Soluție de securitate aplicabilă sistemelor informatice integrate de management al activităților

Adriana-Meda UDROIU

Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București

meda.udroiu@rotld.ro

Abstract: În condițiile complexe ale mediului operațional actual, instituțiile publice se confruntă cu dificultăți acționale cauzate de intensificarea informațională, accelerarea proceselor de muncă, limitarea resurselor și reducerea timpilor de răspuns. O soluție pentru câștigarea și menținerea unui avantaj competitiv poate fi eficientizarea activităților acestor instituții prin implementarea unui sistem informatic integrat de management care, fructificând dezvoltările curente din domeniul IT, să ofere facilități și servicii de calitate, sigure și interoperabile. În același context asigurarea securității sistemului reprezintă unul din principalele obiective privind digitalizarea serviciilor și produselor oferite.

Cuvinte cheie: sistem informatic integrat de management, soluție de securitate, securitatea informației.

A security solution applicable to information integrated system for management of activity

Abstract: Under the complex conditions of the current operational environment, the public institutions face actional difficulties caused by information intensification, accelerating work processes, limiting resources and reducing response times. A solution for gaining and maintaining a competitive advantage can be to streamline the activities of these institutions by implementing an information integrated system for management of activities which offers quality, safe and interoperable facilities and services, using current IT developments. In the same context, ensuring system security is one of the main objectives for digitizing the services and products offered.

Keywords: information integrated system for management of activities, security solution, information security.

1. Introducere

Dezvoltarea și implementarea pe scară largă a tehnologiei informațiilor și comunicațiilor continuă să producă schimbări pe paliere multiple, fiind elementul caracteristic al societății bazate pe cunoaștere. Se constată infuzarea accelerată cu o componentă informatică a majorității elementelor existenței umane, de la activități care țin de rutina zilnică până la procese critice ce influențează securitatea și apărarea națională. Datorită modului specific de culegere, prelucrare, stocare și diseminare a informațiilor, sistemele și aplicațiile bazate pe tehnologia informațiilor și comunicațiilor contribuie la eficientizarea proceselor și activităților de management și producție din cadrul organizațiilor publice și private.

Unele din instituțiile tradițional ierarhice utilizează încă sisteme hibride și soluții informatice eterogene de management al fluxurilor de informații și al activităților specifice. Lipsa unei abordări cuprinzătoare și a unei arhitecturi interoperabile tehnic și procedural la nivelul unui sistem de importanță strategică poate avea consecințe negative asupra performanței economice și funcționale a instituțiilor cu responsabilități în domeniul securității și apărării. Pentru corectarea acestei deficiențe se consideră necesară proiectarea, testarea operațională și implementarea unui sistem integrat pentru managementul activităților specific acestor instituții.

Sistemul trebuie să asigure, într-o manieră integrată, satisfacerea unor cerințe operaționale fundamentale precum automatizarea managementului proceselor, activităților, resurselor, programelor și proiectelor respectivei instituții. Concomitent, sistemul informatic integrat trebuie să asigure managementul automatizat al circuitului informațional intern, securitatea datelor și a

https://doi.org/10.33436/v30i1y202008

documentelor, precum și un cadru unitar de gestiune a informațiilor și rapoartelor, oferind posibilitatea stabilirii de agende comune între entități determinate.

2. Sistem Informatic Integrat de Management al Activităților (SIIMA)

Managementul informaţiei vizează derularea tuturor proceselor necesare pentru culegerea, verificarea, prelucrarea, diseminarea şi managementul informaţiilor, gestionarea resurselor necesare în scopul desfăşurării acestor procese, precum şi realizarea strategiilor, politicilor şi planurilor care să asigure menţinerea unor relaţii favorabile între nevoia de informaţii şi informaţiile reale, exploatabile, specifice mediului de confruntare modern.

Ca urmare a dezvoltărilor tehnologice fără precedent informaţia constituie unul din elementele fundamentale ale analizei şi evaluării securității sistemelor integrate de management. În acest sens apare ca deosebit de relevant fluxul de informaţii între componentele sistemului, mai ales în contextul unei societăţi internaţionale ce reclamă transparenţă şi promovează valorile universalităţii şi cooperării.

Generarea, evaluarea, compararea şi selectarea opţiunilor optime de răspuns este dependentă de selectarea corectă a datelor și informațiilor provenite din mediul operaţional, ierarhizarea corespunzătoare a acestora şi transformarea lor în informaţii relevante din perspectiva sistemului de evaluare şi analiză strategică.

Mediul operaţional actual depăşeşte cu mult graniţele teritoriului naţional, riscurile, ameninţările şi vulnerabilităţile sunt generate din surse noi precum mediul cibernetic, informaţional, economic sau geo-spaţial. În acest context, este necesară dezvoltarea unor mecanisme de schimb de informaţii, dar şi de implementare şi operaţionalizare a unor proceduri specifice, care să respecte nu doar funcţiile de comandă şi control specifice fiecărei structuri naţionale, ci şi regulile de acces la informaţiile sensibile, astfel încât schimbul să fie oportun şi realizat în timp real, cu respectarea tuturor normativelor specifice care reglementează activitatea instituţiilor publice.

De asemenea, trebuie menţionat că mediul operaţional contemporan, influențat de trecerea la digitalizare și societatea 4.0 a favorizat consacrarea conceptului C4ISR (***C**ommand, **C**ontrol, **C**ommunications, **C**omputers, **I**ntelligence, **S**urveillance and **R**econnaissance*), care integrează, pe lângă dimensiunile de comandă şi control, pe cele de comunicaţii, calculatoare, informaţii, supraveghere şi sisteme de recunoaştere.

Sistemul C4ISR are ca scop obţinerea *superiorităţii informaţionale* şi permite liderului să identifice modul de organizare, perfecţionare, concentrare şi repartizare a resurselor, dar, în acelaşi timp, îi permite să realizeze o analiză a fluxului informaţional şi adoptarea deciziilor privind optimizarea acestuia în vederea luării unei decizii în cel mai scurt timp, în scopul devansării ciclului similar al oponentului și obținerii în acest mod al unui avantaj competițional.

Obiectivul fundamental al sistemelor C4ISR îl constituie obţinerea informaţiilor critice ce vizează şi poate influenţa acţiunea forţelor şi luarea deciziei, la momentul de maximă importanţă, prelucrarea lor pentru a oferi forţelor capacitatea de a dispune de o reprezentare completă a mediului de acțiune, pornind de la aceeaşi imagine operaţională, care să permită fructificarea oportunităţilor în îndeplinirea obiectivelor ce pot fi asociate întregii game de acțiuni.

De asemenea, relevantă este şi culegerea şi prelucrarea datelor provenite de la alte autorități și instituţii, dat fiind dificultatea asigurării supremației informaționale prin utilizarea limitativă a resurselor aflate la dispoziţia instituţiilor din cadrul sistemului naţional de apărare, ordine publică şi securitate naţională.

În concluzie, considerăm că un sistem informatic integrat de management al fluxurilor informaționale și al activităților trebuie să fie proiectat conform unei filozofii de tip C4ISR, într-o cadru cuprinzător, ce asigură reziliența serviciilor și facilitățile necesare pentru achiziția, prelucrarea, stocarea și diseminarea sigură a informațiilor specifice, într-un mediu operațional populat de amenințări cibernetice tot mai complexe.

3. Securitate SIIMA

Conceptele de securitate de bază aplicabile SIIMA, precum și realizarea complianței cu standardele în domeniu reprezintă o problematică extrem de importantă în proiectarea securității sistemului. În acest sens, considerăm că explicitarea conceptelor și aplicarea tehnicilor de securitate cibernetică pentru fiecare concept ce definește securitatea sistemului asigură înțelegerea clară a metodelor și tehnicilor utilizate.

3.1. Confidențialitate

Confidențialitatea este conceptul de securitate care se referă la protecția împotriva dezvăluirii neautorizate a informațiilor. Confidențialitatea asigură nu numai secretul datelor, dar poate și ajuta la menținerea integrității lor.

Confidențialitatea este asigurată din punct de vedere tehnologic prin următoarele caracteristici ale sistemului:

- accesibilitatea funcțiilor sistemului este realizată doar prin intermediul conexiunilor securizate SSL/TLS (Secure Sockets Layer/Transport Layer Security);
- conexiunile dintre modulele aplicative și bazele de date sunt securizate prin SSL/TLS;
- interacțiunile dintre module sunt realizate doar prin canale securizate SSL/ TLS la nivel de transport, iar la nivel aplicativ, integrările sunt realizate prin intermediul platformei de integrare WSO2 Enterprise Integrator, serviciile web sunt securizate prin aplicare WS-Security la nivel de mesaje SOAP, aceasta presupunând semnarea digitală și criptarea mesajelor. Acest deziderat de securitate este implementat atât pentru integrările între modulele sistemului cât și pentru cele realizate cu sisteme externe SIIMA.

3.2. Integritate

Integritatea software-ului are două aspecte. În primul rând, trebuie să se asigure că datele care sunt transmise, procesate și stocate sunt la fel de exacte precum inițiatorul și, în al doilea rând, software-ul funcționează în mod fiabil așa cum a fost planificat/proiectat. Integritatea referențială, conceptul de design al bazei de date și semnarea codului, sunt folosite pentru a asigura acest aspect.

Acest deziderat va fi îndeplinit la toate nivelele sistemului:

A. **La nivelul bazei de date**, prin:
   - mecanisme standard ale sistemului de gestiune a bazei de date de asigurare a integrității datelor în fața unor evenimente neprevăzute asociate sistemului pe care rulează (e.g. defecțiuni);
   - generarea de coduri de tip hash, unic asociate înregistrărilor aferente obiectelor informaționale.

B. **La nivel de documente generate de sistem** – documentele de tip PDF generate de sistem vor fi semnate digital, automat, de către sistem, utilizând un certificat digital x509.

C. **La nivel de transport al datelor,** în procesele de integrare cu alte sisteme, va fi aplicat WS-Security [61], respectiv semnarea digitală a mesajelor SOAP transmise astfel încât acestea să fie non-repudiabile. Această funcționalitate va fi executată prin intermediul platformei WSO2 Enterprise Integrator.

3.3. Disponibilitate

Disponibilitatea este conceptul de securitate care se referă la accesul software-ului, a datelor sau a informațiilor pe care le manipulează. Deși scopul general al unui program de continuitate a afacerii (Bussiness Continuity Plan - BCP) poate fi acela de a asigura minimizarea timpilor de întrerupere și impactul asupra întreruperii afacerii este minim, disponibilitatea nu este doar un concept de continuitate a afacerii, ci și unul de securitate software.

Accesul trebuie să țină seama de aspectele "care" și "când" despre disponibilitate. În primul rând, software-ul sau datele pe care le procesează trebuie să fie accesibile numai de către cei autorizați (care) și, în al doilea rând, trebuie să fie accesibile numai în momentul (când) în care este necesar.

3.4. Autentificare

Autentificarea este un concept de securitate care răspunde la întrebarea "Ești cine pretinzi a fi?" Aceasta asigură faptul că identitatea unei entități (persoană sau resursă) este specificată în funcție de formatul pe care software-ul îl așteaptă și validează sau verifică informațiile de identitate care au fost furnizate. Autentificarea multi-factor, adică folosirea a mai mult de un factor pentru autentificare, este considerată a fi mai sigură decât autentificarea cu un singur factor, unde doar unul dintre cei trei factori, cunoștințe, proprietate sau caracteristică este utilizat pentru validarea acreditărilor. Autentificarea multi-factor este recomandată pentru validarea accesului la sisteme care conțin informații sensibile sau critice.

La nivelul SIIMA, prin intermediul modulului de identitate și drepturi de acces este realizat procesul de autentificare, respectiv sunt determinate rolurile de acces asociate utilizatorului autentificat urmând ca acestea din urmă să fie utilizate de fiecare modul funcțional pentru acordarea dreptului de acces la nivel de funcționalitate și resursă informațională.

3.5. Autorizare

Autorizarea este conceptul de securitate în care accesul la obiecte este controlat în baza drepturilor și privilegiilor acordate solicitantului de către proprietarul datelor sau sistemului, sau conform unei politici. Deciziile de autorizare sunt stratificate în plus față de autentificare și nu trebuie să preceadă niciodată autentificarea. Acțiunile unui subiect, cum ar fi crearea, citirea, actualizarea sau ștergerea (CRUD) pe un obiect, depind de nivelul de privilegii al subiectului. Un exemplu de autorizare bazat pe nivelul de privilegii al subiectului este: un utilizator administrativ poate să creeze, să citească, să actualizeze și să șteargă (CRUD) datele, dar unui utilizator anonim îi este permis doar să citească (R), în timp ce unui manager îi este permis doar să creeze, să citească și să actualizeze (CRU) datele.

În cadrul SIIMA, autorizarea accesului este realizată la nivelul fiecărui bloc funcțional în parte, în baza rolurilor de acces deținut de către utilizator. Rolurile sunt obținute de către modulul funcțional prin intermediul modulului de identitate și drepturi de acces, ca urmare a procesului de autentificare.

3.6. Responsabilitate și non-repudiere

Auditul este conceptul de securitate în care tranzacțiile privilegiate și critice ale companiilor sunt înregistrate și urmărite. Auditul este un mecanism pasiv de control al detectivității.

Non-repudierea abordează negarea acțiunilor întreprinse de un utilizator sau de software în numele utilizatorului. Responsabilitatea pentru a asigura ne-repudierea poate fi realizată prin audit atunci când este utilizat împreună cu identificarea. Auditul este un control detectiv și poate fi și un control disuasiv.

Prin urmare, este imperativ să se înregistreze doar ceea ce este necesar, informații la frecvența potrivită. O bună practică ar fi clasificarea jurnalelor atunci când sunt înregistrate utilizând o schemă de bucketing, astfel încât să se poată sorta cu ușurință volume mari de jurnale atunci când se încearcă să se determine acțiunile istorice. Un exemplu a unei scheme de bucketing poate fi "Informational Only", "Administrative", "Business Critical", "Error", "Security" și "Miscellaneous" etc. Frecvența revizuirii jurnalelor trebuie să fie definită de afacere și aceasta depinde, de obicei, de valoarea software-ului sau a datelor pe care le transmite, procesează și stochează.

În cadrul SIIMA, ca urmare a acțiunilor utilizatorilor, sunt jurnalizate evenimentele care țin de consultarea obiectelor informaționale, respectiv modificarea stării oricărui obiect informațional. Aceste evenimente de audit vor fi stocate în baza de date și vor fi disponibile spre consultare administratorului de securitate al sistemului.

3.7. Securitatea rețelei

În ceea ce privește asigurarea securității infrastructurii, acest aspect va fi realizat prin instalarea de module la nivelul rețelei dedicate serverelor SIIMA, care au următoarele funcționalități:

3.7.1. Componentă de analiză a traficului în rețea ce oferă/permite (https://docs.wso2.com):

- interfață standard „libpcap" pentru capturarea de pachete;
- înregistrarea completă a activității din rețea pentru analiza offline și de tip „forensic";
- efectuarea analizei independente de port a protocoalelor straturilor aplicative;
- suport pentru protocoale de nivel de aplicație, inclusiv DNS, FTP, HTTP, IRC, SMTP, SSH, SSL;
- suport pentru IPv6;
- detectarea și analiza tunelurilor (inclusiv Ayiya, Teredo, GTPv1);
- suport pentru modele de programare bazate pe evenimente;
- suport extins pentru urmărirea și gestionarea stării rețelei în timp;
- analiza conținutului fișierelor schimbate la nivel de protocoale de aplicație, inclusiv calculul MD5 / SHA1 pentru amprentare;
- posibilitatea de a declanșa procese externe arbitrare din limbajul scripting;
- monitorizarea securității rețelei și corelarea evenimentelor apărute în rețea;
- analiza pasivă a traficului de rețea pe un port (atât în timp real, cât și offline), inspectarea traficului și detectarea posibilelor atacuri cibernetice pe bază de semnături;
- înregistrarea log-urilor ce conțin activitatea la nivelul rețelei. Log-urile includ nu numai o înregistrare completă a fiecărei conexiuni de rețea, dar și transcrieri aplicative ca: toate sesiunile HTTP cu URI-urile solicitate, anteturi cheie, tipuri MIME și răspunsurile serverului, solicitări DNS cu răspunsuri, certificate SSL, conținutul sesiunilor SMTP ce permit scrierea;
- realizarea unei serii de analize și detectare, inclusiv extragerea de fișiere din sesiuni HTTP, detectare de malware prin interfațare cu registre externe, raportarea versiunilor de software vulnerabile din rețea, identificarea aplicațiilor web, detectarea atacurilor de tip „SSH brute-forcing", validarea lanțurilor de certificate SSL;
- analiza distribuită.

3.7.2. Componentă de detectare a intruziunilor în rețea ce oferă/permite (http://ode.apache.org):

- un set complet de semnături pentru a detecta amenințările cunoscute, comportament rău intenționat și încălcări de politici de securitate;
- detectarea anomaliilor în traficul pe care îl inspectează, având capabilitatea de utilizare a unui set de reguli propriu specializat pentru amenințările emergente și setul de reguli VRT;
- capabilitatea inspectării traficului multi-gigabit într-o singură instanță;
- un motor puternic pentru ecosistemul de monitorizare a securității rețelei, pentru prevenirea și detectarea intruziunilor în rețea, un motor construit pe un nucleu "multi-thread", modern și scalabil;
- un motor de fluxuri TCP/IP scalabil ce oferă: suport IPv6, decodare tunel (Teredo, IP-IP, IP6-IP4, IP4-IP6, GRE), urmărirea sesiunilor, reasamblare fluxuri, motor IP Defrag;
- suport pentru decodarea pachetelor IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, GRE, Ethernet, PPP, PPPoE, Raw, SLL, VLAN, QINQ, MPLS, ERSPAN;

- decodarea stratului aplicativ pentru: HTTP, SSL, TLS, SMB, DCERPC, SMTP, FTP, SSH, DNS, Modbus, ENIP/CIP, DNP3, NFS, NTP;
- motor HTTP: parsare HTTP bazată pe libhtp, logare cereri HTTP, identificarea, extragerea și înregistrarea fișierelor;
- achiziția de pachete – captură de înaltă performanță (AF_PACKET, PF_RING, NETMAP) – captură standard (PCAP, NFLOG), - mod IPS (Netfilter bazat pe Linux -nfqueue , ipfw bazat pe FreeBSD și NetBSD, AF_PACKET bazat pe Linux, NETMAP);
- suport configurare multi-threading (configurabil de la un thread la zeci de thread-uri);
- încărcarea unei cantități mari de host-uri (IP-uri) bazată pe reputația datelor, potrivire pe reputația datelor utilizând cuvântul cheie "iprep";
- suport nativ pentru accelerare hardware de la mai mulți furnizori, în vederea îmbunătățirii vitezei de capturare, precum și PF_RING și AF_PACKET;
- detectarea automată de protocoale, precum: HTTP pe orice port și să aplice logica corespunzătoare de detectare și logare, acest lucru ajutând foarte mult la găsirea de programe malware și canale CnC.

3.7.3. Componentă de colectare și prelucrare/filtrare a datelor ce oferă/permite (https://www.activiti.org/):

- procesarea datelor preluate de pe server;
- citirea datelor dintr-o multitudine de surse simultan, transformarea și apoi trimiterea către destinația preferată;
- un motor de colectare a datelor, cu capabilități de conectare în timp real;
- unificarea dinamică a datelor din surse diferite și normalizarea datelor în destinații alese;
- pentru orice tip de eveniment, îmbogățirea și transformarea cu o gamă largă de plug-in-uri de intrare, filtrare și ieșire, simplificând în continuare procesul de ingestie ;
- sursă de date, un proces de procesare/filtrare și o destinație;
- un pipeline configurat pentru fiecare tip de date colectat, în care este precizată sursa de date, modelul de procesare/filtrare și destinația.

3.7.4. Componentă de stocare, indexare și analiză date centralizată (http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT):

- reprezintă componenta de analiză date centralizată;
- conține un motor de căutare și analiză distribuit, RESTful capabil să rezolve un număr tot mai mare de cerințe de utilizare;
- stochează datele în mod centralizat, astfel încât să poată fi folosite conform cerințelor diverse, de multe ori în mod neașteptat;
- permite efectuarea și combinarea mai multor tipuri de căutări: structurate, nestructurate, geografice, metrice; interogări full-text, arbori BKD pentru stocarea datelor numerice și de geolocație și o structură bazată pe coloane pentru analiză; gruparea datelor analizate în indecși și indexate pe baza mai multor criterii de indexare care să permită atât căutări full-text cât și analize detaliate și agregări pe datele indexate;
- permite un sistem de clustering inteligent, foarte extensibil;
- permite ca un index să poată stoca potențial o cantitate mare de date care poate depăși limitele hardware ale unui singur nod, oferind posibilitatea de a subdiviza indexul în mai multe fragmente;
- permite împărțirea/scalarea orizontală a volumului conținutului, distribuirea și paralelizarea operațiunilor din interiorul fragmentelor (potențial pe mai multe noduri), sporind astfel performanța;

- permite efectuarea uneia sau mai multor copii ale fragmentelor indexului în ceea ce se numesc fragmente de replici sau replici pe scurt;
- oferă o disponibilitate ridicată în cazul în care un fragment, replică/nod nu reușește;
- permite scalarea volumului/ratei de căutare, deoarece căutările pot fi executate pe toate replicile în paralel;
- permite împărțirea în mai multe fragmente a fiecărui index;
- permite ca un index să poată fi replicat zero (adică să nu existe replici) sau de mai multe ori;
- permite ca fiecare index să aibă fragmente primare (fragmentele originale care au fost reproduse din) și fragmente de replici (copiile fragmentelor primare). Numărul de fragmente și replici să poată fi definit pe index în momentul creării indexului. După crearea indexului se poate modifica din când în când numărul de replici și permite căutări rapide și eficiente;
- deține un spectru foarte larg de modalități de interogare a datelor indexate, precum: l-text, Term-levelsearch, Compund, Joining, Geo-queries, Span, Multi-index, Multi-term, Grouping, Aggregations.

3.7.5. Componentă de vizualizare alerte și consultare a datelor ce permite (https://www.activiti.org/):

- vizualizarea și consultarea datelor din Componenta de stocare, indexare și analiză date centralizată și crearea de vizualizări și dashboard-uri peste aceste date;
- vizualizarea în cadrul unei interfețe a alertelor referitoare la sistemele de detecție a intruziunilor la nivel de host-uri și rețea. Panoul de alerte să conțină cel puțin următoarele informații: numărul de evenimente grupate, numărul IP-urilor sursă distincte pentru o alertă dată, numărul de IP-uri de destinație distincte pentru o alertă dată, numărul evenimentelor pentru o alertă dată pe o bază oră, ultimul eveniment - evenimentul de timp a avut loc ultima dată, semnătură IDS a evenimentului, ID de semnătură eveniment, protocol relativ/ recunoscut în ceea ce privește evenimentul, procentajul grupării evenimentului față de numărul total de evenimente;
- vizualizarea în cadrul unei interfețe a conținutului întregului pachet aferent unui eveniment/alertă; Permite vizualizarea în cadrul unei interfețe a jurnalelor din cadrul componentei de analiză a traficului în rețea;
- vizualizarea în cadrul unei interfețe a datelor aferente asset-urilor IT identificate în cadrul rețelei, precum și a fișierelor HTTP provenite din cadrul Componentei de analiză a traficului în rețea;
- vizualizarea în cadrul unei interfețe a evenimentelor grupate sau nu pe un interval de timp;
- libertatea de a alege modul în care se formatează datele;
- crearea de: histograme, grafice liniare, diagrame piezoelectrice, sunburs;
- preluarea datelor din cadrul Componentei de stocare, indexare și analiză date centralizată și expunerea lor.

În cadrul sistemului SIIMA, prin modulul „Monitorizarea securității rețelei de comunicații SIIMA” vor fi preluate log-urile de sistem, respectiv va fi executată analiza traficului subrețelei în care este rezident sistemul.

3.8. Securitate operațională

Securitatea operațională se realizează prin diferite acțiuni la nivelul structurilor/modulelor SIIMA, cum ar fi:

- implementarea unui mecanism de logare a evenimentelor privind accesul utilizatorilor și a tuturor activităților CRUD ale acestora ce asigură trasabilitatea și non-repudierea

tuturor acțiunilor utilizatorilor în cadrul Platformei pentru managementul integrat al activității. Aceste log-uri ale evenimentelor vor fi stocate în baza de date/sistem de fișiere semnate și criptate pentru a asigura trasabilitatea și non-repudierea acțiunilor utilizatorilor;

- definirea și revizuirea periodică a drepturilor administratorilor în Platforma pentru managementul integrat al activității pe baza principiului "LeastPrivilege";
- efectuarea de analize de tip "hardening" asupra Platformei pentru managementul integrat al activității conform unei proceduri de tip "hardening" bazată pe standarde de configurare sigure;
- implementarea unui mecanism de alertare privind gradul de încărcare al procesoarelor, al memoriei, al spațiului la nivelul infrastructurii serverelor Platformei pentru managementul integrat al activității;
- încorporarea securității informațiilor pe tot parcursul ciclului de viață al dezvoltării software al Platformei pentru managementul integrat al activității;
- efectuarea de review-uri de securitate înainte de lansarea unei noi versiuni sau a unei actualizări a unui modul al Platformei pentru managementul integrat al activității;
- implementarea de practici de control al surselor pentru a verifica integritatea codului sursă în timpul procesului de dezvoltare a Platformei pentru managementul integrat al activității;
- implementarea de tehnici de evaluare a riscurilor (de exemplu, application threat modeling) utilizate pentru a identifica potențialele defecte de proiectare a securității modulelor Platformei pentru managementul integrat al activității și vulnerabilității în timpul procesului de dezvoltare software pentru platformă;
- posibilitatea efectuării de către echipa CERT de scanări periodice de vulnerabilități prin scanare preventivă folosind instrumente de scanare automate și teste de securitate manuale, identificarea listei de vulnerabilități și recomandări de remediere (registru de mitigare a riscurilor) pe platformă și păstrarea unui istoric de vulnerabilități din scanări periodice (lunare);
- monitorizarea proactivă de către echipa CERT a securității prin generarea de tablouri de bord - diagrame de evoluție a scorului de securitate privind vulnerabilitățile asociate activelor IT și a serviciilor IT din cadrul Platformei pentru managementul integrat al activității și evaluarea securității bazată pe vulnerabilitățile identificate și severitatea asociată acestora care vor reflecta nivelul de securitate al platformei, precum și individual pentru fiecare echipament sau serviciu IT din cadrul platformei.

3.9. Autorizarea accesului

Accesul la blocurile funcționale va fi realizat strict în baza rolurilor de acces.

Rolurile de acces de tip DEP-* sunt limitative la domeniu lor de definiție, respectiv la departamentul corespunzător acestora. În mod excepțional rolurile DEP-OWNER vor avea acces suplimentar asupra datelor din cadrul departamentelor subordonate.

Accesul la procesele de business vor fi realizate doar respectând următoarele reguli:

- inițiatorul procesului are acces permanent la procesul inițiat;
- oricare utilizator are acces la datele procesului doar dacă este alocat pentru operarea unei etape din cadrul procesului și doar pentru perioada cât intervine asupra procesului.

3.10. Jurnalizarea operațiilor

SIIMA pune la dispoziție un modul funcțional prin intermediul căruia utilizatorul cu rolul SECURITY-ADMIN poate consulta jurnalul de audit generat de modulele SIIMA prin operarea funcțiilor sale. Acest modul va oferi un API de tip serviciul WEB, disponibil pentru toate modulele SIIMA, prin intermediul căruia acestea pot înregistra evenimente de audit generate la nivelul

modulului. Pentru a nu genera riscuri de securitate prin dezvăluirea neautorizată de conținut, înregistrarea de audit va fi definită prin următorii parametri:

- tipul operației ce poate avea următoarele valori standard: ACCESS, CREARE, MODIFCARE, ELIMINARE;
- autorul operației;
- data și ora operației;
- identificatorul obiectului informațional afectat (utilizatorul, documentul, procesul etc.);
- versiunea obiectului informațional (se referă la versiunea generată prin efectuarea operației. Crearea obiectului generează versiunea 1. Modificarea incrementează versiunea cu o unitate. Eliminarea păstrează versiunea obiectului);
- adresa IP de la care a fost executată operația.

Jurnalul de audit va permite filtrarea înregistrărilor de audit în funcție de oricare dintre parametri enumerați mai sus.

3.11. Strategia de backup

Baza de date a sistemului va fi supusă unui backup periodic, automat. Vor fi realizate backup-uri de tip „full" săptămânal, respectiv backup-uri incrementabile cu recurență zilnică.

În același timp un alt nivel de backup este obținut prin replicare activă către nodul HOT STAND BY al bazei de date.

Integritatea fișierelor de backup

Sistemul SIIMA va utiliza un certificat x509 pentru semnarea digitală și criptarea fișierelor backup rezultate.

4. Concluzii

Mediul de operare al instituțiilor este caracterizat de o dinamică accelerată a proceselor și activităților specifice ce se desfășoară preponderent într-un context intensificat informațional. Pentru asigurarea unui mangement eficient și sigur al fluxurilor informaționale și al fluxurilor de lucru asociate acestora, este necesară utilizarea potențialului oferit de aplicațiile practice ale tehnologiei informațiilor și comunicațiilor. De aceea, se impune proiectarea și implementarea unui sistem informatic integrat pentru managementul activităților, bazat pe o soluție informatică open-source integrată care să satisfacă cerințele operaționale identificate. Principalele cerințe operaționale vizează în special implementarea unei componente de automatizare asociată unor procese organizaționale diversificate. Astfel, sistemul trebuie să asigure automatizarea managementului proceselor și activităților instituțiilor publice, automatizarea elaborării, gestionării și monitorizării poiectelor și programelor instituției, automatizarea managementului resurselor precum și gestionarea automatizată a circuitului informațional intern.

Mențiuni

Acest articol a fost posibil prin finanțarea asigurată de Ministerul Educației și Cercetării, UEFISCDI, programul PNIII, proiect cod PN-III-P2-2.1-SOL-2017-09-0102, contract nr. 8SOL/2018, nume: Sistem Informatic Integrat pentru Managementul Activităților (SIIMA).

BIBLIOGRAFIE

1. Activity BPMN, https://www.activiti.org/.
2. Apache ODE (Orchestration Director Engine), http://ode.apache.org.
3. Dan-Şuteu, Şt.-A. (2015). *Apărarea cibernetică în concepţia unor armate moderne*, Buletinul UNAp nr. 3/2015, Editura UNAp. "Carol I", Bucureşti, 2015.
4. GDPR, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf.
5. https://docs.wso2.com/display/ADMIN44x/ Securing+Passwords+in+Configuration+Files.
6. https://docs.wso2.com/display/ADMIN44x/ Enabling+Java+Security+Manager.
7. https://docs.wso2.com/display/ADMIN44x/ Using+Asymmetric+Encryption.
8. https://docs.wso2.com/display/ADMIN44x/Mitigating+Cross+Site+Request+Forgery+Attacks.
9. Udroiu, M., Dan-Şuteu, Şt.-A. (2019). *Sistem informatic integrat pentru managementul activităților în instituțiile militare. Fundamentare teoretică*, Editura UNAp. "Carol I",, București, 2019. https://docs.wso2.com/display/ADMIN44x/Mitigating+Cross+Site+Scripting+Attacks

Adriana-Meda UDROIU activează ca Manager securitatea informației în cadrul Institutului Național de Cercetare-Dezvoltare în Informatică. Are o activitate didactică și de cercetare de peste 20 de ani în domeniul TIC. A obținut titlul de doctor în Sisteme automate la Politehnica București în anul 2003. Este autor a peste 10 volume în domeniul tehnologiei informației și al comunicațiilor și a peste 50 de articole publicate în reviste naționale și internaționale indexate BDI și ISI, precum și director/responsabil al proiectelor de cercetare din ICI București. Este conferențiar universitar asociat la Facultatea de Automatică și Calculatoare din Politehnica București și la Academia Tehnică Militară „Ferdinand I". Principalele domenii de interes pentru activitatea de cercetare sunt: TIC, securitate cibernetică, protecția infrastructurilor critice, securitatea informației, elearning, formare continuă.

Adriana-Meda UDROIU works as Chief Information Security Officer at the National Institute for Research and Development in Informatics. She has a teaching and research activity for over 20 years in the field of ICT. She obtained his PhD degree in Automated Systems at Politehnica București in 2003. She is an author of more than 10 volumes in ICT field and more than 50 articles published in national and international journals BDI and ISI indexed. and she is also adirector/manager in research ICT projects of ICI Bucharest. She is associate professor at Faculty of Automatic Control and Computers, University Politehnica of Bucharest and at the Faculty of Military Electronic and Information Systems, Military Technical Academy „Ferdinand I". The main areas of interest to research are: ICT, cybersecurity, critical infrastructure protection, information security, elearning, lifelong learning.