Contents

INTRODUCERE

Acest curs oferă o introducere în conceptele și abilitățile de bază de securitate necesare pentru instalarea, depanarea și monitorizarea dispozitivelor de rețea pentru a menține integritatea, confidențialitatea și disponibilitatea datelor companiei.

Aceste materiale de curs vă vor ajuta să dezvoltați abilitățile necesare pentru a face următoarele:

Descrieți amenințările de securitate cu care se confruntă infrastructurile de rețea moderne.

Securizarea dispozitivelor Cisco.

Securizați infrastructura de rețea.

Implementați AAA pe routerele Cisco utilizând o bază de date locală de ruter și servere AAA externe.

Reduceți amenințările la adresa routerelor și rețelelor Cisco utilizând liste de control al accesului (ACL).

Implementați proiectarea, managementul și raportarea rețelei securizate.

Implementați setul de caracteristici firewall Cisco IOS.

Reduceți atacurile comune de la nivelul 2.

Implementați un VPN de la site la site.

Implementați un VPN de acces la distanță.

1.1 REGULI

1.0.3 - Ethical Hacking Statement

Programul Cisco Networking Academy se concentrează pe crearea soluțiilor globale de rezolvare a problemelor necesare pentru a construi, scala, securiza și apăra rețelele care sunt utilizate în afacerile noastre și în viața de zi cu zi. Nevoia de specialiști în securitatea rețelei bine pregătiți continuă să crească într-un ritm exponențial. Formarea pentru a deveni un specialist în securitatea rețelei necesită o înțelegere aprofundată și o expunere la modul în care apar atacurile de rețea, precum și la modul în care sunt detectate și prevenite. Aceste abilități vor include în mod natural și învățarea despre tehnicile pe care Actorii de amenințare le folosesc pentru a evita securitatea computerelor și a rețelei.

Accesul neautorizat la date, computere și sisteme de rețea este o infracțiune în multe jurisdicții și este adesea însoțit de consecințe grave, indiferent de motivațiile făptuitorului. Este responsabilitatea cursantului, în calitate de utilizator al acestui material, să cunoască și să respecte legile privind utilizarea computerelor.

1.0.4 - Inclusive Language

Scopul Cisco Networking Academy este de a asigura un viitor incluziv pentru toți. Având scopul nostru în centrul a tot ceea ce facem, vă puteți baza pe Cisco să fie îndrăzneț, curajos și deliberat cu privire la rolul nostru și la acțiunile pe care le vom întreprinde în sprijinul justiției sociale.

Ne alăturăm comunității tehnologice pentru a evolua limbajul pe care îl folosim. Regândirea cuvintelor pe care le folosim este doar una dintre modalitățile de a reduce barierele în calea echității și a respectului. Ca o chestiune de politică, conținutul Cisco Networking Academy ar trebui să fie lipsit de limbaj, grafică și scenarii jignitoare sau sugestive. Schimbăm termenii, după cum se menționează mai jos, cu alternative mai adecvate.

Term/Phrase	**Replacements**
master/slave	primary/secondary OR primary/subordinate OR control/data (for clustering)
whitelist/blacklist	permit (list)/block (list) OR allow (list)/block (list)

Este posibil să vedem în continuare termeni din industrie precum „pălărie neagră” în programa cursului. Se lucrează pentru a modifica și acești termeni.

CAPITOLUL 1. Securing Networks

1.1 TINTE

1.1.1 - Networks Are Targets

Rețelele sunt în mod obișnuit atacate. Este obișnuit să citim în știri despre încă o rețea care a fost compromisă. O căutare rapidă pe internet pentru atacuri de rețea va returna multe articole despre atacurile de rețea, inclusiv știri despre organizațiile care au fost compromise, cele mai recente amenințări la adresa securității rețelei, instrumente pentru atenuarea atacurilor și multe altele.

Pentru a ne ajuta să înțelegem gravitatea situației, Kapersky menține afișarea interactivă Cyberthreat Real-Time Map a atacurilor actuale de rețea. Datele de atac sunt trimise de la produsele de securitate a rețelei Kapersky care sunt implementate în întreaga lume. Figura afișează un exemplu de captură de ecran a acestui instrument web, care arată aceste atacuri în timp real. Multe instrumente similare sunt disponibile pe internet și pot fi găsite căutând hărți pentru amenințări cibernetice.

Fig. 1.1. Harta atacurilor in timp real.

1.1.2 - Reasons for Network Security

Securitatea rețelei se referă direct la continuitatea afacerii unei organizații. Încălcările de securitate ale rețelei pot perturba comerțul electronic, pot cauza pierderea datelor de afaceri,

pot amenința confidențialitatea oamenilor și pot compromite integritatea informațiilor. Aceste încălcări pot duce la pierderi de venituri pentru corporații, furt de proprietate intelectuală, procese și chiar pot amenința siguranța publică.

Menținerea unei rețele securizate asigură siguranța utilizatorilor rețelei și protejează interesele comerciale. Menținerea în siguranță a rețelei necesită vigilență din partea profesioniștilor în securitatea rețelei ai unei organizații. Aceștia trebuie să fie în mod constant conștienți de amenințările și atacurile noi și în evoluție la rețele, precum și de vulnerabilitățile dispozitivelor și aplicațiilor.

Sunt disponibile multe instrumente pentru a ajuta administratorii de rețea să adapteze, să dezvolte și să implementeze tehnici de atenuare a amenințărilor. De exemplu, site-ul web Cisco Talos Intelligence Group, prezentat în figură, oferă informații cuprinzătoare de securitate și amenințări pentru a apăra clienții și a le proteja activele.

Fig. 1.2. Cisco Talos Intelligence Group.

Un alt grup, numit Cisco Product Security Incident Response Team (PSIRT), este responsabil pentru investigarea și atenuarea potențialelor vulnerabilități din produsele Cisco. Figura afișează un exemplu de pagină Cisco Security Advisories care listează aceste vulnerabilități în timp real și oferă administratorilor de rețea informații pentru a ajuta la atenuarea acestora.

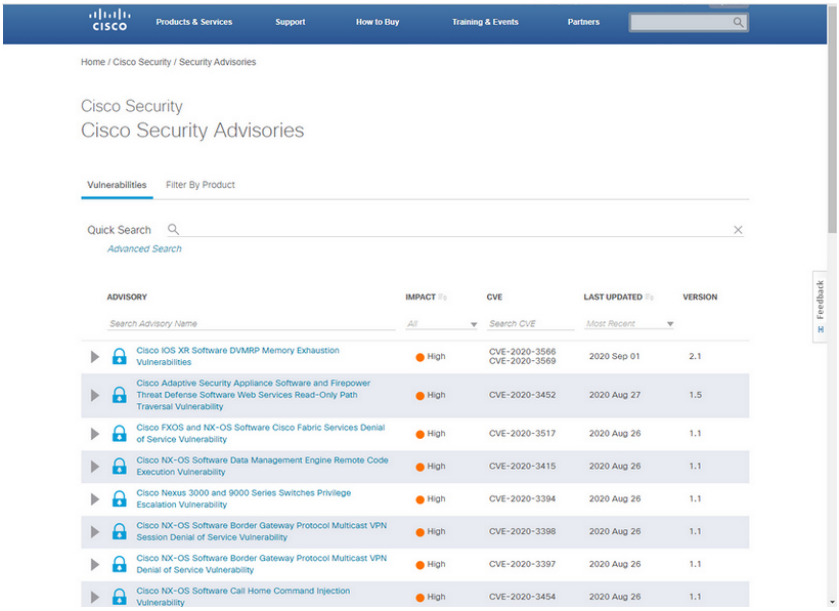

Fig. 1.3. Cisco Product Security Incident Response Team

1.1.3 - Vectors of Network Attacks

Un vector de atac este o cale prin care un actor de amenințare poate obține acces la un server, gazdă sau rețea. Vectorii de atac provin din interiorul sau din exteriorul rețelei corporative, așa cum se arată în figură. De exemplu, Actorii de amenințare pot viza o rețea prin internet, pentru a perturba operațiunile rețelei și pentru a crea un atac de tip denial of service (DoS).

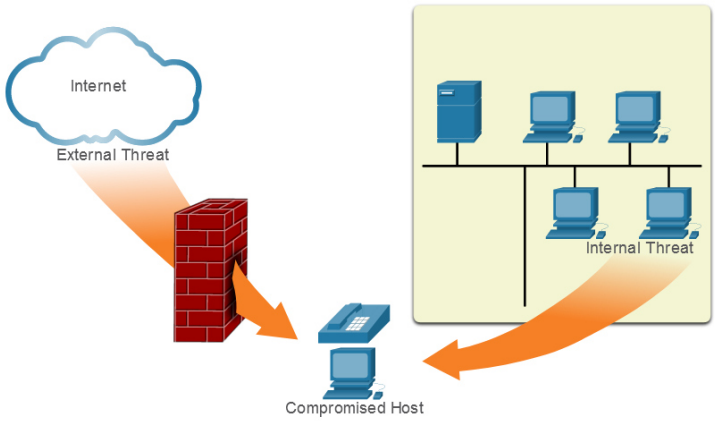

Fig. 1.4. Amenintari externe si interne.

Notă: Un atac DoS are loc atunci când un dispozitiv sau o aplicație de rețea este dezactivată și nu mai este capabilă să accepte cererile de la utilizatori legitimi.

Un utilizator intern, cum ar fi un angajat, poate accidental sau intenționat:

- ***Fure și copieze datele confidențiale pe medii amovibile, e-mail, software de mesagerie și alte medii.***
- ***Compromite serverele interne sau dispozitivele de infrastructură de rețea.***
- ***Deconecteze o conexiune critică la rețea și sa provoace o întrerupere a rețelei.***
- ***Conecteze o unitate USB infectată la un sistem computerizat corporativ.***

Amenințările interne au potențialul de a provoca daune mai mari decât amenințările externe, deoarece utilizatorii interni au acces direct la clădire și la dispozitivele sale de infrastructură. De asemenea, angajații pot avea cunoștințe despre rețeaua corporativă, resursele acesteia și datele sale confidențiale.

Profesioniștii în securitatea rețelelor trebuie să implementeze instrumente și să aplice tehnici pentru atenuarea amenințărilor atât externe, cât și interne.

1.1.4 - Data Loss

Este posibil ca datele să fie cel mai valoros activ al unei organizații. Datele organizaționale pot include date de cercetare și dezvoltare, date de vânzări, date financiare, date despre resurse umane și juridice, date despre angajați, date despre contractanți și date despre clienți.

Pierderea de date sau exfiltrarea datelor este atunci când datele sunt pierdute, furate sau scurse în mod intenționat sau neintenționat în lumea exterioară. Pierderea datelor poate duce la:

- ***Deteriorarea mărcii și pierderea reputației***
- ***Pierderea avantajului competitiv***
- ***Pierderea clienților***
- ***Pierderea veniturilor***
- ***Litigii/acțiuni legale care au ca rezultat amenzi și sancțiuni civile***
- ***Costuri semnificative și efort pentru a notifica părțile afectate și a recupera din încălcare***

Profesioniștii în securitatea rețelei trebuie să protejeze datele organizației. Trebuie implementate diverse controale de prevenire a pierderii datelor (DLP) care să combine măsuri strategice, operaționale și tactice.

Vectorii comuni de pierdere de date sunt afișați în tabel.

Termen	Definitie
Email/Social Networking	Cel mai comun vector pentru pierderea de date include software-ul de mesagerie instantanee și site-urile de social media. De exemplu, e-mailurile sau mesajele IM interceptate ar putea fi capturate și dezvăluie informații confidențiale.
Unencrypted Devices	Un laptop corporativ furat conține de obicei date organizaționale confidențiale. Dacă datele nu sunt stocate folosind un algoritm de criptare, atunci hoțul poate prelua date confidențiale valoroase.
Cloud Storage Devices	Salvarea datelor în cloud are multe beneficii potențiale. Cu toate acestea, datele sensibile se pot pierde dacă accesul la cloud este compromis din cauza setărilor de securitate slabe.
Removable Media	Un risc este ca un angajat să efectueze un transfer neautorizat de date pe o unitate USB. Un alt risc este că o unitate USB care conține date corporative valoroase ar putea fi pierdută.
Hard Copy	Datele corporative ar trebui eliminate în întregime. De exemplu, datele confidențiale ar trebui să fie mărunțite atunci când nu mai sunt necesare. În caz contrar, un hoț ar putea prelua rapoartele aruncate și ar putea obține informații valoroase.
Improper Access Control	Parolele sunt prima linie de apărare. Parolele furate sau parolele slabe care au fost compromise pot oferi atacatorului acces facil la datele corporative.

1.2 Network Topology Overview

1.2.1 - Campus Area Networks

Toate rețelele sunt ținte. Cu toate acestea, accentul principal al acestui curs este pe securizarea rețelelor de zonă de campus (CAN). Campus Area Networks constă din rețele LAN interconectate într-o zonă geografică limitată.

Profesioniștii în rețea trebuie să implementeze diverse tehnici de securitate a rețelei pentru a proteja activele organizației de amenințările din exterior și din interior. Conexiunile la rețele care nu sunt de încredere trebuie verificate în profunzime de mai multe niveluri de apărare înainte de a ajunge la resursele întreprinderii. Acest lucru este cunoscut sub numele de apărare în profunzime.

Figura afișează un exemplu de CAN cu o abordare în profunzime de apărare care utilizează diverse caracteristici de securitate și dispozitive de securitate pentru a-l securiza. Tabelul oferă o Eexplicație a elementelor designului de apărare în profunzime care sunt prezentate în figură.

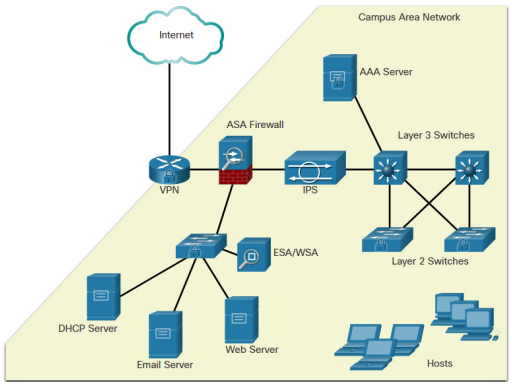

Fig. 1.5. Topologia unei retele de campus.

Termen	Definitie
VPN	Cisco ISR este securizat. Protejează datele în mișcare care circulă de la CAN către lumea exterioară prin stabilirea de rețele private virtuale (VPN). VPN-urile asigură confidențialitatea și integritatea datelor din surse autentificate.
ASA Firewall	Un firewall Cisco Adaptive Security Appliance (ASA) efectuează filtrarea pe baza de stare a pachetelor pentru a filtra traficul de retur din rețeaua exterioară în rețeaua campusului.
IPS	Un dispozitiv Cisco Intrusion Prevention System (IPS) monitorizează continuu traficul de rețea de intrare și de ieșire pentru activități rău intenționate. Înregistrează informații despre activitate și încearcă să o blocheze și să o raporteze.
Layer 3 Switches	Aceste comutatoare de nivel de distribuție sunt securizate și oferă conexiuni de trunchi redundante securizate la comutatoarele de nivel 2. Pot fi implementate mai multe caracteristici de securitate diferite, cum ar fi ACL-uri, DHCP snooping, Dynamic ARP Inspection (DAI) și protecția sursei IP.
Layer 2 Switches	Aceste comutatoare de nivel de acces sunt securizate și conectează porturi orientate către utilizator la rețea. Pot fi implementate mai multe caracteristici de securitate diferite, cum ar fi securitatea porturilor, DHCP snooping și autentificarea utilizatorului 802.1X.
ESA/WSA	Un dispozitiv Cisco Email Security Appliance (ESA) și Web Security Appliance (WSA) oferă apărare avansată împotriva amenințărilor, vizibilitate și control al aplicațiilor, raportare și mobilitate securizată pentru a securiza și controla traficul de e-mail și web.
AAA Server	Un server de autentificare, autorizare și contorizare (AAA) autentifică utilizatorii, autorizează ceea ce au voie să facă și urmărește ceea ce fac.
Hosts	Punctele finale sunt securizate folosind diverse funcții, inclusiv software antivirus și antimalware, caracteristici ale sistemului de protecție împotriva intruziunilor gazdă și funcții de autentificare 802.1X.

1.2.2 - Small Office and Home Office Networks

Este important ca toate tipurile de rețele, indiferent de dimensiune, să fie protejate. Atacatorii sunt, de asemenea, interesați de rețelele de acasă și de rețelele de birouri mici și de birouri de acasă (SOHO). Ei pot dori să folosească gratuit conexiunea la internet a cuiva, să folosească conexiunea la internet pentru activități ilegale sau să vadă tranzacții financiare, cum ar fi achizițiile online.

Rețelele de acasă și SOHO sunt de obicei protejate folosind un router de calitate pentru consumatori. Aceste routere oferă caracteristici de securitate de bază care protejează în mod adecvat activele din interior de atacatorii externi.

Figura afișează un eșantion SOHO care folosește un router wireless de calitate pentru consumatori pentru a-l securiza. Un router wireless de calitate pentru consumatori oferă caracteristici de firewall integrate și conexiuni wireless sigure. Comutatorul Layer 2 este un comutator de nivel de acces care este întărit cu diferite măsuri de securitate. Conectează porturi orientate către utilizator care utilizează securitatea porturilor la rețeaua SOHO. Gazdele wireless se conectează la rețeaua fără fir folosind tehnologia de criptare a datelor Wireless Protected Access 2 (WPA2). Gazdele au instalat de obicei software antivirus și antimalware. Combinate, aceste măsuri de securitate oferă o apărare completă la diferite niveluri ale rețelei.

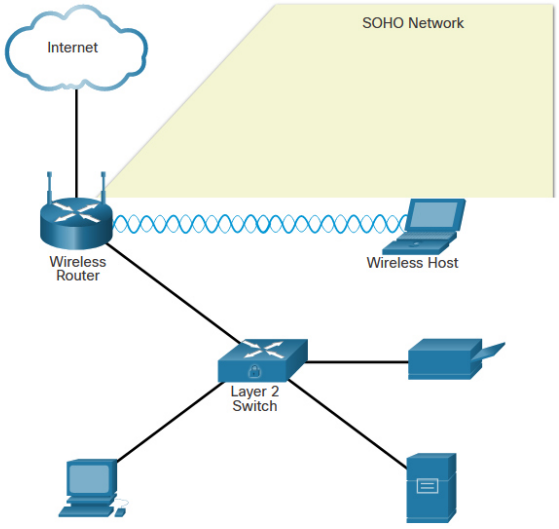

Fig. 1.6. SOHO.

1.2.3 - Wide Area Networks

Rețelele Wide Area Networks (WAN), așa cum se arată în figură, se întind pe o zonă geografică largă, adesea prin internetul public. Organizațiile trebuie să asigure transportul securizat pentru datele în mișcare pe măsură ce acestea se deplasează între site-uri prin intermediul rețelei publice.

Profesioniștii în securitatea rețelei trebuie să utilizeze dispozitive securizate la marginea rețelelor. În figură, site-ul principal este protejat de un ASA, care oferă caracteristici de firewall cu stare și stabilește tuneluri VPN securizate către diferite destinații.

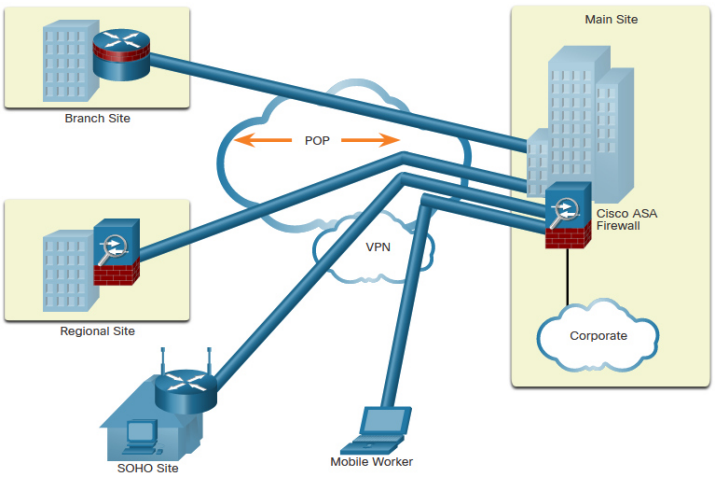

Fig. 1.7. WAN.

Figura prezintă o sucursală, un loc regional, un loc SOHO și un lucrător mobil. O sucursală se conectează la site-ul principal al corporației folosind un ISR consolidat. ISR poate stabili o conexiune VPN permanentă permanentă la firewall-ul ASA al site-ului principal. Un site regional este mai mare decât o sucursală și se conectează la site-ul principal al corporației folosind un ASA. ASA poate stabili o conexiune VPN permanentă permanentă la site-ul principal ASA. Un site SOHO este un mic site de filială care se conectează la site-ul principal al companiei folosind un router wireless Cisco. Routerul wireless poate stabili o conexiune VPN permanentă permanentă la site-ul principal ASA. Alternativ, utilizatorii interni SOHO ar putea folosi clientul Cisco AnyConnect VPN pentru a stabili o conexiune VPN sigură la site-ul principal ASA. Un lucrător mobil este un lucrător la distanță care poate utiliza clientul Cisco AnyConnect VPN pentru a stabili o conexiune VPN sigură la site-ul principal ASA din orice locație.

1.2.4 - Data Center Networks

Rețelele de centre de date sunt de obicei găzduite într-o unitate în afara amplasamentului pentru a stoca date sensibile sau proprietare. Aceste site-uri sunt conectate la site-uri corporative folosind tehnologia VPN cu dispozitive ASA și switch-uri integrate pentru centre de date, cum ar fi comutatoare Cisco Nexus de mare viteză.

Centrele de date de astăzi stochează cantități mari de informații sensibile, critice pentru afaceri. Prin urmare, securitatea fizică este esențială pentru funcționarea lor. Securitatea fizică nu numai că protejează accesul la instalație, ci și oamenii și echipamentele. De exemplu, alarme de incendiu, sprinklere, rafturi pentru servere cu contravântuiri seismice, încălzire

redundantă, ventilație și aer condiționat (HVAC) și sisteme UPS sunt în vigoare pentru a proteja oamenii, echipamentele și datele.

După cum se evidențiază în figură, securitatea fizică a centrului de date poate fi împărțită în două zone:

- ***Securitatea perimetrului exterior*** - Aceasta poate include ofițeri de securitate la sediu, garduri, porți, supraveghere video continuă și alarme de încălcare a securității.
- ***Securitate în interiorul perimetrului*** - Aceasta poate include supraveghere video continuă, detectoare electronice de mișcare, capcane de securitate și senzori biometrici de acces și ieșire.

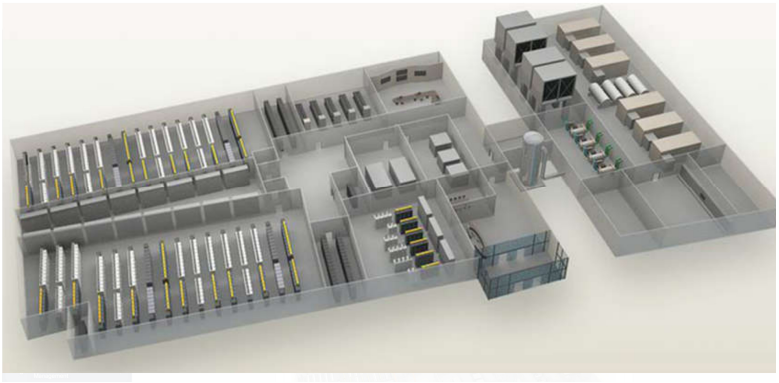

Fig. 1.8. DCN.

Capcanele de securitate oferă acces la sălile de date unde sunt stocate datele centrului de date. După cum se arată în figura de mai jos, o capcană de securitate este similară cu un blocaj de aer. Mai întâi, o persoană trebuie să intre în capcana de securitate utilizând cardul de proximitate si insigna. După ce persoana se află în capcana de securitate, recunoașterea facială, amprentele digitale sau alte verificări biometrice sunt folosite pentru a deschide a doua ușă. Utilizatorul trebuie să repete procesul pentru a ieși din sala de date.

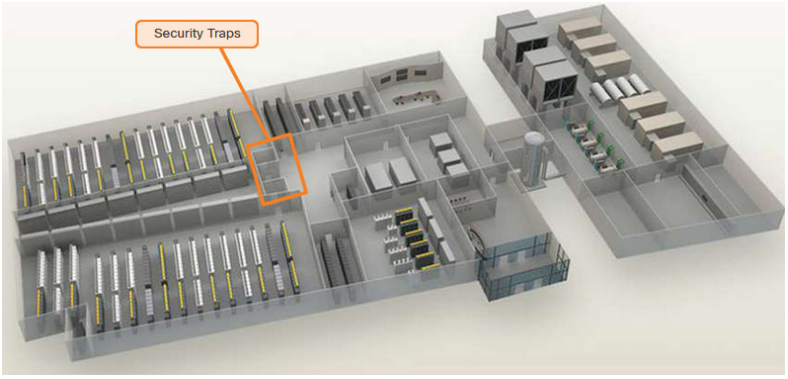

Fig. 1.9. Capcana de Securitate.

Figura de mai jos afișează scanerul biometric de amprentă digitală care este utilizat pentru a securiza accesul la Centrul de date Cisco Allen, din Allen, Texas.

Fig. 1.10. Access biometric.

1.2.5 - Cloud Networks and Virtualization

Cloud-ul joacă un rol tot mai mare în rețelele întreprinderilor. Cloud computing permite organizațiilor să utilizeze servicii precum stocarea de date sau aplicații bazate pe cloud, pentru a-și extinde capacitatea sau capacitățile fără a adăuga infrastructură. Prin însăși natura sa, cloud-ul se află în afara perimetrului tradițional al rețelei, permițând unei organizații să aibă un centru de date care poate sau nu să se afle în spatele firewall-ului tradițional.

Termenii „cloud computing" și „virtualizare" sunt adesea folosiți interschimbabil; cu toate acestea, ele înseamnă lucruri diferite. Virtualizarea este fundamentul cloud computingului. Fără el, cloud computing, așa cum este implementat pe scară largă, nu ar fi posibil. Cloud computing separă aplicația de hardware. Virtualizarea separă sistemul de operare de hardware.

Rețeaua cloud constă din servere fizice și virtuale care sunt de obicei găzduite în centre de date. Cu toate acestea, centrele de date folosesc din ce în ce mai mult mașini virtuale (VM) pentru a furniza servicii de server clienților lor. Virtualizarea serverelor profită de resursele de calcul inactive și consolidează numărul de servere necesare. Acest lucru permite, de asemenea, să existe mai multe sisteme de operare pe o singură platformă hardware. Cu toate acestea, VM-urile sunt, de asemenea, predispuse la atacuri specifice, după cum este enumerat mai jos.

HYPERJACKING - Un atacator ar putea deturna un hypervisor VM (software de control VM) și apoi îl poate folosi ca punct de lansare pentru a ataca alte dispozitive din rețeaua centrului de date.

ACTIVARE INSTANTANEE - Când o VM care nu a fost folosită pentru o perioadă de timp este adusă online, este posibil să aibă politici de securitate învechite care deviază de la securitatea de bază și pot introduce vulnerabilități de securitate.

FURTUNI ANTIVIRUS - Acest lucru se întâmplă atunci când toate mașinile virtuale încearcă să descarce fișiere de date antivirus în același timp.

Pentru echipele de securitate, o strategie ușor de implementat, dar cuprinzătoare, care să răspundă cerințelor afacerii și să apere centrul de date este o necesitate. Cisco a dezvoltat soluția Secure Data Center pentru a opera în acest peisaj imprevizibil de amenințări. Soluția Cisco Secure Data Center blochează amenințările interne și externe la marginea centrului de date.

Componentele de bază ale soluției Cisco Secure Data Center oferă următoarele servicii:

Segmentare sigură - Dispozitivele ASA și un Gateway de securitate virtuală integrat în switch-urile Cisco Nexus Series sunt implementate într-o rețea de centru de date pentru a oferi o segmentare sigură. Acest lucru oferă securitate inter-mașină virtuală granulară.

Apărarea împotriva amenințărilor - Dispozitivele ASA și IPS din rețelele centrelor de date utilizează informații despre amenințări, amprentarea pasivă a sistemului de operare și analiza reputației și contextuală pentru a oferi apărare împotriva amenințărilor.

Vizibilitate - Soluțiile de vizibilitate sunt furnizate folosind software precum Cisco Security Manager, care ajută la simplificarea operațiunilor și raportarea conformității.

1.2.6 - The Evolving Network Border

În trecut, angajații și resursele de date au rămas într-un perimetru predefinit, care era protejat de tehnologia firewall. De obicei, angajații foloseau computere emise de companie conectate la o rețea LAN corporativă care au fost monitorizate și actualizate continuu pentru a îndeplini cerințele de securitate.

Astăzi, punctele finale de consum, cum ar fi iPhone-urile, smartphone-urile, tabletele și mii de alte dispozitive, devin substitute puternice sau completări ale PC-ului tradițional. Din ce în ce mai mulți oameni folosesc aceste dispozitive pentru a accesa informațiile companiei. Această tendință este cunoscută sub numele de Bring Your Own Device (BYOD).

Pentru a se adapta tendinței BYOD, Cisco a dezvoltat rețeaua fără frontiere. Într-o rețea fără margini, accesul la resurse poate fi inițiat de utilizatori din mai multe locații, pe multe tipuri de dispozitive terminale, folosind diverse metode de conectivitate.

Pentru a susține această margine neclară a rețelei, dispozitivele Cisco acceptă funcțiile Mobile Device Management (MDM). MDM oferă dispozitive mobile securizate, monitorizate și gestionate, inclusiv dispozitive deținute de companii și dispozitive deținute de angajați. Dispozitivele gestionate și acceptate de MDM includ nu numai dispozitive portabile, cum ar fi smartphone-uri și tablete, ci și laptopuri și dispozitive de calcul desktop.

DATA ENCRYPTION - Majoritatea dispozitivelor au capabilități de criptare încorporate, atât la nivel de dispozitiv, cât și la nivel de fișier. Caracteristicile MDM pot asigura că numai dispozitivele care acceptă criptarea datelor și o au activată pot accesa rețeaua și conținutul corporativ.

PIN ENFORCEMENT - Aplicarea blocării PIN este primul și cel mai eficient pas în prevenirea accesului neautorizat la un dispozitiv. În plus, politicile de parole puternice pot fi impuse și de un MDM, reducând probabilitatea atacurilor cu forță brută.

DATA WIPE - Dispozitivele pierdute sau furate pot fi șterse de la distanță complet sau parțial, fie de către utilizator, fie de către un administrator prin MDM.

DATA LOST PREVENTION - DLP - În timp ce funcțiile de protecție a datelor (cum ar fi blocarea PIN, criptarea datelor și ștergerea datelor de la distanță) împiedică utilizatorii neautorizați să acceseze date, DLP îi împiedică pe utilizatorii autorizați să facă lucruri neglijente sau rău intenționate cu date critice.

JAILBREAK/ROOT DETECTION - Jailbreaking-ul (pe dispozitivele Apple iOS) și rooting-ul (pe dispozitivele Android) sunt un mijloc de a ocoli gestionarea unui dispozitiv. Funcțiile MDM pot detecta astfel de ocoliri și pot restricționa imediat accesul unui dispozitiv la rețea sau la alte active corporative.

1. Which network type consists of a number of LANs that are connected together across a limited geographic area?

- ◯ SOHO
- ◯ WAN
- ◯ CAN
- ◯ Data Center
- ◯ Cloud

2. Which network type includes a consumer grade router with basic security features to protect inside assets from outside attackers?

- ◯ SOHO
- ◯ CAN
- ◯ WAN
- ◯ Cloud

3. Which network type consists of a number of LANs that are connected together across a limited geographic area?

- ◯ SOHO
- ◯ CAN
- ◯ Data Center
- ◯ Cloud

1.3 Securing Networks Summary

1.3.1 - What Did I Learn in this Module

Starea actuală a lucrurilor

Securitatea rețelei se referă direct la continuitatea afacerii unei organizații. Încălcările de securitate ale rețelei pot perturba comerțul electronic, pot cauza pierderea datelor de afaceri, pot amenința confidențialitatea oamenilor și pot compromite integritatea informațiilor. Aceste încălcări pot duce la pierderi de venituri pentru corporații, furt de proprietate intelectuală, procese și chiar pot amenința siguranța publică. Sunt disponibile multe instrumente pentru a ajuta administratorii de rețea să adapteze, să dezvolte și să implementeze tehnici de atenuare a

amenințărilor, inclusiv Cisco Talos Intelligence Group. Un vector de atac este o cale prin care un actor de amenințare poate obține acces la un server, gazdă sau rețea. Vectorii de atac provin din interiorul sau din exteriorul rețelei corporative. Este posibil ca datele să fie cel mai valoros activ al unei organizații. Trebuie implementate diverse controale DLP, care combină măsuri strategice, operaționale și tactice. Vectorii obișnuiți de pierdere a datelor includ e-mailul și rețelele sociale, dispozitivele de date necriptate, dispozitivele de stocare în cloud, mediile amovibile, copierea pe hârtie și controlul necorespunzător al accesului.

Prezentare generală a topologiei rețelei

Există multe tipuri de rețele. CAN-urile constau din LANS interconectate într-o zonă geografică limitată. Elementele designului de apărare în profunzime includ VPN, firewall ASA, IPS, switch-uri Layer 3, switch-uri Layer 2, ESA/WSA, server AAA și gazde. Rețelele SOHO sunt de obicei protejate folosind routere de calitate pentru consumatori care oferă caracteristici de firewall integrate și conexiuni wireless sigure. Gazdele wireless se conectează la rețeaua fără fir folosind tehnologia de criptare a datelor WPA2. WAN-urile acoperă o zonă geografică largă. Profesioniștii în securitatea rețelei trebuie să utilizeze dispozitive securizate la marginea rețelei. Rețelele de centre de date sunt de obicei găzduite într-o unitate în afara amplasamentului pentru a stoca date sensibile sau proprietare. Securitatea fizică a centrului de date este împărțită în două zone: securitatea perimetrului exterior și securitatea perimetrului interior. Capcanele de securitate necesită ca o persoană să-și folosească ID-ul insigna pentru a intra în prima zonă. După ce persoana se află în capcana de securitate, recunoașterea facială, amprentele digitale sau alte verificări biometrice sunt folosite pentru a deschide a doua ușă. Cloud computing permite organizațiilor să utilizeze servicii precum stocarea de date sau aplicații bazate pe cloud, pentru a-și extinde capacitatea sau capacitățile fără a adăuga infrastructură. Rețeaua reală cloud constă din servere fizice și virtuale care sunt de obicei găzduite în centre de date. Cu toate acestea, centrele de date folosesc din ce în ce mai mult VM-uri pentru a furniza servicii de server clienților lor. Mașinile virtuale sunt, de asemenea, predispuse la atacuri țintite specifice, inclusiv hyperjacking, activare instantanee și furtuni antivirus. Soluția Cisco Secure Data Center blochează amenințările interne și externe la marginea centrului de date. Componentele de bază ale soluției Cisco Secure Data Center oferă segmentare sigură, apărare împotriva amenințărilor și vizibilitate. Din ce în ce mai mulți oameni folosesc aceste dispozitive pentru a accesa informațiile companiei. Această tendință

este cunoscută sub numele de BYOD. Pentru a se adapta tendinței BYOD, Cisco a dezvoltat rețeaua fără frontiere. Într-o rețea fără margini, accesul la resurse poate fi inițiat de utilizatori din mai multe locații, pe multe tipuri de dispozitive terminale, folosind diverse metode de conectivitate. Pentru a suporta această margine neclară a rețelei, dispozitivele Cisco acceptă funcțiile MDM.