AR-IN-A BOX

Awareness Game

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

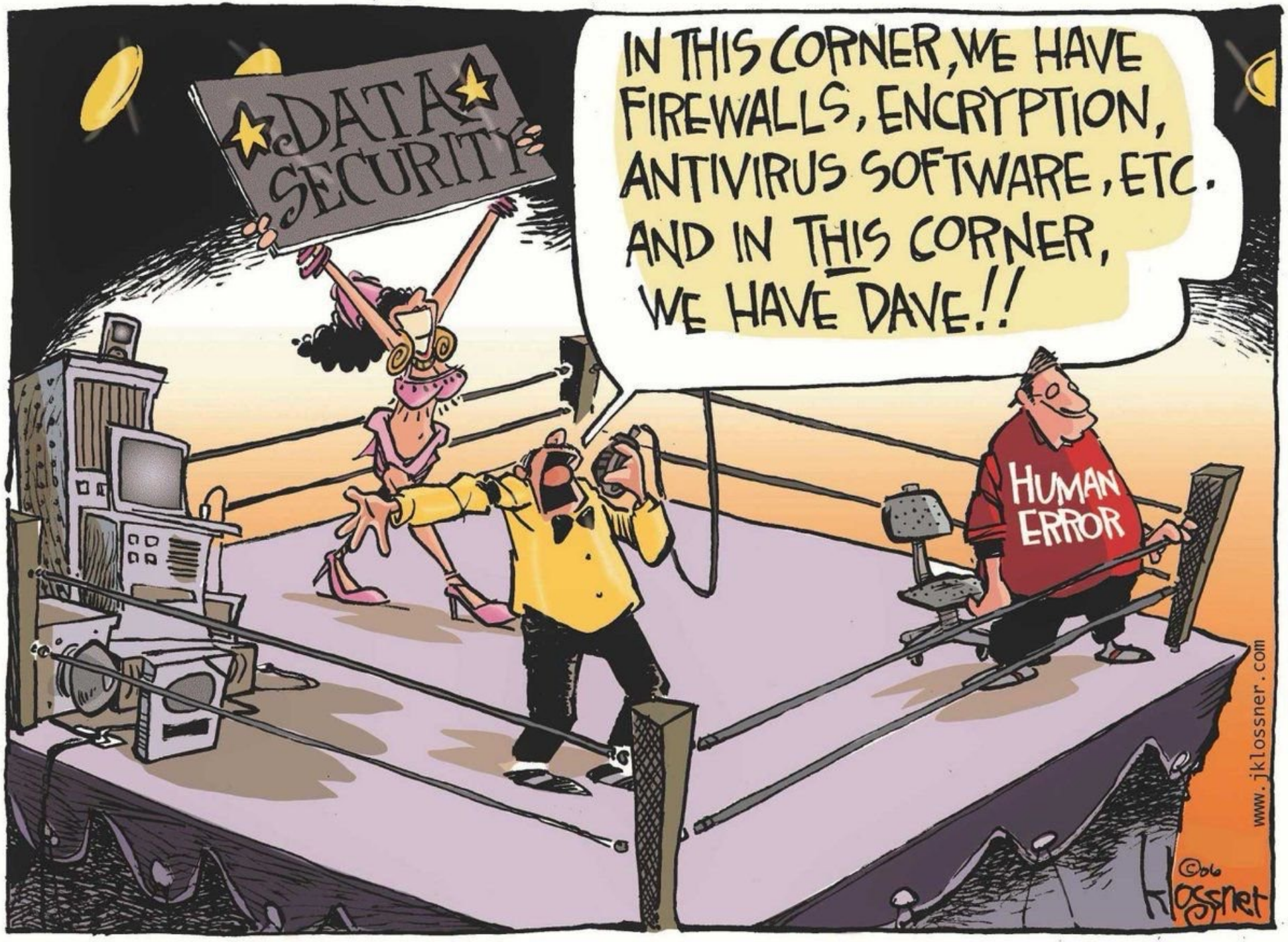
Kiberdrošības izmeklēšanas spēle – iespēja darbinieku izglītošanā

NEESI VĀJĀKAIS ĶĒDES POSMS
APTURI UZBRUKUMU

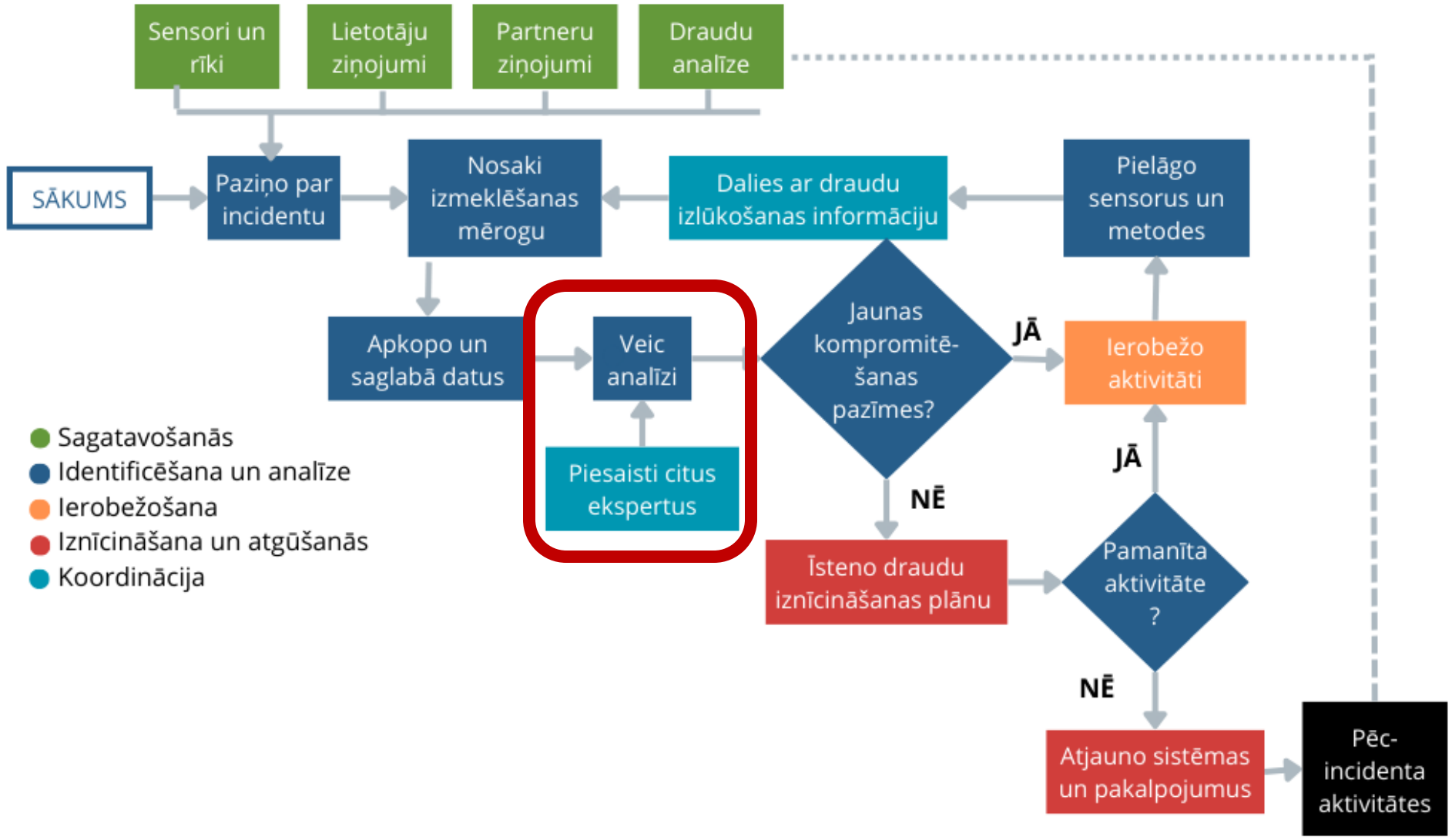
GALDA MĀCĪBAS UN SPĒLES DARBINIEKU IZGLĪTOŠANĀ

Iespējamie uzdevumi

- Pārbaudīt procedūras (*playbooks*)
- Izveidot/ pārbaudīt komunikācijas procesus un koordināciju
- Vairot izpratni par kiberdrošību (*awareness*)
- Attīstīt zināšanas un prasmes
- Wargaming (Blue Team vs Red team)


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06
Klossner

IZMEKLĒŠANAS SPĒLES IETVARS



IZMEKLĒŠANAS SPĒLES UZDEVUMI

- Vairot izpratni par kiberdrošības draudiem
  - sociālā inženierija
  - izspiedējvīrusi
  - datu šifrēšana
  - kompromitēti konti
- Iepazīstināt auditoriju ar izmeklēšanas principiem
  - saglabāto datu nozīme
  - datu korelācija
  - cēloņu un motivācijas noskaidrošana
- Pārrunāt kiberuzbrukuma ietekmi uz
  - uzņēmuma darbību
  - reputāciju (dezinformācija)

SCENĀRIJS – KIBERUZBRUKUMS «MEGACORP»

Vadošais internetveikals «MegaCorp» cietis kiberuzbrukumā.

Šķiet, ka uzbrucēji sākotnējo piekļuvi ieguvuši, izmantojot PIKŠĶERĒŠANU.
Vēl ļaunāk – «MegaCorp» galvenajā ofisā konstatēta NESANKCIONĒTA PIEKĻUVE, un tajā pat dienā uzņēmums cietis no IZPIEDĒJPROGRAMMATŪRAS uzbrukuma. Internetā parādījusies arī DEZINFORMĀCIJA , nodarot lielu kaitējumu «MegaCorp» reputācijai.

Jūs esat Kiberdrošības izmeklētāju komanda, kas nolīgta, lai noskaidrotu, kas veicis ielaušanos, un mēģinātu uzbrucēju apturēt, pirms ir par vēlu. Mēs esam apkopojuši pēc iespējas vairāk informācijas. Izanalizējiet to, cik ātri vien iespējams!

Jums ir maksimums 45 minūtes laika, pirms visi dati tiks izdzēsti.
Lai veicas!

MEGACORP

Spēles noteikumi

- ✓ Izveidojiet 5 -7 cilvēku komandas
- ✓ Izvēlieties komandas vadītāju
- ✓ Sašķirojiet un sadaliet uzdevumus, balstoties uz krāsu kodiem
- ✓ Analizējiet incidentu (izveidojot laika līniju, meklējot anomālijas utt.)
- ✓ Aizpildiet atbildes lapu, lai uzlauztu kodu
- ✓ Atbildiet uz jautājumiem par
  - ✓ uzbrucēja identitāti un motivāciju
  - ✓ uzņēmuma atbildi uz kiberuzbrukumu
- ✓ Spēles laiks: 45 minūtes

ATBILDES LAPA

Kas ir pirmais PIKŠĶERĒŠANAS uzbrukumā cietušais?

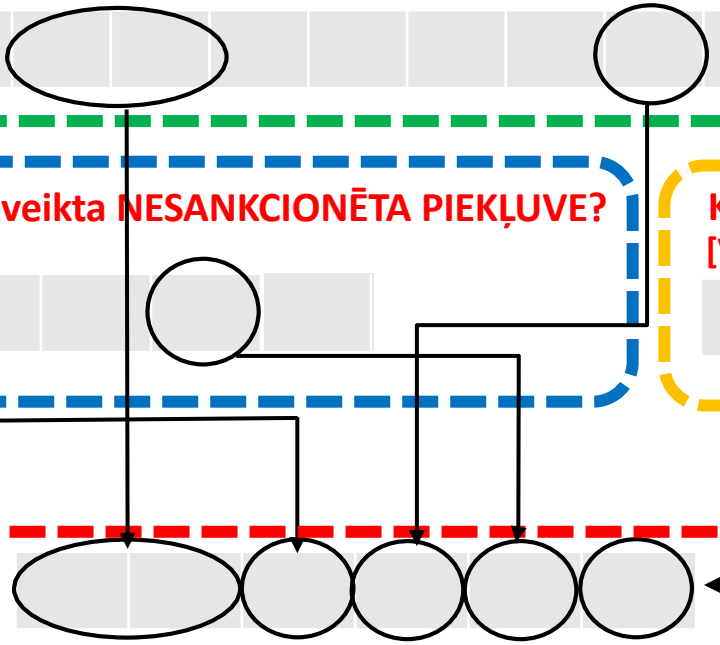
[Uzvārds, Vārds – kā norādīts apliecībā – ar atstarpi*]

Ar kuru apliecību tika veikta NESANKCIONĒTA PIEKĻUVE?

[Apliecības nr*]

Kura MEGACORP darbinieka sociālo mediju konts ir uzlauzts?

[Vārds uzvārds (nevis @nickname) kā rakstīts treknrakstā – bez atstarpēm*]



ŠIFRA ATSLĒGA:

Kāds ir atšifrētā faila nosaukums?

SOCIĀLIE MEDIJI

MonikaDvine
April 2 2022 at 01:00 pm ·

MEGACORP aicina savā komandā IT Speciālistu ar bakalaura vai maģistra grādu IT jomā.

Jums būs iespēja strādāt pie biznesa lietotājprogrammu izstrādes, kas pielāgotas mūsu darbībai.

Atbildība:
-WEB aplikāciju projektēšana, izstrāde, dizains.
-Sadarbošanās ar komandu problēmsituāciju risināšanā.

Kvalifikācija:
- Bakalaura vai maģistra grāds datorzinātnēs vai saistītā jomā
-Pašiniciatīva
-Prasme darbā ar NET Framework, MVC arhitektūru, C#, Azure Databases/SQL Server, Git/Github

AnnaManna and 400 Others 124 Comments

Like Comment Share

IlgonisValis
April 2 2022 at 02:03 pm ·

MEGACORP ir uz attīstību orientēts, moderns uzņēmums, kam rūp kiberdrošība, tāpēc aicinām Tevi - jaunu, spējīgu, talantīgu IT speciālistu - nāc strādā pie mums! #teirdarbs

MonikaDvine and 100 Others 124 Comments

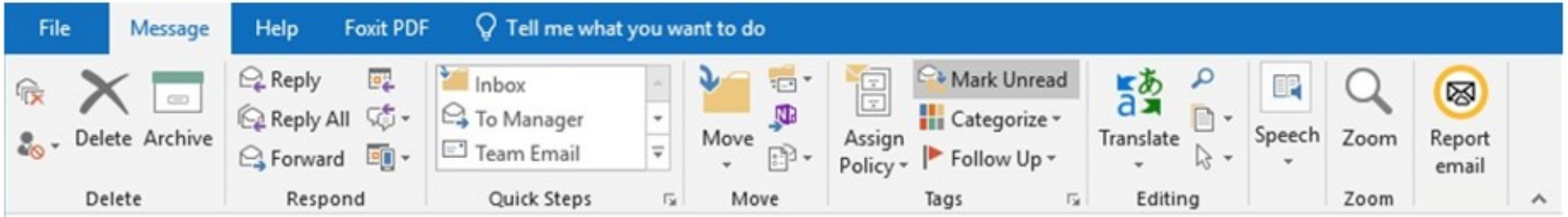
Like Comment Share

MiglaineAnna
@AnnijaM

Mēs, cilvēki, esam lielākie dabas ienaidnieki. Cik koku ir nocirsti, lai mēs varētu izdrukāt savus neskaitāmos dokumentus. Jā, arī es esmu pie vainas. Tomēr ceru, ka mēs varam laboties! #savetheplane t#iestadioku

12:00 PM · Apr 6, 2022

AIZDOMĪGS E-PASTS



09.04.2022 12:08 PM

MA MIGLAINE Anna (Finanšu kontroliere)

Saudzēsim dabu!

To Visi

Cc

Labdien, kolēģi!

Vēlos atgādināt, ka rīt plānojam sanāksmi par pirmo triju mēnešu finanšu rādītājiem.
Ziņojums pieejams šeit: https://intranet.megacorp.lv/zinojumi/012022

Ar sveicieniem,
Anna

MEGACORP

Ofiss
Labrīta iela 438/2
170 Nekurzeme
www.megacorp.lv

Seko mums:

PIEKĻUVES KODI 09.04.22 (0830-0930)

KARTES NR	Uzvārds, vārds	Lasītājs	Datums	Laiks
DS21NM9	Stiprais Ludis	831	09.04.2022	8:30
FA23UB1	Miglaine Anna	831	09.04.2022	8:31
IT23RL2	Negudris Juris	831	09.04.2022	8:38
AL3XZA4	Visspiedis Ivo	831	09.04.2022	9:00
DS21NM9	Stiprais Ludis	833	09.04.2022	9:03
IT21NO6	Melnis Didzis	831	09.04.2022	9:05

MEGACORP darbiniekiem jāreģistrē kartes, ienākot un izejot no ēkas (ieejas/izejas durvis),

bet durvīm uz paaugstinātas drošības zonu (832, 833) tiek reģistrēta tikai ieeja.

ATBILDIET UZ JAUTĀJUMIEM

1. Kā jūs nonācāt pie secinājuma, kurš ir veicis kibernoziegumu? Kāds bija uzbrucēja motīvs?
2. Kā tika uzlauzts uzņēmuma darbinieka sociālo mediju konts? Ko šajā situācijā darīt?
3. Kā būtu jārīkojas uzņēmumam, ja nav bijis iespējams atšifrēt datus? Kādos gadījumos jāapsver iespēja maksāt izspiedējam?

Jautājumi?

daina.ozolina@cert.lv