

MATERIAL MËSIMOR

Në mbështetje të mësimdhënësve për kualifikimin profesional

Teknologji informacioni dhe komunikimi-TIK

Niveli II i KSHK-së

Ky material mësimor i referohet:

- **Lëndës profesionale: “Bazat e sigurisë së të dhënave”, kl. 11 (L-26-764-25)**

Përgatiti:

Anisa Melishte

Dritan Nito

Elida Mesi

Entela Sholla

Kleona Elezi

Tiranë, 2025

Tema 1: Kuadri ligjor dhe rregulloret në sigurinë kibernetike.

1.1 Hyrje

Në ditët e sotme, teknologjia dhe interneti janë bërë pjesë e pandarë e jetës sonë. Ne përdorim rrjete kompjuterike për komunikim, mësim, punë dhe shërbime të ndryshme online. Por, ashtu si në botën reale, edhe në botën digjitale ekzistojnë rreziqe që lidhen me vjedhjen e të dhënave, përhapjen e viruseve apo sulmet ndaj sistemeve kompjuterike. Këto rreziqe quhen kërcënime kibernetike, dhe mbrojtja ndaj tyre quhet siguri kibernetike.

1.2 Kuadri ligjor ndërkombëtar

Siguria kibernetike nuk është vetëm një çështje kombëtare, por edhe një problem global. Interneti nuk njihet kufij, dhe një sulm kibernetik që ndodh në një shtet mund të prekë shumë vende të tjera në të njëjtën kohë. Për këtë arsye, bashkëpunimi ndërkombëtar është shumë i rëndësishëm për të mbrojtur rrjetet, sistemet dhe të dhënat në mbarë botën.

➤ Konventa e Budapestit (2001)

Konventa e Budapestit është dokumenti kryesor ndërkombëtar që ka për qëllim luftimin e krimeve që kryhen përmes kompjuterëve dhe internetit. Ajo është miratuar në vitin 2001 nga Këshilli i Europës, dhe pjesë e saj janë shumë shtete në mbarë botën, përfshirë edhe Shqipërinë.

Konventa e Budapestit krijon **rregulla të përbashkëta** për të mbrojtur përdoruesit dhe rrjetet kompjuterike në mbarë botën, duke ndihmuar që krimet kibernetike të mos mbeten pa u ndëshkuar. **Materiali i plotë në lidhje me përmbajtjen e Konventës gjendet në linkun: <https://rm.coe.int/1680081561>**

➤ Strategjia e BE-së për Sigurinë Kibernetike

Strategjia e BE-së për Sigurinë Kibernetike përcakton objektivat strategjike për një Europë më të sigurt digjitalisht dhe kërkon koordinim mes shteteve anëtare për mbrojtjen e rrjeteve kritike. Strategjia e Bashkimit Europian për Sigurinë Kibernetike është një plan i përbashkët që synon të bëjë Europën më të sigurt dhe më të qëndrueshme në botën digjitale.

Në thelb, Strategjia e BE-së synon të sigurojë që çdo qytetar dhe institucion në Europë të jetë më i mbrojtur në botën online, dhe që shtetet të reagojnë së bashku kundër çdo lloj sulmi kibernetik. Link: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>

➤ Roli i organizatave si ENISA (Agjencia e Bashkimit Europian për Sigurinë Kibernetike)

Organizata të tilla si ENISA (Agjencia e Bashkimit Europian për Sigurinë Kibernetike) kanë një rol shumë të rëndësishëm në sigurinë digjitale të Europës. Qëllimi i tyre kryesor është të ndihmojnë vendet e BE-së, institucionet, organizatat publike dhe private për të parandaluar, zbuluar, menaxhuar dhe reaguar ndaj sulmeve kibernetike. Link zyrtar: <https://www.enisa.europa.eu/>

➤ Rregullorja e BE-së NIS2 (2023)

Rregullorja e BE-së NIS2 (2023) rregullon sigurinë e rrjeteve dhe sistemeve të informacionit, duke vendosur detyrime të reja për institucionet publike dhe bizneset kritike. Link zyrtar: <https://digital-strategy.ec.europa.eu/en/policies/nis-directive>

➤ NATO Cyber Defence Policy

NATO Cyber Defence Policy është politika e NATO-s që përcakton mënyrën se si Aleanca mbron veten nga sulmet kibernetike dhe si bashkëpunon ndërmjet shteteve anëtare në fushën e mbrojtjes digjitale.

Faqja zyrtare: https://www.nato.int/cps/en/natohq/topics_78170.htm

➤ **Normat dhe rezolutat e Kombeve të Bashkuara (UN Norms & Resolutions)**

Normat dhe rezolutat e Kombeve të Bashkuara (*UN Norms & Resolutions*) në fushën e sigurisë kibernetike janë udhëzime ndërkombëtare që synojnë të rregullojnë sjelljen e shteteve në hapësirën kibernetike dhe të ruajnë paqen dhe stabilitetin global. Faqja zyrtare: <https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf>

1.3 Kuadri ligjor kombëtar

Në Shqipëri, siguria kibernetike është bërë një nga fushat më të rëndësishme të mbrojtjes dhe zhvillimit të shoqërisë digjitale. Me rritjen e përdorimit të internetit, rrjeteve kompjuterike dhe shërbimeve online, është shtuar nevoja për rregulla të qarta ligjore që mbrojnë qytetarët, institucionet dhe bizneset nga rreziqet kibernetike. Për këtë arsye, shteti shqiptar ka ndërtuar një kuadër ligjor kombëtar që përcakton detyrimet, përgjegjësitë dhe strukturat që merren me sigurinë e rrjeteve dhe të dhënave. Ligji më i rëndësishëm në këtë fushë është **Ligji nr. 2/2017 “Për sigurinë kibernetike”**, Ky ligj përcakton masat që duhet të merren për parandalimin, zbulimin dhe trajtimin e incidenteve kibernetike. Ky ligj është në përputhje me direktivat e Bashkimit Europian, si Direktiva NIS, duke e afruar Shqipërinë me standardet ndërkombëtare të sigurisë digjitale. Përveç këtij ligji, janë miratuar edhe **akte nënligjore dhe rregullore** që sqarojnë mënyrën e zbatimit në praktikë, si dhe janë ngritur institucione të posaçme, si **Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK)**, që mbikëqyr dhe koordinon veprimet në këtë fushë.

➤ **Ligji nr. 2/2017 “Për sigurinë kibernetike”**

Ky ligj është thelbësor për sigurinë kibernetike në Shqipëri, pasi përcakton rregullat, detyrimet dhe institucionet përgjegjëse për mbrojtjen e rrjeteve dhe sistemeve të informacionit. Ai është pjesë e përpjekjes së Shqipërisë për të harmonizuar ligjet e saj me standardet ndërkombëtare dhe direktivat e Bashkimit Europian, si Direktiva NIS. Ligji i plotë gjendet në linkun: https://aksk.gov.al/wp-content/uploads/2020/07/Ligji-Per_Sigurine_Kibernetike_Nr_2_Date_26.1.2017-1.pdf

➤ **Udhëzimet e AKCESK (Agjencia Kombëtare e Certifikimit Elektronik dhe Sigurisë Kibernetike)**

AKCESK është institucioni kryesor që mbikëqyr zbatimin e ligjit nr. 2/2017 “Për sigurinë kibernetike” dhe harton udhëzime dhe rekomandime për institucionet publike, operatorët e shërbimeve kritike dhe bizneset që përdorin rrjete dhe sisteme të informacionit.

Faqja zyrtare e AKCESK: <https://www.akcesk.gov.al>

➤ **Strategjia kombëtare për Sigurinë Kibernetike (2025–2030)**

Strategjia Kombëtare për Sigurinë Kibernetike (2025–2030) është një dokument strategjik që përcakton objektivat dhe prioritetet për forcimin e reziliencës kibernetike të shtetit. Strategjia Kombëtare për Sigurinë Kibernetike është dokumenti kryesor planifikues dhe udhëzues për politikën e sigurisë digjitale në Shqipëri për periudhën 2025–2030. Ajo synon të përforcojë mbrojtjen e rrjeteve dhe sistemeve kritike, të sigurojë që institucionet publike dhe bizneset të jenë më të përgatitura ndaj sulmeve kibernetike dhe të përputhen me standardet ndërkombëtare.

Link zyrtar: <https://aksk.gov.al/wp-content/uploads/2025/10/Plan-veprimi-2025-2027.pdf>

1.4 Rregullore dhe standarde kryesore

➤ **ISO/IEC 27001 – Standard ndërkombëtar për menaxhimin e sigurisë së informacionit**

ISO/IEC 27001 është një standard ndërkombëtar që përcakton kërkesat për krijimin, zbatimin, mbajtjen dhe përmirësimin e një Sistemi të Menaxhimit të Sigurisë së Informacionit (ISMS) brenda një organizate. Ai

është një nga standardet më të njohura dhe më të përdorura globalisht për të garantuar sigurinë e informacionit.

➤ **ISO/IEC 27002 – Udhëzues për praktikat më të mira në mbrojtjen e të dhënave**

ISO/IEC 27002 është një udhëzues ndërkombëtar që ofron praktika më të mira për menaxhimin dhe mbrojtjen e informacionit brenda organizatave. Ky standard përdoret së bashku me ISO/IEC 27001, por fokusohet më shumë tek kontrollat dhe masat konkrete të sigurisë, ndërsa 27001 përcakton kërkesat për Sistemin e Menaxhimit të Sigurisë së Informacionit (ISMS).

➤ **GDPR - Rregullorja e përgjithshme për mbrojtjen e të dhënave**

GDPR (*General Data Protection Regulation*) është një rregullore e Bashkimit Europian që ka hyrë në fuqi më 25 maj 2018 dhe ka për qëllim të mbrojë të dhënat personale të qytetarëve dhe të rrisë kontrollin e tyre mbi informacionin që përdoret nga organizatat dhe bizneset. Rregullorja është e zbatueshme në të gjitha vendet e BE-së, si dhe në organizatat jashtë BE-së që përpunojnë të dhëna të qytetarëve të BE-së.

1.5 Institucione përgjegjëse për sigurinë kibernetike

- **AKCESK** (Agjencia Kombëtare për Certifikimin Elektronik dhe Sigurinë Kibernetike)
- **CERT Albania** (Njësia kombëtare për reagim ndaj incidenteve kibernetike)
- **Drejtoria e Krimit Kibernetik** (Policia e Shtetit)
- **Njësitë e sigurisë kibernetike në ministrinë dhe institucionet publike.**

Tema 2: Pajisjet për sigurinë kibernetike

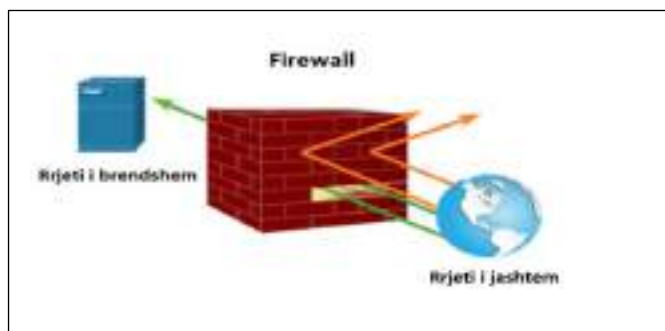
2.1 Hyrje

Në epokën digjitale, ku informacioni dhe të dhënat personale, financiare dhe profesionale ruhen dhe transmetohen në mënyrë elektronike, siguria kibernetike ka marrë një rol thelbësor. Me rritjen e vazhdueshme të kërcënimeve kibernetike, si sulmet e malware, ransomware, phishing apo sulmet ndaj infrastrukturave kritike, mbrojtja e sistemeve kompjuterike është bërë më e nevojshme se kurrë.

2.2 Paisja e sigurisë Firewall

Përkufizimi:

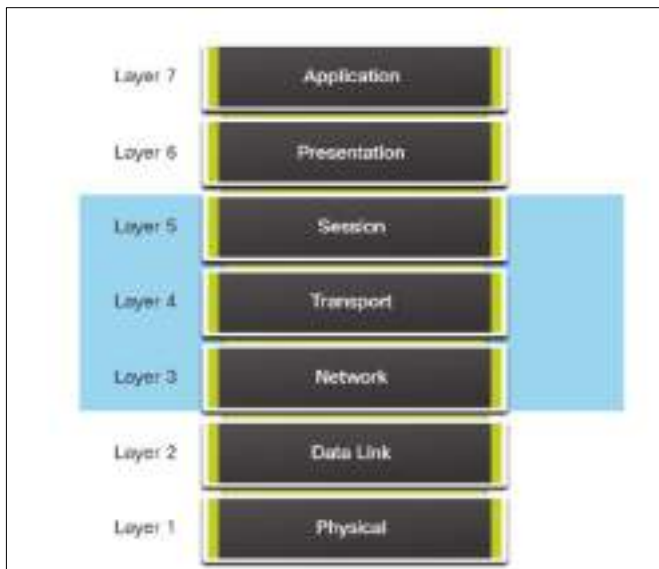
Firewall-i është një pajisje harduer-ike ose software-ike e specializuar, e dizenuar për të kontrolluar dhe filtruar trafikun e rrjetit midis një rrjeti të brendshëm të besueshëm dhe një rrjeti të jashtëm potencialisht të rrezikshëm, si Interneti. Vepron si një barriërë mbrojtëse, duke siguruar që vetëm komunikimet e autorizuara të mund të hyjnë ose të dalin nga rrjeti.



Funksionimi:

- ✓ Firewall-i analizon paketat e të dhënave sipas rregullave të paracaktuara, duke vlerësuar parametra si adresa IP në burim dhe destinacion, portet, protokollet, dhe përmbajtja e paketës.
- ✓ Mund të implementojë politika të avancuara të kontrollit të trafikut, përfshirë filtrimin bazuar në gjendje (*stateful inspection*), kontrollin e aplikacioneve (*application layer filtering*) dhe parandalimin e ndërhyrjeve (*IPS integration*).

Figura 2.2.1: Ilustrim i funksionit të Firewall



Vetitë e zakonshme të Firewall-eve:

Të gjitha firewall-et ndajnë disa karakteristika të përbashkëta:

- Firewall-et janë rezistentë ndaj sulmeve të rrjetit.
- Firewall-et janë pika e vetme tranzitimi midis rrjeteve të brendshme të institucioneve dhe rrjeteve të jashtme, sepse i gjithë trafiku kalon përmes firewall-it.
- Firewall-et zbatojnë politikën e kontrollit të aksesit.

➤ Llojet e Firewall-eve

Është e rëndësishme të kuptojmë llojet e ndryshme të firewall-eve dhe kapacitetet e tyre specifike, në mënyrë që të përdoret firewall-i i duhur për çdo situatë.

Llojet kryesore të firewall-eve:

1- Firewall-i tradicional (*Packet Filtering, Stateless*): Filtron trafikun në bazë të *header*-it të paketës, duke vendosur rregulla të thjeshta për IP-te dhe portet. Firewall me filtrim paketash zakonisht janë pjesë e një firewall-i të router-it, i cili lejon ose ndalon trafikun bazuar në informacionin e Shtresës 3 dhe Shtresës 4. Ata janë firewall-e *stateless* që përdorin një tabelë të thjeshtë si politikë për të filtruar trafikun bazuar në kritere specifike.

Filtrat e paketave nuk përfaqësojnë një zgjidhje të plotë firewall-i, por janë një element i rëndësishëm i politikës së sigurisë së firewall-it.

Filtrat e paketave janë *stateless*, që do të thotë se shqyrtojnë çdo paketë individualisht, jo në kontekstin e gjendjes së një lidhjeje.

2- Firewall-i *stateful*: Analizon gjendjen e lidhjeve dhe monitoron se si paketat lidhen me sesionet ekzistuese, duke ofruar mbrojtje më të avancuar. Firewall-et *stateful* janë teknologjitë më të zakonshme dhe me përdorim më të shumëanshme të firewall-eve. Firewall-et *stateful* ofrojnë filtrim paketash me gjurmim të gjendjes (*stateful*) duke përdorur informacionin e lidhjeve të ruajtur në një tabelë gjendjeje (*state table*). Filtrimi *stateful* është një arkitekturë firewall-i që klasifikohet në shtresën e rrjetit (*network layer*). Ai gjithashtu analizon trafikun në Shtresën 4 dhe Shtresën 5 të modelit OSI.

2.3- Firewall-et me politikë të bazuar në zona (*Zone-Based Policy Firewalls - ZPF*)

Firewall-et me politikë të bazuar në zona (ZPF) përdorin konceptin e zonave për të ofruar fleksibilitet shtesë. Një zonë është një grup prej një ose më shumë ndërfaqesh që kanë funksione ose karakteristika të ngjashme. Zonat ndihmojnë në përcaktimin se ku duhet të aplikohet një rregull ose politikë firewall në Cisco IOS. Politikat e sigurisë për LAN 1 dhe LAN 2 janë të ngjashme dhe mund të grupohen në një zonë për konfigurimet e firewall-it. Si parazgjedhje, trafiku midis ndërfaqesh në të njëjtën zonë nuk është subjekt i asnjë politike dhe kalon lirshëm. Megjithatë, i gjithë trafiku nga një zonë në një tjetër bllokohet. Për të lejuar trafikun midis zonave, duhet të konfigurohet një politikë që lejon ose inspekton trafikun. Përjashtimi i vetëm nga politika parazgjedhje "*deny any*" është zona "*self*" e router-it. Zona *self* është vetë router-i dhe përfshin të gjitha adresat IP të ndërfaqesh të router-it. Konfigurimet e politikave që përfshijnë zonën *self* do të aplikohen për trafikun që ka destinacion dhe burim router-in. Si parazgjedhje, nuk ka politikë për këtë lloj trafiku. Trafiku që duhet marrë parasysh kur dizajnohet një politikë për zonën *self* përfshin trafikun e planeve të menaxhimit dhe kontrollit, si SSH, SNMP dhe protokollet e routing-ut.

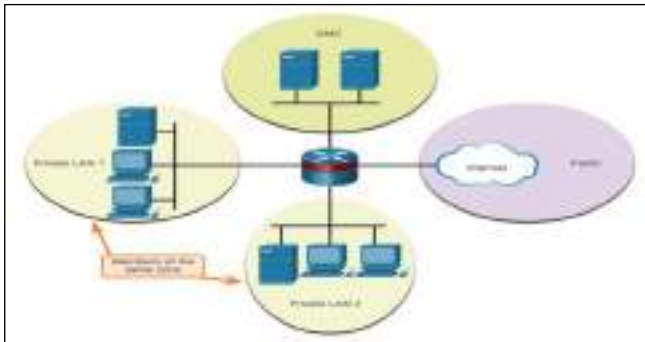
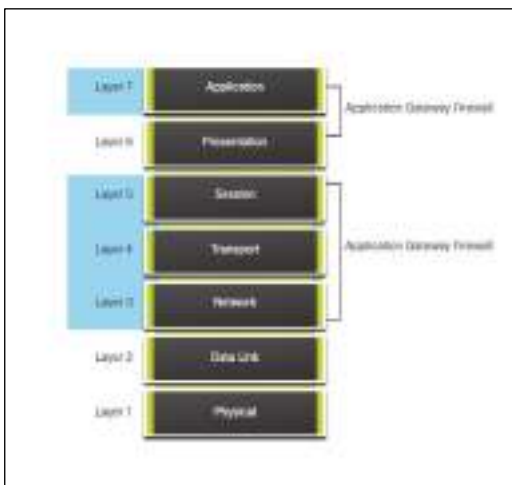


Figura 2.2.4: Firewall në arkitekturën me politikë të bazuar në zona

2-Firewall me Portë Aplikacioni (Application Gateway Firewall): Një firewall me portë aplikacioni (ose firewall proxy), siç tregohet në figurë, filtron informacionin në Shtresat 3, 4, 5 dhe 7 të modelit referencë OSI. Shumica e kontrollit dhe filtrimit të firewall-it bëhet përmes softwareit.

Kur një klient ka nevojë të qaset në një server të largët, ai lidhet me një server proxy. Serveri proxy lidhet me serverin e largët në emër të klientit. Prandaj, serveri sheh vetëm një lidhje nga serveri proxy.



3- Next-Generation Firewall (NGFW): Përfshin filtrim të avancuar bazuar në aplikacione, identitet të përdoruesit, kontroll mbi trafikun e SSL/TLS dhe integrim me mekanizma për zbulimin e kërcënimeve. Firewall-et e gjeneratës së ardhshme (NGFW) shkojnë përtej firewall-eve stateful duke ofruar:

- Parandalim të integruar të ndërhyrjeve (Integrated Intrusion Prevention)
- Ndërgjegjësim dhe kontroll mbi aplikacionet për të identifikuar dhe bllokuar aplikacione të rrezikshme
- Rrugë për përmirësime që përfshijnë burime të ardhshme informacioni
- Teknikat për të adresuar kërcënimet e sigurisë që evoluojnë me kohën

Figura 2.2.9: Shembuj të pajisjeve firewall Next-Generation

2.4 Switch i menaxhueshëm

Një Switch i menaxhueshëm është pajisje rrjeti që jo vetëm ndan trafik brenda një rrjeti lokal (LAN), por gjithashtu lejon kontroll të avancuar, monitorim dhe sigurim të segmentimit të rrjetit. Në thelb, **Switch-i i menaxhueshëm** është një **element kyç për segmentim dhe siguri të rrjetit**, duke punuar ngushtë me **router-e të sigurta** dhe pajisje të tjera për mbrojtjen e rrjetit.



2.5 Pajisjet për parandalimin dhe zbulimin e ndërhyrjeve IDS dhe IPS

IDS (Intrusion Detection System) dhe IPS (Intrusion Prevention System) janë pajisje ose software që monitorojnë rrjetin dhe sistemet për aktivitet të dyshimtë ose sulme të mundshme, duke ofruar nivele të ndryshme të reagimit:

➤ Karakteristikat e IDS dhe IPS

Për të mbrojtur rrjetin nga sulmet e shpejta, kërkohet një ndryshim në paradigmen e arkitekturës së rrjetit. Kjo duhet të përfshijë sisteme të zbulimit dhe parandalimit me kosto efektive, si sistemet e zbulimit të ndërhyrjeve (IDS) ose sistemet më të shkallëzueshme të parandalimit të ndërhyrjeve (IPS). Arkitektura e rrjetit integron këto zgjidhje në pikë hyrjeje dhe dalje të rrjetit.

Kur implementoni IDS ose IPS, është e rëndësishme të njihni llojet e sistemeve të disponueshme, qasjet bazuar në host dhe rrjet, vendosjen e këtyre sistemeve, rolin e kategorive të sinjaleve (signatures), dhe veprimet e mundshme që një router Cisco IOS mund të ndërmarrë kur zbulohet një sulm.

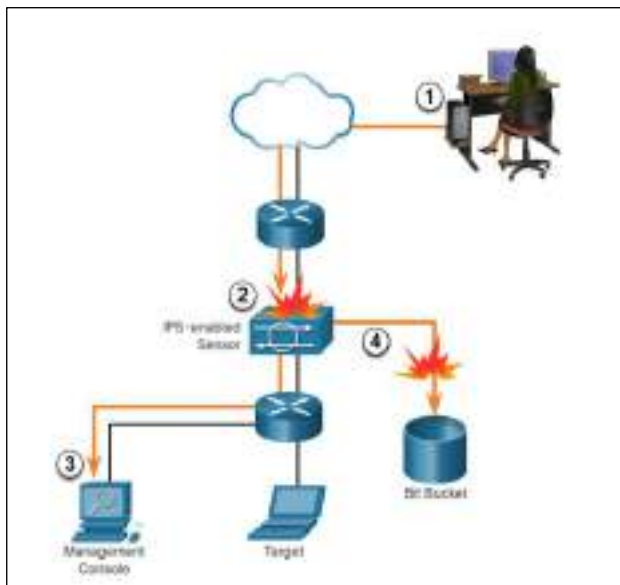


Figura tregon një përdorues në këndin e sipërm të djathtë të lidhur dhe që dërgon trafik në një re. Reja lidhet me një router dhe dërgon trafikun përmes tij. Reja lidhet me një sensor të aktivizuar për IPS, i cili lidhet me një router tjetër që gjithashtu ka lidhje me një konzolë menaxhimi dhe një laptop të etiketuar si “target”. Ka gjithashtu një ikonë për një *bit bucket* pranë sensorit të IPS.

2.7 Pajisje të sigurisë Proxy Server

Proxy Server është një pajisje ose software që **vepron si ndërmjetës** midis përdoruesve të rrjetit lokal dhe internetit. Ai merr kërkesat nga klientët, i përpunon sipas politikave të sigurta dhe i dërgon te destinacioni, duke ofruar përfitime të shumta për sigurinë dhe menaxhimin e trafikut.

Figura 2.5.1 : Ilustrim se si një pajisje IPS trajton trafikun keqdashës

- Të gjithë përdoruesit e LAN dhe Guest mund të kalojnë përmes Proxy Server për kontroll dhe filtrim.
- Proxy Server bashkëpunon me firewall dhe IDS/IPS për të monitoruar dhe menaxhuar trafik të dyshimtë.

2.8 VPN Gateway

VPN Gateway është një pajisje ose software që krijon lidhje të sigurta dhe të koduara midis rrjetit të brendshëm të një organizate dhe përdoruesve ose zyrave që lidhen nga distanca (remote access) ose midis dy degëve (site-to-site).



Figura 2.7.1: Ilustrim i vendosjejes në rrjet të pajisjes së sigurisë Proxy Server

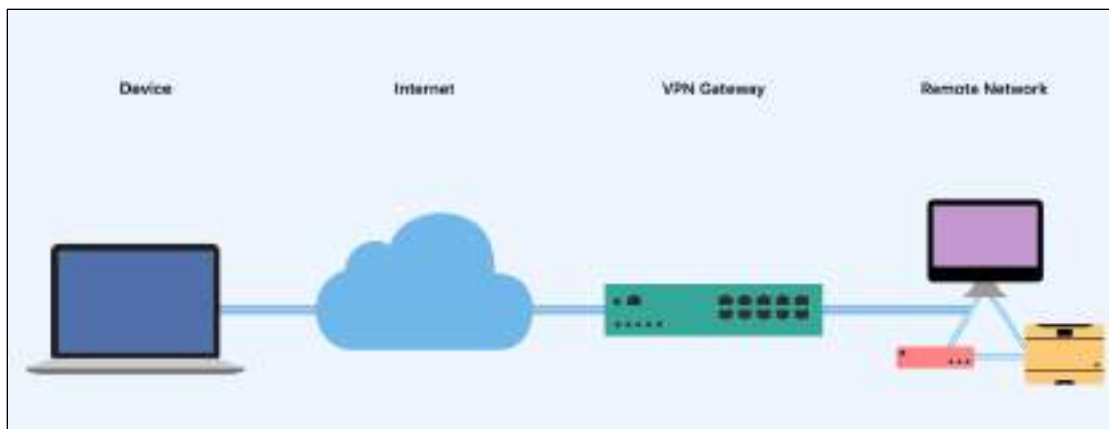


Figura 2.8.1: Ilustrim i VPN Gateway në rrjet

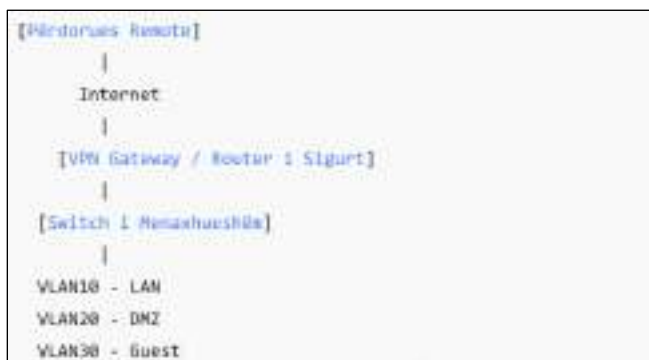
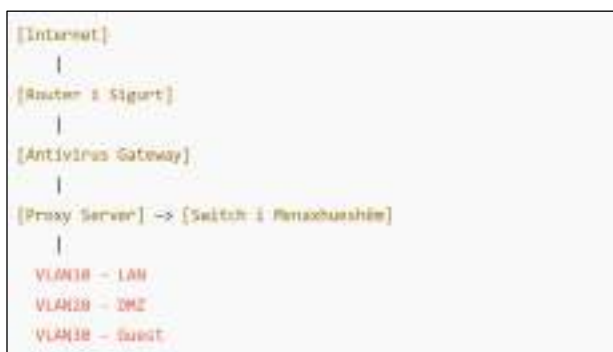


Figura 2.8.2: Ilustrim i vendosjes së VPN Gateway në rrjet

- Trafiku nga përdoruesi remote është i koduar derisa të arrijë në VPN Gateway.
- VPN Gateway mund të kombinohet me **Firewall, IDS/IPS, dhe Proxy Server** për siguri maksimale.

2.9 Antivirus Gateway

Antivirus Gateway është një pajisje ose software që monitoron të gjithë trafikun e rrjetit për të zbuluar dhe bllokuar viruset, malware, spyware dhe kërcënime të tjera para se të arrijnë tek përdoruesit ose serverët. Ai vepron si një shtresë mbrojtëse qendrore për rrjetin, duke parandaluar përhapjen e kërcënimeve.



Të gjithë paketat kalojnë përmes **Antivirus Gateway** për skanim dhe filtrim të malware.

Integrimi me Proxy Server dhe Firewall rrit mbrojtjen kundër kërcënimeve të brendshme dhe të jashtme.

Figura 2.9.1: Ilustrim i vendosjes në rrjet të Antivirus Gateway

2.10 UTM (Unified Threat Management)

UTM është një pajisje e integruar e sigurisë që kombinon disa funksione mbrojtjeje në një platformë të vetme, duke e bërë menaxhimin e rrjetit më të thjeshtë dhe më efikas.

- Të gjitha funksionet e sigurisë janë të integruara në një pajisje.
- Switch-i menaxhon VLAN-et dhe izolimin e segmenteve.
- Trafiku i LAN, DMZ dhe Guest kontrollohet dhe monitorohet nga UTM.

```
[Internet]
|
[DIR / FortiGate / Sophos XG]
|- Firewall
|- Antivirus
|- VPN Gateway
|- IDS/IPS
|- Web Filtering / Proxy
|
[Switch i Menaxhueshëm]
|
VLAN10 - LAN
VLAN20 - DMZ
VLAN30 - Guest
```

Figurë: 2.10.1 Shembull vendosjeje në rrjet UTM



Një rrjet i sigurt nuk është thjesht një firewall apo antivirus; është një strukturë e shumëfishtë e mbrojtjes, ku çdo pajisje ka rol të qartë dhe bashkëvepron për të minimizuar rreziqet dhe për të ruajtur integritetin e të dhënave.

Figura 2.10.2 Skema përmbledhëse e një rrjeti të sigurt

Tema 3: Konfigurime të thjeshta për sigurinë e rrjetit

Siguria e rrjetit është thelbësore për mbrojtjen e informacionit dhe funksionimin normal të pajisjeve që lidhen në rrjet, edhe konfigurimet më të thjeshta dhe bazike mund të ndikojnë ndjeshëm në rritjen e mbrojtjes ndaj sulmeve kibernetike, ndaj aksesit të paautorizuar dhe ndaj keqpërdorimit të burimeve të rrjetit. Kjo temë synon të prezantojë disa nga praktikat elementare, por shumë të rëndësishme, që çdo përdorues apo administrator rrjeti duhet të zbatojë për të forcuar sigurinë.

3.1 Sigurimi i BIOS-it

Një fjalëkalim për Windows, Linux ose Mac mund të anashkalohet. Kompjuteri juaj mund të boot-ohet nga një CD ose flash drive me një sistem operativ tjetër. Pasi të boot-ohet, një përdorues keqdashës mund të ketë qasje ose të fshijë skedarët tuaj.

Vendosja e një fjalëkalimi BIOS ose UEFI mund të parandalojë dikë nga boot-i i kompjuterit. Gjithashtu, parandalon ndryshimin e konfigurimeve të BIOS-it ose UEFI-t.



Figura 3.1.1 Vendosja e një fjalëkalimi BIOS ose UEFI



Në figurën e mësipërme, për shembull, një përdorues duhet të fusë fjalëkalimin e konfigurimit të BIOS-it për të pasur qasje në konfigurimet e tij.

- Të gjithë përdoruesit, pavarësisht nga lloji i llogarisë së tyre, përdorin të njëjtin fjalëkalim BIOS.
- Fjalëkalimet **UEFI** mund të vendosen për përdorues të veçantë, por kërkohet një server autentikimi.

Kujdes: Një fjalëkalim BIOS ose UEFI është relativisht i vështirë për t'u rivendosur, prandaj sigurohuni që ta mbani mend atë.

3.2 Sigurimi i hyrjes në sistemin operativ Windows

Mënyra më e zakonshme e mbrojtjes me fjalëkalim është hyrja në kompjuter. Kjo zakonisht kërkon të futni një fjalëkalim dhe ndonjëherë një emër përdoruesi, siç tregohet në figurë.



Menaxhimi lokal i fjalëkalimeve

Menaxhimi i fjalëkalimeve për kompjuterët **stand-alone** me Windows mund të bëhet **lokalisht** duke përdorur **Windows User Accounts**.

Për të krijuar, fshirë ose modifikuar një fjalëkalim në Windows, përdorni **Control Panel > User Accounts**, siç tregohet në figurë.

Figura 3.2.1: Logimi në sistemin operativ Windows

Është gjithashtu e rëndësishme të sigurohet që kompjuterët të jenë të mbrojtur kur përdoruesit nuk janë pranë tyre. Një **politikë sigurie** duhet të përmbajë një rregull që kërkon bllokimin e kompjuterit kur fillon **screensaver-i**. Kjo siguron që pas një kohe të shkurtër larg kompjuterit, screensaver-i të aktivizohet dhe kompjuteri të mos përdoret deri sa përdoruesi të hyjë përsëri.



Figura 3.2.4 Konfigurimi i fjalëkalimeve

- Në të gjitha versionet e Windows përveç Windows 10, përdorni **Control Panel > Personalization > Screen Saver**, siç tregohet më poshtë.
- Në Windows 10, përdorni **Settings > Personalization > Lock screen > Screen saver settings**. Zgjidhni një screensaver dhe një kohë pritjeje (wait time), pastaj aktivizoni opsionin **On resume, display logon screen**.

➤ Politika lokale e sigurisë në Windows

Në shumicën e rrjeteve që përdorin Windows, **Active Directory** është konfiguruar me **Domains** në një **Windows Server**. Kompjuterët Windows janë pjesë e një domain-i. Administratori konfiguronte një **Domain Security Policy** që zbatohet për të gjithë kompjuterët që i bashkohen domain-it. Politikat e llogarive vendosen automatikisht kur një përdorues hyn në Windows.

Për kompjuterët **stand-alone** që nuk janë pjesë e një domain-i Active Directory, mund të përdoret **Windows Local Security Policy** për të zbatuar cilësimet e sigurisë.

Për të hyrë në **Local Security Policy**, përdorni **Search > secpol.msc** dhe më pas klikoni **secpol**.

Mjeti **Local Security Policy Tool** do të hapet, siç tregohet në figurë.



Figura 3.2.6 Konfigurimi i Local Security Policy

➤ Cilësimet e sigurisë për politikat e llogarive

Politika e sigurisë do të përcaktojë **politikat e fjalëkalimeve** që duhet të ndiqen. **Windows Local Security Policy** mund të përdoret për të zbatuar këto politika të fjalëkalimeve. Kur caktohen fjalëkalimet, **niveli i kontrollit të fjalëkalimeve** duhet të përputhet me nivelin e mbrojtjes që kërkohet.

Shënim: Përdorni gjithmonë **fjalëkalime të forta** sa herë të jetë e mundur.

Zbato historikun e fjalëkalimeve

Përdorni **Account Policies > Password Policy** për të zbatuar kërkesat për fjalëkalime, siç tregohet në figurë. Rishikoni cilësimet aktuale të **Password Policy**.

Konfigurimi i Politikave të Bllokimit të Llogarive (Account Lockout Policies)

Këtu mund të caktoni rregulla për **bllokimin e llogarive** pas disa tentativave të pasuksesshme për hyrje, kohëzgjatjen e bllokimit dhe numrin e tentativave para bllokimit.

Përdorni **Account Policies > Account Lockout Policy** për të parandaluar **sulmet brute-force**, siç tregohet në Figurën 2.

Në një sulm **brute-force**, software-i përpiqet të thyejë një fjalëkalim duke provuar çdo kombinim të mundshëm të karaktereve. Klikoni mbi zonat e veçanta për të mësuar rreth cilësimeve aktuale të **Account Lockout Policy**.

Kjo politikë e bllokimit të llogarive gjithashtu mbron kundër një **sulmi të tipit dictionary**. Ky është një lloj sulmi brute-force që provon çdo fjalë në një fjalor për të fituar qasje.

Një sulmues mund të përdorë edhe **rainbow table**. Rainbow tables janë një përmirësim i metodës së sulmit me fjalor dhe përfshijnë një tabelë të parakalkuluar që përmban të gjitha fjalëkalimet e mundshme në formë të thjeshtë dhe hash-et e tyre përkatëse. Vlera hash e një fjalëkalimi të ruajtur mund të kërkohet në këtë tabelë dhe fjalëkalimi origjinal (plaintext) mund të zbulohet.

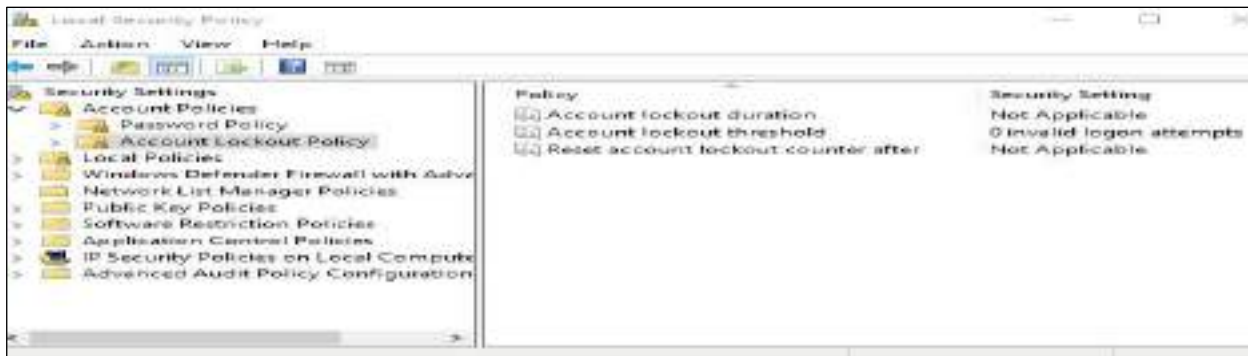


Figura 3.2.7 Konfigurimi i politikave të sigurisë për përdoruesit

Local Policy në **Local Security Policy** përdoret për të konfiguruar **audit policies**, **user rights policies**, dhe **security policies**.

Është e dobishme të regjistrohen përpjekjet e **suksesshme dhe të pasuksesshme për hyrje**. Përdorni **Local Policies > Audit Policy** për të aktivizuar auditimin, siç tregohet në figurë. Në këtë shembull, po aktivizohet **Audit account login events** për të gjithë eventet e hyrjes.

User Rights Assignment dhe **Security Options** ofrojnë një gamë të gjerë opsionesh sigurie që janë jashtë fushës së këtij kursi. Megjithatë, disa nga cilësimet do të eksplorojnë gjatë laboratorit.

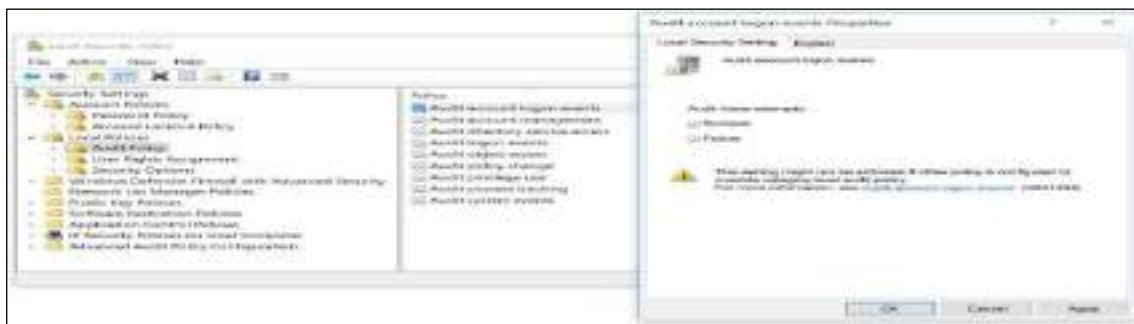


Figura 3.2.8 Cilësimet e sigurisë për politikat lokale

➤ Eksportimi i Local Security Policy

Një administrator mund të ketë nevojë të zbatojë një politikë të gjerë lokale për **user rights** dhe **security options**. Kjo politikë zakonisht duhet të **replikohet** në çdo sistem. Për ta thjeshtuar këtë proces, **Local Security Policy** mund të eksportohet dhe kopjohet në kompjuterë të tjerë Windows.

Hapat për të replikuar një **Local Security Policy** në kompjuterë të tjerë janë:

1. Përdorni **Action > Export List...**, siç tregohet në figurë, për të eksportuar politikën e një host-i të sigurt.
2. Ruani politikën me një emër, për shembull **workstation.inf**, në një media të jashtme.
3. Më pas, importoni skedarin e **Local Security Policy** në kompjuterët e tjerë stand-alone.

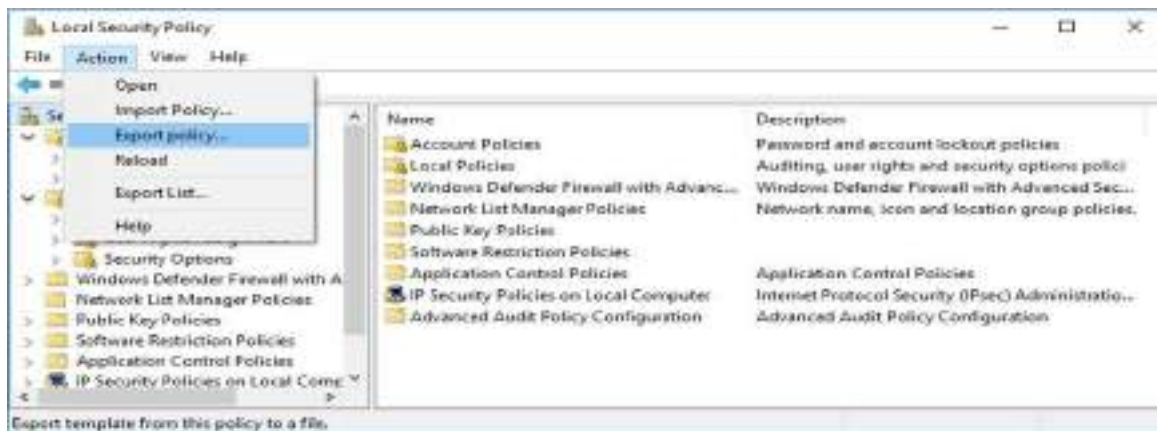


Figura 3.2.9 Eksportimi i Local Security Policy

➤ Menaxheri i përdoruesve dhe grupeve lokale (Local Users and Groups Manager)

Mjeti **Local Users and Groups** mund të kufizojë aftësinë e përdoruesve dhe grupeve për të kryer veprime të caktuara duke caktuar **rights** dhe **permissions**.

- **Rights** – Një “right” autorizon një përdorues të kryejë veprime të caktuara në kompjuter. Shembuj përfshijnë **backup-in e skedarëve dhe dosjeve** ose fikjen e kompjuterit.
- **Permissions** – Një “permission” është një rregull i lidhur me një objekt (zakonisht një skedar, dosje, ose printer). Ai përcakton se cilët përdorues mund të kenë qasje në objekt dhe në çfarë mënyre.

Për të konfiguruar të gjithë përdoruesit dhe grupet në një kompjuter duke përdorur mjetin **Local Users and Groups Manager**, shkruani **lusrmgr.msc** në kutinë e **Search** ose në **Run Line utility**.

Dritarja **Local Users and Groups > Users** tregon **llogaritë aktuale të përdoruesve** në kompjuter. Ajo përfshin llogaritë **built-in administrator** dhe **built-in guest**, siç tregohet në figurë.



Figura 3.2.10 Konfigurimi i kufizimeve për përdoruesit dhe grupet

Duke klikuar dy herë mbi një përdorues ose duke klikuar me të djathtën dhe zgjedhur **Properties**, hapet **dritarja e pronësive të përdoruesit**, siç tregohet në figurën e mëposhtme.

Kjo dritare lejon:

- Ndryshimin e opsioneve të përdoruesit të përcaktuara gjatë krijimit të tij.
- Bllokimin e një llogarie (**lock an account**).
- Caktimin e përdoruesit në një grup përmes skedës **Member of**.
- Kontrollimin e qasjes së përdoruesit në dosje përmes skedës **Profile**

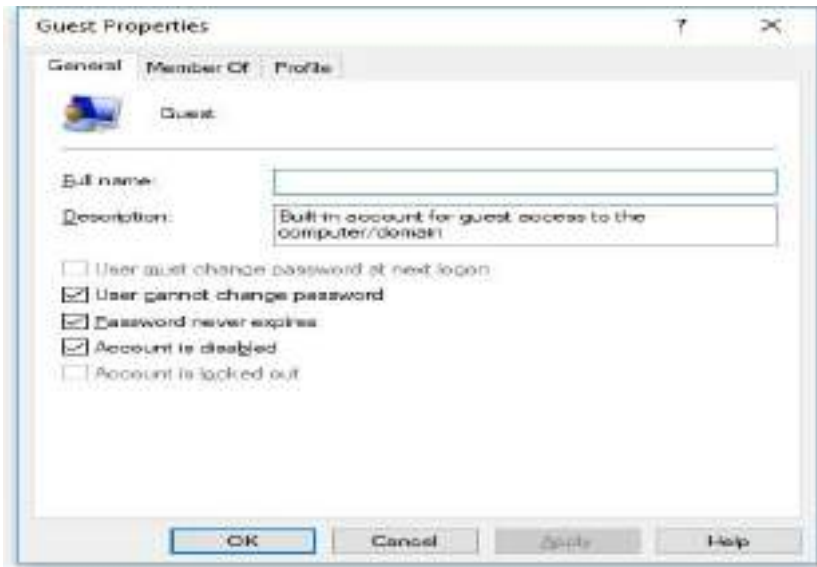


Figura 3.2.11 Dritarja e pronësive të përdoruesit

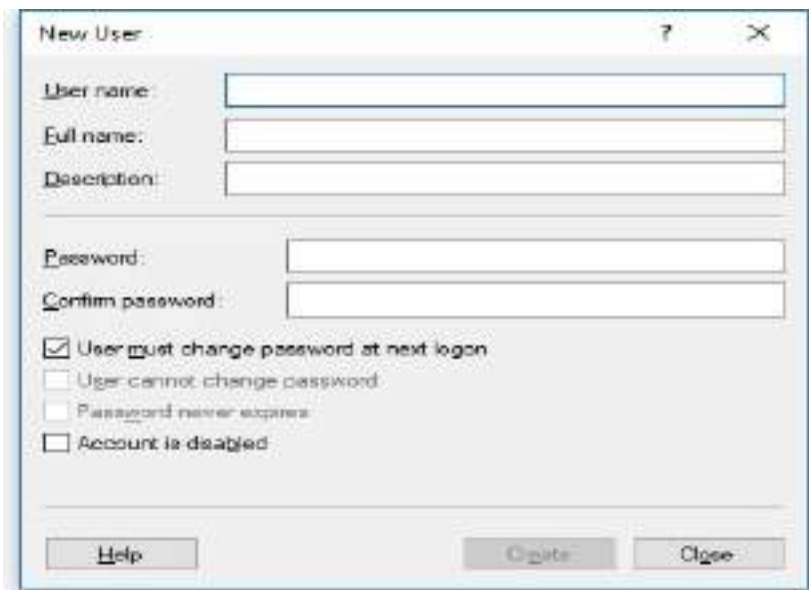


Figura 3.2.11 Dritarja për të shtuar një përdorues

➤ **Menaxhimi i grupeve lokale**

Mjeti **Local Users and Groups Manager** përdoret për të menaxhuar grupet lokale në një kompjuter Windows.

Përdorni: **Control Panel > Administrative Tools > Computer Management > Local Users and Groups** për të hapur **Local Users and Groups Manager**.

Nga dritarja **Local Users and Groups**, klikoni dy herë mbi **Groups** për të listuar të gjitha **grupet lokale në kompjuter**. Ka shumë **grupe të ndërtuara (built-in groups)** të disponueshme, siç tregohet në figurën më poshtë.

Për të shtuar një përdorues, klikoni në **Action menu** dhe zgjidhni **New User**. Kjo hap dritaren **New User**, siç tregohet në figurën e mëposhtme.

Nga kjo dritare mund të caktoni:

- **Username** (emrin e përdoruesit)
- **Full name** (emrin e plotë)
- **Description** (përshkrimin)
- **Account options** (opsionet e llogarisë)

Shënim: Disa versione të Windows gjithashtu përfshijnë llogarinë e ndërtuar **Power User**, e cila ka shumicën e fuqive të një administratori, por për arsye sigurie, i mungojnë disa privilegje të një administratori.

➤ **Menaxhimi i grupeve**

Përdoruesit mund të caktohen në grupe për **menaxhim më të lehtë**. Detyrat që përdoren për të menaxhuar grupet lokale përfshijnë:

- Krijimin e një **Local Group**
- Shtimin e **anëtarëve në grup**
- Identifikimin e **anëtarëve të një grupi lokal**
- Fshirjen e grupit
- Krijimin e një **llogarie lokale përdoruesi**

Kur të jetë e nevojshme të kryhen detyra administrative në kompjuterin lokal, përdorni **Run as Administrator** për të filluar një program duke përdorur kredenciale administrative.



Figura 3.2.12 Dritarja Local Users and Groups Manager për të menaxhuar grupet lokale



Për të krijuar një grup të ri, klikoni **Action > New Group** për të hapur dritaren **New Group**, siç tregohet në figurën e mëposhtme. Nga kjo dritare mund të krijoni **grupe të reja** dhe t'u caktoni **përdorues** atyre grupeve.

Figura 3.2.13 Dritarja për karakteristikat e grupit Guest

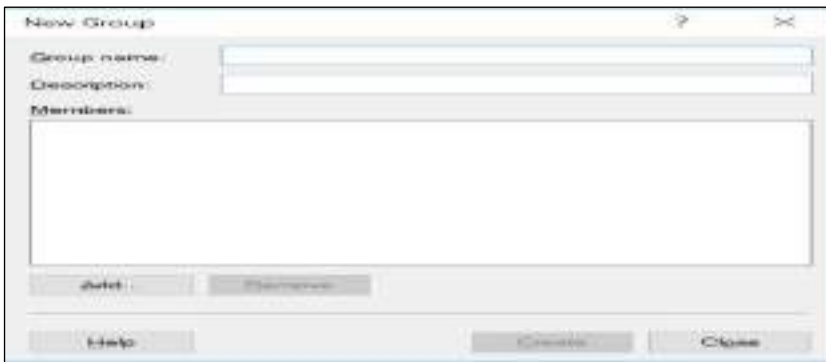


Figura 3.14 Dritarja për të krijuar një grup të ri

3.3 Konfigurimi i Firewall-ve Softuere-ike

Firewall-i softuerik aplikon një grup rregullash mbi transmetimet e të dhënave përmes inspektimit dhe filtrimit të paketave të të dhënave.

Windows Firewall është një shembull i një firewall-i softuerik që ndihmon në parandalimin e qasjes së sulmeve kibernetikë dhe malware-it në kompjuterin tuaj. Ai instalohet automatikisht kur instalohet sistemi operativ Windows.

Shënim: Në Windows 10, Windows Firewall u riemërtua si **Windows Defender Firewall**. Në këtë seksion, termi **Windows Firewall** përfshin edhe **Windows Defender Firewall**.

Cilësimet e **Windows Firewall** konfigurohen përmes dritares së **Windows Firewall**. Për të ndryshuar cilësimet e firewall-it, duhet të keni **privilegje administratori** për të hapur këtë dritare.

Për të hapur dritaren e **Windows Firewall**, përdorni:

Control Panel > Windows Firewall.

Shembulli në figurë tregon dritaren e **Windows 10 Windows Defender Firewall**.



Figura 3.3.1 Windows 10 Windows Defender Firewall

Në figurën më poshtë, rregullat e firewall-it janë të aktivizuara për një **rrjet privat**, një **rrjet për mysafirë ose publik**, ose një **rrjet domain-i korporativ**. Dritarja shfaq cilësimet për rrjetin privat, pasi ai është rrjeti aktualisht i lidhur. Për të parë cilësimet për rrjetet e domain-it ose mysafirëve, klikoni në shigjetën pranë etiketës **Not connected**.



Figura 3.3.3 Windows Firewall

Për të **çaktivizuar ose ri-aktivizuar Windows Firewall** ose për të ndryshuar **cilësimet e njoftimeve** për një rrjet, klikoni në **Change notification settings** ose **Turn Windows Defender Firewall on or off**. Kjo hap dritaren **Customize Settings**, siç tregohet më poshtë.

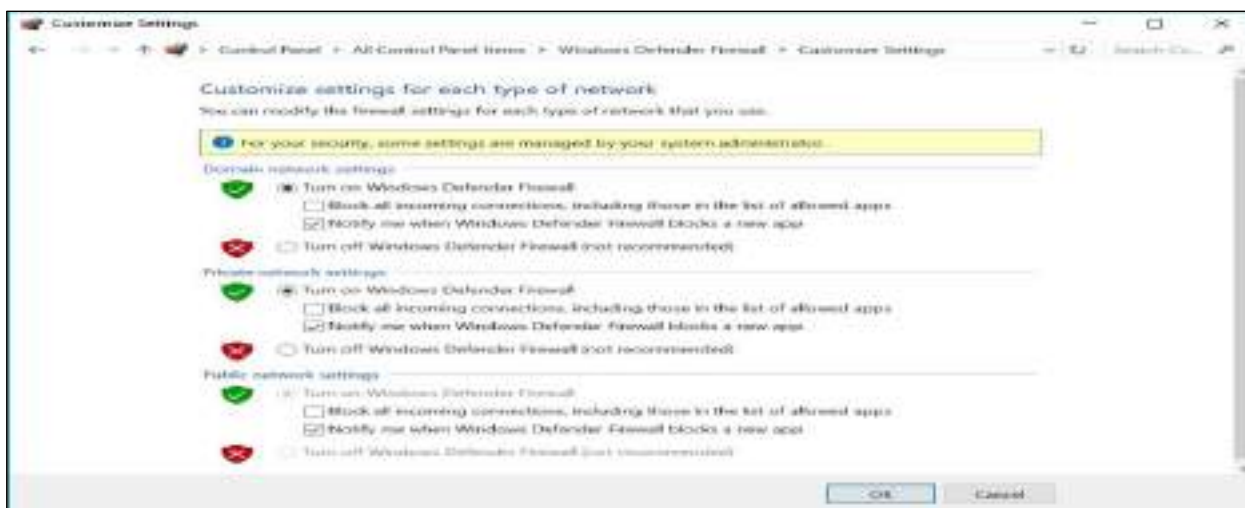


Figura 3.3.4 Konfigurimi I Windows Firewall

Nëse dëshironi të përdorni një **firewall tjetër softuerik**, duhet të çaktivizoni **Windows Firewall**. Për ta bërë këtë, ndiqni hapat e mëposhtëm:

1. Hyni në: **Control Panel > Windows Defender Firewall > Turn Windows Defender Firewall on or off**
2. Zgjidhni **Turn off Windows Defender Firewall (not recommended)** për rrjetin që dëshironi.

Shënim: Windows Firewall është i aktivizuar automatikisht. Mos e çaktivizoni përveçse keni një tjetër software firewall të instaluar dhe aktiv.

➤ **Konfigurimi i përjashtimeve në Windows Firewall**

Ju mund të lejoni ose bllokoni qasjen për **programet ose portet specifike** nga dritarja e Windows Firewall. Për të konfiguruar përjashtimet dhe për të lejuar ose bllokuar aplikacione/porte:

1. Klikoni **Allow an app or feature through Windows Firewall**
2. Kjo hap dritaren **Allowed apps**, ku mund të menaxhoni përjashtimet, siç tregohet më poshtë.

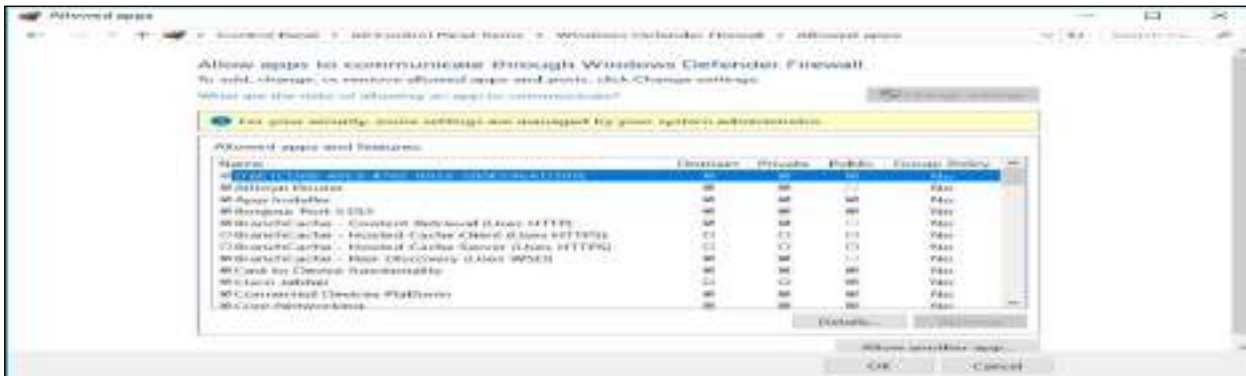


Figura 3.3.5 Konfigurimi i përjashtimeve në Windows Firewall

Nga kjo dritare, mund të **shtoni, ndryshoni ose hiqni** programet dhe portet e lejuara për rrjetet e ndryshme. Hapat për të shtuar programe përmes **Windows Firewall** janë:

1. Hyni në: **Control Panel > Windows Defender Firewall > Allow an app or feature through the Windows Firewall**
2. Klikoni **Change settings** nëse opsioni nuk është gri.
3. Shënoni kutitë për aplikacionet e listuara ose përdorni **Allow another app** nëse programi nuk gjendet në listë.
4. Klikoni **OK**.

3.4 Paketat e shërbimeve të sistemit operativ dhe përditësimet e sigurisë

Përditësimet janë kodet që prodhuesit ofrojnë për të parandaluar që një virus i sapo zbuluar të kryejë një sulm të suksesshëm. Shpesh, prodhuesit kombinojnë përditësimet dhe përmirësimet në një aplikacion të plotë për përditësim, i quajtur paketë shërbimi (service pack).

Windows kontrollon rregullisht faqen e Windows Update për përditësime me prioritet të lartë që mund të ndihmojnë në mbrojtjen e kompjuterit nga kërcënimet e fundit mbi sigurinë. Këto përditësime përfshijnë përditësime sigurie, përditësime kritike dhe paketat e shërbimeve. Në varësi të cilësimeve që zgjidhni, Windows shkarkon dhe instalon automatikisht çdo përditësim me prioritet të lartë që i nevojitet kompjuterit tuaj ose ju njofton kur këto përditësime bëhen të disponueshme.



Figura 3.6.1 Konfigurimi i Windows Update

Tema 4: Software për sigurinë dhe ruajtjen e të dhënave

4.1 Aplikacionet themelore të software-ëve mbrojtës

Mbrojtja e parë në çdo sistem sigurie përbëhet nga mjetet themelore që mbrojnë kompjuterët individualë (të quajtur "endpoints" ose pika fundore) dhe kufijtë e rrjetit. Dy mjetet më themelore dhe të domosdoshme janë programet antivirus dhe firewall-et.



Antivirusi dhe Anti-Malware: Rojet e skedarëve

Programi antivirus është si një roje sigurie që kontrollon çdo skedar dhe program që hyn në kompjuterin tuaj. Ai është krijuar për të gjetur, parandaluar dhe hequr programet e këqija, të njohura me emrin e përgjithshëm "malware". Kjo kategori e gjerë përfshin viruse, krimba, kuaj trojanë, ransomware (që bllokojnë skedarët për të përfituar para nga zhblokimi) dhe spyware (që vjedhin informacionet).

Mënyra se si këto mjete funksionojnë ka evoluar ndjeshëm:

1. Metoda e vjetër: Skanimi i bazuar në nënshkrime (signatures)
Mënyra tradicionale se si funksiononte antivirusi ishte si një "listë e të kërkuarve". Programi skanonte skedarët dhe i krahasonte me një bazë të dhënash gjigante të viruseve të njohur. Kjo bazë të dhënash përmban "nënshkrime" (signatures) ose modele unike (si një gjurmë gishti) të viruseve të njohur. Problemi me këtë metodë është i qartë: ajo është plotësisht e paefektshme kundër viruseve të reja, të panjohura më parë (të quajtura kërcënime "zero-day"), të cilat nuk janë ende në listë.
2. Metoda moderne: Analiza e sjelljes (heuristics)
Për të zgjidhur problemin e viruseve të reja, programet moderne përdorin analiza të sjelljes, të quajtura shpesh "analizë heuristike". Në vend që të kërkojë vetëm për "fytyra" të njohura nga lista e të kërkuarve, kjo metodë përdor inteligjencën artificiale (AI) për të kërkuar sjellje të dyshimtë. Ajo vepron si një detektiv që vëzhgon sistemin për veprime jo normale. Për shembull, nëse një program që sapo keni shkarkuar (p.sh., një lojë e thjeshtë) papritmas përpiket të aksesojë skedarët tuaj të fjalëkalimeve ose të fillojë të fshijë dokumente, antivirusi heuristik e ndalon atë menjëherë, edhe nëse nuk e ka parë kurrë më parë atë program specifik.



3. Metoda e Avancuar: Dhoma e izoluar (sandboxing)

Një teknikë edhe më e avancuar që përdoret nga sistemet moderne është "sandboxing". Mendojeni këtë si një dhomë prove virtuale të izoluar plotësisht. Kur antivirusi has një skedar të dyshimtë, por jo qartësisht keqdashës, ai e ekzekuton atë brenda këtij mjedisi të sigurt. Brenda "sandbox-it", programi mendon se po funksionon në një kompjuter normal, por në të vërtetë nuk mund të prekë ose dëmtojë sistemin real. Antivirusi më pas vëzhgon se çfarë bën programi. Nëse ai përpiqet të kryejë veprime keqdashëse brenda dhomës së izoluar, antivirusi e shkatërron atë dhe e shënon si të rrezikshëm.

4.2 Zbulimi dhe parandalimi i avancuar i kërcënimeve

Firewall-i dhe antivirusi janë mbrojtjet e vijës së parë—dyert dhe drynat e kështjellës. Por çfarë ndodh nëse një sulmues i sofistikuar arrin t'i kalojë ato? Për këtë arsye, organizatat përdorin sisteme të avancuara për të monitoruar në mënyrë aktive për kërcënime brenda mureve.

Këto mjete ndahen në dy kategori kryesore: Sistemet e Zbulimit të Ndërhyrjeve (IDS) dhe Sistemet e Parandalimit të Ndërhyrjeve (IPS).

IDS (Sistemi i Zbulimit të Ndërhyrjeve): Alarmi Pasiv

Mendoni për një IDS si një sistem alarmi me sensorë lëvizjeje brenda kështjellës. Roli i tij kryesor është të zbulojë aktivitetin e dyshimtë dhe të lajmërojë administratorin e sistemit. Një IDS është një mjet pasiv. Ai vëzhgon trafikun e rrjetit, analizon atë për të gjetur shenja sulmesh të njohura ose sjellje anormale, dhe kur gjen diçka, ai gjeneron një alarm ose një regjistrim (log).

E rëndësishme është të përmendim që një IDS nuk e ndërhyr në trafikun. Ai është si një alarm shtëpie që bie me zë të lartë, por nuk e ndalon hajdutin të vazhdojë të vjedhë. Ai ia lë në dorë administratorin që të dëgjojë alarmin dhe të ndërmarrë veprime.

Si e di IDS-ja që po ndodh një sulm?

1. **Detektimi me nënshkrime (Signature-based):** Kërkon modele të njohura sulmesh brenda paketave (p.sh., një varg kodi specifik i një exploit-i). Është i shpejtë dhe i saktë për sulmet e njohura, por dështon ndaj varianteve të reja.
2. **Detektimi i anomalive (Anomaly-based):** Krijon një profil të trafikut "normal" (baseline). Nëse trafiku devijon nga ky normalitet (p.sh., një rritje e papritur e trafikut në orën 3 të mëngjesit), gjenerohet alarm. Kjo kap sulmet e panjohura (zero-day), por ka shkallë të lartë të alarmeve të rreme.

Shkrimi i Rregullave në Snort

Snort është standardi "de facto" për IDS me burim të hapur. Kur kuptojmë sintaksën në Snort është fillojmë të kuptojmë edhe analizën e trafikut.

Struktura e një rregulli Snort: [Action][Protocol] -> ([Options])

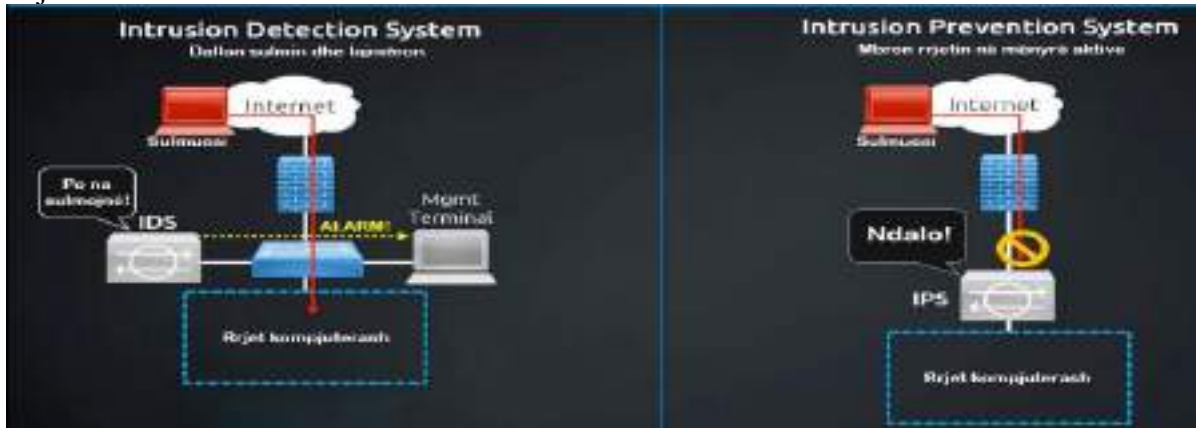
Shembull i detajuar:

```
alert tcp any any -> 192.168.1.0/24 80 (msg:"Dyshim per Sulm Web - SQL Injection"; content:"UNION SELECT"; nocase; sid:1000001; rev:1;)
```

- **alert:** Veprimi - gjenero një alarm. (Mund të ishte drop ose log).
- **tcp:** Protokollin e monitoruar.
- **any any:** Nga çdo IP dhe çdo port burimi (sulmuesi mund të jetë kudo).
- **->:** Drejtimi i trafikut (drejt serverit tonë).
- **192.168.1.0/24 80:** Rrjeti ynë i brendshëm në portin 80 (HTTP).
- **msg:** Mesazhi që shfaqet në log ("Dyshim per Sulm...").
- **content:"UNION SELECT":** Zemra e rregullit. Kërkon për tekstin "UNION SELECT" brenda paketës, që është një shenjë klasike e sulmeve SQL Injection.
- **nocase:** E bën kërkimin të pavarur nga shkronjat e mëdha/vogla.
- **sid:** Signature ID (Identifikuesi unik i rregullit).
- **rev:** Revision (Versioni i rregullit).

IPS (Sistemi i Parandalimit të Ndërhyrjeve): Roja Aktiv

Një IPS është versioni i evoluar dhe *aktiv* i IDS-së. Ai bën gjithçka që bën një IDS—monitoron dhe analizon trafikun—por me një ndryshim thelbësor: kur zbulon një kërcënim, ai *vepron menjëherë* për ta parandaluar atë. Në vend që të jetë thjesht një alarm, një IPS është si një roje sigurie që jo vetëm bërtet "Hajduti!", por edhe e kap hajdutin. Veprimet automatike që një IPS mund të ndërmarrë përfshijnë bllokimin e trafikut nga adresa IP sulmuese, pra ndërprerjen e lidhjes ose bllokimin e paketave keqdashëse përpara se ato të arrijnë objektivin.



Kompromisi i Madh: Problemi i "Alarmit Fals"

Zgjedhja midis një alarmi pasiv (IDS) dhe një roje aktive (IPS) duket e lehtë—sigurisht që roja aktive është më e mirë, apo jo? Në fakt, kjo është një nga zgjedhjet më të vështira në sigurinë e rrjetit dhe përfaqëson një kompromis themelor midis *Sigurisë* dhe *Disponueshmërisë*.

Problemi qëndron te "alarmet false" (false positives). Një alarm fals ndodh kur sistemi identifikon gabimisht trafikun normal dhe të ligjshëm si një sulm.

- Nëse një **IDS** ka një alarm fals, është thjesht *bezdisëse*. Administratori merr një email alarmi, e kontrollon, sheh që ishte një gabim dhe e injoron atë. Nuk ndodh asnjë dëm real.
- Nëse një **IPS** ka një alarm fals, pasojat mund të jenë *katastrofike*. Për shkak se IPS-ja është aktive, ajo do të *bllokojë* trafikun e ligjshëm. Imagjinoni një sistem IPS-je që gabimisht vendos se të gjitha pagesat me karta krediti të klientëve janë një "sulm". Ai do t'i bllokojë ato menjëherë, duke ndaluar funksionimin e biznesit.

Për këtë arsye, shumë organizata përdorin një qasje hibride, duke i konfiguruar IPS-të e tyre me shumë kujdes ose duke i përdorur ato në modalitetin "vetëm zbulim" (duke i kthyer në IDS) derisa të jenë plotësisht të sigurt për rregullat e tyre.

Tema 5: Kriptimi i të dhënave dhe teknikat bazë

Historia e Kriptografisë dhe Shifrat Klasike: Nga Roma e Lashtë te Enigma

Për të kuptuar thellësinë e algoritmeve moderne, është e domosdoshme të analizohen rrënjët e tyre historike. Çdo algoritm modern është, në thelb, një përgjigje ndaj dobësive të paraardhësve të tij. Kriptografia klasike bazohet kryesisht në dy operacione: zëvendësimin (ku karakteret ndërrohen me të tjera) dhe transpozimin (ku karakteret ndërrojnë vendet).

Shifra e Cezarit: Zëvendësimi monoalfabetik dhe dobësitë e tij

Një nga shembujt më të hershëm dhe më pedagogjikë të kriptografisë është **Shifra e Cezarit**, e përdorur nga Jul Cezari rreth vitit 100 p.e.s. për të komunikuar urdhra ushtarakë sekretë te gjeneralët e tij. Kjo metodë klasifikohet si një shifër zëvendësimi monoalfabetik, pasi çdo shkronjë e alfabetit zëvendësohet gjithmonë me të njëjtën shkronjë tjetër brenda të njëjtit mesazh.

Parimi funksionues është zhvendosja (shift). Në variantin klasik të Cezarit, çdo shkronjë zhvendoset me 3

pozicione në të djathtë të alfabetit. Për shembull, shkronja 'A' bëhet 'D', 'B' bëhet 'E', dhe kështu me radhë. Kur arrihet fundi i alfabetit, numërimi rifillon nga fillimi ('X' bëhet 'A'). Në kontekstin e laboratorëve shkollorë, ky koncept mund të vizualizohet lehtësisht përmes krijimit të një "Rrote të Shifrës së Cezarit" (Cipher Wheel). Nxënësit mund të presin dy disqe letre me madhësi të ndryshme, të shkruajnë alfabetin në perimetrin e secilit, dhe t'i bashkojnë në qendër me një pineskë. Rrotullimi i diskut të brendshëm përfaqëson vendosjen e çelësit

Dobësia Fatale: Analiza e Frekuencës

Pavarësisht se u shërbeu romakëve, Shifra e Cezarit është e thyeshme sot, dhe madje ishte e thyeshme edhe në mesjetë pas zbulimit të analizës së frekuencës nga dijetarët arabë. Në çdo gjuhë, disa shkronja përdoren më shpesh se të tjerat. Në gjuhën shqipe, për shembull, zanoret 'Ë', 'A' dhe 'E' kanë frekuencë shumë të lartë. Nëse një kriptanalist sheh që simboli 'G' shfaqet më shpesh në tekstin e shifruar, ai mund të deduktojë se 'G' përfaqëson 'Ë' ose 'A', dhe kështu të zbulojë zhvendosjen (çelësin) pa pasur nevojë të provojë të 25 kombinimet e mundshme.

Shifra Vigenère: Përpjekja për Paprekshmëri

Për të luftuar analizën e frekuencës, kriptografët zhvilluan **Shifrën Vigenère** (e përshkruar fillimisht nga Giovan Battista Bellaso në 1553, por e atribuar Vigenère-it). Kjo është një shifër **polialfabetike**. Dallimi thelbësor është përdorimi i shumë alfabeve të zhvendosura. Në vend të një zhvendosjeje konstante (si +3 te Cezari), zhvendosja ndryshon për çdo shkronjë të mesazhit, bazuar në një fjalë kyçe (Keyword).

Mekanizmi:

Nëse fjala kyçe është "TIK", ajo përsëritet poshtë mesazhit.

- Shkronja e parë e mesazhit kodohet me zhvendosjen e përcaktuar nga 'T'.
- Shkronja e dytë kodohet me zhvendosjen nga 'I'.
- Shkronja e tretë me 'K', dhe cikli rifillon.

Kjo metodë "rrafshon" histogramin e frekuencave. Shkronja 'A' në tekstin e qartë mund të kodohet si 'X' në një pozicion dhe si 'B' në një tjetër, duke e bërë analizën e thjeshtë të frekuencës të padobishme. Për tre shekuj, kjo u quajt *le chiffage indéchiffrable* (shifra e pathyeshme). U desh gjenialiteti i Friedrich Kasiskit në 1863 për ta thyer atë, duke vërejtur se përsëritja e fjalës kyçe krijon modele të përsëritura në tekstin e shifruar, gjatësia e të cilave mund të zbulojë gjatësinë e çelësit.

Telegrami Zimmermann: Kodet që Ndryshuan Luftën Botërore

Në Luftën e Parë Botërore, kriptografia luajti një rol gjeopolitik vendimtar. **Telegrami Zimmermann** ishte një mesazh diplomatik i dërguar në janar 1917 nga Ministri i Jashtëm gjerman, Arthur Zimmermann, drejt Meksikës. Në të, Gjermania i ofronte Meksikës një aleancë ushtarake kundër Shteteve të Bashkuara, duke i premtuar rikthimin e territoreve të humbura (Teksas, Arizona, Nju Meksiko). Kriptografët britanikë të "Room 40" interceptuan dhe dekriptuan mesazhin. Zbulimi i tij dhe publikimi në shtypin amerikan shkaktoi zemërim masiv publik, duke shërbyer si katalizator kryesor për hyrjen e SHBA-ve në luftë, çka ndryshoi rrjedhën e historisë. Ky rast demonstroi se kriptografia nuk është thjesht teknike; dështimi i saj mund të rrezojë perandori.

Makina Enigma: Kulmi i Kriptografisë Elektromekanike

Lufta e Dytë Botërore solli mekanizimin e shifrimit. Makina **Enigma**, e përdorur nga Gjermania Naziste, përfaqësonte një hap gjigant në kompleksitet. Ajo nuk ishte thjesht një pajisje zëvendësimi, por një gjenerator polialfabetik me një periudë përsëritjeje astronomike. Arkitektura e Brendshme e Enigmës: Enigma përbëhej nga tre elementë kryesorë që ndërvepronin për të ngatërruar sinjalin elektrik 13:

1. **Rotorët (Walzen):** Zemra e makinës ishin rotorët e lëvizshëm. Çdo rotor kishte instalime elektrike të brendshme që lidhnin 26 kontaktet hyrëse me 26 kontaktet dalëse në mënyrë të ngatërruar. Me çdo shtypje tasti, rotori i parë rrotullohej një hap (1/26 e rrotullimit). Kur ai përfundonte një rrotullim të plotë, shkaktonte rrotullimin e rotorit të dytë, e kështu me radhë (si odometri i makinës). Kjo do të thoshte se shtypja e shkronjës 'A' tre herë radhazi prodhonte tre shkronja të ndryshme të shifruara, pasi qarku elektrik ndryshonte fizikisht pas çdo gërme.
2. **Reflektori (Umkehrwalze):** Një komponent unik i Enigmës ishte reflektori në fund të vargut të

rotorëve. Ai e kthente sinjalin mbrapsht përmes rotorëve në një rrugë tjetër. Avantazhi i reflektorit ishte se e bënte makinën reciproke: nëse konfigurohej njësoj, shtypja e tekstit të shifruar jepte tekstin e qartë. Por, reflektori kishte një të metë logjike fatale: **asnjë shkronjë nuk mund të kodohej kurrë si vetvetja** (A nuk bëhej kurrë A). Kjo dobësi u shfrytëzua masivisht nga Turing dhe ekipa e tij në Bletchley Park për të eliminuar miliarda kombinime të mundshme gjatë thyerjes së kodit.

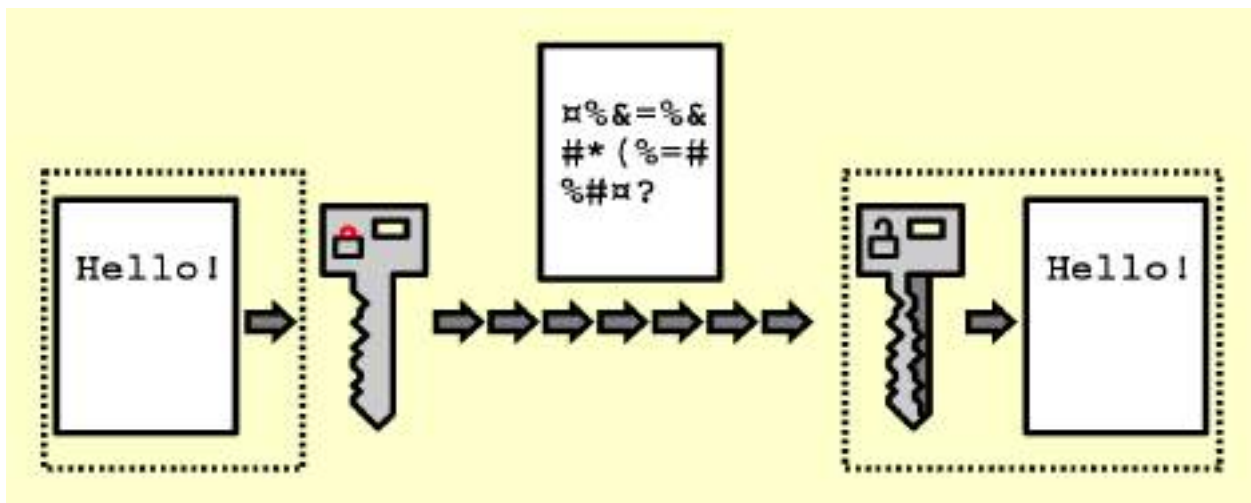
3. **Paneli i Prizave (Plugboard/Steckerbrett):** E vendosur në pjesën e përparme, kjo tabelë lejonte operatorin të ndërronte çiftet e shkronjave me kablllo *para* se sinjali të hynte në rotorë. Kjo shtoi numrin e kombinimeve të mundshme në rreth 158 kuintilionë, duke e bërë sulmin e “brute-force” të pamundur për kohën.

Thyerja e Enigmës nuk u arrit vetëm përmes matematikës, por edhe përmes gabimeve procedurale njerëzore dhe kapjes së librave të kodit nga aleatët (siç ishin ngjarjet me nëndetëset U-boat). Puna e Bletchley Park vlerësohet të ketë shkurtuar luftën me dy vjet, duke shpëtuar miliona jetë.

5.1 Bazat e kriptografisë moderne

Kriptimi është procesi i kthimit të të dhënave të lexueshme në një format të palexueshëm dhe të përzier. Mendojeni sikur po shkruani një mesazh duke përdorur një kod sekret. Për të kuptuar kriptimin, duhet të njihemi me tre terma bazë, duke përdorur një analogji të thjeshtë: një kuti metalike me dryn.

1. **Teksti i qartë (Plaintext):** Ky është mesazhi origjinal, i lexueshëm (p.sh., "Përshëndetje"). Në analogjinë tonë, kjo është letra që doni të dërgoni.
2. **Teksti i koduar (Ciphertext):** Ky është mesazhi i pakuptueshëm pasi të jetë koduar (p.sh., "x5bQ9s2T"). Kjo është kutia e mbyllur me dryn. Ju mund t'ia jepni kujtdo, por askush nuk mund të lexojë letrën brenda saj.
3. **Çelësi (Key):** Kjo është fjala ose metoda sekrete që përdorni për të koduar (mbyllur) dhe dekoduar (hapur) mesazhin. Ky është çelësi fizik i drynit.



Qëllimi kryesor i kriptimit është të ofrojë **konfidencialitet**—duke siguruar që informacioni të jetë i fshehtë dhe i aksesueshëm vetëm për njerëzit e autorizuar. Kjo është jetike për mbrojtjen e të dhënave në dy gjendje të ndryshme: "në qetësi" dhe "në tranzit".

Të Dhënat në tranzit (Data in transit)

Të dhënat në tranzit, të quajtura edhe të dhëna "në lëvizje", janë informacione që po lëvizin aktivisht nga një vend në tjetrin. Shembuj të përditshëm përfshijnë:

- Dërgimi i një emaili.
- Shfletimi i një faqeje interneti (të dhënat lëvizin nga serveri i uebit te shfletuesi).
- Dërgimi i një mesazhi në WhatsApp ose një platformë tjetër bisede.

Kërcënimi kryesor për të dhënat në tranzit është **përgjimi (eavesdropping)**. Për shkak se të dhënat po udhëtojnë përmes rrjetesh publike si interneti, një sulmues mund të "dëgjojë" bisedën dhe të vjedhë informacionin ndërsa ai lëviz. Kriptimi për të dhënat në tranzit (p.sh., HTTPS, TLS) e mbron lidhjen, duke e bërë të pamundur për përgjuesit të kuptojnë të dhënat që kapin.



Të dhënat në qetësi (Data at Rest)

Të dhënat në qetësi janë informacione "inaktive" që janë të ruajtura në një pajisje fizike. Shembujt përfshijnë:

- Skedarët e dokumenteve ose fotot të ruajtura në hard diskun e laptopit.
- Videot e ruajtura në telefonin celular.
- Emaillet e arkivuara në një server.
- Regjistrimet e klientëve në një bazë të dhënash.

Kërcënimi kryesor për të dhënat në qetësi është **aksesi i paautorizuar** ose **vjedhja fizike**. Shumë njerëz mendojnë se të dhënat në qetësi janë më të sigurta, por sulmuesit shpesh i shohin ato si një objektiv më të vlefshëm.

5.2 Kriptimi simetrik dhe asimetrik

Kriptografia moderne është e ndërtuar mbi dy lloje kryesore të kriptimit, të cilët funksionojnë në mënyra shumë të ndryshme për të zgjidhur probleme të ndryshme.

Kriptimi Simetrik (me Çelës Privat)

Kjo është forma më e vjetër dhe më e drejtpërdrejtë e kriptimit. Ajo përdor **një çelës të vetëm, të përbashkët** si për të koduar (mbyllur), ashtu edhe për të dekoduar (hapur) mesazhin.

Parimet e Kriptimit Simetrik

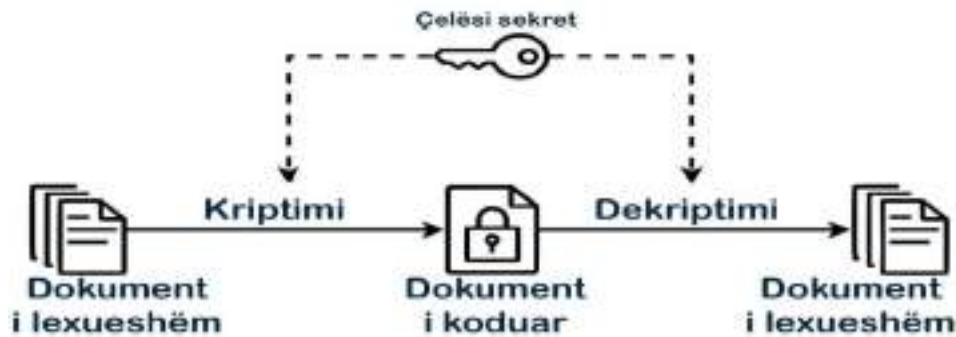
Në skemat simetrike, ekziston një **çelës i vetëm sekret** që përdoret si për enkriptim ashtu edhe për dekriptim. Dërguesi dhe marrësi duhet ta kenë këtë çelës para se të fillojë komunikimi.

Algoritmet simetrike ndahen në dy kategori:

1. **Stream Ciphers:** Kriptojnë të dhënat bit pas biti (si rrjedhë), duke kombinuar tekstin e qartë me një rrjedhë numrash të rastësishëm (keystream) përmes operacionit XOR.
2. **Block Ciphers:** I ndajnë të dhënat në blloqe me madhësi fikse (p.sh., 64 ose 128 bit) dhe kriptojnë secilin bllok si një njësi të vetme. AES bën pjesë në këtë kategori.

Sfidat kryesore të kriptimit simetrik janë menaxhimi i çelësave (si ta dërgojmë çelësin në mënyrë të sigurt?) dhe shkallëzueshmëria (në një rrjet me 100 njerëz, secili duhet të ketë një çelës unik me çdo person tjetër, duke kërkuar mijëra çelësa).

- **Analologjia:** Një mënyrë e mirë për ta kuptuar është ta krahasojmë me një **çelës shtëpie**. Ti përdor çelësin tënd për të mbyllur derën kur largohesh, dhe një person tjetër (p.sh., një anëtar i familjes) përdor një kopje *identike* të të njëjtit çelës për të hapur derën.
- **Përparësia:** Është jashtëzakonisht i **shpejtë** dhe efikas. Kërkon shumë më pak fuqi llogaritëse sesa kriptimi asimetrik. Kjo e bën atë ideal për të koduar sasi të mëdha të dhënash, si p.sh. një film i tërë ose një hard disk i plotë.
- **Dobësia:** Problemi më i madh është **shpërndarja e sigurt e çelësit**. Si ia jepni çelësin sekret shokut tuaj në mënyrë të sigurt pa e vjedhur dikush gjatë rrugës? Nëse e dërgoni me email, dikush mund ta përgjojë, dhe atëherë ai ka çelësin për të gjitha mesazhet tuaja të ardhshme.



Anatomia e AES (Advanced Encryption Standard)

AES është sot standardi *de facto* për qeveritë, bankat dhe sistemet e komunikimit (si WiFi WPA2, VPN, HTTPS). Ai është një shifër blloku që punon me blloqe 128-bitëshe dhe mbështet çelësa me gjatësi 128, 192, ose 256 bit. Struktura e AES është projektuar për të krijuar dy veti thelbësore të sigurisë të identifikuara nga Claude Shannon: **Konfuzion** (marrëdhënia midis çelësit dhe tekstit të shifruar është komplekse) dhe **Difuzion** (ndryshimi i një biti në tekstin e qartë ndryshon gjysmën e bit-ëve në tekstin e shifruar).

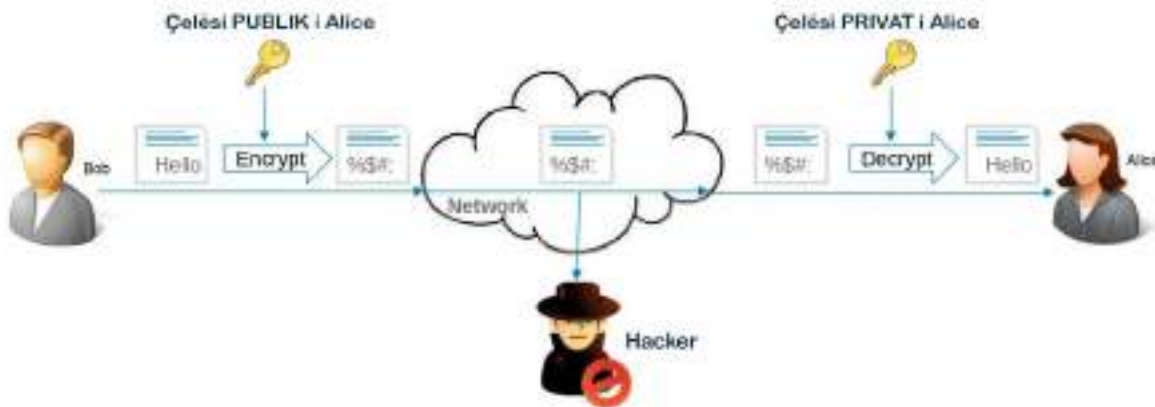
Për shkak të dizajnit të tij efikas, AES është shumë i shpejtë në harduer modern dhe konsiderohet i sigurt kundër të gjitha sulmeve praktike klasike. Deri më sot, nuk ka asnjë metodë praktike për të thyer AES-256 pa zotëruar çelësin.

Kriptimi Asimetrik (me Çelës Publik)

Kriptimi simetrik ka një problem logjistik: si t'ia dërgoj çelësin e fshehtë dikujt në anën tjetër të botës pa e përgjuar askush? Në vitet 1970, Whitfield Diffie, Martin Hellman dhe Ralph Merkle propozuan një koncept revolucionar: **Kriptografinë me Çelës Publik (Asimetrike)**. Kjo metodë e zgjuar u zhvillua pikërisht për të zgjidhur problemin e shpërndarjes së çelësit. Ajo përdor **dy çelësa të ndryshëm** që janë të lidhur matematikisht: një çelës publik dhe një çelës privat.

- **Analologjia:** Një mënyra e mirë për ta kuptuar këtë është ta krahasojmë me një **kuti postare personale** ose me një **dry i hapur**.
 1. **Çelësi Publik:** Ky është si një dry i hapur ose adresa e kutisë postare. Ju mund t'ia jepni një kopje të tij kujtdo në botë—mund ta postoni në faqen tuaj të internetit. Nuk ka rëndësi kush e ka. Njerëzit e përdorin këtë çelës publik *vetëm* për një gjë: *për të mbyllur* (koduar) një mesazh për ju.
 2. **Çelësi Privat:** Ky është çelësi unik që *e hap* atë dry ose atë kuti postare. Ju e mbani këtë çelës sekret dhe nuk ia jepni kurrë askujt.
- Procesi funksionon kështu: Një shok merr drynin tuaj të hapur (çelësin publik), e përdor atë për të mbyllur një kuti që përmban një mesazh për ju, dhe jua dërgon atë. Pasi kutia mbyllet me çelësin tuaj publik, i vetmi person në botë që mund ta hapë atë jeni ju, duke përdorur çelësin tuaj privat.

- **Përparësia:** Zgjidh në mënyrë të shkëlqyer problemin e shpërndarjes së çelësit. Ju kurrë nuk keni nevojë të ndani çelësin tuaj sekret.
- **Dobësia:** Është shumë i **ngadaltë** dhe kërkon shumë fuqi llogaritëse krahasuar me kriptimin simetrik. Do të ishte jopraktike të kodonit një film të tërë me këtë metodë.



Nënshkrimi dixhital kombinon Hashing me Kriptografinë Asimetrike për të garantuar autenticitetin. Ai funksionon në mënyrë të kundërt nga enkriptimi normal i mesazheve. Në enkriptim normal, përdoret çelësi publik i marrësit. Në nënshkrim dixhital, përdoret **çelësi privat i dërguesit**.

Procesi i Nënshkrimit dhe Verifikimit (Ky proces njihet si Shkëmbimi i Çelësve Diffie-Hellman):

1. Dërguesi (Alice) Nënshkruan:

- Alice krijon një dokument.
- Ajo llogarit *Hash-in* e dokumentit (p.sh., "A1B2...").
- Ajo e **enkripton hash-in** me **Çelësin e saj Privat**.
- Ky "Hash i Enkriptuar" është Nënshkrimi Dixhital. Ajo dërgon dokumentin së bashku me nënshkrimin.

2. Marrësi (Bob) Verifikon:

- Bob merr dokumentin dhe nënshkrimin.
- Hapi A: Bob llogarit vetë hash-in e dokumentit të marrë.
- Hapi B: Bob **dekripton** nënshkrimin e Alice-s duke përdorur **Çelësin Publik të Alice-s** (të cilin e ka të gjithë bota). Kjo i jep hash-in origjinal që kishte llogaritur Alice.
- Hapi C: Bob krahason dy hash-et.
 - Nëse përputhen, do të thotë dy gjëra:
 1. Dokumenti nuk është ndryshuar (Integritet).
 2. Nënshkrimi është krijuar vërtet nga çelësi privat i Alice-s, pasi vetëm çelësi i saj publik mund ta dekriptonte atë (Autentifikim).

Kjo teknologji është baza ligjore e kontratave dixhitale, faturave elektronike dhe HTTPS.

Modeli Hibrid: përfitim nga avantazhet e të dy modeleve

Në praktikë, ne nuk zgjedhim një të tjetër, por i kombinojmë në një model hibrid. Kjo është pikërisht ajo që ndodh çdo herë që vizitoni një faqe të sigurt (ato faqe që fillojnë me "https://").

Procesi funksionon kështu:

1. Së pari, shfletuesi juaj dhe faqja e internetit përdorin **kriptimin asimetrik** (të ngadaltë por të sigurt). Ky kriptim përdoret vetëm për një detyrë të vogël dhe të vetme: për të shkëmbyer në mënyrë të sigurt një çelës të ri, të përkohshëm, **simetrik** (i quajtur shpesh një "çelës sesioni").
2. Pasi të dyja palët e dinë këtë çelës të ri simetrik, ata ndalojnë së përdoruri kriptimin asimetrik.
3. Tani përdorin **kriptimin simetrik** (shumë të shpejtë) për të gjithë pjesën tjetër të bisedës, duke koduar të dhënat aktuale me atë çelës të përkohshëm.

Kjo qasje hibride krijon një lidhje që është njëkohësisht edhe jashtëzakonisht e sigurt (falë shkëmbimit

asimetrik të çelësit) edhe e shpejtë (falë kriptimit simetrik të të dhënave).

Tabela 2: Dallimet kryesore: Kriptimi simetrik krahasuar me atë asimetrik

Veçoria	Kriptimi simetrik (çelës i përbashkët)	Kriptimi asimetrik (çelësa të dyfishtë)
Çelësat	Një çelës i vetëm (për të dyja)	Dy çelësa (publik për kodim, privat për dekodim)
Shpejtësia	Shumë i shpejtë	Shumë i ngadalhtë
Përparësia	Efikasiteti për sasi të mëdha të dhënash	Shpërndarje e sigurt e çelësit
Problemi Kryesor	Si ta ndajmë çelësin në mënyrë të sigurt?	Ngadalësia

5.3 Algoritmet e zakonshme të kriptimit në praktikë

Një "algoritëm" kriptografik është thjesht "receta" ose formula specifike matematikore që përdoret për të kryer kriptimin. Ndërsa ekzistojnë shumë algoritme, disa prej tyre janë bërë standarde globale për shkak të sigurisë dhe efikasitetit të tyre. Ata ndahen në dy familje: simetrike dhe asimetrike.

Algoritmet simetrike (për të dhëna në masë)

Këta algoritme përdorin një çelës të vetëm dhe janë të optimizuar për shpejtësi. Ato përdoren për të krijuar vetë të dhënat—skedarët, disqet, etj.

- **DES (Data Encryption Standard) dhe 3DES (Triple DES):** Këto janë algoritme të vjetër. DES, i zhvilluar në vitet 1970, konsiderohet plotësisht i pasigurt sot sepse çelësi i tij 56-bitësh është shumë i shkurtër dhe mund të thyhet lehtësisht nga kompjuterët modernë. 3DES është një përmirësim (që e aplikon DES-in tre herë), por është shumë i ngadalhtë për standardet moderne dhe po hiqet nga përdorimi.
- **AES (Advanced Encryption Standard):** Ky është standardi modern global. I adoptuar nga qeveria e SHBA-së në 2001, AES është jashtëzakonisht i sigurt, i shpejtë dhe efikas. Ai përdoret nga qeveritë, bankat dhe bizneset kudo për të mbrojtur të dhënat e ndjeshme. Kur përdorni mjete si BitLocker ose FileVault për të krijuar hard diskun tuaj, ose kur ziponi një skedar me fjalëkalim, ka shumë të ngjarë të përdorni AES. Ai vjen në tre madhësi çelësash: 128, 192 ose 256 bitësh, ku të gjitha konsiderohen të sigurta.

Algoritmet Asimetrike (Për Shkëmbim Çelësash)

Këta algoritme përdorin dy çelësa (publik/privat) dhe përdoren për të shkëmbyer në mënyrë të sigurt çelësat simetrikë (siç u përshkrua në modelin hibrid) dhe për nënshkrime (signatures) digjitale.

- **RSA:** Ky është një nga algoritmet asimetrikë më të vjetër dhe më të përdorur, i zhvilluar në vitin 1977. Siguria e tij bazohet në vështirësinë ekstreme matematikore të faktorizimit të numrave shumë të mëdhenj primarë. Për dekada, RSA ka qenë si trau i shtëpisë për sigurinë e tregtisë elektronike.
- **ECC (Elliptic Curve Cryptography):** Kjo është një qasje më moderne për kriptimin asimetrik. Përparësia kryesore e ECC ndaj RSA nuk është domosdoshmërisht siguria më e madhe, por *efikasiteti* i jashtëzakonshëm.

Për të krijuar pse ECC është kaq i rëndësishëm, duhet të kuptojmë madhësinë e çelësit. Për të arritur të njëjtin nivel sigurie, një çelës ECC kërkon shumë më pak bit sesa një çelës RSA. Për shembull:

- Një çelës ECC 256-bitësh (që është relativisht i vogël) ofron afërsisht të njëjtin nivel sigurie sa një çelës RSA 3072-bitësh (që është shumë i madh).

Gjenerimi dhe përdorimi i një çelësi RSA 3072-bitësh kërkon shumë fuqi llogaritëse dhe kohë. Kjo është në rregull për një server të fuqishëm, por është një shpenzim i madh baterie dhe fuqie për një telefon celular

ose një orë inteligjente. Për shkak se ECC ofron të njëjtën siguri me çelësa shumë më të vegjël, ai kërkon më pak fuqi dhe është shumë më i shpejtë. Kjo e ka bërë atë standardin ideal për botën moderne të pajisjeve mobile dhe të Internetit të Gjërave (IoT).

5.4 Hashing për integritetin e të dhënave

Deri tani kemi folur për konfidencialitetin (fshehjen). Por siguria ka nevojë edhe për **Integritet** (sigurinë që të dhënat nuk janë ndryshuar rrugës) dhe **Autentifikim** (vërtetimin e identitetit të dërguesit). Këtu hyjnë në lojë Funkzionet Hash dhe Nënshkrimet Dixhitale.

Kriptimi ka një "kushëri" të rëndësishëm të quajtur hashing. Këto dy koncepte shpesh ngatërrohen, por ato bëjnë punë krejtësisht të ndryshme dhe zgjidhin probleme të ndryshme.

Dallimi kryesor është ky:

- **Kriptimi** është një proces **dy-drejtimësh**. Ai është krijuar për të fshehur diçka, por me qëllimin që ajo të zbulohet më vonë. Ju mund ta kodoni (mbyllni) dhe më pas ta dekodoni (hapni) atë, për sa kohë keni çelësin. Qëllimi është **fshehtësia (konfidencialiteti)**.
- **Hashing** është një proces **një-drejtimësh**. Ai merr një hyrje (psh. një skedar ose një fjalëkalim) dhe e kthen atë në një varg unik me gjatësi fikse (p.sh. 64 karaktere). Ky varg quhet "vlerë hash" ose "gjurmë gishtash digjitale". Është e pamundur të kthehesh mbrapsht dhe të gjesh hyrjen origjinale nga u prodhua hashi. Qëllimi është **integriteti**—të provojë që diçka *nuk ka ndryshuar*.

Një funksion i mirë hash ka disa veti kryesore:

1. **I pakthyeshëm:** Është një rrugë një-drejtimëshe.
2. **Gjatësi fikse:** Pavarësisht nëse hyrja është një shkronjë e vetme apo një film i tërë 4K, dalja (hash-i) ka gjithmonë të njëjtën gjatësi (p.sh. SHA-256 prodhon gjithmonë 64 karaktere).
3. **Efekti ortek (Avalanche Effect):** Kjo është vetia më e rëndësishme. Nëse ndryshoni qoftë edhe një shkronjë të vetme në skedarin origjinal, vlera hash do të ndryshojë *plotësisht* dhe në mënyrë të paparashikueshme.

Hashing-u ka dy përdorime kryesore në sigurinë e përditshme:

Përdorimi 1: Për të Ruajtur Fjalëkalimet në Mënyrë të Sigurt

Asnjë sistem i sigurt nuk e ruan fjalëkalimin tuaj në formë të lexueshme. Nëse një kompani e bën këtë, ajo po kryen një neglizhencë të rëndë të sigurisë. Në vend të kësaj, sistemet ruajnë vetëm *hash-in* e fjalëkalimit tuaj. Procesi funksionon kështu:

1. **Regjistrimi:** Ju krijoni një llogari me fjalëkalimin "P@ssword123". Sistemi nuk e ruan këtë fjalë. Ai llogarit hash("P@ssword123") dhe ruan vlerën hash (p.sh., "e866...a43b").
2. **Hyrja (Login):** Ju ktheheni dhe shtypni fjalëkalimin "P@ssword123". Sistemi nuk e krahason këtë me atë që ka ruajtur. Në vend të kësaj, ai llogarit përsëri hash("P@ssword123") dhe merr përsëri "e866...a43b".
3. Më pas, ai krahason *hash-in e ruajtur* me *hash-in e ri*. Nëse dy hash-et përputhen, sistemi e di që ju keni futur fjalëkalimin e saktë dhe ju lejon të hyni.

Kjo metodë është e sigurt sepse edhe nëse një haker vjedh të gjithë bazën e të dhënave të fjalëkalimeve, ai nuk vjedh fjalëkalimet tuaja. Ai vjedh vetëm një listë të gjatë me vlera hash. Për shkak se hash-i është i pakthyeshëm, ai nuk mund ta kthejë "e866...a43b" mbrapsht në "P@ssword123".

Përdorimi 2: Për të verifikuar integritetin e skedarëve (Checksum)

Kur shkarkoni një program ose një skedar të madh nga interneti, faqja e internetit shpesh ju jep një vlerë hash (e quajtur shpesh "checksum") për atë skedar.

Ky është një mjet i fuqishëm verifikimi. Pasi të keni shkarkuar skedarin, ju mund të përdorni një mjet në kompjuterin tuaj për të llogaritur vetë hash-in e skedarit që sapo morët. Më pas, ju krahasoni hash-in tuaj me atë të publikuar në faqen e internetit.

- Nëse hash-et përputhen saktësisht, ju e dini 100% se skedari që keni është identik me origjinalin dhe nuk është dëmtuar gjatë shkarkimit ose, më keq, nuk është modifikuar nga një haker për të futur një

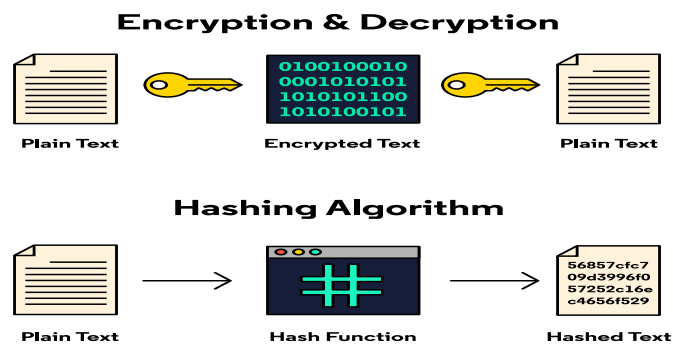
virus.

- Nëse hash-et nuk përputhen (qoftë edhe me një shkronjë të vetme), ju e dini se skedari është i korruptuar ose i manipuluar dhe nuk duhet ta hapni.

Tabela 3: Krahasim i shpejtë: Kriptimi në krahasim me Hashing

Veçoria	Kriptimi	Hashing
Qëllimi	Të mbajë të dhënat të fshehta (Konfidencialiteti)	Të provojë që të dhënat nuk kanë ndryshuar (Integriteti)
A Mund të Kthehet?	Po, me çelësin e duhur (Dy-drejtimësh)	Jo, është e pamundur (Një-drejtimësh)
Përdorimi Kryesor	Sigurimi i skedarëve, emaileve, lidhjeve HTTPS	Ruajtja e fjalëkalimeve, verifikimi i skedarëve

Algoritmi	Karakteristikat	Statusi i Sigurisë
MD5	Prodhon një hash 128-bit. Shpejtë, por matematikisht i thyer.	II Pasigurt: Vulnerabël ndaj "sulmeve të përplasjes" (collision attacks), ku dy skedarë të ndryshëm prodhojnë të njëjtin hash.
SHA-256	Pjesë e familjes SHA-2. Prodhon hash 256-bit.	Standardi Aktual: Përdoret gjerësisht në certifikatat moderne SSL/TLS. Është rezistent ndaj përplasjeve dhe konsiderohet i sigurt për momentin.



5.5 Zbatimi i kriptimit: mbrojtja e disqeve dhe menaxhimi i çelësve

Kuptimi i teorisë së kriptimit është hapi i parë. Hapi i dytë është zbatimi i tij në praktikë për të mbrojtur të dhënat që janë "në qetësi". Kjo përfshin si mbrojtjen e disqeve fizike ashtu edhe menaxhimin e kujdesshëm të çelësve që i mbrojnë ato.

Kriptimi i diskut: Mbrojtja e të dhënave "në qetësi"

Siç u diskutua në nëntemën 5.1, mbrojtja e të dhënave në qetësi është thelbësore për t'u mbrojtur nga vjedhja fizike. Ekzistojnë dy qasje kryesore për këtë:

1. Kriptimi i plotë i diskut (FDE)

Kjo metodë kodon gjithçka në hard disk. Kjo përfshin sistemin operativ, të gjitha programet dhe të gjitha të dhënat. Shembujt më të njohur të FDE janë BitLocker në sistemet Windows dhe FileVault në macOS.

- **Analologjia:** FDE është si të vendosësh një **dryn masiv në derën kryesore të shtëpisë tënde**.
- **Mbrojtja Kryesore:** FDE është mbrojtja më e mirë dhe e vetme kundër *vjedhjes fizike*. Nëse dikush vjedh laptopin tuaj, ai nuk mund të aksesojë asgjë. Pa fjalëkalimin tuaj të hyrjes, disku është thjesht një copë metali me të dhëna të pakuptueshme dhe të përziera.
- **Kufizimi:** Mbrojtja e FDE është efektive *vetëm* kur pajisja është e fikur. Sapo ta ndizni dhe të futni fjalëkalimin tuaj, e gjithë "shtëpia" është e hapur dhe e dekoduar. Nëse largoheni nga laptopi juaj i ndezur dhe pa mbikëqyrje, FDE nuk ju mbron.

2. Kriptimi në nivelin e skedarit (FBE)

Në kontrast me qasjen "gjithçka ose asgjë" të FDE, kjo metodë kodon skedarë ose dosje specifike në mënyrë individuale.

- **Analologjia:** FBE është si të kesh një **kasafortë brenda shtëpisë**. Edhe nëse dera e përparme (FDE) është e hapur (d.m.th., laptopi është i ndezur), dokumentet tuaja më konfidenciale janë ende të mbyllura në kasafortë.
- **Mbrojtja Kryesore:** Një skedar i kriptuar individualisht mbetet i kriptuar pavarësisht se ku e lëvizni. Nëse e kopjoni në një USB ose e dërgoni me email, ai mbetet i koduar dhe kërkon një fjalëkalim të veçantë për t'u hapur.
- **Kufizimi:** Kjo metodë varet nga gjykimi i përdoruesit. Ju duhet të zgjidhni në mënyrë aktive se cilët skedarë të kodoni.

Kujdesi për çelësat: Cikli i jetës së menaxhimit të çelësave

Kur bëhet fjalë për sigurinë, një sistem kriptimi varet nga menaxhimi i çelësave të tij. Mënyra si menaxhohen çelësat është ndoshta pika më e dobët në të gjithë sigurinë. Nuk ka rëndësi sa e fortë është dera juaj (algoritmi AES) nëse e lini çelësin poshtë tapetit (menaxhim i dobët i çelësit).

Menaxhimi i çelësave është procesi i vazhdueshëm i trajtimit të sigurt të çelësave kriptografikë gjatë gjithë jetës së tyre. Ashtu si njerëzit, çelësat kanë një cikël jete të përcaktuar:

1. Faza 1: Krijimi (Generation)

Çelësi duhet të krijohet në mënyrë të sigurt, duke përdorur metoda të vërteta të rastësisë. Një çelës i dobët ose i parashikueshëm e bën të gjithë kriptimin të pavlefshëm.

2. Faza 2: Ruajtja dhe përdorimi (Storage & Use)

Kjo është "jeta" kryesore e çelësit. Ai përdoret në mënyrë aktive për të koduar dhe dekoduar të dhëna. Gjatë kësaj faze, ai duhet të ruhet në mënyrë të sigurt, zakonisht në një "kasafortë çelësash" të quajtur Modul i Sigurisë së Harduerit (HSM) ose një Menaxher Çelësash softuerik, për të parandaluar aksesin e paautorizuar.

3. Faza 3: Rotacioni (Rotation)

Kjo është një praktikë thelbësore e sigurisë. Çelësat duhet të ndryshohen rregullisht, p.sh., çdo 90 ditë ose çdo vit. Arsyeja është të kufizohet dëmi në rast se një çelës vidhet. Nëse një sulmues vjedh një çelës, por ju e ndryshoni atë çdo 90 ditë, sulmuesi ka akses vetëm në të dhënat e 90 ditëve më parë, jo në të dhënat e 10 viteve të fundit. Pasi një çelës "plaket" dhe zëvendësohet, ai vihet në pension—nuk përdoret më për të koduar gjëra të reja, por ruhet në mënyrë të sigurt në rast se na duhet për të dekoduar të dhëna të vjetra.

4. Faza 4: Shkatërrimi (Destruction)

Pasi jemi absolutisht të sigurt se çelësi (dhe të dhënat e vjetra që ai mbron) nuk do të na duhen më kurrë, çelësi duhet të shkatërrohet në mënyrë të sigurt dhe të përhershme. Fshirja e të dhënave pa fshirë çelësin është një rrezik sigurie, pasi dikush që gjen çelësin mund të jetë në gjendje të rikuperojë të dhënat e fshira.



Tema 6: Certifikatat e sigurisë dhe roli i tyre

6.1 Hyrje për certifikatat digjitale dhe besueshmërinë

Në botën fizike, nëse doni të vërtetoni identitetin tuaj, ju tregoni një dokument të lëshuar nga një autoritet i besuar, si p.sh. një pasaportë ose një kartë identiteti. Në botën digjitale, ky rol luhet nga një **certifikatë SSL/TLS**. Një certifikatë SSL/TLS është thjesht një "kartë identiteti digjitale" ose "pasaportë" për një faqe interneti. Ajo shërben si një skedar i vogël të dhënash që lidh në mënyrë kriptografike detajet e një organizate (si emri i saj) me një çelës publik. Kjo "pasaportë" nuk lëshohet nga vetë faqja e internetit (ashtu si ju nuk mund ta printoni vetë pasaportën tuaj). Ajo lëshohet nga një palë e tretë e besuar globalisht e njohur si **Autoriteti i certifikimit (CA)**—mendojeni si zyra qeveritare e pasaportave. Ky autoritet (si DigiCert, Let's Encrypt, etj.) garanton që faqja e internetit është ajo që pretendon të jetë.

Sqarim i shkurtër: SSL krahasuar me TLS

Ju shpesh do të dëgjoni termin "SSL", por vetë protokollin SSL (Secure Sockets Layer) është i vjetëruar dhe konsiderohet i pasigurt. Protokollin modern dhe më i sigurt që përdoret sot quhet TLS (Transport Layer Security). Megjithatë, emri i vjetër "SSL" ka mbetur në përdorim të gjerë. Kur njerëzit thonë "Certifikatë SSL" sot, ata pothuajse gjithmonë nënkuptojnë teknikisht një certifikatë TLS. Për qartësi, ne do t'i referohemi si SSL/TLS. Këto certifikata shërbejnë për tre funksione thelbësore:

1. **Vërtetimi (Identiteti):** Funksioni më i rëndësishëm. Ajo provon identitetin e faqes së internetit. Kur shfletuesi juaj merr certifikatën, ai verifikon që ajo është lëshuar nga një CA i besuar dhe që i përket domeinit që po vizitoni. Kjo ju mbron nga sulmet "Man-in-the-Middle" që kanë të bëjnë me përgjimin e trafikut.
2. **Kriptimi (Fshehtësia):** Kriptimi mundëson krijimin e një lidhjeje të kriptuar (HTTPS) midis jush dhe serverit. Pasi identiteti të jetë vërtetuar, çelësi publik në certifikatë përdoret për të filluar procesin e kriptimit hibrid (siç u diskutua në Temën 5), duke siguruar që të gjitha të dhënat e dërguara (fjalëkalime, numra kartash krediti, etj.) të jenë të fshehta.
3. **Integriteti:** Kjo garanton që të dhënat e dërguara midis jush dhe serverit nuk janë ndryshuar ose manipuluar gjatë rrugës nga një palë e tretë.

Kur vizitoni një faqe interneti, prania e një certifikate të vlefshme SSL/TLS tregohet nga dy shenja të qarta në shiritin e adresave të shfletuesit tuaj: URL-ja që fillon me **https://** (ku 's' do të thotë 'secure' - i sigurt) dhe një **ikonë dryni** pranë adresës.

6.2 Funkzionimi i një lidhje e sigurt: shtrëngimi i duarve dhe zinxhiri i besimit

Pra, si e përdor saktësisht shfletuesi juaj këtë "pasaportë" për të krijuar një lidhje të sigurt? Ai kryen dy procese thelbësore dhe të padukshme për përdoruesin: "shtrëngimin e duarve" për të krijuar lidhjen dhe verifikimin e "zinxhirit të besimit" për të vërtetuar identitetin.

Shtrëngimi i Duarve (Handshake)

"Shtrëngimi i duarve" (Handshake) SSL/TLS është procesi i negociatave midis shfletuesit tuaj (klientit) dhe serverit të uebit. Ky proces është zbatimi praktik i "modelit hibrid" të kriptimit që diskutuam në Temën 5. I gjithë procesi ndodh në më pak se një sekondë, përpara se faqja të ngarkohet. Ja një version i thjeshtuar i "bisedës" që ndodh:

1. **Ju (Shfletuesi):** "Përshëndetje server, dua të lidhem në mënyrë të sigurt. Ja versionet e TLS dhe metodat e kriptimit që përdor unë." (Ky quhet "Client Hello").
2. **Serveri:** "Përshëndetje. Unë zgjedha këtë version të TLS dhe këtë metodë. Ja 'pasaporta' ime (certifikata ime SSL/TLS). Ajo përmban emrin tim dhe 'kutinë time postare të hapur' (celësin tim publik)." (Ky quhet "Server Hello").
3. **Ju:** "Më prit të kontrolloj... Po, kjo pasaportë duket e vlefshme dhe është lëshuar për ty nga një 'zyrë pasaportash' (CA) që unë e besoj. Në rregull, të besoj." (Ky është hapi i vërtetimit).
4. **Ju:** "Tani, le të krijojmë një 'kod sekret për këtë bisedë' (një çelës simetrik i përkohshëm). Po e mbyll këtë kod sekret në 'kutinë tënde postare' (duke përdorur çelësin tënd publik) dhe po ta dërgoj." (Ky është shkëmbimi i celësit).
5. **Serveri:** "E mora mesazhin e koduar. Po e hap me çelësin tim privat. Shkëlqyeshëm, tani e di kodin sekret për këtë bisedë."
6. **Të dy:** "Në rregull. Tani e tutje, do të flasim duke përdorur vetëm këtë kod sekret të shpejtë (kriptim simetrik)." (Ky quhet "Finished").

Në këtë pikë, shtrëngimi i duarve përfundon. Ikona e drynit shfaqet në shfletuesin tuaj, dhe pjesa tjetër e komunikimit është e shpejtë dhe e sigurt.



Zinxhiri i besimit: Pse i besoni një pasaportë?

Hapi 3 në bisedën e mësipërme është thelbësor: "Pse shfletuesi im i beson 'zyrës së pasaportave' (CA)?" Shfletuesi juaj (Chrome, Firefox, Safari) nuk i beson çdo certifikate që sheh. Besimi i tij është i ankoruar në një grup të vogël, të parainstaluar të Autoriteteve të Certifikimit Rrënjë (Root CA) të verifikuara me kujdes. Këto certifikata rrënjë janë të integruara drejtpërdrejt në kompjuterin tuaj ose në sistemin operativ të telefonit tuaj nga prodhuesi (Microsoft, Apple, Google). Ky grup njihet si "dyqani i besimit" (trust store). Besimi funksionon si një hierarki e quajtur "zinxhiri i besimit" (Chain of Trust):

1. **Certifikata rrënjë (Root):** Kjo është si Qeveria Qendrore (p.sh., "DigiCert Root CA"). Shfletuesi juaj i beson asaj në mënyrë absolute sepse ajo është e instaluar në "dyqanin e besimit".
2. **Certifikata e ndërmjetme (Intermediate):** Qeveria (rrënja) nuk lëshon pasaporta vetë. Ajo autorizon Zyrat e Pasaportave Lokale (të ndërmjetmet) për ta bërë këtë. Këto certifikata të ndërmjetme janë të nënshkruara nga Certifikata rrënjë.
3. **Certifikata e Serverit (e juaja):** Kjo është pasaporta aktuale e lëshuar për faqen e internetit të bankës suaj. Ajo nuk është nënshkruar nga Rrënja, por nga Zyra Lokale (e ndërmjetmja).



Kur shfletuesi juaj merr certifikatën e serverit (3), ai kontrollon: "A është nënshkruar kjo pasaportë nga një Zyrë Pasaportash e vlefshme (2)? Po. "A është kjo Zyrë Pasaportash e autorizuar nga Qeveria Qendrore (1) që unë e kam në listën time të besuar? Po." Nëse i gjithë "zinxhiri i besimit" nga serveri te rrënja është i vlefshëm, certifikata pranohet dhe dryni shfaqet.

6.3 Llojet e certifikatave dhe rëndësia e tyre në botën reale

Një nga keqkuptimet më të mëdha rreth certifikatave SSL/TLS është se disa janë "më të sigurta" se të tjerat. E vërteta është se të gjitha certifikatat e vlefshme TLS ofrojnë saktësisht të njëjtin nivel të fortë kriptimi. Për sa i përket fshehtësisë së të dhënave tuaja, një certifikatë falas DV është po aq e sigurt sa një certifikatë e shtrenjtë EV. Dallimi thelbësor midis tyre nuk është te kriptimi, por te niveli i verifikimit të identitetit që CA-ja kryen përpara se të lëshojë certifikatën. Mendoni për to si nivele të ndryshme të kartave të identitetit:

1. Vërtetimet për domeinet (DV - Domain Validated)

- **Analologjia:** Kjo është si një **kartë biblioteke**.
- **Çfarë verifikon:** Ajo provon vetëm një gjë: që ju keni kontroll mbi emrin e domeinit (p.sh., mund të merrni një email në adresën admin@example.com).
- **Procesi:** Ky proces është plotësisht i automatizuar dhe zakonisht zgjat vetëm disa minuta.
- **Për kë është:** Këto certifikata ofrojnë kriptim të plotë, por pothuajse asnjë siguri për identitetin e pronarit të faqes. Ato janë ideale për blogje, faqe personale, ose çdo faqe që nuk mbledh informacione të ndjeshme. (Shërbimi falas Let's Encrypt lëshon certifikata DV).

2. Vërtetimet për organizatat (OV - Organization Validated)

- **Analologjia:** Kjo është si një **patentë shoferi**.
- **Çfarë Verifikon:** Përveç verifikimit të domeinit (si DV), CA kryen verifikim manual të organizatës. Kjo përfshin kontrollimin e emrit ligjor të biznesit, adresës fizike dhe statusit të tij në regjistrat tregtarë.
- **Procesi:** Ky proces kërkon disa ditë punë manuale.
- **Për kë është:** Ky vërtetim ofron një nivel më të lartë besimi dhe është e përshtatshme për biznese, dyqane të vogla online dhe organizata që duan të tregojnë se janë një entitet i ligjshëm.

3. Vërtetime të zgjeruara (EV - Extended Validation)

- **Analologjia:** Kjo është si një **pasaportë diplomatike**.
- **Çfarë verifikon:** Ky vërtetim është niveli më i lartë i besimit. Ajo kërkon një proces verifikimi jashtëzakonisht të rreptë dhe të standardizuar globalisht të ekzistencës ligjore, fizike dhe operacionale të biznesit. Verifikuesi i CA-së duhet të konfirmojë jo vetëm që biznesi ekziston, por që ka autorizuar kërkesën për certifikatë.
- **Procesi:** Ky proces është i ngadaltë, i kushtueshëm dhe mund të zgjasë nga disa ditë deri në disa javë.
- **Për kë është:** Ky vërtetim ofron nivelin më të lartë të besimit dhe përdoret nga bankat, institucionet e mëdha financiare, dhe faqet kryesore të tregtisë elektronike. Në të kaluarën, shfletuesit e tregonin këtë besim duke shfaqur emrin e plotë ligjor të kompanisë në një "shirit të gjelbër" pranë drynit. Edhe pse shumica e shfletuesve e kanë hequr shiritin e gjelbër, niveli i rreptë i verifikimit mbetet.

Tabela 4: Nivelet e besimit: Çfarë verifikon certifikata juaj?

Lloji i certifikatës	Çfarë verifikon?	Niveli i besimit	Për kë është?
DV (vërtetime për domein)	Vetëm që zotëroni emrin e domenit	Ulët	Blogje, faqe personale

OV (vërtetime për organizatat)	Zotërimin e domenit + Ekzistencën e organizatës	I Mesëm	Biznese, dyqane të vogla
EV (vërtetime të zgjeruara)	Verifikim i thellë ligjor dhe fizik i biznesit	I Lartë	Banka, institucione financiare

Menaxhimi i ciklit të jetës dhe revokimi

Një aspekt kritik i sigurisë është menaxhimi i kohëzgjatjes dhe revokimit të certifikatave. Për të minimizuar dëmin në rast vjedhjeje të çelësave, jetëgjatësia maksimale e certifikatave publike është reduktuar vazhdimisht, duke arritur në **397 ditë** (rreth 13 muaj) në vitin 2020. Kur një certifikatë komprometohet para datës së skadimit, ajo duhet të revokohet menjëherë. Shfletuesit përdorin dy metoda kryesore për të kontrolluar statusin e revokimit:

1. **CRL (Certificate Revocation List):** Shfletuesi shkarkon periodikisht një listë të plotë të numrave serialë të certifikatave të revokuara. Kjo metodë është e ngadaltë dhe jo efikase për shkak të madhësisë së listave.
2. **OCSP (Online Certificate Status Protocol):** Shfletuesi dërgon një kërkesë në kohë reale te serveri i CA-së për të pyetur për statusin e një certifikate specifike. Kjo është më e shpejtë, por ka probleme privatësie (CA-ja mëson cilat faqe po vizitoni).
3. **OCSP Stapling:** Kjo është zgjidhja optimale. Vetë serveri i faqes së internetit merr statusin e tij nga CA-ja dhe ia "bashkëngjit" (staples) atë certifikatës kur ia dërgon vizitorit. Kështu, vizitori merr konfirmimin e vlefshmërisë pa pasur nevojë të kontaktojë direkt CA-në, duke ruajtur privatësinë dhe shpejtësinë.

Zgjidhja e Gabimeve të Zakonshme:

Si teknikë të ardhshëm, do të ndesheni shpesh me gabime të certifikatave. Më të zakonshmet përfshijnë:

- NET::ERR_CERT_DATE_INVALID: Certifikata ka skaduar ose ora e kompjuterit të klientit është gabim.
- NET::ERR_CERT_AUTHORITY_INVALID: Certifikata është e vetë-nënshkruar (Self-signed) ose CA-ja nuk njihet nga shfletuesi.
- NET::ERR_CERT_COMMON_NAME_INVALID: Emri i domenit në shiritin e adresës nuk përputhet me emrin në certifikatë (p.sh., certifikata është për www.shembull.com por po aksesohet mail.shembull.com).

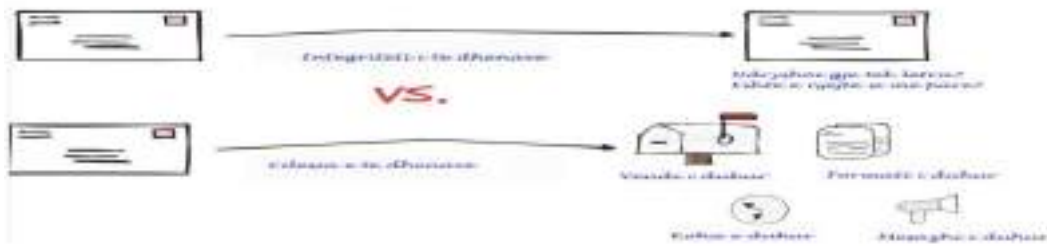
Tema 7: Integriteti dhe mbrojtja e të dhënave

Integriteti i të dhënave është garancia për saktësinë, plotësinë, qëndrueshmërinë dhe besueshmërinë e të dhënave gjatë gjithë ciklit të tyre jetësor. Ai siguron që të dhënat të jenë të besueshme dhe të përshtatshme për qëllimin për të cilin përdoren, duke parandaluar çdo ndryshim të paautorizuar ose aksidental.

Integriteti i të dhënave shpesh ngatërrohet me sigurinë e të dhënave dhe cilësinë e të dhënave, por ato kanë qëllime të ndryshme:

Siguria e të dhënave përqendrohet në mbrojtjen e të dhënave nga qasjet e paautorizuara, vjedhjet ose sulmet keqdashëse.





- ✚ Cilësia e të dhënave mat se sa të besueshme dhe të përshtatshme janë të dhënat për një detyrë specifike, duke marrë parasysh faktorë si aktualiteti dhe rëndësia.
- ✚ Integriteti i të dhënave është parim më i gjerë dhe gjithëpërfshirës që mbështetet nga masat e sigurisë dhe cilësisë së të dhënave për të siguruar që të dhënat të mbeten të sakta dhe të qëndrueshme.

7.1 Llojet e integritetit të të dhënave

Integriteti i të dhënave ndahet në dy kategori kryesore: integritet fizik dhe integritet logjik.

➤ Integriteti Fizik

Ky lloj integriteti mbron të dhënat nga dëmtimet fizike ose korrumpimi që mund të ndodhë gjatë ruajtjes ose marrjes së tyre. Ai mbron të dhënat kundër:

- Dështimeve të pajisjeve: defekte në pajisjet e ruajtjes ose në servera.
- Rreziqeve mjedisore: si ndërprerjet e energjisë elektrike, fatkeqësitë natyrore dhe pluhuri.
- Gabimeve të transmetimit: korrumpimi i të dhënave gjatë transferimit ndërmjet sistemeve.

➤ Integriteti Logjik

Ky lloj integriteti siguron që të dhënat të mbeten të qëndrueshme dhe të sakta ndërsa përdoren në një bazë të dhënash relacione. Ai mbështetet në një grup rregullash të quajtura kufizime të integritetit për të parandaluar mospërputhjet dhe gabimet.

- Integriteti i entitetit: siguron që çdo rresht në një tabelë të bazës së të dhënave të identifikohet në mënyrë unike nga një çelës primar, duke parandaluar përsëritjet ose vlerat bosh.
- Integriteti referencial: menaxhon marrëdhëniet ndërmjet tabelave të bazës së të dhënave duke përdorur çelësa të huaj. Ai parandalon të dhëna të pashoqëruara dhe siguron që referencat ndërmjet tabelave të jenë të vlefshme.
- Integriteti i domenit: siguron që një kolonë në bazën e të dhënave të përmbajë vetëm vlera të vlefshme nga një grup i paracaktuar. Për shembull, një kolonë për moshën mund të kufizohet të pranojë vetëm numra të plotë nga 1 deri në 120.
- Integriteti i përcaktuar nga përdoruesi: përfshin rregulla të personalizuar të krijuara nga përdoruesit për të përmbushur kërkesa të veçanta të biznesit ose rregullore që nuk mbulohen nga llojet e tjera të integritetit.

7.2 Rëndësia e integritetit të të dhënave

Ruajtja e integritetit të të dhënave është thelbësore për çdo organizatë që mbështetet në të dhëna për funksionimin dhe vendimmarrjen e saj, duke:

- Siguron vendimmarrje të sakta: të dhënat e besueshme janë thelbësore për analiza të sakta, që çojnë në vendime të drejta dhe efektive. Të dhënat e gabuara mund të shkaktojnë pasoja negative.
- Mbështet përputhshmërinë me rregulloret në fusha të ndryshme në industri, në shëndetësi dhe financë, që kërkojnë standarde të larta të integritetit të të dhënave.

- Forcon besimin e klientëve: mbrojtja e informacionit të klientëve nga gabimet, manipulimet ose shkeljet ndihmon në ndërtimin dhe ruajtjen e besimit dhe reputacionit.
- Përmirëson efikasitetin e veprimeve: të dhënat e besueshme zvogëlojnë kohën dhe burimet e nevojshme për korrigjimin e gabimeve, duke përmirësuar produktivitetin.
- Lehtëson përdorimin e AI dhe automatizimin e sistemeve që mbështesin përpunimin cilësor të të dhënave në kapacitete të mëdha, si inteligjenca artificiale dhe machine learning, etj.

7.3 Siguria dhe privatësia e të dhënave

Siguria e të dhënave është procesi i mbrojtjes së të dhënave të një organizate dhe parandalimit të humbjes së tyre përmes qasjes së paautorizuar. Kjo përfshin mbrojtjen e të dhënave nga sulmet që mund t'i enkriptojnë ose shkatërrojnë ato, si ransomware, si dhe nga sulmet që mund t'i ndryshojnë ose korrumpojnë të dhënat. Siguria e të dhënave siguron gjithashtu që informacioni të jetë i disponueshëm për këdo brenda organizatës që ka të drejtë ta përdorë.

Privatësia, në kuptimin më të gjerë, është e drejta e individëve, grupeve ose organizatave për të kontrolluar se kush mund të ketë qasje, të vëzhgojë ose të përdorë diçka që ata zotërojnë, si trupi, prona, idetë, të dhënat ose informacioni i tyre personal.

- Kontrolli vendoset përmes kufijve fizikë, socialë ose informacionalë që ndihmojnë në parandalimin e qasjes, vëzhgimit ose përdorimit të padëshiruar. Për shembull:
 - Një kufi fizik, si dera e mbyllur me çelës, parandalon hyrjen e të tjerëve pa leje.
 - Një kufi social, si një klub me anëtarësi, lejon vetëm anëtarët të përdorin burimet e klubit.
 - Një kufi informacional, si një marrëveshje mos-zbulimi (NDA), kufizon shpërndarjen e informacionit te palët e treta.

Rritja e shpejtë e ekonomisë globale të informacionit, e nxitur nga teknologjitë e reja dhe modelet e reja të biznesit, ka sjellë një sasi gjithnjë në rritje të të dhënave personale që mblidhen, përdoren, shkëmbehen, analizohen, ruhen dhe ndonjëherë përdoren për qëllime komerciale. Kjo rritje ka sjellë gjithashtu një numër më të madh shkeljesh të privatësisë, humbje të të dhënave dhe keqpërdorime të tyre.

Si rezultat, kërkesa për privatësi të të dhënave është e drejta për të kontrolluar mënyrën se si mblidhen, ndahen, përdoren, ruhen dhe fshihen të dhënat personale është rritur ndjeshëm, ashtu si edhe nevoja për siguri të të dhënave. Balancimi midis të drejtës së individit për privatësi dhe dëshirës së organizatave për të përdorur të dhënat personale për qëllime të tyre është një sfidë, por mund të arrihet përmes zhvillimit të një Kornize të Privatësisë së të Dhënave (Data Privacy Framework).

Organizatave të gjitha madhësive përballen me sfida të shumta për mbrojtjen e të dhënave të ndjeshme. Më poshtë paraqiten disa nga problemet më të zakonshme që lidhen me sigurinë e të dhënave dhe mënyrat sesi ato mund të ndikojnë në funksionimin e një sistemi informacioni.

➤ **Ekspozimi aksidental**

Një përqindje e madhe e shkeljeve të sigurisë së të dhënave nuk ndodh për shkak të sulmeve keqdashëse, por për shkak të pakujdesisë ose ekspozimit aksidental të të dhënave të ndjeshme. Punonjësit mund të ndajnë, humbasin ose japin qasje në të dhëna pa dashje, shpesh për shkak të mungesës së njohurive mbi politikën e sigurisë. Ky problem mund të reduktohet përmes trajnimit të punonjësve dhe përdorimit të teknologjive të parandalimit të humbjes së të dhënave (Data Loss Prevention – DLP).

➤ **Phishing dhe sulmet e inxhinierisë sociale**

Sulmet e inxhinierisë sociale janë një nga metodat kryesore që përdorin hakerat për të marrë qasje në të dhënat e ndjeshme. Këto sulme bazohen në manipulimin e njerëzve që të zbulojnë informacion privat ose të japin qasje në sisteme të mbrojtura.

Phishing është një formë e zakonshme e inxhinierisë sociale, ku dërgohen mesazhe që duken sikur vijnë nga burime të besuara, por në fakt janë nga sulmues që kërkojnë të mashtrojnë viktimën për të ndarë informacion konfidencial ose për të klikuar në lidhje të dëmshme. Kjo mund të çojë në komprometimin e pajisjeve dhe rrjeteve të organizatës.

➤ **Kërcënimet e brendshme (Insider Threats)**

Kërcënimet e brendshme janë një rrezik i vazhdueshëm për sigurinë e të dhënave. Ato ndahen në tre kategori kryesore:

- Përdoruesit jo-keqdashës – punonjës që shkaktojnë dëme aksidentalisht për shkak të pakujdesisë ose mungesës së njohurive mbi praktikën e sigurta.
- Përdoruesit keqdashës – individë që me qëllim përpiqen të vjedhin të dhëna ose të dëmtojnë organizatën për përfitim personal.
- Përdoruesit e komprometuar – punonjës që nuk janë të vetëdijshëm se llogaritë ose kredencialet e tyre janë komprometuar nga një sulmues i jashtëm.

➤ **Ransomware**

Ransomware është një kërcënim i madh për të dhënat e organizatave. Është një lloj malware që infekton pajisjet dhe enkripton të dhënat, duke i bërë ato të paaksesueshme pa çelësin e dekriptimit. Sulmuesit kërkojnë pagesë (ransom) për të lëshuar çelësin, por shpesh edhe pas pagesës, të dhënat mbeten të humbura. Ransomware mund të përhapet shpejt në një rrjet të tërë dhe, nëse nuk ka kopje rezervë të ruajtura në mënyrë të sigurt, rikuperimi bëhet i pamundur.

➤ **Humbja e të dhënave në Cloud**

Kalimi i të dhënave në mjediset cloud ka përmirësuar ndarjen dhe bashkëpunimin, por ka sjellë edhe rreziqe të reja. Kur të dhënat ruhen në cloud, kontrolli mbi to bëhet më i vështirë. Përdoruesit mund të qasen nga pajisje personale ose rrjete të pasigurta, dhe shpërndarja e skedarëve me persona të paautorizuar mund të ndodhë lehtësisht, si aksidentalisht ashtu edhe qëllimisht.

➤ **SQL Injection**

SQL Injection (SQLi) është një teknikë e zakonshme që përdoret nga sulmuesit për të hyrë në mënyrë të paligjshme në bazat e të dhënave, për të vjedhur informacion ose për të modifikuar të dhënat. Kjo ndodh kur sulmuesi fut kod të dëmshëm në një kërkesë SQL përmes një fushe inputi në një faqe interneti ose aplikacion.

Në vend që sistemi të përpunojë vetëm të dhënat e përdoruesit, ai ekzekuton kodin e dëmshëm të futur nga sulmuesi. SQL injection mund të çojë në ekspozimin e të dhënave të klientëve, vjedhjen e pronës intelektuale ose marrjen e kontrollit të plotë mbi bazën e të dhënave. Kjo ndodh zakonisht për shkak të praktikave të pasigurta në programim dhe mund të parandalohet lehtësisht përmes përdorimit të mekanizmave të sigurt për marrjen e inputeve të përdoruesit.

7.4 Mënyrat për të siguruar dhe mirëmbajtur integritetin e të dhënave

Ruajtja e integritetit të të dhënave është një proces i vazhdueshëm që përfshin kombinimin e kontrollit teknik, politikave dhe kulturës organizative.

- Përdorimi i verifikimit dhe vlefshmërisë së të dhënave: zbatimi i rregullave që kontrollojnë saktësinë dhe plotësinë e të dhënave në momentin e futjes së tyre, si në anën e klientit (formularët në web) ashtu edhe në anën e serverit.
- Vendosja e kontrollit të aksesit: kufizimi i përdoruesve që mund të qasen, modifikojnë ose fshijnë të dhëna bazuar në rolet dhe përgjegjësitë e tyre. Parimi i privilegjit minimal siguron që përdoruesit të kenë vetëm qasjen e nevojshme për detyrat e tyre.
- Kryerja e kopjeve rezervë të rregullta: ruajtja periodike e kopjeve rezervë të të dhënave në vendndodhje të sigurta për t'u mbrojtur nga humbjet për shkak të dështimeve të sistemit, korrupsionit ose sulmeve kibernetike.
- Krijimi i gjurmëve të auditimit: gjenerimi automatik i regjistrave që ndjekin ndryshimet në të dhëna, duke përfshirë se kush dhe kur i ka bërë ato. Kjo ndihmon në gjurmimin e burimit të një gabimi dhe rrit llogaridhënien.
- Zbatimi i enkriptimit të të dhënave: mbrojtja e të dhënave të ndjeshme përmes enkriptimit gjatë transmetimit dhe ruajtjes. Edhe në rast të shkeljes, të dhënat mbeten të palexueshme.

- Zhvillimi i një kornize të qeverisjes së të dhënave: përcaktimi i politikave dhe procedurave të qarta për menaxhimin e të dhënave gjatë gjithë ciklit jetësor, duke përfshirë përcaktimin e roleve dhe përgjegjësi që forcojnë ndjenjën e pronësisë së të dhënave.
- Trajnimi i punonjësve: edukimi i punonjësve mbi rëndësinë e integritetit të të dhënave dhe mënyrat e duhura të menaxhimit për të minimizuar rrezikun e gabimeve njerëzore.

7.5 Masat e sigurisë për privatësinë e të dhënave

Shembuj të masave të sigurisë përfshijnë:

- Menaxhimin e ndryshimeve – monitoron dhe regjistron ndryshimet në strukturën e të dhënave, duke demonstruar përputhje me procedurat e kontrollit.
- Parandalimin e humbjes së të dhënave (Data Loss Prevention – DLP) – monitoron dhe mbron të dhënat gjatë lëvizjes në rrjet, në ruajtje ose në përdorim, për të parandaluar vjedhjen ose përdorimin e paautorizuar.
- Maskimin e të dhënave – anonimizon të dhënat përmes enkriptimit, hashimit ose pseudonimizimit për të mbrojtur të dhënat reale gjatë përdorimit.
- Mbrojtjen e të dhënave – siguron integritet dhe konfidencialitet përmes kontrollit të ndryshimeve, menaxhimit të pyetjeve dhe kufizimit të transferimit të të dhënave përtej kufijve.
- Monitorimin e përdoruesve me privilegje – mbikëqyr përdoruesit që kanë akses të gjerë në bazat e të dhënave dhe ndalon aktivitetet e dyshimta.
- Auditimin e qasjes në të dhëna të ndjeshme – gjurmon qasjen dhe ndryshimet e të dhënave të mbrojtura nga ligjet ose kontratat, duke aktivizuar alarme për shkelje të mundshme.
- Arkivimin e sigurt të gjurmëve të auditimit – siguron që regjistrat e auditimit të mos manipulohen ose fshihen, duke mundësuar analizë forenzike në rast incidenti.

Tema 8: Auditimi dhe testimi i sigurisë së sistemeve

8.1 Konceptet kryesore të auditimit dhe sigurisë së të dhënave

Auditimi i sigurisë është shqyrtimi gjithëpërfshirës dhe i pavarur i sistemeve të informacionit, politikave dhe praktikave të një organizate për të identifikuar dobësitë, për të vlerësuar pajtueshmërinë me rregulloret dhe për të rekomanduar përmirësime të sigurisë.

Ai vlerëson fusha të ndryshme, duke përfshirë konfigurimin e rrjetit, sigurinë fizike, softuerin dhe praktikën e punonjësve, dhe mund të përdorë si metoda manuale ashtu edhe mjete të automatizuara. Kryerja e auditimeve të rregullta ndihmon në mbrojtjen e të dhënave të ndjeshme, parandalimin e shkeljeve dhe sigurimin e pajtueshmërisë me standardet e industrisë dhe kërkesat ligjore.

Organizatat duhet të kryejnë auditime të sigurisë së të dhënave në mënyrë periodike për të identifikuar boshllëqet dhe dobësitë në sistemet e tyre. Auditimet mund të kryhen nga ekipe të brendshme ose nga ekspertë të jashtëm (si në testimet e penetrimit). Rezultatet e auditimeve ndihmojnë organizatën të marrë masa korrigjuese dhe të përmirësojë mbrojtjen e përgjithshme të të dhënave.

➤ Pse duhet të auditojmë dhe të testojmë sigurinë e të dhënave?

1. Përputhshmëria me rregullat në fuqi (p.sh., GDPR, HIPAA, PCI-DSS, ISO 27001)
2. Menaxhimi i riskut - Zbulimi i dobësive dhe boshllëqeve të kontrollit.
3. Sigurimi operacional - Verifikimi që politikat e sigurisë zbatohen në mënyrë korrekte.
4. Parandalimi i incidenteve dhe gatishmëria për reagim
5. Besimi dhe mirëbesimi i palëve të interesuara

8.2 Metodatat e auditimit të sigurisë

Metodologjitë e auditimit të sigurisë janë procese sistematike për vlerësimin e gjendjes së sigurisë së një organizate përmes metodave të ndryshme si testimi i depërtimit, vlerësimet e cenueshmërisë, vlerësimet e rrezikut dhe auditimet e përputhshmërisë. Këto metodologji zakonisht ndjekin një proces me faza, duke përfshirë planifikimin, mbledhjen e informacionit, vlerësimin e rrezikut, testimin, raportimin dhe ndreqjen. Metodologjia specifike e zgjedhur varet nga objektivat e auditimit, të cilat mund të variojnë nga vlerësimet teknike të infrastrukturës deri te kontrollet njerëzore dhe procedurale.

➤ **Auditimi I brendshëm dhe i jashtëm:**

- I brendshëm - Kryhet nga vete ekipet e kompanive apo institucioneve dhe janë procese të vazhdueshme dhe me fokus specifik.
- I jashtëm – Auditues të pavarur që kanë për qëllim kontrollin e përputhshmërisë së sigurisë me legjisllacionin në fuqi dhe certifikimin.

➤ **Baza ligjore e auditimeve të zakonshme:**

- ISO/IEC 27001 & 27002 – Standard ndërkombëtar për kontrollet e sigurisë së informacionit.
- Seria NIST SP 800 - Udhëzime të strukturuar për kontrollet dhe vlerësimet e sigurisë kibernetike.
- COBIT – Qeverisja dhe menaxhimi i proceseve të IT-së.
- SOC 2 – Auditime që përqendrohen në siguri, disponueshmëri, konfidencialitet, etj.

8.3 Proceset audituese

Procesi i auditimit të sigurisë së informacionit është proces sistematik për vlerësimin e kontrolleve të sigurisë, politikave dhe praktikave për gjetjen e vulnerabiliteteve në organizata si dhe sigurimin e përshtatshmërisë ligjore dhe qëndrimet ndaj aspekteve të sigurisë. Procesi përfshin planifikimin, mbledhjen e evidencave, analizat dhe raportimet për të siguruar rekomandimet për zgjidhjet. Ky proces aplikohet në kontrollet teknike, sigurinë fizike, procedurat administrative dhe kapacitetet për menaxhimin e incident response.

➤ **Planifikimi dhe përcaktimi i fushëveprimit**

- Përcaktimi i objektivave, sistemet, rrjedhat e të dhënave dhe palët e interesuara.
- Identifikimi i kërkesave rregullatore.
- Përcaktimi i metodave dhe mjeteve të auditimit.

➤ **Grupi i evidencave**

- Rishikimi i dokumentacionit: Politikat, procedurat, regjistrat.
- Intervista: Personeli i sigurisë, pronarët e sistemit.
- Vëzhgim: Siguria fizike, sjellja e përdoruesit.
- Ekzaminim teknik: Detajet e konfigurimit, listat e aksesit.

➤ **Vlerësimi I kontrollit**

- Kontrollet administrative (politika, trainime)
- Kontrollet teknike (firewall, enkriptim)
- Kontrollet fizike
- Efektiviteti i dizenjimit
- Korrektësia e funksionimit

➤ **Raportimet**

Raporti i auditit përfshin:

- Gjetjet dhe niveli I rrezikut
- Kontrolli I dobësive
- Rekomandime
- Afatet kohore për rikuperimet

8.4 Siguria e API-ve

API-të (Application Programming Interfaces) ekspozojnë shërbime dhe të dhëna për aplikacione të tjera dhe për këtë arsye janë një objekt i zakonshëm i sulmeve. API-të e pasigurta mund të lejojnë qasje të paautorizuar, rrjedhje të të dhënave ose ekzekutim të kodit nga distanca. Për shkak se shumë aplikacione moderne mbështeten në API, sigurimi i tyre është thelbësor për mbrojtjen e të dhënave.

Një strategji efektive e sigurisë së API-ve përfshin:

- Autentifikimin dhe autorizimin e çdo kërkesë për t'u siguruar që përdoruesi ka të drejtë lidhje në rrjet/sistem.
- Kufizimin e shpejtësisë së kërkesave për të parandaluar abuzime dhe sulme të tipit Denial of Service.
- Verifikimin e inputeve për të shmangur injektimet dhe korrumpimin e të dhënave.
- Përdorimin e enkriptimit TLS për mbrojtjen e të dhënave gjatë transmetimit.
- Monitorimin dhe logimin e kërkesave për të identifikuar aktivitetet e pazakonta.
- Përdorimin e një platforme për menaxhimin e API-ve që mundëson kontroll të centralizuar dhe testime të rregullta për dobësi.

8.5 Testimi i depërtimit

Pse na duhet testimi i depërtimit? Epo, para së gjithash, si dikush që është përgjegjës për sigurimin dhe mbrojtjen e një rrjeti/sistemi, ju doni të gjeni çdo rrugë të mundshme sigurimi përpara se keqbërësit t'ju gjejnë të papërgatitur. Për vite me radhë janë zhvilluar dhe zbatuar shumë teknika të ndryshme mbrojtëse (për shembull, antivirus, firewall-e, sisteme parandalimi ndërhyrjesh [IPS], anti-malware). Zakonisht vendosen mbrojtje të avancuara si metoda për të siguruar dhe mbrojtur rrjetet e komunikimit. Por si mund ta dimë nëse këto mbrojtje funksionojnë vërtet dhe nëse janë të mjaftueshme për të mbajtur larg keqbërësit? Sa të vlefshme janë të dhënat që po mbrojmë dhe a po mbrojmë gjërat e duhura? Këto janë disa nga pyetjet që duhet të marrin përgjigje nga një test depërtimi. Nëse ndërtoni një gardh rreth oborrit tuaj me qëllim që ta pengoni qenin tuaj të dalë, ndoshta duhet të jetë vetëm 4 metra i lartë. Nëse shqetësimi juaj nuk është a mund të dalë qeni, por a mund ta ndaloj një keqbërës të hyjë brenda, atëherë ju nevojitet një gardh tjetër - një që do të duhej të ishte shumë më i lartë se 4 metra. Në varësi të asaj që po mbron, mund të dëshironi edhe tela me gjemba në majë të gardhit për të penguar edhe më shumë keqbërësit. Kur bëhet fjalë për sigurinë e informacionit, duhet të bëjmë të njëjtin lloj vlerësimesh në rrjetet dhe sistemet tona. Duhet të përcaktojmë se çfarë po mbrojmë dhe nëse mbrojtjet tona mund t'i rezistojnë kërcënimeve që u imponohen atyre. Këtu hyn në lojë testimi i depërtimit. Thjesht implementimi i një firewall-i, një IPS-i, anti-malware-i, një VPN-i, një firewall-i të aplikacioneve web (WAF) dhe mbrojtjeve të tjera moderne të sigurisë nuk është i mjaftueshëm. Gjithashtu duhet të testoni vlefshmërinë e tyre. Dhe duhet ta bëni këtë rregullisht. Siç e dini, rrjetet dhe sistemet ndryshojnë vazhdimisht. Kjo do të thotë që sipërfaqja e sulmit mund të ndryshojë gjithashtu, dhe kur ndodh, duhet të merrni në konsideratë rivlerësimin e gjendjes së sigurisë me anë të një testi depërtimi.

Testimi i depërtimit është simulimi i një sulmi sigurie (cyberattack) që kryhet nga një ethical hacker për identifikimin e vulnerabiliteteve të shfrytëzimit në sistemet kompjuterike, rrjeta apo aplikacione. Duke i identifikuar qëllimisht dobësitë, një organizatë mund ti rregullojë ato plotësisht para se sulmues të dëmshëm mund ti zbulojnë dhe të forcojnë pozitat e tyre të sigurisë. Hapat për realizimin e një testimi depertimi:

1. Planifikimi dhe përcaktimi i objektivave

- përcaktohen sistemet që do të testohen
- përcaktohet lloji i testit (black-box, gray-box, white-box)
- merret autorizim me shkrim nga institucioni

- përcaktohen kufijtë e testimit (çfarë lejohet dhe çfarë jo)

Pa autorizim, çdo testim është i paligjshëm.

2. Mbledhja e informacionit (Reconnaissance)

- identifikimi i IP-ve të targetit
- identifikimi i portave të hapura
- versionet e shërbimeve (p.sh. web server ose databazë)
- topologjia e rrjetit

3. Analiza e dobësive (Vulnerability assessment)

- krahasimi i versioneve të softuerëve me databaza dobësish (CVE)
- skanime të lejuara të dobësive
- analizimi i konfigurimeve të rrjetit

4. Testimi i dobësive (Exploitation) – i kontrolluar dhe i kufizuar

Në një penetration test të thjeshtë, kjo fazë bëhet me shumë kujdes.

testohen vetëm dobësitë që janë lejuar me autorizim

nuk dëmtohet sistemi, kontrollohet nëse dobësia mund të çojë në akses të paautorizuar dokumentohet çdo hap i tentuar

- “A mund të lexohen të dhënat?”
- “A mund të rriten privilegjet?”
- “A mund të shmangen politikat e aksesit?”

5. Raportimi dhe propozimi i masave

Raporti është pjesa më e rëndësishme në një pen-test professional dhe përfshin:

- dobësitë e identifikuara
- rreziku i secilës dobësi
- hapat që u ndoqën
- evidenca (screenshots, log)
- rekomandimet e sigurisë
- prioritetet e remediimit (kritike, të larta, mesatare, të ulëta)

Tema 9. Menaxhimi i aksesit dhe rolit të përdoruesve

9.1 Konceptet themelore të kontrollit të aksesit

Menaxhimi i aksesit bën të mundur kontrollin se kush mund të hyjë në burimet dixhitale duke përdorur role dhe leje, ndërsa rolet e përdoruesve përcaktojnë nivelin e aksesit të një përdoruesi bazuar në funksionet e tyre të punës. Një sistem i fortë siguron që vetëm individët e autorizuar mund të hyjnë në të dhënat që u nevojiten dhe është një komponent thelbësor i menaxhimit të identitetit dhe aksesit (IAM), i cili menaxhon identitetet dhe të drejtat e aksesit të përdoruesve. Kjo ndihmon në parandalimin e shkeljeve të të dhënave, humbjeve financiare dhe dëmtimit të reputacionit.

➤ Roli i kontrollit të aksesit

Kontrolli i aksesit është një komponent kyç i sigurisë së informacionit që synon të kufizojë hyrjen në sisteme, rrjete dhe të dhëna vetëm për përdoruesit e autorizuar, me qëllim kryesor:

- mbrojtjen e konfidencialitetit të të dhënave
- mbrojtjen e integritetit
- garantimin e disponueshmërisë së shërbimeve
- Komponentët e kontrollit të aksesit
 - Identifikimi – përdoruesi deklaron identitet (username, ID).
 - Autentikimi – vërtetohet se përdoruesi është ai që pretendon.
 - Autorizimi – përcaktohet çfarë aksesit ka përdoruesi në sistem.

- Auditimi – monitorim dhe regjistrim i veprimeve për siguri.

➤ Modelet themelore të kontrollit të aksesit

- DAC (Discretionary Access Control)

Ai që zotëron resurset përcakton kush mund t'i aksesojë. Ky model krijon vështirësi menaxhimi sidomos në organizata të mëdha.

- MAC (Mandatory Access Control)

Vendimet për akses bazohen në nivelet e sigurisë dhe nivelet e autorizimit.

Një autoritet qendror (p.sh., administratori i sigurisë) përcakton politikën dhe nuk mund të ndryshohet nga pronari i objektit. Shpesh përdoret në mjedise shumë të sigurta (p.sh., ushtarake, qeveritare).

- RBAC (Role-Based Access Control)

Akcesi sigurohet bazuar në rolin e përdoruesve të një organizate. Rolet janë një grup të drejtash. Përdoruesve u përcaktohen rolet. Ky është modeli më i zakonshëm që përdorin sot kompanitë.

- ABAC (Attribute-Based Access Control)

Një model sigurie që jep akses në burime bazuar në politika që vlerësojnë atributet e përdoruesit, burimit, veprimit dhe mjedisit. Ndryshe nga RBAC, i cili mbështetet në role fikse, ABAC është dinamik dhe ofron kontroll të detajuar, të vetëdijshëm për kontekstin, duke lejuar përshtatjen në kohë reale ndaj situatave në ndryshim

9.2 Implementimi i aksesit të kontrollit

Implementimi i kontrollit të aksesit përfshin përcaktimin e politikave dhe roleve, zgjedhjen e një modeli aksesit (si RBAC ose ABAC), ngritjen e mekanizmave të vërtetimit dhe autorizimit, si dhe monitorimin dhe auditimin e rregullt të aksesit. Hapat kryesorë përfshijnë identifikimin e kërkesave të sigurisë, zgjedhjen e një sistemi të përshtatshëm të kontrollit të aksesit, zbatimin e privilegjit më të vogël dhe trajnimin e punonjësve mbi procedurat:

1. Planifikimi dhe hartimi i strategjive

- Vlerësimi i nevojave të sigurisë - Identifikoni se çfarë duhet mbrojtur, duke përfshirë burimet dhe proceset.
- Përcaktimi i politikave - Vendosni rregulla të qarta se kush mund të hyjë në çfarë, kur dhe në çfarë kushtesh.
- Zgjidhja e një modeli kontrolli aksesit - Zgjidhni një model që i përshtatet nevojave tuaja.
- Zbatimi i “Zero Trust” - Miratoni një politikë "kurrë mos u besoni, gjithmonë verifikoni", që kërkon verifikim të rreptë për çdo kërkesë aksesit.
- Zbatimi i “Parimi i Privilegjit Më të Vogël” - Jepuni përdoruesve vetëm lejet minimale të nevojshme për punën e tyre

Në menaxhimin e aksesit duhet të konsiderojmë gjithmonë 4 A-të:

- Administrimi
- Autentifikimi
- Autorizimi
- Auditimi

9.3 Konfigurimi i aksesit të kontrollit

- Zgjidhni një sistem:

Zgjidhni teknologjinë dhe sistemet e duhura të kontrollit të aksesit, siç janë zgjidhjet e menaxhimit të identitetit dhe aksesit (IAM).

- Konfiguroni autentifikimin:

Zbatoni metoda të forta autentifikimi, duke përfshirë autentifikimin shumëfaktorësh (MFA).

- Vendosni profile dhe role përdoruesish:

Krijoni profile individuale përdoruesish dhe caktoni atyre role të përshtatshme me leje të paracaktuara.

- Automatizoni sigurimin:

Përdorni mjete të automatizuara për të trajtuar sigurimin dhe heqjen e aksesit të përdoruesit, gjë që zvogëlon gabimet dhe kursen kohë.

- Integroni sistemet:

Lidhni zgjidhjen e kontrollit të aksesit me aplikacionet ekzistuese të sigurisë dhe biznesit.

9.4 Monitorimi dhe mirëmbajtja

- Monitorimi dhe auditimi i rregullt

Monitoroni vazhdimisht lojet e aksesit për veprimtari të dyshimta dhe kryesni auditime periodike për t'u siguruar që lejet janë akoma të vlefshme dhe për të identifikuar vulnerabilitetet.

- Përditësimi i politikave dhe roleve

Rishikoni dhe përditësoni politikat e aksesive dhe rolet pasi detyrat e funksioneve dhe përgjegjësitë ndryshojnë kohë pas kohe.

- Trajtoni punonjësit

Edukoni punonjësit me procedurat e kontrolleve dhe protokollet e sigurisë për t'u siguruar që ata kuptojnë përgjegjësitë e tyre.

Tema 10 : Ruajtja dhe disponueshmëria e të dhënave

10.1 Kuptimi i ruajtjes së të dhënave dhe rëndësia e tyre



Në epokën digjitale, të dhënat janë pasuria më e vlefshme e çdo individ apo institucioni. Ruajtja e të dhënave nënkupton procesin e grumbullimit dhe mbajtjes së informacionit në mënyrë të organizuar, me qëllim përdorimin e tij në të ardhmen. Ky proces siguron që informacioni të mos humbasë, të jetë gjithmonë i disponueshëm dhe të përdoret në mënyrë efektive.

Për shembull, një mësuese që humbet dokumentet e planifikimit për shkak të një virusi, mund t'i

rikuperojë dokumentet nëse i ka ruajtur në *Google Drive* ose në një *USB* rezervë. Nëse jo, ajo do të detyrohet t'i rikrijë nga e para. Kjo tregon rëndësinë e ruajtjes së rregullt të të dhënave.

Ruajtja e të dhënave është një nga funksionet më të rëndësishme të çdo sistemi kompjuterik. Pa të, çdo informacion do të humbiste menjëherë pas fikjes së pajisjes. Rëndësia e ruajtjes shfaqet në disa aspekte:

1. Sigurimi i vazhdimësisë së punës (Continuity of Work)

Në shkolla, kompani apo institucione, ruajtja e të dhënave siguron që dokumentet, projektet dhe informacionet të mos humbasin, por të jenë gjithmonë të aksesueshme.

2. Mbrojtja e informacionit (Data Protection)

Ruajtja e sigurt në media të ndryshme ose në cloud parandalon humbjen e të dhënave për shkak të defekteve, viruseve apo gabimeve njerëzore.

3. Arkivimi (Archiving)

Të dhënat që nuk përdoren më shpesh ruhen për qëllime reference. Kjo është shumë e rëndësishme për institucionet arsimore dhe jo vetëm, të cilat duhet të ruajnë dokumentet zyrtare për vite me radhë.

4. Shkëmbimi i të dhënave (Data Sharing)

Të dhënat e ruajtura mund të ndahen lehtësisht me përdorues të tjerë përmes rrjeteve lokale ose *cloud-it*.

5. Efikasiteti dhe performanca

Përdorimi i teknologjive të reja (si *SSD* ose *Cloud*) rrit shpejtësinë e aksesit dhe përpunimit të të dhënave.

10.2 Llojet e *backup-it*

Backup-i është procesi i krijimit të një kopjeje rezervë të të dhënave për t'u përdorur në rast se versioni origjinal humbet ose dëmtohet. Ai është pjesë thelbësore e sigurisë digjitale dhe përdoret nga individët dhe institucionet. Ekzistojnë tre lloje kryesore të *backup-it*: *Full Backup* (kopje e plotë), *Incremental Backup* (kopje shtesë), dhe *Differential Backup* (kopje dalluese).

1. Backup i plotë (*Full Backup*)

Ky *backup* konsiderohet si forma më bazike dhe më e plotë e ruajtjes, pasi krijon një kopje identike të të gjitha skedarëve dhe dosjeve në një moment të caktuar.

Zakonisht realizohet një herë në javë ose çdo fundjavë, kur kompjuteri është më pak i ngarkuar.

Shembull praktik:

Një nxënës dëshiron të ruajë të gjitha projektet e tij në kompjuterin e shkollës. Ai:

1. Hyn në *File Explorer*.
2. Zgjedh dosjen “Projektet e mia”.
3. Klikon me të djathtën → *Send to* → *External Hard Drive (D:)*.
4. Pasi përfundon, kontrollon që kopja është ruajtur në hard diskun e jashtëm.

Avantazhi: të gjitha të dhënat janë të sigurta në një vend.

Mangësia: zgjat shumë kohë dhe kërkon më shumë hapësirë ruajtjeje.

2. Backup inkremental (*Incremental Backup*)

Ky lloj *backup-i* ruan vetëm ndryshimet që janë bërë që nga *backup-i* i fundit.

Përdoret shpesh në kompani dhe institucione që përditësojnë shumë të dhëna çdo ditë.

Në këtë mënyrë, çdo ditë ruhen vetëm dokumentet e reja ose ato që janë ndryshuar.

Shembull praktik:

1. Instaloni programin *Cobian Backup* (ose përdorni “*Backup and Restore*” në *Windows*).
2. Zgjidhni *Incremental Backup*.
3. Vendosni burimin (p.sh., “*C:\Users\Documents*”) dhe destinacionin (“*E:\Backup*”).
4. Vendosni që programi të bëjë *backup* çdo ditë në orën 18:00.

Avantazhi: kursen hapësirë dhe kohë.

Mangësia: kërkon që të keni të gjitha *backup-et* për të bërë rikuperimin e plotë.

3. Backup diferencial (*Differential Backup*)

Backup diferencial ruan të gjitha ndryshimet që janë bërë që nga *backup-i* i plotë i fundit.

Nëse *backup-i* i plotë bëhet të dielën, atëherë të hënën ruhen vetëm ndryshimet e ditës, të martën ruhen të gjitha ndryshimet nga e diela e deri të martën, e kështu me radhë.

Shembull praktik:

1. Hap programin *AOMEI Backupper*.
2. Zgjedh “*Differential Backup*”.
3. Vendos destinacionin “*Cloud Drive*” (p.sh., *Google Drive* ose *OneDrive*).
4. Programi ruan çdo ditë ndryshimet që nga *backup-i* i plotë i fundit.

Avantazhi: rikuperimi është më i lehtë se *backup-i incremental*.

Mangësia: zë më shumë hapësirë.

10.3 Backup lokal dhe backup në cloud

Backup lokal ruhet në pajisje fizike që ndodhen pranë përdoruesit, si *hard disk*, *USB*, ose *server*.

Këto janë të dobishme për rikuperime të shpejta.

Avantazhet e backup-it lokal

- ✓ Shpejtësi e lartë kopjimi dhe rikuperimi.
- ✓ Nuk kërkon lidhje interneti.
- ✓ Kontroll i plotë nga përdoruesi mbi të dhënat.

Kufizimet

- ✓ Mund të dëmtohet fizikisht nga zjarri, uji apo rënia.
- ✓ Në rast vjedhjeje, të dhënat humbasin bashkë me pajisjen.
- ✓ Kërkon hapësirë dhe kujdes për mirëmbajtje.

Backup në cloud

Cloud Backup ruan të dhënat në serverë të jashtëm përmes internetit (p.sh. *Google Drive*, *OneDrive*, *Dropbox*). Këto servera ruajnë të dhënat në mënyrë të sigurt, shpesh në disa vendndodhje të ndryshme njëkohësisht, për të shmangur humbjet.

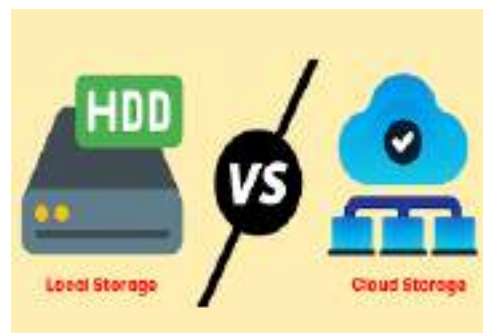
Është më i sigurt dhe mund të aksesohet nga çdo pajisje.

Avantazhet e backup-it në cloud

- ✓ Aksesueshmëri nga çdo vend dhe pajisje me internet.
- ✓ Të dhënat ruhen në mënyrë të koduar (*Encrypted*).
- ✓ Serverat cloud bëjnë *backup automatik* çdo ditë.
- ✓ Nuk rrezikon nga dëmtimet fizike lokale.

Kufizimet

- ✓ Kërkon lidhje të qëndrueshme interneti.
- ✓ Hapësira falas është e kufizuar.
- ✓ Siguria varet nga politika e ofruesit të shërbimit (*Service Provider Security*).



Tipi i Backup-it	Kosto	Shpejtësi	Siguri	Aksesueshmëri
Lokal	Më e lartë në fillim (<i>hardware</i>)	E shpejtë	Mund të rrezikohet nga dëmtimi fizik	Vetëm në një vend
Cloud	Me abonim (mujo/vjetor)	Më e ngadaltë në varësi të internetit	E lartë (enkriptim)	Nga çdo pajisje dhe vend

Shembull praktik 1:

1. Lidh një *hard disk* të jashtëm me kompjuterin.
2. Hape menunë *Settings* → *Update & Security* → *Backup*.
3. Zgjidh opsionin *Add a drive* dhe zgjidh pajisjen.
4. Kliko *Automatically back up my files*.

Kompjuteri do të bëjë *backup* automatikisht çdo ditë.

Shembull praktik 2:

1. Hap *Google Drive*.

2. Krijoni një dosje “*Backup* të dhënash”.
3. Tërhiq (*drag & drop*) dosjen e dokumenteve për ta ngarkuar.
4. Aktivizoj opsionin *Backup and Sync* në *Google Drive* për ruajtje automatike.

10.4 Procesi i rikuperimit të të dhënave

Rikuperimi i të dhënave (*Data Recovery*) është procesi përmes të cilit ne rivendosim informacionin e humbur, të fshirë apo të dëmtuar, në mënyrë që të mund të përdoret sërish.

Ky proces është pjesë shumë e rëndësishme e menaxhimit të sigurisë së të dhënave (*Data Security Management*), sepse ndihmon përdoruesit dhe institucionet të shmangin humbjen e punës së tyre. Humbja e të dhënave (*Data Loss*) mund të ndodhë për shumë arsye, si:

- Fshirje aksidentale (*Accidental Deletion*)
- Sulme nga viruse ose *malware* (*Virus Attacks / Malware*)
- Defekte fizike të pajisjeve (*Hardware Failure*)
- Dështime të sistemit operativ (*System Crash*)
- Ndërprerje elektrike (*Power Failure*)
- Gabime njerëzore (*Human Errors*)

Në çdo rast, rikuperimi i të dhënave mund të kryhet vetëm nëse më parë është realizuar një kopje rezervë (*backup*) ose nëse ekzistojnë versione të ruajtura automatikisht nga sistemi.

Këshilla për rikuperim të suksesshëm

1. Mos shkruani të dhëna të reja në pajisjen ku janë humbur skedarët – kjo mund të mbishkruajë (*overwrite*) informacionin e fshirë.
2. Ruani gjithmonë kopje rezervë automatike (*auto backup*) në *cloud* ose në një disk të jashtëm.
3. Testoni rregullisht programet e backup-it për t’u siguruar që funksionojnë.
4. Nëse disku është dëmtuar fizikisht, mos e hapni vetë – dërgojeni në një qendër rikuperimi profesionale (*Data Recovery Center*).

Procesi i rikuperimit të të dhënave (*Steps in Data Recovery*) nuk është i njëjtë për çdo situatë, por zakonisht përfshin disa hapa standardë:



Hapi (<i>Step</i>)	Përshkrimi (<i>Description</i>)	Shembull praktik (<i>Example</i>)
1. Identifikimi i të dhënave të humbura (<i>Identify Lost Files</i>)	Përdoruesi duhet të përcaktojë se cilat dokumente ose skedarë mungojnë.	Nxënësi vëren që mungon dokumenti “ <i>Projekti.docx</i> ”.
2. Kontrollimi i vendndodhjes së fshirjes (<i>Check Recycle Bin / Trash</i>)	Shpesh, skedarët mund të jenë fshirë, por ndodhen ende në “ <i>Koshi</i> ” (<i>Recycle Bin</i>).	Përdoruesi hap <i>Recycle Bin</i> dhe zgjedh “ <i>Restore</i> ”.
3. Përdorimi i programeve të backup-it (<i>Use Backup Software</i>)	Hapet programi i kopjeve rezervë për të rikthyer versionet e ruajtura.	Përdorimi i <i>AOMEI Backupper</i> , <i>Cobian</i> ose <i>OneDrive Restore</i> .

4. Zgjedhja e kopjes rezervë (Select Backup Version)	Përdoruesi zgjedh versionin më të fundit ose më të qëndrueshëm të skedarit.	Nga “OneDrive → View version history”, zgjedh versionin e mëparshëm.
5. Rikthimi i skedarëve (Restore Files)	Klikohet opsioni “Restore” dhe zgjidhet vendndodhja ku duam t’i rikthejmë.	Ruajtja në një dosje të veçantë “Rikuperime”.
6. Testimi i funksionimit (Test Restored Files)	Pas rikuperimit, dokumentet hapen për të siguruar që janë të plota dhe funksionale.	Hapja e dokumentit “WebDesign.docx” për kontroll.

Këshilla për rikuperim të suksesshëm

5. Mos shkruani të dhëna të reja në pajisjen ku janë humbur skedarët – kjo mund të mbishkruajë (*overwrite*) informacionin e fshirë.
6. Ruani gjithmonë kopje rezervë automatike (*auto backup*) në *cloud* ose në një disk të jashtëm.
7. Testoni rregullisht programet e backup-it për t’u siguruar që funksionojnë.
8. Nëse disku është dëmtuar fizikisht, mos e hapni vetë – dërgojeni në një qendër rikuperimi profesionale (*Data Recovery Center*).

Shembull praktik

Kemi punuar disa ditë në projektin “WebDesign.docx”.

Pas një ndërprerjeje të papritur të energjisë, dokumenti nuk hapet më.

Hapat për rikuperim:

1. Hap programin *OneDrive* dhe shkon te “View version history”.
2. Zgjedh versionin e ruajtur të djeshëm dhe klikon “Restore”.
3. Dokumenti rikthehet në gjendjen që ishte para ndërprerjes.

Ky proces quhet “Version Recovery” dhe përdoret gjerësisht në platforma si *Google Drive*, *Dropbox* dhe *Microsoft OneDrive*.

10.5 Sigurimi i disponueshmërisë së të dhënave

Siguria e të dhënave nënkupton mbrojtjen e informacionit nga qasjet e paautorizuara, dëmtimet apo ndryshimet e paqëllimshme. Masat për mbrojtje përfshijnë përdorimin e fjalëkalimeve të forta, autentifikimin me dy hapa, antivirusët, dhe enkriptimin.

Disponueshmëria do të thotë që të dhënat janë gjithmonë të aksesueshme për përdoruesin e autorizuar. Në një shkollë apo kompani, kjo nënkupton që:

- serverat janë aktivë 24/7,
- *backup*-et janë të verifikuara,
- rrjeti është i mbrojtur nga ndërprerjet.

Si ta sigurojmë disponueshmërinë:

1. Përdorim i *UPS* (pajisje kundër ndërprerjeve elektrike).
2. Përdorim i *Cloud* që ka “*redundancy*” (kopje të shumta të të dhënave në qendra të ndryshme).
3. Përdorim i “*Failover Systems*” – nëse bie një server, tjetri merr menjëherë funksionin.



Tema 11: Monitorimi dhe reagimi ndaj kërcënimeve

11.1 Kuptimi i monitorimit të sistemeve informatike

Monitorimi i sistemeve informatike është një proces i vazhdueshëm që ka për qëllim të mbikëqyrë aktivitetet dhe performancën e pajisjeve, rrjeteve dhe aplikacioneve. Ky proces ndihmon në zbulimin e hershëm të problemeve që mund të ndikojnë në sigurinë ose në funksionimin e sistemit. Përmes monitorimit, mund të sigurohen që të gjitha komponentët e sistemit po funksionojnë siç duhet dhe që nuk ka shenja të ndërhyrjeve ose sulmeve të mundshme. Në botën e teknologjisë, monitorimi përdoret për të parë nëse:

- kompjuterët dhe serverat janë aktivë,
- rrjeti i internetit po punon pa probleme,
- përdoruesit po përdorin sistemin në mënyrë të sigurt,
- nuk ka ndonjë shenjë sulmi ose hyrje të paautorizuar (*unauthorized access*).

Nëse ndodh ndonjë problem, sistemi i monitorimit dërgon një njoftim automatik (*alert*) tek administratori i IT-së, i cili mund të ndërhyjë menjëherë.

Pse është i rëndësishëm monitorimi?

Monitorimi ndihmon në:

1. Zbulimin e hershëm të problemeve: për shembull nëse një kompjuter po mbinxehet, sistemi e tregon menjëherë.
2. Ruajtjen e sigurisë: përmes monitorimit zbulojmë përpjekje për hyrje pa leje.
3. Rritjen e efikasitetit: sepse ndihmon teknikët të zgjidhin shpejt problemet.
4. Parandalimin e dëmeve të mëdha: duke reaguar përpara se problemi të përhapet.



11.2 Mjetet dhe teknikat për monitorimin e sigurisë

Për monitorimin efektiv të sistemeve informatike përdoren një sërë mjesh dhe teknikash që ndihmojnë administratorët të identifikojnë dhe analizojnë aktivitetet në rrjet. Mjetet kryesore janë:

- SIEM (*Security Information and Event Management*) – mbledh dhe analizon informacionin nga ngjarje të ndryshme (log-e) për të zbuluar kërcënime.
- IDS (*Intrusion Detection System*) – zbulon ndërhyrje në sistem.
- IPS (*Intrusion Prevention System*) – ndalon automatikisht ndërhyrjet e zbuluara.
- *Zabbix, Nagios, SolarWinds* – programe që matin temperaturën, trafikun e rrjetit, dhe performancën e serverave.

Këto mjete mbledhin të dhëna nga shumë burime (*server, router, firewall*) dhe i analizojnë për të gjetur anomali. *SIEM*, për shembull, kombinon të dhëna nga ngjarje të ndryshme të sistemit për të krijuar një pamje të plotë mbi sigurinë e rrjetit. Teknikat përfshijnë analizën e *log-eve*, zbulimin e sjelljeve jonormale dhe alarmimin automatik.

Shembull : Administratori i rrjetit instalon *Zabbix* për të monitoruar serverin e shkollës.

Pas disa ditësh, programi dërgon një njoftim: “CPU Usage 90%”.

Kjo do të thotë që serveri po punon mbi kapacitet. Administratori e pastron nga skedarët e panevojshëm dhe performanca përmirësohet menjëherë.

Tabela krahasuese e mjeteve të monitorimit

Mjeti	Qëllimi kryesor	Shembull përdorimi
<i>SIEM</i>	Analizon ngjarjet e sigurisë	Zbulon përpjekje për hyrje pa leje
<i>IDS</i>	Zbulon ndërhyrjet	Njofton kur dikush tenton të hyjë në rrjet
<i>IPS</i>	Parandalon sulmet	Bllokon automatikisht hyrjen e paautorizuar
<i>Zabbix / Nagios</i>	Monitoron performancën	Dërgon alarm kur serveri mbinxehet

11.3 Llojet e kërcënimeve dhe sinjalizimet e tyre

Kërcënimet kibernetike përbëjnë një nga sfidat më serioze të epokës digjitale. Ato shfaqen në forma të ndryshme dhe kanë ndikim të drejtpërdrejtë në pajisjet, rrjetet dhe të dhënat që përdorim çdo ditë. Në thelb, kërcënimet kibernetike janë çdo veprim ose mekanizëm me qëllim të keq që synon të dëmtojë sistemet kompjuterike, të vjedhë informacione ose të ndërpresë funksionimin normal të shërbimeve digjitale. Për shkak të evolucionit të vazhdueshëm të teknologjisë, edhe mënyrat e sulmuesve bëhen çdo vit më të sofistikuara, duke e bërë të domosdoshëm njohjen e tyre dhe të mënyrave të sinjalizimit.



Një ndër kërcënimet më të zakonshme janë viruset kompjuterike, të cilat përhapen përmes skedarëve të infektuar dhe mund të shkaktojnë dëme serioze në funksionimin e pajisjes, duke fshirë të dhëna, duke ngadalësuar sistemin ose duke krijuar hyrje të paautorizuara për sulmuesit. Sinjalizimet e një virusi mund të shfaqen në formën e mesazheve të çuditshme, programeve që hapen vetë, konsumit të lartë të memorjes ose fikjes së papritur të pajisjes.

Malware-i përfshin një gamë të gjerë programesh të dëmshme, ku përveç virusëve përfshihen edhe trojanët, *spyware* dhe *adware*. Një sistem i infektuar nga *malware* mund të ketë shenja si reklama të padëshiruara, ndryshime të paautorizuara në shfletues, instalime programesh që përdoruesi nuk i ka kërkuar dhe ruajtje të dobët të privatësisë, pasi *spyware* mund të vëzhgojë aktivitetin online.

Phishing është një kërcënim që synon mashtrimin e përdoruesit për të zbuluar fjalëkalime, të dhëna bankare apo informacione të tjera të ndjeshme. Ai zakonisht shfaqet në formë emailësh apo faqesh të rreme që imitojnë institucione të besueshme. Shenjat paralajmëruese të *phishing*-ut përfshijnë gabime drejtshkrimore në mesazhe, kërkesa urgjente për veprim të menjëhershëm, adresa emaili të dyshimta dhe lidhje që drejtojnë drejt faqeve jozyrtare.

Ransomware është një ndër sulmet më të rrezikshme, pasi ky lloj *malware*-i enkripton skedarët e përdoruesit dhe më pas kërkon pagesë për t'i rikthyer. Sinjalizimet e para shpesh shfaqen kur përdoruesi nuk mund të hapë dokumente që më parë funksiononin normalisht ose kur ekrani paraqet një mesazh kërcënues që kërkon një shumë të caktuar parash. Ky lloj sulmi paralizon plotësisht pajisjen dhe shpesh kërkon ndërhyrje profesionale.

Sulmet *DDoS* (*Distributed Denial of Service*) kanë për qëllim ndërprerjen e funksionimit të një shërbimi online duke e mbingarkuar atë me kërkesa të shumta në të njëjtën kohë. Sinjalizimet fillestare përfshijnë ngadalësim ekstrem të faqes, ndërprerje të herëpashershme të lidhjes ose pamundësi totale për t'u qasur në shërbim. Këto sulme përdoren shpesh kundër bizneseve, institucioneve apo faqeve me trafik të lartë.

Llojet kryesore të kërcënimeve		
Lloji i kërcënimit	Përshkrimi	Simptomat
<i>Virus / Malware</i>	Programe që dëmtojnë kompjuterin ose vjedhin të dhëna	Kompjuteri ngadalësohet, skedarët fshihen
<i>Phishing</i>	Email ose faqe false që kërkojnë fjalëkalime	Kërkesë për të klikuar një link “të dyshimtë”
<i>Ransomware</i>	Program që mbyll skedarët dhe kërkon pagesë	Nuk hapen dokumentet, shfaqet kërkesë për para
<i>DDoS</i>	Sulm që mbingarkon serverat	Internet shumë i ngadaltë ose ndërprerje e shërbimeve

Pavarësisht llojit të kërcënimit, një element i rëndësishëm është monitorimi i vazhdueshëm i sistemeve. Vëzhgimi i trafikut të rrjetit, krahasimi i aktivitetit të zakonshëm me atë të pazakontë dhe përdorimi i mjeteve të sigurisë ndihmojnë në identifikimin e shpejtë të sinjaleve paralajmëruese. Sa më herët të zbulohet një sulm, aq më të vogla janë pasojat dhe aq më e lehtë bëhet rikuperimi. Monitorimi jo vetëm zbulon probleme, por edhe ndihmon në ndërtimin e një mbrojtjeje më të fortë duke analizuar të dhënat historike dhe duke kuptuar modelin e sulmeve.

Shembull praktik:

Në një shkollë, disa nxënës marrin një email që thotë: “Kliko këtu për notat e fundit.”

Email-i duket zyrtar, por në fakt është një *phishing email*.

Kur klikojnë, u kërkohet të shkruajnë fjalëkalimin e tyre – kështu, sulmuesi merr akses në llogaritë e tyre.

Një sistem monitorimi mund ta zbulojë këtë si “aktivitet të pazakontë të hyrjeve”.

11.4 Reagimi ndaj incidenteve të sigurisë

Në botën digjitale të sotme, asnjë organizatë, biznes apo individ nuk është plotësisht i mbrojtur nga incidentet e sigurisë. Këto incidente mund të përfshijnë sulme kibernetike, akses të paautorizuar, rrjedhje të të dhënave, infektim nga malware, bllokim të sistemeve ose vjedhje informacioni. Për të minimizuar dëmet dhe për të rikthyer funksionimin normal të pajisjeve dhe sistemeve, përdoret një procedurë e veçantë e quajtur **reagimi ndaj incidenteve të sigurisë** (*Incident Response*). Ky proces është i organizuar në disa faza, dhe secila prej tyre ka një rol të rëndësishëm në mbrojtjen e të dhënave dhe vazhdimësinë e punës.



1. Identifikimi i incidentit

Faza e parë është zbulimi i incidentit. Qëllimi është të kuptohet se diçka e pazakontë po ndodh në sistem.

Si identifikohen incidentet?

- Përmes **monitorimit të vazhdueshëm** të sistemeve dhe rrjeteve.
- Me anë të **sinjalizimeve automatike** (alarme sigurie, antivirus, firewall).
- Përmes raportimeve nga përdoruesit që vënë re sjellje të çuditshme (ngadalësime, mesazhe të panjohura, çinstalime, etj.).
- Me analiza ditore të **log-eve të sistemeve** (raportet e aktivitetit).

Shembuj sinjalesh të incidentit:

- një kompjuter po dërgon shumë të dhëna drejt një serveri të panjohur,
- shfaqen dritare që kërkojnë pagesë (ransomware),
- aplikacionet mbyllen vetë pa arsye,
- përdoruesit nuk aksesojnë dot llogaritë e tyre.

2. Analiza e incidentit

Në këtë fazë, ekspertët analizojnë incidentin për të kuptuar:

- Shkakun e incidentit
- Nivelin e dëmtimit
- Llojin e kërcënimit
- Pajisjet e prekura
- Rrezikun për të dhënat
- Mundësinë e përhapjes

Kjo fazë i ndihmon specialistët të vendosin sa urgjent është incidenti dhe si duhet vepruar më tej.

3. Përmbajtja (*Containment*)

Qëllimi i kësaj faze është të ndalohet përhapja e incidentit.

Nëse një virus apo sulm lejohet të vazhdojë, mund të dëmtojë edhe pajisje të tjera. Për këtë arsye, ndërmerren hapa të shpejtë për izolimin e problemit.

Metodat e përmbajtjes:

- Shkëputja e pajisjes së infektuar nga interneti ose rrjeti i brendshëm.
- Ndalimi i qasjes së llogarive të komprometuara.
- Bllokimi i portave të rrjetit që po përdoren për sulm.
- Ndërprerja e aplikacioneve të infektuara.
- Izolimi i sektorëve të serverit.

Shembull praktik:

Nëse një laptop në laborator infektohet nga një virus, puna e parë është që ai të shkëputet menjëherë nga rrjeti Wi-Fi, për të mos përhapur virusin në pajisjet e tjera të shkollës.

4. Eliminimi i kërcënimit

Pasi incidenti është përmbajtur, faza tjetër është heqja plotësisht e kërcënimit nga sistemi.

Çfarë përfshin eliminimi?

- fshirja e *malware*-it,
- çinstalimi i aplikacioneve të rrezikshme,
- ndalimi i proceseve të padëshiruara,
- ndryshimi i fjalëkalimeve të kompromentuara,
- pastrimi i skedarëve të infektuar,
- përditësimi i sistemeve me "*patch*"-et e sigurisë.

Në këtë fazë, sistemi përgatitet për t'u rikthyer në funksion normal.

5. Rikuperimi

Rikuperimi është procesi i rikthimit të punës normale dhe sigurimit që sistemi është i pastër dhe i qëndrueshëm.

Hapat për rikuperim:

- rivendosja e të dhënave nga *backup*-i,
- instalimi i versioneve të pastra të programeve,

- testimi i sistemit për t'u siguruar që kërcënimi është eliminuar,
- monitorimi i përkohshëm i pajisjes për sjellje të dyshimtë.

Qëllimi:

Pajisja të kthehet si më parë, pa rrezikuar një sulm të ri.

6.Rishikimi dhe përmirësimi

Faza e fundit ka të bëjë me nxjerrjen e mësimëve nga incidenti.

Organizatrat analizojnë:

- Ku dështoi sistemi i sigurisë?
- A mund të ishte parandaluar incidenti?
- Cilat masa duhet të përmirësojmë?
- A duhet trajnim shtesë për përdoruesit?

Një raport përfundimtar përgatitet për të dokumentuar incidentin dhe për të forcuar sigurinë në të ardhmen.

Fazat kryesore të reagimit ndaj incidenteve		
Faza	Përshkrimi	Shembull praktik
1. Identifikimi	Zbulimi i incidentit përmes monitorimit	Zbulohet një hyrje e dyshimtë në rrjet
2. Analiza	Përcaktohet shkalla dhe ndikimi i dëmit	Vlerësohet sa kompjuterë janë prekur
3. Përmbajtja	Ndalohet përhapja e kërcënimit	Izolohen pajisjet e infektuara
4. Eliminimi	Hiqet kërcënimi nga sistemi	Përdoret antivirus për pastrim
5. Rikuperimi	Rikthehen funksionet normale	Rivendosen të dhënat nga <i>backup</i>
6. Rishikimi	Analizohet incidenti për të mësuar nga gabimet	Përmirësohen masat e sigurisë

Këshilla praktike për reagim të suksesshëm

1. Mos u nxitoni – veproni me radhë sipas fazave.
2. Mbani gjithmonë *backup* të përditësuar.
3. Ruani të gjitha log-et për analizë të mëvonshme.
4. Mos e fikni menjëherë sistemin — ndonjëherë të dhënat e kujtesës (*RAM data*) ndihmojnë në hetim.

11.5 Menaxhimi dhe dokumentimi i incidenteve të sigurisë

Dokumentimi i incidenteve të sigurisë është një nga hapat më të rëndësishëm në procesin e menaxhimit të tyre. Ai nuk shërben vetëm për të regjistruar atë që ka ndodhur, por është një mjet thelbësor për të nxjerrë mësim, për të parandaluar përsëritjen e problemeve dhe për të ndërtuar një kulturë të fortë sigurie brenda

organizatës. Pa dokumentim, çdo incident mbetet një ngjarje e izoluar dhe rreziku për ta përjetuar sërish është shumë i madh.

Çfarë përfshihet në dokumentim?

Sa herë që ndodh një incident, organizata duhet të përgatisë një raport të plotë. Ky raport duhet të përshkruajë të gjithë rrjedhën e ngjarjes: kur ka nisur problemi, si është zbuluar, kush e ka vënë re i pari dhe çfarë simptomash u shfaqën në sistem. Gjithashtu, raporti duhet të shpjegojë hapat që janë ndërmarrë për ta kontrolluar incidentin, për ta eliminuar dhe për të rikthyer normalitetin teknik. Në fund, dokumentimi përfshin edhe rekomandime konkrete që ndihmojnë organizatën të përmirësojë praktikën e saj të sigurisë.

Vlera e dokumentimit

Dokumentimi nuk është një detyrë që bëhet vetëm për “procedurë”. Ai ka disa funksione shumë të rëndësishme. Para së gjithash, raportet e incidenteve u japin ekipeve teknike mundësinë të analizojnë qetësisht shkakun rrënjësor të problemit. Kjo analizë ndihmon në kuptimin e dobësive që ka sistemi: një fjalëkalim i dobët, një pajisje e papërditësuar, mungesë e politikave të brendshme, apo gabime njerëzore.



Së dyti, dokumentimi është një burim mësimor për stafin.

Duke lexuar raportet e mëparshme, punonjësit kuptojnë çfarë sjelljesh duhet të shmangin, si të reagojnë në situata të dyshimta dhe cilat janë praktikën e sakta për mbrojtjen e të dhënave. Në këtë mënyrë, rritet ndërgjegjësimi dhe zvogëlohet rreziku i gabimeve të ardhshme.

Roli i bashkëpunimit në dokumentim

Një incident i sigurisë nuk ndikon vetëm departamentin e IT-së; ai prek gjithë organizatën. Prandaj edhe dokumentimi kërkon bashkëpunim mes të gjitha palëve: specialistëve të IT-së që analizojnë aspektet teknike, punonjësve që mund të kenë qenë dëshmitarë të ngjarjes, si dhe drejtuesve që marrin vendimet organizative. Nëse bashkëpunimi mungon, raporti mund të dalë i pakompletuar dhe i pasaktë.

Në shumë raste, incidentet shkaktohen nga veprime të thjeshta njerëzore, si klikimi në një lidhje të dyshimtë ose ndarja e fjalëkalimit me dikë tjetër. Në këto raste, dokumentimi e ndihmon organizatën të kuptojë ku duhet fokusuar trajnimi dhe si mund të shmangen situata të tilla në të ardhmen.

Dokumentimi si mjet për përmirësim të vazhdueshëm

Në fund, dokumentimi është një mjet i fuqishëm që ndihmon organizatën të evoluojë në fushën e sigurisë. Çdo incident, sado i vogël, është një mundësi për të mësuar. Raportet krahasohen me njëri-tjetrin, identifikohen përsëritjet dhe analizohen trendet. Kjo i lejon organizatave të ndërmarrin masa të qëndrueshme dhe afatgjata për mbrojtjen e të dhënave dhe sistemeve.

Me kalimin e kohës, raportet krijojnë një “arkiv” të rëndësishëm që tregon historinë e sfidave të sigurisë dhe mënyrën si ato janë kapërcyer. Ky arkiv është i vlefshëm për auditime, trajnime ose planifikim strategjik. Dokumentimi është një pjesë thelbësore e menaxhimit të incidenteve, sepse siguron që çdo përvojë negative të shërbejë si mësim për përmirësim.

Çfarë duhet të përmbajë një raport incidenti?

Elementi	Përshkrimi	Shembull
Data dhe ora	Kur ka ndodhur incidenti	14 mars 2025, ora 10:45
Lloji i incidentit	Çfarë ka ndodhur	<i>Phishing email</i>
Si u zbulua	Kush e raportoi / si u zbulua	Nxënësi njoftoi IT-në

Masat e marra	Çfarë veprimesh u ndërmoren	Fshihet email-i, bllokohet dërguesi
Rezultati	Çfarë ndodhi pas ndërhyrjes	Asnjë dëm i të dhënave
Rekomandime	Si të shmangët në të ardhmen	Trajnim për njohjen e <i>phishing</i> -ut

Tema 12: Siguria në aplikacionet *mobile*

12.1 Kuptimi i sigurisë në aplikacionet *mobile*



Në ditët e sotme, pajisjet *mobile* janë bërë pjesë e pandashme e jetës sonë. Përdorimi i tyre për komunikim, punë, bankë, apo arsim është shumë i përhapur. Megjithatë, për shkak të këtij përdorimi të gjerë, ato janë gjithashtu një objektiv i zakonshëm për sulmet kibernetike.

Siguria në aplikacionet *mobile* nënkupton mbrojtjen e të dhënave, programeve dhe funksioneve të pajisjes nga sulme kibernetike (*cyber attacks*) apo abuzime nga përdorues të paautorizuar.

Një aplikacion i pasigurt mund të përmbajë dobësi që lejojnë sulmuesit të marrin informacion personal, si fjalëkalime apo të dhëna bankare. Prandaj, siguria në aplikacionet *mobile* është një pjesë shumë e rëndësishme e

mbrojtjes së privatësisë dhe integritetit të përdoruesve.

Kujdes!

- Një aplikacion që ruan fjalëkalimet pa *encryption* mund të lejojë që ato të lexohen lehtë nga sulmuesit.
- Një lojë e shkarkuar nga një faqe e panjohur mund të instalojë fshehurazi *spyware* (program spiunimi) në telefon.
- Një aplikacion për modifikimin e fotove që kërkon akses te kontaktet është një shenjë paralajmëruese.

12.2 Rreziqet dhe kërcënimet kryesore në pajisjet *mobile*

Pajisjet *mobile*, si telefonat inteligjentë dhe tabletët, janë bërë mjeti kryesor për komunikim, punë dhe argëtim. Për shkak të përdorimit të gjerë dhe lidhjes së vazhdueshme me internetin, ato ekspozohen ndaj një sërë rreziqesh që mund të ndikojnë në privatësinë, sigurinë dhe funksionimin e tyre.

Disa nga këto kërcënime përfshijnë:

1. *Malware*
2. Aplikacionet e rreme
3. *Phishing*
4. Rrjete publike *Wi-Fi*
5. Humbja dhe vjedhja fizike e pajisjes
6. Vulnerabilitetet e sistemit operativ dhe aplikacioneve
7. Lejet e tepërta të aplikacioneve
8. Sulmet përmes *Bluetooth*-it

12.3 Praktikave të sigurta për përdorimin e aplikacioneve *mobile*

Siguria e pajisjeve *mobile* nuk varet vetëm nga teknologjia, por edhe nga sjellja e përdoruesve. Përdorimi i praktikave të sigurta ndihmon në mbrojtjen e të dhënave personale dhe ul rrezikun nga sulmet kibernetike. Praktikave më të rëndësishme të sigurisë janë:

1. Përdorimi i fjalëkalimeve të forta – *Strong Passwords*

Një *strong password* është fjalëkalim i fortë dhe i vështirë për t'u hamendësuar. Ai duhet të përmbajë:

- shkronja të mëdha dhe të vogla
- numra
- simbole
- të jetë të paktën 8–12 karaktere

Fjalëkalimet e thjeshta janë të rrezikshme, ndaj duhet përdorur kombinime të ndryshme.



2. Autentikimi me dy faktorë – *Two-Factor Authentication (2FA)*

Two-Factor Authentication shton një shtresë sigurie shtesë. Edhe nëse dikush e mëson fjalëkalimin, nuk mund të hyjë pa një kod të dytë:

- në *SMS*
- në *email*
- në aplikacione si *Google Authenticator* ose *Microsoft Authenticator*

2FA është thelbësor për llogaritë bankare dhe rrjetet sociale.

3. Instalimi i aplikacioneve nga burime të sigurta – *Trusted*

Aplikacionet duhet të shkarkohen vetëm nga:

- *Google Play Store*
- *Apple App Store*
- Këto platforma përmbajnë *security checks*, që kontrollojnë viruse dhe sjellje të rrezikshme.



Sources

aplikacionet për

Shkarkimi nga faqe të panjohura rrit rrezikun e *malware*.

4. Përditësimi i pajisjes – *Software Updates*

Software updates janë shumë të rëndësishme, sepse:

- mbyllin boshllëqet e sigurisë (*security vulnerabilities*)
- përmirësojnë funksionimin e pajisjes
- mbrojnë kundër kërcënimeve të reja



Pajisja dhe aplikacionet duhet të jenë gjithmonë të përditësuar.

5. Kontrolli i lejeve të aplikacioneve

Çdo aplikacion kërkon leje (*permissions*) për funksione të caktuara. Përdoruesit duhet të kontrollojnë këto leje rregullisht. Nëse lejet duken të çuditshme, aplikacioni mund të jetë i pasigurt.

6. Shmangia e rrjeteve publike *Wi-Fi*

Rrjetet publike *Wi-Fi* janë të rrezikshme sepse sulmuesit mund të marrin të dhënat që transmetohen.

Për të qenë të sigurt:

- mos fusni fjalëkalime
- mos bëni pagesa online
- përdorni internetin celular kur është e mundur

Në raste të domosdoshme mund të përdoret një *VPN* i besueshëm.

7. Aktivizimi i opsioneve të sigurisë së pajisjes

Pajisjet *mobile* kanë shumë funksione sigurie si:

- *Screen Lock* (PIN, password, fingerprint)
- *Device Encryption* (kriptim i të dhënave)
- *Find My Device / Find My iPhone* (gjetja e pajisjes në rast humbjeje)

Këto duhet të jenë gjithmonë të aktivizuara.

8. Kujdes me mesazhet dhe linket e rreme – *Phishing Messages*

Sulmet *phishing* shpesh vijnë nga numra ose email të panjohur. Ato përmbajnë:

- linke të rrezikshme
- mesazhe që kërkojnë fjalëkalime
- kërkesa për të dhëna personale

Përdoruesit duhet t'i fshijnë menjëherë.

9. Ruajtja e kopjeve rezervë – *Backup*

Backup ndihmon të ruani fotot, dokumentet dhe kontaktet në:

- *Google Drive*
- *iCloud*
- kompjuter

Në rast humbjeje ose prishjeje të pajisjes, të dhënat rikuperohen lehtësisht.

10. Shmangia e “root” dhe “jailbreak”

Rooting (Android) dhe *Jailbreaking* (iOS) heqin mbrojtjet e sigurisë së pajisjes. Kjo:

- rrit rrezikun e sulmeve
- lejon instalimin e aplikacioneve jo të sigurta
- prish garancinë

Pajisja duhet të përdoret në gjendjen e saj origjinale.

Nëse përdoruesit ndjekin këto praktika të sigurta, ata mund të mbrojnë pajisjet e tyre nga shumica e kërcënimeve, të ulin rrezikun e humbjes së të dhënave dhe të ruajnë privatësinë e tyre.

12.4 Mbrojtja e të dhënave personale dhe përditësimet e sigurisë

Pajisjet mobile janë një pjesë e rëndësishme e jetës së çdo përdoruesi dhe në to ruhen të dhëna shumë të vlefshme. Këto të dhëna përfshijnë fotografi personale, video, mesazhe, kontakte, fjalëkalime, dokumente pune, të dhëna bankare dhe informacion shëndetësor. Sa më shumë funksione të përdorim në pajisjen tonë, aq më shumë rritet nevoja për t'i mbrojtur ato nga rreziqet kibernetike.

Pse është e rëndësishme mbrojtja e të dhënave?

Çdo informacion që ruhet në telefon mund të bjerë në duar të gabuara nëse pajisja humbet, vidhet, infektohet nga viruse ose sulmohet nga hakerat. Madje edhe disa aplikacione të pasigurta mund të mbledhin të dhënat tona pa lejen tonë.

Për të shmangur këto rreziqe, përdoruesi duhet të zbatojë disa masa të vazhdueshme sigurie.

1. Përditësimet e sigurisë

2. Kopjet rezervë (Backup)

3. Lejet e aplikacioneve

Rast studimor: Një përdorues humbi telefonin e tij gjatë një udhëtimi. Pajisja nuk kishte kod sigurie dhe nuk ishte bërë asnjëherë backup. Brenda telefonit kishte:

- foto shumë personale,
- dokumente të shkollës dhe punës,
- email-e të rëndësishme,
- informacione bankare,
- fjalëkalime të ruajtura.



Personi që e gjeti telefonin mundi të hapte pajisjen menjëherë dhe të shikonte të gjitha të dhënat, duke shkaktuar humbje të konsiderueshme dhe rrezik të madh për privatësinë!

Si mund të shmangej kjo?

- Me një fjalëkalim të fortë ose bllokim biometrik.
- Me backup të aktivizuar automatikisht.
- Me funksionin *Find My Device* për të mbyllur pajisjen nga distanca.
- Me aplikacione të përditësuara që mbyllnin dobësitë.
- Me kujdes ndaj aplikacioneve të dyshimta.



Ky rast tregon sa shpejt mund të humbasë kontrolli mbi të dhënat nëse nuk merren masat e duhura.

Tema 13 : Siguria ne sistemet Cloud

13.1. Hyrje në cloud dhe bazat e sigurisë

Cloud Computing përfaqëson mënyrën moderne të ofrimit të shërbimeve kompjuterike përmes internetit. Në vend që një organizatë të blejë serverë fizikë, pajisje, hapësirë ruajtjeje ose programe, ajo mund t'i marrë këto si shërbime të gatshme nga një ofrues cloud. Burimet kompjuterike ofrohen me kërkesë (*on-demand*), duke i dhënë përdoruesit mundësinë t'i rrisë ose t'i ulë kapacitetet sipas nevojës.



Cloud-i sjell disa përfitime kryesore:

- **Shkallëzim i menjëhershëm** – sistemi mund të rritet automatikisht kur rritet trafiku.
- **Kosto më të ulëta fillestare** – nuk nevojiten investime në pajisje fizike.
- **Akses global** – shërbimet mund të jenë të disponueshme nga çdo vend.
- **Automatizim i proceseve** – përdorimi i teknologjive si auto-scaling, orchestrimi dhe CI/CD.

Kjo do të thotë se organizatat nuk kanë më nevojë të ndërtojnë infrastrukturë fizike, por rezervojnë kapacitetin e nevojshëm nga ofruesit e cloud si:

- **Amazon Web Services (AWS)**
- **Microsoft Azure**
- **Google Cloud Platform (GCP)**

Në cloud ofrohen tre modele kryesore shërbimi:

1. **IaaS – Infrastructure as a Service** (serverë virtualë, rrjete, ruajtje).
2. **PaaS – Platform as a Service** (mjedise zhvillimi, databaza të menaxhuara).
3. **SaaS – Software as a Service** (aplikacione të gatshme si e-mail, CRM, etj.).



4.

13.1.2. Modeli i përgjegjesisë (Shared Responsibility Model)

Siguria në cloud bazohet në një parim shumë të rëndësishëm: përgjegjësia ndahet mes ofruesit të cloud-it dhe klientit. Ky model quhet **Shared Responsibility Model**.

- Përgjegjësia e ofruesit (Security of the Cloud)

Ofruesi cloud garanton sigurinë e infrastrukturës bazë: qendrat e të dhënave, serverët fizikë, pajisjet e rrjetit, arkitektura e virtualizimit, furnizimi me energji, mekanizmat e aksesit fizik.

- Përgjegjësia e klientit (Security in the Cloud)

Klienti është përgjegjës për çdo gjë që konfigurim vetë: politikat e aksesit (IAM), vendosja e fjalëkalimeve, menaxhimi i çelësve API, rregullat firewall, konfigurimet e databazave, enkriptimi i të dhënave, si dhe sigurimi i vetë aplikacioneve.

Shumica e incidenteve në cloud vijnë jo nga problemi i infrastrukturës, por nga konfigurimet e gabuara të klientëve. Shembuj të zakonshëm janë: një “storage bucket” i lënë hapur publikisht, çelësa API të publikuar në GitHub, ose databaza pa fjalëkalim.

13.1.3. Parimet themelore të sigurisë

Siguria në cloud mbështetet në *Triada CIA (Confidentiality, Integrity, Availability)*

- **Konfidencialiteti** nënkupton mbrojtjen e të dhënave nga qasja e paautorizuar. Në cloud kjo realizohet me enkriptim dhe politika të sakta të aksesit.
- **Integriteti** siguron që të dhënat të mos ndryshohen në mënyrë të paautorizuar. Kjo arrihet përmes kontrolleve të verifikimit, regjistrimit dhe versionimit.
- **Disponueshmëria** siguron që sistemi dhe të dhënat të jenë të arritshme në çdo kohë, duke përdorur mekanizma si kopje rezervë, zona të shumta dhe balancim ngarkese.



13.1.4. Rreziqet dhe kërcënimet në mjediset cloud

Mjedisi cloud, njësoj si çdo sistem digjital, përballet me një sërë rreziqesh:

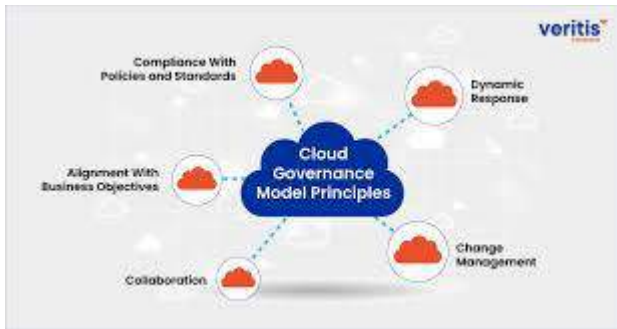
- **Konfigurime të gabuara (Misconfigurations)** – burimi më i shpeshtë i incidenteve.
- **Akses i paautorizuar** – zakonisht vjen nga fjalëkalime të dobëta ose çelësa të komprometuar.
- **API të pasigurta** – mungesa e kontrollit të saktë në endpoint-et API.

- **Sulme DDoS** – tentativa për të bllokuar shërbimin.
- **Sulme të brendshme (Insider Threat)** – persona me akses të ligjshëm që keqpërdorin privilegjet.
- **Data Breach** – ekspozim ose publikim i paqëllimshëm i të dhënave.

13.2. Menaxhimi i burimeve dhe sigurisë në cloud

Cloud Governance është sistemi i politikave, standardeve, kontrolleve dhe proceseve që udhëheq mënyrën se si një organizatë përdor shërbimet cloud.

Qëllimi është të sigurojë **siguri, përputhshmëri, menaxhim të kostos, përgjegjësi (accountability) dhe reduktim të riskut.**



Përfshin elemente si:

- **Policy Enforcement** (zbatim automatik i rregullave)
- **Tagging i burimeve**
- **Cost Governance** (buget, alerts, cost-optimization)
- **Access Governance** (kontroll mbi përdoruesit dhe privilegjet)

Tema 14: Asgjësimi i sigurt i të dhënave dhe pajisjeve

14.1. Hyrje në sigurinë e të dhënave dhe informacionit

Siguria e të dhënave dhe informacionit është procesi i mbrojtjes së informacionit nga qasja e paautorizuar, humbja ose manipulimi. Të dhënat mund të jenë të ndjeshme, si informacion personal, financiare ose dokumente strategjike, ose jo të ndjeshme, si materialet publike. Mosmarrja e masave të duhura për mbrojtjen e tyre mund të çojë në vjedhje identiteti, data leaks dhe humbje reputacioni.

Koncepte:

- **Data Security:** Praktika për të mbrojtur të dhënat nga qasja e paautorizuar, manipulimi ose humbja. **Përfshin encryption, access control, dhe firewalls.**
- **Information Security:** Fokuset në tri shtylla kryesore: Confidentiality (konfidencialiteti), Integrity (integriteti), dhe Availability (disponueshmëria) – modeli CIA.
- Klasifikimi i të dhënave (Data Classification)
 1. **Non-Sensitive Information:** Të dhëna publike, dokumente standarde, broshura, informacion në website.
 2. **Sensitive Information:** Të dhëna personale (PII), financiare, strategjike ose industriale, password, keys.
- Rreziqet kryesore:
 1. **Identity Theft** – vjedhja e të dhënave personale.
 2. **Data Leaks / Breaches** – ekspozim aksidental ose i qëllimshëm i informacionit.
 3. **Unauthorized Access** – qasje nga përdorues të paautorizuar përmes hacking, phishing ose malware.

Shembull : Një kompani humb një USB me të dhëna klientësh. Pa përdorur encryption ose secure deletion, kushdo mund të rikuperojë të dhënat duke përdorur softuer rikuperimi si Recuva ose R-Studio.

Rast Studimi: Një bankë rajonale humb një laptop që përmbante të dhëna personale të 5,000 klientëve. Laptopi nuk kishte encryption dhe fshirja e thjeshtë e skedarëve ishte bërë para largimit të pajisjes.

Pasoja:

- Një individ i paautorizuar përdori softuer rikuperimi për të marrë të dhënat e klientëve, duke shkaktuar rrezik të madh për vjedhje identiteti.
- Banka u përball me humbje reputacioni dhe detyrime ligjore për mosmarrje të masave të duhura për mbrojtjen e të dhënave (non-compliance me GDPR).

Duhet:

- Përdorimi i encryption dhe politika të rrepta për fshirjen dhe menaxhimin e pajisjeve është thelbësor për mbrojtjen e të dhënave.
- Të dhënat e ndjeshme duhet të trajtohen me kujdes maksimal dhe çdo pajisje që largohet duhet të ketë secure deletion të kryer.

14.2. Fshirja dhe asgjësimi i të dhënave

Fshirja e të dhënave nuk do të thotë gjithmonë që ato janë zhdukur. Në shumë raste, skedarët mbeten të rikuperueshëm në hard drive, SSD apo USB. Për të siguruar që informacioni nuk rikuperohet, përdoren metoda të specializuara si **data wiping** ose **secure erasure**, të cilat garantojnë që të dhënat të mos rikuperohen edhe me softuer profesional.

Koncepte:

- **File Deletion:** Fshin vetëm referencën në tabelën e skedarëve; përmbajtja mbetet në disk.
- **Data Wiping / Erasure:** Mbush sektorët me **zeros, ones** ose **random data** për asgjësim të plotë.
- **Pajisjet:** HDD, SSD, USB, cloud, printer hard drives.
- **Rreziqet:** Rikuperimi i të dhënave me softuer profesional (**Photorec, TestDisk, Recuva**).

Shembull: Në një laborator me përdorues të shumtë, fshirja e një dokumenti sekret nuk është e mjaftueshme; përdorimi i secure erase ose Blancco parandalon rikuperimin e të dhënave.

Rast Studimi: Një kompani marketingu largon USB të përdorura nga punonjësit. Para largimit, USB-të ishin thjesht fshirë me metodën standarde, pa përdorur secure deletion.

Pasoja:

- Një ish-punonjës rikuperoi skedarë me fushata marketingu dhe lista klientësh duke përdorur softuer rikuperimi.
- Këto të dhëna u përdorën në mënyrë të paautorizuar nga një kompani konkurrese, duke shkaktuar humbje të të ardhurave dhe reputacionit.

Duhet:

- Çdo pajisje që largohet duhet të kalojë në data wiping ose metodë të sigurt të fshirjes.
- Për pajisjet me SSD, metoda e thjeshtë e fshirjes nuk mjafton për shkak të wear-leveling; duhet përdorur secure erase ose softuer profesional.

14.3. Metodatat e sanitizimit të të dhënave

Sanitizimi i të dhënave është procesi i fshirjes së informacionit në mënyrë që të mos mund të rikuperohet më. Ky proces përdor metoda të standardizuara dhe të njohura ndërkombëtarisht për sigurinë e informacionit, duke mbrojtur të dhënat nga rikuperimi i paautorizuar dhe garantuar përputhshmërinë me rregulloret ligjore.

Metodat kryesore të sanitizimit:

- **Secure Erase (ATA command)** – fshirje e integruar në hard drive.

- **DoD 5220.22-M** – 3 cikle fshirjeje me të dhëna rastësore dhe verifikim.
- **Gutmann Method** – 35 cikle fshirjeje për të mbuluar çdo sektor dhe encoding të mundshëm.
- **Random Data / Write Zero Method** – mbush hapësirat me të dhëna rastësore ose zeros.
- **Standarde ndërkombëtare:** AFSSI-5020, NCSC-TG-025, HMG IS5, RCMP TSSIT OPS-II, CSEC ITSG-06.

Avantazhet: parandalon rikuperimin e të dhënave, garanton privatësinë dhe përputhshmërinë me GDPR dhe ISO 27001.

Shembull: Para riciklimit të USB-ve të përdorura nga nxënësit, përdoret **Gutmann Method** për të parandaluar rikuperimin e projektet studentore.

Rast Studimi: Një universitet ka përfunduar përdorimin e kompjuterëve laboratorikë dhe planifikon t'i japë për riciklim. Pajisjet përmbajnë të dhëna të studentëve, projekte dhe dokumente të ndjeshme. Universiteti përdori vetëm fshirjen standarde, pa sanitizim të sigurt.

Pasojat:

- Një kompani e jashtme e mori një nga kompjuterët dhe rikuperoi skedarë studentësh dhe dokumente të projekteve duke përdorur softuer rikuperimi.
- Disa nga të dhënat u shpërndanë në mënyrë të paautorizuar, duke shkaktuar shqetësime për privatësinë dhe humbje të besueshmërisë së universitetit.

Rekomandohet :

- Pajisjet që largohen nga përdorimi duhet të kalojnë në një metodë të sanitizimit të certifikuar, si DoD 5220.22-M ose Gutmann Method, në mënyrë që të dhënat të jenë të pakthyeshme.
- Përdorimi i metodave të avancuara siguron mbrojtje edhe për pajisjet me SSD, ku fshirja standarde mund të mos jetë efektive.

14.4. Të dhënat që mbeten pas fshirjes (data remanence) dhe rreziqet

Data Remanence janë informacion që nuk fshihet plotësisht nga pajisja edhe pas një fshirjeje standarde. Ky fenomen paraqet një rrezik të madh për sigurinë e informacionit, sepse të dhënat e supozuara të fshira mund të rikuperohen nga individë të paautorizuar. Ky problem shfaqet kryesisht në hard drive magnetik (HDD), solid-state drive (SSD), RAM, SRAM dhe edhe pajisje periferike si printera, kamerat ose USB. Shkaqet e të dhënave që mbeten pas fshirjes (Data Remanence):

- **RAM dhe SRAM:** Memoria tranzitore mund të mbajë informacion për disa sekonda ose minuta pas fikjes (**cold boot attack**).
- **Hard Drive / SSD:** Fshirja standarde shpesh nuk mbulon sektorët e të dhënave, veçanërisht me SSD ku vepron **wear-leveling**.
- **Copy / Cache / Swap Files:** Kopje rezervë dhe memorie cache mund të mbajnë të dhëna të ndjeshme.
- **Cloud Storage dhe Backup:** Fshirja lokale nuk garanton fshirjen nga kopjet cloud ose serverët e jashtëm.



Problemet:

- Rikuperimi i të dhënave pas fshirjes mund të përdoret për **vjedhje identiteti, industrial espionage** ose **shpërndarje të të dhënave sensitive**.
- Pajisjet e ricikluara ose të hedhura mund të jenë një rrezik i madh nëse nuk asgjësohen ose fshihen me metoda të certifikuara.

Parandalimi dhe metodat praktike:

- **Software Data Sanitization:** Përdorim i softuerëve të certifikuar si **Blancco, DBAN, Eraser** për fshirje të sigurt.
- **Degaussing:** Shkatërrim i fushës magnetike për HDD dhe tape media për të zhdukur të dhënat.
- **Shkatërrim Fizik:** Copëtim, shkrirje ose **pulverizim i hard drive-ve dhe flash memory**.

- **Cold Boot Prevention:** Fshirja e RAM pas fikjes, përdorimi i BIOS me encryption dhe teknologji si **Trusted Platform Module (TPM)**.
- **Audit Trail dhe Dokumentim:** Mbajtja e dokumentacionit të fshirjes së sigurt për përputhshmëri me standardet ligjore (ISO 27001, GDPR).
- **Procedurat e Dead Storage:** Pajisjet që nuk përdoren duhet të ruhen në ambient të sigurt përpara fshirjes ose shkatërrimit.

Standardet dhe rekomandimet:

- **NIST 800-88 Guidelines** – për trajtimin dhe fshirjen e sigurt të medieve të ruajtjes së të dhënave.
- **DoD 5220.22-M** – tre cikle mbushjeje me të dhëna rastësore dhe verifikim.
- **Gutmann Method** – 35 cikle mbushjeje për asgjësim të garantuar.

Shembull:

1. Një laborator IT përdor SSD pa kryer **secure erase** dhe përdoruesi i fundit rikuperon projektet dhe dokumentet e klasave duke përdorur softuer **Forensic Recovery Tools**.
2. Një printer multifunksional ruan kopjet e printimeve në hard drive. Pa shkatërrim të disk-ut, çdo informacion i printuar mund të rikuperohet.

14.5. Asgjësimi fizik dhe software i pajisjeve dhe të dhënave

Asgjesimi i të dhënave dhe pajisjeve është procesi i sigurimit që informacioni i ndjeshëm nuk mund të rikuperohet më, qoftë përmes softuerit, qoftë përmes shkatërrimit fizik. Kjo është një pjesë kritike e menaxhimit të sigurisë, sidomos për kompanitë që trajtojnë të dhëna personale, financiare ose dokumente strategjike. Asgjësimi i duhur ndihmon në parandalimin e vjedhjes së identitetit, **data leaks** dhe ekspozimit të informacionit të ndjeshëm.



Metodat e Asgjësimit Softuerik:

- **Software Overwrite / Data Wiping:** Mbush sektorët e ruajtjes me **zeros, ones ose random data**, duke përdorur metoda të certifikuara si **DoD 5220.22-M, Gutmann, ose NIST 800-88**.
- **Secure Erase:** Komandë e integruar në disa HDD/SSD që kryen fshirje të sigurt në nivel hardware.
- **Self Destruct / Remote Data Deletion:** Për pajisjet mobile ose cloud, të dhënat mund të fshihen automatikisht ose në distancë kur pajisja humbet.

Metodat e asgjësimit fizik:

- **Degaussing:** Përdorimi i fushës magnetike për të shkatërruar informacionin në pajisjet magnetike.
- **Crushing / Shredding / Pulverizing:** Shkatërrimi fizik i hard drive-ve, SSD, tape, CD/DVD ose USB.
- **Shkrirja / Incineration:** Metodë ekstreme për mediat që nuk mund të rikuperohen asnjëherë.

Pajisjet e riskuara:

- **Hard Drive / SSD / Flash Media:** Informacioni mbetet edhe pas fshirjes standarde.
- **Printer Hard Drives:** Printerat multifunksional mbajnë kopje të printimeve dhe skedarëve të skanuar.
- **USB, Zip, Jaz, Rev Disks:** Pajisje portative që mund të përmbajnë të dhëna të ndjeshme.

Standardet dhe Rekomandimet:

- **ISO 27001 & NIST 800-88:** Standarde për trajtimin dhe shkatërrimin e sigurt të të dhënave.
- **DoD 5220.22-M, Gutmann, AFSSI-5020, CSEC ITSG-06:** Metoda të certifikuara për sanitizim dhe fshirje të dhënash.
- **Audit Trail:** Çdo asgjësim duhet të dokumentohet për përputhshmëri ligjore dhe auditim.

Shembull

1. Para riciklimit të laptopëve, HDD-të dhe SSD-të kalojnë në **Gutmann Method** ose **ATA Secure Erase**, pastaj copëtohen për siguri maksimale.
2. Printerat multifunksional përdoren në zyra ligjore; disqet e tyre duhet të pastrohen me **software wipe** dhe më pas të shkatërrohen fizikisht.

Rast Studimi: Një bankë planifikon të riciklojë serverët e vjetër dhe USB-të që përmbajnë informacion financiar dhe personal të klientëve. Për të garantuar sigurinë, banka vendos një kombinim metodash:

1. Fshirje e të dhënave me **DoD 5220.22-M**.
2. Përdorim i **secure erase** për SSD-të.
3. Shkatërrim fizik (**shredding**) për HDD-të që nuk mund të fshihen plotësisht.
4. Dokumentim i procesit për auditim të brendshëm dhe përputhshmëri me GDPR.

Pasojat e mundshme nëse nuk merrej kjo masë:

- Rikuperimi i të dhënave nga ish-punonjës ose hakerë.
- Humbje reputacioni dhe gjoha ligjore për mosmarrje të masave të duhura për të mbrojtur të dhënat e klientëve.

Rekomandohet:

- Asgjësimi i sigurt i pajisjeve dhe të dhënave duhet të përdorë një kombinim metodash softuerike dhe fizike.
- Dokumentimi i procesit është po aq i rëndësishëm sa asgjësimi vetë, për qëllime auditimi dhe përputhshmërie ligjore.

Pyetje

1. Cilat metoda softuerike dhe fizike do të përdornit për të asgjësuar HDD, SSD dhe USB në një kompani financiare?
2. Pse është e rëndësishme të kombinohen metoda softuerike dhe fizike për asgjësimin e të dhënave?
3. Analizoni rastin e bankës dhe përshkruani se si çdo metodë kontribuon në sigurinë totale të informacionit.

Tema 15 : Etika dhe privatësia në botën digjitale

Etika e të dhënave (Data Ethics) dhe Inteligjenca Artificiale (AI Ethics) është fusha që shqyrton përdorimin e përgjegjshëm të të dhënave dhe algoritmeve për të mbrojtur individët dhe shoqërinë nga pasojat negative të teknologjisë. Ajo ndihmon organizatat dhe përdoruesit të marrin vendime **të drejta** (fair), transparente dhe të ligjshme (compliant). Kjo temë është veçanërisht e rëndësishme sot, ku AI dhe sistemet autonome po marrin vendime që mund të ndikojnë në jetën e përditshme të njerëzve, nga shëndetësia tek transporti dhe financat.



Konceptet themelore të etikës së të dhënave

1. **Integriteti i të dhënave (Data Integrity):** Të dhënat duhet të jenë të sakta, të plota dhe të verifikueshme.
 - Shembull: Në një sistem spitalor, një gabim në regjistrimin e alergjive të pacientit mund të shkaktojë pasojë serioze.
2. **Privatësia (Privacy / Data Protection):** Të dhënat personale duhet të mbahen konfidenciale dhe të përdoren vetëm për qëllimet e autorizuara.
 - Shembull: Informacioni mjekësor i pacientit nuk duhet të ndahet me palë të treta pa pëlqimin e tij.
3. **Transparenca (Transparency / Explainability):**

Përdoruesit duhet të jenë të informuar mbi mënyrën se si përdoren të dhënat e tyre dhe si funksionon AI.

Shembull: Algoritmet që rekomandojnë kredi bankare duhet të shpjegojnë arsyet për secilën vendim.

Dilemat morale (MIT Moral Machine): Algoritmet autonome shpesh përballen me **vendime morale**: zgjedhja midis dy pasojave që mund të ndikojnë në jetën e njerëzve.



15.3. Parimet e etikës së të dhënave dhe implementimi

Etika e të dhënave është një komponent kyç i përdorimit të Inteligjencës Artificiale (AI) dhe teknologjive digjitale në mënyrë përgjegjëse. Nuk është vetëm teori: ajo udhëzon organizatat dhe zhvilluesit se si të krijojnë politika të qarta, të vlerësojnë vendimet, dhe të zbatojnë rregullore ligjore që mbrojnë individët dhe shoqërinë. Në epokën e Big Data dhe Industry 4.0, vendimet e bazuara në AI mund të kenë ndikim të drejtpërdrejtë në jetë njerëzish, nga pranimi i studentëve të provimit të kredive, ose diagnoza shëndetësore automatike. Pa parime të forta etike, këto vendime mund të jenë të padrejta, diskriminuese, ose jo të ligjshme.

Parimet e Etikës së të Dhënave

1. Guiding Principles (Parimet udhëzuese)

- **Transparenca (Transparency/Explainability):** Përdoruesit dhe vendimmarrësit duhet të kuptojnë si funksionon sistemi AI dhe çfarë të dhënash përdoren.
- **Llogaridhënia (Accountability):** Zhvilluesit dhe organizatat mbajnë përgjegjësi për vendimet e algoritmeve.
- **Drejtësia (Fairness):** Algoritmet nuk duhet të favorizojnë individë ose grupe bazuar në race, gjini, apo status ekonomik.
- **Integriteti (Integrity):** Të dhënat dhe proceset duhet të jenë të sakta, të plotë dhe të besueshme.



2. Qualitative Principles (Parimet cilësore)

- **Privatësia (Privacy / Data Protection):** Mbajtja e të dhënave personale në mënyrë konfidenciale.
- **Respekti ndaj individit (Respect for Individuals):** Sigurimi që vendimet nuk dëmtojnë apo diskriminojnë individët.
- **Beneficial Use:** Teknologjia duhet të përdoret për të mirën e shoqërisë, jo për manipulim ose dëmtim.

3. Governing Principles (Parimet rregullatore / standardet)

- **Përputhshmëria me ligjet:** GDPR, ISO 27001, HIPAA për të dhëna shëndetësore.
- **Standardet profesionale:** IEEE Ethically Aligned Design, OECD AI Principles.
- **Auditimi dhe kontrolli i rregullt:** Organizatat duhet të verifikojnë përdorimin etik të të dhënave dhe AI.

Evaluimi i vendimeve etike

1. Checklist Approach (Lista kontrolli)

- Pyet: “A është ky vendim transparent?”
- “A respektohet privatësia e të dhënave?”
- “A ka pasojë negative për individët?”

2. Consequence Scanning (Analiza e pasojave):

Analizon pasojat e mundshme për individët dhe shoqërinë.

Shembull: Një sistem AI që rekomandon kredi mund të refuzojë grupe të caktuara në mënyrë të padrejtë; analiza e pasojave parashikon këtë problem.

3. **Framework Approach (Kwadri etik):** Krijon një sistem të strukturuar për vendimet etike.

- Përfshin **polici të brendshme, audite të jashtme**, dhe rregullime të algoritmeve për të shmangur diskriminimin.

Raste Studimi:

1. **Kredia financiare dhe AI**

- Një kompani AI përdor model predictive për aprovim kredie.
- Pa framework etik, modeli mund të refuzojë individë nga rajone të caktuara ose nga grupe socio-ekonomike të ulëta.

Me një **Data Ethics Framework**, kompania vlerëson:

- Rrezikun e diskriminimit (bias detection)
- Pasojat ligjore (GDPR compliance)
- Transparencën e vendimeve (explainable AI)

2. **Pranimi në universitet**

- Algoritmi favorshon kandidatët nga rajonet më të pasura.
- Zbatimi i një framework etik lejon:
 - Rregullimin e peshave të algoritmit për të siguruar barazi (fairness adjustment)
 - Auditimin periodik të rezultateve
 - Përfshirjen e njerëzve në vendimmarrje (human-in-the-loop)

3. **Sistemet shëndetësore**

- Sisteme AI për diagnostikim.
- Etika kërkon që të dhënat të anonimizohen, vendimet të jenë të shpjegueshme dhe përdorimi të jetë për qëllime të autorizuara.

Rreziqet reale pa etikë të të dhënave

- **Diskriminimi dhe bias algoritmik:** preferenca për disa grupe dhe penalizim të tjerëve.
- **Shkelja e privatësisë:** përdorimi i të dhënave personale pa pëlqim.
- **Humbja e besimit (Loss of Trust):** përdoruesit humbin besimin në sistemet teknologjike.
- **Pasojat ligjore dhe financiare:** gjopa, humbje reputacioni.

Rast Studimi: Një kompani marketingu përdor AI për targetim reklamash. Të dhënat përfshijnë: moshën, gjininë, vendin e banimit, dhe sjelljen online.

Problematika etike:

- Algoritmi mund të diskriminojë grupe të veçanta.
- Përdoruesit nuk janë informuar se po analizohen të dhënat e tyre.

Zgjidhja etike:

1. Anonimizimi i të dhënave (Data Anonymization)
2. Transparenca: njoftim për përdoruesit se si përdoren të dhënat
3. Framework etik: auditim i rregullt i algoritmit, kontroll për bias, dokumentim i vendimeve

Pyetje

1. Përshkruani tre parime kryesore të etikës së të dhënave dhe japini shembuj nga jeta reale.
2. Analizoni rastin e universitetit: Si mund të rregullohet algoritmi për të respektuar barazinë?
3. Për një kompani marketingu që përdor AI, krijoni një **mini-Data Ethics Framework** që siguron përdorim të drejtë dhe transparent të të dhënave.
4. Identifikoni tre rreziqe kryesore kur vendimet e AI përdoren pa kuadër etik.

Tema 16 : Edukimi i përdoruesve dhe rritja e ndërgjegjësimit për sigurinë

Fjalëkalimet janë **linja e parë mbrojtëse** për çdo sistem, platformë apo llogari online. Rritja e ndërgjegjësimit për përdorimin e fjalëkalimeve të forta ndihmon përdoruesit të:

- Mbrojnë të dhënat personale dhe profesionale.
- Parandalojnë aksesin e paautorizuar.
- Reduktojnë rrezikun e **hacking**, phishing dhe **credential stuffing**.

Karakteristikat e një fjalëkalimi të forte:

- **Gjatësia:** Minimum 12–16 karaktere.
- **Kompleksiteti:** Përbëhet nga shkronja të mëdha, të vogla, numra dhe simbole.
- **Randomi:** Nuk duhet të përdoret asnjë informacion personal (datëlindje, emër, username).
- **Unikaliteti:** Çdo llogari duhet të ketë fjalëkalim unik.

Shembull:

1. Dobët: 123456 / password
2. Mesatar: Summer2024
3. I fortë: V7#!p2Lx9Q@

Menaxhimi i fjalëkalimeve

- **Password managers:** Ruajnë dhe krijojnë fjalëkalime të forta për secilën llogari.
- **Two-Factor Authentication (2FA):** Shton një hap të dytë sigurie (OTP, app authenticator).
- **Rivendosja periodike:** Ndryshimi i fjalëkalimeve sipas politikës së kompanisë ose pas incidentesh.

Shembuj të dobishëm: 1Password, LastPass, Bitwarden – krijojnë dhe ruajnë fjalëkalime komplekse pa humbur kontrollin.

Rreziqet kryesore

- **Phishing:** Email ose mesazhe mashtruese që kërkojnë fjalëkalimet tuaja.
- **Credential stuffing:** Përdorimi i fjalëkalimeve të vjedhura për të hyrë në llogari të tjera.
- **Keylogging:** Malware që regjistron çdo tast të përdoruesit.

Shembull:

1. Një përdorues përdor password123 në Gmail dhe LinkedIn. Hacker merr fjalëkalimin nga një databazë të vjedhur dhe hyn në të dy llogaritë.
2. Një kompani implementon 2FA dhe password manager për të gjithë punonjësit. Numri i incidenteve të sigurisë u reduktua me 80%.
3. **Password spraying attack:** hacker përpiqet fjalëkalime të njohura në shumë llogari. Vetëm përdoruesit me fjalëkalime të forta mbijetojnë.

Rast studimi: Një departament IT në një kompani humb qasje në sistemin e saj për shkak të fjalëkalimeve të dobëta të punonjësve. Pas incidentit:

- Të gjithë punonjësit u trajnuan për **Password Hygiene**.
- U vendos **password manager** i përbashkët.
- Aktivizimi i detyrueshëm i 2FA për email dhe aplikacione kritike.

Rezultati: Nuk pati më incidente për një vit, dhe përdoruesit u bënë më të ndërgjegjshëm për sigurinë.

Pyetje / ushtrime

1. Identifikoni tre fjalëkalime të dobëta dhe sugjeroni versionin e sigurt.
2. Aktivizoni 2FA në një platformë të sigurt (p.sh., Gmail) dhe dokumentoni hapat.
3. Diskutoni avantazhet dhe kufizimet e password managers.
4. Analizoni një rast phishing dhe përshkruani se si mund të shmanget.

16.2. Social engineering dhe siguria fizike

Ky leksion do të mësojë përdoruesit të identifikojnë teknikat mashtruese, të mbrojnë veten dhe organizatën, dhe të përdorin praktika të sigurta fizike. Shumica e sulmeve kibernetike nuk ndodhin përmes softuerit, por përmes manipulimit të njerëzve dhe shkeljeve të sigurisë fizike.



1. **Social Engineering:** Sulmuesi përdor psikologjinë për të marrë informacion të ndjeshëm ose qasje në sisteme.

Koncepte

- **Phishing:** Email ose mesazh mashtrues që duket autentik dhe kërkon të dhëna personale (login/password, numra kartash).
- **Spear Phishing:** Phishing i targetuar për individë specifikë.
- **Vishing:** Telefonatë mashtruese për të marrë informacion.
- **Smishing:** SMS mashtruese që kërkon të dhëna ose instalimin e aplikacioneve të rreme.
- **Pretexting:** Krijimi i një situatë të rreme për të marrë informacion të besueshëm.

Kini parasysh:

- ✓ Social engineers shfrytëzojnë **besimin, urgjencën dhe frikën**.
 - ✓ Përqendrohen tek **punonjësit**, jo tek sistemi teknik.
2. **Siguria fizike:** Garantimi që vetëm personat e autorizuar kanë qasje në pajisje, dhoma sensitive dhe rrjete.
 - **Qasje e autorizuar:** Vetëm punonjësit me kredenciale të vlefshme duhet të hyjnë në zona sensitive.
 - **Kontrolli i pajisjeve:** Monitorimi dhe ruajtja e laptopëve, USB-ve, kartave identifikimi.
 - **Mbrojtja e dhomave dhe serverëve:** Përdorimi i kodeve, kartave magnetike, kamerave.
 - **Politikat e vizitorëve:** Mbikëqyrja e të huajve dhe regjistrimi i tyre.

Shembull teknologjik:

1. **Badge access system + CCTV monitoring** në server room.
2. **Alarm system** në rast hyrjeje të paautorizuar.

Shembuj praktikë

1. **Email phishing:** Një punonjës merr email që duket si nga departamenti IT: “Kliko këtë link për të përditësuar fjalëkalimin”. Nëse hap linkun, malware instalohet.
2. **Tailgating:** Një person i paautorizuar hyn në zyrë duke u ngjitur pas një punonjësi që nuk kontrollon kartën e hyrjes.
3. **Pretexting real:** Sulmuesi fton një punonjës të japë të dhëna për llogaritë e klientëve duke pretenduar se është auditor i jashtëm.

Kini parasysh: Nëse ka dyshime mbi kërkesat për informacion, verifikoni gjithmonë **burimin** përpara se të reagoni.

Rast studimi: Një kompani e marketingut pëson një incident kur një punonjës hap një email phishing që pretendonte të vinte nga CEO-ja (“Urgjent: dërgo informacionin e klientëve”). Sulmuesi merr qasje në të dhënat sensitive dhe dërgon ransomware.

Zgjidhja:

1. Trajnime të rregullta mbi phishing awareness.
2. Teste të rregullta të social engineering (simulime phishing).

3. Vendosja e një policy që kërkon verifikim të të gjitha kërkesave për informacion sensitive, sidomos nga email ose telefon.
4. Siguria fizike: kufizimi i qasjes në server dhe dhoma sensitive.

Rezultati: Përdoruesit bëhen më të ndërgjegjshëm, numri i incidenteve zvogëlohet.

Pyetje / Diskutim

1. Identifikoni tre teknika të social engineering që mund të përdoren kundër punonjësve.
2. Diskutoni se si mund të parandalohet tailgating në një kompani.
3. Simuloni një situatë phishing dhe shkruani një plan reagimi për punonjësit.
4. Listoni masat që mund të merren për mbrojtjen fizike të pajisjeve dhe dhomave sensitive.

16.3. Rrjetet e sigurta (safe networks) & softueri i dëmshëm (malicious software)

Rrjetet e pasigurta janë një nga burimet kryesore të sulmeve kibernetike. Përdoruesit, pajisjet dhe aplikacionet lidhen çdo ditë me internetin, duke i ekspozuar organizatat ndaj rreziqeve.

Për më tepër, pajisjet mund të infektohen me **malware**, i cili shpesh përhapet përmes rrjeteve të dobëta, linkeve të dyshimta ose pajisjeve të jashtme.

Në këtë leksion, përdoruesit do të mësojnë:

- Rreziqet e Wi-Fi publik dhe mënyrat për t'u mbrojtur
- Format kryesore të malware dhe si infektohen pajisjet
- Praktikimet më të mira për të shmangur infeksionet dhe komprometimet e rrjetit

Dallimi i rrjeteve të sigurta dhe të pasigurta

A. Rrjetet e Sigurta (Safe Networks)

Një rrjet i sigurt përdor:

- **Enkriptim të fortë** (WPA3/WPA2)
- **Kontroll të qasjes** (password i fortë, filtrat e pajisjeve, segmentim)
- **Firewall aktiv**
- **Monitoring të trafikut**

Shembull: Router modern me WPA3 + firewall + filtrime MAC + Network Segmentation për zyrat.

2. Rreziqet e Wi-Fi Publik

Wi-Fi publik shpesh është **i paenkriptuar**, duke lejuar sulmuesit:

- **Eavesdropping** – interceptim i trafikut
- **Man-in-the-Middle (MITM)** – manipulim i komunikimit
- **Fake Hotspots / Evil Twin** – rrjet i krijuar nga sulmuesi
- **Session Hijacking** – marrja e sesionit të loguar

Shembull real: Sulmuesi krijon një rrjet me emrin *“FREE AIRPORT WIFI”*. Përdoruesit lidhen dhe të gjitha kërkesat kalojnë përmes sulmuesit.

Mbrojtja në rrjete publike:

- Mos bëni login në *banking, email, platforma pune*.
- Përdorni VPN për të enkriptuar trafikun.
- Shmangni *file sharing* dhe *auto sync*.
- Fikni Bluetooth e Hotspot kur nuk i përdorni.
- Kontrolloni emrin e rrjetit me stafin e vendit

Rrjetet e brendshme të kompanisë (Enterprise Networks)

Këto duhet të përfshijnë:

- **Segmentation** (p.sh. punonjësit ndahen nga serverat kritikë)
- **Zero Trust Network Access (ZTNA)**
- **Policy për pajisjet BYOD**
- **Scans të rregullta të rrjetit**
- **IDS/IPS** (Intrusion Detection / Prevention Systems)

Edhe një klikim gabim (phishing) mund të komprometojë të gjithë rrjetin e organizatës.

Softueri i Dëmshëm (Malicious Software – Malware)

Malware është çdo program që dëmton pajisjen, vjedh të dhëna ose komprometon rrjetin.

2. Llojet kryesore të Malware

- **Virus:** Hyn në file dhe përhapet përmes dokumenteve të infektuara.
- **Worm:** Përhapet automatikisht në rrjet pa ndërhyrje njerëzore.
- **Trojan:** MASKOHET si program normal (p.sh. “PDF Converter Free”).
- **Ransomware:** Enkripton të dhënat dhe kërkon pagesë për t’i rikthyer.
- **Spyware:** Mbledh informacion pa dijeninë e përdoruesit.
- **Adware:** Shfaq reklama të padëshiruara dhe gjurmon aktivitetin.
- **Rootkit:** Fsheh aktivitetin e sulmuesit, duke fshehur procese e file.
- **Keylogger:** Regjistron çdo tast që shtyp përdoruesi.

Si infektohen pajisjet?

- ✓ Klikime në linke të rreme
- ✓ Shkarkim programesh të piratuar
- ✓ Hapja e file-ve .EXE / .ZIP të paautorizuara
- ✓ USB e infektuara
- ✓ Fake updates
- ✓ Email phishing

Shkalla e dëmshmërisë

- **Low-risk:** Adware
- **Medium-risk:** Spyware, Trojans
- **High-risk:** Ransomware, Rootkits

Disa mwnyra mbrojtje:

- ✓ Përdorni **Antivirus profesional** dhe “Real-Time Protection”
- ✓ Përditësoni sistemin rregullisht
- ✓ Mos instaloni programe të panjohur
- ✓ Përdorni **password të fortë + MFA**
- ✓ Mos vendosni USB të çuditshme
- ✓ Kontrolloni linkun para se të klikoni
- Mos hapni file të dyshimta

Rregulli i artë: Nëse diçka duket shumë e mirë për të qenë e vërtetë — mbase është mashtrim.

Shembulli 1: Evil Twin Attack

Një punonjës lidhet me rrjetin “COFFEESHOP_FREE_WIFI”, i krijuar nga sulmuesi. Të gjitha të dhënat e tij kalojnë përmes sulmuesit - email, password, faqet që viziton.

Shembulli 2: Ransomware via Email

Punonjësi hap një file ZIP që pretendon se është “fatura mujore”. Kompjuteri enkriptohet dhe shfaqet mesazhi:

"Pay 300\$ in Bitcoin to recover your files."

Shembulli 3: USB Drop Attack

Sulmuesi lë një USB në parkim me titull “Pagezë Djegie”. Përdoruesi kur e hap, instalohet Trojan dhe sulmuesi merr kontrollin e kompjuterit.

4. RAST STUDIMOR : Sulmi WannaCry (2017)

- Infektoi mbi 300,000 pajisje globalisht
- Shfrytëzoi një dobësi të Windows
- Përhapej automatikisht në rrjet
- Enkriptoi të gjitha file-t
- Ndajti punën e spitaleve në Mbretërinë e Bashkuar për ditë të tëra

Çfarë mësuam?

- Përditësimet e sigurisë janë jetike
- Ransomware është një nga sulmet më shkatërruese
- Rrjetet me konfigurime të dobëta janë lehtë të komprometueshme
- Përdoruesit duhet të trajtohen rregullisht

PYETJE

1. Cilat janë tre rreziqet kryesore të përdorimit të Wi-Fi publik?
2. Përshkruani dy mënyra se si mund të infektohet pajisja me malware.
3. Si funksionon një sulm Man-in-the-Middle?
4. Cilat janë masat që duhet të marrë një përdorues kundër ransomware?
5. Analizoni këtë situatë:
Ju jeni në një kafene dhe shfaqet një rrjet me emrin “Free_WiFi_Office”.

- A lidheni?
- Çfarë duhet të kontrolloni?
- Çfarë rrezikoni?

Shembulli 1: USB i braktisur

Një punonjës gjen USB të braktisur me dokumente sensitive. Nëse lidhet me kompjuterin e kompanisë, malware mund të përhapet ose informacioni të vidhet.

Zgjidhja: Fshini ose enkriptoni të dhënat përpara përdorimit.

Shembulli 2: Fshirja e dokumenteve të vjetra

Punonjësi fshin dokumente Excel dhe Word nga desktop-i pa përdorur “fshirje të sigurt”. File-et mund të rikuperohen nga sulmuesit.

Zgjidhja: Përdor software të fshirjes së sigurt ose enkripto file para fshirjes.

Shembulli 3: Backup të papërdorura

Backup i vjetruar ruhet pa kontroll në një server publik. Sulmuesi mund ta përdorë për të marrë të dhënat e vjetra.

Zgjidhja: Implemento data lifecycle management – skadimi dhe fshirja e backups sipas planit.

RAST STUDIMOR: Shkelje e të dhënave në një kompani shëndetësore

- Një kompani nuk fshiu të dhënat e pacientëve nga serverë të vjetër.
- Serverët u shitën për riciklim pa fshirje të sigurt.
- Të dhënat personale u bënë publike dhe pati humbje reputacioni + gjoba ligjore.

Mësime të nxjerra:

1. Politikat e qarta për asgjësimin e të dhënave janë kritike.
2. Edukimi i përdoruesve dhe stafit IT është vendimtar.
3. Shkatërrimi fizik + fshirja e sigurt = mbrojtje optimale.

PYETJE

1. Përshkruani tre mënyra për të shkatërruar të dhënat fizike (HDD, USB, CD).
2. Analizoni një situatë ku një dokument sensitive u fshi gabimisht, si mund të shmangët rikuperimi i tij?
3. Diskutoni avantazhet e backup-it të koduar.
4. Përse është e rëndësishme të edukosh përdoruesit mbi fshirjen e sigurt të të dhënave?
5. Hartoni një mini-policy të brendshme për **asgjësimin e të dhënave** për departamentin tuaj.