MBLEDHJA STRATEGJIKE E TË DHËNAVE PËR SIGURINË KIBERNETIKE

RËNDËSIA E SIGURISË KIBERNETIKE PËR INFRASTRUKTURAT KRITIKE TË INFORMACIONIT

- Në botën e sotme, siguria kibernetike është thelbësore, sidomos kur flasim për mbrojtjen e Infrastrukturave Kritike të Informacionit (IKI).

- IKI-të, si rrjetet e energjisë, sistemet e ujit, institucionet financiare dhe shëndetësia, janë shtylla jetike për mirëqenien dhe funksionimin e vendit tonë dhe të institucioneve të tij.

- Çdo dëmtim apo ndërprerje e shërbimeve të ofruara nga këto infrastruktura mund të ketë pasoja të rënda për jetën e qytetarëve, ekonominë dhe mjedisin.

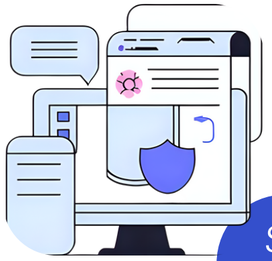
PSE MBLEDHJA STRATEGJIKE E TË DHËNAVE ËSHTË KYÇE?

- Për të forcuar mbrojtjen e këtyre aseteve, nuk mjafton vetëm të reagojmë ndaj incidenteve. Kërkohet një qasje proaktive dhe strategjike në mbledhjen dhe analizimin e të dhënave.

- Mbledhja strategjike e të dhënave na mundëson të kuptojmë më mirë kërcënimet, të identifikojmë dobësitë dhe të marrim vendime të informuara për të parandaluar incidentet para se ato të ndodhin.

- Ky webinar do të shqyrtojë pikërisht këtë – një kuadër për mbledhjen strategjike të të dhënave, i cili është thelbësor për Sigurinë Kibernetike.

ÇFARË DO TË TRAJTOJMË SOT?



Si të mblidhni të dhëna në mënyrë strategjike nga puna juaj e përditshme dhe si t'i interpretoni ato për të rritur nivelin e sigurisë kibernetike.

Si mund të aplikoni analizën e të dhënave në fushën dinamike të sigurisë kibernetike.

Rëndësinë kritike të mbledhjes së të dhënave për mbrojtjen e infrastrukturave dhe rolin që secili prej nesh mund të luajë.

PEIZAZHI I KËRCËNIMEVE: NJË URGJENCË NË RRITJE

Viti 2024 shënoi një përshkallëzim të dukshëm në peizazhin global të kërcënimeve kibernetike, me një rritje të paprecedentë në numrin dhe sofistikimin e sulmeve.

Kostoja mesatare globale e një shkeljeje të të dhënave arriti një nivel historik prej 4.88 milionë dollarësh në 2024, duke shënuar një rritje prej 10% nga viti 2023.

Raporti i Verizon 2024 DBIR analizoi mbi 30,000 incidente sigurie, nga të cilat 10,626 rezultuan me shkelje të konfirmuara të të dhënave dhe preku organizata në 94 vende.

Shfrytëzimi i vulnerabiliteteve, si metoda kryesore për të nisur një shkelje, ka parë një rritje të ndjeshme, pothuajse duke u trefishuar krahasuar me vitin e kaluar.

Elementi njerëzor ishte një komponent në 68% të të gjitha shkeljeve të të dhënave, duke theksuar se njeriu mbetet hallka më e dobët në zinxhirin e sigurisë.

PEIZAZHI I KËRCËNIMEVE: DY RASTE ME IMPAKT TË LARTË

Change Healthcare

Sulmi masiv kibernetik ndaj Change Healthcare preku rreth 190 milionë individë, duke demonstruar ndikimin shkatërrues të sulmeve në shkallë të gjerë. Hetimi i këtij sulmi tregoi që keqbërësit përdorën kredenciale të komprometuara të një portali për remote access, i cili nuk kishte autentifikim me shumë faktorë.

https://www.hipaajournal.com/the-biggest-healthcare-data-breaches-of-2024/

Salt Typhoon

Në 2024 u zbulua se Grupi i Kërcënimit të Vazhdueshëm të Avancuar i (APT) 'Salt Typhoon', i cili besohet se është një grup kinez arriti të kompromet ojë rrjete të shumta telekomunikacioni (si Verizon, AT&T) dhe Thesarin e SHBA-së. Kjo u arrit duke shfrytëzuar "ndreqjet e neglizhuara" (neglected patching) të vulnerabiliteve shpesh të njohura prej kohësh, që mbeteshin të paadresuara.

https://www.picussecurity.com/resource/blog/the-major-cyber-breaches-and-attack-campaigns-of-2024

ÇFARË JANË INFRASTRUKTURAT KRITIKE TË INFORMACIONIT?

Infrastrukturat Kritike të Informacionit janë ato sisteme, asete dhe pjesë të rrjeteve dixhitale, dëmtimi, shkatërrimi, kompromet imi ose ndërprerja e të cilave do të kishte një ndikim të rëndë në sigurinë kombëtare, mbrojtjen, ekonominë, shëndetin publik, sigurinë publike ose mjedisin.

Energjia: *Sistemet e Kontrollit dhe Monitorimit të transmetimit të energjisë elektrike; Sistemet e menaxhimit të digave dhe hidrocentraleve kryesore (p.sh., HEC-et mbi lumin Drin).*

Bankar: *Sistemet qendrore të Bankës së Shqipërisë (p.sh., sistemi i pagesave ndërbankare); Sistemet e bankave të nivelit të dytë që menaxhojnë llogaritë e klientëve.*

RËNDËSIA DHE NDËRLIDHJA E IKI-VE

- *Mbrojtja e IKI-ve është një prioritet kombëtar sepse dëmtimi i tyre do të kishte një ndikim të rëndë në sigurinë kombëtare, mbrojtjen, ekonominë, shëndetin publik, sigurinë publike ose mjedisin."*
- *Në rast incidenti Shërbimet thelbësore për qytetarët dhe bizneset do të pengoheshin.*

Efekti Domino: Sistemet janë të ndërlidhura dhe të ndërvarura fort.

- *Një sulm i suksesshëm në një sektor mund të ketë efekte kaskade në të gjithë infrastrukturat.*
  - *Për shembull, një ndërprerje e madhe e energjisë mund të ndikojë sistemet e komunikimit, transportit dhe shërbimet shëndetësore.*

- *Kjo do të thotë se siguria kibernetike nuk është më thjesht një çështje teknike, por një sfidë thelbësore për stabilitetin ekonomik dhe funksionimin e shoqërisë.*

KUADRI RREGULLATOR

Ligji dhe Direktiva EU për Sigurinë Kibernetike

Ligji "Për Sigurinë Kibernetike", Nr. 25/2024

- Ka për qëllim përcaktimin e masave të sigurisë për arritjen e një niveli të lartë të sigurisë kibernetike për rrjetet dhe sistemet e informacionit në Republikën e Shqipërisë.
- Ndër të tjera, përcakton kriteret mbi të cilat bazohet identifikimi i infrastrukturave kritike dhe të rëndësishme të informacionit.

Direktiva e BE – NIS2

- Përcakton masa që synojnë arritjen e një niveli të lartë të përbashkët të sigurisë kibernetike, me synimin për të përmirësuar funksionimin e tregut të përbashkët."
- Ndër të tjera përcakton detyrimet që Shtetet Anëtare të adoptojnë strategji kombëtare të sigurisë kibernetike dhe të caktojnë autoritete të menaxhimit të krizave kibernetike dhe ekipe të reagimit ndaj incidenteve.

Implikimet Kryesore për Infrastrukturat Kritike të Informacionit

- Nevoja për identifikimin e aseteve dhe sistemeve kritike.
- Detyrimi për vlerësime të rregullta dhe të vazhdueshme të riskut.
- Zbatimi i masave mbrojtëse teknike dhe organizative.
- Raportimi i incidenteve të rëndësishme tek autoritetet kompetente (p.sh., CSIRT Kombëtar pranë AKSK).

Roli i AKSK:

- Mbikëqyrja, bashkëpunimi dhe shkëmbimi i informacionit për sigurinë kibernetike kombëtare.

ÇFARË TË DHËNASH MBLEDHIM PËR SIGURINË KIBERNETIKE

Kategoritë kryesore të të dhënave

- Threat Intelligence - Inteligjenca e Kërcënimeve
- Të Dhënat e Vulnerabiliteteve
- Raportet e Incidenteve
- Compliance Metrics - Metrikat e Pajtueshmërisë

Për të ndërtuar një mbrojtje efektive kibernetike për Infrastrukturat Kritike të Informacionit, ne mbledhim dhe analizojmë lloje të ndryshme të dhënash.

Këto të dhëna na ndihmojnë të kuptojmë kërcënimet, të identifikojmë vulnerabilitetet, të menaxhojmë incidentet dhe të sigurojmë pajtueshmërinë.

THREAT INTELLIGENCE - INTELIGJENCA E KËRCËNIMEVE

Inteligjenca e Kërcënimeve: Të Njohim Armikun

- *Inteligjenca e kërcënimeve është informacion i analizuar dhe i kontekstualizuar mbi kërcënimet ekzistuese ose të mundshme.*

- *Na ndihmon të kuptojmë: Kush po na sulmon, pse, si (TTP-të), dhe çfarë po targetohet (Indikatorët e Kompromentimit - IoC-të).*

Nivelet Kryesore:

- *Inteligjenca Taktike: Informacion për vektorët specifikë të sulmeve, mjetet, dhe Indikatorët e Kompromentimit (IoC-të).*

- *Inteligjenca Operacionale: Fokusohet te Taktikat, Teknikat dhe Procedurat (TTP-të) e aktorëve të kërcënimit dhe motivimet e tyre.*

- *Inteligjenca Strategjike: Jep një pamje të gjerë të peizazhit të kërcënimeve, tendencat afatgjata, dhe motivet e aktorëve shtetërorë.*

TË DHËNAT E VULNERABILITETEVE

Të Njohim Dobësitë Tona

- Identifikimi i pikave të dobëta në sisteme, aplikacione dhe rrjete.
- Përfshin informacione për vulnerabilitete të njohura si CVE-të (Common Vulnerabilities and Exposures).
- Vulnerabilitetet e panjohura më parë, shfrytëzimi i të cilave çon në sulme 'Zero-Day' (zero ditë), paraqesin rrezik të veçantë.
- Shfrytëzimi i vulnerabiliteteve të pa adresuara është trefishuar me një rritje prej 180% si metodë kryesore e shkeljeve në 2024.

Si mblidhen:

- Skanerë automatikë të vulnerabiliteteve, testime depërtimi (Penteration Test), raporte nga prodhuesit.

Përdorimi:

- Përmirësimi proaktiv i sigurisë, analizë e shpeshtësisë së vulnerabiliteteve (vulnerability frequency analysis), etj.

RAPORTET E INCIDENTEVE

Të Mësojmë nga E Shkuara

- Informacion i detajuar mbi sulmet kibernetike që kanë ndodhur.
- Përfshin detaje si: koha, lloji i sulmit, ndikimi, përgjigja, dhe mësimet e nxjerra

Si mblidhen:

- Regjistrat e sistemeve (logs).
- Raportet e përdoruesve.
- Analiza forenzike dixhitale pas incidentit.
- Publikimet zyrtare të raporteve të incidenteve nga Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK) – P.sh., https://aksk.gov.al/raporte-incidentesh/

Përdorimi:

- Analiza pas-incidentit për përmirësimin e mbrojtjeve ekzistuese.
- Identifikimi i modeleve dhe trendeve të reja të sulmeve.
- Parashikimi i incidenteve të ardhshme dhe përgatitja për to.
- Informimi i politikave dhe strategjive të sigurisë.

METRIKAT E PËRPUTHSHMËRISË

Të Matim Performancën dhe Përputhshmërinë

- Metrikat e përputhshmërisë janë të dhëna sasiore që tregojnë performancën e kontrolleve të sigurisë dhe nivelin e përputhshmërisë me rregulloret dhe standardet.
- Përfshijnë Key Performance Indicators (KPIs) – Treguesit Kyç të Performancës – dhe Key Risk Indicators (KRIs) – Treguesit Kyç të Riskut.

Si mblidhen:

- Auditimet e sigurisë,
- Raportet e riskut kibernetik
- sistemet e menaxhimit të log-eve,
- mjetet e monitorimit të përputhshmërisë.

Rëndësia:

- Vendimmarrje e bazuar në të dhëna për investime dhe prioritete në sigurinë kibernetike.
- Vlerësim i efektivitetit të masave mbrojtëse.
- Sigurimi i respektimit të kërkesave rregullatore dhe ligjore, duke shmangur kostot e larta nga gjobat rregullatore në rast shkeljesh.

TË DHËNAT SASIORE DHE CILËSORE

Të Dhënat Sasiore:

- "Janë numerike, të matshme dhe strukturuara. Na tregojnë 'sa', 'sa shpesh', 'ku', 'kur'."

- Shembuj në Sigurinë Kibernetike: Numri i incidenteve, numri i vulnerabiliteteve të zbuluara, shpeshtësia e sulmeve phishing, statistikat e trafikut të rrjetit, kohëzgjatja e ndërprerjeve të shërbimeve.

Të Dhënat Cilësore:

- "Janë përshkruese, kontekstuale dhe ofrojnë thellësi. Na ndihmojnë të kuptojmë 'pse' dhe 'si'."

- Shembuj në Sigurinë Kibernetike: Raportet e incidenteve, intervistat me ekspertët e sigurisë, feedback-u nga stafi për ndërgjegjësimin kibernetik, analiza e motiveve të sulmuesve, përshkrimet e TTP-ve të aktorëve të kërcënimit.

MBLEDHJA PRIMARE E TË DHËNAVE

Kjo qasje përfshin mbledhjen e të dhënave të reja, drejtpërdrejt nga burimi, për qëllime specifike të analizës aktuale.

Shembuj Sasior:

- Rezultatet e testeve të depërtimit (numri i vulnerabiliteteve të zbuluara).
- Të dhënat nga skanerët e vulnerabiliteteve.
- Rezultatet e anketave (p.sh., niveli i ndërgjegjësimit në shifra).

Shembuj Cilësor:

- Intervistat e thelluara me ekspertë të sigurisë (te brendshëm ose të jashtëm).
- Vëzhgimet e drejtpërdrejta të sjelljes së përdoruesve.
- Diskutimet në fokus grupe rreth sfidave të sigurisë.

Karakteristikat:

- Informacioni më i fundit dhe i dedikuar.
- Kontroll i plotë mbi metodologjinë dhe cilësinë.
- Mund të kërkojë më shumë kohë dhe burime.

MBLEDHJA DYTËSORE E TË DHËNAVE

Kjo qasje përfshin përdorimin e të dhënave që tashmë ekzistojnë, të mbledhura më parë nga të tjerë për qëllime të tjera.

Shembuj Sasior:

- Statistika mbi sulmet kibernetike nga raporte të organizatave kërkimore ose kompanive të sigurisë.
- Kostot mesatare globale të shkeljeve .
- Të dhëna nga bazat publike të vulnerabiliteteve (p.sh., databaza të CVE-ve).

Shembuj Cilësor:

- Raportet narrative të incidenteve të sigurisë nga institucione të tjera.
- Artikujt e lajmeve mbi fushatat e fundit të kërcënimeve ose studimet e rasteve publike.
- Informacioni nga Burimet e Hapura (OSINT).

Karakteristikat:

- Shpesh më e shpejtë dhe më ekonomike.
- Akses në sasi të mëdha të dhënash.
- E shkëlqyer për tendenca afatgjata dhe analiza krahasuese.
- Duhet verifikuar relevanca dhe besueshmëria e burimit.

AVANTAZHET DHE DISAVANTAZHET TË DHËNAT PRIMARE DHE DYTËSORE

Të dhënat Primare

Avantazhet

- Specifike dhe Relevante: Të dhënat janë mbledhur saktësisht për qëllimet tuaja, duke siguruar relevancë maksimale.
- Aktuale: Informacion i freskët dhe i përditësuar.
- Kontroll: Kontroll i plotë mbi metodologjinë dhe cilësinë e të dhënave.

Disavantazhet

- Kohë dhe Kosto: Kërkon kohë të konsiderueshme dhe burime financiare/njerëzore.
- Kompleksitet: Mund të jetë e vështirë të zbatohet në shkallë të gjerë.
- Njohuri e Specializuar: Kërkon ekspertizë në dizajnimin e kërkimit dhe mbledhjen e të dhënave.

Të dhënat Dytësore

Avantazhet

- Efikasitet: Më e shpejtë dhe më ekonomike, pasi të dhënat ekzistojnë tashmë.
- Burime të Gjëra: Akses në sasi të mëdha të dhënash që ndoshta nuk do t'i mblidhnit vetë.
- Baza për Analizë: E shkëlqyer për analizën e trendeve afatgjata dhe analiza krahasuese.

Disavantazhet

- Relevancë e Kufizuar: Mund të mos jetë specifikisht e përshtatshme për qëllimin tuaj aktual.
- Cilësia dhe Saktësia: Cilësia mund të ndryshojë; saktësia varet nga burimi origjinal.
- Aktualitet i Kufizuar: Mund të jenë të vjetëruara.
- Mungesa e Kontrollit: Nuk keni kontroll mbi mënyrën si janë mbledhur të dhënat

METODA E TRIANGULIMIT
PËRKUFIZIMI DHE QËLLIMI

Triangulimi

- Është përdorimi i të paktën tre metodave, burimeve, apo këndvështrimeve për të shqyrtuar të njëjtin fenomen.

Qëllimi

- Të rrisë vlefshmërinë dhe besueshmërinë e gjetjeve duke krahasuar dhe konfirmuar të dhëna nga burime të ndryshme.

Kjo metodë ndihmon në minimizimin e paragjykimeve dhe rrit saktësinë e vendimmarrjes.

TRIANGULIMI I BURIMEVE
DISA SHEMBUJ

Vulnerabilitetet

- Të dhëna sasiore të vulnerabiliteteve nga skanerët.
- Intervista cilësore me stafin e IT (për të kuptuar kontekstin).
- Kontrolli i raporteve më të fundit të auditimit, për pikat e dobëta të identifikuara.

Incidentet

- Konfirmimi i një raporti cilësor incidenti.
- Të dhëna sasiore nga log-et e sistemit.
- Informacion nga inteligjenca e kërcënimeve mbi TTP-të.

Ndërgjegjësimi i Punonjësve

- Vlerësimi i ndërgjegjësimit me anketa sasiore.
- Diskutimet në fokus grupe (cilësore).
- Analiza e rezultateve të simulimeve të phishing apo testeve të inxhinierisë sociale.

Ky proces rrit saktësinë e vendimmarrjes dhe ndihmon në minimizimin e paragjykimeve (bias).

TRIANGULIMI I BURIMEVE
SKENAR NE SEKTORIN E ENERGJISË

Problemi

- Hetimi i një ndërprerjeje të papritur dhe në shkallë të gjerë të energjisë, e dyshuar si sulm kibernetik.

Burimi 1 (Primar Sasiore) Analiza e Log-eve të ICS/SCADA

- Analiza e thelluar e log-eve të Sistemit të Kontrollit Industrial (ICS/SCADA) për anomali dhe aktivitet të dyshimtë.
- Identifikimi i pikave të hyrjeve të mundshme dhe kohëzgjatjes së aktivitetit.

Burimi 2 (Dytësor Cilësore) Konsultimi i Inteligjencës së Kërcënimeve

- Konsultimi i raporteve të inteligjencës së kërcënimeve (p.sh., nga Mandiant ose ENISA).
- Kërkimi për Taktikat, Teknikat dhe Procedurat (TTPs) të njohura të grupeve APT (si Salt Typhoon) që synojnë sektorin e energjisë.

Burimi 3 (Primar Cilësore) Intervistimi i Personelit Operacional

- Intervistimi i inxhinierëve të sistemit dhe operatorëve.
- Mbledhja e dëshmive për ndryshimet e papritura në sjelljen e sistemit, alarme, apo ndërhyrje manuale të nevojshme gjatë incidentit.

Rezultati

- Përputhja (ose mospërputhja) e gjetjeve nga këto burime ndihmon në përcaktimin nëse ishte sulm kibernetik, kush ishte përgjegjës, dhe si të parandalohet në të ardhmen, duke e bërë më të sigurtë sektorin energjetik.

SFIDAT E MBLEDHJES SË TË DHËNAVE

Mbledhja dhe analiza e të dhënave të sigurisë kibernetike paraqesin disa sfida. Ndër to mund të përmendim:

- **Vëllimi dhe Kompleksiteti i të Dhënave:** Sasi masive të dhënash nga burime të ndryshme, të vështira për t'u përpunuar dhe kuptuar.
- **Cilësia dhe Saktësia e të Dhënave:** Të dhëna të paplota, të pasakta, ose të vjetruara mund të çojnë në analiza të gabuara.
- **Kufizimet e Burimeve:** Mungesa e burimeve njerëzore të kualifikuara, teknologjive të duhura, ose fondeve.
- **Kompleksiteti i Mjediseve të IT:** Infrastrukturat dixhitale shpesh janë të ndërlikuara dhe të fragmentuara.
- **Bashkëpunimi dhe Shkëmbimi i Informacionit:** Vështirësitë në shkëmbimin e informacionit të ndjeshëm ndërmjet departamenteve, institucioneve, apo palëve të treta.
- **Mungesa e Prioritizimit Organizativ:** Siguria kibernetike mund të mos jetë prioritet i lartë në nivel organizativ.

ASPEKTET ETIKE DHE LIGJORE

Mbledhja e të dhënave për sigurinë kibernetike kërkon ndërgjegjësim të plotë për aspektet etike dhe ligjore.

- **Privatësia dhe Mbrojtja e të Dhënave:** Mbrojtja e te dhenave personale dhe përputhshmëria me rregullore te tilla si GDPR.

- **Transparenca dhe Kufizimi i Qëllimeve të Përdorimit:** Informimi i individëve dhe përdorimi i të dhënave vetëm për qëllime sigurie, statistikore, etj.

- **Balanca Siguri vs. Privatësi:** Gjetja e ekuilibrit mes mbrojtjes së IKI-ve dhe të drejtave individuale.

- **Përgjegjshmëria**: Mbajtja e përgjegjësisë për menaxhimin e sigurt të të dhënave.

KONKLUZIONE DHE HAPAT E ARDHSHËM

Pikat Kryesore të Mësuara

- *Rëndësia jetike e IKI-ve*
- *Peizazhi i kërcënimeve*
- *Mbledhja Strategjike e të Dhënave*
- *Metoda e Triangulimit*
- *Sfidat & Aspekti Etik*

Hapat Konkretë për të Ardhmen

- *Identifikoni dhe vlerësoni asetet kritike.*
- *Forconi higjienën kibernetike*
- *Investoni te elementi njerëzor (ndërgjegjësimi, trajnimi).*
- *Bashkëpunoni dhe shkëmbeni informacion për një siguri kolektive.*

FALEMINDERIT!