

Cyber Ready Kosovo

Udhëzues për të Rinj në Sigurinë Kibernetike

Burimet

Ipsumus, L. R., & Dolor, S. A. (2021). Consequat Elit Sed Do Eiusmod: A Metaphysical Inquiry into Vitae Energetica. Loremia Academic Press.

Rreth nesh

Ne jemi një ekip i Chevening Cybersecurity Fellows nga e gjithë Ballkani. Fellows janë profesionistë me prejardhje të ndryshme në fushën e sigurisë kibernetike, nga ethical hacking dhe forenzika digjitale deri te menaxhimi i rrezikut, qeverisja dhe edukimi në siguri kibernetike.

Ky projekt, Cyber Ready Balkans, financohet nga Zyra e Jashtme, e Komonuelthit dhe e Zhvillimit e Mbretërisë së Bashkuar (FCDO) përmes Programit të Bursave Chevening. Ai lindi nga një mision i përbashkët: të lidhim rajonin, të ngushtojmë hendekun mes arsimit dhe mundësive, dhe t'i prezantojmë të rinjtë me botën e sigurisë kibernetike në një gjuhë që ata e kuptojnë.

Kemi parë nga afër se sa shumë studentë në Kosovë, Maqedoninë e Veriut dhe Mal të Zi kanë talent dhe kuriozitet, por jo udhëzimin apo qasjen e duhur për të hyrë në këtë fushë. Përmes këtij projekti, synojmë ta ndryshojmë këtë.

Përmbajtja

Shpjegimi i Sigurisë Kibernetike

KAPITULLI 1: Pse duhet të të interesojë01

KAPITULLI 2: Çfarë është Siguria Kibernetike07

- 1. Siguria kibernetike në një fjali
- 2. Çfarë ka nevojë për mbrojtje?
- 3. Trekëndëshi i Sigurisë Kibernetike (Triada CIA)
- 4. Çfarë nuk është siguria kibernetike
- 5. Kush punon në sigurinë kibernetike?
- 6. Ti tashmë po praktikon sigurinë kibernetike (deri diku)
- 7. Pse ka rëndësi (më shumë se kurrë)
- 8. Përmbledhje

KAPITULLI 3: Kush janë të mirët dhe të këqijtë12

- 1. Le të flasim për hakerat
- 2. Sistemi i kapelave
- 3. Tipat kriminalë
- 4. Të mirët në kibernetikë (rolet e kapelave të bardha)
- 5. Nuk është gjithmonë thjesht “E drejtë kundër të gabuarës”
- 6. Pra... Çfarë lloj hakeri do që ti të jesh?
- 7. Përmbledhje

KAPITULLI 4: Si ndodhin vërtet sulmet kibernetike19

- 1. Mjafton një klikim
- 2. Zinxhiri i vrasjes kibernetike (i thjeshtuar)
- 3. Shembull nga bota reale (i thjeshtuar)
- 4. Truku bonus: Pivotimi
- 5. Ata duan që ti ta bësh të lehtë
- 6. Përmbledhje: Si ndodhin sulmet

KAPITULLI 5: Llojet e Kërcënimeve Kibernetike (që do t'i shohësh vërtet)25

- 1. Phishing: Kurthi i mesazhit të rremë
- 2. Malware: Pushtuesi i qetë
- 3. Sulmet ndaj fjalëkalimeve: Lidhja jote më e dobët
- 4. Inxhinieria sociale: Të hakojnë ty, jo kompjuterin
- 5. Sulmet në Wi-Fi publik: Kurthi i internetit falas
- 6. Kapja e llogarive: Kur e humb kontrollin
- 7. Aplikacione, shkarkime dhe vegla të rreme: Kali i Trojës
- 8. Dezinformimi: Gënjeshttrat që përhapen si zjarri

KAPITULLI 6: Ku ndodh Siguria Kibernetike33

- 1. Është më e madhe se ç'mendon
- 2. Në shtëpi: Zona jote personale kibernetike
- 3. Në shkollë: Laboratorë për hakerë
- 4. Në punë: Edhe punët me gjysëm orari
- 5. Në publik: Kurthi i Wi-Fi falas
- 6. Në spitale: Sulmet kibernetike mund të vrasin
- 7. Në qeveri: Lufta e ftohtë kibernetike
- 8. Në infrastrukturën kritike: Fikja e dritave
- 9. Kudo që shkon ti
- 10. Përmbledhje: Siguria kibernetike është kudo

KAPITULLI 7: Çfarë bëjnë në të vërtetë profesionistët e sigurisë kibernetike41

- 1. Siguria Kibernetike është një Sport Ekipor
- 2. Mbrojtësit e Vijës së Parë
- 3. Hakerët Etikë
- 4. Ndërtuesit dhe Inxhinierët
- 5. Hetuesit
- 6. Udhëheqësit dhe Komunikuesit
- 7. Prisni: A duhet të jem gjeni i teknologjisë?
- 8. Ku ekzistojnë këto punë?
- 9. Përmbledhje: Gjej Rolin Tënd

KAPITULLI 8: A duhet të jesh gjeni ose programues? 49

1. Miti që i ndal njerëzit
2. Shumë role nuk kërkojnë programim
3. Njerëz të vërtetë, prapavija të vërteta
4. Po me certifikatat si qëndron puna?
5. Po mosha a ka rëndësi?
6. Si të fillosh pa programim
7. A duhet të mësosh programim eventualisht?
8. Përmbledhje: Jo, nuk ke pse të jesh gjeni ose programues

KAPITULLI 9: Siguria kibernetike = Fuqi, Kontroll dhe Liri 55

1. Siguria kibernetike nuk është vetëm mbrojtje
2. KONTROLL: Ti zotëron jetën tënde digjitale
3. FUQI: Ti kupton atë që të tjerët nuk e kuptojnë
4. LIRI: Lëviz pa frikë
5. Bonus: Mund t'i ndihmosh edhe të tjerët
6. Përmbledhje: Kjo është superfuqia jote

KAPITULLI 10: Si të fillosh të mendosh si një hacker (etikisht) 60

1. Hackerët e mirë mendojnë ndryshe
2. Mentaliteti i hackerit = Kuriozitet + Skepticizëm
3. Fillo nga e vogla: Analizo atë që përdor çdo ditë
4. Praktiko "Ndërgjegjësimin Digjital" çdo ditë
5. Përdor të njëjtat mjete si hackerët e vërtetë
6. Mëso të thyesh gjëra që të dish si t'i rregullosh
7. Hakim në mënyrën e duhur (Kufijtë etikë)
8. Mendo si një hacker. Vepro si një mbrojtës.
9. Përmbledhje: Stërvit mendjen si një hacker

KAPITULLI 11: Higjiena kibernetike që mund ta praktikosh sot 67

1. Çfarë është higjiena kibernetike?
2. Përdor fjalëkalime të forta dhe unike
3. Aktivizo Autentifikimin me Dy Faktorë (2FA)
4. Mos kliko linke të rastësishme
5. Mbaj softuerin të përditësuar
6. Shmang Wi-Fi publik (përveç nëse di çfarë bën)
7. Mendo para se të ndash diçka
8. Përdor antivirus (edhe atë falas)
9. Bëj kopje rezervë të të dhënave
10. Fol për këtë
11. Përmbledhje: Zakone të vogla, mbrojtje e madhe

Si të Marrësh Edukim në Siguri Kibernetike në Kosovë

KAPITULLI 1: Pse Kjo Ka Rëndësi 74

KAPITULLI 2: Universitetet – Rruga Akademike 75

KAPITULLI 3: Përtej Universiteteve – Shkolla Profesionale & Trajnime 76

KAPITULLI 4: Platforma Online & Laboratorë 78

KAPITULLI 5: Zgjedhja e Rrugës Tënde 78

Përmbledhje 79

Ku të Punosh në Sigurinë Kibernetike në Kosovë

KAPITULLI 1: Pse Punët në Siguri Kibernetike janë Kudo	80
KAPITULLI 2: Karriera në Sektorin Publik	81
KAPITULLI 3: Karriera në Sektorin Financiar	83
KAPITULLI 4: Sektori Privat & Konsulence	85
Kapitulli 5: OJQ-të & Shoqëria Civile	86
Kapitulli 6: Infrastruktura Kritike	87
Kapitulli 7: Harta e Karrierës Tënde në Cyber	89

Shpjegimi i Sigurisë Kibernetike



Kapitulli 1: Pse duhet të të interesojë

Qëllimi i kapitullit: Të bëjë të kuptosh që siguria kibernetike nuk është vetëm për të cmendurit e IT-së; është në lidhje me ty, jetën tënde dhe të ardhmen tënde. Është menduar për të treguar që ti tashmë je pjesë e botës kibernetike, pavarësisht nëse të pëlqen apo jo.

1. Një thirrje për tu zgjuar

Le të fillojmë me një histori: Arta kishte 12,000 ndjekës në Instagram. Ajo postonte fotografi, shpërndante “reels”, dhe kishte ndërtuar një komunitet të vogël. Një ditë ajo klikoi në një mesazh që i ofronte një “giveaway” për një lente aparati falas. Dukej i vërtetë. Brenda pak minutash, ajo u shkyç. Fjalëkalimi nuk punonte më. Llogaria e saj ishte zhdukur. Dikush e kishte marrë nën kontroll, kishte ndryshuar emailin dhe kishte filluar të mashtronte ndjekësit e saj me skema kriptomonedhash.

Asnjë paralajmërim. Asnjë rrugë kthimi.

2. “Por unë s’jam askush...”

Kështu mendon shumica e njerëzve.

- “Nuk jam i famshëm.”
- “Nuk kam para.”
- “Pse do të më hakonte dikush?”

E vërteta është: atyre nuk u intereson kush je. Hakerët hedhin rrjetë të gjera. Ata duan qasje tek emaili yt, telefoni yt, ndjekësit e tu, skedarët e tu. Pse?

- Të dhënat e tua = mund të shiten.
- Pajisja jote = mund të përdoret për sulme.
- Llogaria jote = mund të mashtrojë të tjerët.
- Identiteti yt = mund të kopjohet.

Nuk je i padukshëm. Je i lidhur. Dhe kjo mjafton.

3. Çfarë është realisht në rrezik?

Siguria kibernetike tingëllon abstrakte. Le ta bëjmë më konkrete. Pa të, mund të humbasësh:

- Bisedat, mesazhet dhe fotot e tua
- Paratë dhe qasjen në bankë
- Reputacionin - përmes postimeve të rreme ose përmbajtjes së publikuar pa leje
- Të ardhmen - aplikimet në kolegji, punë etj., të komprometuara
- Idetë e tua - të vjedhura, kopjuara ose fshira

Nuk është çështje “nëse.” Është çështje “kur.”

4. Po ndodh tashmë në Kosovë

Kjo nuk është vetëm një problematikë e Hollivudit.

Këtu në Kosovë:

- Studentët janë mashtruar me linke të rreme të Erasmus.
- Prindërit kanë klikuar malware në grupe të WhatsApp-it.
- Agjencitë qeveritare janë goditur me DDOS dhe malware.
- Mashtrimet telefonike dhe email-et “phishing” po rriten çdo vit.

Pyet përreth. Dikush që njeh është goditur tashmë.

5. Imagjino jetën tënde digjitale si një shtëpi

Le ta thjeshtojmë. Mendo për telefonin ose laptopin tënd si për shtëpinë tënde.

Mesazhet e tua = bisedat private

Fotot e tua = kujtimet personale

Email-et e tua = puna dhe e ardhmja jote

Tani imagjino ta lësh derën e shtëpisë tënde të hapur. Çdo ditë. Me një shënim ku shkruan: “Shërbeu vetë.”

Duket çmenduri? Kështu jetojnë shumica e njerëzve online. Fjalëkalime të dobëta. Klikime në çdo link që del përpara. Pa asnjë ide se çfarë po funksionon në prapaskenë. Siguria kibernetike është pikërisht kjo: ta mbyllësh derën. Ta kyçësh. Të vësh një alarm.

6. Nuk është vetëm sot. Është e ardhmja jote.

Ti nuk je vetëm online sot. Do të studiosh, të punosh, të dalësh në takim, të bësh banking, të blesh, të votosh dhe ndoshta edhe të drejtosh një biznes online. Çdo gjë është e lidhur. Dhe kjo do të thotë:

- Një shkelje mund të dëmtojë reputacionin tënd.
- Një mashtrim mund të të zbrazë llogarinë.
- Një telefon i hakuar mund ta shkatërrojë intervistën e punës para se të nisë.

Identiteti yt digjital është po aq real sa ai fizik.
Nëse nuk e mbron, dikush tjetër mund ta kontrollojë.

7. Siguria kibernetike = Kontroll, Fuqi, Liri

Harroje imazhin e sigurisë kibernetike si diçka të mërzitshme, teknike ose vetëm për “hakera”. Ja çfarë është vërtet:

- Kontroll - Ti vendos kush i sheh gjërat e tua.
- Fuqi - Nuk mashtroresh. E kupton si funksionojnë gjërat.
- Liri - Mund të lëvizësh i sigurt në botën digjitale.

Të mësosh sigurinë kibernetike nuk është thjesht e zgjuar, është fuqizuese. Të bën më të mprehtë, më të shpejtë, më të vetëdijshë

Është një aftësi që të mbron, të ndihmon të tjerët dhe të hap dyer karriere kudo.

8. Je në rrezik? (Vetë-kontroll i shpejtë)

Përgjigju me sinjeritet:

- A përdor të njëjtin fjalëkalim kudo?
- A ke klikuar ndonjëherë një link të çuditshëm nga Instagram apo WhatsApp?
- A përdor Wi-Fi publik pa VPN?
- A e di nëse email-i yt është ekspozuar ndonjëherë?

Nëse the “po” për ndonjëherë prej tyre...Je tashmë i ekspozuar.

Por mos u shqetëso. Ky udhëzues është këtu për ta ndryshuar këtë.

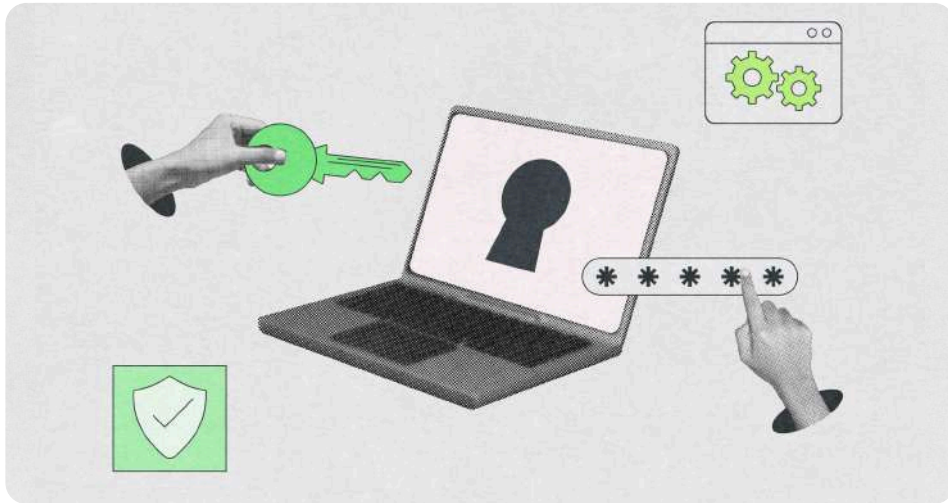
Fjala e fundit

Nuk ke pse të kesh frikë. Duhet të jesh i vetëdijshëm.

Ky është fillimi i të mësuarit se si të mbrosh veten, dhe ndoshta një ditë, të mbrosh edhe të tjerët.

Le të nisim.

KAPITULLI 2: Çfarë është Siguria Kibernetike



Nuk ka të bëjë vetëm me “hacking”.

Ka të bëjë me ta mbajtur jetën tënde digjitale të sigurt, nga brenda jashtë.

1. Siguria kibernetike në një fjali

Siguria kibernetike do të thotë **mbrojtje e kompjuterëve, rrjeteve, pajisjeve dhe të dhënave nga vjedhja, dëmtimi ose keqpërdorimi.**

Është kaq thjeshtë.

2. Çfarë ka nevojë për mbrojtje?

Çdo gjë digjitale:

- Telefoni yt
- Laptopi yt
- Llogaritë e tua
- Fotot, skedarët dhe mesazhet e tua
- Sistemet e shkollës, serverët bankarë, madje edhe infrastruktura e ujit dhe energjisë

Nëse është e lidhur me internet, mund të sulmohet.
Nëse mund të sulmohet, ka nevojë për siguri

3. Trekëndëshi i Sigurisë Kibernetike (Triada CIA)

Ky është “ABC”-ja e sigurisë kibernetike, e përdorur kudo në botë

◆ C – Konfidencialiteti (Confidentiality)

Mbaje privat. Vetëm njerëzit e duhur duhet të kenë akses.

Shembull: Mesazhet e tua nuk duhet të shihen nga të huajt.

◆ I – Integriteti (Integrity)

Mbaje të saktë. Pa ndryshime të paautorizuara.

Shembull: Notat e shkollës nuk duhet të ndryshohen nga dikush tjetër.

◆ A – Disponueshmëria (Availability)

Mbaje të aksesueshme. Duhet të mund ta përdorësh kur të duhet.

Shembull: Llogaria jote bankare online duhet të funksionojë kur futesh.

Siguria kibernetike ka të bëjë me **balancimin e të trijave**.

4. Çfarë nuk është siguria kibernetike

Le të sqarojmë disa keqkuptime.

Nuk është vetëm “hakimi në sisteme.”

Nuk ka të bëjë me të ndenjur në një dhomë të errët duke shtypur kod si në filma.

Nuk është vetëm për gjeni ose për njerëzit e IT-së.

Po, etika për hakim është pjesë e saj. Por ka gjithashtu:

- Analizë rreziku
- Shkrim politikash
- Trajnime për vetëdisimin ndaj sigurisë
- Hetime
- Projektim sistemesh

Siguria kibernetike është një lojë ekipore.

5. Kush punon në sigurinë kibernetike?

Ka shumë role të ndryshme:

- **SOC Analyst** – Vëzhgon për kërcënime 24/7
- **Penetration Tester** – Përpiqet të hyjë në sisteme (ligjërisht!)
- **Incident Responder** – Ndërhyn kur ndodh diçka e keqe
- **Security Engineer** – Ndërton sisteme të sigurta
- **CISO (Chief Information Security Officer)** – Vendos strategjinë e përgjithshme
- **Ekspert i Forenzikës** – Heton kush bëri çfarë

Disa shkruajnë kod.

Disa shkruajnë raporte.

Disa trajnojnë të tjerë.

Ka një rol për çdo lloj mendjeje.

6. Ti tashmë po praktikon sigurinë kibernetike (deri diku)

Nëse ndonjëherë ke:

- Vendosur një fjalëkalim të fortë
- Përdorur autentifikimin me dy faktorë (2FA)
- Raportuar një mesazh të dyshimtë
- Injoruar një link të rrezikshëm

... urime. Ke filluar tashmë. Tani është koha për të shkuar më thellë.

7. Pse ka rëndësi (më shumë se kurrë)

- Sa më shumë të jetojmë online, aq më shumë kemi nevojë për mbrojtje.
- Kompanitë, spitalet, shkollat dhe madje edhe qeveritë nuk mund të funksionojnë pa siguri kibernetike.
- Sulmet nuk janë të rralla. Ndodhin çdo ditë.

Siguria kibernetike nuk është më një fushë e ngushtë. Është një domosdoshmëri.

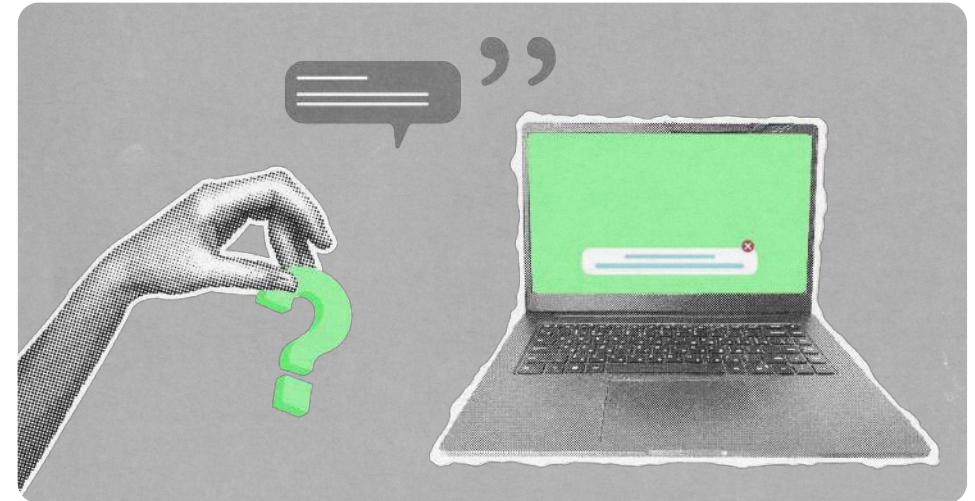
Përmbledhje

Siguria kibernetike ka të bëjë me **mbrojtjen e njerëzve dhe sistemeve në botën digjitale**.

Nuk është një gjë e vetme, është një univers aftësish dhe rolesh.

Dhe nuk ke pse të jesh ekspert për të filluar. Mjafton të jesh kureshtar dhe i vëmendshëm.

KAPITULLI 3: Kush janë të mirët dhe të këqijtë



Në botën e sigurisë kibernetike, jo të gjithë “hakerat veshin duksa.

Disa të mbrojnë. Disa të vjedhin. E disa jetojnë në zonën gri.

1. Le të flasim për hakerat

Thuaj fjalën “haker” dhe shumica e njerëzve e imagjinojnë kështu:

Një djalë me duks, duke shtypur si i çmendur në një bodrum të errët, me kode të gjelbërta që fluturojnë

në ekran

Epo... jo. Kjo është Hollivudi. Ja realiteti:

Një haker është kushdo që kupton si funksionojnë sistemet, dhe si t'i thyejë ose përmirësojë ato.

Ka hakera të mirë. Hakera të këqij. Dhe disa që janë pak nga të dyja.

2. Sistemi i kapelave

Ne i ndajmë hakerat sipas “ngjyrës së kapelës” për të treguar qëllimin e tyre:

◆ Kapelat e Zeza (Black Hats): Të këqijtë

Hyjnë në sisteme pa leje.

Vjedhin, shkatërrojnë, spiunojnë, mashtrojnë, ose mbajnë peng të dhëna për shpërblim.

Pse hakojnë:

- Para (vjedhje kartash krediti, shitje të dhënash
- Ego (“E bëra sepse munda.”)
- Hakmarrje ose kaos
- Misione shtetërore (dmth. hakera të sponsorizuar nga shteti)

Shembuj:

- Banda ransomware që bllokojnë sistemet e spitaleve

derisa të paguhen.

- Një adoleshent që shet hyrje në Instagram.
- Një qeveri e huaj që spiunon zgjedhjet e një vendi tjetër.

◆ Kapelat e Bardha (White Hats): Të mirët

Janë profesionistët e sigurisë që ndihmojnë organizatat të qëndrojnë të sigurt.

Testojnë sisteme me leje, rregullojnë probleme, trajnojnë përdorues, ndalojnë sulme.

Çfarë bëjnë:

- Gjejnë dobësi përpara se ta bëjnë të këqijtë
- Reagojnë ndaj incidenteve kibernetike
- Ndërtojnë rrjete të sigurt
- Trajnojnë ekipe dhe rrisin ndërgjegjësimin

Janë si truporjat digjitale.

◆ Kapelat Gri (Gray Hats): Zona e paqartë

Hakojnë pa leje, por jo për të bërë keq.

Ndonjëherë e bëjnë “për të mirën e përgjithshme”. Por prapë është e rrezikshme.

Shembull:

- Dikush gjen një dobësi në një faqe qeveritare, nuk kërkon leje, por e raporton.
- Mund të shkelë një rregull, por jo me qëllim të keq.

Gjithsesi... qëllimi nuk e fshin pasojën. Kapelat gri ecin në një vijë të rrezikshme.

3. Tipat kriminalë

Le t'i ndajmë disa nga kapelat e zeza që mund t'i hasësh (ose dëgjosh):

◆ Script Kiddies

- Përdorin mjete që nuk i kuptojnë plotësisht
- Shkarkojnë gjëra online dhe i "provojnë" mbi objektiva rastësorë
- Më shumë bezdisës sesa të rrezikshëm... derisa të kenë fat

◆ Krimi i Organizuar

- Hakera seriozë me pagesë
- Funksionojnë si biznese
- Përdorin ransomware, vjedhin të dhëna, kthejnë fitime në kriptovaluta

◆ Hacktivists

- Përzierje e "haker" dhe "aktivist"
- Hyjnë në sisteme për protestë ose përhapje mesazhi politik
- Shembull: Ndryshimi i webfaqeve ose publikimi i dokumenteve

◆ Aktorët Shtetërorë

- Punojnë për qeveri
- Synojnë vende të tjera, kompani, ose grupe politike
- Shumë të trajnuar, me financime, dhe tepër seriozë

4. Të mirët në kibernetikë (rolet e kapelave të bardha)

Në botën reale, kapelat e bardha punojnë si:

- **Penetration Testers (Pentesters)** – Paguhet të hyjë në sisteme përpara se ta bëjnë të këqijtë.
- **SOC Analysts** – Vëzhgojnë sistemet 24/7 për aktivitet të dyshimtë.
- **Incident Responders** – Zjarrfikësit e kibernetikës.
- **Ekspertë Forenzike** – Gjurmues të kush, çfarë, kur dhe si ndodhi një sulm.
- **Inxhinierë Sigurie** – Ndërtojnë mbrojtje si "firewalls", sisteme zbulimi, rrjete të sigurta.

Ata janë ata që mbajnë dritat ndezur - dhe të dhënat e tua të sigurta.

5. Nuk është gjithmonë thjesht "E drejta kundër të gabuarës"

Ndonjëherë gjërat ngatërrohen.

- Një adoleshent hakon sistemin e shkollës nga kureshtja. A është i kapelës së zezë? Apo thjesht i keqorientuar?
- Një sinjalizues publikon mbikëqyrjen e qeverisë. Hero për disa, kriminel për të tjerë.

Siguria kibernetike nuk është gjithmonë bardhë e zi. Por zgjedhjet e tua kanë rëndësi. Qëllimi ka rëndësi. Leja ka rëndësi.

6. Pra... Çfarë lloj hakeri do që ti të jesh?

Nëse je kureshtar... mirë.

Nëse të pëlqejnë enigmat... shkëlqyeshëm.

Nëse do të ndërtohet, mbrosh dhe sigurosh, mirë se erdhe në rrugën e kapelës së bardhë

Bota ka nevojë për hakera me etikë. Jo rebelë pa kauzë, por luftëtarë me qëllim.

Përmbledhje

Hakerat nuk janë një gjë e vetme. Janë njerëz me aftësi, të përdorura për të mirë, për të keq, ose diçka në mes. Sa më shumë kupton si mendojnë hackerat, aq më mirë mund të mbrohesh... ose të bëhesh mbrojtës.

Më pas: Do të shohim si ndodhin sulmet kibernetike, hap pas hapi.

Paralajmërim për zbulim: Shpesh fillon me një klikim të vetëm.

KAPITULLI 4: Si ndodhin vërtet sulmet kibernetike



Hakerat nuk hyjnë si në filma.

Ata planifikojnë. Presin. Të mashtrojnë.
Le ta shpërbëjmë si ndodh një sulm në të vërtetë.

1. Mjafton një klikim

Shumica e sulmeve kibernetike nuk nisin me kode të ndërlikuara. Nisin me ty.

E vërteta? Hakerat nuk “hakojnë”. Ata “hyjnë”, sepse dikush u dha qasje. Le të shohim si ndodh.

2. Zinxhiri i vrasjes kibernetike (i thjeshtuar)

Kjo është strategjia hap pas hapi që ndjek shumica e sulmuesve. Mendoje si një plan loje. Quhet Zinxhiri i vrasjes kibernetike – dhe jo, nuk është nga Call of Duty.

◆ Hapi 1: Zbulimi

Mëso çdo gjë për objektivin.

- Bëjnë një kërkim në Google për ty
- Shfletojnë rrjetet e tua sociale.
- Shikojnë se çfarë software përdor shkolla ose kompania.
- Skanon faqen tënde.
- Kërkon adresën e email-it ose numrin e telefonit.

Pse? Për të planifikuar kurthin perfekt.

◆ Hapi 2: Armatosja

Ndërtojnë sulmin bazuar në atë që gjetën.

- Krijojnë një faqe false (duket si faqja e bankës ose e shkollës).
- Përgatisin një PDF me malware të fshehur.

- Shkruajnë një email që tingëllon real, sikur vjen nga shefi, profesori ose një kompani.

Pse? Që kurthi të duket i padëmshëm.

◆ Hapi 3: Dorëzimi

Dërgojnë kurthin.

- Email
- Mesazhe në rrjete sociale
- Aplikacione mesazhesh
- Reklama të rreme ose shkarkimi të linqeve

Pse? Që të ndërveprosh. Kjo është çelësi.

◆ Hapi 4: Shfrytëzimi

Ti hap skedarin ose klikon linkun.

Tani:

- Malware ekzekutohet në heshtje
- Pajisja jote nis të dërgojë info te sulmuesi
- Futesh në një faqe të rreme dhe shkruan fjalëkalimin real

Pse? Për të marrë kontroll pa e vënë re.

◆ Hapi 5: Instalimi

Janë instaluar hyrje të fshehta

- Malware instalohet përgjithmonë.

- Sulmuesit kanë tani një rrugë të fshehtë brenda.
- Ti ndoshta vazhdon ta përdorësh pajisjen normalisht... por ata janë brenda.

Pse? Për të qëndruar pa u diktuar.

◆ Hapi 6: Komandë & Kontroll

Sulmuesi jep instruksione nga larg.

Mund të:

- Shkarkojë më shumë malware
- Përdorë pajisjen tënde për të sulmuar të tjerë
- Vjedhë fjalëkalime, skedarë ose karta krediti

Pse? Pajisja jote bëhet një mjet

◆ Hapi 7: Veprimet mbi objektivat

Është koha të përfundojë misioni.

- Bllokojnë file-t dhe kërkojnë shpërblim
- Vjedhin para ose të dhëna
- Spiunojnë aktivitetin tënd
- Shkatërrojnë ose fshijnë sistemet

Pse? Ky është qëllimi. Gjithçka tjetër ishte përgatitje.

3. Shembull nga bota reale (i thjeshtuar)

Le të themi që merr këtë email

“Përshëndetje! Ky është administratori i shkollës. Ka një përditësim sigurie për llogarinë tënde. Ju lutemi futuni këtu: school-portal-login.site”

Duket e rregullt. Klikon. Fut të dhënat.

Boom. Ti je brenda. Por... edhe sulmuesi.

Ata tani:

- Hyjnë si ti
- Ndryshon fjalëkalimin tënd
- Shkarkon skedare private
- Dërgon phishing mesazhe tek shokët e klasës duke përdorur emrin tënd

Dhe ja ku një klikim u kthye në shkelje.

4. Truku bonus: Pivotimi

Pasi hakerat hyjnë në një sistem, kërkojnë mënyra për të depërtuar më thellë. Kjo quhet pivoting.

Hakojnë email-in → Përdorin për të hyrë në cloud drive

Hyjnë në një server shkolle → Kalojnë në sistemin e notave

Hakojnë një punonjës → Arrijnë në gjithë kompaninë

Sulmet kibernetike rriten si viruset. Prandaj zbulimi i hershëm është çelësi.

5. Ata duan që ti ta bësh të lehtë

Shumica e sulmuesve nuk duan sfida.

Ata kërkojnë:

- Fjalëkalime të dobëta
- Software të vjetër me të meta të njohura
- Njerëz që klikojnë pa menduar
- Sisteme pa autentifikim dyfaktorësh

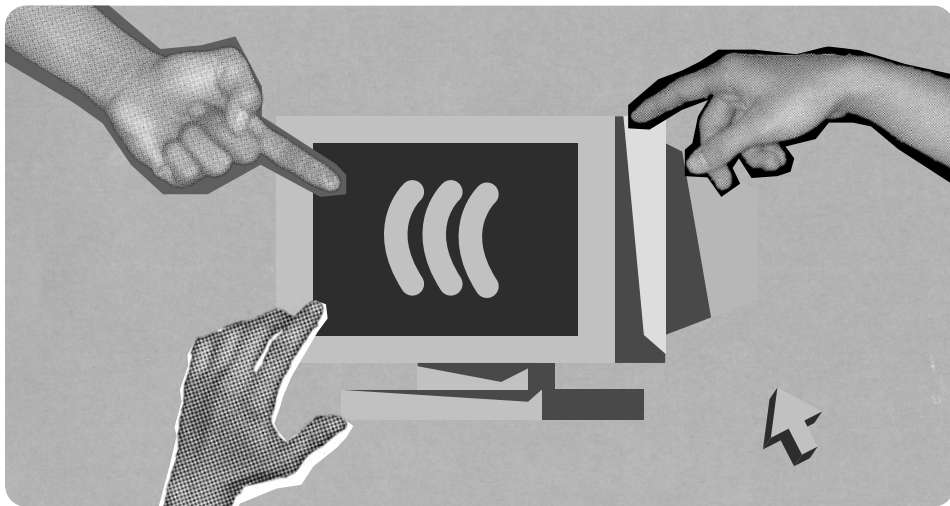
Ata duan pak mundim, shumë fitim. Mos ua jep.

Përmbledhje: Si ndodhin sulmet

1. Të shikojnë.
2. Të mashtrojnë.
3. Hyjnë brenda.
4. Rrinë të qetë.
5. Vjedhin, shkatërrojnë, ose spiunojnë.

Sulmet kibernetike nuk janë magji. Janë të zgjuara, të fshehta dhe të durueshëm.

KAPITULLI 5: Llojet e Kërcënimeve Kibernetike (që do t'i shohësh vërtet)



Harro sulmet si në Hollivud.

Le të flasim për gjërat reale që të godasin: telefoni yt, llogaritë e tua, shokët e tu.

1. Phishing: Kurthi i mesazhit të rremë

Çfarë është: Një email, DM ose mesazh i rremë që tenton të të mashtrojë për të klikuar një link të dëmshëm, për të shkarkuar malware, ose për të dhënë informacione.

Si duket:

- “Pakoja jote u vonua. Kliko këtu për të ndjekur.”
- “Llogaria jote shkollore do të pezullohet. Hyr tani.”
- “Ke fituar një iPhone falas!”

Pse funksionon:

- Duket urgjent.
- Duket i vërtetë.
- Ti klikon pa menduar.

Si ta dallosh:

- Kontrolllo adresën e dërguesit - a duket e çuditshme?
- Kaloi miun mbi link - çon në faqen e vërtetë?
- Gramatikë e keqe ose presion i papritur = flamur i kuq.

Rregulla: Mos kliko lidhje ose mos shkarko skedarë nëse nuk je 100% i sigurt.

2. Malware: Pushtuesi i qetë

Çfarë është: Softuer keqdashës që infekton pajisjen tënde.

Llojet që mund të takosh:

- **Spyware:** Të vëzhgon, regjistron çfarë shkruan.
- **Keyloggers:** Kapin fjalëkalimet dhe mesazhet.

- **Trojans:** Duken si skedar normal, por hapin derën për hakerët.
- **Ransomware:** Bllokon skedarët dhe kërkon pagesë për t'i ç'kyçur.

Si hyjnë:

- Duke klikuar linqe të dyshimta
- Duke shkarkuar lojëra/filma/pirate ose software të piratuar
- Duke futur USB të rastësishëm

Rregulla: Nëse është falas por e dyshimtë... me shumë gjasa është kurth.

3. Sulmet ndaj fjalëkalimeve: Lidhja jote me e dobët

Çfarë është: Hakerat përpiqen të gjejnë, vjedhin ose shtypin fjalëkalimin tënd.

Metodat e zakonshme:

- **Sulm:** Provon mijëra kombinime derisa të hyjë.
- **Mbushje kredencialesh:** Përdor fjalëkalime të rrjedhura nga faqe të tjera që ti ke përdorur.
- **Phishing:** Të mashtrojnë që të shkruash fjalëkalimin në një faqe të rreme.

Shenjat që të kanë goditur:

- Je i ç'kyçur dhe nuk kthehesh dot brenda.
- Merr email për rikthim fjalëkalimi që nuk e ke kërkuar.
- Miqtë të marrin mesazhe të çuditshme nga emri yt.

Rregulla:

- Përdor fjalëkalime të forta dhe unike.
- Aktivizo 2FA (autentifikim me dy faktorë).
- Mos ripërdorni kurrë fjalëkalime.

4. Inxhinieria sociale: Të hakojnë ty, jo kompjuterin

Çfarë është: Truke psikologjike për të të bërë të japësh informacion ose qasje.

Si ndodh:

- “Përshëndetje, jam tekniku i IT-së së shkollës - më dërgo hyrjen tënde shpejt.”
- “Jam shoku i kushëririt tënd, më duhet ndihma jote urgjente.”

Pse funksionon:

- Duam të ndihmojmë.
- Nuk duam të dukemi të pasjellshëm.
- Supozojmë se njerëzit janë ç'thonë se janë.

Rregulla: Gjithmonë verifiko identitetet. Bëhu

i sjellshëm, por skeptik.

5. Sulmet në Wi-Fi publik: Kurthi i internetit falas

Çfarë është: Wi-Fi i hapur në kafe, shkolla, aeroporte mund të jetë i rremë ose i pasigurt.

Çfarë mund të ndodhë:

- Hakerat të shikojnë çfarë bën.
- Mund të kapin fjalëkalime, mesazhe, madje edhe të dhëna pagese.
- Mund të paraqiten si rrjeti që mendon se është i sigurt.

Rregulla:

- Shmang hyrjen në llogari të ndjeshme në Wi-Fi publik.
- Përdor VPN nëse duhet të lidheni.
- Pyete: “A është ky rrjeti zyrtar?”

6. Kapja e llogarive: Kur e humb kontrollin

Çfarë është: Dikush merr kontrollin e email-it, Instagram-it, Snapchat-it apo llogarisë bankare.

Si e bëjnë:

- Phishing
- Fjalëkalime të dobëta
- Rishfrytëzim fjalëkalimesh nga shkeljet e mëparshme
- **SIM-swapping** (marrin nën kontroll numrin tënd të telefonit)

Pse është e rrezikshme:

- Mund të mashtrojnë ndjekësit e tu.
- Të rrjedhin mesazhet private.
- Të të lënë jashtë jetës tënde.

Rregulla:

- Përdor 2FA.
- Monitoro hyrjet.
- Vepro shpejt nëse ndjen diçka të pazakontë.

7. Aplikacione, shkarkime dhe vegla të rreme: Kali i Trojës

Çfarë është: Aplikacione që duken të dobishme, por janë keqdashëse.

Kurthet e zakonshme:

- “Shkarko këtë aplikacion për të parë kush pa profilin tënd!”
- Versione “crack” të lojërave ose mjeteve të editimit

- Aplikacione antivirusi të rreme ose “cleaner”-a

Çfarë bëjnë:

- Vjedhin të dhëna
- Të spiunojnë
- Bllokojnë pajisjen

Rregulla: Shkarko vetëm nga dyqanet zyrtare (App Store/Play Store). Kontrolllo vlerësimet. Shmang faqet e dyshimta.

8. Dezinformimi: Gënjeshtat që përhapen si zjarri

Çfarë është: Përmbajtje e rreme ose mashtruese që synon të mashtrtojë, ndajë apo manipulojë.

Pse ka rëndësi për sigurinë kibernetike:

- Hakerat përdorin lajme të rreme për të shkaktuar kaos.
- Fushatat e dezinformimit synojnë zgjedhje, protesta, ose grupe specifike.
- Ti mund të ndihmosh pa dashje për ta përhapur atë.

Si ta dallosh:

- Kontrolllo burimin.
- Verifiko me një burim të dytë të besueshëm.
- Ji i kujdesshëm me tituj emocionalë ose postime

virale.

Rregulla: Mos u bë marionetë. Mendo para se të shpërndash.

Përmbledhje: Kërcënimet që do të shohësh

Nuk do të shohësh lazerë apo shpërthime.

Do të shohësh:

- Një faqe logimi të rreme
- Një email të dyshimtë
- Një aplikacion “falas” të dyshimtë
- Një mesazh që ndjen se... nuk shkon

Por tani e di se çfarë të kërkosh.

Më pas: Do të shikojmë ku ndodh vërtet siguria kibernetike: shtëpia jote, shkolla, vendi yt. Nuk është vetëm telefoni yt, është kudo.

KAPITULLI 6: Ku ndodh Siguria Kibernetike



Siguria kibernetike nuk është vetëm në ekranin tënd.

Ajo është në shkollën tënde, qytetin tënd, vendin tënd. Është pas skenave të gjithçkaje që i beson.

1. Është më e madhe se ç'mendon

Kur njerëzit dëgjojnë "siguri kibernetike" mendojnë:

- Hakera
- Telefona
- Fjalëkalime

Por është shumë më e madhe.

Siguria kibernetike është mburoja e padukshme që mbron sisteme të tëra:

- Shkolla
- Spitale
- Banka
- Aeroporte
- Qeveri
- Edhe uzina e energjisë dhe uji

2. Në shtëpi: Zona jote personale kibernetike

Shtëpia jote është një fushë beteje digjitale, pa marrë parasysh a e vren ti apo jo..

Pajisjet në rrezik:

- Telefona
- Laptopë
- Smart TV
- Ruterët Wi-Fi
- Asistentët e zgjuar (Alexa, Google Home)

Kërcënimet e zakonshme:

- Fjalëkalime të dobëta të Wi-Fi-së
- Aplikacione të rreme

- Mesazhe phishing
- Malware i shkarkuar nga materialet e paligjshme

Zakone të mira = mbrojtja e mirë.

Kur shtëpia jote është e sigurt, bëhesh më i vështirë për tu sulmuar.

Këshillë: Ndrysho fjalëkalimin e Wi-Fi. Përdor fjalëkalime unike për pajisje. Mbaj softuerin të përditësuar.

3. Në shkollë: Laboratorë për hakerë

Shkollat përdorin shumë teknologji:

- Email
- Sisteme online të notave
- Regjistra studentore
- Platforma mësimore (Google Classroom, Moodle)

Pse sulmohen shkollat:

- Hyrje e lehtë
- Shumë të dhëna personale
- Siguri IT e kufizuar në shumë vende

Çfarë mund të shkojë keq:

- Ndryshimi i notave
- Nxjerrja e provimeve
- Vjedhja e të dhënave private

Këshillë: Mos ndajë hyrjen me miqtë. Raporto çdo gjë të dyshimtë te ekipi i IT të shkollës.

4. Në punë: Edhe punët me gjysëm orari

Nëse punon në një kafiteri, bankë, palestër, apo kudo që trajton:

- Kartat e kreditit
- Informacion klientësh
- Sisteme të brendshme

...ti je në lojën kibernetike tani.

Çfarë duan hakerat:

- Bazat e të dhënave të klientëve
- Akses në lexues kartash
- Hyrjet e punonjësve

Bizneset e vogla = objektiva të mëdha.

Pse? Sepse shpesh janë më të lehta për t'u hakuar

Këshillë: Ki kujdes çfarë hap nga pajisjet e punës. Mos hap email personal apo faqe të dyshimta.

5. Në publik: Kurthi i Wi-Fi falas

Çdo vend që ofron Wi-Fi falas është zonë potenciale rreziku:

- end që ofron Wi-Fi falas është zonë potenciale rreziku:
- Kafe
- Aeroporte
- Biblioteka
- Hotele
- Qendra tregtare

Çfarë mund të ndodhë:

- Hakerat spiunojnë trafikun tënd
- Rrjetet e rreme të bëjnë të lidheni gabim
- Të vjedhin hyrjet në kohë reale

Këshillë: Shmang hyrjen në llogari të ndjeshme në Wi-Fi publik. Përdor VPN nëse duhet.

6. Në spitale: Sulmet kibernetike mund të vrasin

Kjo është serioze.

Spitalet:

- Plot teknologji
- Të lidhura me sisteme kombëtare
- Mbajnë të dhëna kritike

Rreziku real:

- Ransomware mund të bllokojë pajisje që shpëtojnë jetë
- Regjistra e pacientëve mund të vjedhen apo të manipulohen
- Emergjencat mund të pengohen

Kjo nuk është vetëm për të dhëna - është për jetë njerëzish.

7. Në qeveri: Lufta e ftohtë kibernetike

Qeveritë janë gjithmonë në sulm.

Çfarë synohet:

- Sistemet e ID-së kombëtare
- Kontrolli i kufijve
- Infrastrukturat zgjedhore
- Informacione të klasifikuara

Kush qëndron pas:

- Hakera të sponsorizuar nga shteti
- Hacktivistë
- Grupa kriminale të organizuara

Pse? Fuqi, para, ndikim.

Kosova, si çdo vend tjetër, është pjesë e këtij fushëbeteje kibernetike. Prandaj ndërtimi i talenteve lokale në sigurinë kibernetike, me njerëz si ti, është një

prioritet kombëtar.

8. Në infrastrukturën kritike: Fikja e dritave

Mendo për këtë:

- Çfarë nëse energjia fiket në gjithë vendin?
- Çfarë nëse pompuesit e ujit ndalojnë?
- Çfarë nëse fluturimet pezullohen për ditë?

Këto sisteme mbështeten në rrjete që mund të sulmohen.

Kjo quhet **Infrastrukturë Kritike**, dhe mbrojtja e saj është nivel i lartë i sigurisë kibernetike.

Shtetet trajtojnë mbrojtjen kibernetike si mbrojtje kombëtare.

Këtu është pika ku siguria kibernetike bëhet çështje e sigurisë kombëtare

9. Kudo që shkon ti

Siguria kibernetike nuk është një vend. Është një shtresë.

Sa herë që:

- Lidheni
- Hyni me hyrje

- Prek kartelen
- Ndani diçka
- Përdorni teknologji të zgjuar

...ti je pjesë e një sistemi që ka nevojë për mbrojtje.

Prandaj specialistët e sigurisë punojnë në çdo sektor: teknologji, ligj, financë, arsim, shëndet, dhe më shumë.

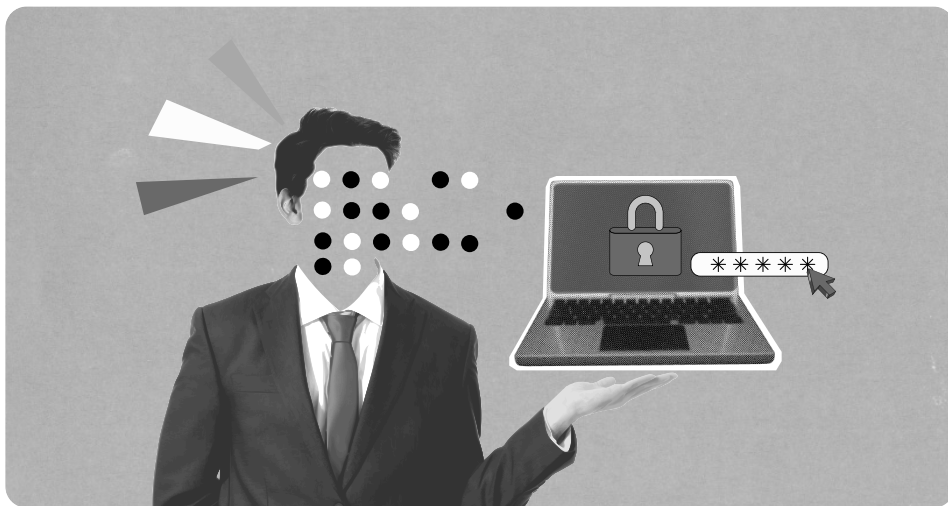
Përmbledhje: Siguria kibernetike është kudo

- Është në shtëpinë tënde, shkollën tënde, punën tënde.
- Mbron bizneset, spitalet dhe kombet.
- Është e padukshme, por jetike.
- Tani e di çfarë rrezikon.

Më pas:

Tani le të shohim se çfarë bëjnë profesionalët e sigurisë kibernetike dhe rolet e ndryshme që mund të kesh në këtë fushë në rritje.

KAPITULLI 7: Çfarë bëjnë në të vërtetë profesionistët e sigurisë kibernetike



Jo të gjithë në fushën e sigurisë kibernetike janë hakerë.

Disa vëzhgojnë. Disa ndërtojnë. Disa rregullojnë. Disa udhëheqin.

Le t'i njohim ekipet.

1. Siguria Kibernetike është një Sport Ekipor

I keni parë kërcënimet. E keni parë fushën e betejës.

Tani njihuni me mbrojtësit: njerëzit që mbajnë të sigurt sistemet, bizneset dhe madje edhe vendet.

Siguria kibernetike nuk është vetëm një punë. Është një botë e tërë rolesh. Aftësi të ndryshme. Mendje të ndryshme. Një mision i vetëm.

Le t'i zbërthejmë.

2. Mbrojtësit e Vijës së Parë

◆ Analisti SOC (Qendra e Operacioneve të Sigurisë)

Janë si rojet e sigurisë së botës digjitale.

Çfarë bëjnë:

- Vëzhgojnë për alarme
- Vënë re aktivitet të pazakontë
- Reagojnë ndaj shenjave të hershme të sulmeve

Do t'ju pëlqente kjo nëse: Ju pëlqejnë enigmat, të dalloni modele dhe të punoni nën presion.

◆ Incident Responder (Reagues ndaj Incidenteve)

Hedhin hapin pas diçkaje që ka shkuar keq.

Çfarë bëjnë:

- Izolojnë shkeljen
- Pastrojnë dëmet
- Gjejnë si ndodhi

Mund t'i mendoni si zjarrfikës të kibernetikës.

Do t'ju pëlqente kjo nëse: Qëndroni i qetë në kaos dhe ju pëlqen të zgjidhni shpejt probleme.

3. Hakerët Etikë

◆ Pentester (Testues i penetrimit)

Quhen edhe “hakerë etikë”. Përpiqen të hyjnë në sisteme, me leje.

Çfarë bëjnë:

- Gjejnë pikat e dobëta para se ta bëjnë sulmuesit e vërtetë
- Simulojnë sulme
- Shkruajnë raporte të detajuara për mënyrën se si hynë

Do t'ju pëlqente kjo nëse: Ju pëlqejnë lojërat e hacking-ut, CTF-të (Capture the Flag), ose të mendoni si keqbërësin, por për një kauzë të mirë.

4. Ndërtuesit dhe Inxhinierët

◆ Inxhinieri i Sigurisë

Ndërton dhe mirëmban mjetet që mbrojnë sistemet.

Çfarë bëjnë:

- Konfigurojnë firewall-e
- Dizajnojnë rrjete të sigurta
- Instalojnë programe sigurie
- Automatizojnë mbrojtjen

Do t'ju pëlqente kjo nëse: Ju pëlqen të ndërtoni gjëra, të shkruani skripte dhe të bëni që sistemet të funksionojnë pa probleme.

◆ Arkitekti i Sigurisë

Dizajnon strategjitë e tëra të sigurisë.

Çfarë bëjnë:

- Planifikojnë si të sigurohen sistemet e mëdha
- Punojnë me inxhinierë dhe menaxherë
- Marrin parasysh si aspektin teknik, ashtu edhe atë të biznesit

Do t'ju pëlqente kjo nëse: Jeni planifikues, mendoni në nivel sistemesh dhe ju pëlqen të dizajnoni zgjidhje në pamje të gjerë.

5. Hetuesit

◆ Eksperti i Forenzikës Digjitale

Pas një incident hetojnë, si një detektiv digjital.

Çfarë bëjnë:

- Ekzaminojnë hyrjet dhe skedarët
- Ndjekin aktivitetin e hakerëve
- Mbledhin prova për gjykata

Do t'ju pëlqente kjo nëse: Ju pëlqejnë hetimet, detajet dhe ndjekja e së vërtetës.

◆ Analisti i Inteligjencës së Kërcënimeve

Studion hakerët dhe kërcënimet në mbarë botën.

Çfarë bëjnë:

- Ndjekin grupet e hakerëve
- Analizojnë prirjet globale
- Paralajmërojnë kompanitë për sulme të reja

Do t'ju pëlqente kjo nëse: Jeni kurioz, strategjik dhe ju pëlqen të qëndroni gjithmonë një hap përpara.

6. Udhëheqësit dhe Komunikuesit

◆ CISO (Shefi i Sigurisë së Informacionit)

Shefi i sigurisë kibernetike.

Çfarë bëjnë:

- Udhëheqin ekipin e sigurisë

- Marrin vendime strategjike
- Menaxhojnë buxhete, rrezik dhe njerëz

Do t'ju pëlqente kjo nëse: Dëshironi të udhëhiqni, të planifikoni dhe të bëni ndryshim në nivelin më të lartë.

◆ Konsulenti / Trajneri i Sigurisë Kibernetike

Punojnë në kompani të ndryshme dhe ndihmojnë të tjerët të kuptojnë rreziqet kibernetike.

Çfarë bëjnë:

- Shkruajnë politika
- Trajnojnë punonjësit
- Këshillojnë ekipet për praktikatat më të mira

Do t'ju pëlqente kjo nëse: Ju pëlqen të shpjegoni gjëra, të punoni me njerëz dhe të përmirësoni sistemet.

7. Prisni: A duhet të jem gjeni i teknologjisë?

Jo.

Disa role kërkojnë aftësi teknike (si programim ose rrjete). Të tjera kërkojnë komunikim të fortë, analiza, ose edhe background në juridik dhe psikologji.

Në fakt:

- Disa nga konsulentët më të mirë kanë qenë dikur mësues.

- Disa nga analistët më të mirë vijnë nga lojërat ose nga ushtria.
- Disa hakerë të jashtëzakonshëm kurrë nuk kanë shkuar në universitet.

Siguria kibernetike ka të bëjë me mënyrën e të menduarit. Kurioz. I përqendruar. Etik. Zgjidhës problemesh.

8. Ku ekzistojnë këto punë?

Kudo.

- Kompani teknologjike
- Banka dhe telekomunikacione
- Spitale dhe shkolla
- Qeveri dhe ushtri
- OJQ dhe organizata ndërkombëtare
- Dhe po, edhe në Kosovë.

Përmbledhje: Gjej Rolin Tënd

Ja e vërteta: Nuk ke pse të jesh haker për të qenë në siguri kibernetike.

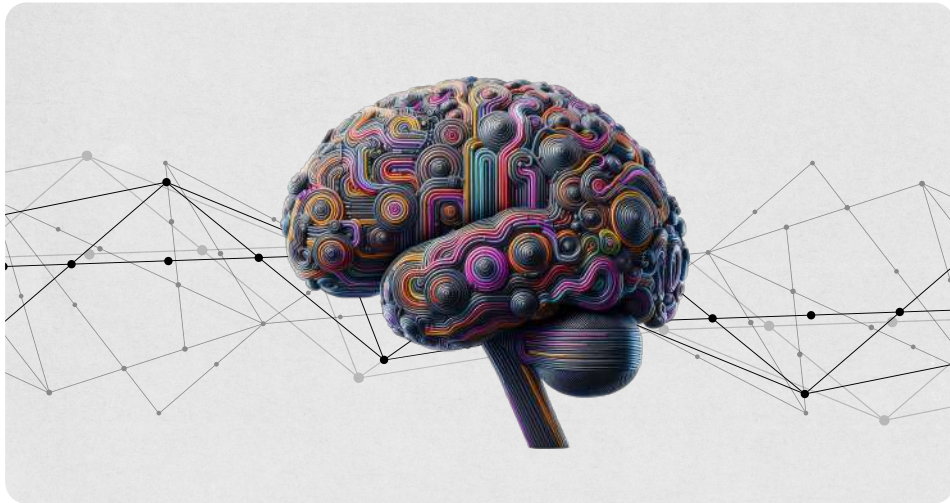
Mund të:

- Vëzhgosh

- Ndërtosh
- Hetosh
- Këshillosh
- Udhëheqësh

Cilat do qofshin pikat e tua të forta, ka një rol për ty.

KAPITULLI 8: A duhet të jesh gjeni ose programues?



Përgjigjja e shkurtër: Jo.

Përgjigjja e gjatë: Le ta shkatërrojmë mitin.

1. Miti që i ndal njerëzit

Kur dëgjon “siguri kibernetike,” çfarë imagjinon?

- Një djalë me kapuç që shkruan 1,000 fjalë në sekondë?
- Një gjeni që ka hakuar NASA-n në moshën 12 vjeç?
- Një programues që flet rrjedhshëm pesë gjuhë programimi?

Ja e vërteta: Nuk ke nevojë të jesh gjeni. Nuk ke nevojë të jesh programues.

Çfarë të duhet në të vërtetë:

- Kuriozitet
- Aftësi për zgjidhjen e problemeve
- Pak durim
- Vullnet për të mësuar

Kaq. Të tjerat mund të mësohen.

2. Shumë role nuk kërkojnë programim

Të jemi të qartë: Ka punë në sigurinë kibernetike ku programimi ndihmon (si testimi i penetrimit ose analiza e malwerëve). Por ka edhe punë ku nuk do të prekësh asnjë rresht kodi.

Shembuj:

- Trajner i ndërgjegjësimit për sigurinë
- Këshilltar politikash
- Analist SOC
- Vlerësues rreziku
- Teknik i forenzikës digjitale
- Analist i inteligjencës së kërcënimeve

Siguria kibernetike është pjesërisht teknologji, pjesërisht strategji, pjesërisht komunikim, pjesërisht psikologji.

3. Çfarë ka më shumë rëndësi në të vërtetë

◆ Të menduarit kritik

A di të ndash një problem në pjesë? A di të ndjekësh gjurmët? Do të habitesh sa shumë sulme ndalen vetëm duke bërë pyetje të zgjuara.

◆ Kurioziteti

Profesionalistët më të mirë të sigurisë janë kuriozë. Ata hulumtojnë. Testojnë. Eksplorojnë.

◆ Komunikimi

Mund të dish rreziqet, por a di t'i shpjegosh për të tjerët? Çdo organizatë ka nevojë për njerëz që mund të mësojnë, prezantojnë dhe udhëheqin.

◆ Etika

Do të kesh qasje në sisteme, të dhëna dhe besim. Etika nuk është opsion; është gjithçka.

4. Njerëz të vërtetë, prapavija të vërteta

Disa nga profesionistët më të mirë të sigurisë kibernetike:

- Nuk kanë shkuar kurrë në universitet
- Kanë filluar në shërbim klienti ose shitje me pakicë
- Kanë ardhur nga ushtria ose policia

- Kanë kaluar nga karriera krejtësisht të pa lidhura

Mund të hysh në këtë fushë nga KUDO.

5. Po me certifikatat si qëndron puna?

Certifikatat mund të jenë një mënyrë e shkëlqyer për të vërtetuar aftësitë, sidomos nëse nuk ke diplomë.

Disa që janë miqësore për fillestarët:

- **CompTIA Security+** – hyrje e gjerë në konceptet e sigurisë kibernetike
- **Cisco CyberOps** – e mirë për rolet SOC
- **Google Cybersecurity Certificate** – e shkëlqyer për të mësuar me ritmin tënd
- **TryHackMe / Hack The Box** – platforma praktike për të ushtruar aftësi

Mund të fillosh me hapa të vegjël. Disa certifikata duhen vetëm disa javë për t'u përgatitur.

6. Po mosha a ka rëndësi?

Shumë i ri? Shumë i vjetër? Nuk ka rëndësi.

- Të rinjtë mund të fillojnë me laboratorë online dhe YouTube.
- 20-vjeçarët mund të kalojnë nga fusha të tjera.
- 30+? 40+? Ti sjell pjekuri dhe përvojë jetësore,

avantazhe të mëdha në udhëheqje, konsulencë ose trajnim.

Nuk ka një rrugë fikse. Ka vetëm rrugën tënde.

7. Si të fillosh pa programim

Ja një udhërrëfyes:

- Mëso bazat nga libra, video ose kurse
- Praktiko zakone të sigurta (fjalëkalime, kujdes ndaj phishing-ut)
- Provo mjete falas si Wireshark, VirusTotal, Shodan
- Shiko në YouTube analiza të sulmeve reale
- Ndiq njerëz të sigurisë kibernetike në rrjete sociale
- Eksploro platforma falas si TryHackMe ose Blue Team Labs
- Merr pjesë në punëtori lokale, takime teknologjike ose CTF

Do të habitesh se sa larg mund të shkosh pa shkruar asnjë rresht kodi.

8. A duhet të mësosh programim eventualisht?

Ndoshta. Ndoshta jo.

Nëse dëshiron të thellohesh (si në hacking, scripting, ose ndërtimin e mjeteve), mësimi i programimit do

të ndihmojë. Por edhe atëherë, mund ta mësosh më vonë. Nuk të duhet për të filluar. Shumica e njerëzve në kibernetikë i kanë mësuar gjërat gjatë punës, hap pas hapi. Mos e lër “mosdijen e kodimit” të të ndalojë.

Përmbledhje: Jo, nuk ke pse të jesh gjeni ose programues

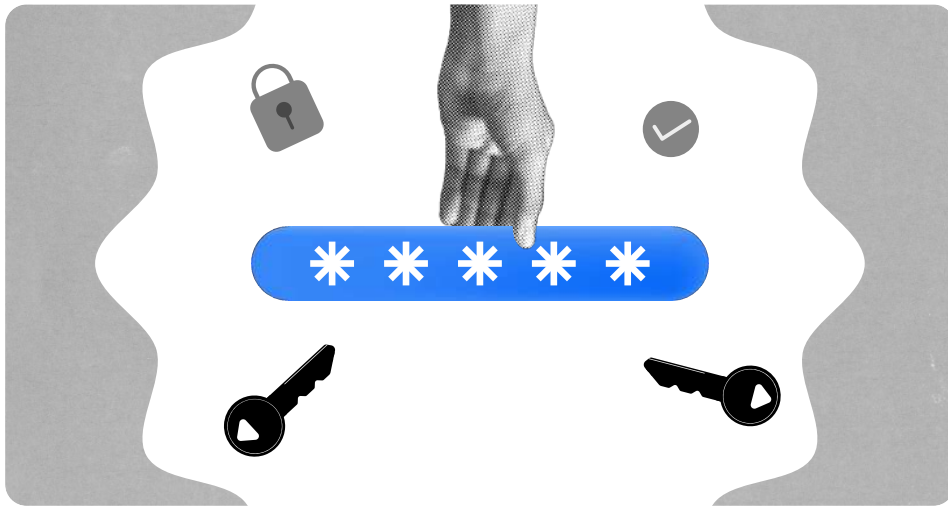
Ajo që të duhet:

- Kuriozitet
- Një mendje e mprehtë
- Një ndjenjë e fortë e së drejtës dhe së gabuarës
- Një dëshirë për të mësuar dhe për të mbrojtur të tjerët

Kjo është ajo që të bën një profesionist të sigurisë kibernetike

Në kapitullin që vjen: Le të flasim pse kjo ka rëndësi përtej parave ose teknologjisë: sepse siguria kibernetike të jep fuqi, kontroll dhe liri.

KAPITULLI 9: Siguria kibernetike = Fuqi, Kontroll dhe Liri



Kjo nuk ka të bëjë vetëm me teknologjinë.

Ka të bëjë me marrjen sërish në dorë të kontrollit mbi jetën tënde, identitetin tënd, të ardhmen tënde.

1. Siguria kibernetike nuk është vetëm mbrojtje

Kur njerëzit dëgjojnë “siguri kibernetike”, mendojnë: “Është për të ndaluar hakerët.” Ky është një pjesë e saj.

Por në thelb, siguria kibernetike ka të bëjë me diçka më të thellë:

- Kontroll
- Fuqi
- Liri

Le t’i zbërthejmë.

2. KONTROLL: Ti zotëron jetën tënde digjitale

Interneti është kaotik. Të gjithë duan vëmendjen, të dhënat dhe kohën tënde. Hakerët. Reklamuesit. Mashtruesit. Aplikacionet. Algoritmet.

Siguria kibernetike të jep mjetet për të marrë kontrollin përsëri:

- Ti vendos kush e sheh përmbajtjen tënde.
- Ti e dallon kur diçka është e dyshimtë.
- Ti cakton rregullat për privatësinë tënde.

Shumica e njerëzve nuk e kontrollojnë jetën e tyre digjitale. Ata thjesht shkojnë me rrjedhën. Siguria kibernetike të zgjon. Ajo të kthen nga një përdorues pasiv në një rojtar aktiv.

3. FUQI: Ti kupton atë që të tjerët nuk e kuptojnë

Të themi të vërtetën: shumica e njerëzve nuk e dinë

çfarë ndodh online. Por ti do ta dish.

- Do dish si ndodhin sulmet.
- Do dish cilat të dhëna po mblidhen.
- Do dish si të mbrosh veten dhe të tjerët.
- Do dish si t'i "thyesh" gjërat në mënyrë etike dhe t'i rregullosh edhe më mirë.

Në një botë plot kërcënime digjitale, dija është fuqi.

Siguria kibernetike të kthen në dikë nga i cili të tjerët varen. Ti nuk humbet. Ti udhëheq.

4. LIRI: Lëviz pa frikë

Sulmet kibernetike krijojnë frikë.

Frikë nga të qenit i vëzhguar.

Frikë nga të qenit i hakuar.

Frikë nga humbja e gjithçkaje.

Por kur di si të mbrohesh, ajo frikë zhduket.

- Nuk bie pre e mashtrimeve.
- Nuk panikohesh nga email-et false.
- Nuk jeton me paranojë, jeton i përgatitur.

Kjo është liria e vërtetë. **Siguria kibernetike të lejon të jetosh online me vetëbesim.**

5. Bonus: Mund t'i ndihmosh edhe të tjerët

Ajo që mëson nuk është vetëm për veten.

Mund të ndihmosh:

- Prindërit e tu të ìu shmangin mashtrimeve
- Shkollën të mbrojë të dhënat e nxënësve
- Vendet e punës të qëndrojnë të sigurt
- Vendin tënd të forcojë qëndrueshmërinë digjitale

Nuk po mbron vetëm veten. Ti je pjesë e një lëvizjeje, e njerëzve etikë, inteligjentë dhe të aftë që e bëjnë internetin më të sigurt. Kjo është ndikim i vërtetë. Kjo është lidhësi i vërtetë.

6. Kjo është më e madhe se një punë

Siguria kibernetike nuk është vetëm diçka që "e bën." Është diçka që je. Është një mënyrë të menduari:

- Dallo rrezikun e fshehur.
- Mendo si sulmuesi.
- Mbro njerëzit.
- Ji më i zgjuar se kërcënimi.

Qoftë si pentester, trajner, konsulent, ose thjesht si dikush që di si të qëndrojnë i sigurt, ti do të ecësh në botë më i mprehtë. Ky është thelbi i gjithë kësaj.

Përmbledhje: Kjo është superfuqia jote

Siguria kibernetike të jep:

- Kontroll mbi të dhënat dhe jetën tënde
- Fuqinë për të kuptuar dhe mposhtur kërcënimet
- Lirinë për të eksploruar botën digjitale pa frikë

Dhe pasi ta kesh këtë?

Askush nuk mund ta të ta marrë.

Në kapitullin tjetër: Si fillon në praktikë? Çfarë mund të bësh sot për të nisur udhëtimin tënd? Le të flasim për këtë.

KAPITULLI 10: Si të fillosh të mendosh si një haker (etikisht)



Për të mposhtur një haker, duhet të mendosh si ai.

Por për të qenë i madh në sigurinë kibernetike, duhet ta bësh këtë **etikisht**

1. Hakerët e mirë mendojnë ndryshe

Hakerët e shohin botën në terma të:

- Si funksionojnë gjërat
- Ku mund të thyhen
- Dhe si mund të rregullohen (ose të shfrytëzohen)

Nuk ka të bëjë me kaos. Ka të bëjë me kuriozitet. Mbrojtësit më të mirë janë kreativ. Ata shohin boshllëqet që të tjerët nuk i shohin. Mënyra e të menduarit është kjo:

“Po sikur të shtyp këtu? Po sikur dikush të ketë harruar të mbyllë këtë pjesë? Çfarë ndodh nëse ndryshoj këtë input?”

Kështu mendojnë hakerët. Dhe tani... ashtu mund të mendosh edhe ti.

2. Mentaliteti i hakerit = Kuriozitet + Skepticizëm

Do të kuptosh sistemet, jo thjesht t'i përdorësh ato. Le ta zbërthejmë:

◆ Kurioziteti

- Ti dëshiron t'i kuptosh sistemet, jo thjesht t'i përdorësh ato.
- Eksploron opsionet, hulumton se si funksionojnë gjërat.
- Pyet: “Çfarë ndodh nëse...?”

◆ Skepticizëm

- Nuk u beson verbërisht linqeve.
- Ti e vë në dyshim çdo hyrje ne faqe.

- Vëren modele të çuditshme që të tjerët i injorojnë.

Të dyja së bashku të bëjnë të fuqishëm. Nuk je më thjesht një “përdorues.” Ti bëhesh një gjuetar.

3. Fillo nga e vogla: Analizo atë që përdor çdo ditë

Provo këtë ushtrim: Shiko aplikacionin ose faqen tënde të preferuar dhe pyet:

- Çfarë ndodh kur klikoj “Forgot password”?
- Po sikur dikush të hamendësonte pyetjen time të sigurisë?
- A mund ta hap këtë në disa skeda dhe ta ngatërroj?
- A ndryshon URL-ja kur hyj? Çfarë tregon?

Nuk po thyen asgjë. Po mëson. Ky është fillimi i rekonesancës: një aftësi kyçe për hakerët etikë.

4. Praktiko “Ndërgjegjësimin Digjital” çdo ditë

Ashtu si mjeshtrit e arteve marciale që qëndrojnë vigjilentë në rrugë, profesionistët e kibernetikës qëndrojnë vigjilentë online. Shembuj:

- Vëren një link të rremë në një mesazh të një miku.
- Sheh që një hyrje në një faqe duket paksa ndryshe.

- Sheh një USB të hedhur diku dhe nuk e fut në kompjuter.

Këto vendime të vogla = mentaliteti i hakerit në veprim. Po stërvit syrin tënd.

5. Përdor të njëjtat mjete si hakerët e vërtetë

Po, seriozisht. Studentët e sigurisë kibernetike përdorin mjetet e njëjta që përdorin hakerët, por në laboratorë, jo në objektiva reale.

Mund të provosh:

- **TryHackMe** (sfida falas me lojëra hacking)
- **Shodan.io** (motor kërkimi për pajisje të ekspozuara)
- **VirusTotal** (skenon linke dhe skedarë për malwerë)
- **Burp Suite** (për testim web; fillo me versionin falas)
- **Wireshark** (shikon çfarë po ndodh në një rrjet)

E rëndësishme: Testo vetëm sisteme që i zotëron vetë ose për të cilat ke leje. Kjo është ajo që të bën etik.

6. Mëso të thyesh gjëra që të dish si t'i rregullosh

Të themi të drejtën: të thyesh gjëra është argëtuese. Por ajo që të bën një white hat (haker i mirë) është qëllimi yt.

Ti i thyen gjërat për të:

- Kuptuar ato
- Përmirësuar ato
- Ndihamuar të tjerët të qëndrojnë të sigurt

Kjo është arsyeja pse kompanitë paguajnë për këtë. Këtë e kërkojnë shkollat, spitalet dhe qeveritë.

7. Hakim në mënyrën e duhur (Kufijtë etikë)

Po:

- Merr pjesë në gara legale Capture The Flag (CTF)
- Hako mjedise testimi si TryHackMe ose Hack The Box
- Mëso nga kanalet e YouTube për hakerë etikë
- Kërko dobësi në sisteme të sigurta, me leje

Jo:

- Mos testo faqe ose aplikacione pa leje
- Mos hyr në llogari që nuk janë të tuat
- Mos shpërndajë të dhëna private ose "rrjedhje" që gjen
- Mos mendo se "po shoh vetëm" nuk bën dëm

Etika nuk ka të bëjë thjesht me rregulla, por me përgjegjësi

8. Mendo si një haker. Vepro si një mbrojtës.

Një haker etik i madh nuk di vetëm truket.

Ai di:

- Si operojnë sulmuesit e vërtetë
- Si mund të dështojnë sistemet
- Si mashtrohen njerëzit

Por gjithashtu:

- Di kur të ndalet
- Respekton kufijtë
- Punon për anën e mirë

Është si një mjeshtër çelësash që ndihmon në përmirësimin e dizajnit të dyerve.

Përmbledhje: Stërvit mendjen si një hake

Për të filluar të mendosh si një haker:

- Ji kurioz
- Vë në dyshim gjithçka
- Eksploro si funksionojnë gjërat
- Praktiko në mënyrë të sigurt
- Dhe vepro gjithmonë etikisht

Në kapitullin tjetër: Para se ta përmbyllim, le të flasim për higjienën kibernetike bazë, zakone të vogla që të mbrojnë që tani, edhe para se të fillosh karrierën.

KAPITULLI 11: Higjiena kibernetike që mund ta praktikosh sot



Nuk ke pse të jesh ekspert për të qëndruar i sigurt online.

Disa zakone të thjeshta bëjnë një ndryshim të madh. Le t'i bëjmë pjesë të jetës tënde të përditshme.

1. Çfarë është higjiena kibernetike?

Higjiena kibernetike është si higjiena personale.

- Lan dhëmbët çdo ditë për të parandaluar prishjen.
- Bën dush që të mos kundërmosh si çantë palestere.

- Pret thonjtë, pastron veshët dhe lan duart

Higjiena kibernetike = zakone të vogla digjitale që parandalojnë probleme të mëdha. Nuk ke nevojë për mjete të avancuara. Vetëm për qëndrueshmëri dhe ndërgjegjësim.

2. Përdor fjalëkalime të forta dhe unike

Nëse e përdor të njëjtin fjalëkalim kudo, është sikur të përdorësh një çelës të vetëm për shtëpinë, makinën, dollapin dhe biçikletën. Nëse ta vjedhin një herë, e zotërojnë gjithë jetën tënde.

Si ta rregullosh:

- Përdor fjalëkalime të ndryshme për çdo faqe.
- Bëji të gjatë (të paktën 12 karaktere).
- Shmang emrat, datat ose hamendjet e lehta.

Këshillë profesionale: Përdor një menaxher fjalëkalimesh (si Bitwarden ose 1Password).

Ai i mban mend të gjitha për ty.

3. Aktivizo Autentifikimin me Dy Faktorë (2FA)

Ky është një nga mbrojtjet më të fuqishme që mund të përdorësh.

Si funksionon:

- Ti hyn me fjalëkalimin tënd.
- Pastaj, konfirmon që je ti me një kod nga telefoni ose aplikacioni.

Edhe nëse dikush e vjedh fjalëkalimin tënd, prapë nuk hyn dot.

Ku ta përdorësh:

- Email
- Rrjete sociale
- Banka
- Çdo gjë e rëndësishme

Aktivizoje. Sot.

4. Mos kliko linke të rastësishme

Nëse diçka duket e dyshimtë, me shumë gjasë është.

Shembuj linqesh mashtruese:

- “Kliko këtu për të marrë çmimin tënd!”
- “Llogaria jote është pezulluar, hyni tani!”
- Linke të shkurtra (bit.ly, tinyurl) nga të panjohur

Çfarë të bësh në vend të kësaj:

- Shko direkt te faqja (mos kliko; shkruaje vetë adresën).

- Vendos maus-in mbi link për të parë ku të çon në të vërtetë.
- Pyet: A do të më kontaktonte realisht kjo kompani në këtë mënyrë?

Nëse je në dilemë, mos kliko. Kurrë.

5. Mbaj softuerin të përditësuar

Po, përditësimet janë bezdisëse. Po, ato kanë rëndësi. Shumica e hakerëve shfrytëzojnë dobësi të vjetra, gjëra që përditësimet i kanë rregulluar tashmë.

Çfarë të përditësosh:

- Telefonin
- Aplikacionet
- Laptopin
- Shfletuesin
- Ruterin (po, edhe atë)

Bëje zakon. Përditësime = rregullime = mbrojtje.

6. Shmang Wi-Fi publik (përveç nëse di çfarë bën)

Wi-Fi publik është si të bërtasësh fjalëkalimet në një sallë plot njerëz.

Opsione më të sigurtat:

- Përdor internetin mobil nëse është e mundur.
- Nëse duhet të përdorësh Wi-Fi publik, mos hyr në llogari të ndjeshme. Përdor një VPN (virtual private network) për të enkriptuar lidhjen

7. Mendo para se të ndash diçka

Një postim qesharak, një selfie e bukur, ose një tweet i zemëruar mund të duken të pafajshëm. Por... mund të:

- Zbulojnë vendndodhjen tënde
- Nxjerrin informacion personal
- Përdoren më vonë për të të imituar

Pyete veten:

- A do të isha në rregull nëse kjo do të behej screenshot dhe dërgohej te të huajt?
- Po zbuloj më shumë se ç'mendoj?

Gjurmët digjitale janë të përhershme. Ec me kujdes.

8. Përdor antivirus (edhe atë falas)

Antivirusi nuk është i përsosur. Por ndihmon të kapë malwerët bazë përpara se të përhapen.

Opsione të mira falas:

- Windows Defender (i integruar në Windows)

- Bitdefender Free
- Avast ose AVG (me kujdes; shmang mbingarkesën e panevojshme)

Mos u mbështet vetëm tek ai. Mendoje si rrip sigurimi, të mos përplasësh është gjithmonë më mirë

9. Bëj kopje rezervë të të dhënave

Nëse bie pre e ransomware, ose laptopi prishet, ose skedarët fshihen...

Do të doje të kishe një backup.

Çfarë të ruash:

- Foto
- Projekte shkollore
- Dokumente
- Çdo gjë që të intereson

Ku ta ruash:

- Disk i jashtëm
- Shërbim cloud (Google Drive, Dropbox, iCloud)

Bëje rregullisht. Vetja jote e së ardhmes do të falënderojë.

10. Fol për këtë

Higjiena kibernetike bëhet më e fortë kur shpërndahet.

Ndihmo:

- Prindërit të përditësojnë pajisjet
- Vëllezërit e motrat të shmangin shkarkimet e dyshimta
- Miqtë të mos përdorin ende “123456” si fjalëkalim

Nuk ke pse të predikosh. Thjesht bëhu ai i zgjuari i grupit.

Siguria përhapet.

Përmbledhje: Zakone të vogla, mbrojtje e madhe

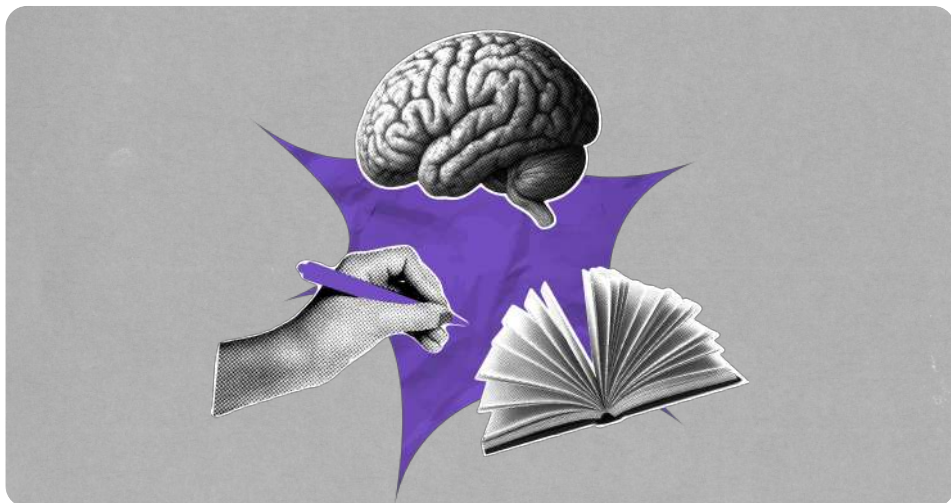
Fillo këtu. Fillo tani.

- Fjalëkalime unike
- 2FA kudo
- Mos kliko linqe të dyshimta
- Përditëso gjithçka
- Bëj backup të dhënave
- Qëndro vigjilent dhe i vetëdijshëm

Nuk ke pse t'i bësh të gjitha menjëherë. Por sa më shpejt të fillosh, aq më i sigurt do të jesh.

Në kapitullin tjetër: Le ta përmbyllim këtë udhëtim me hapat e tu të ardhshëm: si të vazhdosh të mësosh, si të eksplorosh karrierat kibernetike në Kosovë dhe si ta marrësh seriozisht këtë fushë, pa humbur argëtimin.

Si të Marrësh Edukim në Siguri Kibernetike në Kosovë



Pse Kjo Ka Rëndësi

Qëllimi i Kapitullit: T'i tregojë studentëve se nëse duan të bëhen pjesë e botës kibernetike, Kosova ofron rrugë arsimore - si akademike ashtu edhe profesionale që mund t'i çojnë deri atje. Nuk është e nevojshme të shkosh jashtë vendit për të filluar rrugëtimin tënd në fushën e sigurisë kibernetike. Në Kosovë ka universitete, kolegje dhe qendra trajnimi që tani ofrojnë programe të

mirëfillta në këtë fushë. ofrë që dëshiron një diplomë, një trajnim praktik intensiv (bootcamp), apo një certifikatë profesionale, ke mundësi të zgjedhësh.

KAPITULLI 2: Universitetet – Rruga Akademike

1. Universiteti i Prishtinës (FIEK)

- Ende nuk ka një program të dedikuar vetëm për sigurinë kibernetike.
- Por: studentët mund të marrin pjesë në gara, konferenca dhe projekte anësore që zhvillojnë aftësi kibernetike.

2. Universiteti për Biznes dhe Teknologji (UBT)

- Bachelor në Studime të Sigurisë (3 vite, me fokus në Sigurinë Kibernetike).
- Mëson teori + praktikë: politika sigurie, strategji kibernetike dhe aftësi teknike.

3. Kolegji AAB

- Bachelor në Siguri Kibernetike (3 vite).
- Fokus: ndërtimi i një komuniteti kombëtar kibernetik, zhvillimi i kompetencave institucionale, menaxhimi i rrezikut dhe zbatimi i standardeve ndërkombëtare.

4. Kolegji Universum

- Bachelor Profesional në Siguri Kibernetike (3 vite).
- Qasje praktike dhe e orientuar drejt mbrojtjes së sistemeve dhe ndalimit të sulmeve.
- Inkurajon pjesëmarrjen në iniciativa kibernetike kombëtare dhe ndërkombëtare.

KAPITULLI 3: Përtej Universiteteve – Shkolla Profesionale & Trajnime

Jo të gjithë kanë nevojë për një diplomë të plotë. Disa shkolla dhe qendra ofrojnë programe më të fokusuara dhe më të shkurtra.

◆ Cactus Education

- Program i akredituar 2-vjeçar në ICT me drejtim në siguri kibernetike.
- Aftësi: mbrojtja e sistemeve, analiza e rreziqeve, testimi i sigurisë, reagimi ndaj incidenteve.

◆ Roi Academy

- Trajnim intensiv 6–12 muaj.
- Partneritete me industri = projekte praktike.
- Mbulojnë: parandalimin e sulmeve, sigurimin

e sistemeve, mbrojtjen e të dhënave.

◆ Qendra Shtetërore e Trajnimit për Siguri Kibernetike (Ministria e Mbrojtjes & FSK)

- Trajnime të udhëhequra nga ekspertë vendorë dhe ndërkombëtarë.
- Tema: menaxhimi i incidenteve, diplomacia kibernetike, mbrojtja e infrastrukturës kritike.

◆ Qendra e Sigurisë Kibernetike AAB

- Programi i parë profesional i akredituar në Kosovë.
- Bashkëpunime ndërkombëtare: Capitol Technology University (SHBA), laboratorë dhe projekte të përbashkëta.
- Fokus: siguria e të dhënave, analiza e sulmeve kibernetike, mekanizmat e mbrojtjes.

◆ ICT Kosovo

- Module trajnimi profesional.
- Specialitete: Hakerim Etik, Forenzikë Digjitale, Menaxhim i Incidenteve.

◆ Bit Academy

- E themeluar në vitin 2013.
- Programe të shkurtra dhe intensive (1–2 muaj).
- Mbulojnë: Cisco CCNA, Siguri Kibernetike, QA Testing, Web Development dhe më shumë.

KAPITULLI 4: Platforma Online & Laboratorë

◆ Cyberlance

- Trajnim virtual, praktik në fushën e sigurisë kibernetike.
- Simulime realiste = ambient i sigurt për të ushtruar sulme dhe mbrojtje.
- Përdoret nga studentë, profesionistë dhe madje edhe kompani

KAPITULLI 5: Zgjedhja e Rrugës Tënde

Pyet veten:

- A dua një diplomë (3 vite, bazë akademike + bazë të karrieres)?
- Apo preferoj trajnim të shkurtër dhe praktik (muaj, aftësi praktike)?
- Apo dua një kombinim të të dyjave - një diplomë plus certifikata profesionale?

Lajm i mirë: Kosova tani ofron të treja opsionet.

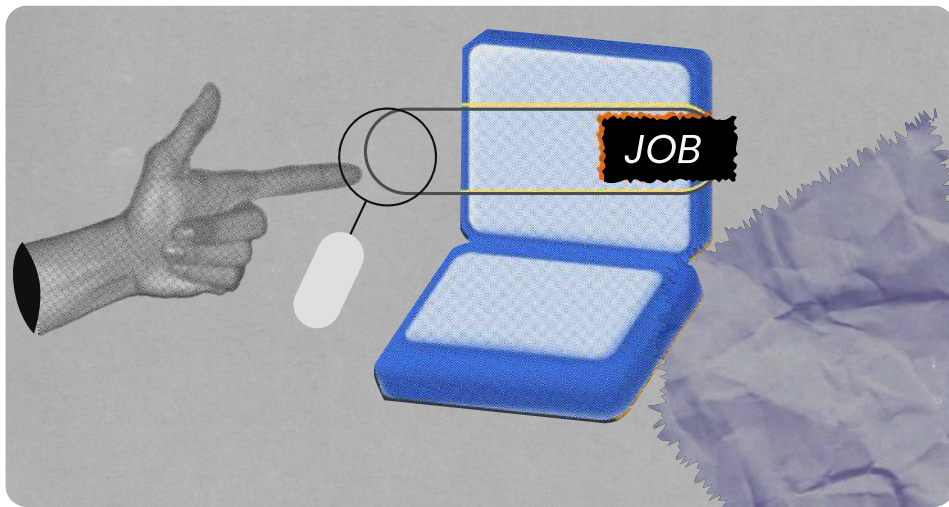
Përmbledhje

Nuk ke nevojë të largohesh nga Kosova për të studiuar sigurinë kibernetike.

- **Universitetet:** UBT, AAB, Universum (programe të dedikuara).
- **Shkolla Profesionale:** Cactus, Roi Academy, Bit Academy, ICT Kosovo.
- **Qendra të Specializuara:** Qendra e Sigurisë Kibernetike AAB, Qendra Shtetërore e Trajnimit.
- **Platforma Online:** Cyberlance.

Zgjedhja jote varet nga sa thellë dëshiron të shkosh - dhe sa shpejt. Në çdo rast, mundësitë tashmë janë këtu.

Ku të Punosh në Sigurinë Kibernetike në Kosovë



KAPITULLI 1: Pse Punët në Siguri Kibernetike janë Kudo

Qëllimi i Kapitullit: T'u tregojë lexuesve se siguria kibernetike nuk është vetëm “një karrierë” - por qindra role të shpërndara në qeveri, banka, kompani teknologjie, OJQ, madje edhe në spitale ose aeroporte.

Siguria kibernetike po rritet me shpejtësi. Çdo organizatë që përdor kompjuterë, rrjete apo të dhëna (pra, pothuajse të gjitha) ka nevojë për mbrojtje

Kjo do të thotë që vendet e punës po hapen në gjithë Kosovën - në qeveri, banka, telekom, startupe dhe infrastrukturë kritike. Nëse i fiton aftësitë, kërkesa për to tashmë të pret.

KAPITULLI 2: Karriera në Sektorin Publik

Qeveria e Kosovës po ndërton institucione të forta në fushën e sigurisë kibernetike. Të punosh këtu do të thotë të mbrosh gjithë vendin.

1. Agjencia për Siguri Kibernetike (ASK)

- Institucioni kryesor për mbrojtjen kibernetike në Kosovë.
- Monitoron, koordinon dhe reagon ndaj kërcënimeve në shkallë vendi.
- Mban regjistrin zyrtar të incidenteve kibernetike.
- Punë: analistë kibernetikë, specialistë politikash, përgjegjës për incidente.

2. Këshilli Shtetëror për Siguri Kibernetike (KSHSK)

- Organ këshillues që bashkon qeverinë, biznesin, organet e rendit dhe akademinë.
- Fokus: strategjia kombëtare, bashkëpunimi dhe vendimet në nivel të lartë

- Punë: ekspertë që kontribuojnë në analiza, hulumtime dhe zhvillim politikash

3. KOS-CERT (Ekipi i Reagimit Emergjent për Kompjuterë)

- CERT-i kombëtar zyrtar i Kosovës, nën rregullatorin e telekomunikimeve (RAEC).
- Zbulon sulme, koordinon reagimin, mbështet hetimet, trajnon institucionet.
- Punon me partnerë ndërkombëtarë si ENISA.
- Punë: specialistë kibernetikë, hulumtues kërcënimesh, inxhinierë rrjeti.
- Hyrje e mirë: praktika dhe pozita si analist i ri.

4. CSIRT-et Sektoriale Kombëtare

- Ekiye të krijuara për sektorët kritikë (energji, shëndetësi, transport, telekom).
- Çdo sektor ndërton ekipin e vet për t'u mbrojtur nga incidentet kibernetike.
- Punë: analistë të fokusuar në rreziqe sektoriale (p.sh. rrjeti elektrik, IT i spitaleve).

5. CSIRT-et e Operatorëve të Shërbimeve Thelbësore

- Çdo operator i shërbimeve kritike (si energjia elektrike, uji, apo transporti) duhet të ketë një CSIRT ose së paku një zyrtar kibernetik.

- Punë: inxhinierë sigurie sistemi, përgjegjës për incidente në shërbimet jetike.

6. CSIRT-et e Ofruesve të Shërbimeve Digjitale (DSP)

- Mbrojnë shërbimet online si platformat cloud, rrjetet sociale apo e-commerce.
- Punë: oficerë të sigurisë kibernetike që monitorojnë funksionimin, mbrojtjen e të dhënave dhe përputhshmërinë me standardet.

KAPITULLI 3: Karriera në Sektorin Financiar

Bankat janë objektiva kryesore për hakerët - që do të thotë edhe punëdhënësit të mëdhenj për profesionistët e sigurisë kibernetike

Banka Qendrore e Kosovës (BQK)

- Vendos rregullat për mbrojtjen kibernetike në sektorin financiar.
- Punëson specialistë për të mbikëqyrur përputhshmërinë dhe menaxhimin e rreziku

Bankat Komerciale (shembuj):

- Raiffeisen Bank
- BKT

- ProCredit Bank
- Banka Ekonomike
- Banka për Biznes
- Ziraat Bank
- PriBank
- Credins Bank
- IS Bank

Rolet përfshijnë:

- CISO (Drejtori i Sigurisë së Informacionit)
- Menaxher i Sigurisë së IT-së
- SOC Analyst (Analist në Qendrën e Operacioneve të Sigurisë)
- Oficer i Forenzikës Digjital

Raiffeisen Bank – Komuniteti Tech4Tech

- I fokusuar në inovacion dhe zhvillim.
- Ekipi i sigurisë kibernetike mbron sistemet bankare dhe bashkëpunon me IT & Komunikimin.
- Ofron praktika dhe hapësira mësimi për studentët e interesuar në siguri kibernetike.

Institucionet Mikrofinanciare (shembuj):

KEP Trust, FINCA, KosInvest, Grameen Trust, Rural Finance Kosovo, ACP. Këta aktorë më të vegjël gjithashtu kanë nevojë për mbrojtje kibernetike, sidomos për bankingun mobil dhe të dhënat e klientëve

KAPITULLI 4: Sektori Privat & Konsulence

Sektori privat është fusha më e larmishme për karrierat në siguri kibernetike. Nga telekomet e mëdha deri te startup-et, çdo kompani që menaxhon të dhëna të ndjeshme ka nevojë për ekspertë.

Kompani të Telekomunikacionit

- IPKO dhe Artmotion menaxhojnë rrjete të mëdha për miliona përdorues.
- Punë: mbrojtës rrjetesh, analistë SOC, testues penetrimi.
- IPKO gjithashtu organizon Konferencën e Sigurisë Kibernetike - mundësi e shkëlqyer për rrjetëzim.

Firma të Sigurisë Kibernetike

- **Arcus Security** – Siguri ofensive, pentesting, red teaming, cloud, inxhinieri sociale.
- **Pretera** – Testim penetrimi në rrjete dhe aplikacione, red teaming.
- **CISTCK LLC** – Pen testing, auditime, inteligjencë mbi kërcënimet.
- **Sentry Security** – Pentesting, siguri e menaxhuar.
- **Void International** – Shërbime të menaxhuara IT + siguri kibernetike.

- **Interandria** – Rrjetëzim, IT, siguri kibernetike me role për fillestarë.
- **Quipu** – Konsulencë IT për banka (me zyrë në Kosovë).
- **XY Cyber** – Sisteme të avancuara të sigurisë kibernetike + AI.

Kompani të Softuerit & Teknologjisë

- **KODE Labs** – Platforma për ndërtesa inteligjente.
- **Starlabs** – Outsourcing, zhvillim, shërbime IT.
- **BBros** – Shërbime AI + siguri kibernetike.
- **Kutia** – Zgjidhje të personalizuar web/softuerike.
- **LinkPlus IT** – Softuer për ndërmarrje, QA, projekte në aviacion/automotiv.
- **Tenton** – Zhvillim web/aplikacione/softueri.
- **Sogody** – E-commerce, platforma AI.
- **xValue** – Shkencë të dhënash + zgjidhje softuerike.

Pse ka rëndësi: Në kompanitë e teknologjisë, rolet e sigurisë kibernetike kombinohen me zhvillimin e softuerit, QA dhe sigurinë në cloud. Nëse je i/e interesuar në kodim, ky sektor është i përkryer.

Kapitulli 5: OJQ-të & Shoqëria Civile

Jo të gjitha punët në siguri kibernetike janë në korporata. OJQ-të në Kosovë gjithashtu punësojnë profesionistë të sigurisë kibernetike për të punuar në vetëdijësim, hulumtime dhe avokim.

- Women4Cyber Kosovo – Pjesë e nismës evropiane për fuqizimin e grave në siguri kibernetike.
- Albanian Cyber Association (ACA) – E fokusuar në të drejtat digjitale, inovacion dhe vetëdijësim.
- Sense Cyber Research Center – Punon në fushën e rregullimit, privatësisë, pronësisë intelektuale dhe krimit kibernetik.
- KCSS (Qendra Kosovare për Studime të Sigurisë) – Hulumton kërcënimet kibernetike, dezinformimin dhe politikat.

Punët këtu shpesh përfshijnë:

- Trajnerë të sigurisë kibernetike
- Hulumtues politikash
- Projektues të fushatave të vetëdijësimit
- Mbrojtës të të drejtave digjitale

Kapitulli 6: Infrastruktura Kritike

Infrastruktura kritike = shtylla kurrizore e vendit. Mbrojtja e saj është mision i sigurisë kombëtare.

Energjia

- KEK (Korporata Energjetike e Kosovës)
- KOSTT (Operatori i Transmetimit)
- KEDS/KESCO (Distribuími & Furnizimi)

Transporti

- Aeroporti Ndërkombëtar i Prishtinës
- Trainkos (hekurudha)
- Autoritetet rrugore/transportuese

Shëndetësia

- Qendra Klinike Universitare e Kosovës (QKUK)
- Instituti Kombëtar i Shëndetësisë Publike
- Spitale/klinika private

Uji

- Kompanitë Rajonale të Ujësjetlësit (p.sh., Prishtina, Hidrodrini)
- Ndërmarrjet komunale për menaxhimin e kanalizimeve

Infrastruktura Digjitale

- IPKO, Vala, ArtMotion (telekom)

Administrata Publike

- Ministritë, komunat, Kuvendi

Prodhimi & Distribuími i Ushqimit

- Fabrikat si Devolli ose Pestova
- Ditributor dhe depo të mëdha

Punët në infrastrukturën kritike shpesh përfshijnë:

- Sigurimin e sistemeve SCADA/industriale
- Monitorimin e rrjeteve për sulme
- Reagim ndaj incidenteve në shërbime jetike

Kapitulli 7: Harta e Karrierës Tënde në Cyber

Ja pamja e përgjithshme e vendeve ku mund të punosh në Kosovë:

- **Qeveria** – Mbronë vendin.
- **Bankat** – Mbronë paratë dhe besimin.
- **Kompanitë Private** – Ndërton dhe siguron teknologjinë.
- **OJQ-të** – Avokon dhe edukon.
- **Infrastruktura Kritike** – Mbanë shoqërinë në funksion.

Siguria kibernetike nuk është një rrugë e vetme. Është një ekosistem. Dhe Kosova po e ndërton atë me shpejtësi.

