Fișa de documentare

Tema 2. Dezvoltarea unei politici de securitate în rețea

1. Principiile securității informației

Principiu	**Semnificație și exemplu**
Confidențialitate	Informația este accesibilă numai persoanelor autorizate. Exemplu: acces restricționat la dosarele elevilor.
Integritate	Datele sunt protejate împotriva modificării sau distrugerii neautorizate. Exemplu: detectarea alterării unui document.
Disponibilitate	Datele și serviciile sunt accesibile atunci când utilizatorii autorizați au nevoie de ele. Exemplu: restaurarea după o defecțiune.
Autentificare și autorizare	Autentificarea verifică identitatea declarată; autorizarea stabilește operațiile permise. Un cont valid nu oferă automat acces la toate resursele.
Trasabilitate și nerepudiere	Jurnalele ajută la reconstituirea acțiunilor. Semnăturile digitale pot susține dovada originii și integrității; valoarea probatorie depinde și de gestionarea cheilor și de context.

2. Amenințări și riscuri în rețea

O amenințare poate produce un prejudiciu; o vulnerabilitate este o slăbiciune care poate fi exploatată. Riscul se evaluează luând în considerare probabilitatea și impactul asupra activității. Sursele pot fi externe sau interne, intenționate ori accidentale. Testarea de securitate autorizată trebuie deosebită de accesul neautorizat.

Amenințare	**Efect posibil**	**Măsuri de reducere**
Spam și phishing	Mesaje nedorite sau înșelătoare; furt de date și credențiale.	Filtrare, instruire și verificarea solicitărilor printr-un canal cunoscut.
Malware și ransomware	Executarea de cod malițios, furtul ori criptarea datelor.	Actualizări, protecție endpoint, limitarea privilegiilor și copii de siguranță testate.
Compromiterea conturilor	Acces folosind parole furate, reutilizate sau ghicite.	Parole unice, MFA și monitorizarea autentificărilor.
Spoofing	Falsificarea unei identități sau a originii unui mesaj.	Validarea identității; pentru e-mail, SPF, DKIM și DMARC.
Interceptare și alterare	Citirea traficului sau modificarea datelor în tranzit.	Canale criptate și autentificate, validarea certificatelor.

Amenințare	Efect posibil	Măsuri de reducere
Acces neautorizat	Exploatarea serviciilor expuse ori a configurărilor greșite.	Firewall, segmentare, actualizări și revizuirea permisiunilor.
DoS și DDoS	Supraîncărcarea și indisponibilitatea serviciilor.	Limitarea traficului, redundanță și protecție coordonată cu furnizorul.
Erori și incidente fizice	Ștergere accidentală, furt, incendiu sau întreruperea energiei.	Control fizic, protecția alimentării și proceduri de recuperare.

Precizări importante

Spam nu înseamnă automat phishing. Un mesaj poate părea credibil chiar dacă este fraudulos. SPF, DKIM și DMARC reduc anumite forme de falsificare a domeniului, dar nu garantează că mesajul este sigur sau că un cont legitim nu a fost compromis.

Codul malițios poate fi livrat prin atașamente, macrocomenzi, aplicații și extensii compromise sau vulnerabilități. JavaScript nu este în sine un virus. Referințele la appleturi Java și ActiveX nu mai constituie o bază adecvată pentru prezentarea securității navigatoarelor moderne.

3. Soluții de protecție pe mai multe niveluri

Apărarea în profunzime combină măsuri care previn, detectează și limitează incidentele. Nici antivirusul, nici firewallul, nici criptarea nu asigură singure securitatea unei rețele.

3.1 Dispozitive și infrastructură

- Inventarierea calculatoarelor, echipamentelor de rețea, aplicațiilor și serviciilor cloud; eliminarea componentelor fără suport sau izolarea lor justificată.
- Actualizarea sistemelor, aplicațiilor și firmware-ului, cu prioritate pentru vulnerabilitățile exploatate și serviciile expuse la internet.
- Configurări sigure, dezactivarea serviciilor inutile, controlul instalării aplicațiilor și protecție antivirus sau EDR. EDR detectează comportamente suspecte și sprijină investigarea și răspunsul.

3.2 Rețea și comunicații

- Firewallul permite sau blochează traficul după reguli documentate. Segmentarea separă utilizatorii, serverele, oaspeții și dispozitivele IoT și limitează propagarea unui incident.
- Accesul de la distanță se acordă prin soluții aprobate, cu autentificare puternică și permisiuni limitate. Apartenența la rețeaua internă nu trebuie să fie singurul motiv pentru acordarea încrederii.
- Comunicațiile folosesc protocoale criptate și autentificate, precum HTTPS/TLS și SSH. Criptarea protejează conținutul interceptat; nu împiedică fizic interceptarea și nu securizează un dispozitiv deja compromis.

3.3 Date și continuitate

- Datele se clasifică după sensibilitate; accesul, partajarea și păstrarea se stabilesc în funcție de această clasificare. Cheile de criptare se protejează separat de date.
- Copiile de siguranță trebuie protejate, inclusiv prin copii offline sau imuabile, iar restaurarea trebuie testată. Sincronizarea fișierelor nu înlocuiește automat un backup independent. [3]

- Jurnalele și alertele trebuie analizate de persoane desemnate. Accesul fizic la echipamente, cabluri și spațiile tehnice trebuie controlat.

4. Parole și autentificare multifactor

Conform NIST SP 800-63B-4, parola folosită ca unic factor trebuie să aibă minimum 15 caractere; în MFA este permis un minimum de 8 caractere. Acestea sunt praguri, nu o garanție de securitate. Sunt recomandate parole lungi, unice și un manager de parole. Ghidul nu cere combinații obligatorii de majuscule, cifre și simboluri și exclude schimbarea periodică fără motiv; schimbarea este necesară când există dovezi de compromitere.

MFA combină factori diferiți: ceva ce știi, ceva ce deții sau o caracteristică biometrică. Două parole nu reprezintă MFA. Se preferă metode rezistente la phishing, precum cheile de securitate și passkeys implementate corespunzător. Codurile de recuperare trebuie păstrate în siguranță.

5 Elaborarea politicii de securitate

Politica stabilește ce trebuie protejat, cine răspunde și ce reguli se aplică. Procedurile descriu cum se execută aceste reguli. Un document util leagă cerințele de riscuri și precizează cum se verifică respectarea lor.

5.1 Etapele de lucru

1. Inventarierea și delimitarea domeniului. Se includ dispozitivele, utilizatorii, datele, serviciile cloud, accesul de la distanță și furnizorii relevanți.
2. Evaluarea riscurilor. Se identifică resursele critice, amenințările și punctele slabe; măsurile se prioritizează după impact și probabilitate.
3. Stabilirea regulilor. Se definesc accesul, utilizarea acceptabilă, actualizările, protecția datelor, backupul, monitorizarea și raportarea incidentelor.
4. Atribuirea responsabilităților. Conducerea aprobă politica și resursele; administratorii implementează măsurile; utilizatorii respectă regulile și raportează problemele.
5. Implementarea și instruirea. Se configurează controalele, se comunică procedurile și se verifică dacă utilizatorii știu să le aplice.
6. Verificarea și revizuirea. Se testează măsurile și recuperarea, se urmăresc indicatorii și se actualizează politica după incidente sau schimbări importante.

NIST CSF 2.0 organizează managementul securității în șase funcții: Guvernare, Identificare, Protejare, Detectare, Răspuns și Recuperare. Acestea susțin un proces continuu, adaptat organizației. [2]

5.2 Structura minimă a documentului de politică

Componentă	Conținut de precizat
Identificare	Titlu, versiune, responsabil, aprobator, data intrării în vigoare și data revizuirii.
Scop și domeniu	Resursele, persoanele și activitățile la care se aplică.
Reguli și roluri	Cerințe verificabile, responsabilități și modul de acordare sau retragere a accesului.
Incidente și continuitate	Canal de raportare, persoane de contact, priorități și proceduri de recuperare.

Componentă	Conținut de precizat
Excepții și verificare	Justificare, aprobare, termen de expirare, măsuri compensatorii și dovezi ale verificărilor.

5.3 Exemple de indicatori

Procentul conturilor administrative cu MFA; numărul vulnerabilităților critice restante; procentul restaurărilor testate cu succes; timpul până la raportarea și tratarea unui incident. Țintele și termenele se stabilesc în funcție de riscurile și resursele organizației.

6. Aplicare într-un laborator informatic

Exemplele următoare pot fi adaptate într-o politică pentru laborator. Ele sunt reguli propuse, care trebuie aprobate și configurate pentru mediul concret.

- Fiecare utilizator primește un cont individual, cu drepturi limitate la activitățile necesare. Conturile administrative sunt separate de cele utilizate curent.
- Instalarea programelor și modificarea configurărilor de securitate sunt permise numai persoanelor autorizate. Echipamentele personale și mediile USB se folosesc conform regulilor laboratorului.
- Rețeaua pentru oaspeți este separată de resursele interne. Accesul la fișiere se acordă pe roluri și se retrage când nu mai este necesar.
- Administratorul verifică actualizările, alertele și copiile de siguranță. Politica stabilește explicit frecvența verificărilor și persoana care le confirmă.

6.1 Reacția la un incident suspect

Utilizatorul oprește interacțiunea cu mesajul sau aplicația suspectă și anunță imediat responsabilul desemnat. Nu șterge dovezile și nu încearcă remedieri improvizate. Personalul autorizat izolează sistemele afectate, păstrează jurnalele, investighează cauza, elimină compromiterea și validează recuperarea înainte de reconectare. Planul trebuie exersat.

6.2 Verificarea înțelegerii

1. De ce o parolă corectă nu îi permite utilizatorului accesul la orice fișier?
2. Cum ajută backupul la disponibilitate și de ce trebuie testată restaurarea?
3. Ce diferență există între un firewall și o soluție EDR?
4. Pentru un cont compromis, propune două măsuri preventive și două acțiuni de răspuns.