LUNA EUROPEANĂ A SECURITĂȚII INFORMATICE

CENTRUL NAȚIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ
CERT-RO

GHID

Referitor la rolul structurilor de tip CERT şi utilitatea CERT-urilor private

Ghid realizat de către:

isec fair and true

o companie

provision® protect your business

în cadrul campaniei de conștientizare a riscurilor de securitate cibernetică derulată în Romania sub egida ECSM de către CERT-RO.

www.cert-ro.eu/tag/ecsm

BE AWARE, BE SECURE.
www.enisa.europa.eu/cybersecmonth

Cuprins

1. Scopul documentului

Scopul prezentului document este de a familiariza cititorii cu noţiunea de CERT (Computer Emergency Response Team /Echipa de Răspuns la Urgenţe Cibernetice) şi a rolului pe care structurile de acest tip, atât din domeniul public cât şi din cel privat, îl joacă în prevenirea, detectarea şi intervenţia la incidentele de securitate cibernetică.

2. Ce este un CERT?

Acronimul CERT provine de la termenul în limba engleză Computer Emergency Response Team, ce poate fi tradus în limba română drept Echipa de Răspuns la Urgenţe Cibernetice. O traducere mai apropiată a acestui termen este Echipa de Răspuns la Incidente de Securitate Cibernetică, care se mapează pe o abreviere ceva mai utilizată în spaţiul European, CSIRT (Computer Security Incident Response Team).

Oricare ar fi denumirea acestora, echipele de răspuns la incidente îşi au originea în trecut, cu mult înaintea apariţiei sistemelor informatice.

Comunităţile locale din antichitate îşi protejau bunurile şi animalele domestice împotriva atacurilor prădătorilor de orice tip, precum hoardele de nomazi sau fiarele sălbatice, utilizând un sistem de avertizare timpurie format din câini sau iscoade, care notificau grupurile de oameni însărcinaţi cu paza acestora şi cu prima intervenţie.

Organizarea forţelor militare din ultimele secole presupune, de asemenea, o echipă de răspuns la incidente, precum celula de gardă ce păzeşte perimetrul unităţii militare şi punctele vitale din interiorul acesteia. Aceasta intervine prima în cazul unui incident precum atacul unor intruşi, santinela jucând atât rol de element de avertizare a echipei lărgite cât şi de intervenţie directă asupra atacatorului.

În zilele noastre suntem deja familiarizaţi cu intervenţia unor echipe specializate la incidente precum incendii de foc, inundaţii, accidente cu victime omeneşti, ameninţări şi incidente teroriste, sau evenimente violente izolate ori generate de mulţimi mari de oameni. Toate aceste echipe au rolul de a reduce impactul unor incidente în curs de derulare, dar şi de a preveni ca aceste tipuri de incidente să producă daune în viitor, fie prin diminuarea probabilităţii acestora, precum instruirea populaţiei cu privire la modul de prevenire a incendiilor, fie prin reducerea impactului, aşa cum este cazul unui cutremur de proporţii, prin diseminarea informaţiilor privind reacţia pe durata unui astfel de eveniment natural care nu poate fi prevăzut sau evitat.

Odată cu dezvoltarea infrastructurilor de tehnologia informaţiei şi comunicaţii, au apărut ameninţări importante la adresa utilizatorilor acestora, precum coduri maliţioase de tipul viruşilor şi viermilor informatici, care s-au materializat din ce în ce mai mult, afectând un număr important de persoane şi activităţi.

Ca şi în celelalte domenii, nevoia de a reacţiona rapid cu specialişti care înţeleg complexitatea unor astfel de ameninţări a dus la apariţia echipelor de răspuns la incidente de securitate informatică, cunoscute ca echipe CERT sau CSIRT. Acestea sunt formate din specialişti în securitate cibernetică, şi au atât rolul de a interveni urgent în situaţii complexe cât şi rol de prevenire a apariţiei unor incidente similare pe viitor.

Activităţile unui CERT sunt din ce în ce mai diversificate, în funcţie de resursele sale interne, de nivelul de susţinere din partea comunităţii deservite de către acestea dar şi de gradul de cooperare cu organizaţiile şi specialiştii din aria în care îşi desfăşoară activitatea sau din zonele adiacente.

3. Activităţile unui CERT

Echipele de tip CERT au apărut în principal ca urmare a nevoii de răspuns la incidente de securitate cibernetică, ceea ce a oferit o pondere majoră serviciilor reactive oferite de acestea. Exista, însă, şi o latură proactivă a serviciilor, dezvoltată din ce în ce mai mult ca urmare a identificării cauzelor primare ale incidentelor de securitate şi a modalităţilor de prevenire a acestora, care tinde să se dezvolte din ce în ce mai mult în ultimii ani.

Manualul echipelor CSIRT[1] defineşte serviciile unui CSIRT pe trei categorii:

- Servicii reactive
- Servicii proactive
- Servicii de management al calităţii securităţii

Să le definim pe rând în termeni care nu presupun cunoştinţe avansate în domeniul IT sau al securităţii cibernetice.

3.1. Servicii reactive oferite de o echipă CERT

3.1.1. Alerte şi avertizări

Deşi alertele şi avertizările ar putea fi interpretate drept acţiuni proactive, acestea se referă la acele notificări imediate care fac referire la incidente de securitate aflate în desfăşurare, precum noi viruşi sau viermi care afectează un număr din ce în ce mai mare de calculatoare, atacuri informatice complexe de natură recentă care afectează un anumit tip de organizaţii, precum bănci, companii energetice, agenţii guvernamentale, ori noi acţiuni ingenioase de inginerie socială menite să obţină date privind cărţile de credit sau date cu caracter personal, care au succes exponenţial.

Dacă facem o paralelă în istoria umanităţii, aceste alerte şi avertizări au existat încă din antichitate. Să ne gândim la pandemiile de tuberculoză, holeră sau ciumă, atunci când lumea era avertizată cu privire la numărul sporit de cazuri de îmbolnăvire şi deces, primind indicaţii pentru a se proteja. Existau situaţii în care, în lipsa unui antidot, oamenii erau îndemnaţi să izoleze persoanele infectate şi să nu circule prin zone aglomerate. Inclusiv în cadrul epidemiei recente de SARS au existat astfel de alerte şi avertizări.

În domeniul IT exista un proces bine definit de alertare şi avertizare pe care echipele CERT îl au în portofoliu, şi care presupune notificarea imediată prin canale multiple de tip email, telefonic sau portaluri web, atât a populaţiei care utilizează calculatoare şi echipamente similare, cât şi a organizaţiilor deservite de echipa CERT sau a altor echipe CERT din lume.

De exemplu, la apariţia unui nou tip de ameninţare informatică, echipa CERT RO poate fi anunţată de un CSIRT al unei companii private care a detectat-o. CERT RO cooperează cu diverse organizaţii specializate în analiză de malware şi cu echipe CERT partenere din ţară şi de peste hotare, identifică

[1] *Handbook for Computer Security Incident Response Teams (CSIRTs)*, 2nd Edition, April 2003

cauza primară şi modul de acţiune ale respectivei ameninţări, şi apoi alertează organizaţiile deservite din mediul guvernamental, dar şi alte echipe CERT guvernamentale şi din mediul privat, cu privire la noua ameninţare şi la modalităţile de protejare împotriva acesteia, precum şi la modul în care poate fi redus impactul în cazul în care ameninţarea s-a materializat sub diferite forme.

3.1.2. Tratarea propriu zisă a incidentelor de securitate

Activitatea de bază a echipelor CERT este intervenţia propriu-zisă la apariţia unui incident de securitate cibernetică. Acest lucru presupune o intervenţie la locul incidentului sau acordarea de suport la distanţă prin intermediul telefonului, emailului sau a unor aplicaţii software dedicate.

În cazul intervenţiei la locul incidentului, echipa CERT analizează sistemele informatice afectate, ia măsuri de limitare a pagubelor, de exemplu prin izolarea unei zone de reţea afectata de malware, face o analiză detaliată a evenimentului pentru identificarea cauzei primare a acestuia şi culege probe pentru a putea susţine o eventuală plângere penală şi un proces împotriva persoanei sau instituţiei care a generat incidentul.

Atunci când intervenţia la locul incidentului nu este posibila, fie datorită locației geografice distante, fie din lipsa de resurse ale echipei CERT ori din alte motive, aceasta poate acorda sprijin distant echipelor locale de intervenţie, care pot fi formate din personal IT sau chiar specializat în securitatea sistemelor informatice.

Nu în ultimul rând, o echipă CERT poate coordona răspunsul la un incident de securitate major, care afectează mai multe organizaţii ori a cărui complexitate cere participarea mai multor echipe specializate în domenii diferite. Autoritatea echipei CERT joacă un rol determinant în astfel de situaţii, fie că vorbim de o autoritate impusă de legi, fie că vorbim de o autoritate obţinută în timp prin competenţă şi rezultate.

Făcând o paralelă cu procesul de intervenţie la accidente rutiere soldate cu victime, echipele de intervenţie de la faţa locului pot cuprinde atât poliţişti, care izolează locul accidentului şi fluidizează traficul, colectând în paralel probe care pot duce la identificarea cauzei evenimentului rutier, cât şi echipe de descarcerare, de stingere a incendiilor şi, desigur, echipe medicale. Echipa medicală analizează la fata locului gravitatea problemelor medicale ale victimelor şi ia măsuri rapide de reducere a riscurilor de deces şi de natură medicală.

Există atât o cooperare permanentă între cele trei echipe de specialişti, cât şi o coordonare a acţiunilor din partea echipei specializate, care poate aparţine Inspectoratului pentru Situaţii de Urgenţă. În cazul în care echipa medicală nu poate ajunge rapid la locul accidentului, aceasta poate oferi suport prin telefon către persoane aflate la faţa locului, capabile astfel să acorde primul ajutor victimelor.

Echipele CERT trebuie să aibă obligatoriu în portofoliu acest tip de serviciu, chiar şi atunci când funcţionează cu efective şi resurse financiare limitate, deoarece răspunsul la incidente este activitatea principală aşteptată de către clienţii deserviţi de acestea. Inclusiv denumirile CERT şi CSIRT au o referire intrinsecă la serviciul de intervenţie în caz de incidente sau urgenţe de natură cibernetică.

3.1.3. Managementul vulnerabilităţilor

Sistemele informatice şi de comunicaţii sunt realizate de fiinţe umane, şi drept urmare, nu sunt perfecte, putând avea diferite vulnerabilităţi atât în echipamentele hardware cât şi în sistemele de operare ori aplicaţiile software instalate pe acestea.

Procesul de descoperire a vulnerabilităţilor şi de identificare a modalităţilor de reducere a acestora, acele patch-uri de securitate cunoscute de utilizatorii obişnuiţi de calculatoare personale, poate intra în atribuţiile unei echipe de tip CERT. Pentru aceasta este nevoie de resurse tehnice bine specializate în analiză de coduri de programare, de coduri maşină, cu cunoştinţe temeinice în protocoale de comunicaţie, protocoale de sisteme industriale, şi în multe alte domenii adiacente.

Există, din fericire, comunităţi diverse care identifică astfel de vulnerabilităţi, precum cele din mediile academice sau cele ale furnizorilor de soluţii IT sau chiar ale specialiștilor în domeniul securităţii informatice, pasionaţi de astfel de activităţi. Echipele CERT pot primi sprijin şi informaţii de la aceste comunităţi, şi pot la rândul lor, să contribuie la descoperirea unora noi, în funcţie de cunoştinţele tehnice pe care le au.

O activitate importantă este însă coordonarea acestui proces de management al vulnerabilităţilor, constând din obţinerea informaţiilor despre noi vulnerabilităţi şi diseminarea acestora numai după crearea unor patch-uri de reducere a acestora de către furnizorii soluţiilor IT sau de comunicaţii afectate.

Ne putem imagina o situaţie în care o echipă de specialişti în domeniul securităţii informatice descoperă o vulnerabilitate în dispozitivele medicale de ventilație artificială utilizate în sălile de intervenţie chirurgicală sau în cele de terapie intensivă.
Echipa CERT de la nivel naţional este informată despre această nouă vulnerabilitate şi iniţiază un dialog cu producătorii sistemelor tehnice respective pentru dezvoltarea unui patch de securitate, în paralel luând măsuri de reducere a şansei de exploatare a acestei vulnerabilităţi în cooperare cu managerii spitalelor de urgenţă, de exemplu prin monitorizarea permanentă a acestor echipamente, ori chiar prin izolarea lor de către reţeaua IT interna, în cazul în care acestea ar fi conectate la ea. Aceasta situație, deşi pare extrasă din filmele de anticipaţie, este una reală şi obişnuită pentru echipele CERT moderne.

3.1.4. Culegerea probelor

Pe durata unui incident este important să avem în vedere, pe lângă reducerea impactului acestuia, identificarea probelor care ar putea ajuta la descoperirea cauzei primare a evenimentului de securitate şi la susţinerea în faţa instanţei a vinovăţiei persoanei care a produs incidentul.

În cazul incidentelor de securitate cibernetică, această activitate presupune identificarea fişierelor de pe un calculator atacat, care au fost instalate de un criminal cibernetic în mod direct sau prin intermediul unui cod maliţios precum troieni, viruşi sau viermi informatici, sau chiar descoperirea unor probe digitale pe calculatorul de pe care a fost lansat atacul, care atestă faptul că acesta a stat la originea acţiunii criminale.

Acest proces poate fi derulat doar de specialişti în investigaţii digitale din echipe specializate, care utilizează soluţii hardware şi software dedicate pentru clonarea în siguranţă a suporţilor de informaţie, precum hard-discurile, menite să păstreze nealterate probele originale precum conţinutul fişierelor şi datele la care acestea au fost create, modificate şi accesate. Uneltele specializate în

investigaţii digitale presupun şi păstrarea fişierelor probă în formate acceptate de jurişti, amprentate cu o ştampilă de timp în formatul original, similar probelor criminalistice din lumea reală care sunt păstrate în pungi sigilate şi înseriate.

Echipele CERT pot juca acest rol atât pe durata incidentelor cât şi post factum, datorită experienţei personalului specializat în astfel de evenimente, la fel cum o echipă de investigaţii criminale din lumea non-IT îl joacă atunci când intervine la un incident real cu victime umane ori după ce acesta sa desfăşurat, căutând probe video, audio, obiecte implicate în incident, urme de violenţă şi probe care pot fi analizate inclusiv prin metode moderne, precum maparea ADN.

3.2. Servicii proactive oferite de o echipă CERT

Din ce în ce mai mult, echipele CERT oferă servicii menite să prevină apariţia unor incidente de securitate sau să diminueze impactul acestora în momentul producerii acestora, prevenţia fiind calea cea mai bună în asigurarea securităţii cibernetice, similar altor domenii.

Dacă luăm ca exemplu domeniul medical, este de la sine înţeles că prevenirea unor afecţiuni grave prin mijloace de informare şi monitorizare permanentă a stării de sănătate reprezintă cea mai bună cale în creşterea nivelului de sănătate a populaţiei.

3.2.1. Anunţurile

Anunţurile pe care o echipă CERT le face pentru organizaţiile deservite pot include alerte privind noi atacuri, tipuri de vulnerabilităţi ori noi unelte de atac cibernetic, toate acestea având drept urmare securizarea suplimentară a unor infrastructuri IT şi de comunicații, şi în final reducerea suprafeței de atac şi a impactului final al ameninţărilor informatice.

Anunţurile pot include o componentă reactivă, definită mai sus, în cadrul serviciilor de alertare şi avertizare, ca urmare a unor incidente deja în derulare, dar şi o componentă preventivă, pentru organizaţiile încă neafectate de ameninţarea în cauză ori care încă nu au realizat că deţin sisteme informatice compromise ca urmare a manifestării acesteia.

3.2.2. Urmărirea evoluţiei tehnologiei

Una dintre cele mai importante activităţi pe care o echipă CERT le desfășoară este urmărirea progreselor tehnologice din domeniul IT&C şi a noilor vectori de atac ce pot afecta infrastructuri existente.

În domenii în care tehnologia evoluează rapid, precum cel al telecomunicaţiilor şi serviciilor IT, o echipă CERT trebuie să înţeleagă concepte relativ noi, precum „Voice over IP” (Voce peste IP) sau IPTV (Televiziune prin IP), „Video on Demand” (Video la cerere), 3G, 4G, dar şi modalităţile criminale prin care furnizorii şi utilizatorii acestora pot fi afectaţi.

În domeniul infrastructurilor energetice, de asemenea, este nevoie de o monitorizare a progresului tehnologic care include automatizarea excesivă a proceselor de producere, transport şi distribuţie a energiei electrice. Acestea încep să se bazeze din ce în ce mai mult pe sisteme de control industrial

conectate la reţele publice de comunicaţii, sisteme ce fac obiectul unor noi tipologii de atac cibernetic, cu impact devastator asupra tuturor sectoarelor economice dar şi asupra vieţii şi sănătăţii oamenilor.

Rolul echipelor CERT este să înţeleagă progresul tehnologic şi modul în care criminalii cibernetici sau adaptat acestuia, pentru a putea identifica modalităţi de protecţie în faţa imaginaţiei unei elite negative a hackerilor.

3.2.3. Evaluările de securitate

Pentru a înțelege mai ușor conceptul de evaluare de securitate, ne putem îndrepta atenția spre domeniul medical, în care evaluarea periodica a stării de sănătate a persoanelor, prin intermediul unor analize medicale uzuale, reprezintă un proces proactiv, care ajută la identificarea atât a unor vulnerabilități la diferite tipuri de afecțiuni cât şi la descoperirea în faze incipiente a unor afecțiuni existente. Desigur, această evaluare proactivă duce la anumite recomandări şi tratamente menite să sporească imunitatea organismului uman la diferite afecțiuni sau să reducă gradul celor existente.

În domeniul cibernetic, evaluările de securitate au rolul de a identifica vulnerabilitățile sistemelor informatice şi de comunicații la ameninţările cunoscute sau încă neidentificate. în urma acestor evaluări sunt propuse măsuri de reducere a riscurilor de exploatare a vulnerabilităților de către persoane rău intenționate.

Evaluările pot merge chiar pana la simularea unui atac real asupra sistemelor, prin exploatarea vulnerabilităților descoperite de către echipa de testare. Acest tip de acțiune este cunoscut drept test de penetrare şi are avantajul ca poate demonstra ce poate face cu adevărat un criminal informatic asupra sistemului testat. Fără doar şi poate, este de preferat ca o astfel de acțiune să fie derulată de o echipă CERT specializată în teste de penetrare, şi nu o entitate malițioasă care are cu totul alte intenții decât cele proactive.

3.2.4. Configurarea şi menținerea soluțiilor de securitate

In urma evaluărilor de securitate, echipele CERT pot recomanda deținătorilor infrastructurilor IT&C să implementeze anumite tehnologii de securitate, precum soluții antivirus, firewall ori sisteme de prevenire a intruziunilor, şi sa configureze echipamentele hardware şi aplicațiile sofware în conformitate cu cele mai bune practici de securitate, dezvoltate de comunitatea internațională a specialiștilor în domeniu.

Mai mult decât atât, echipele CERT se pot implica activ în configurarea sistemelor respective şi în administrarea soluțiilor de securitate, atunci când organizația deservită nu are resursele umane necesare.

Dacă rămânem pentru exemplificare în domeniul medical, există situaţii în care medicul recomandă, în urmă unor evaluări medicale a sănătăţii pacientului, un tratament injectabil. Deşi uşor de înţeles că şi concept de către pacient, acesta nu are competenţele şi resurse corespunzătoare pentru a implementa recomandările medicului şi apelează la personal specializat pentru „modificarea configuraţiei” organismului prin injectare, în acest caz un asistent medical, echivalentul unui specialist CERT din domeniul IT. Experienţă anterioară îl face pe acesta să aplice tratamentul în siguranţă şi cu

uşurinţă, la fel cum un specialist CERT configurează fără efort suplimentar un sistem informatic vulnerabil la ameninţări informatice.

3.2.5. Dezvoltarea uneltelor de securitate

Deşi în general restrânsă, activitatea de dezvoltare a unor unelte de securitate dedicate organizaţiilor deservite de echipa CERT este una care poate diferenţia o astfel de echipă şi arată capabilităţi ce ies din obişnuit. Uneltele de securitate pot fi aplicaţii complete sau doar componente de tip plug-in care extind funcţionalităţi ale celor utilizate de comunitate, precum platforme de testare a securităţii sau soluţii de distribuire automată a patch-urilor.

Ca exemplu, în cazul în care este descoperită o nouă vulnerabilitate într-o aplicaţie de monitorizare a stării unui pacient, echipa CERT naţională sau care deserveşte în mod direct sectorul medical poate dezvolta un modul de scanare care să identifice toate sistemele vulnerabile dintr-o instituţie medicală sau chiar un exploit, adică un mic program care, odată ataşat unei platforme specializate de atac precum Metasploit sub forma unui modul Ruby, să poată încerca exploatarea acestei vulnerabilităţi, în mod nedistructiv, pentru a demonstra uşurinţa cu care un atacator rău intenţionat ar putea pune în pericol viaţa sau sănătatea unui pacient.

3.2.6. Servicii de detectare a intruziunilor

Activitatea proactivă cu cel mai mare impact pozitiv asupra securităţii informatice este cea de detectare a intruziunilor, realizată prin intermediul analizelor complexe de loguri generate de echipamente diverse, care presupun atât unelte specializate ce pot corela evenimente provenind din surse diferite, şi care pot procesa cantităţi uriaşe de date, cât şi personal de analiză foarte specializat care să poată interpreta logurile şi să poată înţelege gravitatea unor evenimente derulate aproape în timp real.

Aceste servicii presupun analiză logurilor şi alertarea echipelor IT de intervenţie în cazul detectării unor evenimente ce ies din normal sau care urmează tipologia unor atacuri cibernetice cunoscute.

Datorită nivelului ridicat de specializare a personalului care poate derula o astfel de activitate şi a costului ridicat al uneltelor ce permit colectarea şi corelarea logurilor de la componentele infrastructurii IT, acest serviciu este de multe ori externalizat către echipele CERT naţionale, sectoriale sau private, precum cele ale furnizorilor de servicii de management al securităţii.

Un exemplu comparativ îl putem găsi în cazul organizaţiilor ale căror clădiri sunt protejate de firmele private de securitate fizică, care intervin cu echipe specializate în caz de efracţie după ce sistemele tehnice de securitate au semnalat către dispeceratul societăţii de pază o intruziune neautorizată în una din locaţii, detectată prin intermediul senzorilor care monitorizează punctele de acces sau spaţiile interioare din clădire.

3.2.7. Diseminarea informaţiilor din domeniul securităţii

În cadrul echipelor CERT există în general un proces de diseminare a informaţiilor din domeniul securităţii IT&C, menit să structureze într-o manieră logică şi prietenoasă avalanşă de
Informaţii provenită din surse publice, dar şi propriile ghiduri, recomandări, alerte, tutoriale sau publicaţii.

Acest proces optimizează efortul de informare a organizaţiilor deservite de CERT şi îi convinge pe specialiştii acestora să revină pentru a afla noutăţi din domeniul în care activează.

3.3. Servicii de management al calităţii securităţii

În funcţie de nivelul de expertiză şi resursele echipelor CERT, acestea pot oferi servicii suplimentare care nu sunt specifice procesului de răspuns la incidente de securitate, precum analiză de risc, elaborarea planurilor de continuitate a afacerii şi a planurilor de recuperare în caz de dezastre, consultanţă de securitate, instruirea personalului organizaţiilor deservite în domeniul securităţii informaţiei, cursuri de securitate IT sau a informaţiei ori evaluări şi certificări de produse.
Expertiza câştigată în urma intervenţiei la incidente de securitate este un atu important pe care îl deţin echipele CERT care oferă astfel de servicii adiţionale.

3.3.1. Analiză de risc

O echipă CERT care intervine frecvent la incidente de securitate complexe evaluează în termeni preciși riscurile care pot impacta o organizaţie, având experienţă atât în determinarea ameninţărilor din mediu, a probabilităţii cu care acestea pot afecta anumite tipuri de organizaţii sau de sisteme informatice şi de comunicaţii ce prezintă un grad specific de vulnerabilitate, cât şi a impactului probabil pe care ameninţările respective, odată materializate, l-ar genera asupra acesteia.

Făcând o paralelă în domeniul militar, cei mai buni specialişti în proiectarea măsurilor de securitate ale unui teatru de operaţiuni militare sunt cei care au participat deja în acţiuni militare desfăşurate în diverse colţuri ale lumii, aceştia anticipând cu uşurinţă ameninţările majore şi implicit riscurile la care este supus un astfel de teatru.

3.3.2. Elaborarea planurilor de continuitate a afacerii şi de recuperare în caz de dezastre

Mergând mai departe, o echipă CERT experimentată poate elabora planul de recuperare în caz de dezastre pentru diferite organizaţii, în cazul incidentelor cu impact major, precum şi paşii care trebuie urmaţi pentru a asigura supravieţuirea acestora în cazul unor incidente de acest tip.

Continuând paralela de la punctul anterior, foştii combatanţi de pe fronturile de luptă, pe lângă măsurile de securitate recomandate pentru noile teatre de operaţiuni, în baza experienţei reale de reacţie în situaţii limită, pot recomanda cu uşurinţă paşii de urmat în cazul apariţiei unui incident major, de exemplu în cazul unui atac ţintit cu rachete aer-sol asupra bazei militare aflate pe front, paşi meniţi să asigure supravieţuirea trupelor şi a echipamentelor de luptă.

3.3.3. Consultanţă de securitate

Organizaţiile deservite de o echipă CERT pot beneficia de experienţă acesteia atunci când intenţionează să implementeze noi sisteme, aplicaţii sau chiar procese de business sau să sporească securitatea celor existente. Consultanţă de securitate poate presupune chiar dezvoltarea de politici şi

proceduri interne organizaţiei, menite să structureze procesele interne ale acesteia şi să asigure cadrul de management al securităţii.

3.3.4. Instruirea în domeniul securităţii informaţiei

La fel cum specialiştii în stingerea incendiilor instruiesc periodic persoanele care lucrează în clădiri de birouri sau pe platforme industriale, în scopul prevenirii unor incidente nedorite, echipele CERT transferă informaţii utile privind asigurarea securităţii informaţiei la nivel de utilizator de sistem informatic sau de aplicație, prin sesiuni de instruire directă sau prin canale diverse, precum cel online.

Procesul de instruire are rolul de a reduce numărul de incidente şi impactul acestora prin sporirea nivelului de conştientizare a riscurilor de securitate de către utilizatorii finali de sisteme informatice.

3.3.5. Cursuri de securitate IT sau a informaţiei

Dacă instruirea în domeniul securităţii informaţiei are rolul de a conştientiza marea masă a utilizatorilor de sisteme informatice cu privire la riscurile de securitate cibernetică, cursurile specifice de securitate IT se adresează cu precădere personalului IT sau din zona securităţii informaţiei şi a managementului continuităţii afacerii, fără a exclude şi alte categorii de specialişti. Cursurile sunt bazate pe o curricula care poate include metode concrete de tratare a unui incident de securitate, modul de utilizare a uneltelor specializate în procesul de răspuns la incidente sau paşii unei investigaţii digitale.

3.3.6. Evaluări şi certificări de produse

Echipele CERT pot oferi servicii de evaluare a produselor ce urmează a fi utilizate de către organizaţiile deservite, oferind acestora un anumit nivel de încredere vis a vis de securitatea produsului respectiv cât şi de utilitatea şi conformitatea acestuia cu practicile de securitate recomandate.

Dacă facem o paralelă în viaţa de zi cu zi, aceste evaluări reprezintă filtrul pe care părinţii îl aplică atunci când copii doresc să îşi cumpere o jucărie, o carte sau dulciuri. Părinţii verifică vârsta recomandată pentru acel joc sau carte şi analizează eticheta cu ingrediente în cazul dulciurilor, aplicând experienţa lor pentru protejarea persoanelor dragi.

Procesul formal prin care se declară nivelul de securitate al produselor dedus din activitatea de evaluare îl reprezintă certificarea acestora, un astfel de produs certificat putând fi utilizat cu încredere în arhitecturile IT&C ale organizaţiilor deservite.

4. Tipurile de CERT

În funcţie de organizaţiile pe care le deservesc, de nivelul de autoritate sau de competentele pe care le deţin, echipele CERT se încadrează în una sau mai multe din categoriile următoare:

- CERT naţional
- CERT guvernamental
- CERT academic

- CERT privat

4.1. CERT naţional

Echipele de tip CERT naţional reprezintă punctele de contact naţionale pentru incidentele de securitate cibernetică, şi au rol de coordonare a celorlalte echipe CERT guvernamentale în cazul unor incidente majore la nivelul unei ţări sau al unui sector economic.

Acestea au, în general o autoritate impusă prin lege dar şi o autoritate dată de competenţe ale personalului specializat în intervenţii la o gamă largă de incidente de securitate de complexitate sporită.

În România, CERT-RO reprezintă centrul naţional de răspuns la incidente de securitate cibernetică, punctul naţional de contact cu structurile de tip similar, care asigură elaborarea şi diseminarea politicilor publice de prevenire şi contracarare a incidentelor din cadrul infrastructurilor cibernetice, potrivit ariei de competenţă, analizând în plus disfuncţionalităţile procedurale şi tehnice la nivelul infrastructurilor cibernetice.

Serviciile pe care echipa CERT-RO le oferă:

- Serviciile publice de tip preventiv:
  - Anunţuri privind evenimente în domeniu.
  - Anunţuri privind ameninţări nou-identificate pe plan naţional şi interrnational ▪ Cercetare şi informare privind noutăţile tehnologice în domeniu.
  - Realizarea, la cerere, de auditări şi evaluări de securitate sau teste de penetrare.
  - Estimarea vulnerabilităţilor şi punerea la dispoziţie de situaţii actualizate privind încercările de intruziune şi servicii de localizare a surselor atacurilor, pe baza informaţilor transmise de furnizorii de reţele şi servicii de comunicaţii electronice. ▪ Diseminarea informaţiilor de securitate cibernetică.
- Serviciile publice de tip reactiv:
  - Alerte şi atenţionări privind apariţia unor activităţi premergătoare atacurilor.
  - Gestiunea incidentelor la nivel naţional, în cooperare cu celelalte echipe CERT.
  - Diseminarea rezultatelor investigaţii lor incidentelor de securitate cibernetică cu respectarea prevederilor acordurilor de cooperare încheiate cu partenerii CERT-RO.
- Serviciile publice de consultanţă pentru managementul calităţii serviciilor de securitate cibernetică:
  - Analize de risc aplicate la nivel local şi la nivel naţional privind infrastructurile cibernetice.
  - Planificarea asigurării funcţionării continue şi a recuperării în caz de dezastre.
  - Atestarea managementului securităţii ciberneticce şi a incidentelor cibernetice.
  - Pregătirea echipelor de tip CERT, a echipelor de audit în domeniul securităţii reţelelor, cu prioritate a celor incluse în infrastructura critică naţională

4.2. CERT guvernamental

Echipele CERT guvernamentale asigură servicii agenţiilor guvernamentale şi chiar cetăţenilor unei ţări, în mod direct. Serviciile oferite sunt similare unui CERT naţional, însă acoperă în general doar sectoarele peste care echipa CERT are autoritate impusă prin diferite ordine şi reglementări.

Exemple de echipe CERT guvernamentale sunt CERTMIL, care deserveşte structurile Ministerului Apărării Naţionale şi CORIS-STS, desemnată să prevină şi să răspundă la incidentele legate de securitatea sistemelor informatice şi de comunicaţii ale Serviciului de Telecomunicaţii Speciale şi ale beneficiarilor acestuia.

În prezent există o tendinţă de dezvoltare a unui nou tip de CERT guvernamental, specializat în protecţia infrastructurilor critice din diferite sectoare de activitate, cu precădere a sistemelor de control industrial şi de automatizare a proceselor critice. În Statele Unite există deja o astfel de entitate[5], care oferă atât servicii proactive cât şi reactive. De exemplu, un astfel de CERT îşi propune să protejeze viaţa şi sănătatea pacienţilor spitalelor din întreaga comunitate, care utilizează infrastructuri IT specifice domeniului medical, precum echipamente din săli de urgenţă sau specifice terapiei intensive, ori echipamentele specifice laboratoarelor de analize medicale, care sunt din ce în ce mai mult vizate de specialişti în descoperirea breşelor de securitate.

4.3. CERT academic

Echipele de tip CERT academic furnizează servicii şcolilor, liceelor, universităţilor şi institutelor de cercetare, uneori şi datorită conectării acestora la o infrastructură de telecomunicaţii comună, aşa cum este cazul RoEduNet CSIRT.
Avantajele unui astfel de CERT vin din expertiza ştiinţifică de nivel ridicat, graţie mediului universitar în care găsim cercetători şi studenţi dornici să descopere noi ameninţări cibernetice şi soluţii adecvate pentru reducerea riscurilor asociate. O serie de teze de cercetare, de masterat sau de doctorat pot contribui la sporirea nivelului de excelentă în domeniul securităţii cibernetice al unei echipe CERT de tip academic.

4.4. CERT privat

Din ce în ce mai mult îşi fac simţită prezenţa echipele CERT private, care aduc în acest club select al echipelor de răspuns la incidente cibernetice specialişti recunoscuţi pentru competentele lor în unul din cele mai complexe domenii ale tehnologiei informaţiei.

Fie că vorbim de echipe CERT ale producătorilor de tehnologie hardware şi software, care reacţionează tot mai rapid în momentul descoperirii unor vulnerabilităţi de securitate în soluţiile pe care le dezvolta şi le oferă pe piaţă, fie că vorbim de echipe specializate din organizaţiile private mari menite să răspundă la incidentele care le atinge propriile procese de business sau clienţii direcţi ai acestora, fie că ne referim la echipe CERT comerciale care oferă servicii proactive, reactive şi de management al calităţii securităţii contra cost, echipele private reprezintă un partener extrem de puternic pentru cele de tip naţional, guvernamental sau academic.

În aceste echipe găsim specialişti de top, consultanţi costisitori de securitate super specializaţi pe nişe ale domeniului său care au o viziune completă asupra unor incidente complexe datorată activităţii în

cadrul unor multiple organizaţii din sectoare economice diverse, presărată cu incidente de tipologii diferite.

5. Utilitatea CERT-urilor private

De ce este nevoie de echipe CERT private?

Unul din motivele fundamentale este acela că incidentele de securitate care vizează infrastructuri ale organismelor publice şi private au o tendinţă de creştere exponenţială, ce nu poate fi contracarată doar de către echipele CERT din domeniul public, în care resursele sunt limitate.

Este nevoie ca în fiecare organizaţie privată mare din punct de vedere al infrastructurii IT&C să existe o echipă de răspuns care, pe de o parte, să ofere servicii pentru protejarea propriei companii, şi pe de altă parte să coopereze cu echipele CERT naţionale, precum CERT-RO, acestea din urmă putând facilita într-un mod anonimizat schimbul de idei şi competenţe care pot reduce timpul de identificare a unei soluţii de răspuns la incident. În plus, experienţa câştigată în urma acestui incident poate fi transferată tuturor partenerilor privaţi ai echipei CERT naţionale, fără costuri suplimentare. Este vorba, dacă vreţi, de o reţea de experţi a căror expertiza este partajată printr-un hub naţional, în beneficiul tuturor.

Cu cât se înființează mai multe CERT-uri în organizaţii private, cu atât reţeaua de experţi capabili să trateze incidente de securitate complexe este mai bogată în rezultate remarcabile.

În prezent, la nivel naţional, funcţionează echipe CERT private în diferite sectoare, cu precădere în domeniile vizate agresiv de incidente de securitate cibernetică, precum cel al telecomunicaţiilor sau din mediul bancar. Aceste echipe sunt, de obicei, derivate din echipele responsabile cu asigurarea securităţii informaţiei sau a securităţii IT&C, şi cuprind specialişti din zona tehnică, familiarizaţi cu infrastructura care susţine procesele de business, cât şi din alte departamente, precum cel de relaţii publice, juridic, financiar sau administrativ.

Producătorii de soluţii hardware şi software sunt obligaţi să reacţioneze din ce în ce mai rapid atunci când un specialist în domeniul securităţii IT descoperă o breşă importantă, care, o dată exploatată de o persoană cu intenţii maliţioase, poate impacta major organizaţiile care le-au achiziţionat anterior. În cazuri mai puţin fericite, în care pe piaţa neagră apare deja un exploit care ar putea compromite sistemele critice bazate pe acele soluţii software sau hardware, producătorii au un timp de reacţie care tinde la zero, iar o echipă CERT poate face diferenţa.
Aceasta are deja capacitatea de a reacţiona rapid cu soluţii temporare de limitare a impactului în cazul exploatării vulnerabilităţii descoperite, până la dezvoltarea unei soluţii de remediere complete, cum sunt patch-urile de securitate. Colaborarea cu echipele CERT guvernamentale şi naţionale este foarte importantă, întrucât acestea pot comunica rapid organizaţiilor deservite metodele temporare de protecţie pentru acele tipuri de echipamente sau programe software, uneori chiar pe canale securizate, non-publice.

Companiile specializate în furnizarea de servicii de securitate informatică încep să împacheteze oferta proprie în servicii de tip CERT, pe care le oferă contra cost pe bază de abonament sau a unei taxe plătite o singură dată. De exemplu, ca servicii reactive, sunt deja disponibile pe piaţa de securitate din ţara noastră soluţii management al vulnerabilităţilor, de monitorizare şi răspuns la incidentele de securitate ce vizează infrastructurile IT&C ale clienţilor, având administrarea în cloud din perspectiva clienţilor, servicii de investigaţii digitale pe durată şi după încheierea evenimentelor de securitate.

Serviciile proactive sunt, la rândul lor, foarte dezvoltate, incluzând atât evaluări de securitate şi teste de penetrare cât şi managementul soluţiilor de securitate şi al configuraţiilor echipamentelor de infrastructură, sau chiar detecţia intruziunilor prin soluţii oferite ca serviciu, în cloud sau în reţeaua beneficiarilor. Poate cele mai răspândite servicii sunt cele de management al calităţii securităţii, precum analizele de risc, planificarea continuităţii afacerii, consultanţă de securitate pe diferite segmente sau chiar instruirea şi cursurile de securitate informatică.

Echipele CERT private de tip comercial acţionează ca un CERT guvernamental pentru companiile private sau publice deservite, iar colaborarea cu echipele CERT naţionale, precum CERT-RO, nu poate fi decât benefică tuturor. Există o anumită cerinţă de anonimitate din partea companiilor private, lesne de înţeles pe piaţă din ce în ce mai concurenţială din ţara noastră, iar această cerinţă se poate atinge mult mai uşor prin intermedierea unui CERT privat comercial, cu care există acorduri ferme de confidenţialitate. Un CERT naţional poate fi informat de către un CERT privat cu privire la noi tipuri de incidente de securitate, în condiţii de anonimitate deplină, dar cu detalii tehnice suficiente pentru a se găsi o rezolvare în comunitatea naţională şi internaţională de experţi.

6. **Concluzie**

Echipele de tip CERT, fie ele de tip naţional, precum CERT-RO, fie guvernamentale, academice sau private, au un rol precis şi foarte important în limitarea daunelor pe care incidentele de securitate cibernetică le pot produce organizaţiilor publice sau private, şi nu în ultimul rând utilizatorilor individuali de sisteme informatice şi de comunicaţii.

Ca şi în alte domenii precum cel al sănătăţii sau al prevenirii şi stingerii incendiilor, echipele CERT acţionează pe trei direcţii complementare, oferind servicii proactive, reactive şi de management al calităţii proceselor de securitate propriu zise.

Colaborarea între echipele de tip CERT publice şi private este esenţială în condiţiile în care criminalitatea informatică are o tendinţă ascendentă de tip exponenţial atât în plan cantitativ cât şi calitativ, numărul de atacuri cibernetice de complexitate ridicată având drept scop obţinerea unor venituri ilicite greu de imaginat în trecut, transmiterea unor mesaje din partea activiştilor radicali sau chiar câştigarea războiului cibernetic de către hackeri înregimentaţi de state de pe glob, crescând cu mult peste pragul la care apărarea se poate duce în mod izolat.

Mai mult decât atât, CERT-RO poate acţiona drept catalizator al specialiştilor în securitate informatică ce activează în cadrul echipelor private de răspuns la incidente, facilitând comunicarea deschisă între aceştia şi obţinerea unui rezultat mai important decât suma celor realizate separat.

Recomandăm cu tărie că organizaţiile care au de protejat procese critice să îşi construiască o proprie echipa de răspuns la incidente de securitate sau sa se arondeze la una din echipele CERT existente în tara noastră, precum cea naţională, CERT-RO, cele guvernamentale sau academice, ori unei echipe CERT private de tip comercial.

7. **Despre autori**

Compania ISEC Associates oferă clienților săi un portofoliu complet de servicii de securitate cibernetică, acoperind întreg spectrul serviciilor reactive, proactive şi de management al calității securității specifice unei echipe de tip CERT, printre care managementul riscurilor de securitate, stabilirea cerințelor de securitate şi implementarea acestora în cadrul proiectelor IT complexe, evaluări de securitate şi teste de penetrare, detecția şi managementul complet al incidentelor de securitate, managementul vulnerabilităților, planificarea continuității afacerii sau instruirea de securitate pentru angajați.

ISEC Associates face parte din Provision IT Group, furnizor principal al celor mai renumite soluții de securitate IT, training şi servicii profesionale pentru clienții din România, un centru recunoscut de experți, în care inovația a reprezentat o direcție strategică încă de la înființarea sa, în anul 1997.

8. **Bibliografie**

- *Handbook for Computer Security Incident Response Teams (CSIRTs)*, Moira J. West-Brown Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, Mark Zajicek *First release: December 1998; 2nd Edition: April 2003*

- *O abordare pas cu pas a modului de creare a unui CSIRT,* ENISA, Produs final WP2006/5.1 (CERT-D1/D2)