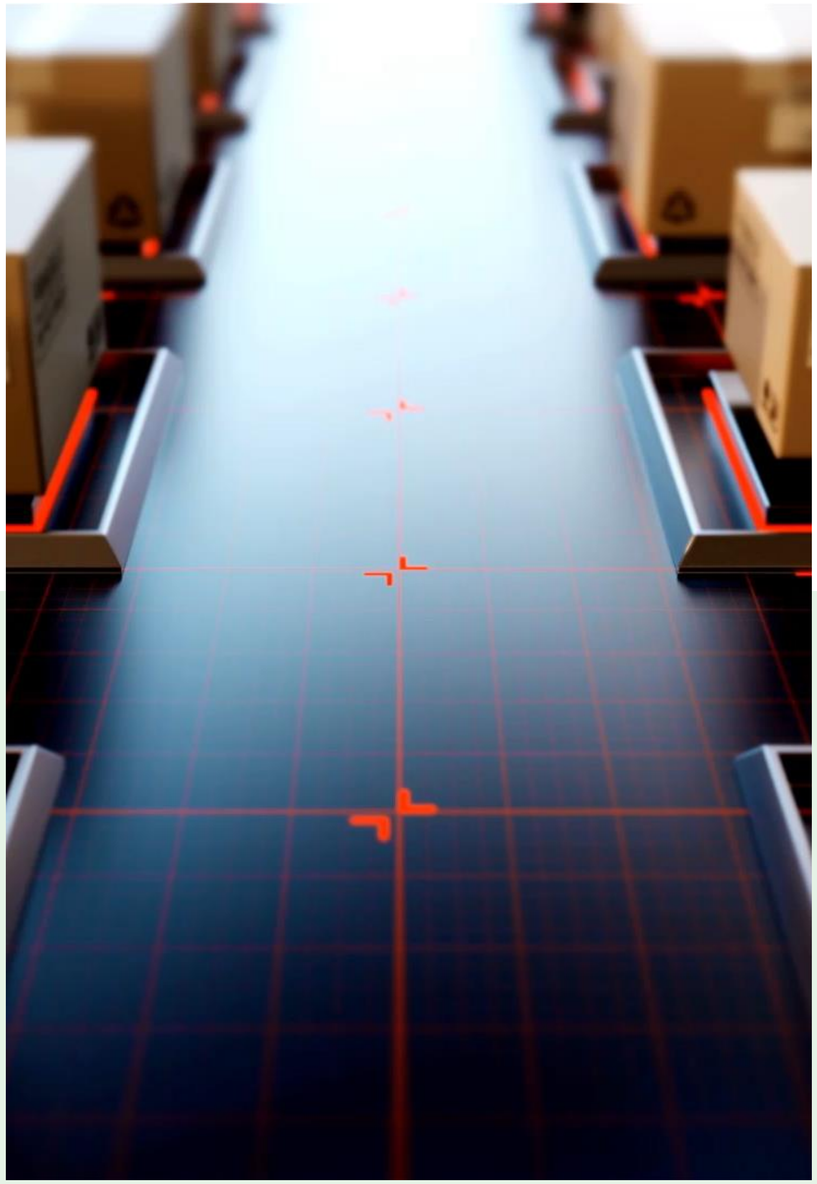
Databreaches

- Threat level: **Medium to High**
- Risk of data leaks due to misconfigurations and improper decommissioning of (medical) equipment
- Phishing attacks now include MFA bypass



DDoS

- Threat level: **Low to Medium**
- Threat dependent on geopolitical developments
- Attacks not sophisticated but nonetheless disrupting

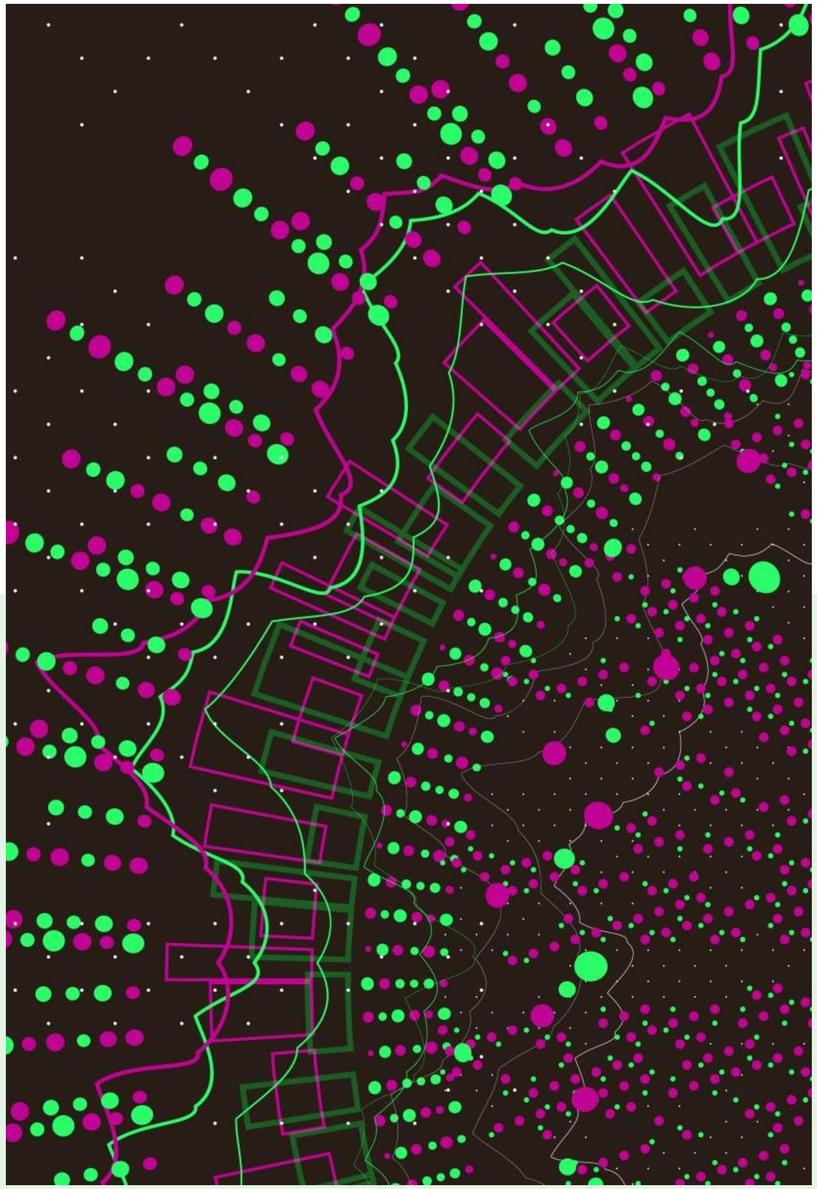


DDoS *at suppliers*

Threat level: **Medium**

Impact highly dependent on the delivered service

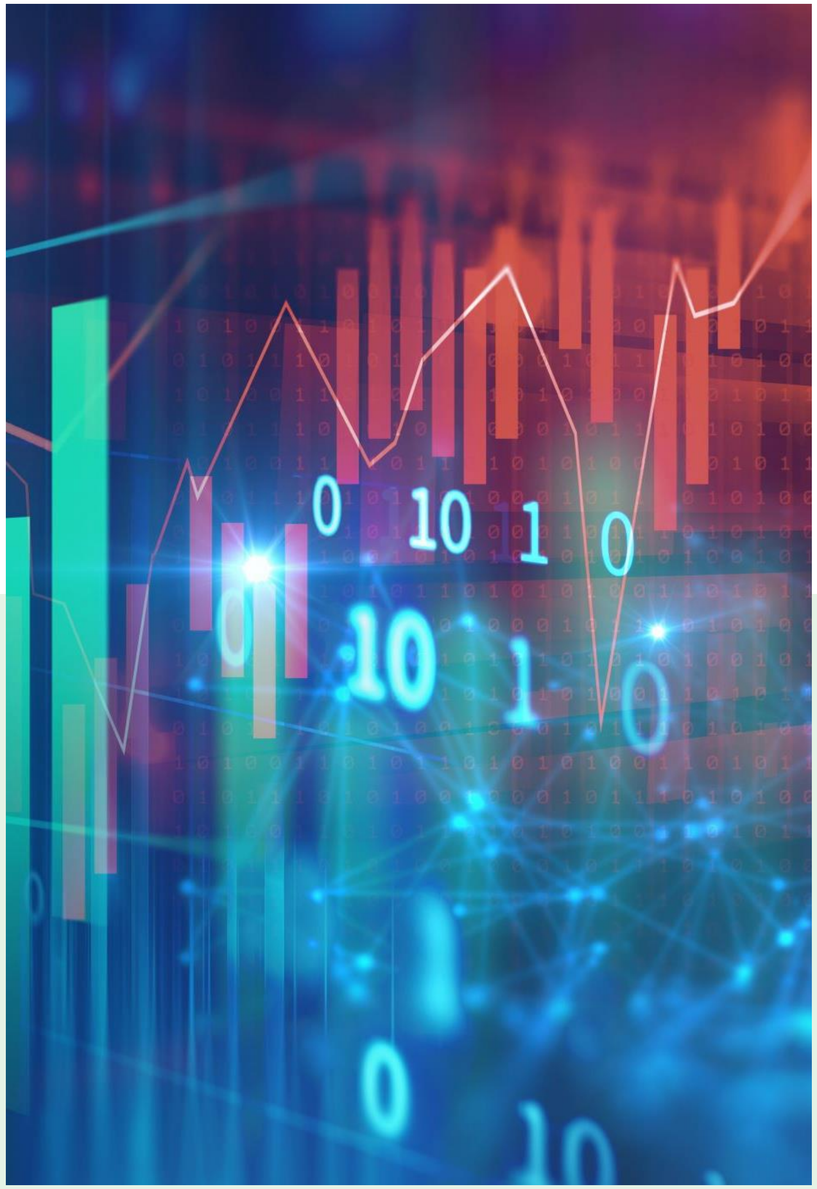
Absence of DDoS mitigations at suppliers a risk



Cyber espionage by state actors

Threat level: **Low to High**

Threat dependent on healthcare institutions level of research



Digital financial fraud

Threat level: **Medium**

Frequent occurrence

Often easily countered by a rigid financial process

NIS2

NIS2 Article 23

3. An incident shall be considered to be significant if:

(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;

(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

Questions:

What does '**is capabable of causing**' mean?

What does '**severe operational disruption**' mean?

Work in progress:

Dutch ministries – in close cooperation with the Dutch National CSIRT and sectoral CSIRTs - develop the current draft regulation in further details.

Disclaimer

- The proposal is an early draft and subject to change
- Uncertain if incident notification thresholds will be sectoral

Possible threshold values for incident notification

Goals:

1. Has a preventive effect due to lessons learned and the findings and reports from, amongst others, the competent authority
2. Create a representative image of the amount and type of incidents
3. No disproportional administrative burden for entities

Possible threshold values for incident notification*

Continuity

- More than 5% of patients / clients can’t receive or can only partially receive:
    - Planned care
    - Intensive care
- More than 5% of personnel within the primary care process can’t work, or only partially
- More than 5% of the institution's revenue is at stake due to continuity impact
- More than 8 hours of continuity impact of services not related to the previous points

* Source = WS3 NIS Incident Reporting: Guidelines for notification criteria for important and essential entities

Possible threshold values for incident notification

Integrity, confidentiality and authenticity

- Incidents with a malicious activity at its root leading to impact on integrity, confidentiality or authenticity of patient- or client data
- Incidents with impact on integrity of confidentiality of data of multiple personnel

Possible threshold values for incident notification

Social impact and media attention

- Incidents that could get national attention in the media

Possible threshold values for incident notification

Malicious activities

- Ransomware/wiperware
- Supply chain attacks
- Known vulnerability exploitation
- Data breach on databases containing sensitive information
- Compromise of ICT systems and software in isolated networks
- Compromise of user with administrator rights in critical components of the ICT infrastructure
- Data exfiltration from the network
- Identification of APT related IoC or other malware with disruptive or destructive capability in critical assets.
- Large-scale DDoS attack
- Identification of unauthorized users on critical assets (information systems, network equipment)
- Highly elaborated spearphishing campaigns

Possible threshold values for incident notification

Destructive activities

- Incidents resulting in/stemming from malicious or accidental destruction of physical/digital assets that support the essential services of an essential or important entity
- Incidents where natural or legal person(s) harmed (injury and/or death, and/or material damage, and/or non-material damage) during incident or as a result of the incidents

Possible threshold values for incident notification

Healthcare sector specific criteria

- Indications of compromise of:
  - Medical hard- and software
  - Tracking systems of patients/clients
  - Linking- and exchange systems of medical information
- Incidents during which medical information is unlawfully modified, stolen or deleted
- More than 2 hours of unavailability of important or critical medical systems

Questions?

Stichting Z-CERT

www.z-cert.nl