UN STUDIU PRIVIND SITUAȚIA ÎN DOMENIUL RĂSPUNSULUI LA INCIDENTE

Mihnea Horia Vrejoiu
mihnea@dossv1.ici.ro

Mădălina Cornelia Zamfir
madalina@ici.ro

Ştefan Alexandru Preda
stefanalex@ici.ro

Vladimir Florian
vladimir@ici.ro

Institutul Național de Cercetare-Dezvoltare în Informatică - ICI Bucureşti

Rezumat: Problematica atacurilor informatice, a intruziunilor frauduloase în rețele, a compromiterii sistemelor, a blocării serviciilor sau a furtului de date este de mare actualitate, în contextul actual al expansiunii informatizării pe scară largă, atât la nivelul instituțiilor de stat cât şi al entităților private de diferite dimensiuni. Efectele negative ale acestora, precum şi costurile considerabile generate direct sau indirect şi cele pentru remedierea daunelor produse de acestea, au condus la necesitatea dezvoltării şi implementării de metode şi măsuri specifice de răspuns eficient şi rapid la astfel de incidente de securitate informatică. Articolul de față prezintă rezumativ rezultatele şi concluziile unui studiu statistic bazat pe un sondaj realizat în anul 2014 sub egida institutului SANS™ care oferă o imagine privind situația pe plan mondial cu privire la răspunsul la incidente şi unele direcții de viitor în acest domeniu.

Cuvinte cheie: răspuns la incidente (RI), echipă de RI, atac de tip DDoS, malware, acces neautorizat, compromitere/furt de date, gestionarea informațiilor şi evenimentelor de securitate.

Abstract: The problematics of informatics attacks, fraudulent network intrusion, system compromise, blocking of services, or data breach/theft, is of great actuality in the current context of expansion of the large scale informatization, both at the state institutions level and at the private entities of various dimensions level. Their negative effects, and also the high costs generated directly or indirectly, and those for the remedy of the damages produced, led to the necessity of developing and implementing specific methods and procedures for an efficient and quick response to such computer security incidents. This paper briefly presents the results and conclusions of a survey performed in 2014 by the SANS™ Institute, which provides an overview of the worldwide situation in the incident response (IR), and some future directions in this field.

Keywords: incident response (IR), IR team, DDoS attack, malware, unauthorized access, data breach/theft, security information and event management (SIEM).

1. Introducere

Incidența şi riscurile în continuă creştere ale acțiunilor de intruziune frauduloasă ostilă în sistemele informatice ale diferitelor instituții, organizații şi companii, de stat sau private, de diferite dimensiuni, precum şi costurile importante cauzate de efectele negative ale acestora şi cele aferente eliminării lor, au condus la necesitatea dezvoltării şi implementării unor metode şi măsuri specifice de răspuns eficient şi rapid la astfel de incidente de securitate informatică, a adaptării, actualizării, îmbunătățirii şi eficientizării continue a acestora.

Având în vedere actualitatea continuă şi utilitatea potențială a acestor informații, prezentăm în articolul de față (redactat inițial în toamna anului 2014), sintetic, rezultatele şi concluziile unui studiu statistic bazat pe un sondaj cu chestionare realizat în anul 2014 sub egida prestigiosului institut britanic SANS [1], privind situația bunelor practici pe plan mondial în legătură cu răspunsul la incidente (RI) de securitate în legătură cu sistemele informatice şi principalele direcții de acțiune pentru viitor avute în vedere de principalii actori din domeniu.

În cadrul sondajului s-au exprimat 259 de profesionişti, dintre care majoritatea (88%) cu roluri în RI – manageri, analişti de securitate, investigatori legişti în criminalitate informatică – din companii şi organizații de diferite mărimi (de la sub 100 de angajați la peste 20.000), din peste 19 domenii (incluzând tehnologie şi tehnologia informației – TI, servicii financiare, educație, sănătate şi industrie farmaceutică, guvernamental, militar, energie, utilități, asigurări etc.), acoperind o vastă arie geografică, reprezentând 13 regiuni şi țări diferite de pe tot globul.

2. Rezultatele studiului

Prezentăm în cele ce urmează o analiză statistică şi o sinteză privind metodele şi acţiunile de răspuns la incidente (RI) reieşite din sondaj ca fiind întreprinse până acum, precum şi avute în vedere pe viitor ca „bune practici", structurate pentru fiecare din cele şase etape ale unui proces de răspuns la incidente (RI) [2][3]:

- pregătirea;
- identificarea şi detecţia;
- izolarea;
- eliminarea / înlăturarea;
- remedierea şi restaurarea;
- lecţiile învăţate.

2.1 Etapa de pregătire

În etapa de pregătire a capacităţii şi capabilităţilor de RI ale unei organizaţii, o componentă primordială constă în definirea rolurilor şi responsabilităţilor. Este foarte important ca aceasta să se realizeze printr-un proces colaborativ, implicând obţinerea de informaţii şi suport din partea nivelurilor superioare ale managementului, precum şi a componentelor afacerii care sunt deţinătoare / proprietare de date. În cadrul sondajului, 43% dintre repondenţi au menţionat că nu s-a parcurs un astfel de proces colaborativ care să conducă la realizarea unui plan formal şi a unor proceduri de RI. Din nefericire, în absenţa acestora se ajunge adesea în situaţia de a trebui să fie imaginate soluţii şi proceduri şi să fie evitate potenţiale situaţii sensibile legate de anumite politici specifice tocmai în momentele de criză.

Repondenţii au mai indicat că izolarea RI de alte componente ale afacerii (36%) şi impedimentele de natură legală / DO (drepturile omului) în investigare / monitorizare (14%), reprezintă adesea obstacole serioase, ceea ce nu poate decât să confirme efectele negative ale lipsei unor proceduri formalizate pentru investigaţiile presupuse de RI. Trebuie subliniat faptul că prin eforturi colaborative realizarea a unui plan formal de RI al unei organizaţii pot fi evitate situaţiile în care obiectivele RI nu ar fi complet corelate cu acordurile privind nivelul serviciilor (*service level agreements* – SLA) şi cu continuitatea afacerii.

Tabelul 1 - Factorii principali care afectează eficienţa RI într-o organizaţie (conform [1])

Lipsa de timp pentru revizuirea/antrenarea procedurilor	*62%*
Lipsa unui buget pentru instrumente şi tehnologie	*59%*
Lipsa unei echipe formale de RI sau a unui serviciu de RI	*55%*
Slaba vizibilitate în configuraţiile/vulnerabilităţile sistemelor/punctelor de acces	*52%*
Lipsa planurilor şi procedurilor de RI	*43%*
Dificultăţi în corelarea evenimentelor de pe sisteme diferite	*38%*
Izolarea între RI şi alte grupuri	*36%*
Dificultatea în depistarea şi înlăturarea atacurilor sofisticate	*27%*
Accesarea înregistrărilor implicate cu instrumente de sincronizare	*19%*
Dificultăţi în găsirea instrumentelor pentru investigarea noilor tehnolgii	*16%*
Impedimente de natură legală/DO	*14%*
Lipsa unor furnizori de servicii de încredere disponibili	*12%*
Probleme de jurisdicţie cu serviciile cloud	*9%*
Alte probleme de jurisdicţie	*5%*
Altele	*3%*

Crearea şi compunerea efectivă a unei echipe de RI reprezintă o altă componentă cheie a etapei de pregătire. Majoritatea repondenţilor (55%) a desemnat lipsa unei echipe formale de RI, cu membri dedicaţi ca fiind un obstacol pentru un RI eficient. Este o realitate faptul că multe organizaţii nu îşi permit alocarea de fonduri pentru a se crea o echipă dedicată, al cărei unic

obiectiv să fie detectarea şi răspunsul la incidente. Totuşi, un management de răspuns eficient necesită o atribuire explicită a responsabilităţilor, implementarea unei metodologii şi a unor proceduri de RI eficiente. Trebuie menţionat faptul că, din cauza complexităţilor diferite ale infrastructurilor de reţea şi a numărului diferit de puncte de acces ale acestora, nu se poate defini o structură ideală standard de echipă RI care să fie valabilă pentru orice organizaţie.

Un al treilea aspect important în pregătirea capacităţii de RI vizează dezvoltarea proactivă de instrumente de securitate specifice pentru RI la punctele de acces, anterior apariţiei unei acţiuni de compromitere a acestora. Astfel de instrumente permit monitorizarea continuă în timp real a punctelor de acces ale companiei şi, dacă aceasta se realizează în etapa de pregătire – înainte de apariţia unui incident – senzorii de la punctele de acces pot furniza o pistă completă de audit pentru a ajuta la înţelegerea unui atac şi la investigarea adecvată a mediului pe baza datelor istorice şi a celor în timp real. O majoritate a repondenţilor (52%) a desemnat lipsa de vizibilitate a vulnerabilităţilor sistemului/punctului de acces ca fiind un obstacol pentru un RI eficient. Aceasta pune în lumină o problemă comună: multe organizaţii încă instalează instrumente de securitate ca reacţie la apariţia unei breşe în loc de a o face ca pregătire pentru cazul apariţiei uneia.

2.2 Etapa de identificare şi detecţie. Metode de detecţie

Trebuie acceptat faptul că în prezent atacarea şi compromiterea punctelor de acces ale reţelelor informatice este practic inevitabilă. Nu se mai pune problema dacă, ci când se va întâmpla acest lucru. De aceea, după pregătirea pentru un astfel de moment, următorul pas important este detectarea efectivă a unei astfel de compromiteri a unui punct de acces. Pentru aceasta, asigurarea unei monitorizări continue automatizate reprezintă o componentă importantă.

În acest sens, din sondaj s-au desprins trei tehnici ca fiind cele mai utilizate de către participanţi: scanarea cu agenţi după indicatori (96%), analiza capturii reţelei (93%) şi răspunsul la alerte de *firewall*, IPS/IDS sau UTM (91%); (*IPS/IDS = intrusion prevention/detection system, UTM = unified threat management)*.

Din punct de vedere al gradului de automatizare, trebuie menţionat faptul că au fost raportate niveluri înalte de automatizare pentru scanările bazate pe agenţi şi alerte de tip *firewall*/IPS/IDS/UTM, dar al doilea cel mai înalt nivel de automatizare raportat (46%) a fost la detecţie, utilizându-se agenţi de detectare a intruziunii la nivel de sistem gazdă (*host-based intrusion detection* – HIDS). Totuşi, faptul că 16% dintre participanţi au declarat că nu utilizează HIDS deloc a condus la scăderea popularităţii HIDS abia pe locul şase. Astfel, primele cinci cele mai utilizate instrumente de detecţie sunt reprezentate în Tabelul 2.

Tabelul 2 - Cele mai populare instrumente de detecţie (conform [1])

Tehnologie	**Procent utilizare**
Scanare indicatori la nivel de reţea cu agenţi	*96%*
Analiza capturii reţelei	*93%*
Răspuns la alerte firewall/IPS/IDS sau UTM	*91%*
Notificări sau reclamaţii de la utilizatori	*85%*
Analiza manuală a jurnalelor	*85%*

Pe de altă parte, tehnologiile cel mai puţin utilizate au reieşit a fi: decriptarea SSL la frontiera reţelei (39% nu utilizează), controlul punctelor de acces, cum ar fi controlul accesului la reţea (*network access control* – NAC) sau managementul dispozitivelor mobile (*mobile device management* – MDM) (33% nu utilizează) şi instrumentele proprii dezvoltate, specifice mediului respectiv (31% nu utilizează).

Ca o observaţie, utilizarea redusă a primelor trei dintre cele de mai sus, în ciuda utilităţii de netăgăduit a tehnologiilor respective pentru asigurarea unui control preventiv la punctele de intrare ale reţelelor şi a diminuării riscurilor de infectare cu *malware* a acestora (mai ales prin conectarea dispozitivelor mobile care sunt cele mai expuse prin conectarile multiple neprotejate la diferite *hotspot*-uri), se poate datora fie unor posibile complicaţii sau dificultăţi de implementare efectivă constatate de participanţi, fie faptului că respectivele tehnologii, odată implementate, ar putea

introduce oarecare limitări, restricționări, complicări şi/sau îngreunări ale accesului, ceea ce ar penaliza inacceptabil momentan fluxurile normale de lucru ale utilizatorilor.

În ceea ce priveşte utilizarea restrânsă a instrumentelor proprii, dezvoltate individual, aceasta ar putea fi explicată prin faptul că utilizarea instrumentelor disponibile comercial satisfac într-o măsură suficientă necesitățile participanților pentru gestionarea informațiilor şi evenimentelor de securitate (*security information and event management* – SIEM). Pe de altă parte, este posibil totuşi şi ca participanții să nu dețină expertiza necesară proiectării, dezvoltării şi mentenanței unor astfel de instrumente proprii.

Mai trebuie menționat faptul că analiza manuală a jurnalelor prezintă încă o rată mai înaltă de adoptare decât utilizarea SIEM şi există un procent neneglijabil dintre utilizatori care se mai bazează încă pe analiza manuală a jurnalelor pentru identificarea incidentelor.

2.3 Etapa de izolare

Durata scursă de la detectarea inițială a unui incident până la izolarea sistemelor afectate astfel încât să se stopeze posibile alte infecții şi să se prevină furtul altor date este foarte importantă. Unul din scopurile cele mai importante ale RI este acela de a menține pierderile şi impactul asupra organizației cât mai reduse, la un nivel acceptabil.

Intervalul mediu de timp cel mai comun de la descoperirea unui incident până la izolarea fizică sau virtuală a sistemelor afectate, declarat de 19% din repondenți, a fost de 4–8 ore. Alți 16% au indicat chiar un interval de 1–4 ore, în timp ce 14% au menționat ca fiind necesare între 2 şi 7 zile pentru izolare.

2.4 Etapa de eliminare / înlăturare

În primul rând, la primirea unei alerte pe baza indicatorilor la nivelul rețelei sau gazdei, o echipă de RI trebuie să realizeze o triere în sistem/sisteme pentru a confirma corect un incident de securitate. În general, pentru confirmarea stării sistemului alertat, se realizează conectări la distanță.

Prin utilizarea unor instrumente (agenți) de investigare criminalistică de tip RI la distanță pe sistemele de acces este redus timpul necesar colectării datelor pentru triere, izolarea sistemului putând fi astfel accelerată cu minute sau chiar ore prețioase. În cazul în care astfel de agenți nu sunt disponibili, fie pot fi rulate la distanță alte *script*-uri de supraveghere a sistemului respectiv, fie un tehnician de TI sau de securitate de la fața locului poate fi însărcinat să efectueze trierea local. Unele instrumente de RI la nivel de organizație au adăugat deja facilități prin care sunt automatizate confirmarea alertei, izolarea şi rezolvarea incidentului. Sunt astfel eliberate resurse umane importante iar timpul de la detecție până la izolare este redus.

Trebuie făcută observația că în cazul intruziunilor în rețea, implicând atacatori sofisticați, în momentul trierii inițiale a sistemelor potențial compromise, ia practic naştere o cursă între echipa de RI şi atacator. Efectele rulării unor instrumente de colectare/triere pe sistemele care prezintă abateri de la activitatea normală pot pune în gardă atacatorul asupra faptului că a început detecția. În consecință, este de aşteptat ca acesta din urmă, odată ce suspectează demararea acțiunii de detecție, să încerce minimizarea/eliminarea urmelor proprii în rețea, prin ştergerea fişierelor aferente atacului de pe sistemele compromise şi/sau să acționeze în sensul modificării modului de comportament propriu pentru evitarea sau îngreunarea detectării pe mai departe. În mod normal, este cu atât mai bine cu cât se lasă mai puțin timp unui atacator pentru a reacționa după detecție.

Un procent mare din repondenți au menționat intervale de timp mai mari până la izolare. Astfel, 15% au raportat perioade de peste 7 zile şi 11% au raportat chiar o lună sau mai mult. Este posibil ca unele dintre aceste organizații să fi ales în mod intenționat să nu izoleze imediat sistemele afectate ci, mai degrabă, să monitorizeze activitatea atacatorului în scopul identificării logicii/scopului amenințării şi a tuturor mecanismelor utilizate pentru aceasta. Astfel, echipa de RI poate înțelege mai bine amenințarea şi poate colecta indicatori relevanți despre compromitere (*indicators of compromise* – IOC), pe baza cărora poate detecta atacuri ulterioare, care altfel ar fi putut trece neobservate.

2.5 Etapa de remediere şi restaurare

Remedierea cu succes implică eliminarea atacatorului şi componentelor atacului din rețea şi revenirea la funcționarea normală, respectiv recuplarea sistemelor (*online*) şi restaurarea disponibilității serviciilor ce fuseseră afectate pentru clienții interni şi externi.

În cazul a numeroase incidente critice există implicații financiare pentru fiecare minut în care rețeaua sau serviciile de sistem ale organizației sunt afectate, fie că e vorba de un server web, fie de o stație de lucru a unui angajat. Din acest motiv, timpul necesar unei organizații pentru a parcurge etapele de la detectarea unui incident critic până la remedierea completă este foarte important.

În urma sondajului, s-a constatat că răspunsul cel mai întâlnit (22%) a indicat un interval de 2–7 zile de la detectare până la remediere. Însumat, 29% din repondenți au indicat mai mult de o săptămână pentru remedierea incidentului, iar 4% chiar peste 12 luni, sau nu au remediat niciodată problema. Totodată, acționarea în următorii doi ani în sensul îmbunătățirii/perfecționării proceselor de remediere a fost nominalizată de 54% dintre repondenți, ceea ce poate fi interpretat în sensul că intervalele temporale efective de la detecție la remediere nu sunt tocmai acceptabile de cele mai multe ori.

O componentă a pregătirii de RI este reprezentată de colaborarea cu managementul de nivel superior pentru definirea unei ferestre acceptabile până la întrerupere (*acceptable interruption window* – AIW). Aceasta reprezintă durata pe care un incident poate continua înainte ca întreruperea pe care o poate cauza să devină inacceptabilă din punctul de vedere al consecințelor sale. În cadrul organizațiilor de diferite dimensiuni trebuie să se dimensioneze şi să se stabilească astfel de AIW funcție de modelele de afacere proprii.

Lipsa unor procese de RI bine dezvoltate, subdimensionarea personalului de investigație/RI intern sau deja disponibil şi accesul limitat la instrucțiuni/proceduri de remediere specifice amenințării pot constitui impedimente în remediere. În astfel de situații legate de aceste resurse inexistente, sau doar parțial disponibile, organizațiile au dificultăți în determinarea corectă a încadrării unei intruziuni şi, în general, nu reuşesc:

- să realizeze analiza sistemului inițial pentru a identifica semnătura/amprenta *malware*-ului şi comportamentul atacatorului şi a genera indicatori de compromitere;
- să efectueze scanarea şi identificarea corespunzătoare a alte puncte de acces compromise ale rețelei, implicate în intruziune;
- să lărgească eficient aria de analiză pentru a include puncte de acces fără *malware* activ, pe baza urmelor şi artefactelor din sistem şi utilizarea conturilor compromise anterior;
- să reducă pagubele potențiale prin dezactivarea aplicațiilor sau serviciilor specifice care constituie mijloace pentru compromiterea/furtul datelor.

2.6 Lecțiile învățate

Lecțiile învățate din experiențele avute de participanți pot reieşi din analiza răspunsurilor acestora în ceea ce priveşte îmbunătățirile în RI avute în vedere pentru perioada următoare.

Astfel, o primă lecție învățată ar fi nevoia de o mai mare automatizare şi integrare cu tehnologia SIEM. Un total de 68% dintre repondenți a indicat această integrare ca fiind zona unde estimează că sunt necesare îmbunătățiri în decursul următoarelor 24 de luni.

O a doua îmbunătățire, menționată de 59% dintre participanți a fost creşterea vizibilității în ceea ce priveşte amenințările şi vulnerabilitățile.

Aceste două tipuri de îmbunătățiri vizează o detecție mai rapidă şi mai eficientă a anomaliilor, care să ducă la o diminuare a duratei în care un atacator rămâne nedetectat în mediu.

Îmbunătățirea timpilor de răspuns este un deziderat pentru 42% dintre repondenți pentru următoarele 24 de luni. În particular, pe măsură ce echipele de RI capătă mai multă experiență şi eficiența detecției se îmbunătățeşte, focalizarea tinde să se mute pe creşterea eficienței proceselor de colectare şi corelare a datelor pentru RI.

Tabelul 3 - Îmbunătățiri în RI planificate de organizații în următoarele 24 de luni (conform [1])

O mai mare automatizare şi integrare cu SIEM pentru raportări şi analize	*68%*
Mai bună vizibilitate a amenințărilor şi vulnerabilităților asociate specifice	*59%*
Îmbunătățirea proceselor de remediere şi urmărire	*54%*
Îmbunătățirea abilităților de identificare a sistemelor afectate şi a surselor	*42%*
Îmbunătățirea timpilor de răspuns	*42%*
Altele	*20%*

3. Concluzii

Câteva dintre concluziile principale ale studiului [1] sunt sintetizate după cum urmează:

- o parte importantă (26%) dintre profesioniştii de RI chestionați nu sunt satisfăcuți de capacitatea actuală de RI a organizațiilor lor, considerând-o ineficientă, în timp ce numai 9% o consideră ca fiind eficientă. Principalele impedimente semnalate se referă la lipsa timpului pentru revizuirea şi antrenarea procedurilor (62%) şi respectiv, la lipsa bugetelor pentru instrumente şi tehnologii specifice (60%);
- definirea incidentelor la nivel de organizație este adesea destul de vagă, ceea ce determină o supraîncărcare a echipelor de RI – şi aşa insuficiente – cu sarcini care în mod normal nu ar trebui să le revină acestora. Aria tipurilor de incidente considerate este astfel foarte largă, nefiind limitată doar la intruziuni în rețea şi *software* periculos/malițios (*malicious software*), iar echipele de RI ajung să fie însărcinate (şi) cu gestionarea acceselor neautorizate din surse interne sau externe, atacuri de tip DDoS (*distributed denial of service*), utilizare internă necorespunzătoare sau pierderi de date;
- obstacolele cele mai importante în gestionarea eficientă a incidentelor au fost identificate ca fiind lipsa unei structuri definite de echipă dedicată RI (55%), precum şi a unor planuri şi proceduri formale de RI (43%);
- organizațiile nu au implementate încă măsuri pentru colectarea şi corelarea informațiilor specifice asociate amenințărilor, pentru identificarea şi blocarea/eliminarea viitoare a unor atacuri similare;
- obiectivul principal avut în vedere pentru îmbunătățirea pe viitor a proceselor de RI (68%), îl constituie automatizarea şi integrarea instrumentelor de tip SIEM (*security information and event management*).

4. Recomandări

Pe baza rezultatelor studiului, organizațiile pot ajunge la eficientizarea proceselor de RI, prin implementarea următoarelor recomandări [1]:

a) O mai bună definire a termenului „incident"

În recomandările Institutului Național de Standarde şi Tehnologie de pe lângă Departamentul Comerțului din S.U.A. [4], un incident de securitate informatică este definit ca fiind „o încălcare sau o tentativă de încălcare a politicilor de securitate ale unui sistem informatic, a politicilor de utilizare acceptabilă, sau a practicilor standard de securitate". Totuşi, în practică, organizațiile dau diferite interpretări în legătură cu ce tipuri de evenimente intră sub această definiție. În lipsa unei definiri clare şi unanim acceptate pentru ceea ce intră şi ceea ce nu intră în categoria de „incident", se poate întâmpla ca o echipă de RI să fie copleşită cu trierea, investigarea şi tratarea unor evenimente care, în mod normal, nu ar fi trebuit să o implice direct. Pe de altă parte, având o definire acceptată, este mai uşor să fie adăugate metrici (măsuri) adecvate, sau indicatori cheie de performanță (*key performance indicators* – KPI), pentru detecție şi remediere, pe baza cărora să se poată justifica asigurarea unui buget corespunzător / suplimentar.

O politică bună de RI la nivelul unei organizații, concepută în etapa de pregătire a procesului de RI trebuie neapărat să includă o definire explicită a acelor tipuri de incidente care intră în responsabilitatea echipei de RI. În absența unor astfel de precizări, acesteia i se pot atribui în mod

nefericit unele sarcini minore şi irelevante din punct de vedere al RI, de genul investigării oricărei încălcări a politicilor de utilizare acceptabilă, sau urmăririi/localizării echipamentelor şi/sau dispozitivelor pierdute sau furate.

Toţi actorii implicaţi sau interesaţi trebuie să agreeze asupra conţinutului definit pentru termenul „incident" înainte de stabilirea atribuţiilor echipei de RI, deoarece numai astfel pot fi definite cu claritate rolurile şi responsabilităţile echipei de RI. Mai trebuie menţionat că politicile şi procedurile de RI trebuie să furnizeze şi alte detalii, cum ar fi de exemplu condiţiile în care un membru al echipei de RI poate decupla din reţea sau închide/opri un sistem.

b) Asigurarea securităţii proceselor celorlalte componente ale afacerii

Toţi proprietarii/deţinătorii de date şi persoanele care gestionează/întreţin echipamentele şi/sau dispozitivele de tehnologia informaţiei (TI) ale organizaţiei trebuie pregătiţi/educaţi pentru a implementa cele mai bune practici de securitate.

Dezvoltatorii de *software* intern trebuie să includă (şi) consideraţii de securitate în ciclul de dezvoltare. Astfel, echipa de RI va avea mai puţine probleme cu vulnerabilităţi ale aplicaţiilor dezvoltate „în casă".

Tehnicienii care asigură suport pentru utilizatori trebuie să deţină o bună înţelegere a trierii sistemului şi să fie antrenaţi astfel încât să poată discerne corect o problemă între utilizator şi o infecţie de tip *malware*.

Proprietarii/deţinătorii de date trebuie să înţeleagă avantajele asociate bunelor practici cum sunt cerinţa accesului cu privilegii minime la date şi auditarea evenimentelor specifice sistemului şi aplicaţiei.

c) Urmărirea costurilor RI pentru justificarea necesarului de instrumente şi personal de RI

În absenţa unor măsurători precise ale costurilor implicate în gestionarea unui incident, este aproape sigur că bugetul destinat activităţilor de RI va avea de suferit. O tehnică recomandată pentru justificarea necesităţii de resurse suplimentare de personal şi/sau de *hardware* şi *software*, este aceea de urmărire a costurilor proceselor şi procedurilor curente ineficiente.

Costurile directe pentru angajarea unor servicii de investigare de RI de la terţi şi deplasarea pentru un RI la distanţă, ca şi costurile indirecte determinate de scăderea productivităţii în cazul alocării şi şcolarizării de personal pentru RI pe durata unui incident apărut, precum şi al procesării manuale a datelor şi jurnalelor sunt măsuri/metrici ce pot fi utile în justificarea necesităţii de resurse suplimentare.

Tabelul 4 - Procentul din bugetul pentru securitate alocat RI (conform [1])

Necunoscut	*38,6%*
Nu există (0%)	*29,5*
4-5%	*11,4%*
5-10%	*6,8%*
1-2%	*6,8%*
peste 10%	*4,5%*
2-3%	*2,3%*

Costurile de dezvoltare şi întreţinere de instrumente de RI proprii ale organizaţiei pot reprezenta un capitol substanţial în bugetul anual al unei echipe de securitate. Pe de altă parte, existenţa acestor instrumente adecvate poate simplifica substanţial procesul de achiziţie de date anost şi consumator de timp şi permite echipei să realizeze mai mult cu mai puţin şi să reducă duratele în toate etapele RI.

A reieşit că aproape 30% din repondenţi nu alocă pentru RI nicio parte din bugetul lor pentru securitate, în timp ce alţi 39% nu au cunoştinţă dacă au alocat un buget pentru RI (sau cât de mare a fost acesta).

Printre consecinţele lipsei unui buget pentru RI sau a vizibilităţii asupra a ceea ce un astfel de buget acoperă se numără riscul de terminare şi pierdere a licenţelor curente sau imposibilitatea

obținerii unor licențe pentru *software* esențial, incluzând instrumente de monitorizare la nivel de rețea sau gazdă, suite de investigare criminalistică şi instrumente de colectare şi analiză a datelor.

d) Urmărirea măsurilor/metricilor de RI pentru justificarea necesarului de instrumente de RI şi dimensionarea adecvată a echipei de RI

În ciuda climatului actual de securitate, 14% dintre repondenții la sondaj lucrează în organizații în care nu există echipe dedicate pentru RI. Această lipsă a unei echipe formale a fost citată ca principal obstacol în tratarea eficientă a incidentelor.

Mulți manageri de securitate găsesc dificilă justificarea alocării de personal dedicat permanent RI, deoarece frecvența sau volumul incidentelor de securitate la nivelul organizației tind să fie mai degrabă ciclice şi nicidecum continue. Pe de altă parte, s-a dovedit că majoritatea echipelor de RI au un mai mare succes şi o mai mare eficiență în detecția şi izolarea incidentelor în cazul utilizării unei monitorizări continue proactive şi aplicării răspunsului corespunzător, decât în cazul unor procese de reacție punctuală, intermitentă.

Recomandarea este ca organizațiile să dețină o echipă de RI dedicată, dimensionată adecvat, precum şi capabilități de monitorizare continuă şi de răspuns corespunzător la orice moment. Metricile utilizate pentru justificarea necesarului de personal şi/sau instrumente de RI să aibă în vedere trei intervale de timp: de la infectarea inițială până la detecție, de la detecție până la izolare şi, respectiv, de la detecție până la remediere.

BIBLIOGRAFIE

1. **TORRES, A.:** Incident Response: How To Fight Back, A SANS Survey Sponsored by Bit9 + Carbon Black, Advisor: Jacob Williams, SANS™ Institute – UK (www.sans.org), August 13, 2014 (http://www.sans.org/reading-room/whitepapers/analyst/incident-response-fight-35342).
2. **ZAMFIR, M. C.; FLORIAN, V.; PREDA, Ş. A.:** Cercetări referitoare la extrapolarea principiilor sistemelor cu imunitate naturală la activitățile echipelor de tip CERT (Computer Emergency Response Team) pentru optimizarea şi particularizarea raportului securitate-accesibilitate. Analiza rezultatelor cercetărilor de referință în domeniul imunității naturale (biologice) şi a sistemelor de imunitate artificială existente. Definirea principiilor şi mecanismelor ce pot fi aplicate în România privind optimizarea bazelor de date şi infrastructurilor suport pentru achiziția informațiilor relative la incidente. Elaborarea de proceduri de lucru pentru echipe CERT privind răspunsul la incidente şi formularea de propuneri de reglementări. Proceduri de lucru pentru echipe CERT privind răspunsul la incidente şi propuneri de reglementări. – Raport de cercetare, etapa I a proiectului PN0923-0302, ICI Bucureşti, iunie 2014.
3. **ZAMFIR, M. C.; FLORIAN, V.; PREDA; VREJOIU, M. H.:** Cercetări referitoare la extrapolarea principiilor sistemelor cu imunitate naturală la activitățile echipelor de tip CERT (Computer Emergency Response Team) pentru optimizarea şi particularizarea raportului securitate-accesibilitate. Experimentarea rezultatelor cercetărilor şi supunerea lor dezbaterii comunității TIC. – Raport de cercetare, etapa a II-a a proiectului PN0923-0302, ICI Bucureşti, decembrie 2014.
4. **CICHONSKI, P.; MILLAR, T.; GRANCE, T.; SCARFONE, K.:** Computer Security Incident Handling Guide - Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-61 Revision 2, August 2012, CODEN: NSPUE2 (http://dx.doi.org/10.6028/NIST.SP.800-61r2
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)