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

privind detectarea viruşilor

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 privind detectarea viruşilor

Introducere

Numărul incidentelor de securitate şi costurile ce rezultă din întreruperea şi restabilirea serviciilor RIC sunt în continuă creştere. Câteva dintre acţiunile care pot fi luate pentru reducerea riscurilor şi scăderea costurilor incidentelor de securitate sunt: implementarea unor reguli severe de securitate, blocarea accesului inutil la RIC, detectarea în timp util şi minimizarea efectelor cauzate de incidente de securitate.

Scopul

Scopul Regulamentului de Detectare a Viruşilor din RIC este de a descrie măsuri ce trebuie luate pentru prevenirea, detectarea şi îndepărtarea programelor de tip virus, vierme sau altele asemănătoare.

Audienta

Regulamentul de Detectare a Viruşilor a Resurselor Informatice şi de Comunicaţii 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.

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

- *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.
- *Virus*: Un program care se auto-ataşează la un fişier executabil sau la o aplicaţie vulnerabilă şi care generează efecte deranjante sau distructive. Un fişier virus se execută în momentul în care este accesat un fişier infectat.
- *Vierme*: Un program care se auto-copiază într-o altă parte a unui sistem informatic. Aceste copii pot fi create pe acelaşi calculator sau pot fi trimise către alte calculatoare prin intermediul reţelei. Prima utilizare a termenului descria un program care se multiplică într-o reţea de calculatoare, folosind resursele sau calculatoarele neutilizate din reţea pentru a distribui aceste copii. Unii dintre aceşti viermi reprezintă o ameninţare la adresa securităţii din cauză că folosesc resursele RIC pentru a se multiplica, cauzând încărcare suplimentară a reţelei. Un vierme este asemănător unui virus prin faptul că se auto-copiază, diferenţa constând în faptul că un vierme nu are nevoie să se ataşeze la anumite fişiere sau sectoare pentru a se multiplica.
- *Cal Troian*: De obicei un program de tip virus sau vierme care este ascuns sub aparenţa unui program atractiv sau inofensiv. Victimele pot primi un astfel de virus prin email sau prin transfer prin reţea sau de pe un mediu de stocare extern.

REGULAMENT privind detectarea viruşilor

1. Toate staţiile de lucru de sine stătătoare sau conectate la reţeaua de comunicaţii a Universităţii, trebuie să utilizeze programe antivirus.

2. Programele antivirus nu trebuie dezactivate.

3. Configuraţia programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului.

4. Frecvenţa actualizărilor automate a programului antivirus trebuie asigurată de către utilizator.

5. Orice server de fişiere conectat la reţeaua instituţiei trebuie să utilizeze un program antivirus în scopul detectării şi curăţirii viruşilor care pot infecta fişierele puse la dispoziţie.

6. Orice server sau *gateway* pentru e-mail trebuie să folosească un program antivirus pentru e-mail şi trebuie să respecte regulile de instalare şi de utilizare a acestui program.

7. Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie raportat imediat Serviciului Management Integrat IT.

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.
8. Lege nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.
9. Lege nr. 455 din 18 iulie 2001 privind semnătura electronică.
10. Lege nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public.
11. HOTĂRÂRE nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică.
12. Ordin nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal.
13. 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.
14. 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.
15. Hotărâre nr. 781 din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu.
16. Lege nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate.