Universitatea de Arte
George Enescu
Iași

MINISTERUL EDUCAȚIEI ȘI CERCETĂRII ȘTIINȚIFICE
Universitatea de Arte "George Enescu"
Serviciul de Informatizare și Activități tipografice

Str. Costache Negruzzi 7-9 T: 0040 232 / 237301 informatizareuage@gmail.com
700126, Iași, RO www.arteiasi.ro

STRATEGIA DE SECURITATE IT

1. Securizarea serverelor și monitorizarea traficului de internet.

În rețeaua UAGE există servere ce utilizează sisteme de operare tip Microsoft Windows Server și care găzduiesc aplicații cu acces online pe bază de IP real. Aceste aplicații deservesc diversele departamente ale universității, incluzând totodată baze de date: University management system (UMS) - pentru secretariatele facultăților, Liberty - pentru Bibliotecă, Premier – pentru Contabilitate și Administrativ, Legis – pentru Oficiul juridic și Resurse umane, Registrul Matricol Unic – pentru secretariatele facultăților. În afara serverelor enumerate mai există servere ce utilizează sisteme de operare de tip Linux, folosite fie ca și router - cazul serverului ce susține traficul de internet pentru sediile din str. Costache Negruzzi și cel din str. Sărărie, fie ca și server pentru site-urile aparținând UAGE, server de e-mail, server pentru aplicații cloud, e-learning etc.

În afara acestora, mai exista un router hardware tip Cisco, ce deserveste traficul de internet pentru sediul din str. Cuza Vodă.

Configurarea, securizarea și monitorizarea acestor servere se face conform următoarelor proceduri:

- **Serverele bazate pe Microsoft Windows Server**
  - Instalarea Microsoft Windows Server se execută doar pe stații performante, cu arhitectură tip server, specifică funcționării non-stop;
  - Alimentarea de la rețeaua electrică a serverului se face prin intermediul unei unități UPS, ce asigură protecție la șocuri electrice și funcționează ca o baterie atunci când se înregistrează întreruperi ale alimentării cu electricitate;
  - Sistemul de operare poate fi configurat astfel încât, atunci când bateria ajunge la un nivel minim stabilit, acesta să poată lansa comanda de închidere a serverului, pentru a evita închiderea bruscă a acestuia, fapt ce poate duce la coruperea sau pierderea datelor stocate sau la deteriorarea componentelor hardware;
  - Este recomandată eliminarea altor conturi de utilizator și păstrarea unui singur cont de administrator, în cazul serverelor ce găzduiesc aplicații și baze de date cu acces online, fără a fi nevoie de deployment pe stații client din rețeaua internă;
  - Parolarea alfanumerică (conține litere și cifre) a conturilor de administrator;
  - Se actualizează zilnic, de pe site-ul Microsoft, cu update-uri de securitate și stabilitate a sistemului de operare;

- Instalarea de aplicații antivirus performante și programarea updatării zilnice (cel puțin) a bazei acestora de date urmată de scanarea fișierelor serverului. Dacă este cazul, se poate activa și configura, conform nevoilor, protecția firewall;
- Se recomandă instalarea și configurarea doar a acelor opțiuni ale sistemului de operare (server role) necesare scopului dedicat al serverului;
- Este recomandată evitarea instalării de aplicații care nu sunt absolut necesare scopului dedicat al serverului (codecuri, playere, browsere, office etc.)
- Monitorizarea la distanță (remote) a serverului se poate face activând funcția de remote acces a sistemului de operare, configurată cu acces doar pentru contul de administrator. Se recomandă, de asemenea, activarea și configurarea aplicației firewall pentru remote acces;
- Pentru serverele unde, din diverse motive tehnice, nu poate fi activat și configurat satisfăcător un firewall, se recomandă dezactivarea funcției remote acces și înlocuirea acestea cu o aplicație ce permite controlul serverului la distanță printr-o conexiune virtuală securizată;
- Sistemul de operare Windows trebuie programat să realizeze backup-ul datelor ce le conține și a configurărilor sale la sfârșitul fiecărei săptămâni de lucru. Un astfel de backup se face pe un alt dispozitiv de stocare decât HDD-ul pe care sistemul este instalat și care conține datele ce trebuie salvate. Astfel, copia de siguranță se poate realiza pe un alt HDD intern, pe un HDD extern, pe un network adress storage securizat (NAS) sau pe un alt calculator din rețeaua internă dedicat;
- Se recomanda realizarea unor copii de siguranță (backup) și cu o terță aplicație (Acronis, Clonezilla etc.) decât cea oferită de sistemul de operare, cel puțin o dată pe lună;
- În plus, tot pentru siguranța datelor, se recomandă, de la bun inceput, instalarea sistemului de operare pe o matrice RAID de tip mirroring.

❖ **Serverele bazate pe sisteme de operare Linux**

Procedurile de configurare, securizare, monirorizare și backup pentru sistemele server ce rulează sisteme de operare Linux (distribuții Linux) sunt, în principiu, aceleași ca la serverele bazate pe Microsoft Windows.

Avantajele sistemelor de operare Linux sunt legate de gratuitatea lor, de numărul mare de distribuții diponibile și de faptul că sunt mai puțin expuse atacurilor de tip malware sau hacker. Dezavantajele față de sistemele de operare Windows sunt legate de numarul inferior de aplicații consacrate dezvoltate pentru ele, de suportul tehnic al celor care le produc și de dicerse probleme de compatibilitate și stabilitate.

Diferențele între distribuțiile Linux cât și față de Windows derivă și din scopul, rolul pe care îl îndeplineste un server. În general serverele Linux sunt preferate pentru: router internet, server pentru hostare site-uri, server de email, cloud etc. Astfel, sunt de menționat următoarele proceduri:

- Actualizarea zilnică cu update-uri de securitate și stabilitate a sistemului de operare se face doar de pe unul dintre serverele dedicate distribuției de Linux folosite și nu de pe serverele altor distribuției. Este necesară, după caz, verificarea

periodică a configurării automate de update, în vederea confirmării adreselor serverelor pentru download;

- În afară de update-urile menționate se recomandă verificarea periodică (de obicei 6-12 luni) pentru apariția unei versiuni superioare a distribuției. Se recomandă ca această nouă versiune să fie testată pe un server de probă înainte de a fi instalată pe serverul de lucru;
- Accesul, monitorizarea și alertarea remote este mult mai facilă în cazul serverelor cu distribuții Linux, oferta de aplicații gratuite fiind mai bogată. Se pot configura alerte pentru breșe de securitate, pierderea conexiunii internet sau shutdown neprogramat ce pot fi primite de către administratorul de sistem pe mail sau SMS;
- Serverele dedicate traficului de internet (routere) pot fi configurate astfel încât să aibă o listă de excluderi (acces blocat) pentru adrese de internet sau IP-uri cunoscute sau înregistrate ca fiind amenințări de securitate;
- În afară de metodele de backup menționate în cazul serverelor Windows, metode ce pot fi aplicate asemănător și pentru Linux, se recomandă și salvarea configurației setărilor (config) sistemului de operare, după ce a fost testat cu succes. Aceasta se realizează mai ușor decât un backup clasic și este foarte utilă atunci când se înregistrează un update necorespunzător sau o corupere, din diverse motive, a kernelului distribuției, ori când dorim reinstalarea distribuției pe un server similar sau asemănător (pentru sistemele linux nu e nevoie de serial sau activare la o nouă instalare);

2. Utilizarea stațiilor de lucru și a rețelei de internet

În afară de servere, rețeaua UAGE pune la dispoziție utilizatorilor, prin intermediul adminitratorilor de rețea, elemente de rețea active (routere WiFi, switch-uri), câteva clase de adrese IP interne, calculatoare, siteme de operare Microsoft Windows și aplicații compatibile cu licență.

Dintre procedurile de urmat în vederea utilizării corespunzătoare, atât de către membrii Serviciului Informatizare cât și de către utilizatorii obișnuiți, a inventarului hardware-software și a facilităților puse la dispoziție în rețeaua informatică a UAGE, sunt de menționat:

- Fiecare utilizator, angajat al universității, primește, în funcție de cerințele postului și de priorități, conform unui referat aprobat de către departamentele specifice (contabilitate, adminstrativ, conducerea universității) o stație de lucru (PC sau laptop). Această stație îi este atribuită în inventar, din inventarul existent al universității, fie prin achiziționare (echipament nou), fie în urma ocupării unui post eliberat care a avut în inventarul sau o stație de lucru. Același lucru este valabil și în cazul perifericelor, consumabilelor sau echipamentelor de birotică atașate (boxe, cameră web, claviaturi, printere, cartușe etc.) și a aplicațiilor software utilizate. Prioritățile, necesitățile și nivelul de acces la facilități hardware și software (inclusiv birotică și accesorii) și la facilitățile rețelei UAGE sunt stabilite individual sau colectiv (după caz, angajați sau studenți);

- Fiecare stație are atribuită o adresă IP prin care se identifică în rețea și se poate conecta la internet și la aplicațiile sau bazele de date de pe servere. Pe fiecare stație de lucru se instalează doar software cu licență sau freeware, open source, după caz. Este interzisă instalarea de către utilizatori a altor aplicații fără licență sau altele decât cele instalate de către membrii Serviciului Informatizare cât și stergerea sau modificarea adresei IP. De asemenea este interzisă stocarea și utilizarea pe stația de lucru de conținut ce încalcă legile dreptului de autor sau alte legi în vigoare. Fiecare utilizator își asumă în orice moment atât aplicațiile rulate cât și conținutul stocat pe stația lui de lucru;
- Nu este permisă schimbarea structurii hardware a stațiilor de lucru și nici deteriorarea intenționată sau prin manevrarea necorespunzătoare a echipamentelor primite în inventar sau altor echipamente apatinând infrastructurii informatice a universității;
- Accesul fiecărui utilizator la stația de lucru se face pe baza de user și parola individuală. Userul sau parola pot fi schimbate la cerere de către personalul IT. Aceste date trebuie știute doar de către utilizator;
- Modificarea datelor din aplicațiile cu acces online la bazele de date găzduite de serverele din rețeaua UAGE se face conform nivelului de acreditare pentru aplicația respectivă a fiecărui utilizator, cu acces tot pe bază de user și parolă, fiind asumată de utilizatorul respectiv;
- Este necesar ca fiecare utilizator să salveze periodic datelor sensibile, necesare, pe alte dispozitive decât stația de lucru: stick USB, HDD extern, mail etc., pentru a se evita pierderea lor în caz de avarie tehnică;
- Se recomandă scanarea antivirus a tuturor dispozitivelor externe introduse în porturile stației de lucru (stick USB, HDD extern, e-SATA etc.). De asemenea, se recomandă ca aceste dispozitive de stocare să nu mai fie folosite pe nicio altă stație de lucru, în vederea evitării infectării malware;
- Membrii serviciului informatizare nu își asumă trainingul utilizatorilor în vederea folosirii unor aplicații ce țin de specificul activității fiecăruia, conform fișei postului (aplicații Office, editare, grafică, prelucrare audio-video etc.).
- Studenții universității au acces la laboratoarele universității, ce utilizează tehnică de calcul, sub supravegherea cadrelor didactice sau laboranților și se pot loga la stațiile de lucru doar pe conturi de utilizator cu acces limitat (nu au privilegii de administrator, nu pot modifica setarile sistemului);
- Accesul la resursa de internet a universitții, fie că se face prin adresă IP fixă sau prin IP dinamic (WiFi), prin intermediul browserelor de net, aplicațiilor de tip messenger, mail, cloud etc., se face conform legilor în vigoare și regulamentelor universității. Este interzisă accesarea de siteuri ori adrese cu conținut neadecvat sau care pot propaga atacuri malware, descărcarea de conținut care nu respectă legislația drepturilor de autor. Nu este permisă, de asemenea, utilizarea de aplicații ce au ca efect exploatarea în exces a rețelei de internet (flodarea) sau pentru atacuri malware ori de tip hacker asupra retelei UAGE ori a altor rețele, browsing anonim etc. O parte dintre aceste interdicții și recomandări este cuprinsă și în prevederile 2703/05.07.2010 aprobat de conducerea universității.

- ❖ În cazul nerespectării acestor proceduri/recomandări, care sunt aduse la cunoştinţa utilizatorilor în momentul predării echipamentelor, se trece la identificarea utilizatorilor care le-au încălcat şi apoi sesizarea conducerii universităţii sau, după caz, autorităţilor îndreptăţite a aplica prevederile regulamentelor universităţii şi legislaţiei specifice în vigoare. De asemenea, se interzice accesul la reţea a utilizatorului respectiv până la clarificarea situaţiei astfel create;

3. Remediere a defecţiunilor tehnice ce pot apărea în reţeaua de internet

În reţeaua informatică a UAGE pot apărea defecţiuni tehnice sau avarii datorate defectării unor echipamente, ori utilizării necorespunzătoare de către utiluizatori a unor resurse hardware şi software ale reţelei.

Una dintre cele mai importante avarii, care afectează procesul de lucru al colectivului universităţii şi constituie prioritate spre rezolvare, o reprezintă întreruperea conexiunii de internet. Pentru remedierea acesteia se recomandă următoarele **proceduri**:

- ❖ **Identificarea tipului de defecţiune**
  - ➢ Se verifică accesul în exterior de pe serverele cu rol de router, DNS primar (pentru sediile din str. Costache Negruzzi) şi secundar (sediul din str. Sărărie 189)
  - ➢ Dacă serverul nu are ieşire la internet se verifică cu un tester de reţea sau cu alte mijloace specifice starea de funcţionare a convertorului de fibră optică şi a distribuitorului de fibră către reţeaua internă. Se mai verifică de asemenea, luând legătura cu centrul ROEDU (furnizorul serviciilor de internet pentru sistemul public de învăţământ) din Iaşi, situat în incinta Univ. Al. I. Cuza, dacă nu există întreruperi ale semnalului în sistemul public (avarii, lucrări etc.). Tot în acest caz se verifică dacă sistemul de operare Linux nu a fost corupt din pricina unui update sau ca urmare a unui atac informatic;
  - ➢ Dacă serverul tip router are ieşire la internet se verifică accesul din interiorul reţelelor interne către router. Apoi, prin excludere şi deconectări succesive, se verifică elementele active de reţea (switchuri, routere WiFi) de pe fiecare etaj în parte, pentru a micşora aria de căutare a posibilei defecţiuni, până la identificarea acesteia;
  - ➢ Aceleaşi proceduri se aplică şi în cazul unui router internet dedicat de tip Cisco.

- ❖ **Remedierea defecţiunii**

În funcţie de tipul defecţiunii identificate sunt de urmat o serie de proceduri intre care menţionăm:

- ➢ Se aşteaptă restabilirea semnalului internet în sistemul public, anunţând toate departamentele universităţii de existenţa întreruperii şi timpul estimat împreună cu responsabilii ROEDU până la restabilirea semnalului;
- ➢ Înlocuirea convertorului sau a distribuitorului de fibră optică;
- ➢ Înlocuirea sau repararea eventualelor surse defecte de alimentare cu curent electric a echipamentelor de reţea;

- Reconfigurarea hardware/software (după caz) sau înlocuirea serverului Linux pentru internet sau a routerului Cisco dedicat;
- Înlocuirea switch-urilor sau routerelor WiFi identificate ca defecte în rețea sau reconfigurarea celor compromise din punct de vedere software. După caz, se încearcă și identificarea împrejurărilor care au dus la compromiterea funcțională a routerelor configurabile;
- Verificarea cablajelor din patch panel, switch, router sau prize din rețeaua de calculatoare pentru a vedea dacă nu au fost reconectate necorespunzător (accidental sau intenționat);
- Urmărirea traficului în și dinspre rețeaua internă spre exterior, identificarea și izolarea stațiilor client cu trafic neobisnuit. Verificarea stațiilor de lucru sau serverelor din aria unde a fost identificată "sursa" întreruperii în rețea, pentru a stabili dacă prin acea stație s-a desfășurat un atac informatic cauzat fie de infectărea cu malware, fie de folosirea de către un utilizator a unor aplicații sau proceduri nepermise;

4. Securizarea adreselor de email instituționale

Serviciul de Informatizareși Activități tipografice pune la dispoziția comunității academice serviciul de email folosit pentru comunicații academice. Utilizatorii unui cont de email se supun regulilor și procedurilor generale de securitate informatică.

- Accesul la email (client web-based) se realizează din pagina web principală a universității, www.arteiasi.ro . Se folosește protocolul de securitate destinat transferului de informație criptată, https, cu un certificat digital gratuit.
- Pe serverul de email este instalată o aplicație antivirus si anti-spam care verifică mesajele. Reprezentanții IT recomandă utilizatorilor să permită accesul mesajelor cu eticheta Spam dar să le direcționeze către un folder pentru a identifica eventuale mesaje "fals pozitive".
- Parola folosită trebuie să fie una puternică formată din minim 8 caractere să conțină litere majuscule, cifre sau/si caractere speciale;
- Parola este confidențială nu se destăinuie și nu se notează în calculator sau la vedere;
- Utilizatorii trebuie să fie conștienți de implicațiile folosirii unei parole neadecvate sau înscrierea acestei adrese pe diverse site-uri, altele decat cele în scopuri academice.
- Utilizatorii pot obține lămuriri de la reprezentanții IT ai Universității dacă sunt ambiguități în privința unui email receptionat chiar si de la persoane cunoscute, pentru a evita atacuri tip phishing sau infectări locale ori în rețea.

Întocmit,
Dr. Ing. Bogdan Anghel

Inf. Adriana Neica

Șef Serviciu de Informatizare și Activități tipografice
Inf. Emilian Popa