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

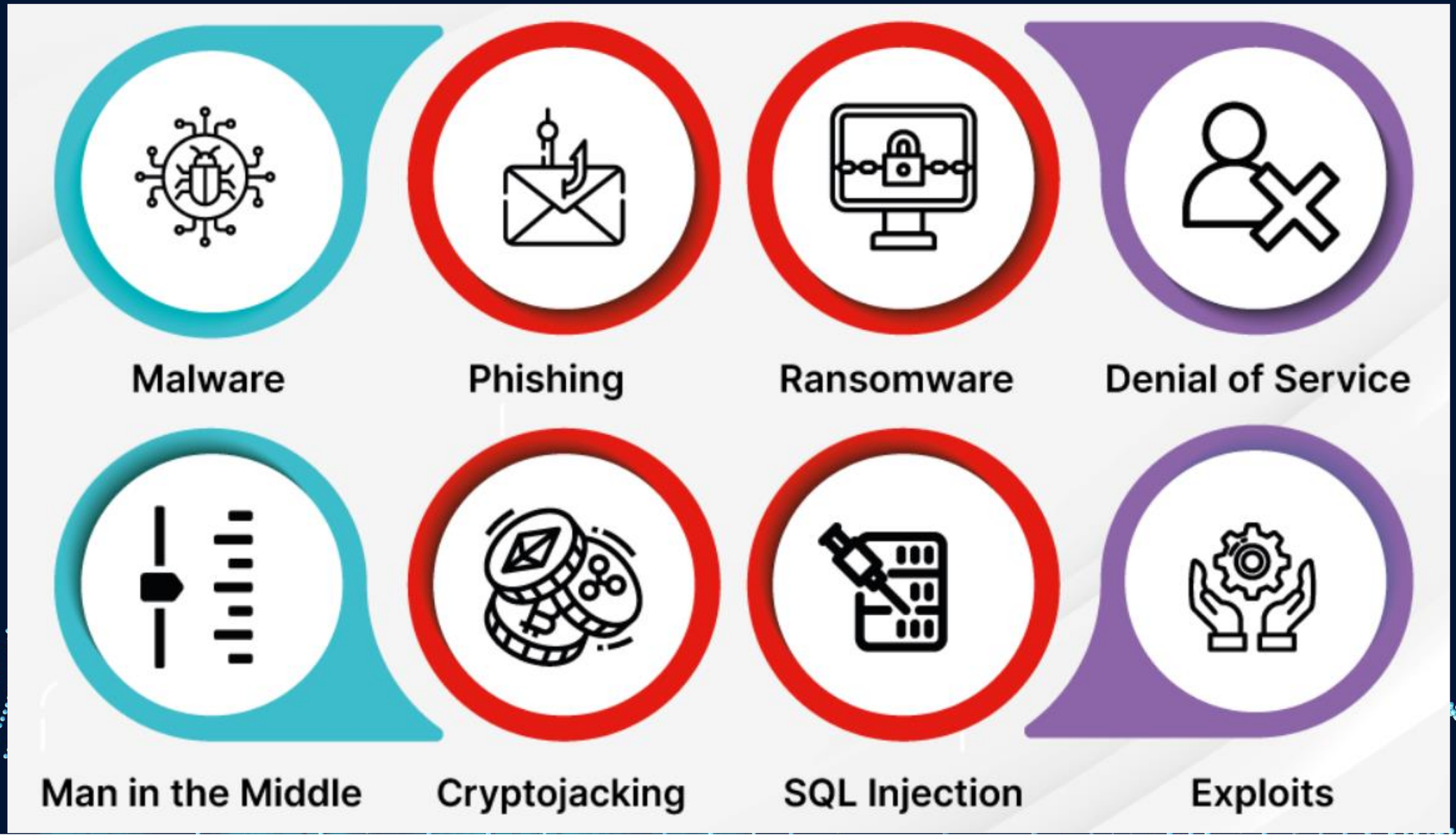
https://www.linkedin.com/in/idaka/

Çfarë është një sulm kibernetik?

Një veprim me qëllim të keq për të dëmtuar, ndërhyrë ose mare të dhëna ne menyre jo ligjitime nga një sistem kompjuterik.

1 sulm kibernetik cdo 29 sekonda

Llojet e Sulmeve Kibernetike

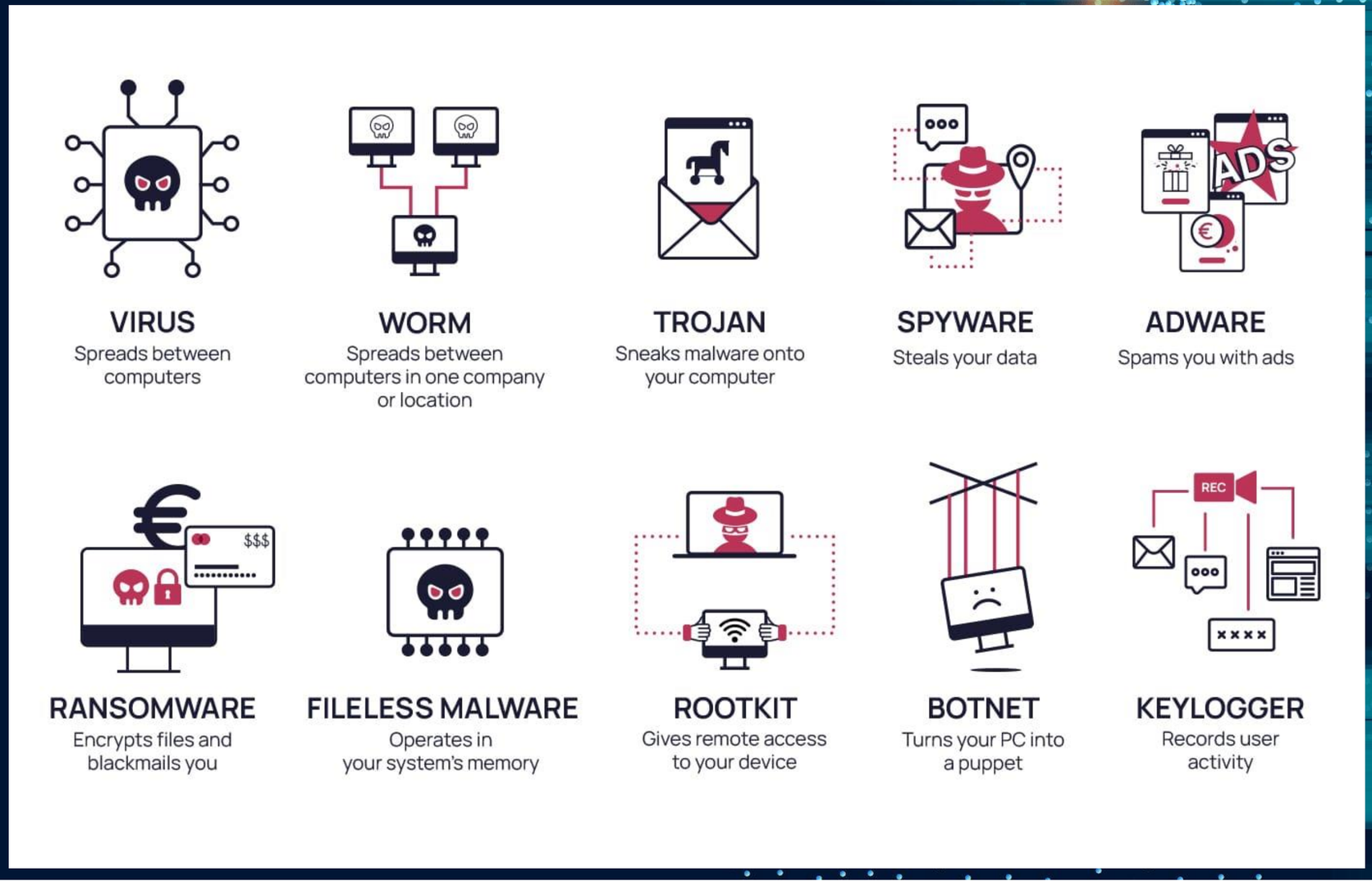


Sulmet “Phishing”

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

Sulmet “Malware”

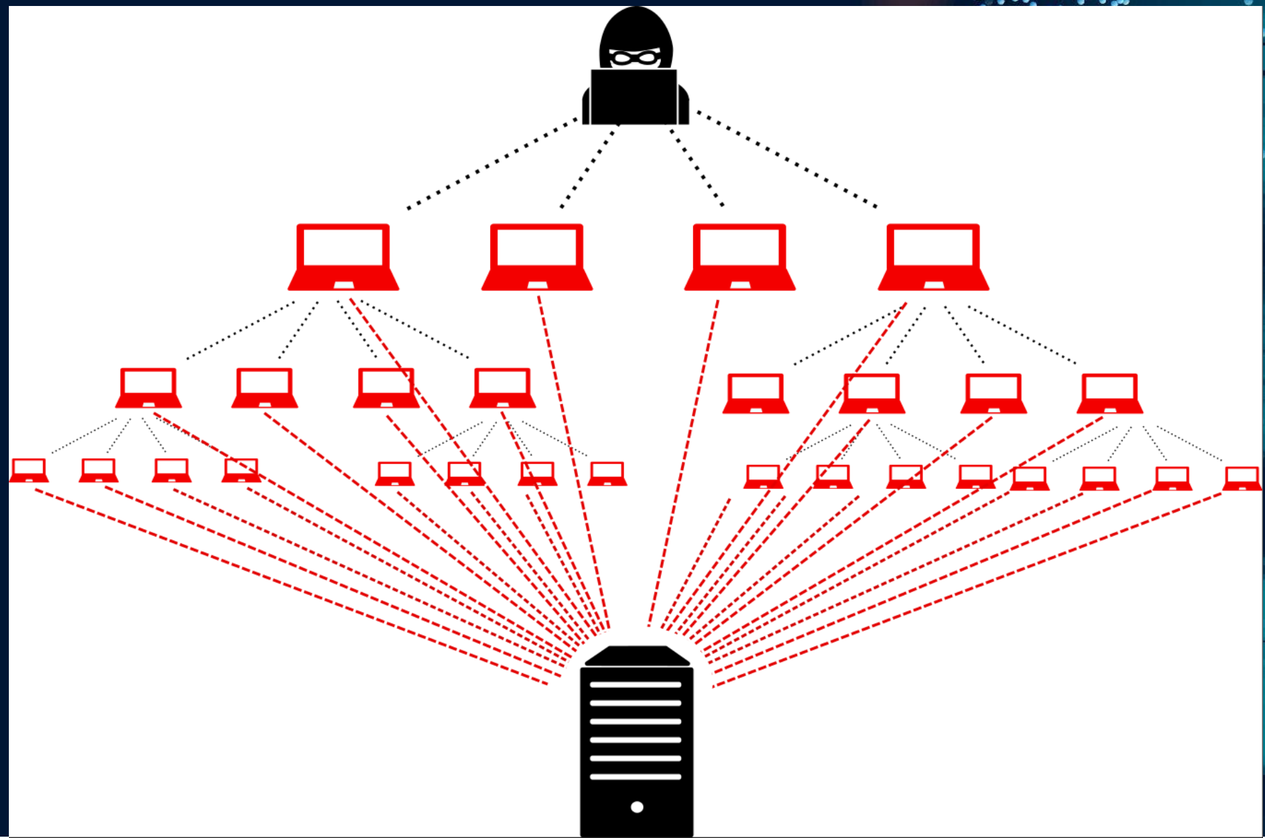
Program keqdashës që infekton dhe ne disa raste dëmton sistemet kompjuterike



Sulmet “DDoS”

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

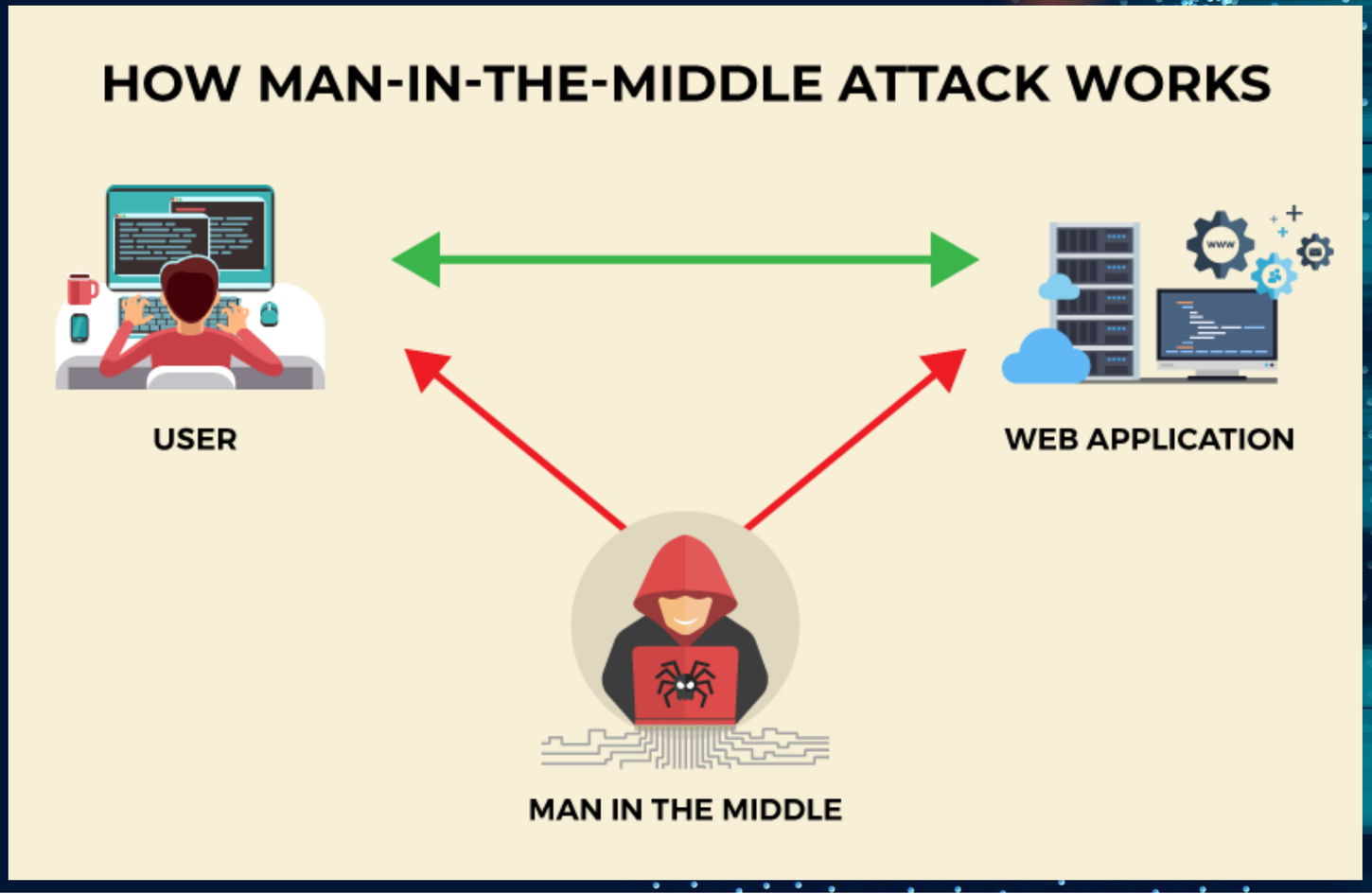
Realizohet duke perdorur shume njesi kompjuterike njekohesisht, te cilat dergojne kerkesa drejt te njejtit sherbim/server.



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 bllokon aksesin në të dhënat e një kompjuteri, rrjeti ose pajisje tjetër digjitale, duke kërkuar një shpërblim për të kthyer qasjen.

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 kompromet imit 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.

Vektorët 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 te kompanise/institucionit per te lajmeruar departamentet perkatese nese ka dyshime per “Inxhinjeri Sociale”
- Edukimi i stafit te kompanise/institucionit per te njohur dhe kuptuar e-mailet jo legjitime.
- Perdorimi i Antiviruseve te perditesuar dhe me licensa legjitime.
- Perditesimi i programeve dhe sisteme operative ne kompjuterat tone.
- Perdorimi i rrjeve VPN.
- Perdorimi i fjalekalimeve te gjata dhe komplekse.
- Perdorimi i faktoreve shtese te aksesit ne llogarite tona.
- Perdorimi i kopjeve te sigurta te informacioneve apo te dhenave tona te rendesishme.

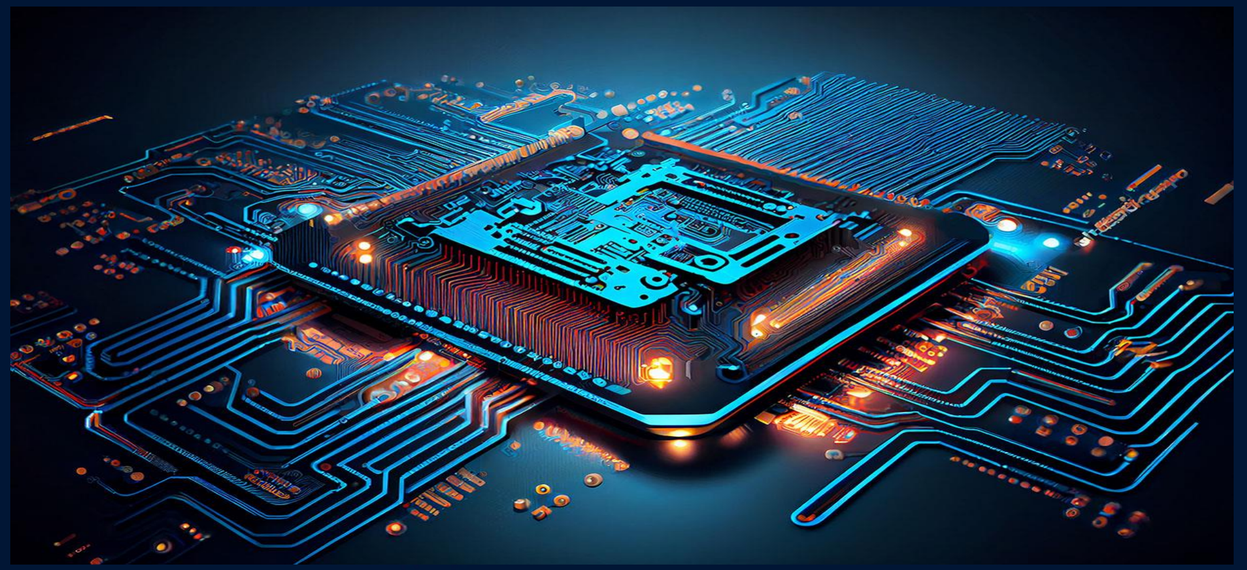
Mbrojtja ndaj Sulmeve Kibernetike - Praktikat më të Mira

- Perdorimi i filtrave te avancuar per detektimin e emaileve jo legjitime.
- Skedulimi i rregullt i kopjeve rezerve te te dhenave (Backup).
- Perdorimi i pajisve te avancuara mbrojtese te rrjetit (Next Generation Firewall).
- Perdorimi i teknikave te zbutjes se sulmeve DDoS.
- Enkriptimi i te dhenave.
- Testimi here pas here i programeve apo sistemeve qe perdorni per “vulnerabilitete”.
- Vendosja e fjalekalimeve te komplekse per pajisjet qe perdorim ne rrjetet tona.
- Perditesim i vazhdueshem i Firmwareve te pajisjeve IoT.
- Implementim i politikave te qarte te sigurise ne organizate.
- Monitorim i vazhdueshem dhe autitim i aktivitetit te brendshem.

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