Lecția 1: Concepte fundamentale și terminologie în securitatea informațională

Tema: Fundamentele securității informaționale **Universitatea Tehnică a Moldovei Lector:** Maxim Masiutin, Asistent universitar

Introducere

Bună ziua tuturor. Bine ați venit la prima noastră lecție din cadrul cursului Tehnologii ale Securității Informaționale. În următoarele trei luni, vom explora lumea fascinantă și extrem de importantă a securității informaționale. Astăzi, începem cu conceptele fundamentale pe care se bazează tot ceea ce urmează.

Înainte de a aborda tehnologii, atacuri sau mecanisme de apărare specifice, trebuie să stabilim un vocabular comun. Securitatea informațională are propriul său limbaj, iar înțelegerea precisă a acestor termeni este esențială. Un singur concept înțeles greșit poate duce la un sistem configurat incorect, iar un sistem configurat incorect poate duce la o breșă care afectează milioane de persoane.

Permiteți-mi să încep cu o întrebare: câți dintre voi ați auzit în acest an la știri despre o breșă de securitate a datelor? Bănuiesc că toată lumea a ridicat mâna. Breșele de securitate a datelor sunt acum atât de frecvente încât aproape le așteptăm. Conform Cybersecurity Ventures, costul global al criminalității cibernetice este estimat să atingă 13 trilioane de dolari până în 2028. Această cifră este mai mare decât PIB-ul majorității țărilor. Iată de ce suntem astăzi aici.

Partea 1: Securitatea informațională vs. securitatea cibernetică

Să începem prin clarificarea a doi termeni care sunt adesea folosiți interschimbabil, dar au semnificații distincte: securitatea informațională și securitatea cibernetică.

Securitatea informațională, uneori numită InfoSec, este practica de protejare a informațiilor împotriva accesului, utilizării, dezvăluirii, perturbării, modificării sau distrugerii neautorizate. Observați că această definiție nu specifică modul în care sunt stocate informațiile. Securitatea informațională acoperă documentele pe hârtie dintr-un dulap de fișiere la fel de bine ca și

datele dintr-un server cloud. Dacă ați văzut vreodată un aviz cu "Doar personal autorizat" pe o ușă, aceasta este securitatea informațională în acțiune.

Securitatea cibernetică este un subset al securității informaționale care se ocupă în mod specific de protejarea sistemelor electronice, rețelelor și datelor împotriva atacurilor digitale. Când vorbim despre paravane de protecție, sisteme de detecție a intruziunilor sau software malițios, ne aflăm în domeniul securității cibernetice.

Iată o modalitate practică de a înțelege diferența: dacă cineva pătrunde într-un birou și fură documente tipărite cu date ale clienților de pe un birou, acesta este un incident de securitate informațională, dar nu un incident de securitate cibernetică. Dacă cineva pătrunde de la distanță într-o bază de date și descarcă aceleași înregistrări, acesta este atât un incident de securitate informațională, cât și un incident de securitate cibernetică.

Pe parcursul acestui curs, ne vom concentra în principal pe securitatea cibernetică, dar rețineți întotdeauna că aceasta există în contextul mai larg al securității informaționale. Cel mai sofisticat paravan de protecție din lume nu vă poate proteja dacă un angajat lasă documente confidențiale în tren.

Partea 2: Triada CID

Acum ajungem la cel mai fundamental model din securitatea informațională: Triada CID. Nu, aceasta nu are nicio legătură cu Central Intelligence Agency. În contextul nostru, CID înseamnă **Confidențialitate**, **Integritate** și **Disponibilitate**. Aceste trei proprietăți formează fundamentul fiecărei decizii de securitate pe care o luăm.

Permiteți-mi să desenez acest model pe tablă sub forma de triunghi. Fiecare colț reprezintă una dintre aceste proprietăți, iar un sistem securizat trebuie să le mențină pe toate trei în echilibru.

Confidențialitatea

Confidențialitatea înseamnă asigurarea faptului că informațiile sunt accesibile doar celor autorizați să le acceseze. Când protejăm confidențialitatea, prevenim dezvăluirea neautorizată a informațiilor.

Gândiți-vă la contul vostru bancar. Doar voi și angajații autorizați ai băncii ar trebui să poată vedea soldul contului vostru. Dacă un străin oarecare ar putea vizualiza informațiile voastre financiare, aceasta ar fi o încălcare a confidențialității.

Confidențialitatea este amenințată de diverse atacuri:

- **Interceptarea (eavesdropping)**: cineva interceptează traficul de rețea pentru a vă citi e-mailurile
- **Supravegherea vizuală (shoulder surfing)**: cineva vă urmărește când introduceți parola

- **Ingineria socială**: cineva vă păcălește să dezvăluiți informații confidențiale
- **Breșe de securitate a datelor**: atacatorii fură baze de date care conțin informații personale

Protejăm confidențialitatea prin:

- **Criptare**: conversia datelor într-un format ilizibil fără cheia corespunzătoare
- **Controale de acces**: asigurarea că doar utilizatorii autorizați pot accesa resurse specifice
- **Autentificare**: verificarea identității utilizatorilor înainte de a le acorda acces
- **Securitate fizică**: încuietori, pază și spații securizate

Permiteți-mi să vă dau un exemplu din lumea reală. În 2017, breșa de la Equifax a expus informațiile personale a 147 de milioane de americani. Mai recent, **breșa 23andMe (2023)** a expus date genetice sensibile a aproape 7 milioane de utilizatori prin intermediul testării automate de credențiale (credential stuffing). Lecția de aici este că confidențialitatea necesită vigilență constantă atât asupra sistemelor, cât și asupra accesului utilizatorilor.

Integritatea

Integritatea înseamnă asigurarea faptului că informațiile rămân exacte, complete și nealterate, cu excepția modificărilor efectuate de părțile autorizate. Când protejăm integritatea, prevenim modificarea neautorizată a datelor.

Luați în considerare un sistem de înregistrări medicale. Dacă un pacient este alergic la penicilină, această informație trebuie să rămână exactă în fișa sa medicală. Dacă un atacator sau o eroare software ar modifica acea înregistrare, consecințele ar putea fi fatale. De aceea contează integritatea.

Integritatea este amenințată de:

- **Atacuri de tip man-in-the-middle**: un atacator interceptează și modifică datele în tranzit
- **Software malițios**: viruși sau viermi care corup sau modifică fișiere
- **Amenințări din interior**: angajați care modifică intenționat înregistrări
- **Defecțiuni hardware**: erori de disc care cauzează coruperea datelor
- **Erori software**: erori de programare care modifică neintenționat datele

Protejăm integritatea prin:

- **Hashing**: crearea unei amprente digitale a datelor pentru a detecta modificări
- **Semnături digitale**: verificarea criptografică a sursei și integrității datelor
- **Controlul versiunilor**: urmărirea tuturor modificărilor pentru a detecta schimbări neautorizate
- **Controale de acces**: limitarea celor care pot modifica datele
- **Sume de control (checksum)**: verificarea matematică a faptului că datele nu au fost alterate

Iată un exemplu care ilustrează importanța integrității. În 2010, viermele Stuxnet a vizat instalațiile nucleare iraniene. Nu a furat date; în schimb, a modificat instrucțiunile trimise centrifugelor, făcându-le să se rotească la viteze incorecte, în timp ce afișa operatorilor valori normale. Acesta a fost un atac asupra integrității cu consecințe fizice. Centrifugele s-au autodistrus, întârziind programul nuclear al Iranului cu ani.

Disponibilitatea

Disponibilitatea înseamnă asigurarea faptului că informațiile și sistemele sunt accesibile utilizatorilor autorizați atunci când este necesar. Când protejăm disponibilitatea, prevenim întreruperea serviciului.

Imaginați-vă că trebuie să retrageți bani de la un bancomat, dar sistemele băncii nu funcționează. Sau luați în considerare un spital în care medicii nu pot accesa fișele pacienților în timpul unei urgențe. Disponibilitatea înseamnă asigurarea faptului că sistemele funcționează atunci când aveți nevoie de ele.

Disponibilitatea este amenințată de:

- **Atacuri de tip Denial of Service (DoS)**: supraîncărcarea sistemelor cu trafic pentru a le face indisponibile
- **Atacuri de tip Distributed Denial of Service (DDoS)**: atacuri DoS din mai multe surse simultan
- **Ransomware**: software malițios care criptează datele, făcându-le indisponibile până la plata unei răscumpărări
- **Defecțiuni hardware**: căderea serverelor, defectarea discurilor, întreruperi de rețea
- **Dezastre naturale**: inundații, incendii, cutremure care deteriorează infrastructura
- **Pene de curent**: întreruperi ale alimentării cu energie electrică care opresc sistemele

Protejăm disponibilitatea prin:

- **Redundanță**: existența unor sisteme de rezervă gata să preia funcțiile dacă sistemele principale cedează
- **Copii de siguranță (backup)**: copii periodice ale datelor stocate separat de original. Obiectivul timpului de recuperare (RTO) este critic aici; copiile de rezervă sunt inutile dacă restaurarea durează săptămâni (așa cum s-a văzut în recentele atacuri ransomware precum MGM Resorts).
- **Planificarea recuperării în caz de dezastru**: proceduri pentru restabilirea operațiunilor după un incident major
- **Echilibrarea încărcăturii (load balancing)**: distribuirea traficului pe mai multe servere
- **Atenuarea DDoS**: sisteme concepute pentru a absorbi sau devia atacurile masive de trafic

Permiteți-mi să vă ofer un exemplu privind disponibilitatea. În 2016, botnetul Mirai a întrerupt servicii majore de internet prin DDoS. Mai dramatic, **pana CrowdStrike (2024)** (CrowdStrike este un furnizor de soluții de securitate a punctelor terminale) a arătat cum o

singură actualizare software defectuoasă ar putea bloca milioane de sisteme Windows la nivel global, consemnând la sol zboruri și oprind spitale. Acest lucru a demonstrat că amenințările la adresa disponibilității pot proveni de la furnizori de încredere, nu doar de la atacatori.

Echilibrarea triadei

Iată ceva important de înțeles: aceste trei proprietăți intră adesea în conflict una cu alta. Îmbunătățirea uneia o poate afecta uneori pe alta.

De exemplu, pentru a maximiza confidențialitatea, ați putea cripta toate datele și solicita mai multe forme de autentificare. Dar aceasta ar putea afecta disponibilitatea, deoarece utilizatorii autorizați ar putea întâmpina dificultăți în a accesa rapid datele de care au nevoie.

Pentru a maximiza disponibilitatea, ați putea elimina toate controalele de acces și stoca datele pe multe servere. Dar aceasta ar distruge confidențialitatea, deoarece oricine ar putea accesa orice.

Profesioniștii în securitate trebuie să echilibreze constant aceste cerințe concurente în funcție de contextul specific și toleranța la risc a organizației lor. Nu există un răspuns universal corect.

Partea 3: Dincolo de Triada CID – Proprietăți suplimentare de securitate

Deși Triada CID ne-a servit bine timp de decenii, cerințele moderne de securitate s-au extins. Să discutăm trei proprietăți suplimentare care sunt acum considerate esențiale.

Autentificarea

Autentificarea este procesul de verificare a faptului că cineva sau ceva este cine sau ce pretinde a fi. Înainte de a putea aplica orice control de acces, trebuie mai întâi să știți cine face solicitarea.

Autentificarea implică de obicei trei factori primari:

- **Ceva ce știți**: o parolă sau un cod PIN
- **Ceva ce aveți**: un smart card, telefon sau un token de securitate
- **Ceva ce sunteți**: date biometrice precum amprentele digitale sau recunoașterea facială

Sistemele moderne utilizează, de asemenea, **atribute contextuale** (uneori numite "Ceva ce faceți" sau "Undeva unde vă aflați") pentru a spori securitatea fără a necesita acțiuni explicite din partea utilizatorului:

- **Locație**: coordonate GPS sau geolocalizare IP

- **Comportament**: ritmul de tastare, modele de mișcare a mouse-ului sau momentul zilei

Autentificarea multi-factor (MFA) combină doi sau mai mulți dintre acești factori. Când vă conectați la bancă și primiți un mesaj text cu un cod, utilizați doi factori: ceva ce știți (parola) și ceva ce aveți (telefonul). Atributele contextuale sunt adesea folosite pentru **autentificarea bazată pe risc (RBA)** pentru a decide dacă sunt necesare provocări suplimentare.

Non-repudiereaasigură că un Subiect nu poate nega o acțiune sau inacțiune anterioară. Aceasta oferă dovada originii (expeditorul nu poate nega trimiterea) și dovada livrării (destinatarul nu poate nega primirea), mergând dincolo de simplele contracte legale

Non-repudierea înseamnă că o parte nu poate nega efectuarea unei acțiuni. Dacă semnați un contract, non-repudierea garantează că nu puteți pretinde ulterior că nu l-ați semnat.

În lumea digitală, non-repudierea se realizează prin semnături digitale și jurnalizare completă. Când un director aprobă o tranzacție financiară cu semnătura sa digitală, nu poate nega ulterior că a aprobat-o, deoarece dovezile criptografice demonstrează implicarea sa.

Non-repudierea este crucială pentru:

- Probe legale în instanță
- Trasee de audit pentru conformitate
- Responsabilitate în tranzacțiile financiare
- Prevenirea fraudei

Responsabilitatea

Responsabilitatea înseamnă posibilitatea de a urmări acțiunile până la entitatea care le-a efectuat. Fiecare acțiune dintr-un sistem ar trebui să fie atribuibilă unui utilizator sau proces specific.

Responsabilitatea necesită:

- Autentificare puternică pentru identificarea utilizatorilor
- Jurnalizare completă pentru înregistrarea acțiunilor
- Stocare securizată a jurnalelor pentru prevenirea modificării lor
- Revizuirea periodică a jurnalelor pentru detectarea anomaliilor

Fără responsabilitate, este imposibil să investigați incidentele, să aplicați politicile sau să trageți persoanele la răspundere pentru acțiunile lor.

Partea 4: Active, amenințări, vulnerabilități și riscuri

Să discutăm acum patru concepte interconectate care sunt fundamentale pentru analiza de securitate: activele, amenințările, vulnerabilitățile și riscurile.

Activele

Un **activ** este orice lucru de valoare pe care o organizație dorește să îl protejeze. Activele pot fi tangibile sau intangibile.

Active tangibile includ:

- Servere și calculatoare
- Echipamente de rețea
- Clădiri și facilități
- Documente fizice

Active intangibile includ:

- Date și baze de date
- Software și aplicații
- Proprietate intelectuală
- Reputația brandului
- Încrederea clienților

Când efectuăm analiza de securitate, trebuie mai întâi să identificăm ce încercăm să protejăm. Nu puteți securiza ceea ce nu știți că aveți.

Amenințările

O **amenințare** este orice cauză potențială a unui incident nedorit care ar putea dăuna unui activ sau organizației. Amenințările pot fi intenționate sau accidentale, interne sau externe.

Amenințări externe intenționate:

- Hackeri care urmăresc câștiguri financiare
- Actori statali care desfășoară spionaj
- Hactiviști care fac declarații politice
- Competitori care fură secrete comerciale

Amenințări interne intenționate:

- Angajați nemulțumiți care sabotează sisteme

- Persoane din interior care fură date pentru vânzare
- Contractori care depășesc accesul autorizat

Amenințări accidentale:

- Angajați care accesează link-uri de phishing
- Administratori care configurează incorect sistemele
- Dezvoltatori care introduc erori

Amenințări de mediu:

- Dezastre naturale
- Pene de curent
- Defecțiuni hardware

Vulnerabilitățile

O **vulnerabilitate** este o slăbiciune care poate fi exploatată de o amenințare pentru a obține acces neautorizat sau a cauza daune. Vulnerabilitățile există în sisteme, procese și persoane.

Vulnerabilități tehnice:

- Software neactualizat cu defecte de securitate cunoscute
- Paravane de protecție configurate incorect care permit trafic neautorizat
- Algoritmi de criptare slabi care pot fi sparți
- Parole implicite care nu au fost niciodată schimbate

Vulnerabilități de proces:

- Lipsa politicilor de securitate
- Instruire insuficientă a angajaților
- Proceduri inadecvate de răspuns la incidente
- Lipsa revizuirilor de acces

Vulnerabilități umane:

- Susceptibilitate la inginerie socială
- Tendința de a folosi parole slabe
- Neraportarea activităților suspecte
- Neglijența în respectarea procedurilor

Riscurile

Riscul este potențialul de pierdere sau daună atunci când o amenințare exploatează o vulnerabilitate. Riscul se calculează de obicei astfel:

Risc = Amenințare x Vulnerabilitate x Impact

Sau, uneori simplificat:

Risc = Probabilitate x Impact

Unde probabilitatea este șansa ca o amenințare să exploateze o vulnerabilitate, iar impactul este consecința dacă aceasta se produce.

Să ilustrez cu un exemplu. Presupuneți că organizația voastră folosește un server web care rulează software vechi cu o vulnerabilitate cunoscută. Amenințarea o reprezintă hackerii care ar putea exploata această vulnerabilitate. Vulnerabilitatea este software-ul neactualizat. Riscul depinde de cât de probabil este ca atacatorii să găsească și să exploateze această vulnerabilitate și ce daune ar putea cauza.

Dacă serverul este pe internetul public și conține date ale cardurilor de credit ale clienților, riscul este foarte ridicat. Dacă serverul este pe o rețea izolată și conține doar materiale de marketing publice, riscul este mult mai scăzut.

Înțelegerea riscului ne permite să prioritizăm eforturile de securitate. Nu putem proteja totul în mod egal, așa că trebuie să ne concentrăm mai întâi pe riscurile cele mai mari.

Partea 5: Incidente de securitate vs. breșe de securitate

Studenții confundă adesea acești termeni, așa că să îi clarificăm.

Un **incident de securitate** este orice eveniment care compromite potențial confidențialitatea, integritatea sau disponibilitatea unui activ informațional. Incidentele includ:

- Tentative de atac, chiar dacă sunt nereușite
- Încălcări ale politicilor
- Defecțiuni ale sistemelor
- Activități suspecte

O **breșă de securitate** este un incident de securitate care are ca rezultat accesul neautorizat confirmat la date, aplicații, servicii, rețele sau dispozitive. Toate breșele sunt incidente, dar nu toate incidentele sunt breșe.

Iată un exemplu: dacă cineva încearcă să se conecteze la contul vostru cu o parolă incorectă, acesta este un incident. Dacă reușește să se conecteze fără autorizare, aceasta este o breșă.

Organizațiile trebuie să detecteze, să răspundă și să învețe atât din incidente, cât și din breșe. Procedurile de răspuns la incidente, pe care le vom aborda ulterior în acest curs, definesc modul de gestionare a acestor situații.

Partea 6: Apărarea în profunzime

Apărarea în profunzime este o strategie de securitate care utilizează mai multe straturi de protecție. Dacă un strat cedează, celelalte rămân pentru a asigura securitatea. Acest concept provine din strategia militară, unde castelele aveau șanțuri, ziduri, turnuri și gărzi înarmate, fiecare strat făcând penetrarea mai dificilă.

În securitatea informațională, apărarea în profunzime include:

Stratul fizic: gărzi, încuietori, garduri, camere de supraveghere

Stratul perimetral: paravane de protecție, sisteme de detecție a intruziunilor, zone demilitarizate

Stratul de rețea: segmentarea rețelei, VPN-uri, liste de control al accesului

Stratul gazdei: software antivirus, paravane de protecție la nivel de gazdă, gestionarea actualizărilor

Stratul aplicației: validarea datelor de intrare, practici de programare securizată, paravane de protecție pentru aplicații web

Stratul datelor: criptare, controale de acces, prevenirea pierderii datelor

Stratul uman: instruire privind conștientizarea securității, politici, verificarea antecedentelor

Arhitectura Zero Trust: În timp ce apărarea tradițională în profunzime se bazează pe un perimetru puternic, **Zero Trust** presupune că rețeaua este deja compromisă. Acesta funcționează pe principiul "nu avea niciodată încredere, verifică întotdeauna". Fiecare cerere de acces este complet autentificată, autorizată și criptată înainte de a acorda acces, indiferent de unde provine.

Fiecare strat adresează amenințări diferite și oferă protecție suplimentară. Un atacator trebuie să penetreze mai multe straturi pentru a ajunge la activele valoroase, făcând atacurile reușite mult mai dificile.

Partea 7: Securitate prin proiectare și securitate implicită

Două principii ne ghidează în modul în care ar trebui să construim sisteme securizate de la început.

Securitatea prin proiectare (security by design) înseamnă luarea în considerare a securității pe parcursul întregului ciclu de viață al dezvoltării, nu ca o măsură ulterioară. Când arhitecții proiectează o clădire, includ ieșirile de urgență și sistemele de stingere a incendiilor de la început. Nu le adaugă după ce construcția este finalizată. Același principiu se aplică

sistemelor informaționale. **Modelarea amenințărilor**: O abordare structurată (folosind cadre precum **STRIDE**) pentru identificarea amenințărilor în faza de colectare a cerințelor

- Decizii de arhitectură securizată
- **Testarea securității**: Analiza periodică a codului și teste de penetrarelor în faza de colectare a cerințelor
- Decizii de arhitectură securizată
- Testarea securității pe parcursul dezvoltării
- Revizuiri de securitate înainte de implementare

Securitatea implicită (security by default) înseamnă că sistemele ar trebui să fie securizate în configurația lor implicită. Utilizatorii nu ar trebui să fie nevoiți să activeze caracteristicile de securitate; ar trebui să fie nevoiți să le dezactiveze în mod explicit, dacă doresc.

Exemple de securitate implicită:

- Parole solicitate imediat după instalare
- Servicii de rețea dezactivate, cu excepția cazului în care sunt activate explicit
- Criptare activată implicit
- Privilegii minime acordate implicit

Abordarea opusă, în care sistemele sunt livrate nesecurizate și utilizatorii trebuie să configureze securitatea, duce la nenumărate vulnerabilități deoarece mulți utilizatori nu modifică niciodată setările implicite.

Partea 8: Aplicații practice

Să închei cu câteva aplicații practice ale celor învățate astăzi.

Scenariul 1: Proiectarea unei noi aplicații

Când organizația voastră dezvoltă un nou portal pentru clienți, ar trebui să:

1. Identificați activele: datele clienților, credențialele de autentificare, înregistrările tranzacțiilor
2. Identificați amenințările: hackeri, persoane din interior rău intenționate, expunere accidentală
3. Identificați vulnerabilitățile: potențial de injecție SQL, autentificare slabă, jurnalizare insuficientă
4. Calculați riscurile: risc ridicat de furt al datelor clienților
5. Aplicați controale: criptați datele (confidențialitate), validați intrările (integritate), implementați servere redundante (disponibilitate)

6. Implementați apărarea în profunzime: paravan de protecție, WAF, programare securizată, criptare, monitorizare

Scenariul 2: Evaluarea unui furnizor

Când selectați un furnizor cloud, întrebați:

- Cum protejează confidențialitatea? (Criptare, controale de acces)
- Cum asigură integritatea? (Sume de control, controlul versiunilor)
- Care este SLA-ul lor de disponibilitate? (Garanții de funcționare, redundanță)
- Cum gestionează incidentele? (Proceduri de răspuns, notificare)
- Ce certificări dețin? (ISO 27001, SOC 2)

Scenariul 3: Răspunsul la o tentativă de phishing

Dacă un angajat primește un e-mail suspect:

1. Nu accesați link-uri și nu descărcați atașamente
2. Raportați echipei de securitate (acesta este un incident)
3. Echipa de securitate analizează amenințarea
4. Dacă credențialele au fost compromise, devine o breșă
5. Implementați controale suplimentare (instruire, filtrarea e-mailurilor)
6. Documentați lecțiile învățate

Partea 9: Instrumente moderne de gestionare a riscurilor (EASM & GRC)

1. Gestionarea Suprafeței Externe de Atac (EASM)

Instrumentele EASM sunt concepute pentru a descoperi riscurile "necunoscute". Ele scanează internetul din exterior (așa cum ar face un atacator) pentru a găsi fiecare activ digital pe care o organizație îl deține—inclusiv servere uitate, bucket-uri cloud sau IT-ul din umbră (shadow IT).

- **Obiectiv principal:** Descoperirea și cartografierea vulnerabilităților dintr-o perspectivă externă.
- **Exemple cheie:**
- **IONIX:** Se concentrează pe cartografierea suprafeței "reale" de atac, inclusiv lanțuri complexe de aprovizionare digitală și dependențe cloud.
- **UpGuard / SecurityScorecard:** Oferă un "scor de securitate" (similar unui scor de credit) pentru organizația voastră și furnizorii voștri terți.

- **Public țintă:** Ingineri de securitate, echipe de informații despre amenințări.
- **Analogie: Inspectorul de clădiri.** Acesta se plimbă în exteriorul clădirii căutând crăpături, ferestre deschise și încuietori stricate despre care nu știați că există.

2. Guvernanță, Risc și Conformitate (GRC)

Instrumentele GRC sunt "registrele" interne ale securității. Ele urmăresc politicile, auditurile și riscurile cunoscute. Ele ajută la asigurarea faptului că organizația respectă legile (precum GDPR) sau standardele (precum ISO 27001).

- **Obiectiv principal:** Urmărirea conformității, documentarea riscurilor interne și gestionarea auditurilor.
- **Exemple cheie:**
- **RSA Archer:** O platformă tradițională, de nivel enterprise, pentru gestionarea riscului corporativ și a conformității.
- **OneTrust:** Puternic concentrată pe riscul de confidențialitate și guvernanța datelor.
- **Public țintă:** CISO, ofițeri de risc, manageri de conformitate.
- **Analogie: Dulapul cu dosare.** Acesta stochează planurile, rapoartele de inspecție și certificatele care dovedesc că clădirea este legal conformă codului.

Avantaje și dezavantaje

Categorie	Avantaje	Dezavantaje
EASM	Găsește amenințări tehnice imediate; aproape că nu necesită configurare manuală pentru a începe scanarea.	Poate genera "zgomot" (fals pozitive); nu vă spune cum să reparați politica din spatele riscului.
GRC	Centralizează toate datele de risc; esențial pentru trecerea auditurilor și cerințelor legale.	Povară administrativă grea; se bazează pe introducerea manuală a datelor ("garbage in, garbage out").

Concluzie

Astăzi am acoperit conceptele fundamentale care formează baza securității informaționale:

1. **Securitatea informațională vs. securitatea cibernetică**: InfoSec protejează toate informațiile; securitatea cibernetică se concentrează pe sistemele electronice
2. **Triada CID**: Confidențialitatea, Integritatea și Disponibilitatea sunt cei trei piloni ai securității
3. **Proprietăți suplimentare**: Autentificarea, non-repudierea și responsabilitatea extind modelul de bază

4. **Active, amenințări, vulnerabilități și riscuri**: Înțelegerea acestor relații permite planificarea eficientă a securității
5. **Incidente vs. breșe**: Incidentele sunt compromisuri potențiale; breșele sunt acces neautorizat confirmat
6. **Apărarea în profunzime**: Mai multe straturi de protecție oferă reziliență
7. **Securitate prin proiectare și implicită**: Integrați securitatea de la început

În lecția următoare, vom explora în detaliu peisajul amenințărilor, examinând cine ne atacă, de ce o face și ce metode utilizează. Vom discuta, de asemenea, despre cadre precum MITRE ATT&CK care ne ajută să înțelegem și să categorisim amenințările.

Aveți întrebări înainte de a încheia?

Întrebări de discuție

1. În ce scenarii ar putea intra în conflict proprietățile triadei CID și cum ar trebui organizațiile să rezolve astfel de conflicte?
2. Cum schimbă principiul "securității prin proiectare" modul în care abordăm dezvoltarea software comparativ cu abordările tradiționale?
3. Care sunt cele mai mari provocări cu care se confruntă organizațiile în implementarea apărării în profunzime și cum pot fi abordate?

Vă mulțumesc pentru atenție. Ne vedem la următoarea sesiune.

Întrebări de recapitulare

1. Explicați diferența dintre securitatea informațională și securitatea cibernetică. Cum se suprapun și cum diferă ariile lor de acoperire?
2. Definiți cele trei componente ale triadei CID și oferiți un exemplu din lumea reală în care fiecare este preocuparea principală.
3. Cum extind autentificarea, non-repudierea și responsabilitatea modelul de bază CID?
4. Descrieți relația dintre active, amenințări, vulnerabilități și riscuri. Cum ajută înțelegerea acestui lanț în planificarea securității?
5. Care este diferența dintre un incident de securitate și o breșă de securitate? De ce contează această distincție?
6. Explicați strategia apărării în profunzime și oferiți exemple de controale la trei niveluri diferite.

7. Ce înseamnă "securitate prin proiectare" și cum diferă de adăugarea securității după implementare?
8. Dați un exemplu de scenariu în care două elemente ale triadei CID intră în conflict.

Termeni-cheie

- **Responsabilitate (Accountability)**: Proprietatea care asigură că acțiunile unei entități pot fi urmărite în mod unic până la acea entitate
- **Activ (Asset)**: Orice lucru de valoare pentru o organizație, inclusiv date, hardware, software și personal
- **Autentificare (Authentication)**: Procesul de verificare a unei identități declarate
- **Disponibilitate (Availability)**: Asigurarea că utilizatorii autorizați au acces oportun și fiabil la informații și resurse
- **Breșă (Breach)**: Un incident confirmat în care datele sunt accesate sau dezvăluite fără autorizare
- **Triada CID (CIA Triad)**: Cele trei obiective fundamentale de securitate: Confidențialitate, Integritate și Disponibilitate
- **Confidențialitate (Confidentiality)**: Prevenirea dezvăluirii neautorizate a informațiilor
- **Securitate cibernetică (Cybersecurity)**: Protecția sistemelor electronice, rețelelor și datelor împotriva atacurilor
- **Apărare în profunzime (Defense in Depth)**: O strategie de securitate care utilizează mai multe straturi de controale
- **Incident (Incident)**: O compromitere potențială sau tentată a politicilor sau practicilor de securitate
- **Securitatea informațională (Information Security)**: Protecția informațiilor în toate formele împotriva accesului, utilizării, dezvăluirii sau distrugerii neautorizate
- **Integritate (Integrity)**: Asigurarea că datele nu au fost modificate în mod neautorizat
- **Non-repudiere (Non-repudiation)**: Garanția că cineva nu poate nega efectuarea unei acțiuni
- **Risc (Risk)**: Potențialul de pierdere rezultat dintr-o amenințare care exploatează o vulnerabilitate
- **Securitate implicită (Security by Default)**: Sisteme livrate cu cea mai securizată configurație ca setare implicită
- **Securitate prin proiectare (Security by Design)**: Integrarea securității în sisteme din cele mai timpurii etape de proiectare
- **Amenințare (Threat)**: O cauză potențială a unui incident nedorit care poate rezulta în daune

- **Vulnerabilitate (Vulnerability)**: O slăbiciune într-un sistem care poate fi exploatată de o amenințare

Referințe și lecturi suplimentare

Pentru cei interesați de o explorare mai aprofundată:

- ISO/IEC 27000:2022 pentru definiții formale ale termenilor de securitate
- NIST Glossary of Key Information Security Terms