Contents

CAPITOLUL 3. MITIGATING THREATS

3.0 Introduction

3.0.1 - Motivatie

Apărarea rețelei este treaba unui profesionist în securitate.

- *Cum poți să fie informat cu privire la actualul climat de Securitate ?*
- *Ce organizații pot ajuta să fim informati cu privire la cele mai recente riscuri și instrumente ?*
- *Ce legătură au ceapa și anghinarea cu securitatea ?*

3.0.2 - Obiective

Cunoasterea instrumentelor și procedurilor pentru a atenua efectele cauzate de malware și atacurile comune de rețea.

Topic Title	Topic Objective
Defending the Network	Descrierea metodelor și resurselor pentru protejarea rețelei.
Network Security Policies	Explicarea mai multor tipuri de politici de securitate a rețelei.
Secure the Network	Cunoasterea scopului platformelor de securitate.
Mitigating Common Network Attacks	Descrierea tehnicilor utilizate pentru a atenua atacurile comune de rețea.
Cisco Network Foundation Protection Framework	Explicarea modului de securizare a celor trei zone funcționale ale routerelor și comutatoarelor Cisco.

3.1 Defending the Network

3.1.1 - Network Security Professionals

Organizațiile se confruntă cu pierderi de productivitate atunci când rețelele lor sunt lente sau nu răspund. Obiectivele de afaceri și profiturile sunt afectate negativ de pierderea și coruperea datelor. Prin urmare, din perspectiva afacerilor, este necesar să se minimizeze efectele hackerilor cu intenții rele.

Profesioniștii în securitatea rețelei sunt responsabili de menținerea asigurării datelor pentru o organizație și de asigurarea integrității și confidențialității informațiilor. În mod ironic, hacking-ul a avut efectul neintenționat de a crea o cerere mare de profesioniști în securitatea

rețelei. Ca urmare a creșterii exploatărilor hackerilor, a sofisticarii instrumentelor pentru hackeri și din cauza legislației guvernamentale, soluțiile de securitate a rețelei s-au dezvoltat rapid în anii 1990, creând noi oportunități de muncă în domeniul securității rețelei.

Rolurile de muncă de specialist în securitate în cadrul unei întreprinderi includ Chief Information Officer (CIO), Chief Information Security Officer (CISO), Manager Operațiuni de securitate (SecOps), Chief Security Officer (CSO), Manager de securitate și Inginer de securitate a rețelei. Indiferent de titlurile postului, profesioniștii în securitatea rețelei trebuie să fie întotdeauna cu un pas înaintea hackerilor:

- *Ei trebuie să-și îmbunătățească în mod constant setul de abilități pentru a fi la curent cu cele mai recente amenințări.*
- *Ei trebuie să participe la cursuri și ateliere de lucru.*
- *Ei trebuie să se aboneze la fluxuri în timp real privind amenințările.*
- *Ei trebuie să examineze site-urile web de securitate în fiecare zi.*
- *Aceștia trebuie să păstreze familiaritatea cu organizațiile de securitate a rețelei. Aceste organizații au adesea cele mai recente informații despre amenințări și vulnerabilități.*

Organizația Cyber Security Education descrie o serie de cariere în domeniul securității cibernetice și oferă resurse care pot ajuta in pregătirea pentru acele cariere.

Notă: În comparație cu alte profesii din tehnologie, securitatea rețelei are o curbă de învățare foarte abruptă și necesită un angajament pentru dezvoltarea profesională continuă.

3.1.2 - Network Intelligence Communities

Pentru a proteja eficient o rețea, profesioniștii în securitate trebuie să fie informați cu privire la amenințări și vulnerabilități pe măsură ce acestea evoluează. Există multe organizații de securitate care oferă informații despre rețea. Ei oferă resurse, ateliere și conferințe pentru a ajuta profesioniștii în securitate. Aceste organizații au adesea cele mai recente informații despre amenințări și vulnerabilități.

Mai jos sunt enumerate câteva organizații importante de securitate a rețelei.

SANS - Resursele Institutului SysAdmin, Audit, Network, Security (SANS) sunt în mare parte gratuite la cerere și includ:

- *Internet Storm Center - popularul sistem de avertizare timpurie pe internet*

- *NewsBites, rezumatul săptămânal al articolelor de știri despre securitatea computerelor.*
- *@RISK, rezumatul săptămânal al vectorilor de atac nou descoperiți, vulnerabilități cu exploit-uri active și explicații despre cum au funcționat atacurile recente*
- *Alerte de securitate flash*
- *Sala de lectură - peste 1.200 de lucrări de cercetare originale premiate.*
- *SANS dezvoltă și cursuri de securitate.*

Mitre - Mitre Corporation menține o listă de vulnerabilități și expuneri comune (CVE) utilizate de organizațiile de securitate proeminente, ceea ce le face mai ușor să partajeze date. CVE servește ca un dicționar de nume comune (adică, identificatori CVE) pentru vulnerabilitățile cunoscute de securitate cibernetică.

FIRST - Forum of Incident Response and Security Teams (FIRST) este o organizație de securitate care reunește o varietate de echipe de răspuns la incidente de securitate informatică din organizații guvernamentale, comerciale și educaționale pentru a promova cooperarea și coordonarea în schimbul de informații, prevenirea incidentelor și reacția rapidă.

SecurityNewsWire - Un portal de știri de securitate care reunește cele mai recente știri de ultimă oră referitoare la alerte, exploatări și vulnerabilități.

$(ISC)^2$ - Consorțiul Internațional de Certificare a Securității Sistemelor Informaționale (ISC^2) oferă produse educaționale neutre și servicii de carieră pentru mai mult de 75.000 de profesioniști din industrie din peste 135 de țări.

CIS - Centrul pentru Securitate pe Internet (CIS) este un punct central pentru prevenirea, protecția, răspunsul și recuperarea amenințărilor cibernetice pentru guvernele de stat, locale, tribale și teritoriale (SLTT) prin Centrul Multi-State de Partajare și Analiză a Informațiilor (MS-ISAC).). MS-ISAC oferă avertismente și consiliere 24x7 pentru amenințări cibernetice, identificarea vulnerabilităților și atenuarea și răspunsul la incidente.

Pentru a rămâne eficient, un profesionist în securitatea rețelei trebuie să:

Fie la curent cu cele mai recente amenințări – Aceasta activitate include abonarea la fluxuri în timp real referitoare la amenințări, consultarea periodică a site-urilor web legate de securitate, urmărirea blogurilor și podcas-urilor de securitate și multe altele.

Îmbunătățirea continua a abilităților - Aceasta include participarea la cursuri, ateliere și conferințe legate de securitate.

Notă: Securitatea rețelei are o curbă de învățare foarte abruptă și necesită un angajament pentru dezvoltarea profesională continuă.

3.1.3 - Network Security Certifications

Sute de mii de locuri de muncă legate de securitatea rețelei rămân neocupate în fiecare an. Cererea de profesioniști în securitatea rețelei depășește cu mult numărul de solicitanți calificați. Obținerea certificărilor recunoscute de securitate a rețelei îmbunătățește considerabil calificările pentru aceste posturi. Există numeroase certificări.

Certificarile pentru profesioniștii în securitatea rețelei sunt oferite de următoarele organizații:

- *Certificare globală de asigurare a informațiilor (GIAC)*
- *Consorțiul Internațional de Certificare a Securității Sistemelor Informaționale (ISC)*[2]
- *Asociația de Audit și Control al Sistemelor Informaționale (ISACA)*
- *Consiliul Internațional al Consultanților în Comerț E-E (CE-Council)*
- *Certified Wireless Security Professional (CWSP)*

Cisco a înlocuit certificarea Cisco Certified Network Associate Security (210-260 IINS) cu o nouă certificare CCNP Security. Această certificare constă din două examene, un examen de bază de securitate și un examen de concentrare. Este necesar un singur examen de concentrare. Examenul de implementare și operare Cisco Security Core Technologies (350-701 SCOR) servește ca o poartă de acces la certificările CCNP și CCIE de securitate. De asemenea, oferă certificare de bază de securitate. Examenul de bază acoperă concepte de securitate, amenințări și tehnici și tehnologii de atenuare. Specializările se concentrează în profunzime pe tehnologiile specifice de securitate Cisco. Examenele de concentrare de securitate Cisco Certified Specialist sunt după cum urmează:

- ***300-710 SNCF - Network Security Firepower***
- ***300-715 SISE - Implementarea și configurarea Cisco Identity Services Engine***
- ***300-720 SESA - Securizarea e-mailului cu Cisco Email Security Appliance***
- ***300-725 SWSA - Securizarea Web-ului cu Cisco Web Security Appliance***
- ***300-730 SVPN - Implementarea soluțiilor securizate cu rețele private virtuale***
- ***300-735 SAUTO - Automatizarea și programarea soluțiilor de securitate Cisco***

Există multe modalități de pregătire pentru aceste certificări, inclusiv auto-studiu, învățământ cu examen privat și învățământ superior. Organizația Learning at Cisco, împreună

cu partenerii săi de învățare, oferă informații și instruire pentru majoritatea examenelor de certificare Cisco.

3.1.4 - Communications Security: CIA

Securitatea informațiilor se ocupă cu protejarea informațiilor și a sistemelor de informații împotriva accesului, utilizării, dezvăluirii, întreruperii, modificării sau distrugerii neautorizate. Triada CIA servește ca fundație conceptuală pentru domeniu.

Figura arată Triada CIA constând din Confidențialitate, Integritate și Disponibilitate.

Fig. 3.1. Triada CIA.

După cum se arată în figură, triada CIA constă din trei componente ale securității informațiilor:

1. ***Confidențialitate*** *- Numai persoanele, entitățile sau procesele autorizate pot accesa informațiile sensibile.*
2. ***Integritate*** *- Aceasta se referă la protecția datelor împotriva modificărilor neautorizate.*
3. ***Disponibilitate*** *- Utilizatorii autorizați trebuie să aibă acces neîntrerupt la resursele și datele de rețea de care au nevoie.*

Datele din rețea pot fi criptate (făcute nelizibile pentru utilizatorii neautorizați) folosind diverse aplicații de criptare. Conversația dintre doi utilizatori de telefoane IP poate fi criptată. Fișierele de pe un computer pot fi, de asemenea, criptate. Acestea sunt doar câteva exemple.

Criptografia poate fi folosită aproape oriunde există comunicare de date. De fapt, tendința este ca toate comunicațiile să fie criptate.

3.2 Network Security Policies

3.2.1 - Network Security Domains

Este vital ca profesioniștii în securitatea rețelei să înțeleagă motivele securității rețelei. De asemenea, trebuie să fie familiarizați cu cerințele organizaționale pentru securitatea rețelei, așa cum sunt încorporate de cele 14 domenii de securitate a rețelei.

Domeniile oferă un cadru pentru discutarea securității rețelei și înțelegerea nevoilor operaționale care ar trebui să fie abordate de fiecare organizație.

Există 14 domenii de securitate a rețelei specificate de Organizația Internațională pentru Standardizare (ISO)/Comisia Electrotehnică Internațională (IEC). Descrise de ISO/IEC 27001, aceste 14 domenii servesc la organizarea, la un nivel înalt, a vastului tărâm al informațiilor și activităților sub umbrela securității rețelei. Aceste domenii au unele paralele semnificative cu domeniile definite de certificarea Certified Information Systems Security Professional (CISSP).

Cele 14 domenii sunt destinate să servească drept bază comună pentru dezvoltarea standardelor de securitate organizațională și a practicilor eficiente de management al securității. Ele ajută, de asemenea, la facilitarea comunicării între organizații.

Aceste 14 domenii oferă o separare convenabilă a elementelor de securitate a rețelei. Deși nu este important să sse memoreze aceste 14 domenii, este important să conștientizam existența lor și declarația oficială de către ISO. În standardul ISO 27001, acestea sunt cunoscute ca cele 14 seturi de control din anexa A. Ele vor servi ca referință utilă în munca unui profesionist în securitatea rețelei.

1. ***Information Security Policies*** *- Această anexă este concepută pentru a se asigura că politicile de securitate sunt create, revizuite și menținute.*
2. ***Organization of Information Security*** *- Acesta este modelul de guvernanță stabilit de o organizație pentru securitatea informațiilor. Atribuie responsabilități pentru sarcinile de securitate a informațiilor în cadrul unei organizații.*
3. ***Human Resources Security*** *- Aceasta se referă la responsabilitățile de securitate legate de angajații care se alătură, se mută / părăsesc o organizație.*

4. ***Asset Management*** *- Aceasta se referă la modul în care organizațiile creează un inventar și o schemă de clasificare a activelor informaționale.*
5. ***Access Control*** *- Aceasta descrie restricția drepturilor de acces la rețele, sisteme, aplicații, funcții și date.*
6. ***Cryptography*** *- Aceasta se referă la criptarea datelor și la gestionarea informațiilor sensibile pentru a proteja confidențialitatea, integritatea și disponibilitatea datelor.*
7. ***Physical and Environmental Security*** *- Aceasta descrie protecția instalațiilor și echipamentelor fizice de calculator din cadrul unei organizații.*
8. ***Operations Security*** *- Acesta descrie gestionarea controalelor tehnice de securitate în sisteme și rețele, inclusiv apărarea împotriva programelor malware, backupul datelor, înregistrarea și monitorizarea, gestionarea vulnerabilităților și considerațiile de audit. Acest domeniu este, de asemenea, preocupat de integritatea software-ului care este utilizat în operațiunile de afaceri.*
9. ***Communications Security*** *- Aceasta se referă la securitatea datelor, așa cum sunt comunicate în rețele, atât în cadrul unei organizații, cât și între organizație și terți, cum ar fi clienții sau furnizorii.*
10. ***System Acquisition, Development, and Maintenance*** *- Acest lucru asigură că securitatea informațiilor rămâne o preocupare centrală în procesele unei organizații de-a lungul întregului ciclu de viață, atât în rețelele private, cât și în cele publice.*
11. ***Supplier Relationships*** *- Aceasta se referă la specificarea acordurilor contractuale care protejează informațiile și activele tehnologice ale unei organizații care sunt accesibile de către terți care furnizează bunuri și servicii organizației.*
12. ***Information Security Incident Management*** *- Acesta descrie cum să se anticipeze și să se răspunda la încălcările securității informațiilor.*
13. ***Business Continuity Management*** *- Acesta descrie protecția, întreținerea și recuperarea proceselor și sistemelor critice pentru afaceri.*
14. ***Compliance*** *- Acesta descrie procesul de asigurare a conformității cu politicile, standardele și reglementările de securitate a informațiilor.*

3.2.2 - Business Policies

Politicile de afaceri sunt liniile directoare care sunt dezvoltate de o organizație pentru a-și guverna acțiunile. Politicile definesc standarde de comportament corect pentru afacere și pentru angajații săi.

În rețea, politicile definesc activitățile care sunt permise în rețea. Aceasta stabilește o bază de utilizare acceptabilă. Dacă în rețea este detectat un comportament care încalcă politica de afaceri, este posibil să fi avut loc o încălcare a securității.

O organizație poate avea mai multe politici de ghidare, așa cum sunt enumerate mai jos:

Company policies - Aceste politici stabilesc regulile de conduită și responsabilitățile atât ale angajaților, cât și ale angajatorilor.

Politicile protejează drepturile lucrătorilor, precum și interesele de afaceri ale angajatorilor.

În funcție de nevoile organizației, diverse politici și proceduri stabilesc reguli privind conduita angajaților, prezența, codul vestimentar, confidențialitatea și alte domenii legate de termenii și condițiile de angajare.

Employee policies - Aceste politici sunt create și menținute de personalul de resurse umane pentru a identifica salariul angajaților, programul de plată, beneficiile angajaților, programul de lucru, vacanțele și multe altele.

Acestea sunt adesea furnizate noilor angajați pentru a le revizui și semna.

Security policies - Aceste politici identifică un set de obiective de securitate pentru o companie, definesc regulile de comportament pentru utilizatori și administratori și specifică cerințele de sistem.

Aceste obiective, reguli și cerințe asigură în mod colectiv securitatea unei rețele și a sistemelor informatice dintr-o organizație.

La fel ca un plan de continuitate, o politică de securitate este un document în continuă evoluție, bazat pe schimbări în peisajul amenințărilor, vulnerabilități și cerințele de afaceri și ale angajaților.

3.2.3 - Security Policy

O politică de securitate cuprinzătoare are o serie de beneficii, inclusiv următoarele:

i. *Demonstrează angajamentul unei organizații față de securitate*
ii. *Stabilește regulile pentru comportamentul așteptat*

iii. *Asigură consecvența în operațiunile sistemului, achiziția și utilizarea software-ului și hardware-ului și întreținerea*

iv. *Definește consecințele juridice ale încălcărilor*

v. *Oferă personalului de securitate sprijinul conducerii*

Politicile de securitate sunt folosite pentru a informa utilizatorii, personalul și managerii cu privire la cerințele unei organizații pentru protejarea activelor tehnologice și informaționale. O politică de securitate specifică, de asemenea, mecanismele care sunt necesare pentru a îndeplini cerințele de securitate și oferă o linie de bază de la care să se achiziționeze, să se configureze și să se auditeze sistemele și rețelele de computere pentru conformitate.

Politicile care pot fi incluse într-o politică de Securitate sunt:

Identification and authentication policy - Specifică persoanele autorizate care pot avea acces la resursele rețelei și la procedurile de verificare a identității.

Password policies - Se asigură că parolele îndeplinesc cerințele minime și sunt schimbate în mod regulat.

Acceptable Use Policy (AUP) - Identifică aplicațiile și utilizările de rețea care sunt acceptabile pentru organizație. De asemenea, poate identifica ramificații dacă această politică este încălcată.

Remote access policy - Identifică modul în care utilizatorii de la distanță pot accesa o rețea și ce este accesibil prin conectivitate de la distanță.

Network maintenance policy - Specifică sistemele de operare ale dispozitivelor de rețea și procedurile de actualizare a aplicațiilor pentru utilizatorul final.

Incident handling procedures - Descrie modul în care sunt gestionate incidentele de securitate.

Una dintre cele mai comune componente ale politicii de securitate este un AUP. Aceasta poate fi denumită și o politică de utilizare adecvată. Această componentă definește ce utilizatorii au voie și ce nu au voie să facă asupra diferitelor componente ale sistemului. Aceasta include tipul de trafic care este permis în rețea. AUP ar trebui să fie cât mai explicit posibil pentru a evita neînțelegerile.

De exemplu, un AUP ar putea enumera anumite site-uri web, grupuri de știri sau aplicații cu lățime de bandă intensivă care nu pot fi accesate de computerele companiei sau din rețeaua

companiei. Fiecărui angajat ar trebui să li se ceară să semneze un AUP, iar AUP-urile semnate ar trebui păstrate pe durata angajării.

3.2.4 - BYOD Policies

Multe organizații trebuie să accepte acum și Bring Your Own Device (BYOD). Acest lucru le permite angajaților să-și folosească propriile dispozitive mobile pentru a accesa sistemele, software-ul, rețelele sau informațiile companiei.

BYOD oferă mai multe beneficii cheie întreprinderilor, inclusiv productivitate crescută, costuri reduse de IT și operare, mobilitate mai bună pentru angajați și atractivitate mai mare atunci când vine vorba de angajarea și păstrarea angajaților.

Cu toate acestea, aceste beneficii aduc, de asemenea, un risc crescut de securitate a informațiilor, deoarece BYOD poate duce la încălcări ale datelor și la o mai mare răspundere pentru organizație.

Ar trebui dezvoltată o politică de securitate BYOD pentru a realiza următoarele:

- *Specificarea obiectivelor programului BYOD.*
- *Identificarea angajaților care își pot aduce propriile dispozitive.*
- *Identificarea dispozitivelor ce vor fi acceptate.*
- *Identificarea nivelului de acces acordat angajaților atunci când folosesc dispozitive personale.*
- *Descrierea drepturilor de acces și activităților permise personalului de securitate de pe dispozitiv.*
- *Identificarea reglementărilor ce trebuie respectate atunci când sunt utilizate dispozitivele angajaților.*
- *Identificarea măsurilor de siguranță de pus în aplicare dacă un dispozitiv este compromis.*

Printre cele mai bune practici de securitate BYOD pentru a ajuta la atenuarea vulnerabilităților BYOD pot fi:

Password protected access - Utilizarea parolelor unice pentru fiecare dispozitiv și cont.

Manually control wireless connectivity - Oprirea conexiunilor Wi-Fi și Bluetooth atunci când nu sunt în uz. Conectarea numai la rețele de încredere.

Keep updated – Păstrarea, întotdeauna, sistemului de operare actualizat al dispozitivului și alte programe software. Software-ul actualizat conține adesea corecții de securitate pentru a atenua cele mai recente amenințări sau exploatări.

Back up data - Activarea backup-ul dispozitivului în cazul în care acesta este pierdut sau furat.

Enable "Find my Device" - Abonarea la un serviciu de localizare a dispozitivelor cu funcție de ștergere de la distanță.

Provide antivirus software – Furnizare de software antivirus pentru dispozitivele BYOD aprobate.

Use Mobile Device Management (MDM) software - Software-ul MDM permite echipelor IT să implementeze setări de securitate și configurații software pe toate dispozitivele care se conectează la rețelele companiei.

3.2.5 - Regulatory and Standards Compliance

Există și reglementări externe privind securitatea rețelei. Profesioniștii în securitatea rețelelor trebuie să fie familiarizați cu legile și codurile de etică care sunt obligatorii pentru profesioniștii în securitatea sistemelor informaționale (INFOSEC).

Multe organizații sunt mandatate să dezvolte și să implementeze politici de securitate. Reglementările de conformitate definesc ce organizații sunt responsabile pentru furnizarea și răspunderea în cazul în care nu se conformează. Reglementările de conformitate pe care o organizație este obligată să le respecte depind de tipul de organizație și de datele pe care organizația le gestionează.

3.3 Security Tools, Platforms, and Services

3.3.1 - The Security Onion and The Security Artichoke

Security Onion - O analogie comună folosită pentru a descrie o abordare de apărare în profunzime este numită „ceapa de securitate". După cum este ilustrat în figură, un actor de amenințare ar trebui să dezlipească nivelul de apărare al unei rețele, într-un mod similar cu curățarea unei cepe. Numai după ce a pătruns fiecare nivel, actorul amenințării va ajunge la datele sau sistemul țintă.

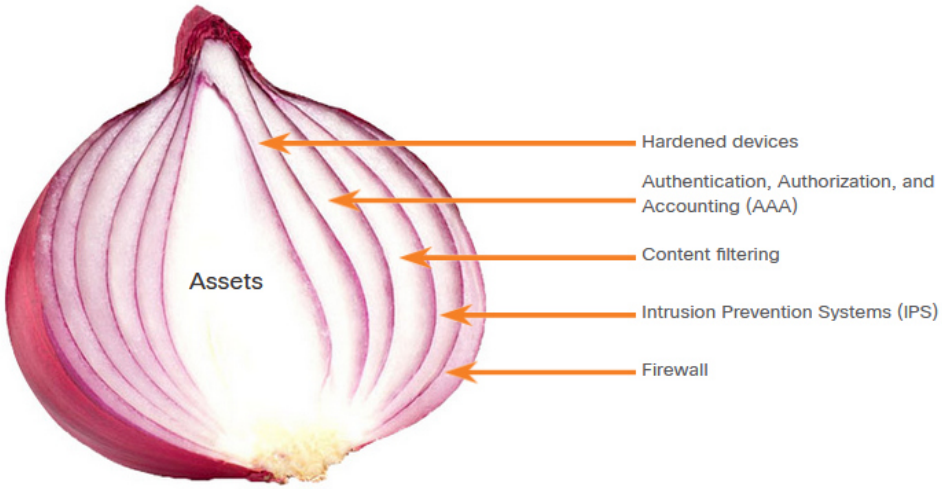

Fig. 3.2. Comparatie nivelurilor de aparare si distributia foilor de ceapa.

Figura cu ceapă de securitate arată o ceapă cu diferite niveluri în interior. Ceapa este etichetată drept bun. În dreapta sunt cuvinte și săgeți care indică diferitele niveluri:

- ***dispozitive întărite;***
- ***autentificare, autorizare și contabilitate (A A A);***
- ***filtrarea continutului;***
- ***sisteme de prevenire a intruziunilor (I P S);***
- ***firewall.***

Notă: Ceapa de securitate descrisă în această pagină este o modalitate de a vizualiza apărarea în profunzime. Acest lucru nu trebuie confundat cu suita Security Onion de instrumente de securitate a rețelei.

Security Artichoke - Peisajul în schimbare al rețelelor, cum ar fi evoluția rețelelor fără granițe, a schimbat această analogie cu „anghinarea de securitate”, de care beneficiază actorul amenințării.

După cum este ilustrat în figură, actorii amenințărilor nu mai trebuie să dezlipească fiecare strat. Trebuie doar să îndepărteze anumite „frunze de anghinare”. Bonusul este că fiecare „frunză” a rețelei poate dezvălui date sensibile care nu sunt bine securizate.

De exemplu, este mai ușor pentru un actor de amenințare să compromită un dispozitiv mobil decât să compromită un computer sau un server intern care este protejat de niveluri de apărare. Fiecare dispozitiv mobil este o frunză. Și frunză după frunză, totul îl conduce pe hacker la mai multe date. Inima anghinării este locul unde se găsesc cele mai confidențiale date. Fiecare frunză oferă un nivel de protecție, oferind simultan o cale de atac.

Nu toate frunzele trebuie îndepărtate pentru a ajunge în miezul anghinării. Hackerul scoate armura de securitate de-a lungul perimetrului pentru a ajunge la „inima” întreprinderii.

În timp ce sistemele care se confruntă cu internet sunt de obicei foarte bine protejate, iar protecțiile limitelor sunt de obicei solide, hackerii persistenti, ajutați de un amestec de pricepere și noroc, găsesc în cele din urmă un gol în acel exterior dur prin care pot intra și merge unde doresc.

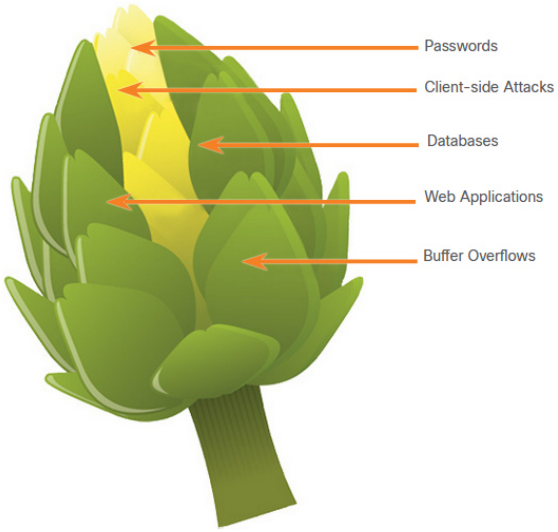

Fig. 3.3. Security Artichoke.

Figura cu anghinare de securitate arată o anghinare cu diferite secțiuni în interiorul ei. Cuvintele din dreapta au o săgeată care indică secțiunile individuale ale anghinării:

- *parole;*
- *atacuri din partea clientului;*
- *baze de date;*
- *aplicații web;*
- *suprascrierea memoriei tampon.*

3.3.2 - Security Testing Tools

Hackingul etic implică utilizarea multor tipuri diferite de instrumente pentru a testa rețeaua și dispozitivele finale. Pentru a valida securitatea unei rețele și a sistemelor acesteia, au fost dezvoltate multe instrumente de testare a securității rețelei. Testarea de penetrare implică utilizarea tehnicilor și instrumentelor hackerilor pentru a evalua puterea măsurilor de

securitate a rețelei. Cu toate acestea, multe dintre aceste instrumente pot fi utilizate și de către actorii amenințărilor pentru exploatare.

Actorii amenințărilor au creat și diverse instrumente de hacking. Aceste instrumente sunt scrise în mod explicit din motive nefaste. De asemenea, personalul de securitate cibernetică trebuie să știe cum să folosească aceste instrumente atunci când efectuează teste de penetrare în rețea.

Notă: Multe dintre aceste instrumente sunt bazate pe UNIX sau Linux; prin urmare, un profesionist în securitate ar trebui să aibă un fundal puternic UNIX și Linux.

password crackers - Parolele sunt cea mai vulnerabilă amenințare de securitate. Instrumentele de spargere a parolelor sunt adesea denumite instrumente de recuperare a parolei și pot fi folosite pentru a sparge sau recupera parola. Acest lucru se realizează fie prin eliminarea parolei originale, după ocolirea criptării datelor, fie prin descoperirea completă a parolei. Descoperitorii de parole fac în mod repetat presupuneri pentru a sparge parola și a accesa sistemul. Exemple de instrumente de spargere a parolelor includ John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack și Medusa.

wireless hacking tools - Rețelele wireless sunt mai susceptibile la amenințările la securitatea rețelei. Instrumentele de hacking fără fir sunt folosite pentru a sparge în mod intenționat o rețea fără fir pentru a detecta vulnerabilitățile de securitate. Exemple de instrumente de hacking wireless includ Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep și NetStumbler.

network scanning and hacking tools - Instrumentele de scanare a rețelei sunt folosite pentru a sonda dispozitivele de rețea, serverele și gazdele pentru porturi TCP sau UDP deschise. Exemple de instrumente de scanare includ Nmap, SuperScan, Angry IP Scanner și NetScanTools.

packet crafting tools - Instrumentele de creare a pachetelor sunt folosite pentru a proba și a testa robustețea unui firewall folosind pachete forjate special concepute. Exemple de astfel de instrumente includ Hping, Scapy, Socat, Yersinia, Netcat, Nping și Nemesis.

packet sniffers - Instrumentele de mirosire (sniffer) de pachete sunt folosite pentru a captura și analiza pachete în rețelele LAN sau WLAN tradiționale Ethernet. Instrumentele includ Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy și SSLstrip.

rootkit detectors - Un detector de rootkit este un verificator de integritate a directoarelor și fișierelor folosit de pălăriile albe pentru a detecta kiturile root instalate. Exemple de instrumente includ AIDE, Netfilter și PF: OpenBSD Packet Filter.

fuzzers to search vulnerabilities - Fuzzers sunt instrumente folosite de actorii amenințărilor atunci când încearcă să descopere vulnerabilitățile de securitate ale unui sistem informatic. Exemple de fuzzere includ Skipfish, Wapiti și W3af.

forensic tools - Hackerii cu pălărie albă folosesc instrumente criminalistice pentru a adulmeca orice urmă de dovezi existente într-un anumit sistem informatic. Exemple de instrumente includ Sleuth Kit, Helix, Maltego și Encase.

Debuggers - Instrumentele de depanare sunt folosite de black hats pentru a face inginerie inversă a fișierelor binare atunci când scrieți exploit-uri. Ele sunt, de asemenea, folosite de pălăriile albe atunci când analizează programele malware. Instrumentele de depanare includ GDB, WinDbg, IDA Pro și Immunity Debugger.

hacking operating systems - Sistemele de operare de hacking sunt sisteme de operare special concepute, preîncărcate cu instrumente și tehnologii optimizate pentru hacking. Exemple de sisteme de operare special concepute pentru hacking includ Kali Linux, SELinux, Knoppix, Parrot OS și BackBox Linux.

encryption tools - Aceste instrumente protejează conținutul datelor unei organizații atunci când acestea sunt stocate sau transmise. Instrumentele de criptare folosesc scheme de algoritmi pentru a codifica datele pentru a preveni accesul neautorizat la date. Exemple de aceste instrumente includ VeraCrypt, CipherShed, Open SSH, OpenSSL, OpenVPN și Stunnel.

vulnerability exploitation tools - Aceste instrumente identifică dacă o gazdă la distanță este vulnerabilă la un atac de securitate. Exemple de instrumente de exploatare a vulnerabilităților includ Metasploit, Core Impact, Sqlmap, Social Engineer Tool Kit și Netsparker.

vulnerability scanners - Aceste instrumente scanează o rețea sau un sistem pentru a identifica porturile deschise. Ele pot fi, de asemenea, utilizate pentru a scana vulnerabilități cunoscute și pentru a scana mașini virtuale, dispozitive BYOD și baze de date clienți. Exemple de aceste instrumente includ Nipper, Securia PSI, Core Impact, Nessus, SAINT și Open VAS.

3.3.3 - Data Security Platforms

Platformele de securitate a datelor (DSP) sunt o soluție de securitate integrată care combină instrumente tradiționale independente într-o suită de instrumente care sunt făcute să funcționeze împreună. Instrumentele de securitate care protejează și monitorizează rețelele sunt adesea realizate de diferiți furnizori. Poate fi dificil să se integreze aceste instrumente în așa fel încât să se poată obține o singură viziune asupra securității rețelei. Pot fi necesare resurse semnificative pentru a avea diferite dispozitive și software sub o singură soluție de control. În plus, integrarea datelor din instrumente atât de diverse într-o vizualizare cuprinzătoare de monitorizare a rețelei poate fi foarte dificil de creat și întreținut.

Un astfel de DSP este platforma Helix de la FireEye. FireEye Helix este o platformă de operațiuni de securitate bazată pe cloud, care permite organizațiilor să integreze multe funcționalități de securitate într-o singură platformă. Helix oferă management de evenimente, analiză a comportamentului rețelei, detectare avansată a amenințărilor și orchestrare, automatizare și răspuns (SOAR) pentru securitatea incidentelor pentru răspuns la amenințări pe măsură ce sunt detectate. Helix se bazează, de asemenea, pe informații despre amenințări FireEye Mandiant, răspuns la incident și expertiză în materie de securitate.

Un alt DSP integrat este Cisco SecureX. SecureX face un pas mai departe prin integrarea sa puternică cu portofoliul Cisco Secure. Portofoliul Cisco Secure constă dintr-un set larg de tehnologii care funcționează ca o echipă - oferind interoperabilitate cu infrastructura de securitate, inclusiv tehnologii terțe. Acest lucru are ca rezultat o vizibilitate unificată, automatizare și o apărare mai puternică. Platforma Cisco SecureX funcționează cu diverse produse care se combină pentru a vă proteja rețeaua, utilizatorii și punctele finale, marginea cloudului și aplicațiile. Funcționalitatea SecureX este încorporată într-un portofoliu mare și divers de produse de securitate Cisco, inclusiv firewall-uri de ultimă generație, VPN, analiză de rețea, motor de servicii de identitate, protecție avansată împotriva malware-ului (AMP) și multe alte sisteme care funcționează pentru a securiza toate aspectele unei rețele. . SecureX integrează, de asemenea, o gamă de instrumente de securitate terță parte.

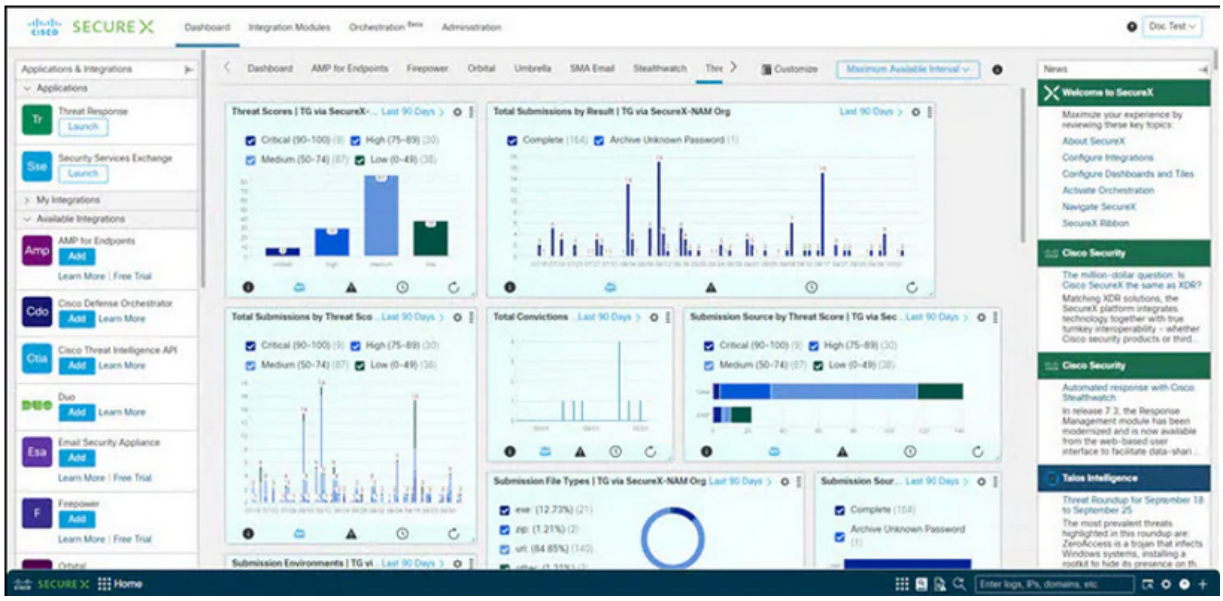

Fig. 3.4. Platforma Securex.

3.3.4 - Security Services

Serviciile de informații despre amenințări și securitate permit schimbul de informații despre amenințări, cum ar fi vulnerabilități, indicatori de compromis (IOC) și tehnici de atenuare. Aceste informații nu sunt partajate doar personalului, ci și sistemelor de securitate. Pe măsură ce apar amenințările, serviciile de informații despre amenințări creează și distribuie reguli de firewall și IOC-uri către dispozitivele care s-au abonat la serviciu.

Un astfel de serviciu este Cisco Talos Threat Intelligence Group, prezentat în figură. Talos este una dintre cele mai mari echipe comerciale de informații despre amenințări din lume și este compusă din cercetători, analiști și ingineri de talie mondială. Scopul Talos este de a ajuta la protejarea utilizatorilor întreprinderii, a datelor și a infrastructurii de adversarii activi. Echipa Talos colectează informații despre amenințările active, existente și emergente. Talos oferă apoi protecție completă împotriva acestor atacuri și malware abonaților săi.

Produsele Cisco Security pot folosi informațiile despre amenințări Talos în timp real pentru a oferi soluții de securitate rapide și eficiente. Cisco Talos oferă, de asemenea, software, servicii, resurse și date gratuite. Talos menține seturile de reguli de detectare a incidentelor de securitate pentru instrumentele de securitate de rețea Snort.org, ClamAV și SpamCop.

Fig. 3.5. TALOS.

O serie de servicii de securitate a rețelei gestionate sunt disponibile de la furnizori precum Cisco, Sentinel Intrusion Prevention Systems, IBM, AT&T și Core Security. Aceste organizații oferă o gamă largă de servicii, inclusiv securitate gestionată ca serviciu (SECcaaS sau SaaS).

3.4 Mitigating Common Network Attacks

3.4.1 - Defending the Network

Vigilență constantă și educație continuă sunt necesare pentru a apăra rețeaua împotriva atacurilor. Următoarele sunt cele mai bune practici pentru securizarea unei rețele:

- *Elaborarea unor politici de securitate scrise pentru companie.*
- *Educarea angajaților referitor la riscurile ingineriei sociale și dezvoltarea strategiilor de validare a identităților prin telefon, prin e-mail sau în persoană.*
- *Controlarea accesului fizic la sisteme.*
- *Folosirea parolelor puternice și schimbarea acestora des.*
- *Criptarea și protejara cu parolă a datelor sensibile.*

- *Implementare hardware și software de securitate, cum ar fi firewall-uri, IPS, dispozitive de rețea privată virtuală (VPN), software antivirus și filtrarea conținutului.*
- *Efectuare de copii de siguranță și testare în mod regulat a fișierelor de rezervă.*
- *Închiderea serviciilor și porturilor inutile.*
- *Păstrarea patch-urile la zi instalându-le săptămânal sau zilnic, dacă este posibil, pentru a se preveni depășirea tamponului și atacurile de escaladare a privilegiilor.*
- *Efectuarea auditurilor de Securitate periodica pentru a testa rețeaua.*

3.4.2 - Mitigating Malware

Programele malware, inclusiv viruși, viermi și cai troieni, pot cauza probleme serioase pe rețele și dispozitivele finale. Administratorii de rețea au mai multe mijloace de a atenua aceste atacuri.

Notă: tehnicile de atenuare sunt adesea denumite în comunitatea de securitate „contramăsuri”.

O modalitate de a atenua atacurile virușilor și cailor troieni este software-ul antivirus. Software-ul antivirus ajută la prevenirea infectării gazdelor și a răspândirii de coduri rău intenționate. Este nevoie de mult mai mult timp pentru a curăța computerele infectate decât pentru a menține software-ul antivirus și definițiile antivirus actualizate pe aceleași mașini.

Software-ul antivirus este cel mai răspândit produs de securitate de pe piață în prezent. Mai multe companii care creează software antivirus, cum ar fi Symantec, McAfee și Trend Micro, se ocupă de detectarea și eliminarea virușilor de mai bine de un deceniu. Multe corporații și instituții de învățământ achiziționează licențe în volum pentru utilizatorii lor. Utilizatorii se pot conecta la un site web cu contul lor și pot descărca software-ul antivirus de pe desktop-urile, laptopurile sau serverele lor.

Produsele antivirus au opțiuni de automatizare a actualizărilor, astfel încât noile definiții de viruși și noile actualizări de software să poată fi descărcate automat sau la cerere. Această practică este cea mai critică cerință pentru menținerea unei rețele fără viruși și ar trebui să fie oficializată într-o politică de securitate a rețelei.

Produsele antivirus sunt bazate pe gazdă. Aceste produse sunt instalate pe computere și servere pentru a detecta și elimina virușii. Cu toate acestea, ele nu împiedică virușii să intre în rețea, așa că un profesionist în securitatea rețelei trebuie să fie conștient de virușii majori și să țină evidența actualizărilor de securitate cu privire la virușii emergenti.

O altă modalitate de a atenua amenințările malware este de a împiedica fișierele malware să intre în rețea. Dispozitivele de securitate din perimetrul rețelei pot identifica fișierele malware cunoscute pe baza indicatorilor lor de compromis. Fișierele pot fi eliminate din fluxul de date primit înainte de a provoca un incident. Din păcate, actorii amenințărilor sunt conștienți de această contramăsură și își modifică frecvent malware-ul suficient de mult încât să evite detectarea. Aceste exploit-uri vor intra în rețea și, de asemenea, vor evita software-ul antivirus. Nicio tehnică de atenuare nu poate fi 100% eficientă. Incidentele de securitate vor avea loc.

3.4.3 - Mitigating Worms

Viermii sunt mai mult bazați pe rețea decât virușii. Atenuarea viermilor necesită consecvență și coordonare din partea profesioniștilor în securitatea rețelei.

După cum se arată în figură, răspunsul la un atac de viermi poate fi împărțit în patru faze: izolare, inoculare, carantină și tratament.

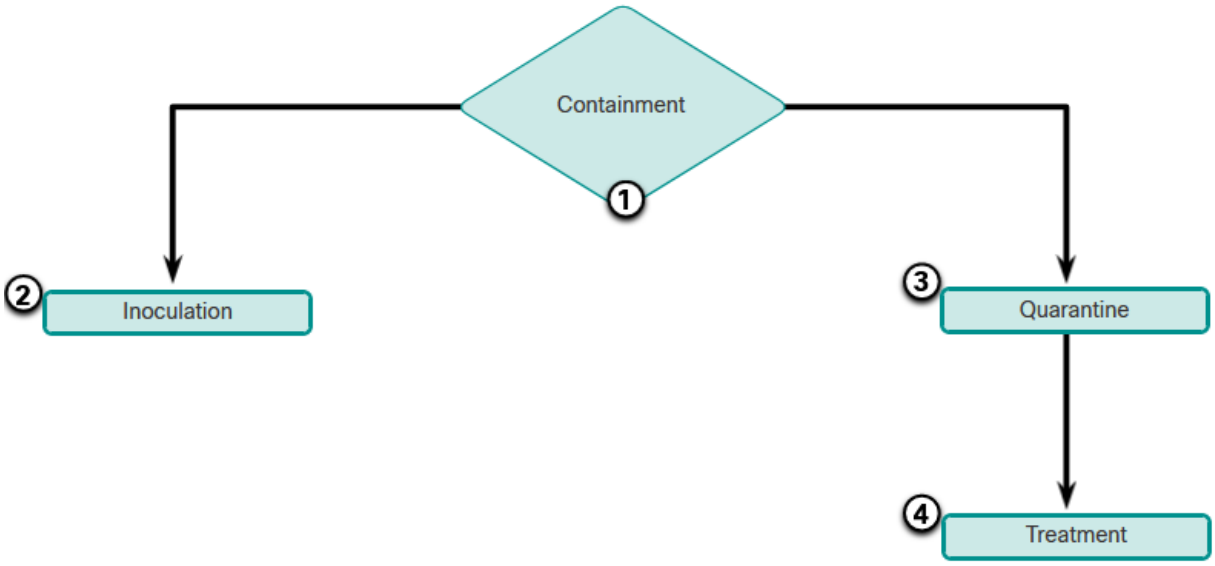

Fig. 3.6. Contramasuri in atac cu virusi.

1. Containment - contaminare - Faza de izolare presupune limitarea răspândirii unei infecții cu viermi în zonele rețelei care sunt deja afectate. Acest lucru necesită compartimentarea și segmentarea rețelei pentru a încetini sau opri viermele și pentru a preveni gazdele infectate în prezent să țintească și să infecteze alte sisteme. Limitarea necesită utilizarea atât a ACL-urilor de ieșire, cât și de intrare pe routere și firewall-uri la punctele de control din rețea.

2. Inoculare – Inoculation - Faza de inoculare se desfășoară paralel cu sau ulterior fazei de izolare. În timpul fazei de inoculare, toate sistemele neinfectate sunt patch-uri cu noutatile

furnizorului corespunzător. Procesul de inoculare privează și mai mult viermele de orice ținte disponibile.

3. Carantină - Quarantine -Faza de carantină implică urmărirea și identificarea mașinilor infectate în zonele conținute și deconectarea, blocarea sau îndepărtarea acestora. Acest lucru izolează aceste sisteme în mod corespunzător pentru faza de tratament.

4. Tratament - Treatment - Faza de tratament presupune dezinfectarea activă a sistemelor infectate. Acest lucru poate implica terminarea procesului de vierme, eliminarea fișierelor modificate sau a setărilor de sistem pe care viermele le-a introdus și corecția vulnerabilității pe care viermele a folosit-o pentru a exploata sistemul. Alternativ, în cazuri mai severe, sistemul poate fi necesar să fie reinstalat pentru a se asigura că viermele și produsele secundare ale acestuia sunt îndepărtate.

3.4.4 - Mitigating Reconnaissance Attacks

Atacurile de recunoaștere sunt de obicei precursorul altor atacuri care au intenția de a obține acces neautorizat la o rețea sau de a perturba funcționalitatea rețelei. Un profesionist în securitatea rețelei poate detecta când este în desfășurare un atac de recunoaștere, primind notificări de la alarme preconfigurate. Aceste alarme sunt declanșate atunci când anumiți parametri sunt depășiți, cum ar fi numărul de solicitări ICMP pe secundă. O varietate de tehnologii și dispozitive pot fi utilizate pentru a monitoriza acest tip de activitate și a genera o alarmă. Dispozitivul Adaptive Security Appliance (ASA) de la Cisco oferă prevenirea intruziunilor într-un dispozitiv autonom. În plus, Cisco ISR acceptă prevenirea intruziunilor bazată pe rețea prin imaginea de securitate Cisco IOS.

Atacurile de recunoaștere pot fi atenuate în mai multe moduri, inclusiv următoarele:

- *Implementarea autentificării pentru a asigura accesul adecvat.*
- *Folosirea criptării pentru a face inutile atacurile de sniffer de pachete.*
- *Utilizarea instrumentelor anti-sniffer pentru a detecta atacurile de sniffer de pachete.*
- *Implementarea unei infrastructuri comutate.*
- *Folosind un firewall și IPS.*

Instrumentele software și hardware anti-sniffer detectează modificări ale timpului de răspuns al gazdelor pentru a determina dacă gazdele procesează mai mult trafic decât ar indica

propriile încărcări de trafic. Deși acest lucru nu elimină complet amenințarea, ca parte a unui sistem general de atenuare, poate reduce numărul de cazuri de amenințare.

Criptarea este, de asemenea, eficientă pentru atenuarea atacurilor de tip sniffer de pachete. Dacă traficul este criptat, folosirea unui sniffer de pachete este de puțin folos, deoarece datele capturate nu pot fi citite.

Este imposibil să se atenueze scanarea portului, dar utilizarea unui sistem de prevenire a intruziunilor (IPS) și a unui firewall poate limita informațiile care pot fi descoperite cu un scanner de porturi. Sweep-urile ping pot fi oprite dacă ecoul ICMP și răspunsul la eco sunt dezactivate pe routerele edge; cu toate acestea, atunci când aceste servicii sunt dezactivate, datele de diagnosticare a rețelei se pierd. În plus, scanările de porturi pot fi executate fără scanări complete de ping. Scanările durează pur și simplu mai mult deoarece sunt scanate și adresele IP inactive.

Fig. 3.7. Reconnaissance Attack Mitigation Techniques.

3.4.5 - Mitigating Access Attacks

Sunt disponibile mai multe tehnici pentru atenuarea atacurilor de acces. Acestea includ securitatea puternică a parolelor, principiul încrederii minime, criptografia, aplicarea sistemului de operare și a corecțiilor aplicației.

Un număr surprinzător de atacuri de acces sunt efectuate prin simpla ghicire a parolelor sau atacuri de dicționar în forță brută împotriva parolelor. Pentru a ne apăra împotriva acestui fapt, se creeaza și se aplica o politică de autentificare puternică care să includă:

- **Utilizare de parole puternice** - Parolele puternice au cel puțin opt caractere și conțin litere mari, litere mici, cifre și caractere speciale.
- ***Dezactivarea conturilor după ce a avut loc un anumit număr de conectări nereușite*** - Această practică ajută la prevenirea încercărilor continue de utilizare a parolei.

De asemenea, rețeaua ar trebui să fie proiectată folosind principiul încrederii minime. Aceasta înseamnă că sistemele nu ar trebui să se folosească unul pe altul în mod inutil. De

exemplu, dacă o organizație are un server de încredere care este utilizat de dispozitive care nu sunt de încredere, cum ar fi serverele web, serverul de încredere nu ar trebui să aibă încredere în dispozitivele care nu sunt de încredere necondiționat.

Criptografia este o componentă critică a oricărei rețele moderne securizate. Se recomandă utilizarea criptării pentru accesul de la distanță la o rețea. Traficul protocolului de rutare ar trebui, de asemenea, să fie criptat. Cu cât traficul este criptat mai mult, cu atât mai puține oportunități au hackerii de a intercepta date cu atacuri de tip man-in-the-middle.

Utilizarea protocoalelor de autentificare criptate sau hashing, împreună cu o politică puternică de parole, reduce foarte mult probabilitatea atacurilor de acces de succes.

În cele din urmă, educarea angajaților cu privire la riscurile inginerii sociale și dezvoltarea strategiilor de validare a identităților prin telefon, prin e-mail sau în persoană. Autentificarea multifactorială (MFA) a devenit din ce în ce mai comună. În această abordare, autentificarea necesită două sau mai multe mijloace independente de verificare. De exemplu, o parolă poate fi combinată cu un cod care este trimis printr-un mesaj text. Software-ul sau dispozitivele separate pot fi folosite pentru a genera jetoane care sunt bune pentru o singură utilizare. Aceste valori de simbol, atunci când sunt furnizate cu o parolă, oferă un nivel suplimentar de securitate care împiedică utilizarea parolelor care au fost ghicite sau furate de actorii amenințărilor.

În general, atacurile de acces pot fi detectate prin revizuirea jurnalelor, utilizarea lățimii de bandă și încărcările proceselor. Politica de securitate a rețelei ar trebui să specifice că jurnalele sunt menținute în mod oficial pentru toate dispozitivele și serverele din rețea. Prin examinarea jurnalelor, personalul de securitate al rețelei poate determina dacă a avut loc un număr neobișnuit de încercări eșuate de conectare.

3.4.6 - Mitigating DoS Attacks

Unul dintre primele semne ale unui atac DoS este un număr mare de plângeri ale utilizatorilor cu privire la resursele indisponibile sau la performanța rețelei neobișnuit de lentă. Pentru a minimiza numărul de atacuri, un pachet software de utilizare a rețelei ar trebui să ruleze în permanență. Analiza comportamentului rețelei poate detecta modele neobișnuite de utilizare care indică faptul că are loc un atac DoS. Un mijloc de detectare a comportamentului neobișnuit al rețelei ar trebui să fie cerut de politica de securitate a rețelei a organizației. Un

grafic de utilizare a rețelei care arată o activitate neobișnuită ar putea indica, de asemenea, un atac DoS.

Atacurile DoS ar putea fi o componentă a unei ofensive mai mari. Atacurile DoS pot duce la probleme în segmentele de rețea ale computerelor atacate. De exemplu, capacitatea de pachete pe secundă a unui router între internet și o rețea LAN ar putea fi depășită de un atac, compromițând nu numai sistemul țintă, ci și dispozitivele de rețea prin care trebuie să treacă traficul. Dacă atacul este efectuat la o scară suficient de mare, regiuni geografice întregi de conectivitate la internet ar putea fi compromise.

Din punct de vedere istoric, multe atacuri DoS au fost provenite din adrese falsificate. Routerele și switch-urile Cisco acceptă o serie de tehnologii anti-spoofing, cum ar fi securitatea porturilor, snoopingul Dynamic Host Configuration Protocol (DHCP), IP Source Guard, Dynamic Address Resolution Protocol (DAI) Inspection și listele de control al accesului (ACL).

3.5 Cisco Network Foundation Protection Framework

3.5.1 - NFP Framework

Cadrul Cisco Network Foundation Protection (NFP) oferă linii directoare complete pentru protejarea infrastructurii de rețea. Aceste linii directoare formează baza pentru furnizarea continuă a serviciilor.

NFP împarte în mod logic routerele și comutatoarele în trei zone funcționale, așa cum se arată în figură:

1. ***Plan de control -*** *Responsabil pentru rutarea corectă a datelor. Traficul planului de control constă din pachete generate de dispozitive necesare pentru funcționarea rețelei în sine, cum ar fi schimburile de mesaje ARP sau anunțurile de rutare OSPF.*
2. ***Plan de management*** *- Responsabil cu gestionarea elementelor de rețea. Traficul planului de management este generat fie de dispozitivele de rețea, fie de stațiile de gestionare a rețelei folosind procese și protocoale precum Telnet, SSH, TFTP, FTP, NTP, AAA, SNMP, syslog, TACACS+, RADIUS și NetFlow.*
3. ***Data plane (Forwarding plane) -*** *Responsabil cu transmiterea datelor. Traficul planului de date constă în mod normal în pachete generate de utilizator care sunt transmise între dispozitivele finale. Majoritatea traficului circulă prin router sau comutator prin intermediul avionului de date.*

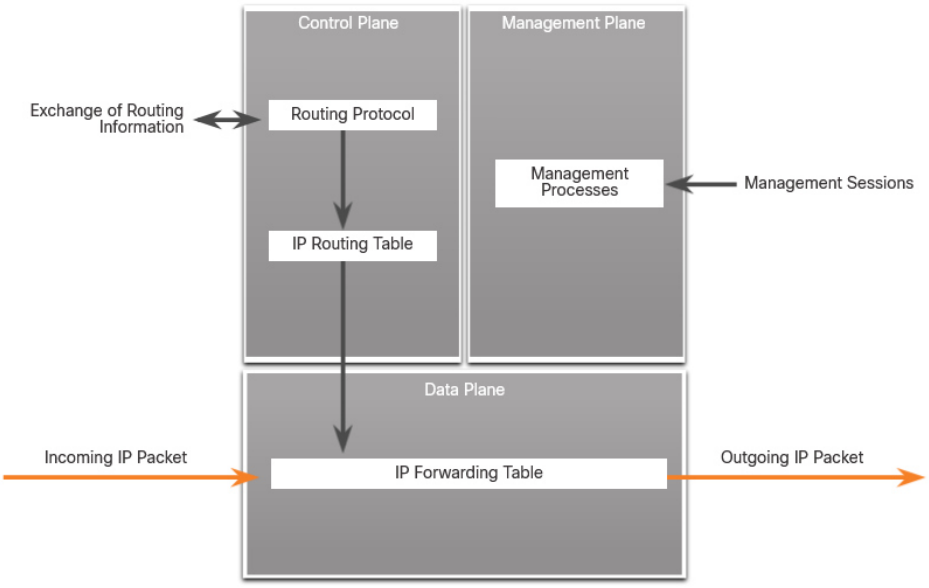

Fig. 3.8. NFP.

3.5.2 - Securing the Control Plane

Traficul planului de control constă din pachete generate de dispozitive necesare pentru funcționarea rețelei în sine.

Securitatea planului de control poate fi implementată folosind următoarele caracteristici, așa cum se arată în figură:

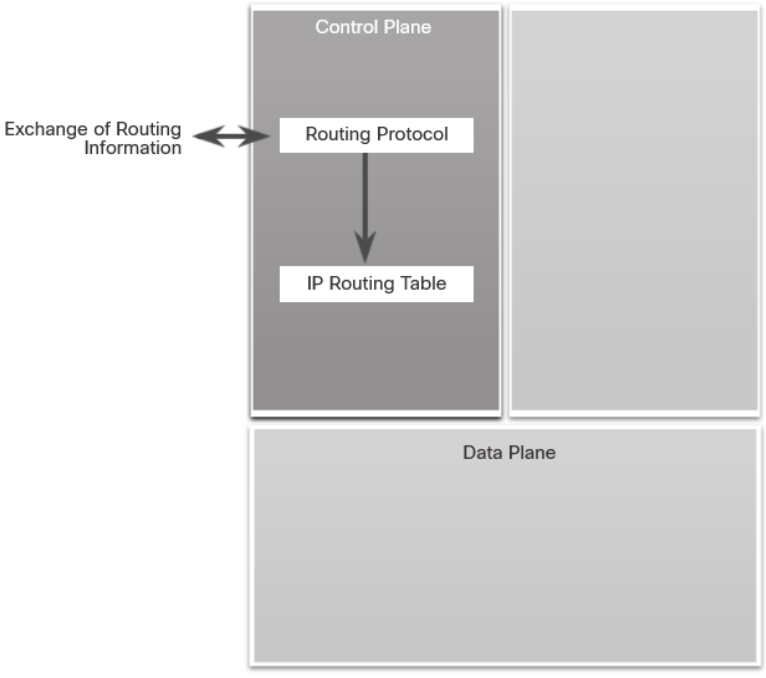

Fig. 3.9. Control Plane.

Autentificarea protocolului de rutare - Autentificarea protocolului de rutare sau autentificarea vecinului împiedică un router să accepte actualizări frauduloase de rutare. Majoritatea protocoalelor de rutare acceptă autentificarea vecinului.

Control Plane Policing (CoPP) - CoPP este o caracteristică Cisco IOS concepută pentru a permite utilizatorilor să controleze fluxul de trafic care este gestionat de procesorul de rută al unui dispozitiv de rețea.

AutoSecure - AutoSecure poate bloca funcțiile planului de management și serviciile și funcțiile planului de redirecționare ale unui router.

CoPP este conceput pentru a preveni traficul inutil să copleșească procesorul de rută. Caracteristica CoPP tratează planul de control ca pe o entitate separată cu propriile porturi de intrare (intrare) și ieșire (ieșire). Un set de reguli poate fi stabilit și asociat cu porturile de intrare și ieșire ale avionului de control.

3.5.3 - Securing the Management Plane

Traficul planului de management este generat fie de dispozitivele de rețea, fie de stațiile de gestionare a rețelei care utilizează procese și protocoale precum Telnet, SSH și TFTP, etc. Planul de management este o țintă foarte atractivă pentru hackeri. Din acest motiv, modulul de management a fost construit cu mai multe tehnologii menite să atenueze astfel de riscuri.

Fluxul de informații dintre gazdele de gestionare și dispozitivele gestionate poate fi în afara benzii (OOB), în cazul în care informațiile circulă într-o rețea în care nu există trafic de producție. Poate fi, de asemenea, în bandă, unde informațiile circulă prin rețeaua de producție a întreprinderii, internetul sau ambele.

Securitatea planului de management poate fi implementată folosind următoarele caracteristici, așa cum se arată în figură:

Politica de conectare și parole - Restricționează accesibilitatea dispozitivului. Limitează porturile accesibile și restricționează metodele de acces „cine” și „cum”.

Prezentarea notificării legale - Afișează notificări legale. Acestea sunt adesea dezvoltate de consilierul juridic al unei corporații.

Asigurarea de confidențialitate a datelor - Protejează datele sensibile stocate local de a fi vizualizate sau copiate. Utilizează protocoale de management cu autentificare puternică pentru a atenua atacurile de confidențialitate care vizează expunerea parolelor și a configurațiilor dispozitivelor.

Controlul accesului bazat pe roluri (RBAC) - Se asigură că accesul este acordat numai utilizatorilor, grupurilor și serviciilor autentificate. RBAC și serviciile de autentificare, autorizare și contabilitate (AAA) oferă mecanisme pentru a gestiona eficient controlul accesului.

Autorizare de acțiuni - Restricționează acțiunile și vizualizările care sunt permise de un anumit utilizator, grup sau serviciu.

Activarea raportelor accesului de gestionare - Jurnale și conturi pentru toate accesul. Înregistrează cine a accesat dispozitivul, ce s-a întâmplat și când a avut loc.

RBAC restricționează accesul utilizatorului în funcție de rolul utilizatorului. Rolurile sunt create în funcție de funcțiile de job sau de sarcină și sunt atribuite permisiuni de acces pentru anumite active. Utilizatorii sunt apoi alocați unor roluri și li se acordă permisiunile care sunt definite pentru acel rol.

În Cisco IOS, caracteristica de acces CLI bazată pe roluri implementează RBAC pentru accesul de gestionare a routerului. Caracteristica creează diferite „vizualizări” care definesc ce comenzi sunt acceptate și ce informații de configurare sunt vizibile. Pentru scalabilitate, utilizatorii, permisiunile și rolurile sunt de obicei create și menținute într-un server de depozit central. Acest lucru face ca politica de control al accesului să fie disponibilă pentru mai multe dispozitive. Serverul de depozit central poate fi un Cisco Identity Services Engine (ISE) care poate oferi servicii de rețea de autentificare, autorizare și contabilitate (AAA).

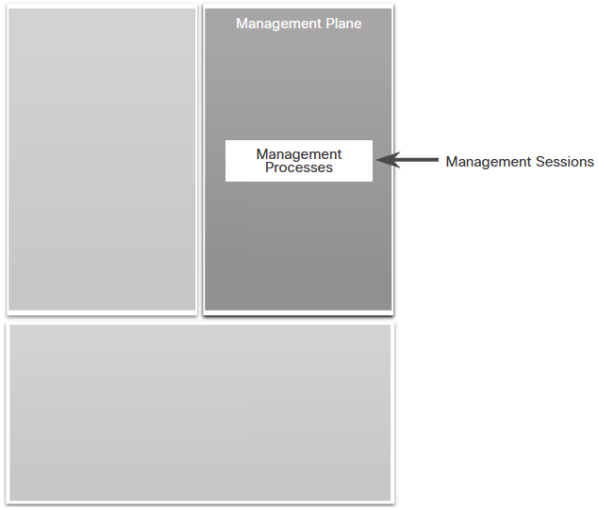

Fig. 3.10. Management Plane.

3.5.4 - Securing the Data Plane

Traficul din planul de date constă în cea mai mare parte din pachete de utilizator transmise prin router prin planul de date. Securitatea planului de date poate fi implementată folosind ACL-uri, mecanisme anti-spoofing și caracteristici de securitate Layer 2, așa cum se arată în figură.

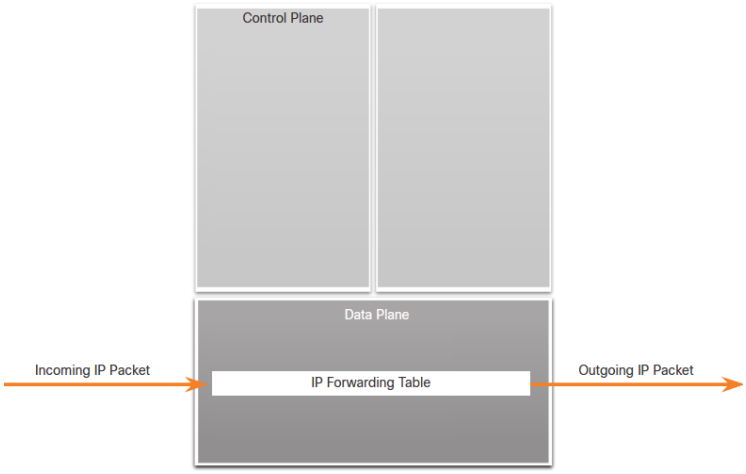

Fig. 3.11. Data Plane.

ACL-urile efectuează filtrarea pachetelor pentru a controla ce pachete se deplasează prin rețea și unde le este permis să ajungă. ACL-urile sunt folosite pentru a securiza planul de date într-o varietate de moduri:

- ***Blocarea traficului nedorit sau a utilizatorilor*** - ACL-urile pot filtra pachetele de intrare sau de ieșire pe o interfață. Acestea pot fi utilizate pentru a controla accesul pe baza adreselor sursă, adreselor de destinație sau a autentificării utilizatorilor.
- ***Reducerea șanselor de atacuri DoS*** - ACL-urile pot fi utilizate pentru a specifica dacă traficul de la gazde, rețele sau utilizatori poate accesa rețeaua. Caracteristica de interceptare ASA TCP este un mecanism care poate fi folosit pentru a proteja gazdele finale, în special serverele, de atacurile TCP SYN-flooding.
- ***Atenuarea atacurilor de falsificare*** - ACL-urile permit practicienilor în securitate să implementeze practici recomandate pentru a atenua atacurile de falsificare.
- ***Asigurarea controlului lățimii de bandă*** - ACL-urile pe o legătură lentă pot preveni traficul în exces.
- ***Clasificarea traficului pentru a proteja planurile de management și control*** - ACL-urile pot fi aplicate pe liniile vty.

ACL-urile pot fi, de asemenea, utilizate ca mecanism antispoofing prin eliminarea traficului care are o adresă sursă nevalidă. Aceasta înseamnă că atacurile trebuie inițiate de la adrese IP valide, accesibile, ceea ce permite ca pachetele să fie urmărite până la inițiatorul unui atac.

Caracteristici, cum ar fi Unicast Reverse Path Forwarding (uRPF), pot fi utilizate pentru a completa strategia antispoofing.

Switch-urile Cisco Catalyst pot folosi funcții integrate pentru a ajuta la securizarea infrastructurii de nivel 2. Următoarele instrumente de securitate de nivel 2 sunt integrate în comutatoarele Cisco Catalyst:

Securitate port - Previne falsificarea adreselor MAC și atacurile de inundare a adreselor MAC.

Snooping DHCP - Previne atacurile clientului asupra serverului și comutatorului DHCP.

Inspecție dinamică ARP (DAI) - Adaugă securitate ARP prin utilizarea tabelului de snooping DHCP pentru a minimiza impactul atacurilor de otrăvire și falsificare ARP.

IP Source Guard (IPSG) - Previne falsificarea adreselor IP prin utilizarea tabelului de snooping DHCP.

ATENTIE - Acest curs se concentrează pe diferitele tehnologii și protocoale utilizate pentru a securiza planurile de management și date.

VERIFICAREA ACUMULARII CONCEPTELOR.

1. Which NFP plane would typically use out-of-band (OOB) access?

- ◯ control plane
- ◯ management plane
- ◯ data plane

2. Which NFP plane uses CoPP?

- ◯ control plane
- ◯ management plane
- ◯ data plane

3. Which NFP plane is responsible for applying access control lists (ACLs)?

- ◯ control plane
- ◯ management plane
- ◯ data plane

4. The control plane is responsible for which of the following features? (Choose three.)

- ☐ routing protocol authentication
- ☐ blocking unwanted traffic or users
- ☐ logs and accounts for all access
- ☐ port security
- ☐ route processor traffic
- ☐ mitigating spoof attacks
- ☐ role-based access control
- ☐ password policy
- ☐ AutoSecure

3.6 SUMMARY

Apărarea rețelei

Profesioniștii în securitatea rețelei sunt responsabili de menținerea asigurării datelor pentru o organizație și de asigurarea integrității și confidențialității informațiilor. Un profesionist în securitate trebuie să fie informat despre amenințări și vulnerabilități pe măsură ce acestea evoluează. Există mai multe organizații de securitate a rețelei care vă țin la curent, inclusiv SANS, Mitre, FIRST, SecurityNewsWire, ISC2 și CIS. Certificarile pentru profesioniștii în securitatea rețelei sunt oferite de următoarele organizații:

GIAC

ISC2

ISACA

CE-Consiliu

CWSP

Securitatea informațiilor se ocupă cu protejarea informațiilor și a sistemelor de informații împotriva accesului, utilizării, dezvăluirii, întreruperii, modificării sau distrugerii neautorizate. Triada CIA servește ca fundație conceptuală pentru domeniu. Triada CIA constă din trei componente ale securității informațiilor: Confidențialitate, Integritate și Disponibilitate.

Politici de securitate a rețelei

Există 14 domenii de securitate a rețelei specificate de ISO/IEC. Descrise de ISO/IEC 27002, aceste 14 domenii servesc la organizarea, la un nivel înalt, a vastului tărâm al informației sub umbrela securității rețelei. Aceste domenii au unele paralele semnificative cu domeniile definite de certificarea CISSP. Cele 14 domenii sunt destinate să servească drept bază comună pentru dezvoltarea standardelor de securitate organizațională și a practicilor eficiente de management al securității. Ele ajută, de asemenea, la facilitarea comunicării între organizații. În rețea, politicile definesc activitățile care sunt permise în rețea. Politicile care pot fi incluse într-o politică de securitate includ politica de identificare și autentificare, politicile de parole, politica de utilizare acceptabilă, politica de acces la distanță, politica de întreținere a rețelei și procedurile de tratare a incidentelor. O politică de securitate este un „document viu”, ceea ce înseamnă că documentul este actualizat în mod regulat pe măsură ce cerințele tehnologice, comerciale și ale angajaților se modifică. Multe companii trebuie, de asemenea, să pună politici în jurul BYOD. Există și reglementări externe privind securitatea rețelei.

Profesioniștii în securitatea rețelelor trebuie să fie familiarizați cu legile și codurile de etică care sunt obligatorii pentru profesioniștii INFOSEC.

Instrumente de securitate, platforme și servicii

Există două analogii comune care sunt folosite pentru a descrie o abordare de apărare în profunzime: ceapa de securitate și anghinarea de securitate. Cu Security Onion, un actor de amenințare ar trebui să dezlipească nivelul de apărare al unei rețele, într-un mod similar cu curățarea unei cepe. Peisajul în schimbare al rețelelor, cum ar fi evoluția rețelelor fără granițe, a schimbat această analogie cu „anghinarea de securitate", de care beneficiază actorul amenințării. Actorii de amenințări nu mai trebuie să dezlipească fiecare strat. Trebuie doar să îndepărteze anumite „frunze de anghinare". Pentru a valida securitatea unei rețele și a sistemelor acesteia, au fost dezvoltate multe instrumente de testare a penetrației în rețea. Categoriile acestor instrumente includ instrumente de spargere a parolelor, instrumente de hacking fără fir, instrumente de scanare și hacking de rețea, instrumente de creare a pachetelor, sniffer de pachete, detectoare de rootkit, fuzzers pentru căutarea vulnerabilităților, instrumente criminalistice, depanatoare, sisteme de operare de hacking, instrumente de criptare, instrumente de exploatare a vulnerabilităților, și scanere de vulnerabilitate. Serviciile de informații privind amenințările permit schimbul de informații despre amenințări, cum ar fi vulnerabilități, IOC și tehnici de atenuare. Un astfel de serviciu este Cisco Talos Threat Intelligence Group.

Atenuarea atacurilor comune la rețea

Următoarele bune practici sunt utilizate pentru securizarea unei rețele: dezvoltarea unei politici de securitate scrise, educarea angajaților, controlul accesului fizic la sisteme, utilizarea parolelor puternice și schimbarea lor des, criptarea și parola - protejarea datelor sensibile, implementarea hardware și software de securitate, efectuarea de copii de siguranță și testați fișierele de rezervă, închideți serviciile și porturile inutile, mențineți patch-urile la zi și efectuați audituri și teste de securitate. Administratorii de rețea au mai multe mijloace de a atenua atacurile malware. Principalul mijloc de atenuare a atacurilor viruși și troieni este software-ul antivirus, cel mai răspândit produs de securitate de pe piață în prezent. Cu toate acestea, ele nu împiedică virușii să intre în rețea, așa că un profesionist în securitatea rețelei trebuie să fie conștient de virușii majori și să țină evidența actualizărilor de securitate cu privire la virușii emergenti. Viermii sunt mai mult bazați pe rețea decât virușii. Răspunsul la

un atac de viermi poate fi împărțit în patru faze: izolare, inoculare, carantină și tratament. Atacurile de recunoaștere sunt de obicei precursorul unor atacuri suplimentare, cu intenția de a obține acces neautorizat la o rețea sau de a perturba funcționalitatea rețelei. Un profesionist în securitatea rețelei poate detecta când este în desfășurare un atac de recunoaștere, primind notificări de la alarme preconfigurate. Atacurile de recunoaștere pot fi atenuate în mai multe moduri, inclusiv următoarele: implementați autentificarea pentru a asigura accesul adecvat, folosiți criptarea pentru a face inutile atacurile de sniffer de pachete, folosiți instrumente anti-sniffer pentru a detecta atacurile de sniffer de pachete, implementare.