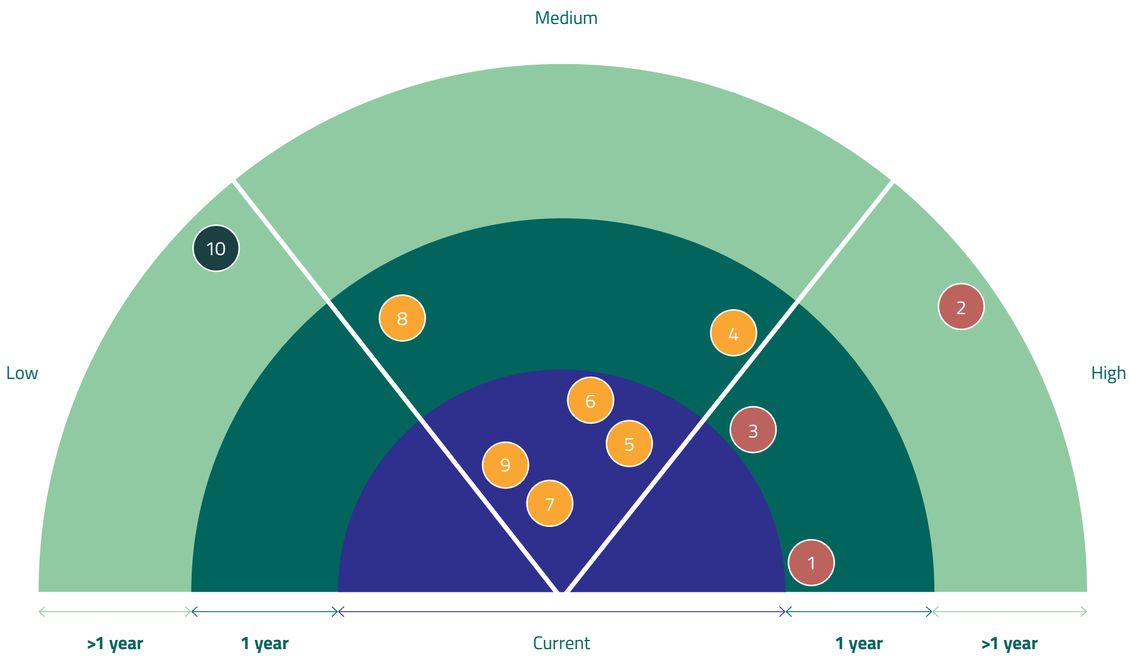
Threat Landscape 2024



Threat radar

The threat radar represents the timing, impact, and therefore the severity of the threat to healthcare. The position of the various dots in the inner circle, middle circle, or outer circle indicates when something is expected to become a threat.

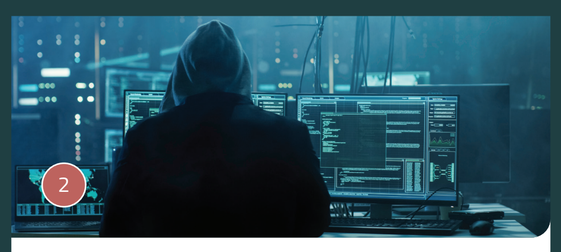
Colour	Impact
	High
	Medium
	Low

At present | Short term <1 year | Long term >1 year

Threats – Trends and insights

Ransomware and data leak extortion

This threat has slightly increased compared to 2023. Strikingly, every healthcare institution, regardless of type and size, is a potential target. Moreover, the theft of (personal) data is becoming increasingly important.



Espionage at research institutions

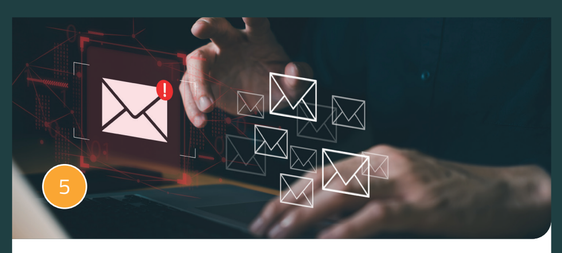
Governments use digital espionage to obtain valuable knowledge and information for their own political and economic interests. In some cases actors also deploy ransomware either as a distraction or for personal gain.

Ransomware attack on supplier

A significant number of suppliers to European healthcare organisations have been affected. Ransomware has disrupted processes, and caused databreaches. However, the impact in the Netherlands in 2024 remains limited.

DDoS attack on supplier

Various sectors supplying to healthcare were targeted, such as telecom- & service providers, and information technology & services. As a result, some digital services were unavailable or had reduced availability for a period of time. This included certain Microsoft services and an EHR solution.



Credential phishing

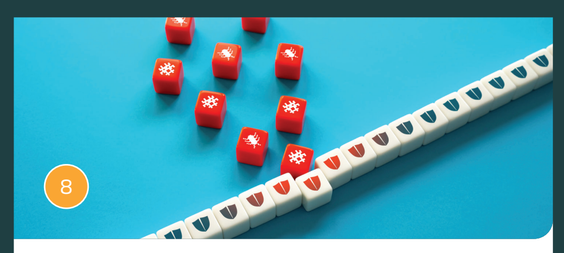
MFA is important but not a guarantee. New phishing techniques are capable of bypassing some MFA methods, allowing malicious actors to gain access to email inboxes and other platforms linked to these login credentials.

Malware

In many cases, the impact of malware incidents is limited, and the infection is fixed quickly. However, some healthcare institutions have been found to have malware used by ransomware actors. Cybercriminals are increasingly using infostealers to steal passwords or to continue an attack.

Insider threats

The frequency varies greatly depending on the type of insider threat. Unintentional data breaches occur regularly. Notable incidents this year involved former employees or contractors who stole data or threatened to do so.



DDoS

In 2024, the Dutch healthcare sector experienced fewer DDoS attacks than in 2023. Geopolitical developments didn't result in an increase in the number of incidents.

Financial fraud

The impact of financial fraud was limited in 2024. In some cases, this led to financial damage. At one hospital and one primary care organisation, it resulted in salary payments being made to the 'wrong' bank account.

Espionage at healthcare providers

Countries with an offensive cyber programme are primarily interested in stealing scientific research. Therefore, it is unlikely that healthcare institutions without such research activities will become a target.

Stay one step ahead with the Z-CERT Threat Landscape 2024

In this Cybersecurity Threat Landscape for healthcare, we provide insight into the current state of cybersecurity in the sector. We outline the lessons learned over the past year and offer tips and guidelines that can help create a more digitally secure healthcare sector.

Download at **english.Z-CERT.nl/threatlandscape2024**

The **English** version will be available from **March 5, 2025**

The Dutch healthcare digitally secure