

WEBINAR

Sulmet kibernetike, Vektoret e sulmeve dhe mbrojtja ndaj tyre





Ilir Daka

Specialist i Sigurise Kibernetike

Autoriteti Kombetar per Sigurine Kibernetike

14 vjet ne IT dhe Siguri Kibernetike

- Telekomunikacion
- Real Estate
- Sigurime
- Trajner ne Rrjeta Kompjuterike



<https://www.linkedin.com/in/idaka/>



Çfarë është një sulm kibernetik?

Një veprim me qëllim të keq për të dëmtuar, ndërhyrë ose marrë të dhëna në mënyrë jo ligjitime nga një sistem kompjuterik.

1 sulm kibernetik cdo 29 sekonda



Llojet e Sulmeve Kibernetike



Malware



Phishing



Ransomware



Denial of Service



Man in the Middle



Cryptojacking



SQL Injection



Exploits

Sulmet “Phishing”

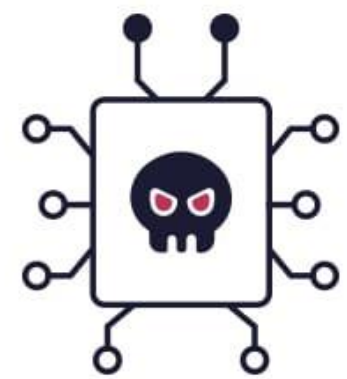
- Teknikë mashtrimi që përdor email ose mesazhe të rreme për të vjedhur informacione sensitive.





Sulmet “Malware”

Program keqdashës që infektion dhe në disa raste dëmton sistemet kompjuterike



VIRUS
Spreads between computers



WORM
Spreads between computers in one company or location



TROJAN
Sneaks malware onto your computer



SPYWARE
Steals your data



ADWARE
Spams you with ads



RANSOMWARE
Encrypts files and blackmails you



FILELESS MALWARE
Operates in your system's memory



ROOTKIT
Gives remote access to your device



BOTNET
Turns your PC into a puppet



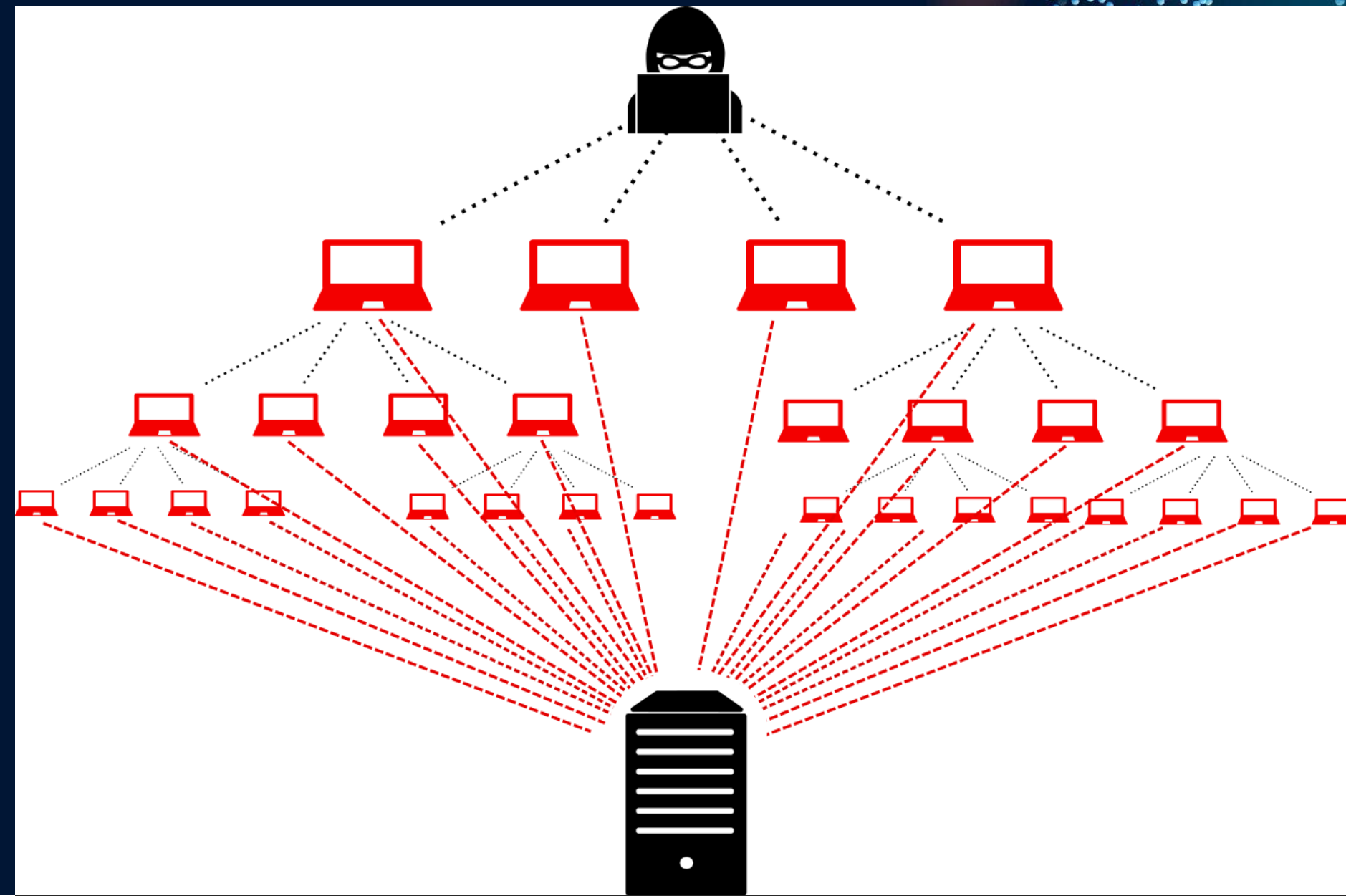
KEYLOGGER
Records user activity



Sulmet “DDoS”

Sulme te cilat realizohen me qellim bllokimin e disponueshmerise se nje sistemi.

Realizohet duke perdorur shume njesi kompjuterike njekoheisht, te cilat dergojne kerkesa drejt te njejtit sherbim/server.

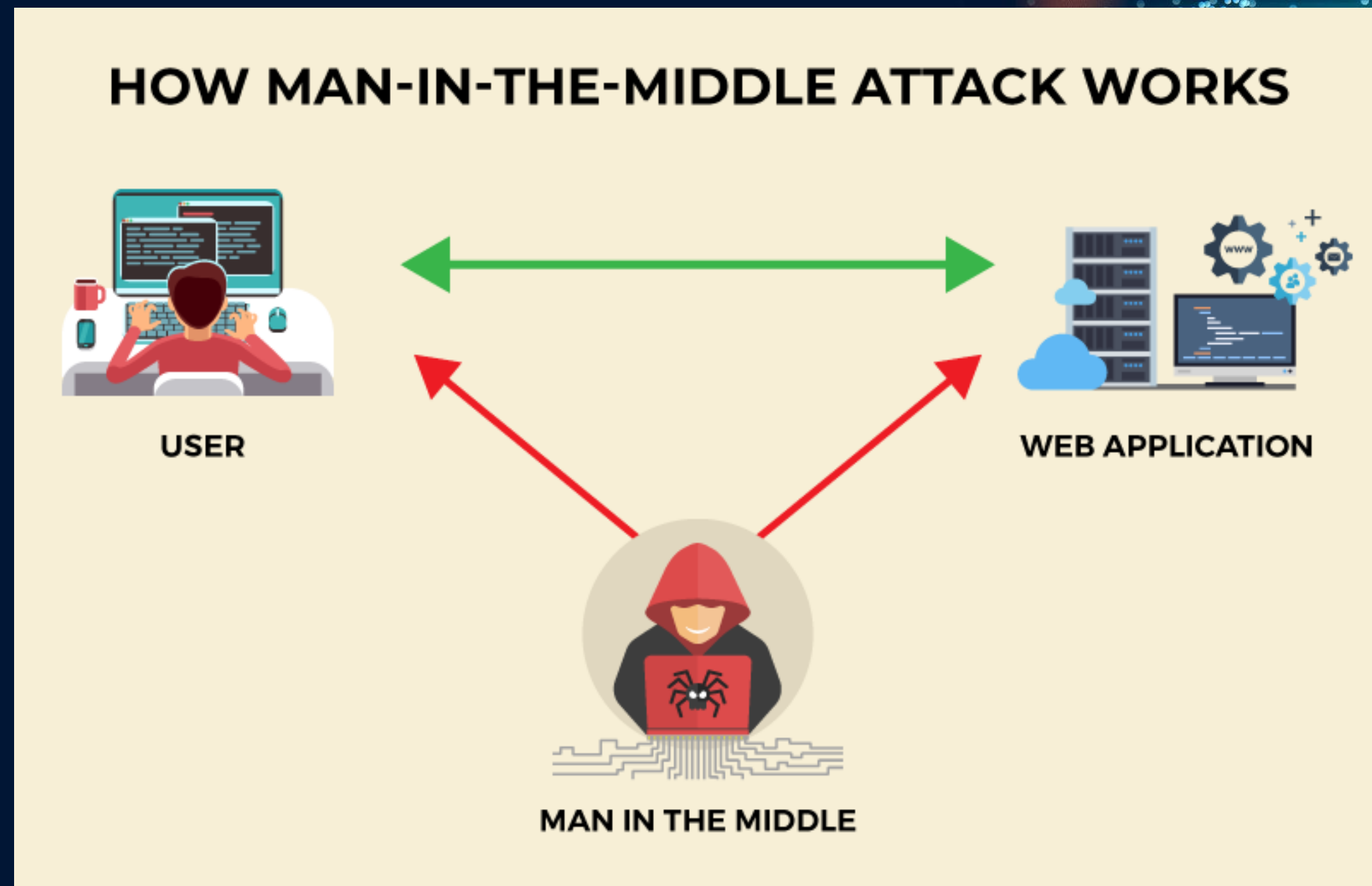




Sulmet “Man-in-the-Middle (MitM)”

Sulme te cilat realizohen kur nje “Hacker” futet ne mes te komunikimit legjitim, me qellim manipulimin apo vjedhjen e te dhenave.

Krysisht shikohet ne rrjetet publike te WiFi





Sulmet “Ransomware”

Një ransomware është një lloj malware (software malinj) që enkripton ose bllokton aksesin në të dhënat e një kompjuteri, rrjeti ose pajisje tjetër digjitale, duke kërkuar një shpërblim për të kthyer qasjen.

DarkoderCrypt0r

Your Files has been Encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday. Once the payment is checked, you can start decrypting your files immediately.

Contact
If you need our assistance, send a message by clicking <Contact Us>.

We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!

TIME TO PAYMENT RELEASE:
3 DAYS

TIME TO LOST YOUR ARCHIVES:
5 DAYS

Send \$300 worth of bitcoin to this address:
1KoWzXydNnrRfu2mcSbY6n7mnevkvQ6WBU **COPY**

BITCOIN ACCEPTED HERE!

CHECK PAYMENT **DECRYPT**



Vektoret e Sulmeve - Inxhinieria Sociale

Inxhinieria sociale është një teknikë manipulimi psikologjik që përdor ndikimin njerëzor për të mashtuar njerëzit në të dhënien e informacionit konfidencial ose për të kryer veprime të caktuara. Në thelb, është art i të bindurit dikujt të bëjë diçka që ata normalisht nuk do të bënin.



Vektoret e Sulmeve - E-mail dhe Phishing

E-maili ka qenë dhe vazhdon të jetë një nga kanalet kryesorë për sulmuesit kibernetikë për të depërtuar në sistemet kompjuterike dhe rrjetet. Përmes e-mail-eve, ata mund të shpërndajnë malware, të kryejnë sulme phishing, dhe të vjedhin informacion sensitiv.





Vektoret e Sulmeve - Rrjetet e Pambrojtura dhe IoT

Me rritjen e ndërlidhjes së pajisjeve dhe zgjerimin e Internet of Things (IoT), rrjetet e pambrojtura dhe pajisjet IoT janë bërë një nga vektorët më të mëdhenj të sulmeve kibernetike.

- Rrjetet e pambrojtura janë ato që nuk kanë implemente një nivel të mjaftueshëm të sigurisë kibernetike. Këto rrjete janë shpesh të ekspozuara në internet dhe mund të sulmohen lehtësisht nga hakerët.
- Internet of Things (IoT) përfshin një gamë të gjerë pajisjesh të lidhura me internetin, nga termostatet e inteligjente deri në kamerat e sigurisë. Këto pajisje shpesh kanë të meta të sigurisë dhe mund të shfrytëzohen nga hakerët për të hyrë në rrjete më të mëdha.



Vektoret e Sulmeve - Vulnerabilitetet e Softuerëve

Vulnerabilitetet e softuerëve janë një nga shkaqet kryesore të komprometimit të sistemeve kompjuterike. Këto janë dobësi të identifikuara në softuer që mund të shfrytëzohen nga sulmuesit për të fituar akses të paautorizuar në sistemet e kompjuterit.

•Ideologji: Besimi në një shkak më të madh (p.sh., aktivistë politikë).

•Kuriozitet: Dëshira për të eksploruar sistemet e organizatës.

Vektoret e Sulmeve - Burimet e Brendshme (Insider Threat)



Një nga kërcënimet më të nënvlerësuara për sigurinë kibernetike është ai që vjen nga brenda një organizate: burimet e brendshme ose insider threat. Këto janë individë që kanë akses legjitim në sistemet dhe të dhënat e një organizate, por që i përdorin ato për qëllime të paautorizuara.

Fitim financiar: Shitja e të dhënave konfidenciale, shantazhi.

Hakmarrje: Për shkak të një mospajtimi me organizatën.

Ideologji: Besimi në një shkak më të madh (p.sh., aktivistë politikë).

Kuriozitet: Dëshira për të eksploruar sistemet e organizatës.

Mbrojtja ndaj Sulmeve Kibernetike - Praktikat më të Mira



- Edukimi i stafit të kompanise/institucionit për të lajmeruar departamentet perkatëse nëse ka dyshime për “Inxhinjeri Sociale”
- Edukimi i stafit të kompanise/institucionit për të njohur dhe kuptuar e-mailet jo legjitime.
- Përdorimi i Antiviruseve të përditësuar dhe me licensa legjitime.
- Përditësimi i programeve dhe sistemeve operative në kompjuterat tuaja.
- Përdorimi i rrjeve VPN.
- Përdorimi i fjalekalimeve të gjata dhe komplekse.
- Përdorimi i faktoreve shtesë të aksesit në llogarite tuaja.
- Përdorimi i kopjeve të sigurta të informacioneve apo të dhënave tuaja të rëndësishme.

Mbrojtja ndaj Sulmeve Kibernetike - Praktikat më të Mira



- Perdorimi i filtrave të avancuar për detektimin e emailve jo legjitime.
- Skedulimi i rregullt i kopjeve rezerve të të dhënave (Backup).
- Perdorimi i pajisjeve të avancuara mbrojtëse të rrjetit (Next Generation Firewall).
- Perdorimi i teknikave të zbutjes së sulmeve DDoS.
- Enkriptimi i të dhënave.
- Testimi here pas here i programeve apo sistemeve që përdorni për “vulnerabilitete”.
- Vendosja e fjalëkalimeve të kompleksë për pajisjet që përdorim në rrjetet tona.
- Përditësim i vazhdueshëm i Firmwareve të pajisjeve IoT.
- Implementim i politikave të qarta të sigurisë në organizatë.
- Monitorim i vazhdueshëm dhe auditim i aktivitetit të brendshëm.

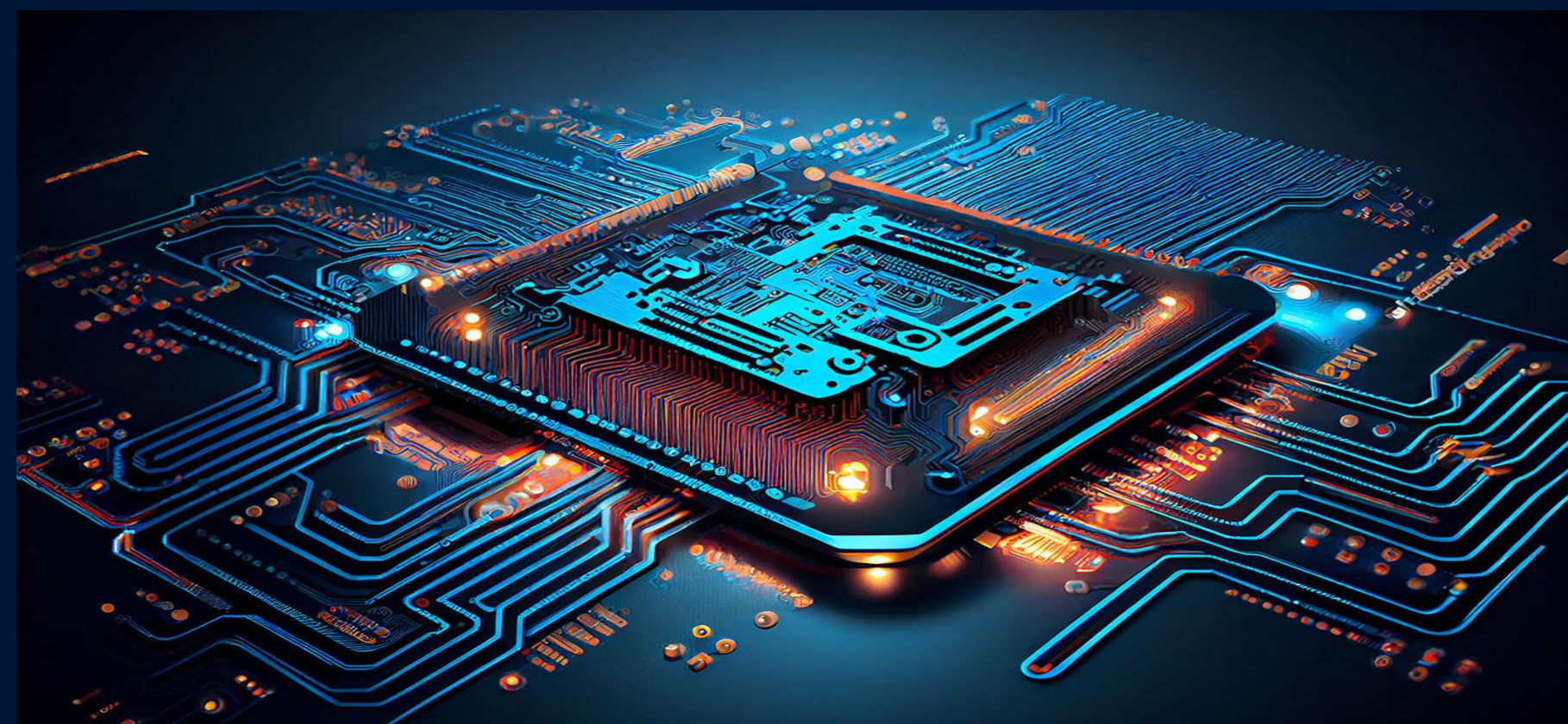
Te rejat e Teknologjise dhe Sigurise



ITELIGJENCA ARTIFICIALE



QUANTUM COMPUTING



PYETJE



<https://aksk.gov.al/>



<https://www.facebook.com/aksk.gov.al>



<https://www.instagram.com/aksk.gov.al/>



<https://www.linkedin.com/company/aksk-gov-al/>





Faleminderit Qendroni te Sigurte