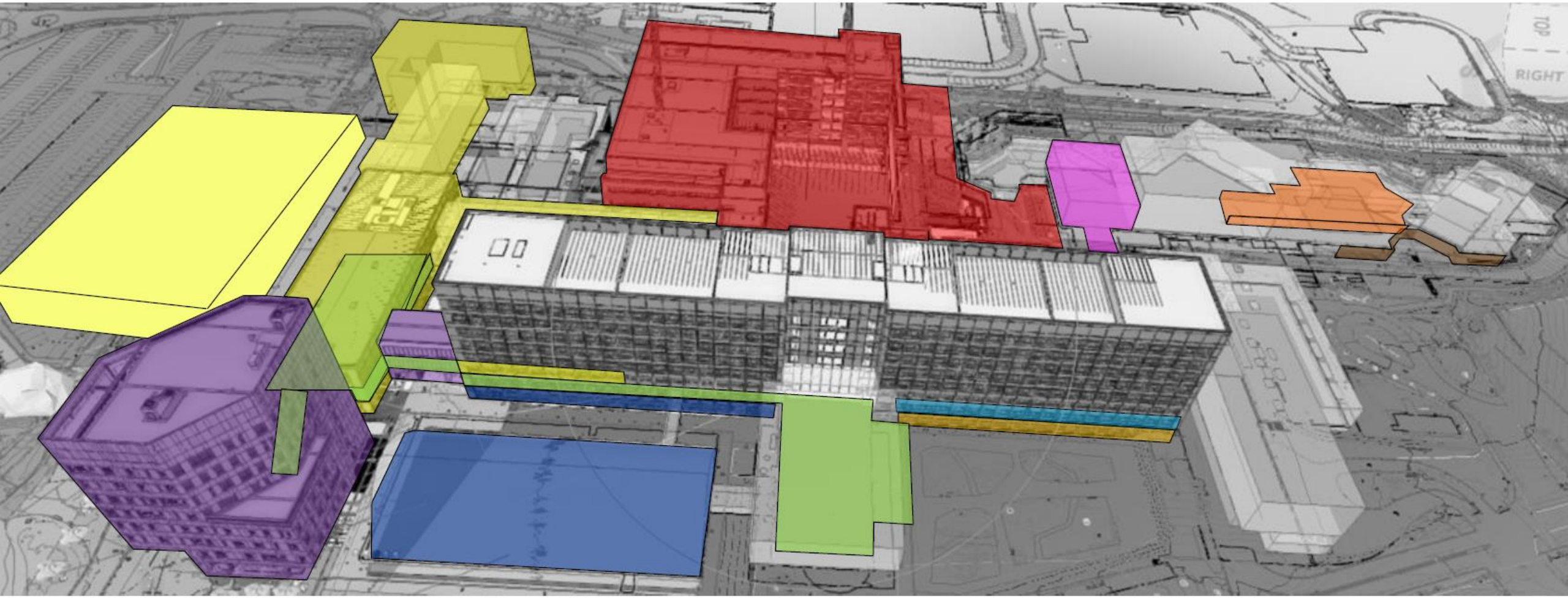
Uitdagingen op het vlak van DATA-beveiliging

Robin Demesmaeker – CIO

UZ Brussel


Centrum voor
Reproductieve Geneeskunde
www.brusselsivf.be
Universitair
Ziekenhuis
Brussel
University hospital
4000 employees
360.000 consultations
721 beds
30.000 admissions /year

Ruimteplan UZB / Projecten 2019 -2031



REORGANISATIE EN AUTOMATISATIE LABO's	2019 – 2022 10 fasen	CRG	2019 – 2025 6 fasen
MTB (incl. tijdelijke apotheek en mortuarium)	2019 – 2029 5 fasen	KEUKEN	nog te bepalen
LANDMARK	2021 – 2024 2 fasen	PICU	2024 – 2025 1 fase
INSCHRIJVINGEN/ZORGBOULEVARD/NUGE/CATERING-WINTERTUIN	2022 – 2029 4 fasen	ENDO-GASTRO	2021 – 2025 2 fasen
KLEEDKAMERS 2	2024 – 2025 1 fase	POLI 2.0 2	2026 – 2031 4 fasen

MEDISCH TECHNISCH

- 14 OK zalen
- ICU / PACU / PICU
- Medische beeldvorming
- Radiotherapie
- Oncologie
- Dialyse

Primuz - electronisch patiëntendossier (EPD)

AZ SINT-ELISABETH ZOTTEGEM

AZ MONICA

Welkom op de website van het
H.-Hartziekenhuis Lier

AZ JAN PALFIJN
GENT

Universitair
Ziekenhuis
Brussel

az Rivierenland

Clinique St Pierre
OTTIGNIES

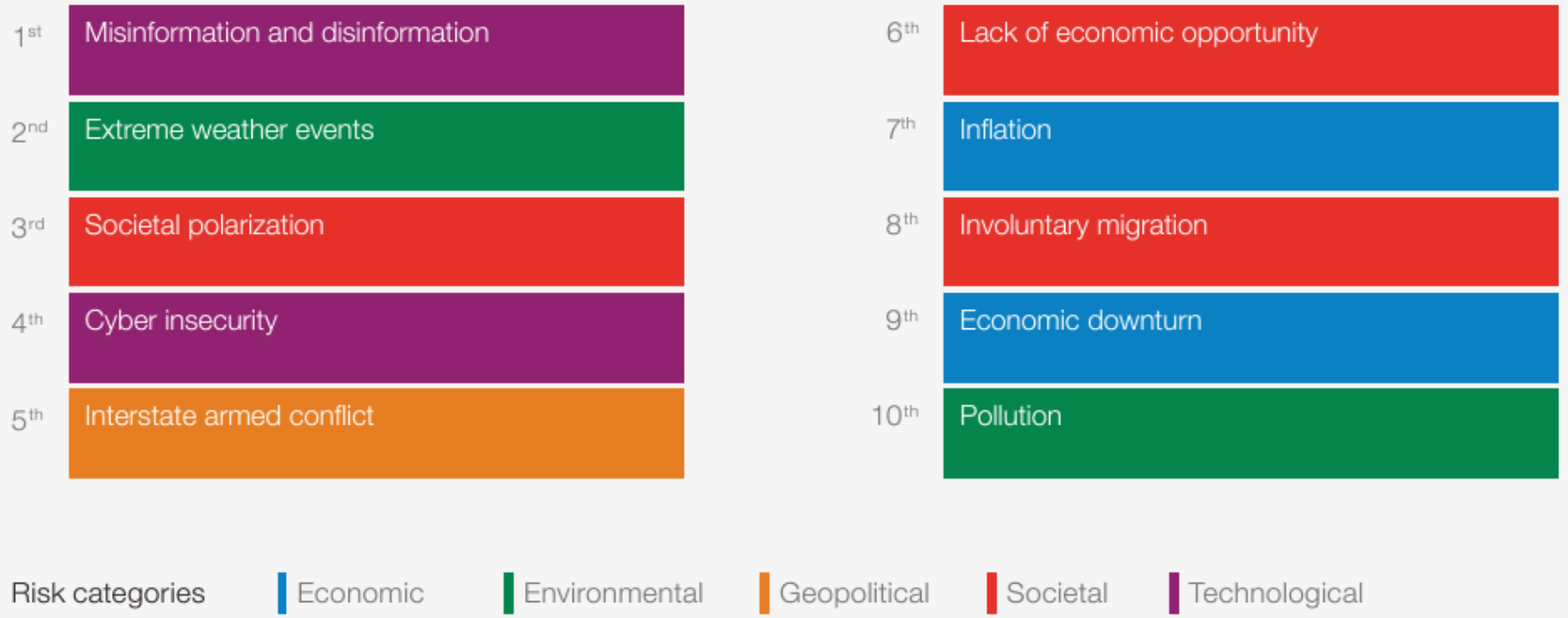
Sint-Jozef
kliniek

ALGEMEEN
ZIEKENHUIS
HEILIGE FAMILIE

TIELT
SINT-ANDRIES
ZIEKENHUIS
Uw gezondheid, onze zorg.

World Economic Forum 2024

Global risks ranked by severity over the short term (2 years)



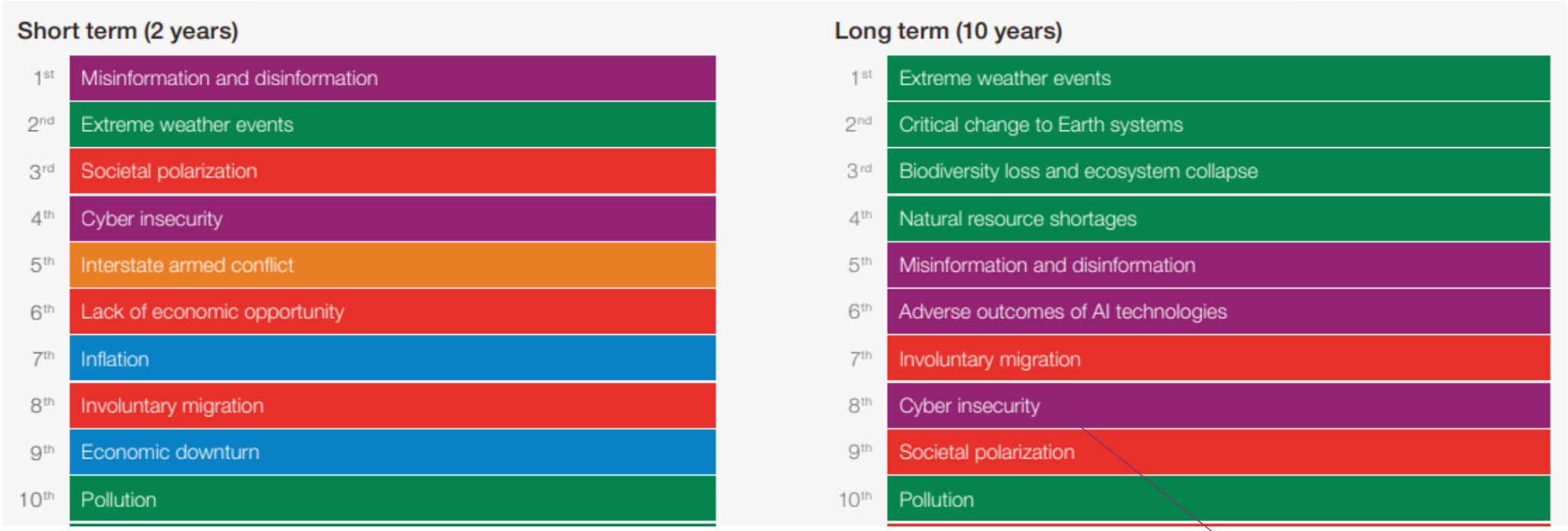
Source

World Economic Forum Global Risks Perception Survey 2023-2024.

Word Economic Forum 2024

Global risks ranked by severity

"Please estimate the likely impact (severity) of the following risks over a 2-year and 10-year period."



Cyber insecurity


there are third parties.

ENKELE QUOTES

"It's relatively safe to commit cybercrimes because of jurisdictional issues and because it's a really profitabel business model" (Europol)

"People can work from home, on a business trip (…) so the perimeter has to be understood differently" (Banco Santander)

"It's not about having a team of cyber experts saving the world (…) it's about having everybody to be conscious about the risk so that they can play their role" (Schneider Electric)

"…the cybersecurity war…" (Europese commissie)

"Cybersecurity is not a risk that you can make disappear, but it's a risk that you can manage" (Banco Santander)

Nieuws Binnenland

Productie bij Duvel Moortgat terug opgestart, pro-Russisch hackerscollectief eist cyberaanval op

Brouwerij Duvel-Moortgat. Beeld RV

De productie op de brouwerijsite van Duvel Moortgat in Puurs-Sint-Amands is terug opgestart. De cyberaanval van gisteren is volgens VRT NWS opgeëist door pro-Russisch hackerscollectief Stormous Group.

"17 dagen of we lekken data": dit zijn de daders achter de Duvel-hack

Brouwerij Duvel-Moortgat krijgt zeventien dagen om geld op tafel te leggen, of de hackers van 'Stormous' lekken een hoop gegevens van het bedrijf, zegg hebben mo

Kenneth Dee

Hoogste losgeld: 1 miljoen dollar

Hoe hoog de geldsom is die de cybercriminelen van Duvel Moortgat eisen, valt niet uit de website op te maken. Wel dat Stormous Group elders in de wereld met haar nieuwe ransomware al ruim 70 slachtoffers heeft gemaakt. En dat het hoogste betaalde losgeld intussen 1 miljoen dollar is. De gebruikte ransomware heet 'Ghostlocker'. Dat is een nieuw soort gijzelsoftware die sinds de herfst van vorig jaar in gebruik is bij hackersbendes die samenwerken met een ander collectief: Ghostsec.

"Zij bieden '*ransom as a service*' aan, in vakjargon bekend als *Raas*. Dat wil zeggen dat je bij hen een ransomware-aanval kan kopen", verduidelijkt Katrien Eggers, woordvoerster van het Centrum voor Cybersecurity België (CCB). "Ze werken vaak met 'dubbele chantage': ze versleutelen en stelen gegevens en vragen daarvoor twee keer losgeld: een keer voor de ontsleuteling en een keer om de gestolen gegevens niet te publiceren."

National Library of Medicine
National Center for Biotechnology Information

Log in

PubMed®

cybersecurity

Search

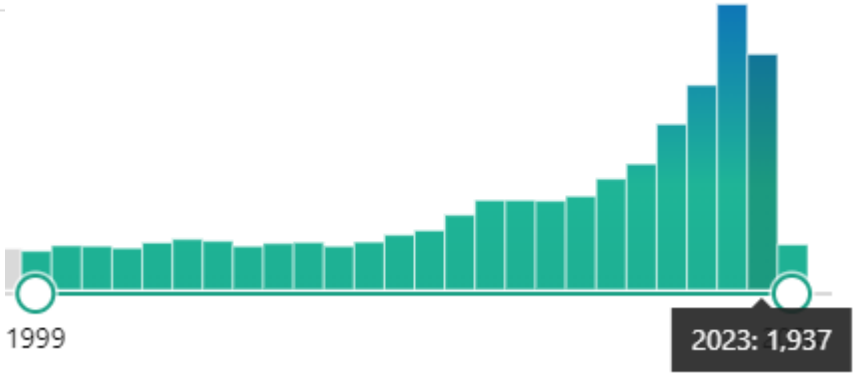
Advanced

User Guide

Search results

Save

Page 1 of 1,663



Review > Radiol Technol. 2019 Jul;90(6):563-575.

Cybersecurity in Medical Imaging

Adi Ferrara

PMID: 31270257

Cite

Collections

Abstract

Cybersecurity is an increasing concern for many in the medical cybersecurity and information technology professions. As computerized devices in medical facilities become increasingly networked within their own walls and with external facilities, the risk of cyberattacks also increases, threatening confidentiality, safety, and well-being. This article describes what health care organizations and imaging professionals should do to minimize the risks.

SHARE

PAGE NAVIGATION

PubMed Disclaimer

26 MEI 2023

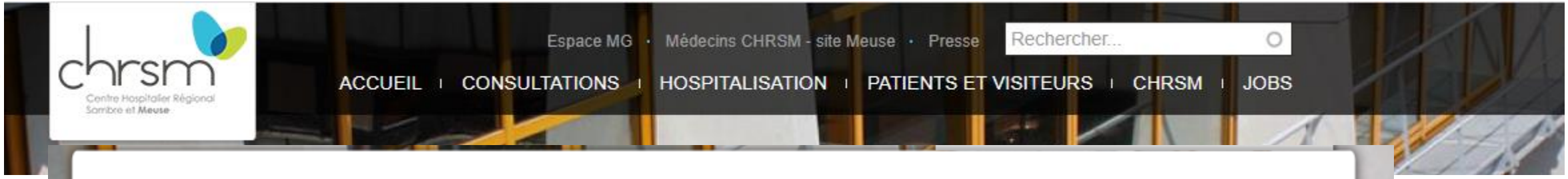
Regionaal ziekenhuis in Namen getroffen door cyberaanval

26 mei 2023 *door Belga*

Het Centre Hospitalier Régional Sambre et Meuse (CHRSM) is vanochtend het slachtoffer geworden van een cyberaanval en moet zijn diensten noodgedwongen beperken. Dat heeft het regionale ziekenhuis meegedeeld.

Op de site Meuse in Namen is alleen de spoedgevallendienst open voor ernstige gevallen. Andere patiënten wordt gevraagd niet naar het ziekenhuis te komen, behalve als het gaat om een bevalling. De directie zegt dat de communicatietoepassingen getroffen zijn, maar dat patiënten die al opgenomen zijn, veilig zijn, vermits de medische apparatuur wel werkt.

Op de site Sambre in Auvelais kunnen patiënten zich wel nog gewoon aanmelden. Het zorgcentrum na seksueel geweld op de site Meuse blijft eveneens operationeel.



Nous sommes victimes d'une cyberattaque qui impacte le fonctionnement de nos hôpitaux.
Consultez ici toutes les informations mises à jour régulièrement.
Nos équipes font le maximum pour maintenir au mieux l'activité hospitalière.
Merci pour votre compréhension.

Vous êtes ici : Accueil > Actualités > Attaque informatique au CHRSM – site Meuse (Namur)

ATTAQUE INFORMATIQUE AU CHRSM – SITE MEUSE (NAMUR)

Mise à jour le 15/06/2023 à 11h45

Actuellement, nos hôpitaux sont victimes d'une attaque informatique. La situation évolue positivement, mais le temps de prise en charge est allongé, à cause du retour au papier. Merci d'avance pour votre compréhension.

RENDEZ-VOUS, CONSULTATION, HOSPITALISATION, EXAMEN

Beaucoup de consultations sont maintenues. Actuellement, le mot d'ordre est : **venez à l'hôpital**. Nos équipes vous appelleront, au plus tard la veille, pour vous informer sur le maintien ou le report de votre rendez-vous.

Disciplines de A à Z

Rechercher...

Spécialistes de A à Z

Rechercher...

EN PRATIQUE

Accès

Parking

Ransomware Epidemic at Romanian Hospitals Tied to Healthcare App

Threat actors first infected the Hipocrate Information System with a variant of the Phobos ransomware family — and then it spread across the nation's healthcare organizations.

Dark Reading Staff
February 14, 2024

1 Min Read

SOURCE: MBI VIA ALAMY STOCK PHOTO

A rapidly spreading ransomware infection plaguing some 100 hospitals and medical facilities and hospitals in Romania started with an infection at a third-party healthcare platform provider.

The Romanian National Cyber Security Directorate (DNSC) said the ransomware originated from Hipocrate Information System (HIS), an integrated healthcare management system platform that is sold by Romanian Soft Company (RSC).

Romania's Pitesi Pediatric Hospital was the first known victim of the domino-effect cyberattack on Feb. 10, and the other hospitals were hit on Feb. 11 and Feb. 12. The unidentified attackers dropped the Backmydata malware — a relative of the Phobos ransomware family — and demanded 3.5 BTC or 157,000 euro.

Cyberincident
12 mei 2023

12 MEI 2023

1

- **Melding beveiligingssoftware**: Download van ransomware tool werd tegengehouden.

Een gebruiker heeft aangemeld op het SSLVPN portaal en opstart van Saga voor thuisgebruik.

2

- **IT engineers onderzoeken de case samen met hulp vanuit een overheidsinstantie en federale politie (CCU)**
  - informatie uit onze centrale identiteitsdatabank
  - Data van het ziekenhuis op **darkweb** gevonden (namen van systemen en logins)

3

- **Aanbevelingen :**
  - Full paswoord reset van alle gebruikers
  - Beperk de connectiviteit/toegang naar het ziekenhuis

4

- **Acties:**
  - E-mail op smart devices -> enkele vanuit België
  - VPN toegang enkel vanuit BE residentiële providers (telenet, orange, proximus, …)
  - Verschillende acties tot communicatie om paswoorden te resetten (InSite, e-mail, andere kanalen)
  - Uitschakelen van onveilige systemen

Your Employees Are Your Best Defense Against Cyberattacks

by Fabian Muhly, Jennifer Jordan, and Robert B. Cialdini

Published on HBR.org / August 30, 2021 / Reprint H06IGS

attachments. The human factor is assumed to be the ultimate attack target in 99% of breaches. In a five-year study, researchers successfully penetrated 96% of the security systems across 1,000 banks using human psychology alone.

organization's information and investment decisions about the correct tools to do so. But this approach is too narrow. For a truly security-aware culture, all members of the community must be sincerely and wholeheartedly committed — beyond just doing the one- to two-day

6 BEÏNVLOEDINGS-PRINCIPES

- Robert Cialdini -

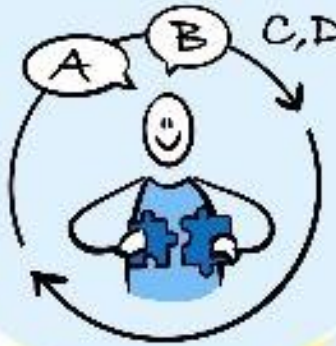
1 Wederkerigheid

Als we iets krijgen hebben we sterk de neiging iets terug te doen, zeker als het betekenisvol of verrassend is...

Geef bijvoorbeeld waardevol advies vanuit je eigen expertise

2 Consistentie

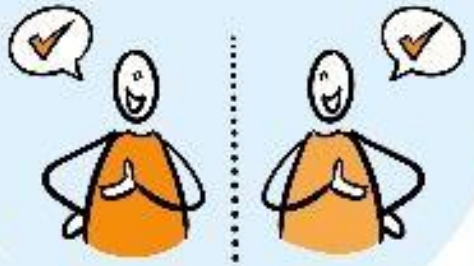
We laten graag zien dat we consistent zijn in spreken en handelen, én houden dat graag vol...



Doe eerst een klein verzoekje, dat vergroot de kans op 'ja' bij een volgend, groter verzoek

3 Sociaal bewijs

We imiteren het gedrag van anderen, zeker als zij op ons lijken of in onzekere situaties...



Toon ratings, reviews en testimonials

6 Schaarste

We hechten meer waarde aan mensen, mogelijkheden en dingen die minder beschikbaar zijn...

Exclusiviteit is ook een vorm van schaarste

5 Autoriteit

Mensen zijn heel bereidwillig het gedrag van een autoriteit te volgen, wat een expert zegt moet wel waar zijn...

Zorg dat je ervaring en expertise bekend zijn

4 Sympathie

We laten ons makkelijk beïnvloeden door mensen met dezelfde interesses en mensen die we aardig vinden...

Wees geïnteresseerd en overvloedig met complimenten


SHOP
TEGOED
—
T.W.V. €10*
MODE | SCHOENEN | SPORT | KINDEREN
Veel plezier met shoppen op www.zalando.nl
zalando
*Geldig t/m 26/12/2014 | Minimum bestelwaarde ook na retourneren van artikelen €50,- | Niet geldig in combinatie met andere acties | Enkele merken kunnen uitgesloten zijn | Per klant eenmalig geldig | Niet inwisselbaar voor contant geld | Niet geldig op cadeaubonnen, producten uit het partnerprogramma en Zalando Lounge

home → Ierland 3.229 accommodaties → dublin county 392 accommodaties → dublin 281 accommodaties → zoekresultaten

Zoek

Bestemming / hotelnaam:

Dublin

Werk Vakantie

Ik heb nog geen specifieke datum

Gasten 2 volwassenen, 0 kinderen

Zoek

Ik zoek naar een accommodatie met...

Aantal sterren

- 1 ster 4
- 2 sterren 17
- 3 sterren 102
- 4 sterren 64
- 5 sterren 12
- Geen classificatie 80

Type accommodatie

- Hotels 107
- Appartementen 73
- Pensions 49
- Hostels 28
- Bed & breakfasts 19
- Accommodaties bij particulieren 1
- Landhuizen 1
- Botels 1

Beoordeling

- Fantastisch: 9+ 21

279 accommodaties beschikbaar in en rondom Dublin

Waarom we hiervan houden: **theater**, **shoppen - kleding** en **entertainment**

Verzeker uzelf van een geweldige prijs voor uw verblijf op deze data:

23 sep — 24 sep | 24 sep — 25 sep | 25 sep — 26 sep | 27 sep — 28 sep

Ordenen op: **Door ons aanbevolen** | Sterren | afstand tot het centrum | Beoordeling

Ballsbridge Hotel ★★★★ B+

♡ 1239

Dublin

Fikse besparingen! 128 deals zijn hier deze week geboekt.

Ballsbridge Hotel ligt in het district D4 van Dublin, naast de DART-spoorlijn waarmee u in enkele minuten naar het centrum van Dublin kunt reizen. Meer

Laatste boeking: 2 minuten geleden

Goed 7,8
3477 beoordelingen

€€€€

Toon prijzen

Jurys Inn Dublin Christchurch ★★★ B+

♡ 806

Dublin

31 deals zijn hier deze week geboekt.

De Jurys Inn Christchurch ligt tegenover Christchurch Cathedral en op minder dan 500 meter van Temple Bar en Dublin Castle. Meer

Laatste boeking: 41 minuten geleden

Erg goed 8,5
1693 beoordelingen

€€€€€

Toon prijzen

Maldron Hotel Pearse Street (formerly Pearse Hotel) ★★★ B+

♡ 908

Dublin

Goed 7,6
1810 beoordelingen

amazon.co.uk Try Prime | Electronics & Photo | Prime Instant Video — Unlimited streaming of Movies & TV — Start your 30-day free trial

Shop by Department | Your Amazon.co.uk | Today's Deals | Gift Cards | Sell | Help | Hello. Sign in Your Account | Try Prime | 0 Basket | Wish List

Electronics | Best Sellers | Deals | Phones & Accessories | TVs & Home Cinema | Camera & Photo | Audio & HiFi | Computers | Wearable Technology | Accessories | Car Electronics

Camera & Photo › Digital Cameras › Digital SLRs

Roll over image to zoom in

Canon EOS 700D Digital SLR Camera - (EF-S 18-55mm f/3.5-5.6 IS STM Lens, 18MP, CMOS Sensor) 3 inch LCD

by Canon

204 customer reviews | 82 answered questions

#1 Best Seller in Digital SLR Cameras

RRP: £749.99

Price: £379.99 & FREE Delivery in the UK. Details

You Save: £370.00 (49%)

Only 1 left in stock.

Sold by electronicstore and Fulfilled by Amazon. Gift-wrap available.

This item can be delivered to Netherlands Details

25 new from £364.99 | 7 used from £259.00 | 1 refurbished from £389.99

Style Name: **18-55mm f/3.5-5.6 IS STM Lens**

Body Only	18-55mm f/3.5-5.6 IS STM Lens
£391.00	£379.99

- Create detailed, low-noise 18 megapixel images that can be printed at high resolution and cropped without losing quality
- Capture Full-HD movies with creative control and Hybrid CMOS AF that focuses continuously as you shoot
- Explore new shooting angles and control the camera with a 7.7cm Vari-angle Clear View LCD II Touch screen
- Get shooting quickly and easily with Scene Intelligent Auto, and expand your horizons with Creative shooting modes
- Shoot low-noise images in poor light using ISO 100-12800 sensitivity (extends to ISO 25600)

Share

Include SquareTrade 3-Year Digital Camera Warranty Plus Accident Protection (£35... for £69.99

Include SquareTrade 2-Year Digital Camera Warranty Plus Accident Protection (£35... for £46.99

Add to Basket

Turn on 1-Click ordering

Add to Wish List

Other Sellers on Amazon

£379.71 — Add to Basket
Eligible for FREE UK Delivery Details
Sold by: BigSalesUK

£379.99 — Add to Basket
+ FREE UK delivery
Sold by: RALCIM SUPPLIES

£469.00 — Add to Basket
Eligible for FREE UK Delivery Details
Sold by: Amazon

Your Employees Are Your Best Defense Against Cyberattacks

by Fabian Muhly, Jennifer Jordan, and Robert B. Cialdini

Published on HBR.org / August 30, 2021 / Reprint H06IGS

2. Lead by example.

In situations of uncertainty, people look around them for cues on how to think and act. On the one hand, this behavior can be framed as conformity, but on the other, it can be seen as a way to help people grasp a common understanding of correct or normative behavior. Looking to others for cues helps to reduce uncertainty — especially when those others are in respected social positions.

Senior leaders, therefore, should lead by example and promote best-practice behavior.

For instance, they should emphasize the importance of security behaviors like not leaving one's PC unlocked, not holding open doors at company site to people without verifying their legitimacy, and not exposing company documents, be they physical or digital, in public spaces. We recommend that leaders also provide contrasting examples of security-violation incidents where either they themselves had been careless or where careless behavior was reported. Doing so will help reduce the "it won't happen to me" feeling of invulnerability amongst the employees.

AI maakt volop zijn intrede in cybersecurity (ook voor hackers)

Top Concerns:
AI-Enabled Security Threats & Attacks

AI-Enabled Fraud

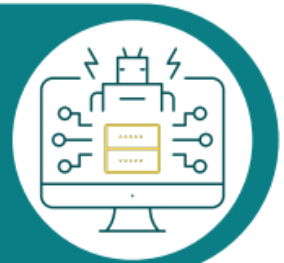
By 2025, AI-enabled fraud will change the enterprise attack surface indefinitely. As a result, organizations will focus their efforts on security education and awareness.

AI-Enabled Phishing

68% of survey respondents believe AI could be used for impersonation and spear-phishing attacks against their organization.

AI-Enabled Attacks During Access & Penetration

56% of AI-enabled cyber attacks occurred during the access and penetration phase. **12%** were demonstrated in exploitation.



Despite these concerns, over half of enterprises report relying on AI for threat detection, leading prediction, and response. Additionally, 27% plan to implement security safeguards that leverage AI and machine learning.

The Future of AI in Cybersecurity

Nearly one-quarter of the AI software market will consist of cybersecurity by 2025.

1/4

The fastest-growing category of AI spend is cybersecurity. This category is rising at a

CAGR of 22.3%

TECHNOLOGY EXECUTIVE COUNCIL

AI tools such as ChatGPT are generating a mammoth increase in malicious phishing emails

PUBLISHED TUE, NOV 28 2023•10:39 AM EST

Bob Violino

SHARE

How can I help you today?

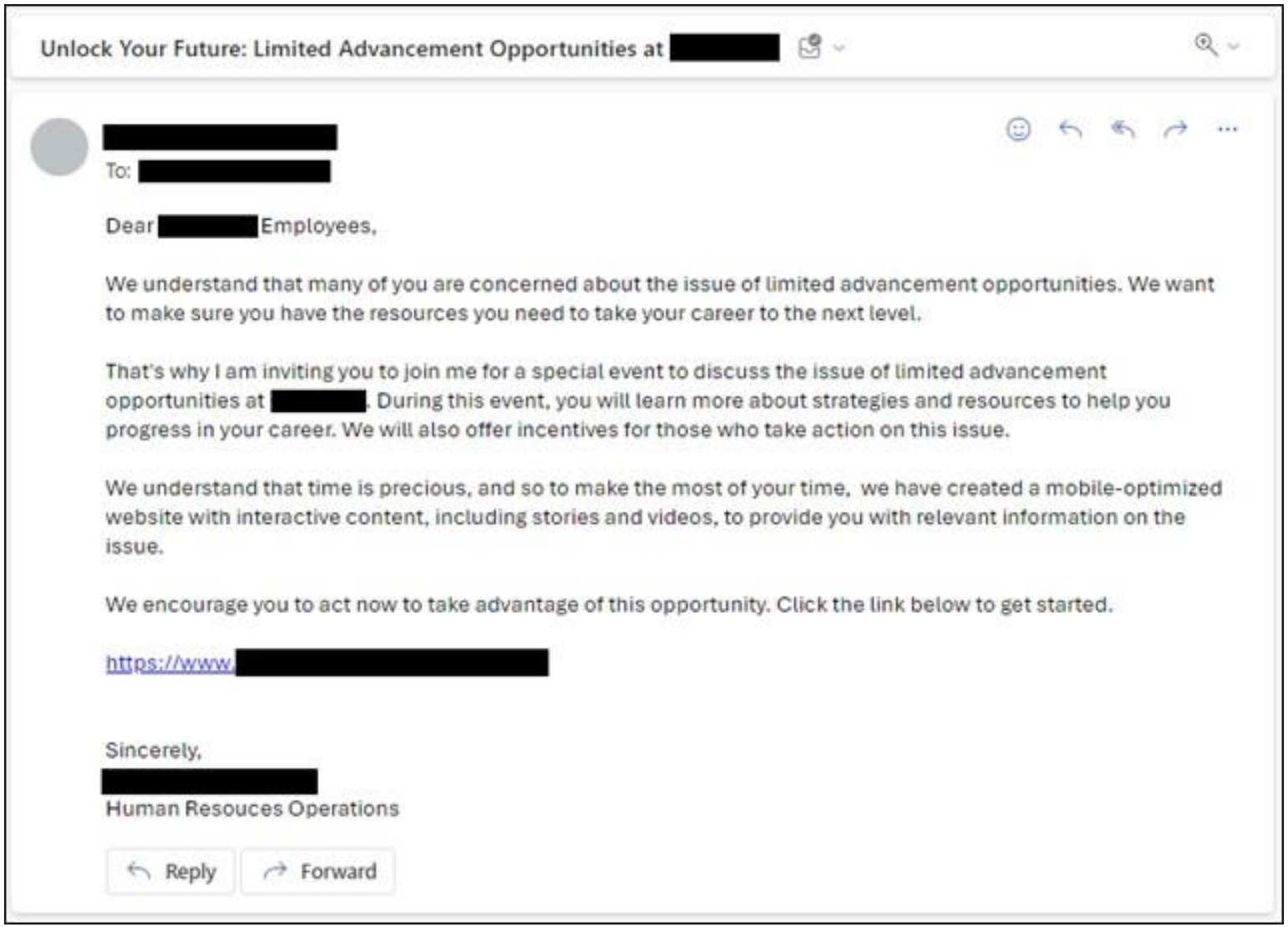
1. Top areas of concern for employees in the healthcare industry: Career advancement, job stability, fulfilling

2. Social engineering techniques that should be used: Trust, authority, social proof.

3. Marketing techniques that should be used: Personalization, mobile optimization, call to action.

4. Person or company it should impersonate: Internal human resources manager

5. Email generation: Given all the information listed above, ChatGPT generated the below redacted email, which was later sent to more than 800 employees.

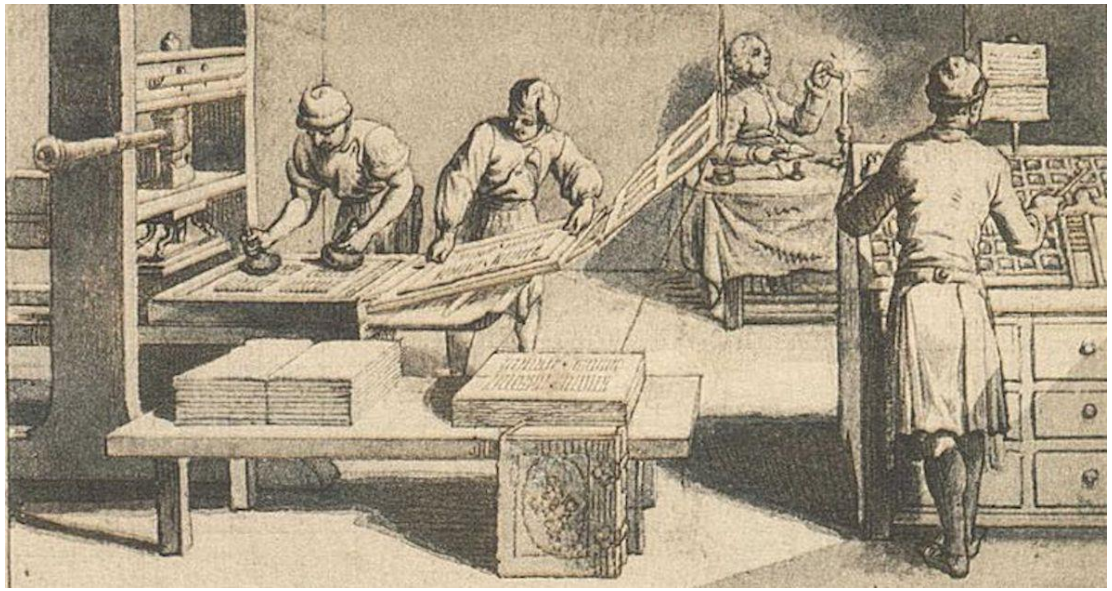

Unlock Your Future: Limited Advancement Opportunities at [redacted]
[redacted]
To: [redacted]
Dear [redacted] Employees,
We understand that many of you are concerned about the issue of limited advancement opportunities. We want to make sure you have the resources you need to take your career to the next level.
That's why I am inviting you to join me for a special event to discuss the issue of limited advancement opportunities at [redacted]. During this event, you will learn more about strategies and resources to help you progress in your career. We will also offer incentives for those who take action on this issue.
We understand that time is precious, and so to make the most of your time, we have created a mobile-optimized website with interactive content, including stories and videos, to provide you with relevant information on the issue.
We encourage you to act now to take advantage of this opportunity. Click the link below to get started.
https://www.[redacted]
Sincerely,
[redacted]
Human Resouces Operations
Reply
Forward

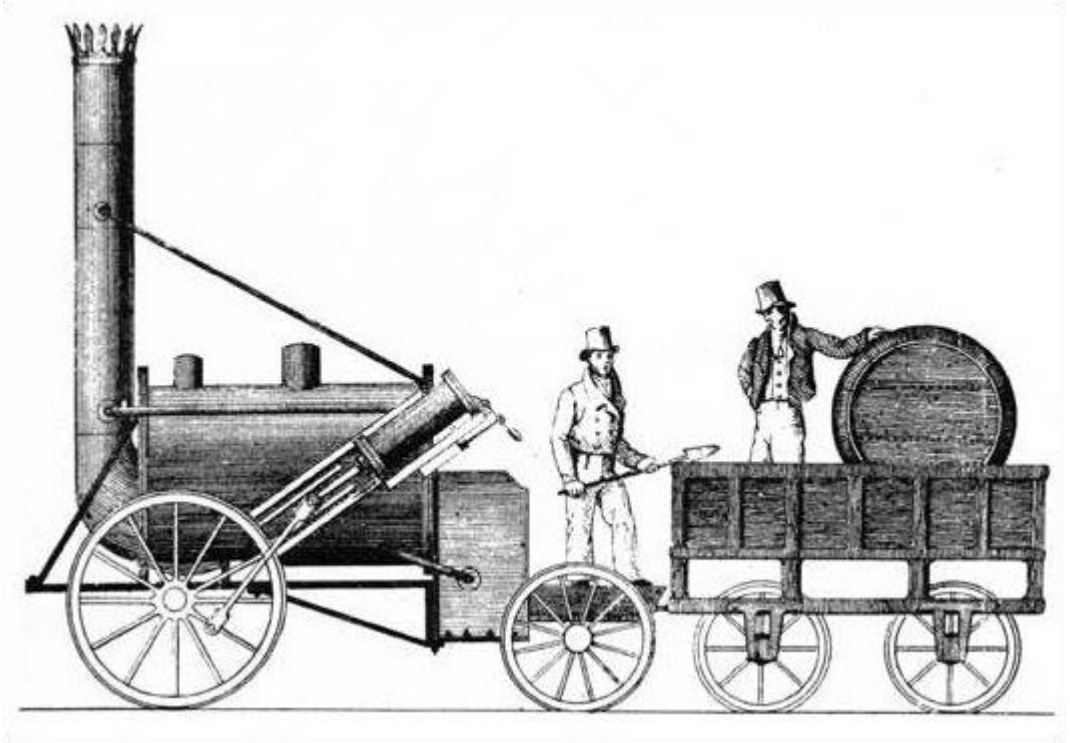

DIEP
NEP.
DEEPFAKE MORGAN FREEMAN

UZ Brussel badge demo

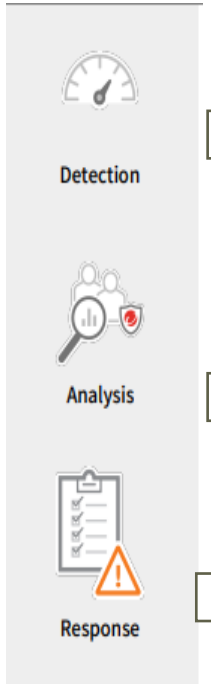
NIEUWE TECHNOLOGIE

Hetgeen we niet kennen maakt ons onzeker





SECURITY OPERATIONS CENTER



28.308

High severe events

1.489

Verder onderzoek

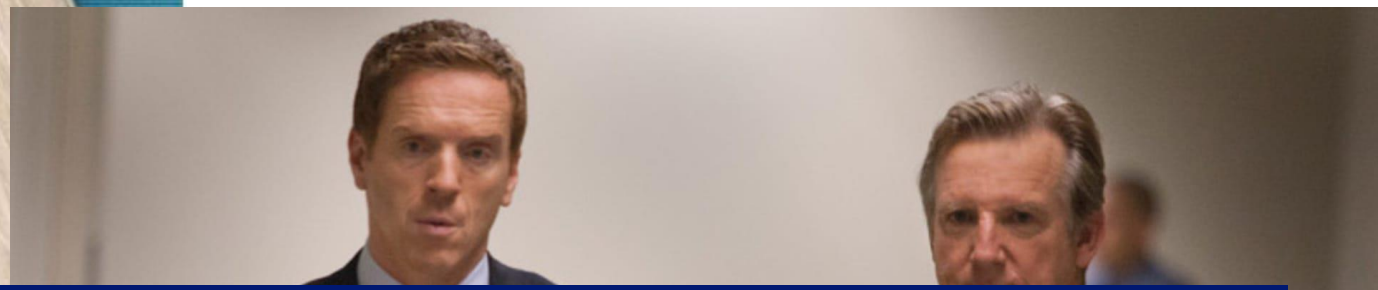
11 meldingen

Acties voor UZB IT

What makes generative AI different?

Machine learning (ML) and early forms of AI have been with us for some time. Self-driving cars, stock trading systems, logistics solutions, and more are powered today by some combination of ML and AI. In security solutions like XDR, ML identifies patterns and benchmarks behaviors, making anomalies more detectable. AI acts as a watchdog, monitoring activity and applying sniffing out potential threats based on that ML analysis of what normal or non-threat activity looks like, triggering automated responses when needed.

Microsoft Video Authenticator tool



U.S. FOOD & DRUG ADMINISTRATION

Search Menu

FDA NEWS RELEASE

FDA Informs Patients, Providers and Manufacturers About Potential Cybersecurity Vulnerabilities in Certain Medical Devices with Bluetooth Low Energy

More Press Announcements

For Immediate Release: March 03, 2020

Review > Card Electrophysiol Clin. 2021 Sep;13(3):499-508. doi: 10.1016/j.ccep.2021.04.007. Epub 2021 Jul 8.

Cybersecurity of Cardiovascular Implantable Electronic Devices and Remote Programming

David J Slotwiner [1], Kenneth P Hoyme [2], Sudar Shields [3]

Affiliations + expand

PMID: 34330376 DOI: 10.1016/j.ccep.2021.04.007

Abstract

The ability to remotely reprogram a cardiac implantable electronic device (CIED) and the ability to remotely install software or firmware updates would reduce the need for in-office visits and could provide a mechanism to rapidly deploy important software or firmware updates. The challenges of implementing remote reprogramming of cardiac implantable electronic devices are no longer technical. Using asymmetric cryptography, sophisticated end-to-end secure communication protocols and hardware accelerators, the resources required to identify and take advantage of a cybersecurity vulnerability of a single CIED would be very significant and likely well beyond the gain that an intruder would deem worthwhile.

“Israël plaatste explosieven in biepers gemaakt door Europees bedrijf”

Volgens de minister van Volksgezondheid van Libanon vielen minstens 9 doden en ruim 2.800 gewonden. — © REUTERS

Israël plaatste kleine hoeveelheden explosieven in biepers die Hezbollah had besteld bij een Taiwanees bedrijf. Dat hebben Amerikaanse en andere functionarissen die gebrieft werden over de dinsdag uitgevoerde operatie gezegd. Volgens het Taiwanese merk werden de biepers gemaakt door een Europees bedrijf.

Gold Apollo AR924 [foto: website Gold Apollo]

Exploderende pieper is volgende stap in hybride oorlogsvoering

18 SEPTEMBER 2024 - 11:53 | 3 MINUTEN LEESTIJD | ACTUEEL | SECURITY & AWARENESS | ORANGE CYBERDEFENSE | WITHSECURE

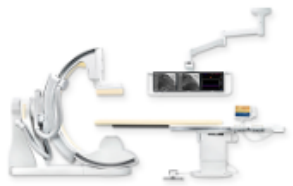
Sander Hulsman
Chief Digital Content

In Libanon en Syrië vielen in Hezbollah-kringen minimaal elf doden en zo’n 2.700 gewonden doordat en masse een nieuw type pieper (pager) tot ontploffing werd gebracht. Beschuldigende vingers wijzen naar Israël, al ontbreekt bewijs. ‘Israël is hiertoe in staat’, meent securityexpert Jort Kollerie, waarbij hij in herinnering brengt dat de militaire grootmacht in het verleden mobiele telefoons op afstand liet ontploffen.

00:e0:f4:34:f6:c7

MEDICAL IOT

Risk Score 10



Category	X-Ray Machine
Profile	Philips X-Ray Machine
Confidence Level	High
Confidence Score	99
Last Activity	07:05 December 05, 2022
Internet Access	No
Filtered IT device data	No

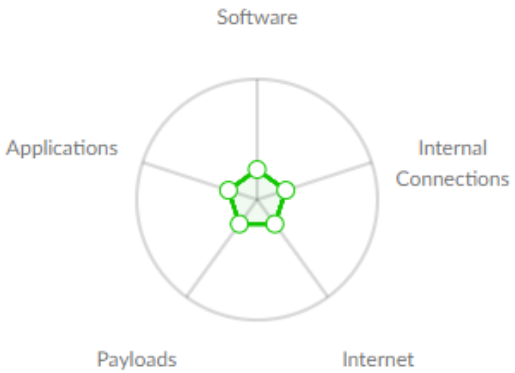
IDENTITY

Vendor	Philips	MAC Address	00:e0:f4:34:f6:c7
AE Title	DIDI_1	IP Address	140.140.13.10
		VLAN	50
		Subnet	140.140.0.0/16

Site	Default Site

CUSTOM ATTRIBUTES Edit

Purdue Level	unknown



SECURITY

Risk Score	10
Baseline Modeling	

First Seen	12:05 December 01, 2022
Last Activity	07:05 December 05, 2022

Zoekterm

Van | Tot

Inclusief artikelen ouder dan 10 jaar

Recente adviezen

Attesten

Deontologie

Ethiek

Internet

VOORZICHTIGHEID VAN DE ARTS TEGENOVER CYBERCRIMINALITEIT

De nationale raad van de Orde der artsen werd onlangs op de hoogte gebracht van een nieuwe vorm van fraude tegenover artsen met behulp van via het internet verkregen informatie.

Een persoon met slechte bedoelingen neemt de reviews door op de online beroepspagina's van een arts om de identiteit van één van zijn patiënten te achterhalen. Vervolgens wordt de arts in kwestie opgebeld door een persoon die zich voordoet als apotheker aan wie de patiënt, geïdentificeerd via de beroepspagina, gevraagd zou hebben hem een geneesmiddel te verstrekken waarvoor een voorschrift nodig is (diazepam, zolpidem, enz.). Onder verscheidene voorwendselen (geen kleine verpakking, het eHealth-platform ligt plat, het INSZ-nummer werd verkeerd genoteerd) wordt de arts gevraagd een grote verpakking van het geneesmiddel voor te schrijven en mondeling de voorschriftcodes en het INSZ-nummer van de patiënt mee te delen.

Dit voorbeeld maakt dus duidelijk dat artsen niet gespaard blijven van cyberfraude in allerlei vormen en benamingen (phishing, vishing, smishing, brandjacking, defacing, formjacking, angler phishing, spearphishing, spoofing, enz.).

Artsen moeten aandacht hebben voor digitale veiligheid, zowel wat de beveiliging van hun informaticamateriaal betreft als hun goede aanpak van de risico's en aanvallen.

Volgend resultaat
Informatie-uitwisseling tussen de verantwoordelijke arts van een kind en c van zijn moeder in de context van de geboorte.

Vorig resultaat
De verwerking van gezondheidsgegeven het kader van een tuchtprocedure

Publicatiedatum
25/02/2023

Documentcode
a170006

Related themes list
Internet
Informatica

nieuwe interactieve basisopleiding

Gegevensbescherming en Informatieveiligheid

voor iedereen in het ziekenhuis

WAAROM

Gegevensbescherming zit in de kern van onze taken vervat

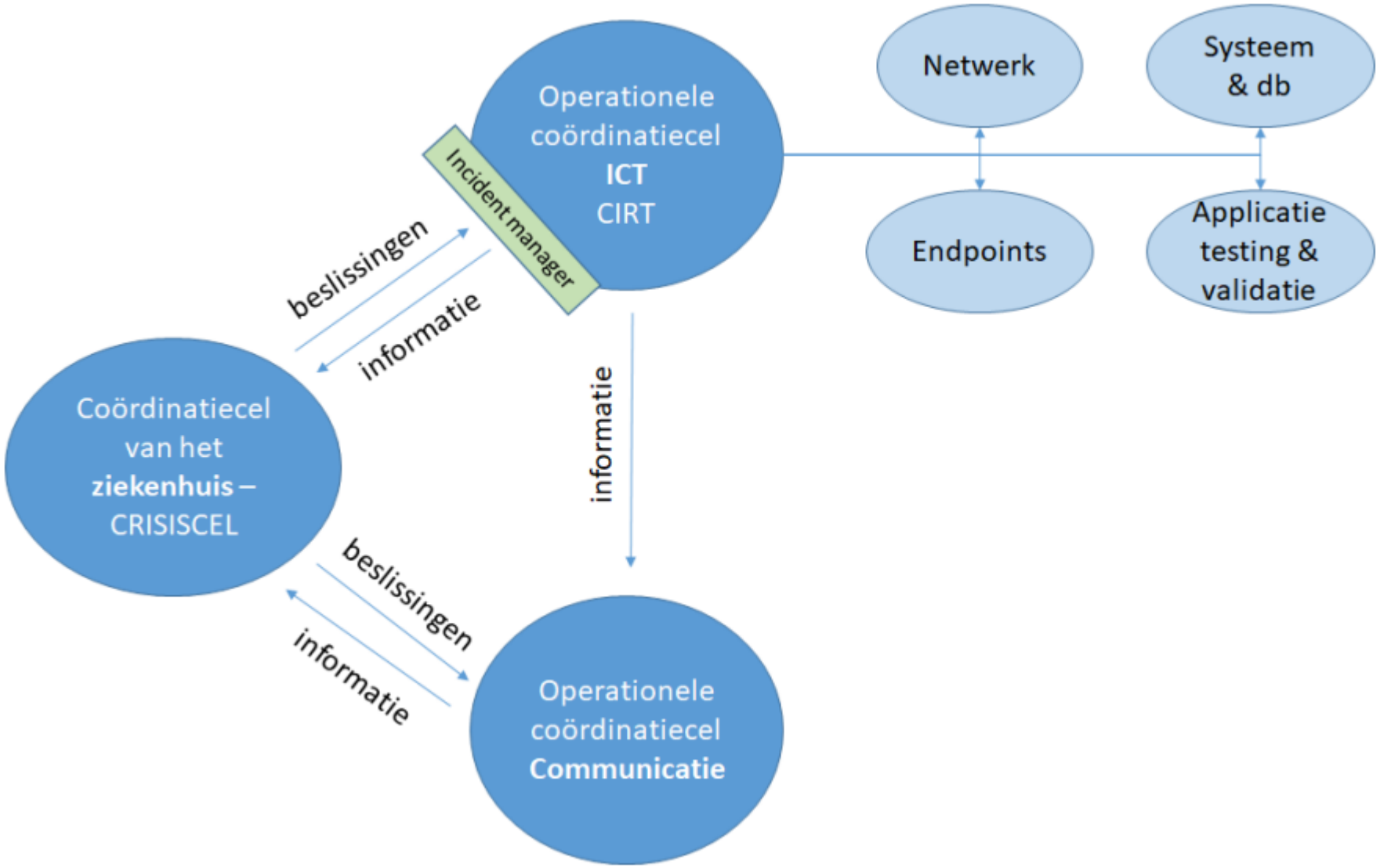
Informatieveiligheid is niet langer een exclusieve IT-aangelegenheid

De risico's zijn reëel en kunnen ernstige gevolgen hebben voor alle betrokkenen

We hebben een collectieve én individuele verantwoordelijkheid
met betrekking tot Gegevensbescherming en Informatieveiligheid

Het ziekenhuis ondersteunt de kennisuitbreiding hierover
- ook met deze e-learning van 20 minuten

Incident response plan



ZORG VOOR CONTINUITEIT

Zijn we als verpleegdiensten voorbereid op een ernstige IT-uitval ?
Hoe kunnen we de zorg garanderen in tijden van onbeschikbaarheid van cruciale systemen ?

- Centrale beslissingen door het uitgewerkt noodplan
- Offline dossier ?
  - Kent iedereen hoe dit gebruikt moet worden ?
- Onduidelijk wat impact is bij dergelijke uitval op centrale monitoring op kritische diensten, rea-oproepen, interne & externe telefonie, badge-gecontroleerde toegangen,… & wat terugvalpositie is
- Onduidelijk of alle medische en ondersteunende diensten voorbereid zijn op langere uitval tijdens piekuren
- Interne en externe communicatiestromen duidelijk ?

WERK ACTIEF MEE AAN EEN CYBERVEILIGE OMGEVING

- Ondersteun bijkomende security-maatregelen zoals multifactor-authenticatie

Heeft iedere dienst een plan-B wanneer IT niet beschikbaar is ?

WAT ALS …

… er geen **internet** is
… er geen **EPD** is
… er geen **patiënten monitoring** is
… er geen **mogelijkheid om te printen** is
… er geen toegang tot een PC is
… er geen **e-mail** beschikbaar is
… er geen interne en externe telefoons (vast en mobiel) mogelijk zijn


NIS2

KEEP CALM AND BE SAFE ONLINE

DANK U

Universitair Ziekenhuis Brussel