E ardhmja e Sigurisë Kibernetike: Çfarë po ndodh në epokën e Inteligjencës Artificiale?

Përmbajtja

Hyrje në Siguri Kibernetike

I. Çfarë është Siguria Kibernetike?

Siguria kibernetike është praktika e mbrojtjes së sistemeve kompjuterike, rrjeteve, pajisjeve dhe të dhënave nga kërcënimet kibernetike. Kjo përfshin përdorimin e teknologjive, proçeseve dhe kontrolleve për të parandaluar, zbuluar dhe adresuar sulmet dhe shkeljet e sigurisë.

II. Siguria kibernetike mbulon një gamë të gjerë fushash dhe përfshin elemente si:

1. *Konfidencialiteti*: Sigurimi që të dhënat janë të aksesueshme vetëm nga ata që kanë autorizim.
2. *Integriteti:* Garantimi që informacioni nuk ndryshohet në mënyrë të paautorizuar ose të papritur.
3. *Disponueshmëria:* Të dhënat dhe sistemet janë të qasshme për përdoruesit e autorizuar kur janë të nevojshme.

Hyrje në Siguri Kibernetike

III. **Pse është e Rëndësishme Siguria Kibernetike?**

- ***Mbrojtja e Informacionit Personal*:** Në një epokë ku të dhënat personale ruhen online, siguria është thelbësore për të parandaluar vjedhjet e identitetit.
- ***Siguria Kombëtare*:** Infrastrukturat kritike dhe të rëndësishme varen nga teknologjia dhe janë objektiva të mundshme për sulmet.
- ***Besimi në Teknologji*:** Bizneset dhe përdoruesit duhet të ndihen të sigurt në përdorimin e teknologjive.

IV. **Hapat e Parë për Mbrojtje Kibernetike**

- ***Përdorimi i Fjalëkalimeve të Forta*:** Fjalëkalime komplekse dhe unike për secilën llogari.
- ***Përdorimi i Antiviruseve*:** Instalimi dhe përditësimi i rregullt i programeve mbrojtëse.
- ***Përditësimet e Rregullta (Update)*:** Sistemet operative dhe aplikacionet duhet të përditësohen për të adresuar dobësitë.
- ***Ndërgjegjësimi*:** Edukimi i përdoruesve për kërcënimet kibernetike dhe mënyrat e mbrojtjes.

Hyrje në Siguri Kibernetike

Sulmet Kibernetike më të zakonshme

Phishing (Sulmet Mashtruese)

1. Sulmuesi paraqitet si një entitet i besuar për të marrë informacione sensitive, si fjalëkalime ose të dhëna bankare.
2. Shembull: E-maile false që duken sikur vijnë nga banka ose shërbime online.

Ransomware

1. Një lloj malware që enkripton të dhënat dhe kërkon pagesë për t'i rikthyer ato.
2. Shembull: Sulmet WannaCry dhe LockBit.

Malware (Programe Dashakeqe)

1. Programe ose kode që dëmtojnë pajisjet, vjedhin të dhëna, ose ndërpresin funksionet e sistemeve.
2. Llojet e Malware: Viruset, trojanët, spyware, dhe adware.

SQL Injection

1. Shfrytëzimi i dobësive në aplikacione për të manipuluar bazat e të dhënave duke injektuar kode dashakeqe.
2. Shembull: Marrja e të dhënave personale nga një uebsajt i pasigurt.

Denial of Service (DoS) dhe Distributed DoS (DDoS)

1. Sulme që mbingarkojnë një server ose rrjet me trafik për ta bërë të paaksesueshëm.
2. Shembull: Sulmet ndaj uebsajteve të mëdha si shërbimet bankare.

Man-in-the-Middle (MITM)

1. Sulmuesi futet mes komunikimit të dy palëve dhe intercepton ose modifikon informacionin.
2. Shembull: Përgjimi i trafikut në rrjete publike Wi-Fi.

Social Engineering

1. Manipulimi i njerëzve për të marrë informacione ose akses pa përdorur teknologji.
2. Shembull: Marrja e kredencialeve përmes bisedave të gënjeshtërta telefonike.

Hyrje në Siguri Kibernetike

IT Security Management Framework

Një strukturë udhëzuese që ndihmon organizatat të implementojnë dhe të menaxhojnë masat e sigurisë kibernetike. Kjo përfshin praktikat dhe standardet më të mira për mbrojtjen e të dhënave dhe sistemeve.

- *Shembuj:* ISO/IEC 27001, NIST Cybersecurity Framework, COBIT.
- *Qëllimi:* Sigurimi i një qasjeje të strukturuar për të identifikuar, menaxhuar dhe minimizuar rreziqet.

Governance – Policies and Compliance

Governance i referohet udhëheqjes strategjike që siguron se aktivitetet e sigurisë kibernetike janë në përputhje me objektivat e organizatës dhe rregulloret ligjore.

- ***Policies (Politikat):*** Rregulla dhe procedura të cilat përcaktojnë se si trajtohen të dhënat dhe sistemet.
  - Shembull: Politikat e përdorimit të pranueshëm (Acceptable Use Policies - AUP).
- ***Compliance (Përputhshmëria)****:* Përshtatja me ligjet dhe rregulloret e sigurisë, si GDPR, PII, HIPAA, PCI DSS.
  - Shembull: Ruajtja dhe mbrojtja e të dhënave personale sipas GDPR.

Cybersecurity Ethics

Etika e sigurisë kibernetike përfshin standardet morale dhe profesionale që duhet të ndjekin profesionistët e sigurisë në punën e tyre.

- *Parimet Etike:*
  - Respektimi i privatësisë së individëve.
  - Përdorimi i njohurive për të ndihmuar dhe mbrojtur, jo për të dëmtuar.
  - Zbulimi përgjegjës i dobësive të sigurisë (Responsible Disclosure).
- *Rëndësia:* Ndihmon në ndërtimin e besimit dhe parandalimin e abuzimeve.

Hyrje në Siguri Kibernetike

States of Data (Guarding against Data Breaches)

Të dhënat ndodhen në tre gjendje kryesore, dhe çdo gjendje kërkon masa të veçanta sigurie:

1. *Data at Rest (Të dhëna në gjendje statike)*: Të dhënat që janë të ruajtura në serverë, ose arkiva.
    - Masat e Sigurisë: Enkriptimi i të dhënave, kontrolli i aksesit, dhe rezervimi i sigurt.
2. *Data in Transit (Të dhëna në tranzit)*: Të dhënat që transferohen midis sistemeve ose rrjeteve.
    - Masat e Sigurisë: Përdorimi i protokolleve të sigurta si TLS/SSL dhe VPN.
3. *Data in Use (Të dhëna në përdorim):* Të dhënat që janë duke u përpunuar nga aplikacionet ose përdoruesit.
    - Masat e Sigurisë: Monitorimi i aplikacioneve dhe përdorimi i memorieve të siguruara.

Countermeasures

Kundërmasat janë teknika ose teknologji që përdoren për të parandaluar, zbuluar, dhe për t'iu përgjigjur kërcënimeve.

- *Shembuj:*
    - Firewall dhe IDS/IPS për mbrojtje nga sulmet në rrjet.
    - Antivirus dhe Anti-malware për parandalimin e programeve dashakeqe.
    - Multi-factor Authentication (MFA) për të siguruar qasje të autorizuar.

Defense In-depth (Mbrojtja në Thellësi)

Defense in-depth është një qasje shumë-shtresore për sigurinë kibernetike, ku përdoren masa të ndryshme sigurie për të mbrojtur të dhënat dhe sistemet në nivele të ndryshme.

- *Shembuj të Shtresave të Mbrojtjes:*
    a. Shtresa Fizike: Mbrojtja e qendrave të të dhënave dhe pajisjeve.
    b. Shtresa e Rrjetit: Përdorimi i firewall, IDS/IPS, dhe VLAN-ve.
    c. Shtresa e Aplikacioneve: Parandalimi i sulmeve si SQL Injection dhe Cross-Site Scripting.
- Avantazhi: Nëse një shtresë kalohet, shtresat e tjera vazhdojnë të sigurojnë mbrojtje.

Hyrje në Siguri Kibernetike

Cybersecurity Operations Management

Ky proces përfshin menaxhimin e operacioneve të sigurisë për të zbuluar dhe adresuar kërcënimet në kohë reale.

- *Aktivitetet Kryesore:*
  - Monitorimi i vazhdueshëm i rrjeteve dhe sistemeve.
  - Incident Response (Përgjigjja ndaj incidenteve).
  - Vlerësimi dhe menaxhimi i dobësive (Vulnerability Management).
- *Mjetet dhe Teknologjitë:* SIEM, SOAR, dhe monitorimi i log-eve.

Asetet e Sigurisë

Security devices janë teknologjitë dhe pajisjet që përdoren për të mbrojtur rrjetet dhe të dhënat kundër kërcënimeve.

- *Shembuj të Pajisjeve dhe Infrastrukturës:*
  - Firewall: Mbron rrjetin nga trafik i paautorizuar.
  - IDS/IPS: Zbulon dhe ndalon aktivitetet e dyshimta.
  - VPN: Siguron një lidhje të enkriptuar për komunikim të sigurt.
  - Antivirus dhe Anti-malware: Parandalon dhe eliminon programet dashakeqe.
  - SIEM (Security Information and Event Management): Monitoron dhe analizon aktivitetet në kohë reale për të zbuluar kërcënimet.
- *Qëllimi:* Këto mjete formojnë një shtresë mbrojtjeje që siguron siguri proaktive dhe reaktive ndaj kërcënimeve.

Hyrje në Inteligjencë Artificiale

Çfarë është Inteligjenca Artificiale?

AI është një fushë e shkencës kompjuterike që synon të krijojë sisteme që mund të imitojnë sjelljen dhe inteligjencën njerëzore.

Hyrje në Inteligjencën Artificiale

Si Është e Krijuar AI (përbërja e saj)?

Të Dhënat (Data):
Baza e AI-së: AI mbështetet në Big Data për të mësuar dhe për të marrë vendime.
Shembull: Algoritmet përdorin të dhëna nga burime të ndryshme si teksti, imazhet, videot, ose të dhëna sensorësh.

Algoritmet dhe Modelet Matematikore:
Algoritmet janë grup udhëzimesh që AI ndjek për të analizuar dhe përpunuar të dhëna.
Modelet matematikore përdoren për të identifikuar modele dhe për të parashikuar rezultate.

Mësimi i Makinerive (Machine Learning - ML):
Procesi i të Mësuarit: Algoritmet e mësimit të makinerive përdorin të dhënat për të mësuar rregulla ose modele pa u programua r drejtpërdrejt.
Shembuj: Regresioni, klasifikimi, dhe grupimi (clustering).

Mësimi i Thellë (Deep Learning - DL):
Neural Networks: Modelet e mësimit të thellë përdorin rrjete neurale artificiale që imitojnë funksionin e trurit të njeriut.
Aplikime: Njohja e fytyrës, përpunimi i gjuhës natyrore (NLP), dhe drejtimi autonom.

Infrastruktura Kompjuterike:
Hardware i Fuqishëm: Sistemet AI kërkojnë hardware të fuqishëm, si procesorët grafikë (GPU) dhe TPU-të, për të trajtuar sasitë e mëdha të të dhënave.
Cloud Computing: Shërbimet cloud si Google Cloud, AWS, dhe Azure ofrojnë burime për zhvillimin e AI-së.

Trajnimi i Modeleve:
Trajnimi: Algoritmet trajnohen me të dhëna për të mësuar modele dhe për të përmirësuar saktësinë.
Validimi: Modelet testohen me të dhëna të reja për të siguruar se janë të sakta dhe të dobishme.

Hyrje në Inteligjencë Artificiale

Si Funksionon AI?

1. **P**ërpunimi i të Dhënave:
AI fillon duke marrë të dhënat e papërpunuara dhe duke i organizuar në formate të përdorshme.
Shembull: Një sistem AI mund të analizojë të dhënat nga miliona transaksione financiare për të zbuluar mashtrime.

2. Analiza dhe Nxjerrja e Modeleve:
AI përdor algoritme për të analizuar të dhënat dhe për të gjetur modele.
Shembull: Një sistem që parashikon motin analizues modelet e të dhënave historike.

3. Vendimmarrja:
Pasi AI përpunon të dhënat, ajo merr vendime bazuar në analizën e saj.
Shembull: Një algoritëm që përcakton nëse një email është spam ose jo.

4. Mësimi i Vazhdueshëm (Continuous Learning):
AI vazhdon të mësojë nga të dhënat e reja për t'u përmirësuar.
Shembull: Një sistem AI në një automjet autonom mëson nga të dhënat e rrugës dhe përmirëson aftësinë e drejtimit.

5. Ndërveprimi me Njerëzit:
AI mund të ndërveprojë me përdoruesit përmes ndërfaqeve si zëri, tekstet, ose imazhet.
Shembull: Chatbot-ët si Siri dhe Alexa që marrin komanda dhe ofrojnë përgjigje.

Hyrje në Inteligjencë Artificiale

1950: Turing Test (or Imitation Game)

- Prezantimi i Testit të Turingut, një metodë për të vlerësuar aftësinë e makinave për të treguar sjellje inteligjente të ngjashme me njerëzit.

1966: ELIZA Chatbot

- Krijimi i ELIZA, një nga chatbot-et e para, e zhvilluar nga Joseph Weizenbaum për të simuluar komunikimin njerëzor.

1970-1980: First AI Winter

- Periudha e parë e "AI Winter", një kohë me pritshmëri të ulëta dhe financime të kufizuara për kërkimet në AI.

1980: John Searle's "Chinese Room" thought experiment vs Turing Test

- Eksperimenti i mendimit "Dhoma Kineze" nga John Searle, i cili ngriti dyshime rreth idesë së AI që vërtet kupton në vend që të ndjekë rregulla.

1990s: Advent of Neural Networks

- Shfaqja dhe përdorimi i rrjeteve neuronale për të trajtuar probleme komplekse të të dhënave dhe të mësuarit makinerik.

2000s: Big Data & Deep Learning

- Përparimet në të dhënat masive (big data) dhe zhvillimi i thelluar i mësimit (deep learning), që revolucionarizuan aplikimet e AI.

2022: Google LaMDA

- Prezantimi i LaMDA nga Google, një model avancuar për përpunimin e gjuhës natyrore me kapacitet për biseda më të sofistikuara.

Përdorimet Kryesore të Inteligjencës Artificiale

- ***Shëndetësia:*** **Diagnoza mjekësore, analiza e të dhënave gjenetike, dhe zhvillimi i barnave.**
- ***Financa:*** **Parashikimi i tregut, zbulimi i mashtrimeve, dhe automatizimi i proceseve.**
- ***Transporti:*** **Automjetet autonome dhe menaxhimi i trafikut.**
- ***Marketingu:*** **Personalizimi i përmbajtjes dhe rekomandimet për konsumatorët.**
- ***Siguria Kibernetike:*** **Identifikimi i kërcënimeve dhe automatizimi i reagimeve.**

Shembuj të AI në përditshmëri

- ***Asistentë Virtualë dhe Smart Devices:*** Siri, Alexa, dhe Google Assistant për menaxhim të përditshëm.
- ***Rekomandime të Personalizuara****:* Netflix, Spotify dhe YouTube për përmbajtje të përshtatur.
- ***Shëndetësia:*** Diagnostikimi dhe trajtimi i personalizuar me algoritme të AI.
- ***Siguria Kibernetike:*** Zbulimi i kërcënimeve dhe mbrojtja e të dhënave.
- ***Transporti:*** Automjete autonome si Tesla për siguri dhe efikasitet.
- ***E-commerce:*** Rekomandime për produkte bazuar në preferencat e përdoruesve.
- ***Edukimi Online:*** Platforma si Coursera dhe Duolingo për personalizim të mësimit.
- ***Financa:*** Zbulimi i mashtrimeve dhe analiza e transaksioneve bankare.

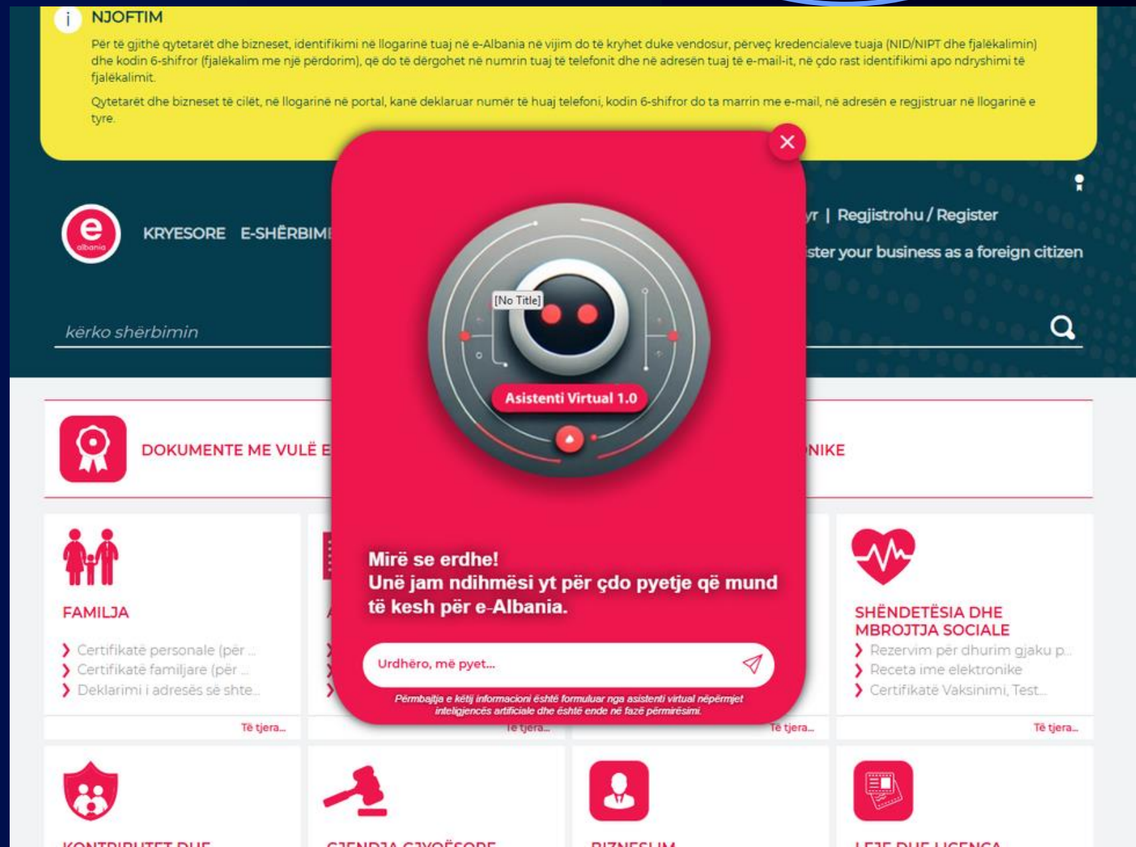
E-Albania dhe Implementimi i Chatbot-it AI

Inovacioni i Ri:

- E-Albania ka implementuar një asistent virtual të bazuar në inteligjencën artificiale (AI) për të ndihmuar qytetarët me pyetje dhe orientim për shërbimet publike online.

Qëllimi Kryesor:

- Përmirësimi i përvojës së përdoruesit.
- Rritja e aksesit dhe efikasitetit të shërbimeve publike.
- Ofrimi i përgjigjeve në kohë reale për pyetje dhe kërkesa.
- Funksionalitetet e Chatbot-it:
- Ofron udhëzime dhe ndihmë për përdoruesit në përdorimin e platformës.
- Jep informacion mbi dokumentet dhe aplikimet e ndryshme.
- Mundëson një qasje më të shpejtë dhe më të thjeshtë për qytetarët.
- Rëndësia: Ky zhvillim reflekton angazhimin e e-Albania për të përqafuar teknologjitë më të avancuara dhe për të rritur transparencën dhe ndërveprimin me qytetarët.



Ndikimi i Inteligjencës Artificiale në Sigurinë Kibernetike

(Mjet i dyfishtë për Sulmuesit dhe Mbrojtësit e Sigurisë)

Inteligjenca Artificiale (AI) ka transformuar sigurinë kibernetike, duke u bërë një mjet i domosdoshëm për mbrojtjen nga kërcënimet gjithnjë e më komplekse.

Aplikimet kryesore të AI përfshijnë:

- **Zbulimi dhe Reagimi ndaj Kërcënimeve:** AI analizon trafikun dhe identifikon anomalitë për të zbuluar kërcënimet më shpejt.
- **Parashikimi dhe Menaxhimi i Rreziqeve:** Analiza parashikuese ndihmon në parandalimin e sulmeve përpara se të ndodhin.
- **Automatizimi i Procesit të Mbrojtjes:** AI automatizon identifikimin e dobësive dhe reagimin ndaj incidenteve.
- **Raporte të Inteligjencës Kibernetike:** Gjenerimi i raporteve për kërcënimet më të fundit për të mbajtur mbrojtësit të informuar.

Pavarësisht përfitimeve të saj, AI sjell gjithashtu sfida, si përdorimi i saj nga sulmuesit për të zhvilluar sulme më të sofistikuara. Sidoqoftë, ndikimi i saj pozitiv në forcimin e sigurisë mbetet i jashtëzakonshëm.

AI – Një Mjet për Sulmuesit

1

Automatizimi

AI mund të përdoret nga sulmuesit për të automatizuar dhe zgjeruar aktivitetet e tyre keqdashëse, si:

- Gjenerimi i email-eve të personalizuara për phishing, më bindëse dhe të sofistikuara.
- Nxitja e sulmeve të shpërndara në shkallë të gjerë të mohimit të shërbimit (DDoS).

2

Shmangia dhe Fshehja

Aktorët keqdashës mund të përdorin AI për të zhvilluar teknika që shmangin zbulimin nga sistemet e sigurisë, si:

- Gjenerimi i maluerëve polimorfikë ose fshehja e aktiviteteve të tyre që të duken të padëmshme.

2

Sulme të Targetuara dhe Inteligjente

Aktorët keqdashës përdorin AI për të përmirësuar saktësinë dhe efektivitetin e sulmeve, duke i bërë ato më të vështira për t'u zbuluar dhe parandaluar.

- Analizimi i modeleve të sjelljes së përdoruesve për të krijuar sulme më bindëse, si phishing i personalizuar.
- Identifikimi i objektivave specifikë përmes analizës së të dhënave të mëdha (Big Data).

Shembull – Deepfake për Mashtrim Financiar

- Në vitin 2019, sulmuesit përdorën teknologjinë deepfake për të manipuluar zërin e një drejtuesi ekzekutiv të një kompanie energjetike gjermane. Ata imituan zërin në mënyrë të bindshme, duke udhëzuar një punonjës të transferonte 243,000 dollarë në një llogari të kontrolluar prej tyre. Deepfake u përdor për të krijuar një regjistrim të zërit që përputhej me theksin dhe mënyrën e të folurit të drejtuesit, duke bërë që kërkesa të dukej plotësisht legjitime.
- **Mësimet e Nxjerra dhe Masa Mbrojtëse:**
- **Edukimi i Punonjësve:** Rritja e ndërgjegjësimit për mashtrimet financiare dhe përdorimin e teknologjive të reja për manipulim.
- **Procedura Shtesë Verifikimi:** Konfirmimi i kërkesave financiare përmes metodave të shumta, si telefonata të drejtpërdrejta ose verifikimi fizik.
- **Teknologji Anti-Deepfake:** Përdorimi i mjeteve të sofistikuara për të zbuluar përmbajtje të manipuluara me AI.

Ky rast tregon sofistikimin në rritje të sulmeve kibernetike dhe rrezikun e përdorimit të AI për qëllime mashtruese, duke theksuar rëndësinë e masave të forta mbrojtëse dhe ndërgjegjësimit të organizatave.

Shembull – Sulme Adversariale ndaj Modeleve të AI

- Në vitin 2021, studiuesit zbuluan se sulmuesit mund të mashtronin modelet e AI duke ndryshuar në mënyrë të qëllimshme të dhënat e input-it.

  Këto sulme përdoren për:
- Manipulimin e Sistemeve të Njohjes së Fytyrës: Për shembull, një maskë e krijuar me AI që shmang njohjen e saktë të fytyrës.
- Mashtrim në Analizën e Imazheve: Ndryshime të vogla në imazhe që i bëjnë modelet të japin rezultate të gabuara.
- Dobësimin e Besueshmërisë së Modeleve: Sulmet e tilla mund të përdoren për të manipuluar sistemet autonome si automjetet e vetëdrejtuara.
- Ky rast tregon dobësitë e sistemeve të AI ndaj sulmeve të sofistikuara dhe nevojën për rritjen e mbrojtjes kundër manipulimeve të tilla.

Shembull – Automatizimi i Sulmeve të Shtrirjes së Fjalëkalimeve: Rasti i vitit 2020

- Në vitin 2020, sulmuesit përdorën inteligjencën artificiale për të provuar miliona kombinime të kredencialeve në faqet e internetit, duke shënjestruar llogari të përdoruesve. AI u përdor për:
- **Analizimin e të Dhënave të Vjedhura:** Algoritmet analizuan kredencialet nga rrjedhjet e të dhënave për të identifikuar modele dhe kombinime të përdorura zakonisht.
- **Prioritizimin e Kombinimeve me Probabilitet të Lartë:** Kjo rriti shanset e suksesit për akses të paautorizuar në llogari.
- **Automatizimin e Procesit:** Mënyra automatike e testimit të miliona fjalëkalimeve në kohë të shkurtër e bëri sulmin më efikas dhe të vështirë për t'u zbuluar.

- Ky rast nënvizon fuqinë e AI për të rritur sofistikimin e sulmeve kibernetike dhe nevojën për masa mbrojtëse si autentifikimi me shumë faktorë (MFA) dhe monitorimi i vazhdueshëm i sistemeve.

AI – Një Mjet për Mbrojtësit

1

Zbulimi dhe Reagimi ndaj Kërcënimeve

- AI mund të analizojë trafikun në rrjet dhe sjelljen për të identifikuar kërcënimet potenciale më shpejt dhe me më pak gabime se sistemet tradicionale.
- Automatizimi i procesit të reagimit ndaj incidenteve.

2

Identifikimi dhe Menaxhimi i Dobësive

AI mund të ndihmojë në gjetjen e dobësive të pranishme në sisteme dhe aplikacione, duke ofruar rekomandime për të adresuar këto probleme përpara se të shfrytëzohen nga sulmuesit.

3

Vlerësimi i Rrezikut

Analiza e rreziqeve përmes BIG DATA-ve dhe modeleve të parashikimit për të përcaktuar nivelin e kërcënimit dhe prioritetin e masave mbrojtëse.

AI – Një Mjet për Mbrojtësit

4

Raporte të Inteligjencës Kibernetike

AI mund të gjenerojë dhe analizojë raporte për kërcënimet më të fundit dhe sjelljen e sulmuesve, duke ndihmuar ekipet e sigurisë të jenë më të përgatitura.

5

Analiza Parashikuese dhe Siguria Adaptuese

AI përdoret për të parashikuar kërcënime bazuar në modelet e mëparshme dhe për të përshtatur masat mbrojtëse në kohë reale për të shmangur sulmet.

6

Asistentë Kognitivë

Asistentët me AI mund të ndihmojnë profesionistët e sigurisë duke ofruar informacion të personalizuar dhe duke ndihmuar në zgjidhjen e problemeve komplekse në kohë reale.

Shembull – Monitorimi dhe Reagimi ndaj Kërcënimeve në Kohë Reale

- Në vitin 2020, platforma Darktrace ndihmoi një kompani financiare të zbulonte dhe të ndalonte një sulm të brendshëm që synonte të vidhte të dhëna sensitive. AI u përdor për:
- Mësimin e Sjelljes Normale të Rrjetit: Algoritmet e mësimit të makinerive analizuan trafikun e zakonshëm për të krijuar një model të sjelljes normale.
- Identifikimin e Aktivitetit Anormal: Platforma zbuloi sjellje të dyshimta që devijonin nga modeli normal, si transferime të paautorizuara të të dhënave.
- Ndërhyrje të Shpejtë: Paralajmërimi në kohë reale i lejoi ekipit të sigurisë të ndërhynte menjëherë, duke parandaluar vjedhjen e informacionit.
- Ky rast tregon fuqinë e AI për monitorimin e vazhdueshëm dhe reagimin e shpejtë ndaj kërcënimeve, duke përmirësuar mbrojtjen e organizatave nga sulmet e sofistikuara.

Shembull – Parandalimi i Sulmeve Phishing

Në vitin 2021, Microsoft Defender përdori inteligjencën artificiale për të bllokuar mbi 30 miliardë emaile phishing dhe malware brenda një viti. AI u përdor për:

- Analizimin e Modeleve të Mesazheve: Algoritmet shqyrtuan strukturën dhe përmbajtjen e emaileve për të identifikuar tipare të zakonshme të phishing-ut.
- Identifikimin e Mesazheve të Dyshimta: Teknologjia zbatoi analiza të avancuara për të zbuluar emaile që përpiqeshin të mashtronin përdoruesit ose të shpërndanin malware.
- Parandalimin e Sulmeve në Kohë Reale: Bllokoi emailet e rrezikshme përpara se të arrinin në kutitë postare të përdoruesve.
- Ky rast tregon fuqinë e AI për të mbrojtur organizatat dhe përdoruesit nga sulmet phishing në shkallë të gjerë, duke përmirësuar sigurinë dhe reduktuar ndjeshëm rreziqet e mashtrimit.

Shembull – Analiza e Sjelljes së Përdoruesve për Zbulimin e Kërcënimeve të Brendshme

- Në vitin 2022, një institucion shëndetësor përdori platformën Splunk për të zbuluar një punonjës që po aksesonte të dhëna pacientësh pa autorizim. AI u përdor për:
- Analizimin e Sjelljes së Përdoruesve: Algoritmet identifikuan modelet normale të aksesit dhe aktivitetit të punonjësve.
- Zbulimin e Aktivitetit të Pazakontë: Veprimet e punonjësit devijuan nga sjellja e zakonshme, si aksesimi i të dhënave të ndjeshme pa arsye të qartë.
- Identifikimin e Kërcënimit të Brendshëm: Teknologjia sinjalizoi aktivitetin si të dyshimtë, duke mundësuar që ekipi i sigurisë të ndërhynte me shpejtësi.
- Ky rast thekson rëndësinë e përdorimit të AI për të zbuluar kërcënimet e brendshme dhe për të mbrojtur të dhënat sensitive nga abuzimi i mundshëm.

AI & Cyber:
Sfidat në Adoptimin e Inteligjencës Artificiale për Sigurinë Kibernetike

Kosto të Larta të Implementimit

Kostoja e lartë e implementimit dhe mirëmbajtjes së teknologjive të sigurisë kibernetike të bazuara në AI është domethënëse.

Varësia nga Personeli i Kualifikuar

Zbatimi efektiv i zgjidhjeve të bazuara në AI kërkon personel me aftësi të larta.

Shqetësime Etike

Përdorimi i AI në sigurinë kibernetike ngre dilema etike, si cenimi i privatësisë, prirja algoritmike, dhe përdorimi i mundshëm për mbikëqyrje ose censurë.

Kompleksitetet Rregullatore

Kornizat rregullatore jo të përshtatshme dhe sfidat ligjore që lidhen me privatësinë e të dhënave dhe sigurinë mund të pengojnë zbatimin efektiv të zgjidhjeve të bazuara në AI.

Ndikimet Etike të Inteligjencës Artificiale (AI) në Sigurinë Kibernetike

Drejtësia (Fairness)	Transparenca (Transparency)	Mbikëqyrja Njerëzore (Human Oversight	Privatësia (Privacy)	Pranimi Shoqëror (Social Acceptance)
Sigurimi që sistemet e sigurisë kibernetike të bazuara në AI: ◦ Marrin vendime të paanshme. ◦ Trajtojnë të gjithë individët dhe organizatat në mënyrë të barabartë, pa diskriminim ose ndikime të pabarabarta.	Promovimi i transparencës në mjetet e sigurisë kibernetike të bazuara në AI, në mënyrë që: • Procesi i vendimmarrjes të jetë i kuptueshëm. • Të jetë i mbajtur përgjegjës.	• Parandalimi i pasojave të paqëllimshme. • Sigurimi që vendimet kritike të merren me gjykim dhe përgjegjësi njerëzore.	Mbrojtja e privatësisë dhe të drejtave të të dhënave të individëve, edhe kur mjetet e sigurisë kibernetike të bazuara në AI mbledhin dhe analizojnë sasi të mëdha informacioni personal dhe të ndjeshëm.	Kultivimi i besimit ndërmjet komuniteteve përmes komunikimit transparent rreth: • Aplikimeve të AI. • Përfitimeve potenciale. • Kornizave etike të vendosura për të zbutur rreziqet.

Roli i AI në zgjidhjen e sfidave globale

AI ka potencialin të luajë një rol të rëndësishëm në adresimin e sfidave globale, të tilla si ndryshimet klimatike, varfëria dhe sëmundjet.

Ndryshimet Klimatike

AI mund të përdoret për të optimizuar konsumin e energjisë, për të zhvilluar teknologji të qëndrueshme dhe për të monitoruar ndryshimet mjedisore.

Global Health

AI mund të ndihmojë në diagnostikimin e sëmundjeve, zbulimin e ilaçeve dhe mjekësinë e personalizuar, duke përmirësuar rezultatet e kujdesit shëndetësor.

Zhvillimi i Qëndrueshëm

AI mund të kontribuojë në zhvillimin e qëndrueshëm duke optimizuar menaxhimin e burimeve, duke promovuar energjinë e rinovueshme dhe duke reduktuar mbetjet.

Rreziqet e mundshme dhe strategjitë e zbutjes për AI

Ndërsa AI ofron përfitime të mëdha, ka edhe rreziqe të mundshme që duhet të adresohen. Është thelbësore që këto rreziqe të zbuten përmes zhvillimit dhe rregullimit të përgjegjshëm.

Siguria dhe Siguria e AI

Sigurimi që sistemet e AI janë të sigurta dhe të sigurta është thelbësore për të parandaluar pasojat e padëshiruara dhe përdorimin e keq.

Zhvendosja e punës dhe përçarja ekonomike

Ndikimi i IA në punësim kërkon shqyrtim të kujdesshëm dhe strategji për të zbutur zhvendosjen e mundshme të punës.

E ardhmja e Ai in Cyber Security

a) Inteligjencë më e Avancuar dhe Autonome

- Parashikimi: Sistemet e AI do të bëhen më të pavarura, duke marrë vendime pa nevojën për ndërhyrje njerëzore në rastet e reagimit ndaj kërcënimeve.
- Shembull: Platforma si Darktrace po zhvillojnë algoritme që jo vetëm monitorojnë, por edhe neutralizojnë kërcënimet në kohë reale.

b) Parashikimi i Kërcënimeve përmes Analizës së Të Dhënave

- Parashikimi: AI do të përdorë analiza parashikuese për të identifikuar modelet dhe tendencat e kërcënimeve kibernetike para se ato të ndodhin.
- Si funksionon: Algoritmet do të përpunojnë miliarda ngjarje sigurie për të ofruar paralajmërime të hershme për sulmet.

c) Inteligjenca Gjeneruese për Mbrojtje

- Parashikimi: Algoritmet si GPT do të përdoren për të simuluar sulme dhe për të testuar dobësitë në sisteme.
- Përfitimi: Organizatat do të kenë mjete për të parashikuar taktikat e sulmuesve dhe për të adresuar dobësitë para se ato të shfrytëzohen.

d) Përshtatshmëria e Sistemeve të Sigurisë

- Parashikimi: AI do të zhvillojë sisteme mbrojtëse që përshtaten automatikisht me kërcënimet e reja në kohë reale.
- Shembull: Një sistem që përshtat politikën e firewall-it bazuar në aktivitetin kibernetik të detektuar në rrjet.

Si Mendohet të Ndikohet Siguria Kibernetike nga AI

a) Automatizimi i Reagimeve ndaj Incidenteve

- Ndikimi: Koha e reagimit do të reduktohet ndjeshëm me përdorimin e AI për të identifikuar, analizuar dhe neutralizuar kërcënimet në kohë reale.
- Shembull: SOAR (Security Orchestration, Automation, and Response) që përdor AI për të automatizuar trajtimin e incidenteve.

b) Reduktimi i Sulmeve të Brendshme

- Ndikimi: Analiza e sjelljes së përdoruesve nga AI do të ndihmojë në identifikimin e veprimeve të dyshimta të kryera nga brenda organizatës.
- Shembull: Splunk përdor AI për të monitoruar aktivitetet e përdoruesve dhe për të identifikuar devijimet nga normalja.

c) Mbrojtje ndaj Malware Polimorfik

- Ndikimi: AI do të jetë në gjendje të identifikojë dhe neutralizojë malware që ndryshon kodin e tij për të shmangur zbulimin.
- Shembull: Algoritmet e mësimit të thellë që analizojnë sjelljen e malware në vend të kodit të tij.

d) Përmirësimi i Sigurisë së IoT (Internet of Things)

- Ndikimi: Pajisjet IoT, që shpesh janë të ekspozuara ndaj kërcënimeve, do të mbrohen më mirë përmes sistemeve të fuqizuara nga AI që monitorojnë dhe analizojnë trafikun në rrjet.
- Shembull: Armis Security përdor AI për të siguruar pajisjet IoT kundër sulmeve.

e) Forcimi i Sistemeve të Enkriptimit

- Ndikimi: AI mund të ndihmojë në zhvillimin e algoritmeve të reja të enkriptimit për t'u mbrojtur kundër kompjuterave kuantikë që mund të deshifrojnë enkriptimin tradicional.
- Shembull: Algoritmet post-kuantike për të siguruar të dhënat në mjediset e avancuara teknologjike.

Sfida dhe Rreziqe për të Ardhmen

a) Përdorimi i AI nga Sulmuesit

- Ndërsa AI përmirëson sigurinë, ajo mund të përdoret gjithashtu nga sulmuesit për të krijuar sulme më të sofistikuara, si deepfake ose phishing të personalizuar.

b) Varësia nga AI

- Rritja e varësisë nga sistemet e AI mund të krijojë dobësi nëse këto sisteme manipulohen ose dështojnë.

c) Nevoja për Korniza Etike dhe Ligjore

- Duhet një kornizë e qartë për përdorimin etik të AI në mënyrë që të mbrohet privatësia dhe të shmanget përdorimi i paautorizuar i teknologjisë.

FALEMINDERIT!

www.aksk.gov.al

Rruga “Papa Gjon Pali II”, Nr.3, Kati I Tiranë

info@aksk.gov.al