Informacijska varnost v praksi: pot do skladnosti z NIS2 in kaj nam povedo analize vrzeli

dr. Benjamin Lesjak

CNN World

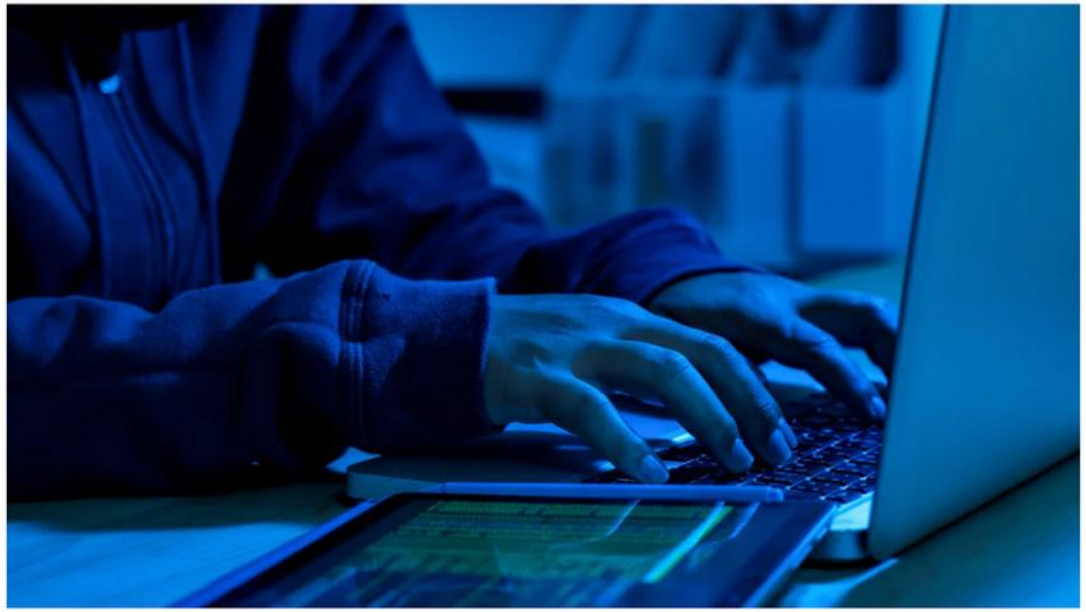
Sign in

World / Asia

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024



Authorities are increasingly concerned at the damaging potential posed by artificial intelligence technology. boonchai wedmakawand/Moment RF/Getty Images

(CNN) — A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call, according to Hong Kong police.

The elaborate scam saw the worker duped into attending a video call with what he thought

24UR.COM

Nizozemska banka svari: Imejte pri sebi gotovino za nujne primere

Amsterdam, 21. 05. 2025 18.38 | Posodobljeno pred 11 urami

PREDVIDEN ČAS BRANJA: **2 min**

AVTOR U.Z.

KOMENTARJI 95

Nizozemska centralna banka državljanom svetuje, naj imajo zaradi naraščajočih kibernetskih groženj pri roki gotovino za nujne primere. 70 evrov na odraslega in 30 evrov na otroka bo zadostovalo za kritje osnovnih stroškov za obdobje 72 ur.

Nizozemska centralna banka (DNB) je državljanom svetovala, naj imajo v primeru katastrofe ali izrednih razmer, kot so naraščajoče geopolitične napetosti in kibernetske grožnje, ki bi lahko ogrozile plačilni sistem države, pri roki dovolj gotovine za obdobje treh dni.

V primeru, da elektronski plačilni sistemi ne bi delovali, naj imajo pri sebi 70 evrov gotovine na odraslo osebo in 30 evrov gotovine na otroka.

"Pomislite na izpad elektrike, tehnično motnjo v banki ali izpad Wi-Fi-ja. Potem morda ne boste mogli plačevati tako, kot ste vajeni. Plačilo z gotovino pa je skoraj vedno mogoče. Takšen znesek v gotovini bo zadoščal za kritje osnovnih stroškov, kot so voda, hrana, zdravila in prevoz za obdobje 72 ur," so zapisali.

Univerza tako zagotavlja, da se storitve počasi vračajo v običajno delovanje.

PREBERITE ŠE:

Univerzo v Mariboru naj bi napadli ruski hekerji z izsiljevalskim virusom

Povečani varnostni ukrepi pri prijavi

Študentje so bili obveščeni, da je prijava v Microsoftov sistem M365, ki vključuje aplikacije, kot so **Teams** in e-poštne storitve, znova omogočena.

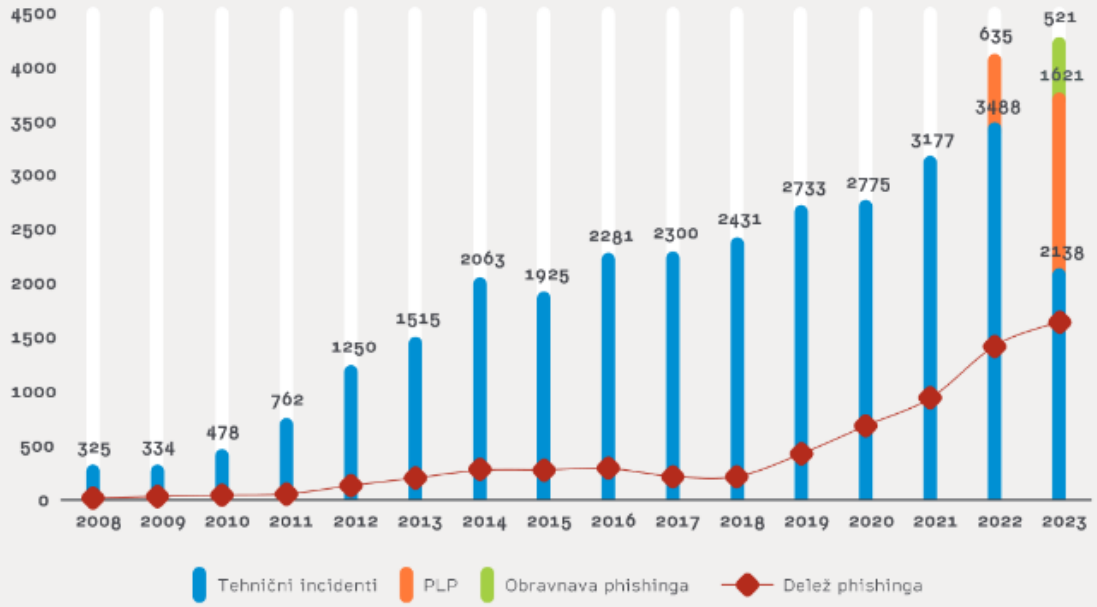
Pri tem pa morajo za dodatno varnost zamenjati svoja gesla.

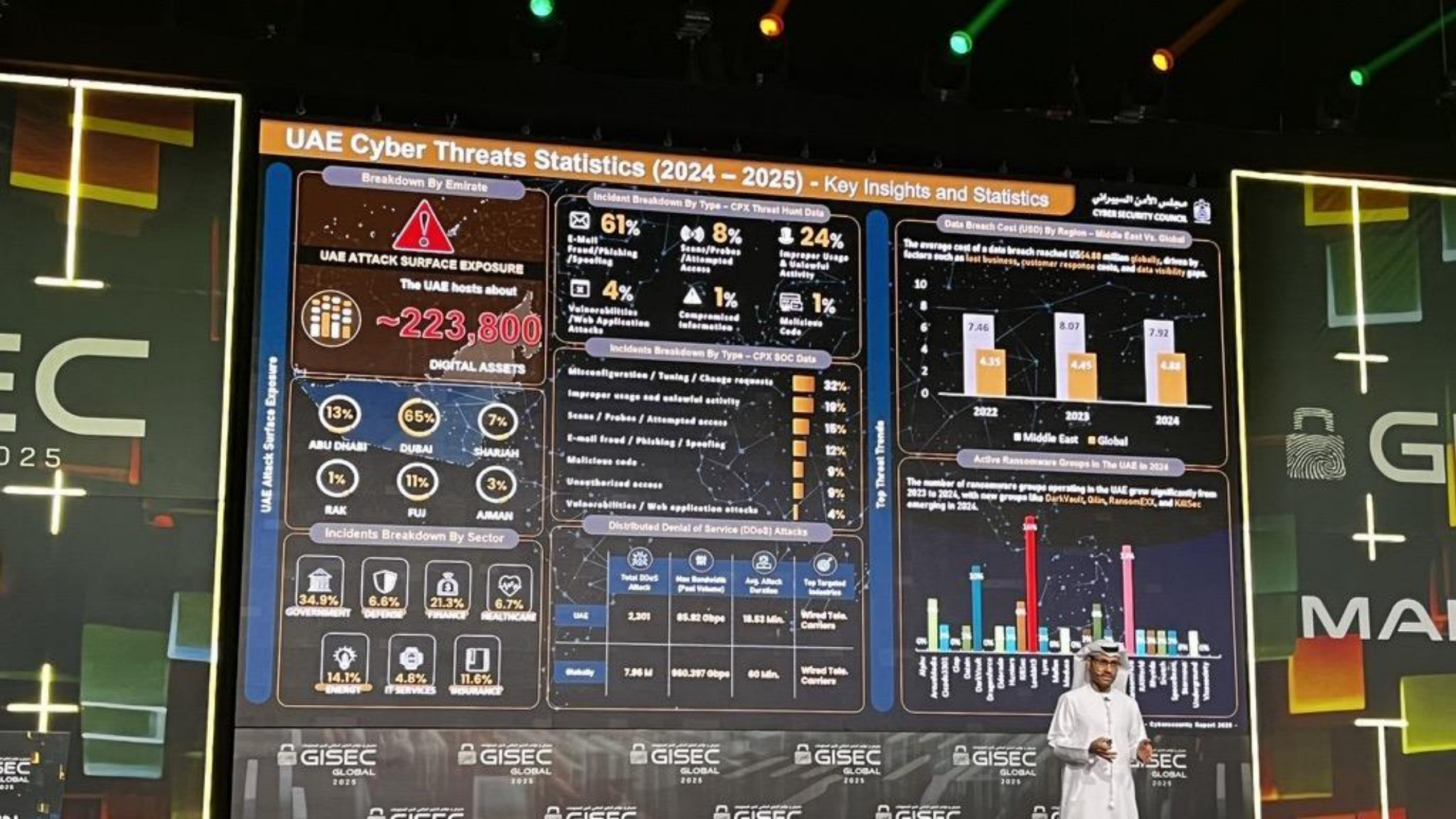
> Novo geslo mora biti sestavljeno iz vsaj 12 znakov, ki vključujejo kombinacijo črk, številk in simbolov, kar omogoča večjo varnost.
>
> Poleg tega univerza uvaja večfaktorsko avtentikacijo za vse redno vpisane študente, ki morajo kot drugi faktor izbrati aplikacijo **Microsoft Authenticator**.

DATAINFO

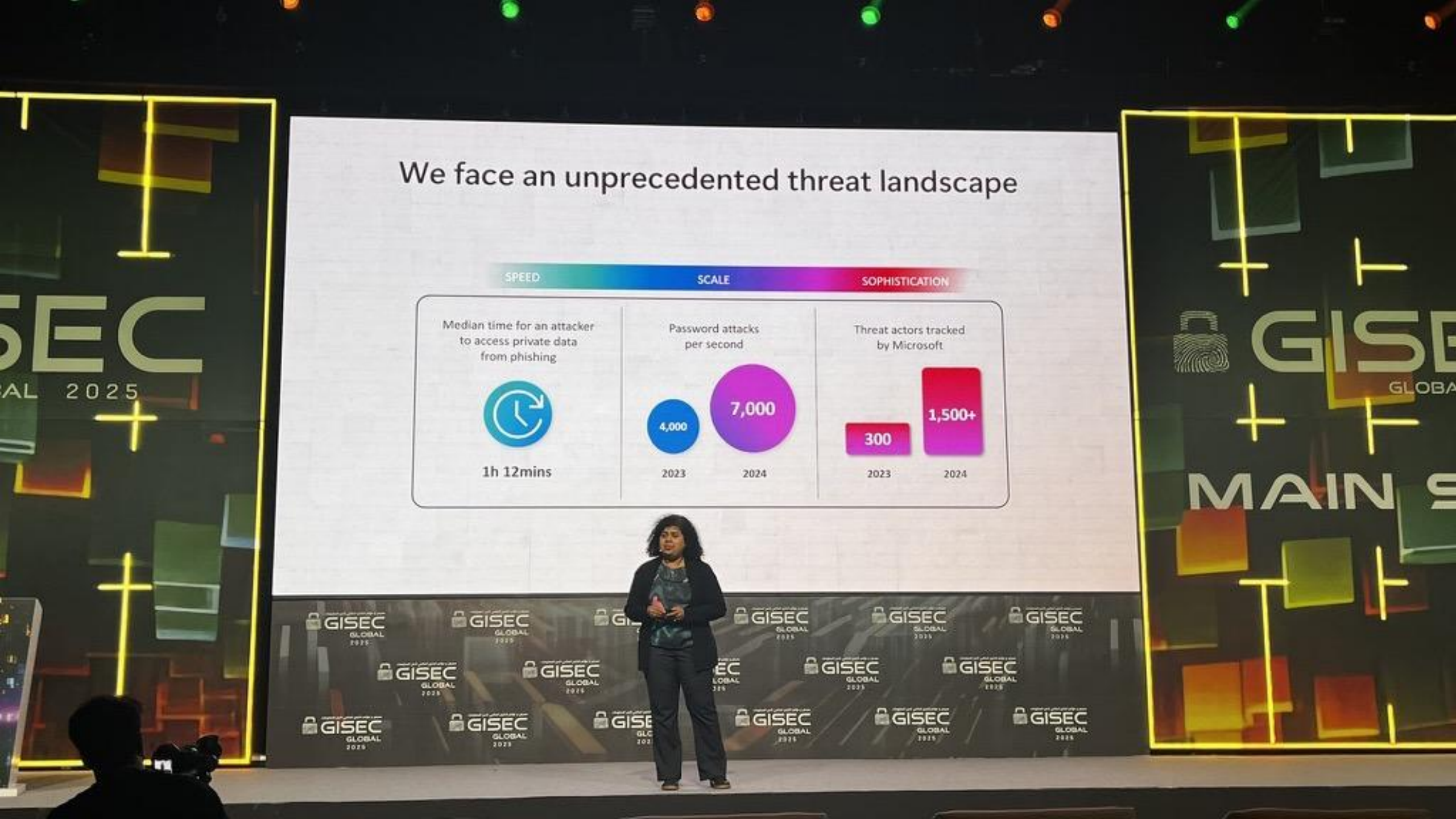
Število napadov raste ...

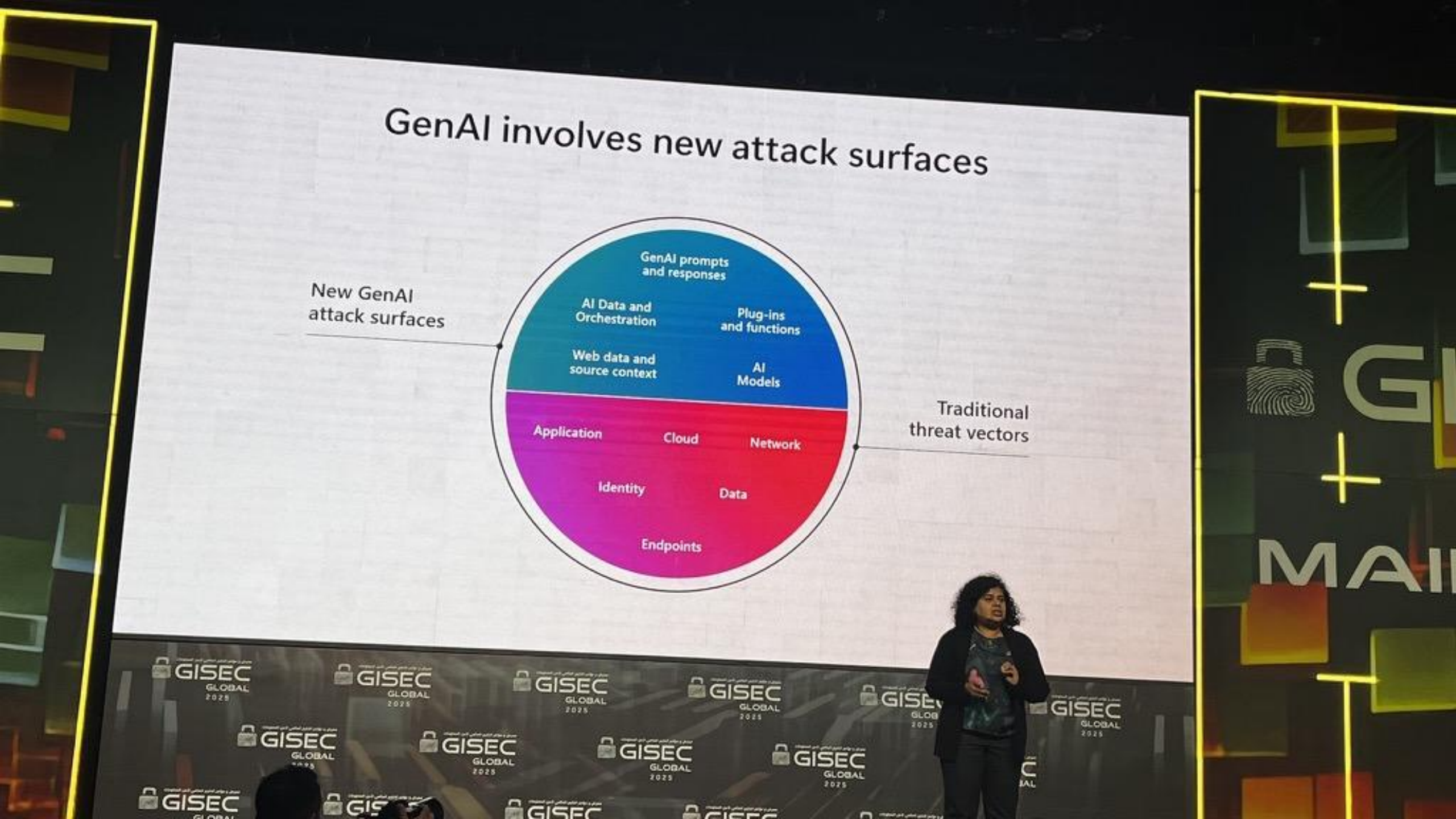
INCIDENTI SKOZI LETA




UAE Cyber Threats Statistics (2024 – 2025) - Key Insights and Statistics
CYBER SECURITY COUNCIL
UAE Attack Surface Exposure
Breakdown By Emirate
UAE ATTACK SURFACE EXPOSURE
The UAE hosts about
~223,800
DIGITAL ASSETS
13% ABU DHABI
65% DUBAI
7% SHARJAH
1% RAK
11% FUJ
3% AJMAN
Incidents Breakdown By Sector
34.9% GOVERNMENT
6.6% DEFENSE
21.3% FINANCE
6.7% HEALTHCARE
14.1% ENERGY
4.8% IT SERVICES
11.6% INSURANCE
Incident Breakdown By Type – CPX Threat Hunt Data
61% E-Mail Fraud/Phishing /Spoofing
8% Scans/Probes /Attempted Access
24% Improper Usage & Unlawful Activity
4% Vulnerabilities /Web Application Attacks
1% Compromised Information
1% Malicious Code
Incidents Breakdown By Type – CPX SOC Data
Misconfiguration / Tuning / Change requests 32%
Improper usage and unlawful activity 19%
Scans / Probes / Attempted access 15%
E-mail fraud / Phishing / Spoofing 12%
Malicious code 9%
Unauthorized access 9%
Vulnerabilities / Web application attacks 4%
Top Threat Trends
Distributed Denial of Service (DDoS) Attacks
Total DDoS Attack
Max Bandwidth (Peak Volume)
Avg. Attack Duration
Top Targeted Industries
UAE 2,301 85.82 Gbps 18.53 Min. Wired Tele. Carriers
Globally 7.96 M 960.397 Gbps 60 Min. Wired Tele. Carriers
Data Breach Cost (USD) By Region – Middle East Vs. Global
The average cost of a data breach reached US$4.88 million globally, driven by factors such as lost business, customer response costs, and data visibility gaps.
10
8
6
4
2
0
7.46
4.35
8.07
4.45
7.92
4.88
2022
2023
2024
Middle East
Global
Active Ransomware Groups In The UAE In 2024
The number of ransomware groups operating in the UAE grew significantly from 2023 to 2024, with new groups like DarkVault, Qilin, RansomEXX, and KillSec emerging in 2024.
GISEC GLOBAL 2025


مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
Total Disclosed Incidents
52,659
AI Detected
46%
Incident Severity
4%
Critical
15%
High
23%
Medium
58%
Low
Cyber Kill Chain
72%
Reconnaissance
8%
Weaponization
5%
Delivery
3%
Exploitation
9%
Installation
2%
Comand & Control
1%
Action On Objectives
Affected Sectors
Education 1%
Energy 5%
Finance 18%
Government 29%
Healthcare 4%
IOT 26%
Military 3%
Transport 14%
Total Alerts
29,483
OT Risk Score
4.2
Alerts Severity
4%
Critical
15%
High
23%
Medium
58%
Low
Vulnerabilities
Total
4%
15%
58%
23%
Top 5 Vulnerabilities
Affected Sectors
Airports 9%
Energy 14%
Finance 5%
Government 22%
33%
Ports 17%


We face an unprecedented threat landscape
SPEED
SCALE
SOPHISTICATION
Median time for an attacker to access private data from phishing
1h 12mins
Password attacks per second
4,000
7,000
2023
2024
Threat actors tracked by Microsoft
300
1,500+
2023
2024
GISEC
GLOBAL
2025


GenAI involves new attack surfaces
New GenAI attack surfaces
GenAI prompts and responses
AI Data and Orchestration
Plug-ins and functions
Web data and source context
AI Models
Application
Cloud
Network
Identity
Data
Endpoints
Traditional threat vectors
GISEC GLOBAL 2025

Nova zakonodaja o informacijski varnosti

- UREDBA EU o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije (postopno uveljavljanje)
- UREDBA EU DORA (finančni sektor, januar 2025)
- DIREKTIVA EU CER o odpornosti kritičnih subjektov (17. oktober 2024, slovenski Zakon o kritični infrastrukturi)
- DIREKTIVA EU NIS 2 (17. oktober 2024)
- ZINFV-1 (pred glasovanjem v Državnem zboru)
- Slovenski zakon ZVOP-2 - 23. člen (uporaba člena od 26.1.2026)

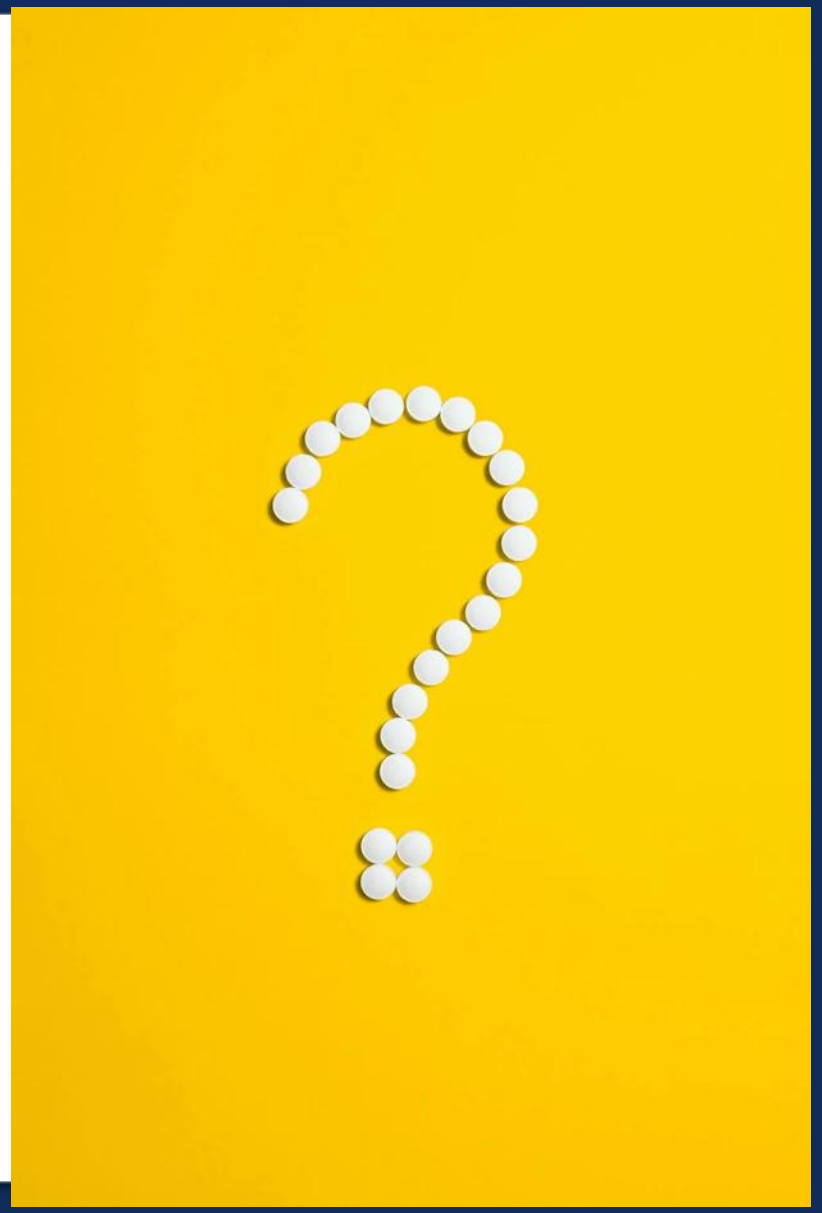
- **Nemoteno delovanje države v vseh varnostnih razmerah.**
- **Krepitev odpornosti na kibernetske grožnje pri bistvenih dejavnostih za družbo.**

Cca. 1.000 novih zavezancev (ocene gredo do 2.000)

- Javni ali zasebni subjekti

- 50+ zaposlenih
- 10 mio promet
- 10 mio bilančna vsota
- Kriterij dejavnosti

- Nekateri bodo zavezanci ne glede na dejavnost!



NIS 2 BISTVENI SUBJEKTI (visoko kritični sektorji)

NIS 2 - PRILOGA I: VISOKO KRITIČNI SEKTORJI

1. energija (elektrika, daljinsko ogrevanje in hlajenje, nafta, plin, vodik);
2. promet (zračni, železniški, vodni, cestni);
3. bančništvo (kreditne institucije);
4. infrastruktura finančnega trga (upravljalci mest trgovanja, centralne nasprotne stranke);
5. zdravje (izvajalci zdravstvenega varstva, referenčni laboratoriji, proizvajalci medicinskih pripomočkov);
6. pitna voda (dobavitelji in distributerji pitne vode kot glavne dejavnosti);
7. odpadna voda (podjetja, ki zbirajo, odvajajo ali čistijo komunalno odpadno vodo kot glavno dejavnost);
8. digitalna infrastruktura (DNS, TLD, oblačne storitve, podatkovni centri, ponudniki storitev zaupanja);
9. upravljanje storitev IKT (ponudniki upravljanih varnostnih storitev);
10. javna uprava (na centralni ravni države, na regionalni ravni);
11. vesolje (upravljalci talne infrastrukture, ki podpira opravljanja vesoljskih storitev).

NIS 2 POMEMBNI SUBJEKTI (drugi kritični sektorji)

NIS2 - PRILOGA II: DRUGI KRITIČNI SEKTORJI

1. Poštne in kurirske storitve (izvajalci določenih poštnih in kurirskih storitev);
2. Ravnanje z odpadki (izvajalci – glavna dejavnost);
3. Izdelava, proizvodnja in distribucija kemikalij (proizvodnja in distribucija določenih snovi);
4. Pridelava, predelava in distribucija živil (prodaja na debelo, industrijska pri(e)delava);
5. Proizvodnja določenih vrst izdelkov (medicinski pripomočki; računalniki, elektronski in optični izdelki, proizvodnja električnih naprav, proizvodnja drugih strojev in naprav, proizvodnja motornih vozil, prikolic, polprikolic, proizvodnja drugih vozil in plovil);
6. Digitalni ponudniki (spletne tržnice, spletni iskalniki, platforme storitev družbenega mreženja);
7. Raziskave (raziskovalne organizacije).

ZAVEZANCI NE GLEDE NA VELIKOST: ZInfV-1 (3. in 6. čl.) + NIS2

Javni in zasebni subjekti iz NIS 2 Priloge I in II ne glede na velikost:

- ponudniki javnih elektronskih komunikacijskih omrežij;
- ponudniki storitev zaupanja;
- registri vrhnjih domenskim imen in sistemskih domenskim imen;
- edini ponudnik storitev, ki je bistvena za ohranjanje kritičnih ali gospodarskih dejavnosti v RS;
- motnja pri opravljanju storitve lahko pomembno vplivala na javni red, javno varnost ali javno zdravje;
- motnja pri opravljanju storitve lahko povzročila pomembno sistemsko tveganje, zlasti ob čez mejnem vplivu;
- subjekt kritičen zaradi njegovega posebnega pomena na državni, regionalni ali lokalni ravni za določen sektor ali vrsto storitve ali za druge medsebojno odvisne sektorje v RS;
- gre za subjekt javne uprave na državni ravni ali na regionalni ravni in
- gre za subjekt javne uprave na lokalni ravni, če pri slednjem izhaja iz njegove ocene tveganja, da opravlja storitve, katerih motnje bi lahko pomembno negativno vplivale na ključne družbene ali gospodarske dejavnosti.

ZAVEZANCI (dodatno)

- **Kritični subjekti, določeni na podlagi Zakona o kritični infrastrukturi** (Direktiva (EU) 2022/2557 (CER)), ne glede na njihovo velikost.
- Subjekti, ki opravljajo storitve registracije domenskih imen, ne glede na velikost.
- Subjekti lokalne samouprave, mestne občine in občine, ki imajo sedeže v krajih, kjer je sedež upravnih enot (teh je 58).
- Subjekti, ki jih Vlada RS identificira kot pomembne, zaradi pomembnega negativnega vpliva na življenje, zdravje ali okolje v primeru incidenta.
- Subjekti, ki so bili določeni po (trenutnem) ZInfV pred 16.1.2023
- NIS2 se NE uporablja za subjekte javne uprave iz področja nacionalne varnosti, javne varnosti, obrambe ali kazenskega pregona, vključno s preprečevanjem, preiskovanjem, odkrivanjem in pregonom kaznivih dejanj.

23. člen ZVOP-2 – bliža se konec triletnega prehodnega obdobja

- **Zakon o varstvu osebnih podatkov (ZVOP-2) je bil objavljen v Uradnem listu RS št. 163/22 dne 27. decembra 2022.**
- **ZVOP-2 se je začel uporabljati 26. januarja 2023 (razen nekaj izjem!!)**
- **116. člen ZVOP-2 : „Obdelave osebnih podatkov iz prvega odstavka 23. člena tega zakona se uskladijo z določbami 23. člena tega zakona v roku treh let od uveljavitve tega zakona.“**
- **Začetek uporabe 23. člena ZVOP-2 je 26. januar 2026!**

Zavezanci po 23. členu ZVOP-2

(1) **Za informacijske sisteme,** v katerih:

1. se izvajajo obdelave osebnih podatkov, določenih v zakonih, ki urejajo področja upravnih notranjih zadev, finančne uprave, državljanstva, Slovenske obveščevalno-varnostne agencije, obrambe, **zdravstvenega varstva, obveznega zdravstvenega zavarovanja, uveljavljanja pravic iz javnih sredstev** ter kazenskih in prekrškovnih evidenc, **ali**
2. se obdelujejo osebni podatki **več kot 100.000 posameznikov na podlagi zakona**, razen obdelav osebnih podatkov iz 3. poglavja 2. dela tega zakona, **ali**
3. **upravljavec ali obdelovalec kot svojo temeljno dejavnost izvaja obsežne obdelave posebnih vrst osebnih podatkov**, **ali**
4. se obdeluje **posebne vrste osebnih podatkov več kot 10.000 posameznikov**,

Velikost subjekta po 23. členu ZVOP-2 ni pomembna *(število zaposlenih ali letni prihodki)*

23. člen ZVOP-2 pri odločanju nima kriterija velikosti, kot ga pozna ZINFV-1 (NIS2) ali Zakon o kritični infrastrukturi (CER) Pomembna je samo dejavnost obdelave podatkov in količina (število) posameznikov, ki so v vaših sistemih.

VERJETNO NE:	VERJETNO DA:
• Občina (ne mestna) • Zavod za kulturo … • Komunalno podjetje • Zasebno podjetje, ki ima veliko bazo posameznikov (ne občutljivi podatki in ne ogromna baza) • Osnovna, srednja šola in vrtec	• Zdravstveni zavod • Lekarna • Koncesionarji v zdravstvu • Ponudniki programske opreme za zdravstvo • 100.000+ oseb v bazi podatkov • 10.000+ oseb občutljivi podatki

Sprememba 23. člena ZVOP-2, ki jo ureja 67. člen ZINFV-1 (tretje branje v DZ)

Velja dne 21.5.2025:

- se smiselno uporabljajo določbe o varnostnih zahtevah in priglasitvi incidentov iz zakona, ki ureja informacijsko varnost, ki se nanašajo na izvajalce bistvenih storitev, če upravljavec glede teh obdelav ni dolžan izvajati ukrepov po zakonu, ki ureja informacijsko varnost

Besedilo načrtovanih sprememb v ZINFV-1:

67. člen
(sprememba Zakona o varstvu osebnih podatkov)

V Zakonu o varstvu osebnih podatkov (Uradni list RS, št. 163/22) se v 23. členu v prvem odstavku besedilo »o varnostnih zahtevah in priglasitvi incidentov iz« spremeni v »o ukrepih za obvladovanje tveganj in priglasitvi incidentov iz IV. poglavja«, besedilo »izvajalce bistvenih storitev« pa se nadomesti z besedilom »bistvene subjekte«.

(Verjetno) velja od sprejema ZINFV-1 dalje: maj/junij 2025:

- *se smiselno uporabljajo določbe o ukrepih za obvladovanje tveganj in priglasitvi incidentov iz IV. Poglavja zakona ki ureja informacijsko varnost, ki se nanašajo na bistvene subjekte, če upravljavec glede teh obdelav ni dolžan izvajati ukrepov po zakonu, ki ureja informacijsko varnost.*

Dokumentacija po predlogu ZInfV-1

1. Politika varnosti informacijskih sistemov
2. Popis sredstev in upravljavcev
3. Analiza tveganj z metodologijo
4. Načrt neprekinjenega poslovanja
5. Načrt obnovitve delovanja
6. Načrt odzivanja na incidente (SI-CERT oz CSIRT)
7. Načrt varnostnih ukrepov – CIA (celovitost, zaupnost, razpoložljivost)
8. Politika presoje učinkovitosti ukrepov

Ukrepi po 23. členu predloga ZInfV-1

1. Podpora vodstva in vključitev varnosti v letne načrte.
2. Zagotavljanje integritete kadrov (pred, med in po zaposlitvi).
3. Osnovne prakse kibernetske higiene in usposabljanje.
4. Varnost človeških virov, upravljanje dostopov in identitet.
5. Izvajanje in upravljanje varnostnih kopij podatkov.
6. Dnevniški zapisi o delovanju sistemov.
7. Upravljanje omrežnih in informacijskih sistemov z določeno odgovornostjo.
8. Politike in postopki glede kriptografije in šifriranja.
9. Upravljanje prometa in komunikacij.
10. Varnost dobavne verige in zahteve do ključnih dobaviteljev.
11. Fizično in tehnično varovanje prostorov in dostopov.
12. Varnost aplikacij, vključno z razvojem, vzdrževanjem in razkrivanjem ranljivosti.
13. Upravljanje in preprečevanje izrab tehničnih ranljivosti.
14. Zaščita pred zlonamerno kodo, zaznavanje in preprečevanje incidentov.
15. Uporaba večfaktorske ali neprekinjene avtentikacije.
16. Varne komunikacije (glasovne, video, besedilne) in sistemi za nujne primere.
17. Politike in postopki za uporabo oblačnih storitev.

1. Podpora vodstva in vključitev varnosti v letne načrte

3. Osnovne prakse kibernetske higiene in usposabljanje

2. Integriteta kadrov pred, med in po zaposlitvi

4. Preverjanje identitete, ravni dostopov, upravljanje pooblastil

15. Večfaktorska ali neprekinjena avtentikacija

5. Varnostne kopije podatkov

6. Dnevniški zapisi

12. Varnost aplikacij, razvoj, vzdrževanje, ranljivosti

7. Upravljanje omrežij in informacijskih sistemov z jasno odgovornostjo

11. Fizična in tehnična zaščita prostorov in dostopov

14. Zaščita pred zlonamerno programsko kodo, zaznavanje vdorov

8. Politike in postopki glede kriptografije in šifriranja

9. Upravljanje prometa in komunikacij

16. Varne komunikacije in sistemi za nujne primere

10. Varnost dobavne verige in zahteve do dobaviteljev

13. Upravljanje in preprečevanje izrab tehničnih ranljivosti

17. Politike in postopki za uporabo oblačnih storitev

Priglašanje pomembnih incidentov

- **Zavezanci in obveznosti**
  - Bistveni in pomembni subjekti morajo **nemudoma** priglasiti vse pomembne incidente pristojni skupini **CSIRT.**
- **Slovenski nacionalni CSIRT**
  - **SI-CERT (deluje pod Arnesom)**
  - **Državni CSIRT, ki deluje v okviru Urad Vlade RS za informacijsko varnost**
- **Posebna pozornost**: čezmejni ali medsektorski incidenti zahtevajo obveščanje **enotne kontaktne točke**.

Časovni okvir in poročanje

- **V 24 urah** po zaznavi: zgodnje sporočilo z osnovnimi podatki o incidentu, morebitni zlonamernosti in čezmejnem vplivu.
- **V 72 urah**: priglasitev incidenta z začetno oceno vpliva, resnosti in indikatorji ogroženosti.
- **Po potrebi**: vmesno poročilo (na zahtevo CSIRT).
- **V 1 mesecu**: končno poročilo z opisom incidenta, vzroki, ukrepi in čezmejnimi posledicami.
- **Če incident traja**: poročilo o napredku in končno poročilo najpozneje mesec po razrešitvi.

GAP analize s področja informacijske varnosti

- **Kaj nas je zanimalo?**
- Kako zrelo je podjetje pri zagotavljanju zahtev iz predloga Zakona o informacijski varnosti (ZInfV-1):
  - Dokumentacija
  - Varnostni ukrepi
- Ali obstaja ustrezna dokumentacija in praksa?
- Kakšna je dejanska stopnja skladnosti?
- Kje so vrzeli med zahtevami zakonodaje in realnostjo?
- **Metodologija**: zbiranje informacij, intervjuji, razgovori, tehnike opazovanja in analize, odgovarjanje na vprašalnike, pregled dokumentacije.

Vključena podjetja

- Več 10 podjetij
- Področja: zdravstvo in gospodarstvo
- Število zaposlenih: med 60 in 800
- Letni promet v 2023: med 4 in 78,4 mio
- Bilančna vsota v 2023: med 4,3 in 74,4 mio

Metoda ocenjevanja

Status	Ocena	Pomen
Neobstoječe	1	Popolno pomanjkanje prepoznavne zahteve, politike, postopka, nadzora dokumentacije ipd.
Začetno	2	Razvoj se je začel in za izpolnitev zahteve je potrebno še veliko truda (časa/sredstev).
Omejeno	3	Zahteva se izvaja in napreduje, vendar še ni dokončana.
Definirano	4	Razvoj zahteve je bolj ali manj dokončan, čeprav manjkajo podrobnosti in/ali se še ne izvaja v celoti, uveljavlja in/ali ga najvišje vodstvo še ne podpira aktivno.
Urejeno	5	Razvoj je končan, postopek/nadzor je bil izveden in pred kratkim vpeljan.
Optimizirano	6	Zahteva je v celoti izpolnjena, deluje v celoti, kot je bilo pričakovano, je dokumentirana in se aktivno spremlja ter izboljšuje, kar je mogoče dokazati z revizijo.
Se ne uporablja	0	Določena zahteva za organizacijo ni relevantna in se zato ne uporablja. Organizacija mora utemeljiti zakaj zahteva ni relevantna.

Številčno ocenjevanje

- Področjem smo po lastni presoji dodali uteži: 1, 1,5 in 2.
- Končni izračun smo prilagodili na standardno lestvico od 1 do 5.
  - 1 – Neustrezno (visoko tveganje)
  - 2 – Osnovna skladnost, večje vrzeli
  - 3 – Delna skladnost, možne izboljšave
  - 4 – Zadovoljiva skladnost, nekaj šibkosti
  - 5 – Visoka skladnost, zrel sistem

- **Končni izračun GAP analiz izbranih podjetij:**

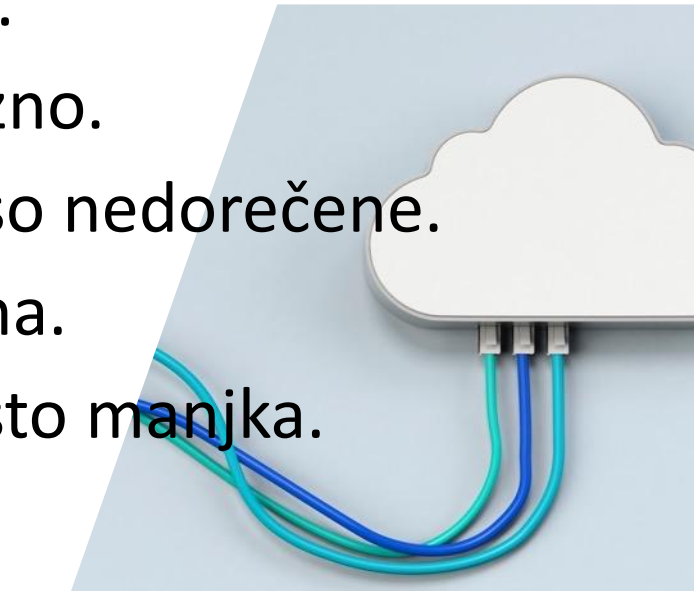
ocena med 1,5 in 3,7

Ključne ugotovitve 1/2

- Popisi informacijskih sredstev so pogosto nepopolni ali zastareli.
- Analiza tveganj ni sistematična in redko dokumentirana.
- Sprejemljiva raven tveganja večinoma ni določena.
- Načrti za neprekinjeno poslovanje so redki ali neobstoječi.
- Postopki za obnovo sistemov niso formalizirani ali testirani.
- Načrti odzivanja na incidente so pomanjkljivi ali improvizirani.
- Obveščanje CSIRT ni jasno opredeljeno v večini organizacij.

Ključne ugotovitve 2/2

- Varnostni ukrepi se izvajajo brez celovitega načrta.
- Vodstvo ni aktivno vključeno v področje informacijske varnosti.
- Upravljanje dostopov ni enotno ali formalno urejeno.
- Usposabljanje zaposlenih je pomanjkljivo ali neobvezno.
- Politike varnostnega kopiranja pogosto manjkajo ali so nedorečene.
- Centralizirano upravljanje dnevniških zapisov je izjema.
- Uporaba MFA je delna in dokumentacija o njej pogosto manjka.



Več informacij

- Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) je objavil Priročnik kibernetske varnosti (priročnik), ki ponuja ključne smernice in priporočila za zaščito informacijskih sistemov pred kibernetskimi grožnjami.

- https://www.gov.si/assets/vladne-sluzbe/URSIV/Datoteke/Prirocnik-kibernetske-varnosti.pdf


AI

Vaša vprašanja in komentarji

benjamin@datainfo.si
02 620 43 00