ROMÂNIA
MINISTERUL EDUCAŢIEI NAȚIONALE
UNIVERSITATEA DIN ORADEA

Adresa: C.P. nr.114, Oficiul Poştal Oradea 1,Str. Universităţii nr. 1, Oradea, România
Telef: +40 0259 / 432830 +40 0259 / 408 190, Fax: +40 0259/ 432789
E-mail: rectorat@uoradea.ro, Pagina web: www.uoradea.ro

REGULAMENT

de monitorizare a Resurselor Informatice şi de Comunicaţii

AVIZAT	APROBAT
Consiliul de Administrație (CA)	**Senatul Universității din Oradea (SUO)**
Hotărîrea CA nr. 27	Hotărîrea SUO nr. 29
Data: 20.05.2013	Data: 17.06.2013

REGULAMENT de monitorizare a Resurselor Informatice şi de Comunicaţii

Introducere

Monitorizarea RIC pentru asigurarea securităţii sistemului este o metodă utilizată pentru a confirma funcţionalitatea şi eficienţa măsurilor de securitate. Această activitate constă în următoarele (fără a se limita numai la aceste exemple):

- Detectarea automată a intruşilor prin intermediul sistemelor de înregistrare (logare).
- Jurnale *Firewall*
- Jurnale ale activităţii conturilor utilizator
- Jurnale ale scanărilor reţea
- Jurnale ale aplicaţiilor
- Jurnale ale solicitărilor de suport tehnic
- Jurnale ale erorilor din sisteme şi servere.

Scopul

Scopul Regulamentului de Monitorizare a RIC este stabilirea regulilor şi procedurilor pentru verificarea funcţionalităţii şi eficienţei măsurilor de securitate. De asemenea această activitate urmăreşte detectarea situaţiilor de evitare sau dezactivare a controalelor. Unul din beneficiile monitorizării securităţii este identificarea din timp a tentativelor de fraudă sau a infracţiunilor şi a vulnerabilităţilor sistemelor componente ale RIC. Alte beneficii includ: rezolvarea reclamaţiilor, monitorizarea serviciilor, estimarea performanţelor sistemelor în vederea întocmirii planurilor de modernizare, etc.

Audienta

Regulamentul de Monitorizare a RIC al Universităţii din Oradea se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a Universităţii din Oradea.

Definiţii

- *Resurse Informatice şi de Comunicaţii* (RIC): toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unităţi de stocare, şi toate activităţile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepţioneze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframeuri, servere, calculatoare personale, calculatoare-agendă (*notebookuri*, *laptop*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la reţea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicaţii, medii de reţea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilităţile, programele şi

datele care sunt proiectate, construite, puse în funcţiune (operaţionale) şi menţinute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia.

- *Inginerul de sistem/Administratorul de reţea* îndeplineşte şi funcţia de *Administrator al Resurselor Informatice si de Comunicare* (ARIC)[1], precum şi pe cea de *responsabil cu Securitatea RIC*[2]. Este persoana de contact intern şi extern a Universităţii din Oradea pentru orice problemă în legătură cu securitatea RIC. Directorul SMIIT poate numi o altă persoană în funcţia de responsabil cu probleme de securitate.
- *Utilizator*: O persoană, o aplicaţie automatizată sau process utilizator autorizat de către Universitatea din Oradea, în conformitate cu procedurile şi regulamentele în vigoare, să folosească Resursele Informatice şi de Comunicaţii.
- *Abuz de privilegii:* Orice acţiune întreprinsă în mod voit de un utilizator, care vine în contradicţie cu regulamentele Universităţii din Oradea şi/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acţiunii respective.
- *Reţea locală (LAN):* O reţea de comunicaţii de date ce este distribuită pe o zonă restrânsă (de regulă la nivelul unui grup de lucru). Reţeaua locală oferă comunicaţii între calculatoare şi periferice la o viteză de transfer mare şi cu puţine erori

REGULAMENT de monitorizare a Resurselor Informatice şi de Comunicaţii

1. Monitorizarea Resurselor Informatice şi de Comunicaţii (RIC) se va face astfel încât să fie posibilă detectarea în timp util a atacurilor informatice şi a situaţiilor de încălcare a regulamentelor de securitate. Echipamentele utilizate pentru monitorizare (dedicate sau nu) vor urmări şi înregistra:

   - Tipul traficului (ex. structura pe protocoale şi servicii) extern şi conţinutul acestuia în cazurile în care acest lucru se impune sau este ordonat.

   - Tipul protocoalelor şi a echipamentelor conectate la RIC, conţinutul acestuia în cazurile în care acest lucru se impune sau este ordonat.

   - Parametrii de securitate pentru sistemele individuale (la nivelul sistemelor de operare).

2. Fişierele jurnal vor fi examinate regulat în vederea detectării eventualelor atacuri informatice şi abateri de la regulamentele de securitate ale Universităţii. În această categorie intră următoarele (fără a se limita doar la acestea):

   - Jurnale ale sistemelor de detectare automată a intruşilor;

   - Jurnale *Firewall*;

   - Jurnale ale activităţii conturilor utilizator;

   - Jurnale ale scanărilor reţea;

[1] Responsabil la nivelul instituţiei cu administrarea RIC ale Universităţii din Oradea
[2] Până la înfiinţarea postului de Ofiter responsabil cu Securitatea RIC (OSRIC)

- Jurnale ale aplicaţiilor;
- Jurnale ale solicitărilor de suport tehnic;
- Jurnale ale erorilor din sisteme şi servere.

3. Serviciul Management Integrat IT, sau personalul autorizat al Departamentelor / Centrelor sau Facultăţilor, va efectua, în mod regulat (cel puţin o dată la şase luni), verificări pentru detectarea:
   - Echipamentelor de reţea conectate neautorizat;
   - Parolelor utilizator care nu respectă regulamentele
   - Serviciilor de reţea neautorizate;
   - Serverelor de pagini de web neautorizate;
   - Echipamentelor ce utilizează resurse comune nesecurizate;
   - Utilizării de modem-uri neautorizate;
   - Licenţelor pentru sistemele de operare şi programele instalate.
4. Orice neregulă privind respectarea regulamentelor de securitate va fi raportată către Serviciul Management Integrat IT în scopul efectuării de investigaţii.

Măsuri Disciplinare

Încălcarea acestui regulament se sancţionează prin măsuri disciplinare care pot include:

- In cazul angajatilor UO, se va proceda la suspendarea accesului la resurse, respectiv la alte masuri disciplinare – conform legislatiei in vigoare
- Încetarea relaţiilor contractuale (de colaborare) în cazul contractanţilor, consultanţilor sau voluntarilor;
- Suspendarea accesului la resurse în cazul studenţilor;
- Interzicerea accesului la Resursele Informatice şi de Comunicaţii.

Toate acţiunile care contravin legilor vor fi raportate organelor competente.

Referinţe

1. http://dcd.uaic.ro/?page_id=90
2. http://www.uaiasi.ro/diacd/
3. http://www.usamvcluj.ro/CIC/documente/Plan%20de%20securitate.pdf
4. RFC 1244 – Site Security Handbook: http://www.ietf.org/rfc/rfc1244.txt
5. ISO 17799 – Standard detaliat de securitate:
6. Lege nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei.
7. Lege nr. 676 din 21 noiembrie 2001 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor.

10. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.
11. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
12. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public.
13. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
14. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal.
15. Ordin nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.
16. Ordin nr. 54 din 18 aprilie 2002 privind stabilirea unor situaţii în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidenţa Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.
17. Hotărâre nr. 781 din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu.
18. Lege nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate.