Casus ransomware: Ziekenhuis

18 juni 2024

CYBER RADIANT

SECURITY IS A MATTER OF PERSPECTIVE

Hospitals targeted by LockBit ransomware attack in Germany

SC Staff December 28, 2023

BleepingComputer reports that emergency care operations at three hospitals across Germany were confirmed by the Katholische Hospitalvereinigung Ostwestfalen hospital network to have been disrupted following a LockBit ransomware attack against the hospitals' IT infrastructure on Christmas Eve morning.

Romanian hospital ransomware crisis attributed to third-party breach

Emergency impacting more than 100 facilities appears to be caused by incident at software provider

Connor Jones

Wed 14 Feb 2024 // 15:48 UTC

The Romanian national cybersecurity agency (DNSC) has pinned the outbreak of ransomware cases across the country's hospitals to an incident at a service provider.

Britse ziekenhuizen verzetten 800 operaties wegens ransomware-aanval

zaterdag 15 juni 2024, 09:56 door **Redactie**, 0 **reacties**

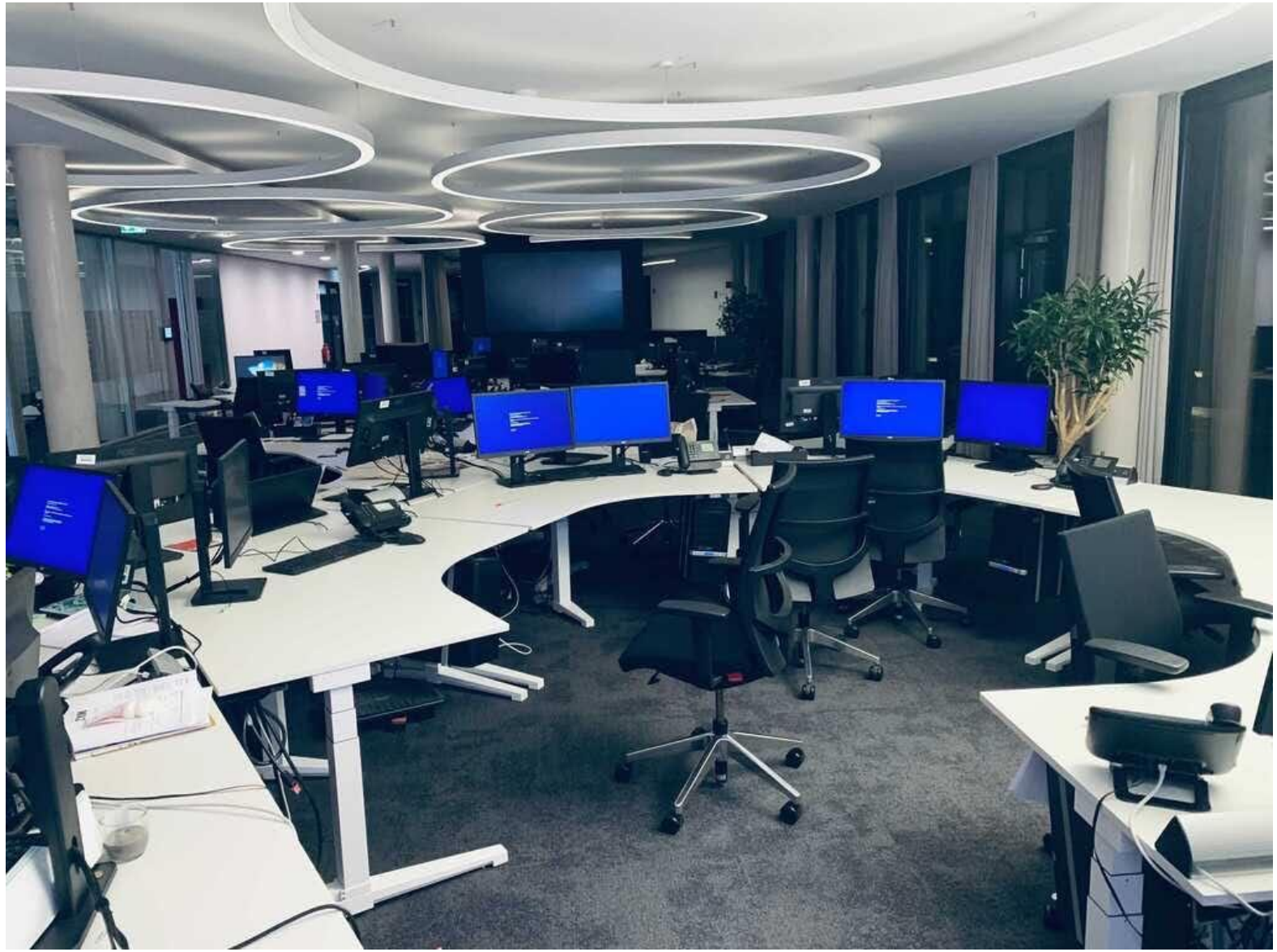
Twee ziekenhuizen in Londen hebben wegens een **ransomware-aanval** achthonderd operaties en zevenhonderd poliklinische behandelingen moeten verzetten. Dat heeft de Britse gezondheidszorg NHS **bekendgemaakt**. De aanval vond plaats tegen Synnovis, een laboratorium dat bloedtests voor ziekenhuizen en zorgorganisaties in Londen verwerkt.

Casus

~ 1.000 medewerkers

Europees ziekenhuis

Corona-periode



Hello!
We warned you, but you even didn't replied

Forced shutdown of devices can lead to the loss of all data. Do not forcibly disconnect storage volumes from hosts,
don't interrupt process. Damaged information cannot be recovered.
All data is properly protected against unauthorized access by steady encryption technology.
Contact us by following emails.

xxxxx@mailfence.com
xxxxx@onionmail.org
It's just a business.
We can help you to quickly recover all your files.
We will explain what kind of vulnerability was used to hack your network.

If you will not cooperate with us, you will never know how your network was compromised. We guarantee this will happen again.
Register new email account at secure mail service like mailfence, protonmail to be sure that outgoing email not blocked by spam filter.
Don't use gmail!
WARNING!

Don't report to police. They will suspend financial activity of company and negotiation process.

Wat was er aan de hand?

70% van de systemen versleuteld

Geen data gestolen

Hoe is de impact beperkt?

Netwerkverbindingen dichtgezet

Communicatie naar buiten niet mogelijk

Hoe is er hersteld?

Contact met criminelen

Back-ups beschikbaar

Systemen herstellen

Nieuwe wachtwoorden

De impact

En toen werd er een patiënt binnengebracht op de spoedeisende hulp..

De impact

Systemen herstellen dat doe je maar als hier geen patiënten meer zijn..

De impact

De onmacht bij de directie..

De impact

De IT-afdeling: zes maanden later..

Overzicht tips

1. Stel een stappenplan voor incidenten op en wees voorbereid
2. Bepaal je belangrijkste bedrijfsprocessen en waar mogelijk manuele procedures
3. Zorg dat relevante documentatie voor herstel, zoals netwerktekeningen en contactgegevens, beschikbaar is als systemen onbereikbaar zijn
4. Bepaal vooraf de kaders ten aanzien van contact met en betaling aan cybercriminelen
5. Stel vooraf een communicatieplan en -templates op
6. Zorg ervoor dat systeemlogging beschikbaar is
7. Zorg voor mentale ondersteuning waar nodig
8. Zorg voor voldoende ontspanning en gezond eten en drinken
9. Weet welke (externe) expertise in te schakelen in het geval van een security-incident
10. Weet of je een cyberverzekering hebt en wanneer en hoe je deze kan inschakelen
11. Test de back-ups periodiek: herstel en toegang

Bedankt voor je aanwezigheid

Lisa de Wilde
lisa@cyberradiant.nl

Lucinda Sterk
lucinda@lucindasterk.nl

CYBER RADIANT

SECURITY IS A MATTER OF PERSPECTIVE

Achtergrond

Methodiek

IN	THROUGH	OUT
Hoe de cybercriminelen initiële toegang tot de organisatie verschaffen	Hoe de cybercriminelen de kansen op een succesvolle aanval vergroten	Hoe de cybercriminelen hun doelen bereiken en schade aanrichten

Wat ging eraan vooraf - ransomware

IN

Phishing verspreiden

Malware verspreiden

Wachtwoorden misbruiken

Kwetsbaarheden misbruiken

THROUGH

Omgeving verkennen

Rechten verhogen

OUT

Back-up vernietigen

Data exfiltreren

Systemen versleutelen

Betaling ontvangen