TLP:WHITE

Zicht op cyberrisico's

COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

DIGIVAARDIG
IN DE ZORG

Mijn naam is

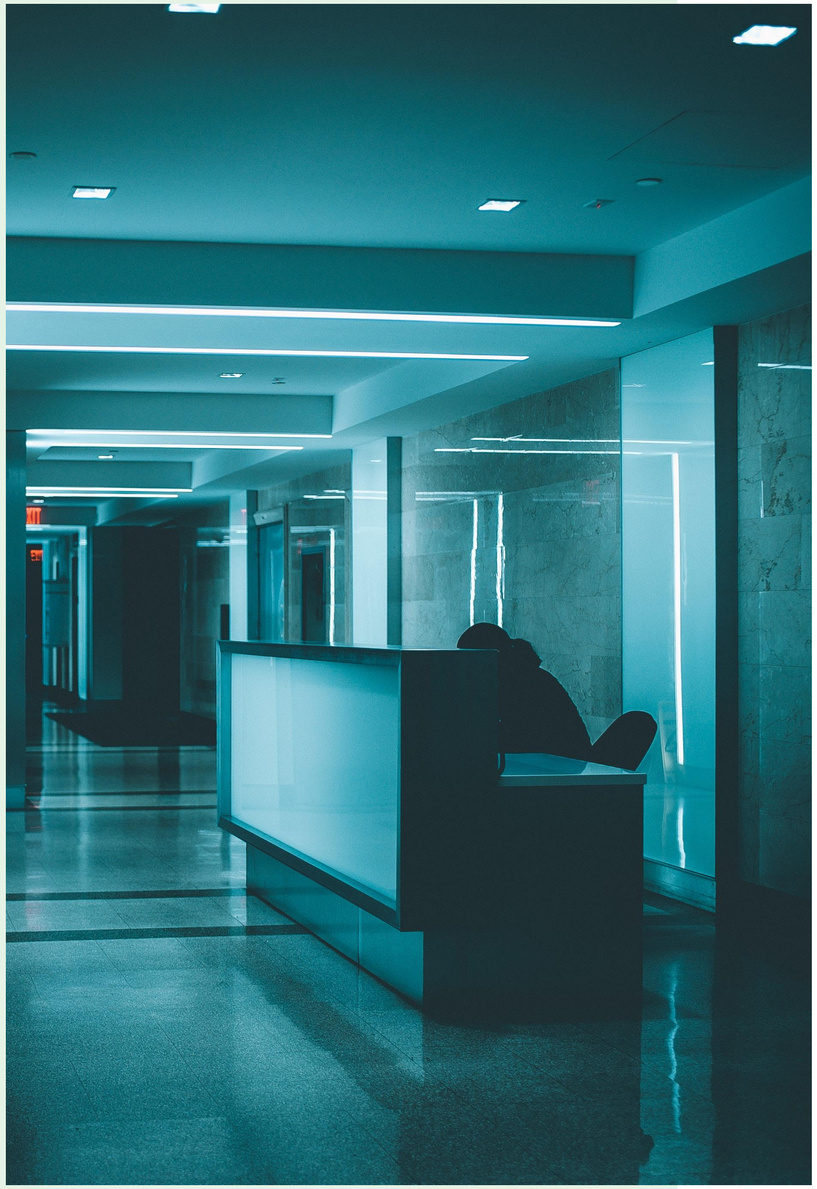
Rik Sentveld

Ik ben werkzaam als Senior Cybersecurity Support Specialist bij Z-CERT. Hiervoor was ik 24 jaar werkzaam bij het Ministerie van Defensie waarvan de laatste 5 jaar als cybersecurityspecialist en docent bij het Cyber Warfare & Training Centre. Mijn kennis van cybersecurity, social engineering, OSINT en gedragsanalyse gebruik ik tegenwoordig om de zorgsector te beveiligen.

Introductie

- Webinar wordt opgenomen
    - Zet uw webcam uit indien u niet in beeld wilt komen

- Ruimte voor vragen op het einde



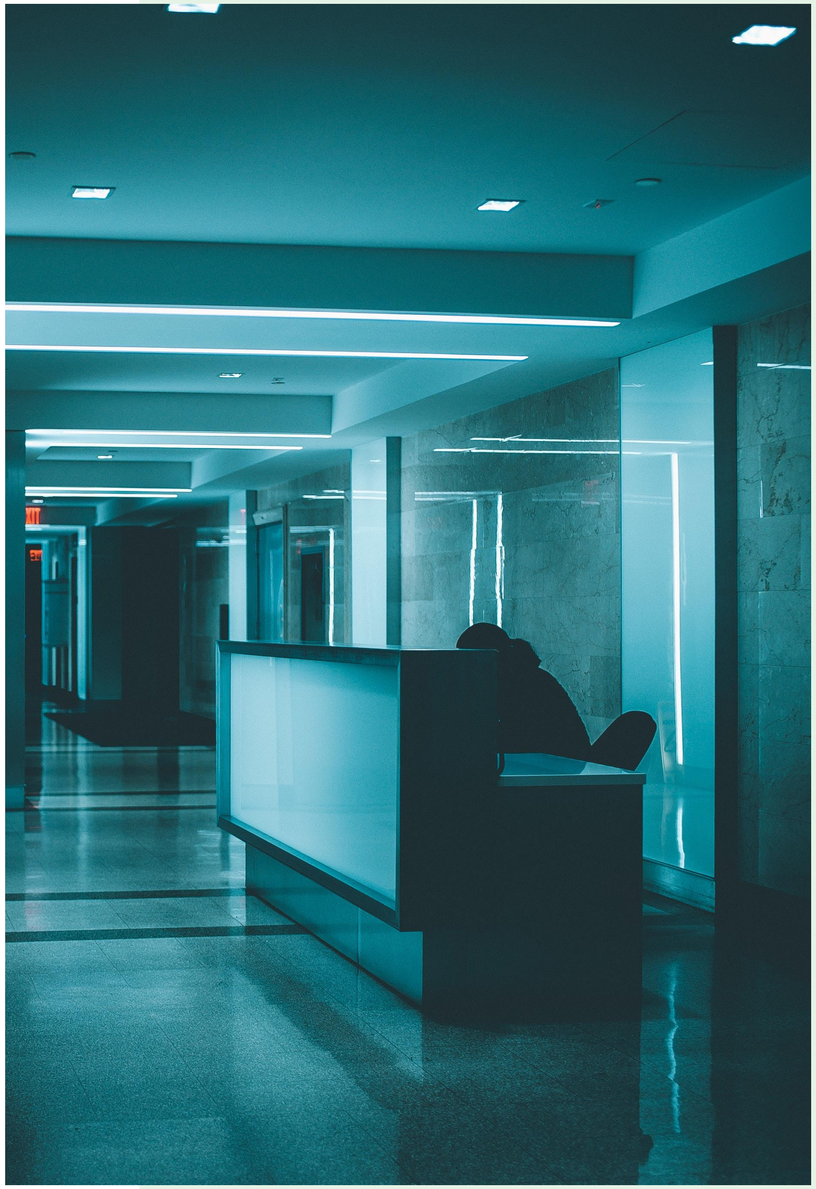
Wat we vanmiddag gaan bespreken

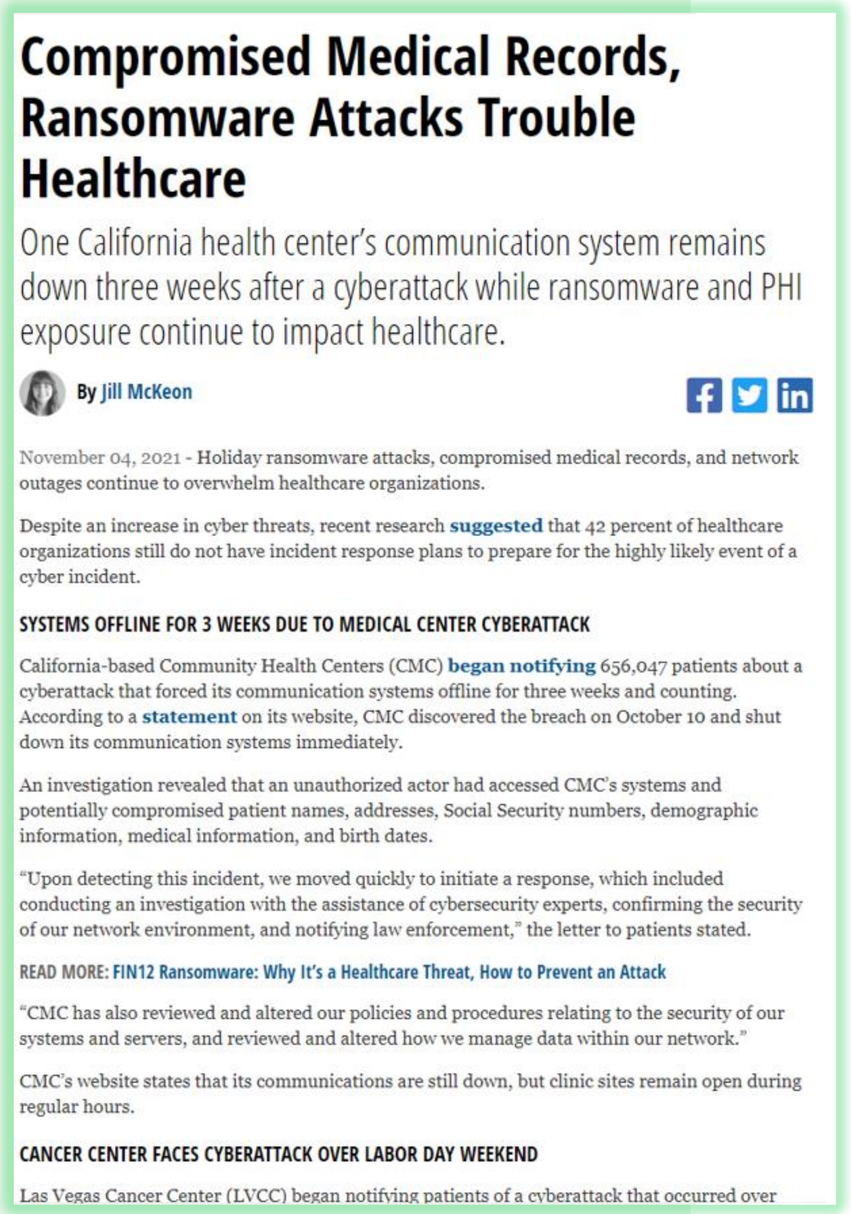
- Cyberrisico’s, wat zijn het?
- Wat kun je er tegen doen?
- Wat brengt de toekomst?
- Q&A

Cyberrisico’s:

De “big three”:

1. Ransomware
2. Datalekken
3. Fraude





Compromised Medical Records, Ransomware Attacks Trouble Healthcare

One California health center's communication system remains down three weeks after a cyberattack while ransomware and PHI exposure continue to impact healthcare.

By Jill McKeon

November 04, 2021 - Holiday ransomware attacks, compromised medical records, and network outages continue to overwhelm healthcare organizations.

Despite an increase in cyber threats, recent research **suggested** that 42 percent of healthcare organizations still do not have incident response plans to prepare for the highly likely event of a cyber incident.

SYSTEMS OFFLINE FOR 3 WEEKS DUE TO MEDICAL CENTER CYBERATTACK

California-based Community Health Centers (CMC) **began notifying** 656,047 patients about a cyberattack that forced its communication systems offline for three weeks and counting. According to a **statement** on its website, CMC discovered the breach on October 10 and shut down its communication systems immediately.

An investigation revealed that an unauthorized actor had accessed CMC's systems and potentially compromised patient names, addresses, Social Security numbers, demographic information, medical information, and birth dates.

"Upon detecting this incident, we moved quickly to initiate a response, which included conducting an investigation with the assistance of cybersecurity experts, confirming the security of our network environment, and notifying law enforcement," the letter to patients stated.

READ MORE: FIN12 Ransomware: Why It's a Healthcare Threat, How to Prevent an Attack

"CMC has also reviewed and altered our policies and procedures relating to the security of our systems and servers, and reviewed and altered how we manage data within our network."

CMC's website states that its communications are still down, but clinic sites remain open during regular hours.

CANCER CENTER FACES CYBERATTACK OVER LABOR DAY WEEKEND

Las Vegas Cancer Center (LVCC) began notifying patients of a cyberattack that occurred over

Cyberrisico: Ransomware

'De incidenten leidden tot datalekken, vertragingen in leveringen, stagnatie van onderhoud, maar ook ernstige verstoringen van operationele processen'

- De **grootste** digitale dreiging in de zorgsector;
- Aanzienlijke **stijging** in 2021;
- Veel incidenten bij **leveranciers.**

Cyberrisico: Datalekken

- Vaak veroorzaakt door **menselijk handelen**;
- Snel **grote hoeveelheden** (patiënt)data;
- Grote (maatschappelijke) **impact.**

'Shocking' hack of psychotherapy records in Finland affects thousands

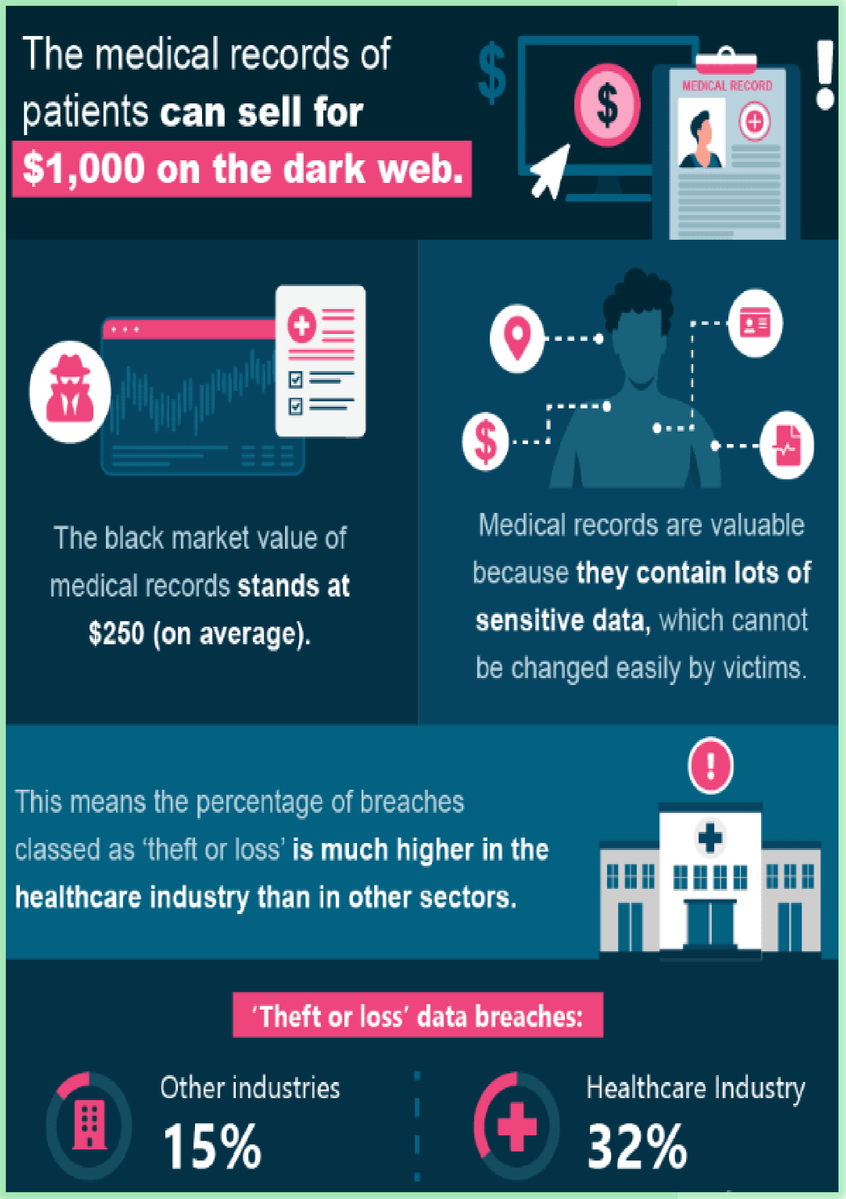
Distressed patients flood support services after hack of private firm Vastaamo

Vastaamo patients reported receiving emails with demands for €200 to prevent the documents' publication. Photograph: Kimmo Brandt/EPA

The confidential treatment records of tens of thousands of psychotherapy patients in Finland have been hacked and some leaked online, in what the interior minister described as "a shocking act".

Distressed patients flooded victim support services over the weekend as Finnish police revealed that hackers had accessed records belonging to the private company Vastaamo, which runs 25 therapy centres across Finland. Thousands have reportedly filed police complaints over the breach.

Many patients reported receiving emails with a demand for €200 (£181) in bitcoin to prevent the contents of their discussions with therapists being made public.



Infographic: safetydetectives.com

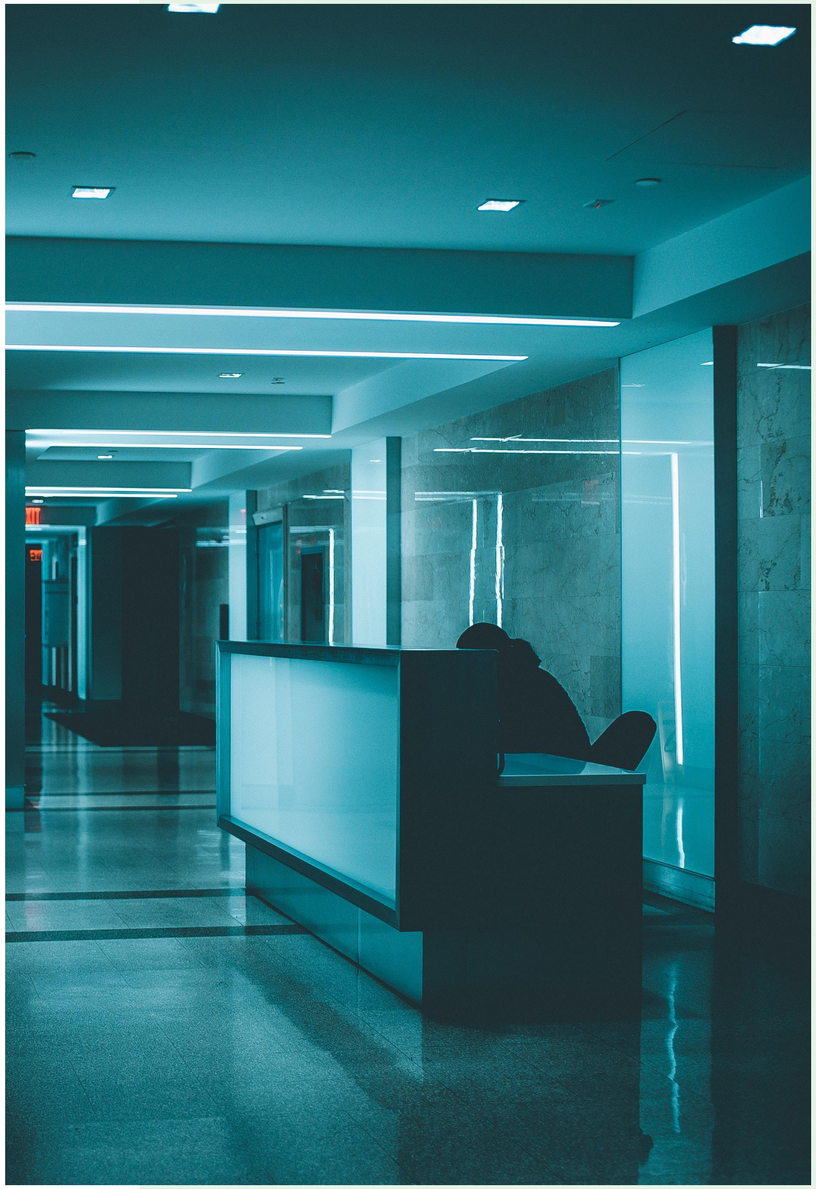
Cyberrisico: Fraude

- Diefstal van **wachtwoorden** door phishing;
- **Financiële** fraude;
- **Reputatieschade**, publiek vertrouwen.

'Omdat het hier om communicatie gaat zonder kwaadaardige software of malafide formulieren, worden deze pogingen minder vaak onderschept en is security awareness training op dit onderwerp zeer belangrijk.

Wat kun je er tegen doen?

- Basismaatregelen op orde
  (zie b.v. Z-CERT wegwijzer, gids NCSC);
- Voorbereiden op mogelijke incidenten;
- Afstemmen met leveranciers en IT-providers.



Wat brengt de toekomst?

- Meer phishing incidenten;
- Meer ransomware vanuit (cyber)criminelen;
- Mogelijk meer incidenten bij leveranciers.

Tijd voor wat vragen...

Q&A

DIGIVAARDIG
IN DE ZORG

Stichting Z-CERT

www.z-cert.nl