Cuprins

1 Scop si obiective

Menţinerea securităţii reţelelor şi a sistemelor informatice prin managementul noilor versiuni şi a patch-urilor de securitate (patch management) este o practică concepută pentru a preveni în mod proactiv exploatarea vulnerabilităţilor IT existente în cadrul organizaţiei. Prin aplicarea de actualizări de software sau firmware (patch-uri) legate de securitatea sistemelor IT se urmăreşte reducerea sau eliminarea vulnerabilităţilor şi implicit reducerea timpului petrecut şi a cheltuielilor necesare pentru a răspunde atacurilor.
Acest document

- Defineste condiţiile care permit menţinerea nivelului minim de Securitate pentru resursele hardware si software
- Descrie regulile de instalare a versiunilor noi software: firmware, patch-uri securitate etc., in conformitate cu recomandările producătorilor sau masuri de corective recomandate de aceştia.
- Asigura informarea obligatorie a OSE cu privire la vulnerabilităţile si masurile corective corective de securitate care privesc resursele reţelelor şi sistemelor informatice (hardware şi software) identificate si publicate de către producătorii/furnizorii resurselor respective.

2 Domeniul de aplicare

Această procedură se referă în mod specific la vulnerabilităţi care pot fi abordate printr-o actualizare de software sau firmware (patch) şi se aplică tuturor produselor software utilizate pe sistemele IT ale organizatiei.
Cuprinde toate sistemele pentru care organizaţia are responsabilitate administrativă, inclusiv sistemele gestionate sau găzduite de terţi în numele său.

3 Documente de referinta şi conexe

- Legea nr .64/2004 pentru ratificarea Conventiei Consiliului Europei privind criminalitatea informatica, Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal si protectia vietii private in sectorul comunicatiilor electronice,
- Legea nr. 677/2001 pentru protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date,
- Legea nr. 455/2001 privind semnatura electronica, Convenţia privind Criminalitatea Informatică a Consiliului Europei, Declaraţie privind libertatea comunicării pe Internet a Consiliului Europei.
- Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice.
- Directiva (UE) 2016/1148 a Parlamentului European şi a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice în Uniune.
- Ordonanţă de Urgenţă nr. 119 din 22 iulie 2020 pentru modificarea şi completarea Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice.
- HG nr.963/2020 pentru aprobarea Listei serviciilor esenţiale
- HG nr. 976/2020 privind aprobarea valorilor de prag pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul reţelelor şi sistemelor informatice ale operatorilor de servicii esenţiale.
- HG nr. 1003/2020 NORME TEHNICE de stabilire a impactului incidentelor pentru categoriile de operatori de servicii esenţiale şi furnizori de servicii digitale.
- Ordinul nr. 600/2019 privind aprobarea Normelor metodologice de organizare şi funcţionare a Registrului operatorilor de servicii esenţiale.
- Ordinul nr. 599/2019 privind aprobarea Normelor metodologice de identificare a operatorilor de servicii esenţiale şi furnizorilor de servicii digitale.
- Ordinul nr. 601/2019 pentru aprobarea Metodologiei de stabilire a efectului perturbator semnificativ al incidentelor la nivelul reţelelor şi sistemelor informatice ale operatorilor de servicii esenţiale.
- Ordinul nr. 1323/2020 pentru aprobarea Normelor tehnice privind cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice aplicabile operatorilor de servicii esenţiale.
- Ordinul nr. 559/2021 559 privind aprobarea Regulamentului pentru atestarea şi verificarea auditorilor de securitate cibernetică.
- Decizia nr. 88/2020 privind aprobarea Listei standardelor şi specificaţiilor europene şi internaţionale.

4 Definitii si prescurtari

- Resurse Informatice şi de Comunicaţii (RIC): toate dispozitivele de tipărire/imprimare, de afişare, unităţi de stocare precum şi toate activităţile asociate calculatorului care implică utilizarea unui dispozitiv capabil să recepţioneze email, să navigheze pe siteuri Web, cu alte cuvinte, capabil să transmită, stocheze sau sa administreze, date electronice (servere, calculatoare personale, laptop-uri, echipamente conectate la reţea şi controlate prin calculator, telefoane, faxuri).
- Inginerul de sistem/Administratorul de reţea îndeplineşte şi funcţia de Administrator al Resurselor Informatice si de Comunicare.
- Cont de Utilizator: colectie de setari folosite de Windows si alte sisteme de operare pentru a intelege preferintele si pentru a controla fisierele accesate, sarcinile de executat, dispozitivele si resursele care pot fi folosite, etc.
- Un cont de utilizator poate avea urmatoarele atribute:
  - un nume de cont,
  - un identificator unic,
  - o parola
  - o imagine de profil,
  - un tip de utilizator,
  - un grup de utilizatori.
- Utilizator: O persoană, o aplicaţie automatizată sau proces autorizat de către Societatea OSE să folosească Resursele Informatice şi de Comunicaţii, în conformitate cu procedurile şi regulamentele în vigoare.
- **Patch**. Patch-urile software sunt adesea necesare pentru a remedia problemele existente cu software-ul care este observat după lansarea iniţială. Multe dintre aceste patch-uri au legătură cu securitatea
- **Vulnerabilităti.** În securitatea informaţiei, o vulnerabilitate este o slăbiciune a unui calculator sau a unei reţele, ce permite unui atacator să reducă asigurarea informaţiei. Vulnerabilitatea este intersecţia a trei elemente: susceptibilitatea unui sistem sau defectul, accesul atacatorului la defect şi capacitatea atacatorului de a exploata defectul.[1] Pentru a exploata vulnerabilitatea, atacatorul trebuie să dispună de cel puţin o unealtă aplicabilă sau tehnică pentru a se conecta la slăbiciunea unui sistem. În acest context, vulnerabilitatea este de asemenea cunoscută ca suprafaţă de atac.
- **Netbios**. este un acronim pentru Network Basic Input/Output System. Acesta oferă servicii legate de stratul de sesiune al modelului OSI, permiţând aplicaţiilor de pe computere separate să comunice printr-o reţea locală.
- **Lightweight Directory Access Protocol**. Este un protocol de aplicaţie standard deschis, neutru din punct de vedere al furnizorului, pentru accesarea şi menţinerea serviciilor de informaţii de director distribuit printr-o reţea de Protocol Internet. Serviciile de director joacă un rol important în dezvoltarea aplicaţiilor intranet şi Internet, permiţând schimbul de informaţii despre utilizatori, sisteme, reţele, servicii şi aplicaţii în întreaga reţea.
- **Ftp.** Protocolul de transfer de fişiere este un protocol de reţea standard utilizat pentru transferul de fişiere de computer între un client şi server într-o reţea de calculatoare. (File Transfer Protocol, n.d.)
- **SMTP**. Simple Mail Transfer Protocol este un protocol de comunicare pentru transmiterea poştei electronice. Ca standard internet, SMTP a fost definit pentru prima dată în 1982 de RFC 821 şi actualizat în 2008 de RFC 5321 la adăugări SMTP extinse, care este varietatea protocolului în utilizarea pe scară largă astăzi. (Simple Mail Transfer Protocol, n.d.)
- **Simple Network Management Protocol** este un protocol Internet Standard pentru colectarea şi organizarea informaţiilor despre dispozitivele gestionate în reţelele IP şi pentru modificarea acestor informaţii pentru a schimba comportamentul dispozitivului. Dispozitivele care acceptă de obicei SNMP includ modemuri de cablu, routere, switch-uri, servere, staţii de lucru, imprimante şi multe altele.
- **Phishing-ul** este încercarea frauduloasă de a obţine informaţii sensibile, cum ar fi numele de utilizator, parolele şi detaliile cardului de credit, disimulându-se ca o entitate de încredere într-o comunicare electronică. De obicei, efectuate prin falsificarea e-mail sau mesagerie instant, de multe ori direcţionează utilizatorii să introducă informaţii personale la un site web fals, care se potriveşte cu aspectul site-ului legitim.
- **TLS** Transport Layer Security şi predecesorul său acum învechit, Secure Sockets Layer, sunt protocoale criptografice concepute pentru a oferi securitatea comunicaţiilor printr-o reţea de calculatoare. Mai multe versiuni ale protocoalelor găsesc o utilizare pe scară largă în aplicaţii precum navigarea pe web, e-mailul,

mesageria instant şi voice over IP. Site-urile web pot utiliza TLS pentru a securiza toate comunicaţiile dintre serverele şi browserele lor web.

- **HTTPS** Hypertext Transfer Protocol Secure este o extensie a Hypertext Transfer Protocol. Este folosit pentru o comunicare securizată printr-o reţea de calculatoare şi este utilizat pe scară largă pe Internet. În HTTPS, protocolul de comunicare este criptat utilizând Transport Layer Security sau, anterior, predecesorul său, Secure Sockets Layer. Protocolul este, prin urmare, de asemenea, adesea menţionată ca HTTP prin TLS, sau HTTP prin SSL.
- **SSH**. SSH utilizează criptografia cu cheie publică pentru a autentifica computerul la distanţă şi pentru a-i permite să autentifice utilizatorul, dacă este necesar. Există mai multe modalităţi de utilizare a SSH; una este să utilizaţi perechi de chei public-privat generate automat pentru a cripta pur şi simplu o conexiune la reţea şi apoi să utilizaţi autentificarea prin parolă pentru a vă conecta.

5 Descrierea procedurii

5.1 Nivelul minim de securitate a resurselor

Măsurile de mai jos se aplică tuturor dispozitivelor conectate la reţeaua organizaţiei. Exemple de astfel de dispozitive includ echipamente de reţea, servere, desktopuri, laptopuri, tablete, telefoane inteligente, imprimante etc.
Nivelul minim de securitate a resurselor este detaliat pe activitatile majore din ciclul de viata al unui echipament IT, cat si pentru fiecare tip de echipament.
Nivelul minim de securitate a resurselor este detaliat in acest document pentru

- Servere
- Servere Web publice
- Firewall

5.2 Nivelul minim de securitate pentru Servere.

Implementarea acestei cerinte OSE se va efectua de catre in urmatorii paşi

- Securizarea sistemul de operare de bază.
- Instalarea, configurarea şi securizarea software-ul serverului.
- Folosirea de mecanisme adecvate de protecţie a reţelei (de exemplu, firewall, router de filtrare a pachetelor şi proxy).
- Folosirea de procese sigure de administrare şi întreţinere, inclusiv aplicarea de corecţii şi upgrade-uri, monitorizarea jurnalelor, copii de siguranţă ale datelor şi ale sistemului de operare şi testare periodică de securitate.

5.2.1 Securizarea sistemul de operare de bază.

Pentru securizarea sistemului de operare sunt necesari următorii paşi de bază:

5.2.1.1 Aplicarea de Patch-uri şi upgrade-ul sistemului de operare.

Odată ce un sistem de operare este instalat, Administratorul RIC va aplica patch-uri necesare sau upgrade-uri pentru a corecta pentru vulnerabilităţile cunoscute. Orice vulnerabilităţi cunoscute pe care le are un sistem de operare vor fi adresate înainte de a-l utiliza pentru a găzdui un server sau pentru a-l expune în alt mod utilizatorilor de încredere. Pentru a detecta şi corecta în mod adecvat aceste vulnerabilităţi, Administrator RIC este responsabil pentru următoarele activităţi:

- Identificarea vulnerabilităţilor şi a patch-urilor aplicabile
- Atenuarea vulnerabilităţilor temporar, dacă este necesar şi dacă este fezabil (până când corecţiile sunt disponibile, testate şi instalate).
- Instalarea remedierii permanente (patch-uri, upgrade-uri etc.)

5.2.1.2 Întarirea şi configurarea sistemul de operare pentru a aborda securitatea în mod adecvat

Administratorul RIC vor efectua următorii paşi pentru a întări şi configura în siguranţă un sistem de operare de pe un server.

5.2.1.3 Dezactivarea de servicii, aplicaţii şi protocoalelor de reţea inutile

Administratorul RIC va elimina toate serviciile, aplicaţiile şi protocoalele de reţea (de exemplu, IPv4, IPv6) care nu sunt necesare şi dezactivaţi orice astfel de componente inutile care nu pot fi eliminate. Dacă este posibil, va instala configuraţia minimă a sistemului de operare şi apoi va adăuga, elimina sau dezactiva serviciile, aplicaţiile şi protocoalele de reţea după cum este necesar. Tipurile comune de servicii şi aplicaţii care ar trebui, de obicei, să fie eliminate dacă nu sunt necesare (sau dezactivate dacă nu pot fi eliminate) includ următoarele:

- Servicii de partajare a fişierelor şi imprimantelor (de exemplu, Partajarea fişierelor şi imprimantelor de către Sistemul de intrare/ieşire de bază al reţelei Windows [NetBIOS], FTP)
- Servicii de reţea wireless
- Programe de control de la distanţă şi de acces la distanţă, în special cele care nu îşi criptează puternic comunicaţiile (de exemplu, Telnet)
- Servicii de director (de exemplu, Lightweight Directory Access Protocol [LDAP], Network Information System [NIS])
- Servere şi servicii web
- Servicii de e-mail (de exemplu, SMTP)
- Compilatoare de limbi şi biblioteci
- Instrumente de dezvoltare a sistemului
- Instrumente şi utilităţi de gestionare a sistemului şi a reţelei, inclusiv Simple Network Management Protocol (SNMP).
- Administratorul RIC va determina serviciile care urmează să fie activate pe un server.

5.2.1.4 Configurarea autentificării utilizatorilor sistemului de operare

Pentru servere, Administratorul RIC va defini utilizatorii autorizaţi care pot configura sistemul de operare sunt limitaţi la un număr mic de administratori de server desemnaţi. Pentru a impune restricţii de politică, dacă este necesar, Administratorul RIC va configura sistemul de operare pentru a autentifica un utilizator potenţial, solicitând dovada că utilizatorul este autorizat pentru un astfel de acces. Chiar dacă un server permite accesul neautentificat la majoritatea serviciilor sale, accesul administrativ şi alte tipuri de acces specializat se va limita la anumite persoane şi grupuri. Administrator IT este responsabil pentru următoarele activităţi:

- **Eliminarea sau dezactivarea conturilor implicite care nu sunt necesare.** Se vor elimina (ori de câte ori este posibil) sau dezactiva conturile inutile pentru a elimina utilizarea lor de către atacatori, inclusiv conturile de oaspeţi de pe computerele care conţin informaţii sensibile. Pentru conturile implicite care trebuie păstrate, inclusiv conturile de oaspeţi, va restricţiona sever accesul la conturi, inclusiv modificarea numelor (acolo unde este posibil şi în special pentru conturile de administrator sau la nivel rădăcină) şi parolele pentru a fi în concordanţă cu politica de parolă organizaţională.
- **Dezactivarea conturilor non-interactive** – Administrator IT va dezactiva conturile (şi parolele asociate) care trebuie să existe, dar nu necesită o conectare interactivă. Pentru sistemele Unix, va dezactiva shell-ul de conectare sau va furniza un shell de conectare cu funcţionalitate NULL (de exemplu, /bin/false).
- **Crearea grupurile de utilizatori** – Administrator IT va atribui utilizatori grupurilor corespunzătoare. Apoi va atribui drepturi grupurilor, aşa cum este documentat în planul de implementare.
- **Crearea conturile de utilizator** - Planul de implementare identifică cine va fi autorizat să utilizeze fiecare computer şi serviciile sale. Administrator IT va creea numai conturile necesare si va permite utilizarea conturilor partajate numai atunci când nu există alternative viabile.
- **Configurare sincronizarea automată a timpului** - Unele protocoale de autentificare, cum ar fi Kerberos, nu vor funcţiona dacă diferenţa de timp dintre gazda client şi serverul de autentificare este semnificativă, astfel încât serverele care utilizează astfel de protocoale ar trebui să fie configurate pentru a sincroniza automat timpul sistemului cu un server de timp fiabil. De obicei, serverul de timp este intern pentru organizaţie şi utilizează Network Time Protocol (NTP) pentru sincronizare; serverele NTP disponibile public sunt, de asemenea, disponibile pe Internet.
- **Verificarea politicii de parolă a OSE** - Administrator IT va seta parolele de cont asa cum este definit in I54 PRASI, Procedură privind accesul şi securitatea resurselor şi informaţiilor.
- **Configurarea serverelor pentru a preveni ghicirea parolelor** - Dacă sistemul de operare oferă capacitatea, Administrator IT il va configura pentru a creşte perioada dintre încercările de conectare cu fiecare încercare nereuşită. Dacă acest lucru nu este posibil, alternativa este de a refuza autentificarea după un număr limitat

de încercări eşuate la trei. Contul este "blocat" pentru o perioadă de timp (o ora) sau până când un utilizator cu autoritatea corespunzătoare îl reactivează.

- **Configurarea corespunzătoare a controalelor de resurse.** Administrator IT va seta cu atenţie a controalelor de acces şi va implementa refuzul accesului neautorizat al personalului, va limita privilegiului de execuţie al majorităţii instrumentelor legate de sistem numai la administratorii de sistem autorizaţi si va activa mecanismele de logare / inregistrare si audit, pentru a monitoriza încercările de acces la resurse protejate.

5.2.2 Instalarea în siguranţă a software-ului serverului

În multe privinţe, instalarea şi configurarea sigură a software-ului serverului reflectă procesul de operare discutat în secţiunea Principiul general, ca şi înainte, este de a instala numai serviciile necesare pentru server şi de a elimina orice vulnerabilităţi cunoscute prin patch-uri sau upgrade-uri. Orice aplicaţii, servicii sau scripturi inutile care sunt instalate trebuie eliminate imediat după finalizarea procesului de instalare. În timpul instalării software-ului serverului, Administrator IT va efectua următorii paşi:
In cazul instalarilor de noi servere, se vor urma cerintele si recomandarile producatorului sau a comunitatii opn source.

- In caz de upgrade, se face o salvare a intregului server la nivel de sistem de operare si de aplicatii, prin snapshot (crearea unei imagini identice)
- Se aplica upgrade sau updateul sistemului de operare si se mai creaza un snapshot (o imagine de back identica, care devine noul baseline de la care se poate incepe restaurarea masinii in viitor)
- Va aplicare orice patch-uri sau upgrade-uri pentru a corecta vulnerabilităţile cunoscute în software-ul serverului.
- Va crea un disc fizic dedicat sau o partiţie logică (separată de sistemul de operare şi aplicaţia server) pentru datele serverului, dacă este cazul.
- Va elimina sau dezactiva toate serviciile instalate, dar nu sunt necesare (de exemplu, gopher, FTP, HTTP, administrare la distanţă).
- Va elimina sau dezactiva toate conturile de utilizator implicite care nu sunt necesare create de instalarea serverului.
- Va elimina documentaţia producătorilor de pe server.
- Va elimina toate fişierele de exemplu sau de testare de pe server, inclusiv conţinutul eşantion, scripturile şi codul executabil.
- Va elimina toate compilatoarele care nu sunt necesare.
- Va aplica şablonul de securitate corespunzător sau scriptul de întărire pe server.
- Pentru serverele orientate spre exterior, va reconfigura bannerele de serviciu pentru a nu raporta serverul şi tipul şi versiunea sistemului de operare
- Va configura bannere de avertizare pentru toate serviciile care acceptă astfel de bannere.
- Va configura fiecare serviciu de reţea pentru a asculta conexiunile client numai pe porturile TCP şi UDP necesare

5.2.3 Configurarea controalelor de acces

Majoritatea sistemelor de operare ale serverului oferă capacitatea de a specifica privilegiile de acces individual pentru fişiere, dispozitive şi alte resurse computaţionale pe acea gazdă. Orice informaţii pe care serverul le poate accesa utilizând aceste controale pot fi distribuite potenţial tuturor utilizatorilor care accesează serverul. Este probabil ca software-ul serverului să includă mecanisme pentru a furniza controale suplimentare de acces la fişiere, dispozitive şi resurse specifice funcţionării sale. Este important să setaţi permisiuni identice atât pentru sistemul de operare, cât şi pentru aplicaţia server; în caz contrar, utilizatorilor li se poate acorda prea mult sau prea puţin acces. Administratorul va lua in considerare modul cel mai bun de configurare a controalelor de acces pentru a proteja informaţiile stocate pe servere din două perspective:

- Sa limiteze accesul aplicaţiei server la un subset de resurse computaţionale.
- Sa limiteze accesul utilizatorilor prin controale de acces suplimentare impuse de server, unde sunt necesare niveluri mai detaliate de control al accesului.

Stabilirea corespunzătoare a controalelor de acces poate contribui la prevenirea divulgării de informaţii sensibile sau restricţionate care nu sunt destinate diseminării publice. În plus, controalele de acces pot fi utilizate pentru a limita

utilizarea resurselor în cazul unui atac DoS împotriva serverului. În mod similar, controalele de acces pot impune separarea taxei asigurându-se jurnalele de server nu pot fi modificate de administratorii de server şi potenţial asigura că procesul de server este permis numai pentru a adăuga la fişierele jurnal.
Administratorul RIC va controla accesul la fişierele tipice după cum urmează:

- Software de aplicaţie şi fişiere de configurare
- Fişiere legate direct de mecanismele de securitate:
    - Fişiere hash de parolă şi alte fişiere utilizate în autentificare
    - Fişiere care conţin informaţii de autorizare utilizate la controlul accesului
    - Materiale-cheie criptografice utilizate în serviciile de confidenţialitate, integritate şi non-repudiere
    - Jurnal server şi fişiere de audit de sistem
    - Software de sistem şi fişiere de configurare
    - Fişiere de conţinut server.

Administratorul RIC va implementa si verifica cum ca aplicaţia serverului se va executa numai sub o identitate unică de utilizator individual şi de grup, cu controale de acces foarte restrictive.
Administratorul RIC va seta noi identităţi de utilizator şi de grup pentru utilizarea exclusivă de către software-ul serverului. Aceste noi identitati vor fi independente de toţi ceilalţi utilizatori şi grupuri şi unice.
În timpul iniţializării, serverul poate fi necesar să ruleze cu privilegii rădăcină (Unix) sau administrator/sistem (Windows);
Administratorul RIC va configura serverul pentru

- a reduce privilegiile lui la cele ale utilizatorului de server după efectuarea funcţiilor sale de iniţializare.
- a limita fişierele care pot fi accesate de procesele de service. Aceste procese au acces doar în citire la acele fişiere necesare pentru a efectua serviciul şi nu au acces la alte fişiere, cum ar fi fişierele jurnal de server.

Administratorul RIC va configura controalele de acces la sistemul de operare gazdă server pentru a impune următoarele:

- Procesele de serviciu sunt configurate să ruleze ca utilizator cu un set strict limitat de privilegii (adică nu se execută ca root, administrator sau echivalent).
- Procesele de service pot scrie numai pe server fişiere de conţinut şi directoare, dacă este necesar.
- Fişierele temporare create de software-ul serverului sunt limitate la un subdirector specificat şi protejat corespunzător (dacă este posibil). Accesul la aceste fişiere temporare este limitat la procesele de server care au creat fişierele (dacă este posibil).
- Software-ul serverului nu poate salva (sau, în unele cazuri, citi) fişiere în afara structurii de fişiere specificate dedicate conţinutului serverului.

5.2.4 Constrângerile de resurse ale serverului

Pentru a atenua efectele anumitor tipuri de atacuri DoS, Administratorul RIC va configura serverul pentru a limita cantitatea de resurse de sistem de operare pe care le poate consuma, prin:

- Instalarea conţinutului serverului pe un alt hard disk sau partiţie logică decât sistemul de operare şi software-ul serverului.
- Plasarea unei limite a cantităţii de spaţiu pe hard disk care este dedicată încărcărilor, dacă sunt permise încărcările pe server. Incărcările vor fi plasate pe o partiţie separată pentru a oferi o asigurare mai puternică că limita hard disk-ului nu poate fi depăşită.
- Dacă încărcările sunt permise pe server, aceste fişiere nu pot fi citite de server decât după ce se utilizează un proces de revizuire automată sau manuală pentru a le filtra. Această măsură împiedică utilizarea serverului pentru a propaga malware sau software piratat în trafic, instrumente de atac, pornografie etc.
- Limitarea dimensiunii fiecărui fişier încărcat, ceea ce ar putea limita efectele potenţiale ale unui atac DoS care implică încărcarea multor fişiere mari.
- Stocarea fişierele jurnal într-o locaţie care este dimensionată corespunzător, daca este posibil, pe o partiţie separată.
- Configurarea numărului maxim de procese de server şi / sau conexiuni de reţea pe care serverul ar trebui să le permită.

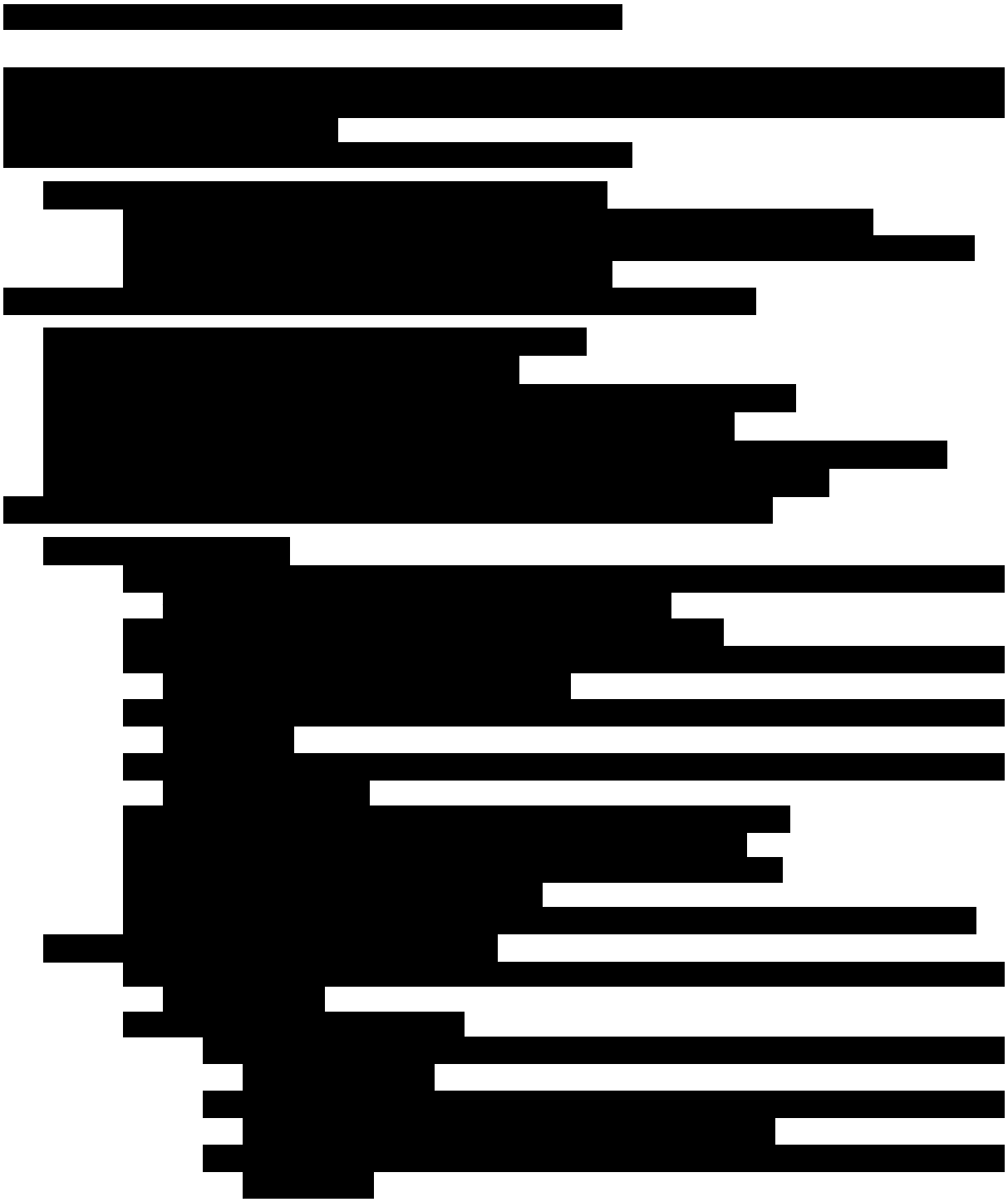
De asemenea, Administratorul RIC va configura timeout-urile de conectare la reţea (timpul după care se renunţă la o conexiune inactivă) la o limită minimă de timp acceptabilă, conexiunile stabilite vor expira cât mai repede posibil, deschizând noi conexiuni pentru utilizatorii legitimi.

5.2.5 Menţinerea securităţii serverului

5.2.5.1 Revizuirea şi păstrarea fişierelor jurnal

Administratorul RIC va revizui fişierele jurnal zilnic şi atunci când a fost observată o activitate suspectă sau a fost emis un avertisment de ameninţare.

Administratorul RIC va arhiva fişierele jurnal pentru o perioadă de timp de 6 luni.



[redacted]

[redacted]

[redacted]

5.6.2 Prioritizarea vulnerabilităţilor.

Se combină datele despre vulnerabilităţi, informaţii despre ameninţări şi oferă un scor de risc uşor de înţeles, astfel încât se poate prioritiza vulnerabilităţile pentru remedierea prioritizata a acestora.
Riscul pe care vulnerabilităţile îl prezintă pentru sisteme şi aplicaţii se bazează pe probabilitatea ca o vulnerabilitate să fie exploatată şi pe impactul generat în cazul în care confidenţialitatea, integritatea sau disponibilitatea activelor informaţionale au fost compromise. Probabilitatea ca o vulnerabilitate să fie exploatată este crescută în relaţie directă cu posibilitatea accesării sistemului sau a aplicaţiei din alte sisteme.
Impactul asupra activelor informaţionale se bazează pe clasificarea informaţiilor activelor. Trebuie luat în considerare impactul (ridicat, moderat sau scăzut) în cazul în care confidenţialitatea, integritatea sau disponibilitatea sunt compromise şi cel mai înalt rating individual de impact pentru expunere utilizat în tabelul de mai jos.
Nivelul de risc

Impact (confidenţialitate, integritate, disponibilitate)	Expunerea		
	Sisteme fără conexiune de reţea la datele de producţie	Sisteme cu conexiune de reţea la datele de producţie (fără expunere în Internet)	Sisteme care sunt disponibile public din Internet
Ridicat	Moderat	Ridicat	Ridicat
Moderat	Scăzut	Moderat	Ridicat
Scăzut	Scăzut	Scăzut	Mediu

5.6.3 Remedierea vulnerabilitatilor – aplicarea patchurilor sau aplicarea de noi versiuni software

Vulnerabilităţile descoperite în timpul scanărilor trebuie remediate pe baza evaluării riscului (vezi Tabelul de la jos) şi a gravităţii vulnerabilităţii identificate de instrumentul de scanare, conform tabelului de mai jos.

Nivelul de risc	Severitatea vulnerabilităţii		
	Scăzută sau Recomandare	Medie	Ridicată sau Critică

Ridicat	La discreţia Administratorului RIC sau a dezvoltatorului aplicatiei	Plan de acţiune în 30 zile, Rezolvare în 6 luni	Plan de acţiune în 14 zile, Rezolvare în 1 lună
Moderat	La discreţia Administratorului RIC sau a dezvoltatorului aplicatiei	La discreţia Administratorului RIC sau a dezvoltatorului aplicatiei	Plan de acţiune în 30 zile, Rezolvare în 6 luni
Scăzut	La discreţia Administratorului RIC sau a dezvoltatorului aplicatiei	La discreţia Administratorului RIC sau a dezvoltatorului aplicatiei	La discreţia Administratorului RIC sau a dezvoltatorului aplicatiei

Tabelul - Remedierea vulnerabilităţilor

Administratorul RIC sau dezvoltatorul aplicatiei dezvoltata intern (dupa caz) analizeaza vulnerabilităţile pentru a ajusta ratingul de severitate, dacă este necesar.
Persoanele care gestionează scanările de vulnerabilităţi trebuie să notifice Seful Departamentului IT lunar (sau cel mai tarziu trimestrial) despre vulnerabilităţi neremediate pe sisteme sau aplicaţii care rulează în producţie.
Sistemele cu valoare ridicată sau cu risc ridicat sunt tratate înaintea altor sisteme.
Toate vulnerabilităţile care se încadrează în Severitate Ridicată sau Critică si Medie, pentru sistemele IT cu impact critic vor fi mai întâi evaluate în ceea ce priveşte gravitatea şi controalele necesare (patching; oprirea/eliminarea serviciilor afectate de vulnerabilitate; adaptarea sau adăugarea controalelor de acces; monitorizarea sporită; creşterea gradului de conştientizare).
Masurile necesare vor fi acţionate prin procedura de management al schimbărilor, dacă sunt generate de Sisteme cu nivel de risc Ridicat si vulnerabilitati de severitate Severitate Ridicată sau Critică sau prin procedura de răspuns la incident, dacă sunt sunt generate de Sisteme cu nivel de risc ridicat si vulnerabilitati de severitate Critica.
Patch-urile disponibile trebuie să fie evaluate de risc, ţinând cont de echilibrul dintre riscurile la instalare şi neinstalare, înainte de a putea fi luată decizia finală cu privire la controalele necesare.
Patch-urile trebuie testate, si mai intai aplicate de către Administratorul RIC dupa cum urmeaza

- se face o salvare a intregului server la nivel de sistem de operare si de aplicatii, prin snapshot (crearea unei imagini identice)
- Se aplica upgrade sau updateul sistemului de operare si se mai creaza un snapshot (o imagine de back identica, care devine noul baseline de la care se poate incepe restaurarea masinii in viitor)

Deciziile de control al vulnerabilităţilor sunt urmărite (şi pot fi auditate) fie prin procedura de management al schimbărilor, fie prin procedura de răspuns la incident.
Seful Departamentului IT, responsabilul echipei de dezvoltare aplicatii interne si Responsabilul NIS primeşte **rapoarte lunare despre gestionarea vulnerabilităţilor**, inclusiv informaţii despre numărul de vulnerabilităţi identificate în fiecare activ organizaţional, de controale suplimentare sunt aplicate, ce probleme nesoluţionate există şi cum s-a schimbat imaginea de la întâlnirea anterioară.
Dacă gestionarea noilor versiuni şi a patch-urilor este externalizată, trebuie să existe contracte de stabilire a nivelului de servicii (SLA) care să răspundă cerinţelor politicii de securitate a organizaţiei şi să descrie responsabilităţile referitoare la patch-uri. Dacă implementarea corecţiilor este responsabilitatea terţei părţi, departamentul IT trebuie să verifice dacă corecţiile au fost aplicate.
Administratorul RIC are urmatoarele responsabilitati pentru infrastuctura IT (servere, sisteme de operare, aplicatii COTS) si responsabilul fiecarei aplicatii dezvoltate intern (pentru aplicatia dezvoltata) :

- Scanarea planificata conform tabelului Tabelul – Frecvenţa scanărilor pentru infrastuctura IT
- Intretinerea unei solutii care sa asigure monitorizarea surselor de securitate pentru vulnerabilităţi, patch - uri şi metode de remediere, precum şi a ameninţărilor emergente, prin analiza siteurilor de specialitate ale producatorilor hardware si software (in cazul produselor COTS) sau a forumurilor de specialitate, in cazul produselor software open source si verificarea saptamanala situatiei vulnerabilitatilor.
- verificarea originii şi integrităţii noii versiuni şi a patch-ului inainte de instalarea acestora.
- implementarea patch-urilor.

Departamentul IT trebuie să menţină un inventar al resurselor IT atât hardware cât şi software. Gestionarea patch-urilor trebuie să încorporeze toate resursele IT existente.
Gestionarea patch-urilor trebuie să aibă prioritate pe baza severităţii vulnerabilităţii pe care patch-ul o adresează.

Dacă patch-urile nu pot fi finalizate în intervalul de timp enumerat în tabelul de mai sus, trebuie să se pună în aplicare controale compensatorii în intervalele de timp de mai sus
Dacă un patch necesită o repornire a sistemului pentru finalizara instalării, repornirea trebuie să aibă loc în intervalele de timp descrise mai sus.

5.6.4 Exceptii

In cazul in care riscurile aplicarii parchurilor de Securitate sunt ridicate, Administratorul RIC propune catre Seful Departamentului IT neaplicarea patchurilor care sunt evaluate a fi periculoase pentru mediile de productie si continuarea operarii fara o versiune de software sau patrch acceptată de furnizor sau producător. Propunerea se inainteaza in forma unui raport scris, Numit **Cerere de exceptie**, care contine atat motivatiile pentru care nu se recomanda aplicarea de patchuri, dar si recomandari pentru aplicarea de masuri tehnice si organizatorice detective sau compensatorii. Aceasta este aprobata de catre Seful Departamentului IT si situatia este integristrata la nivel centralizat la Departament IT intr-un **Registru al Exceptiilor de catre Administratorul RIC**, dar si la nivelul Administratorului RIC in **Evidenta Detectia de vulnerabilitati si aplicarea de Patch-uri**
Odata cu aprobarea exceptiei, Administratorul RIC semneaza **Formularul de alerta la risc** si propune actualizarea **Registrului de riscuri** al departamentului IT.
Formularul de alerta la risc, Registrul de riscuri, Cerere de exceptie si Evidenta Detectia de vulnerabilitati si aplicarea de Patch-uri sunt aprobate de catre Seful Departamentului IT.
Odata cu utilizarea unei versiuni invechite, in functie de tipul masurilor tehnice si organizatorice detective sau compensatorii, se urmareste procedura de achiziţie, dezvoltare şi mentenanţa a sistemelor informatice sau procedura de management al schimbarilor, dupa caz.

6 Responsabilităţi

Conducerea OSE

- Numeşte conducătorii structurilor organizaţionale ale OSE şi le alocă responsabilitatea desfăşurării proceselor operaţionale
- Numeşte proprietarii sistemelor informatice din ariile de business corespunzătoare atribuţiilor stabilite prin ROF
- Aproba profilele organizaţionale din punctul de vedere al utilizării tehnologiei informaţiei şi al controlului accesului

Administrator sistem IT sau dezvoltator de aplicatie software

- Completeaza **Cerere de exceptie**
- se ingrijeste de intretinerea si actualizarea **Evidenta Detectia de vulnerabilitati si aplicarea de Patch-uri**
- se ingrijeste de intretinerea si actualizarea **unui Registru al Exceptiilor** la nivelul Departamentului IT
- completeaza si semneaza **Formularul de alerta la risc**
- propune actualizarea **Registrului de riscuri** al departamentului IT.

Seful Departamentului IT

- Aproba **Cerere de exceptie**
- Monitorizeaza **Evidenta Detectia de vulnerabilitati si aplicarea de Patch-uri**
- Monitorizeaza **Registrul al Exceptiilor** la nivelul Departamentului IT
- Aproba **Formularul de alerta la risc**
- Aproba actualizarea **Registrului de riscuri** al departamentului IT.

Responsabilul NIS

- revizuieşte cererile de schimbare ce pot avea un impact semnificativ asupra securităţii informaţiilor OSE ;
- verifică periodic îndeplinirea cerinţelor definite prin prezenta procedură.