ANALIZA POLITICILOR DE SECURITATE PENTRU DISPOZITIVELE TERMINALE DIN REȚELELE UNIVERSITARE

Denis MALISENCU

Departamentul Telecomunicaţii şi Sisteme Electronice, Grupa SISRC-211M,
Facultatea Electronică şi Telecomunicaţii, mun. Chişinău, Republica Moldova.

Autorul corespondent: Denis Malisencu, denis.malisencu@tse.utm.md

Rezumat. *Politicile de securitate reprezintă un set de obiective pentru universitate, reguli de comportament pentru utilizatori şi administratori şi cerinţe pentru sistem care vor asigura în mod colectiv securitatea reţelelor şi a sistemelor informatice dintr-o universitate. Politicele de securitate sunt un „document viu", ceea ce înseamnă că documentul nu este niciodată finalizat şi este actualizat continuu pe măsură ce cerinţele tehnologiei şi ale angajaţilor se schimbă.*

Cuvinte cheie*: dispozitive terminale, reţea, date, securitate informaţională, atacuri cibernetice, dispozitive de securitate.*

Introducere

Toată securitatea începe cu intenția conducerii de a proteja resursele universității. Cu toate acestea, gestionarea datelor care se deplasează împreună cu o mulțime de dispozitive mobile tinde să sfideze standardele stabilite și acceptate de utilizatori pentru desktopuri, servere etc. Politicile de securitate cuprind un set de obiective pentru universitate, reguli de comportament pentru utilizatori și administratori și cerințe pentru sistem care vor asigură în mod colectiv securitatea rețelelor și a sistemelor informatice dintr-o universitate. Politicile date de securitate sunt un „document viu", ceea ce înseamnă că documentul nu este niciodată finalizat și este actualizat continuu pe măsură ce cerințele tehnologiei și ale angajaților se schimbă.

Politici de securitate

O politică de securitate traduce, clarifică și comunică poziția de gestionare a securității, astfel cum este definită în principiile de securitate la nivel înalt. Politica de securitate acționează ca o punte între aceste obiective de management și cerințele specifice de securitate. Aceasta informează utilizatorii, personalul și managerii cu privire la cerințele lor obligatorii pentru protejarea activelor tehnologice și informaționale. O politică de securitate a tehnologiei informației (IT) identifică regulile și proceduri pentru toate persoanele care accesează și utilizează activele și resursele IT ale unei organizații. Astfel, o politică de securitate IT eficientă este un document unic pentru fiecare organizație, cultivat din perspectivele oamenilor cu privire la toleranța la risc, modul în care își văd și valorifică informațiile și disponibilitatea rezultată pe care o mențin asupra acelor informații.

Figura 1 prezintă ierarhia unei structuri de politici corporative care vizează satisfacerea eficientă a tuturor nevoilor organizaționale.

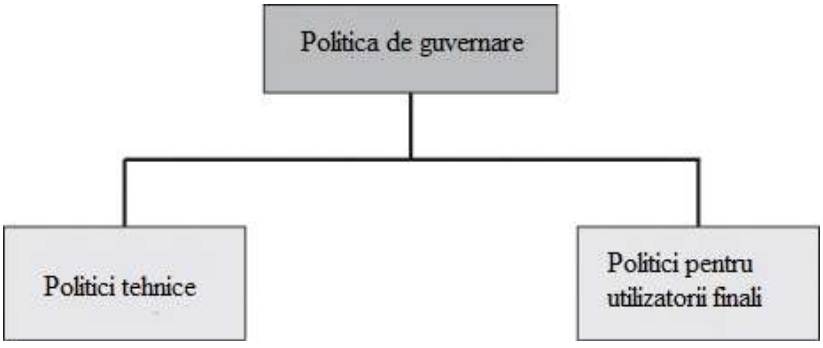

Figura 1. Structura politicelor corporative

- Politica de guvernare: Această politică este un tratament la nivel înalt al conceptelor de securitate care sunt importante pentru universitate. Politica de guvernare controlează toate interacțiunile legate de securitate între unitățile de afaceri și departamentele universității.
- Politici privind utilizatorii finali: acest document acoperă toate subiectele de securitate importante pentru utilizatorii finali.
- Politici tehnice: membrii personalului de securitate folosesc politici tehnice pe măsură ce își îndeplinesc responsabilitățile de securitate pentru sistem.

Una dintre cele mai comune componente ale politicii de securitate este o politică de utilizare acceptabilă. Această componentă definește ceea ce utilizatorii au voie și nu au voie să facă pe diferite componente ale sistemului, inclusiv tipul de trafic permis în rețele. Politica dată ar trebui să fie cât mai explicită posibil pentru a evita ambiguitatea sau neînțelegerea. De exemplu, o politică ar putea enumera categoriile de site-uri web interzise.

Componentele de bază ale unei politici includ:

- Scop - o scurtă declarație care să explice obiectivele și rezultatele conducerii. În multe cazuri, scopul include cerințele impuse de reglementările locale, de stat sau federale. De asemenea, politica ar trebui să precizeze clar de ce este necesară.
- Domeniul de aplicare – descrie aplicarea politicii. Există două tipuri de politici: la nivel de program și specifice problemei. Politicile la nivel de program se aplică tuturor activităților, sistemelor și dispozitivelor din întreaga organizație. O organizație poate aplica politici specifice problemei aspectelor unei activități, sistem sau dispozitiv care necesită constrângeri de politici diferite de cele prevăzute de o politică de program aplicabilă.
- Responsabilitatea - descrie punctul de contact pentru întrebări sau cereri de modificare, cine este responsabil pentru supravegherea conformității și cine poate aproba modificările.
- Conformitatea – oferă managementului recurs atunci când un angajat sau un manager nu respectă politica. Adesea, departamentul de resurse umane (HR) are deja în vigoare politici disciplinare care se aplică nerespectării oricărei politici a companiei.

Metode de atac, tipuri de controale şi dispozitive de securitate

Înainte de a implementa o politica de securitate pentru o rețea, mai întâi și întâi, e nevoie de a cunoaște tipurile de atac care pot afecta rețeaua. Scopul final al atacatorilor este de a obține acces sau de a modifica datele de valoare. Obiectivele lor sunt de obicei servere, stații de lucru sau alte computere conectate la rețelele universității. O strategie de atac a rețelei este de a încerca de a ocoli sau dezactiva rețeaua sau dispozitivele de securitate prin exploatarea vulnerabilităților, care duce la extragerea datelor sau modificarea lor.

- Investigarea – atacatorii folosesc investigarea pentru a descoperi vulnerabilitățile serverelor sau rețelelor. Exista o varietate de instrumente gratuite care permit scanarea sistemelor, în care în final arată toate vulnerabilitățile rețelei/serverului, ceea ce ii ajută pe atacatori in spargerea rețelei.
- Exploatarea – protocoalele folosite pe internet și în rețelele universitare au fost concepute pentru disponibilitate si confidențialitate. Respectiv, atacatorii abuzează și exploatează in folosul lor lipsa de securitate a TCP/IP și a celorlalte protocoale sau dispozitive care nu dispun de o anumită securitate mai performantă. Există mai multe metode de exploatare care sunt reflectate în Tab 1.

Controalele de securitate definesc tehnicile utilizate de către administratorii de sistem pentru a securiza rețelele de comunicații. La fel ca alte tipuri de controale de securitate, controalele de rețea pot fi clasificate în diferite tipuri, în funcție de funcția lor principală. Mai jos, în Tab. 2, sunt reprezentate tipurile de control și funcțiile pe care le îndeplinesc.

Tabelul 1.

Metode de atac

Denumirea atacului	Metoda de exploatare
Sniffing	Interceptarea și examinarea traficului de rețea
Spoofing	Uzurparea unei gazde de rețea sau a unui utilizator
Man-in-the-Middle	Atac cibernetic în care atacatorul transmite în secret și, eventual, modifică comunicările dintre două părți care cred că comunică direct între ele.
Hijacking	Are loc atunci când un intrus preia controlul unei sesiuni între un server și client.
Replay attack	O formă de atac de rețea în care transmiterea validă a datelor este repetată sau întârziată cu rea intenție sau în mod fraudulos.
Password cracking	Este procesul de recuperare a parolelor din datele care au fost stocate sau transmise de un sistem informatic sub formă amestecată.
Exploatarea sistemului sau a aplicației	Odată ce un atacator intră în contact cu un sistem la oricare dintre protocoalele stratului aplicației, cum ar fi FTP, Telnet, SSH, HTTP, HTTPS, SNMP și altele, punctele slabe ale sistemului de operare sau ale aplicațiilor pot fi exploatate pentru obțineți acces neautorizat

Tabelul 2.

Tipurile de control

Tipurile de control	Funcția controlului
Controalele preventive	Caută să oprească sau să prevină atacurile sau intruziunile înainte ca acestea să apară. Firewall-urile, sistemele de prevenire a intruziunilor, gateway-urile web și izolarea fizică a cablurilor de rețea și a dispozitivelor sunt toate exemple de controale preventive.
Controalele detective	Caută să detecteze atacurile sau intruziunile în curs sau după (în mod ideal, foarte curând după aceea) au avut loc deja. Sistemele de detectare a intruziunilor, colectarea și revizuirea jurnalelor, sistemele de gestionare a informațiilor și evenimentelor de securitate (SIEM), software-ul AntiVirus și supravegherea video în centrele de date și facilitățile de comunicații sunt exemple de controale detective.
Controalele administrative	Îi conduc pe utilizatori - angajați, facultate, studenți, contractori și parteneri - să urmeze proceduri specifice. Exemplele includ politici împotriva conectării hub-urilor, switch-urilor sau routerelor necinstite la rețea, utilizarea sniff-urilor de trafic din rețea, serviciile de rețea neautorizate și procedurile de aprovizionare a conturilor de acces la rețea.
Controalele tehnice	Impun adesea controale administrative, dar pot limita sau preveni activitatea / traficul rețelei sau pot izola segmente de rețea sau utilizatori pentru a spori securitatea generală. Exemplele includ controlul accesului la rețea, obiecte de politică de grup, autentificare puternică, criptare și tehnologia rețelei private virtuale (VPN).

Controlul rețelei trebuie să fie plasat strategic astfel încât să poată fi controlat și monitorizat tot traficul de rețea care circulă în și din rețelele interne ale universității, adică Intranet-ul său. Aceste controale sunt esențiale pentru funcționalitatea și securitatea rețelei și, prin urmare, trebuie să fie tolerante la erori și să aibă copii de rezervă disponibile. În plus, acestea trebuie să fie capabile să proceseze volumul maxim de trafic de rețea anticipat. Acest lucru este deosebit de important pentru universitățile mai mari, cu lățime de bandă agregată extrem de mare. Tehnologiile utilizate pentru a asigura transmiterea/recepția datelor dar și pentru a securiza rețelele sunt enumerate în tabelul 3.

Tabelul 3.

Comenzile tipice ale perimetrului

Echipamentele/Comenzile	Descrierea
Routere	Routerul este de obicei capabil să permită sau să refuze conexiunile, dar scopul său principal este să direcționeze traficul la frontiera de rețea
Firewall	Firewall-urile blochează sau limitează traficul, de obicei prin portul TCP / UDP
IDS / IPS	Un sistem de detectare a intruziunilor și / sau un sistem de prevenire a intruziunilor adaugă un strat suplimentar de protecție, examinând, limitând sau blocând traficul care a fost permis prin firewall-ul de frontieră
Prevenirea pierderii de date (DLP)	Unele soluții DLP inspectează tot traficul de rețea pentru a detecta sau bloca datele confidențiale de la ieșirea din Intranet
Firewall-uri „Next Generation”	Termenul „NextGen” este un termen de marketing folosit de unii furnizori pentru a implica un nivel mai ridicat de performanță și, prin urmare, un nivel mai ridicat de protecție. În timp ce multe dintre aceste produse funcționează așa cum sunt publicate, acestea îndeplinesc în esență aceleași funcții sau funcții combinate ca firewall și tehnologia IDS / IPS.
Web Gateway	Un gateway web sigur nu stă neapărat la perimetru, ci filtrează traficul web, oferind funcționalități IDS / IPS mai granulare pentru trafic sau conținut web.
Traducerea adreselor de rețea (NAT)	Nu este strict un control de securitate, dar, NAT limitează vizibilitatea punctelor finale din cadrul Intranetului universitar de potențialii atacatori de pe Internet.

Concluzii

Scopul acestui articol a fost de analiza politicile de securitate pentru dispozitivele terminale din rețelele universitare. O politică de securitate, așa cum s-a explicat în prima secțiune, este un document unic pentru fiecare organizație, care identifică reguli și proceduri pentru toate persoanele care accesează și utilizează activele și resursele IT ale unei organizații.

În cadrul Instituțiilor Academice, care prestează un spectru larg de servicii electronice, mai ales începând cu anul 2020 și pandemia cu Covid-19, atunci când a avut loc migrarea studiilor din mediul tradițional în online, implementarea politicelor de securitate joacă un rol strategic, deoarece stabilește termenii în care angajații și studenții pot utiliza infrastructura IT universitară.

Implementarea controalelor de securitate care să satisfacă așteptările administrației universitare și configurarea corectă a dispozitivelor de rețea diminuează riscurile cibernetice asociate domeniului educațional.

Mulţumiri.

Vreau sa adresez mulţumiri cu totul speciale, doamnei Alexei Arina, Lect.univ., pentru coordonarea şi ajutorul oferit care a dus la bun sfârşit acesta lucrare. Mi-a permis să mă folosesc de propriile-i instrumente de investigare, şi nu m-a lipsit de sprijin şi orientare.

Referinţe

1. Information Security Manager, IT Security Policy, Version 3.0, Feb 2020, 11 p. Disponibil: *https://www.hud.ac.uk/media/policydocuments/IT-Security-Policy.pdf*
2. A Case Study Tarumanagara University, Campus Network Design And Implementation Using Top Down Approach, 2011 , 6 p. Disponibil: *http://eprints.undip.ac.id/36065 /1/ bagus_mulyawan.pdf.*
3. Information Security Plan, April 27, 2020, 27 p. Disponibil: *https://www.wku.edu/policies/docs/index.php?policy=79*
4. Catherine Paquet, Implementing Cisco IOS Network Security (IINS 640-554) Foundation Learning Guide, 2nd Edition, Nov 30 , 2013, 784 p, Chapter 3 Security Policies. Disponibil: *https://www.ciscopress.com/articles/article.asp? p=1998559 & s eqNum=3.*
5. EDUCAUSE, Network Security. Disponibil:*https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/network-security*
6. MALISENCU, D. Elaborarea politicilor de securitate pentru dispozitivele terminale din rețelele universitare. Teză de licență, Municipiul Chișinău (MD): Universitatea Tehnică a Moldovei, 2021.