Analiza costurilor unui atac cibernetic

Adrian Victor VEVERA, Adriana Meda UDROIU

Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București
B-dul Mareșal Alexandru Averescu, Nr. 8-10, 011455, București, România
victor.vevera@ici.ro, meda.udroiu@rotld.ro

Rezumat: Atacurile cibernetice s-au dezvoltat și creează pagube într-o serie largă de domenii. Daunele unui atac pot conduce la costuri de zeci de milioane dolari sau pot duce la dizolvarea completă a unei industrii. Problema este că impactul este din ce în ce mai mare, deoarece suprafața în care atacatorii pot să activeze este din ce în ce mai extinsă. De aceea, este imperios necesară prevenirea atacurilor. Această lucrare prezintă o analiză detaliată asupra costurilor unui atac cibernetic bazată pe statistici efectuate de marile companii precum și de cercetători, referitoare la costurile pentru prevenirea unui atac, costurile în funcție de tipurile de atac, dar și cele pentru rezolvarea pagubelor.

Cuvinte cheie: atac cibernetic, costuri, prevenire.

Cost analisy for cyberattack

Abstract: Cyber attacks have developed and created damage in a wide range of areas. The damage to an attack can lead to costs of tens of millions of dollars or may lead to the complete dissolution of an industry. The problem is that the impact is increasing, because the surface in which attackers can activate is more and more widespread. Therefore, it is imperative to prevent attacks. This paper presents a detailed analysis of the cost of a cyber attack based on statistics by large companies as well as by researchers on the costs of preventing an attack, the costs of attack types, but the ways to solve the damage.

Keywords: cyberattack, costs, prevention.

Introducere

Dezvoltarea tehnologiei a însemnat un progres și o reconfigurare majoră a modului în care companiile își desfășoară activitatea. Din păcate, noile tehnologii nu includ doar beneficii, ci favorizează și o serie de riscuri precum creșterea breșelor de securitate atât în cadrul companiilor, cât și în cadrul oricărui sistem care este conectat printr-o rețea Internet. Astfel, atacurile cibernetice s-au dezvoltat și creează pagube într-o serie largă de domenii, iar pe viitor amenințările vor crește în volum și vor fi din ce în ce mai sofisticate.

Motivația atacatorilor a devenit mai puternică și crimele cibernetice au luat amploare de-a lungul timpului datorită intereselor financiare. Acest lucru a contribuit la dezvoltarea organizațiilor specializate în furtul informației. Atacurile cibernetice produc prejudicii financiare, dar totodată pot afecta reputația unei companii precum și întreaga dezvoltare pe termen lung. Furtul de informații și discontinuitatea activității continuă să reprezinte cele mai mari costuri externe ale unei țări. Anual, furtul de informații generează 44% din totalul costurilor externe. În ultimii doi ani, costurile atacurilor cibernetice au crescut cu un procentaj de 23% față de anii anteriori, companiile raportând atacuri majore la intervale de timp scurte. Costurile atacurilor au ajuns la o medie de aproximativ 11,7 milioane de dolari. De aceea, marile companii alocă sume mari de bani pentru a putea preveni atacurile, dar și pentru a remedia eventualele daune apărute. De aceea, implementarea soluțiilor avansate de securitate informațională a devenit o necesitate. Focusul în cazul atacurilor cibernetice este asupra prevenirii lor, dar anumite servicii de securitate și protecție nu furnizează întotdeauna cele mai bune servicii, iar unele pagube nu pot fi evitate. Recuperarea și detecția continuă să reprezinte cele mai costisitoare activități interne asociate cu infracționalitatea cibernetică. Acestor activități li se atribuie aproape jumătate din totalul costurilor interne pe an.

Definiții

Un atac cibernetic poate fi definit ca încercarea rău-voită de a produce prejudicii temporare sau permanente componentelor dintr-o rețea Internet. Dintre atacurile cibernetice, le amintim pe cele asupra infrastructurilor critice deoarece prezintă cel mai mare impact asupra unui întreg sistem, referindu-ne aici la un întreg oraș sau chiar la o întreagă țară. Atacurile pornesc de la exploatarea unui vulnerabilități a sistemului. Vulnerabilitățile conduc la furtul de informații, sabotaj, spionaj, prejudicii asupra informațiilor confidențiale etc. O organizație de atacatori vinde informațiile confidențiale furate, în schimbul unor sume de bani sau le păstrează pentru eventuale atacuri viitoare. Acestea sunt doar câteva dintre cele mai întâlnite strategii, dar atacatorii nu se opresc doar aici, iar informațiile pot fi folosite în numeroase scopuri.

Odată cu dezvoltarea tehnologiei crește și cantitatea de informații și astfel controlul asupra sistemelor nu poate fi complet ducând la apariția vulnerabilităților. În ultimii ani s-a înregistrat un număr de aproximativ 190 de vulnerabilități dintre care 49% au fost încadrate ca fiind critice, iar 42% ca fiind severe. Amintim câteva dintre cele mai importante tipuri de atacuri produse de vulnerabilități critice.

În primul rând, vulnerabilitățile care pot fi exploatate se referă și la persoane, nu numai la sisteme informatice. Atacurile de tip social engineering aduc în prim plan omul şi greşelile lui. Atacatorul trebuie doar să posede doar anumite tehnici de persuasiune. Astfel, el încearcă să câştige încrederea utilizatorilor, obținând astfel drepturi pentru a se putea conecta la sisteme. În multe cazuri, această metodă este cea mai uşoară formă de obţinere de acces la un sistem informaţional.

În continuare, amintim atacurile cunoscute sub numele de Denial-of-Service (DoS). Atacurile DoS sunt printre cele mai frecvente atacuri și vizează întreruperea serviciilor unei reţele sau ale unui server. Scopul unui atac DoS este de a genera o cantitate foarte mare de trafic care face sistemul sa nu mai funcţioneze normal sau chiar să îl întrerupă.

Un virus este un program creat să distrugă datele sau echipamentele unui calculator. Viruşii sunt programe cu dimensiuni foarte mici, ascunşi fie în fişiere executabile fie ataşaţi unor programe. Aceștia au scopul de a distruge datele din calculator sau chiar componentele acestuia.

Tot în această categorie a virușilor vom vorbi și despre viermi. Aceștia sunt programe care se multiplică în cadrul unei reţele de calculatoare şi reprezintă un pericol mare deoarece foloseşte resursele calculatorului provocând supraîncărcarea sistemului.

Calul Trojan este un virus ascuns în spatele altor programe lăsând o uşă deschisă prin care un hacker poate controla calculatorul. Alte exemple din categoria troienilor au ca scop principal atacul spre un server, trimiţând mii de solicitări pe secundă.

Sql injection este un atac prin care sunt inserate comenzi de SQL în cadrul aplicațiilor web cu scopul de a obține informații din baza de date. Un atacator poate folosi această metodă cu scopul de a obține credențialele de autentificare sau pentru a trece de macanismele de autorizare. Mai mult de atât atacatorul poate modifica baza de date afectând integritatea datelor.

Tot din punct de vedere al atacurilor asupra aplicațiilor web, amintim cross-site scripting injection. În cadrul atacului sunt trimise scripturi cu scopul de a impersonaliza utilizatorii autorizați pentru a obține informații sau control asupra sistemului.

Atacul cunoscut sub numele de man-in-the-middle reprezintă un atac asupra protocolului de comunicare. O persoană neautorizată interceptează, capturează și monitorizează comunicarea dintre două entități fără ca acestea să o poată detecta. Acest atac întrerupe brețele de securitate, atacatorul obținând controlul asupra sistemului și fiind astfel capabil să modifice datele, să introducă viruși, să întrerupă complet funcționalitățile sistemului.

Dintre cele mai importante atacuri apărute în ultima perioadă, amintim incidentele cu WannaCry, Pentya, CryptoLocker, TeslaCryp, SimpleLocker și Eternal vigilance. Una dintre cele mai grave daune provocate în urma unui atac este furtul de aproximativ 143 milioane de conturi furate din cadrul companiei Equifax. Astfel, furtul de informații rămâne una dintre cele mai costisitoare consecințe ale unui atac. Conform studiilor realizate pierderea de informații reprezintă componenta cea mai costisitoare în cazul unui atac precum și cea mai predispusă, iar numărul de pierderi a crescut cu un procentaj de 10% pe parcursul unui an. În acest scop organizațiile și-au restabilit prioritățile pentru a face față noilor atacuri.

Costurile unui atac cibernetic la nivelul unei companii

În continuare încercăm să înțelegem mai bine importanța deciziilor pentru investiții în cadrul unei companii luând în considerare două aspecte majore: costurile pentru prevenirea atacurilor și costurile pentru dezvoltarea tehnologiilor proprii companiei. S-a constatat că investiția se axa pe dezvoltarea unor tehnologii vechi sau nu suficient de bune, ceea ce ducea la o vulnerabilitate mai mare în cazul unui atac. Conform unui studiu realizat sunt prezentate în imaginea de mai jos aspectele pozitive sau negative ale investițiilor în funcție de tehnologiile alese.

Prezentul studiu se bazează pe evaluările făcute asupra a 254 de companii și 2182 de interviuri în țări precum Australia, Germania, Franța, Japonia, Regatul Unit, Statele Unite. După cum se observă în graficul anterior sistemele de securitate inteligente și controlul avansat al accesului și al identității au crescut cu un procent de 67%, respectiv 63% și reprezintă topul tehnologiilor dezvoltate de marile companii. Unul dintre motivele principale pentru dezvoltarea tehnologiilor menționate anterior este profitul obținut întrucât acestea reduc costurile unui atac cu aproximativ 2.8 milioane de dolari. Există de asemenea alte tehnologii care ar reduce costurile unui atac, dar profitul nu ar fi la fel de mare. De aceea, chiar dacă oportunitățile există, costurile trebuie recalculate înaintea fiecărei investiții. De asemenea, utilizarea anumitor tehnologii trebuie calculată și în funcție eficiență și impactul asupra afacerii propriu-zise a companiei. Totodată, inovația tehnologică poate reprezenta și un mare dezavantaj, deoarece companiile nu pot ține pasul astfel încât să dezvolte propriile tehnologii și să facă investiții în sistemele de securitate. De aceea, conform studiilor realizate, baza pentru un sistem de securitate puternic și eficient este reprezentată de identificarea părților critice și protejarea acestora. Protecția acestor componente reduce costurile alocate securității, face grea misiunea atacatorilor și diminuează pagubele rezultate în urma unui atac.

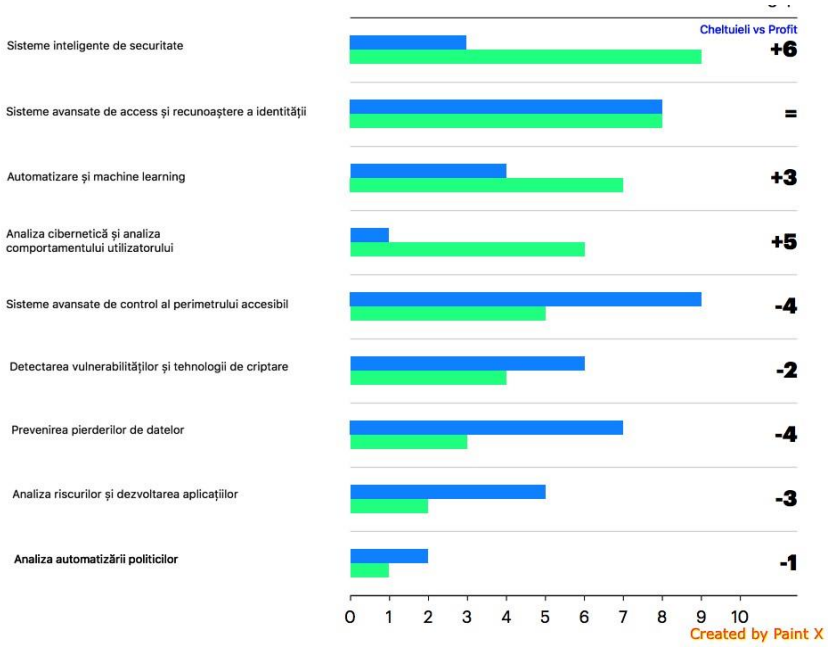

Figura 1. Aspectele pozitive și negative ale investițiilor

Au fost definiți anumiți pași imperios necesari protecției unui sistem cu scopul de a reduce costurile unui atac. Aceștia au fost realizați în urma studiilor efectuate care au condus la rezultate remarcabile în cazul unui atac. Astfel amintim costurile unei companii în cazul unui atac sunt de aproximativ 2,4 milioane de dolari, durata de soluționare și diminuare a pagubelor este de 23 de zile în cazul unui atac extern și de 50 de zile în cazul unui atac intern.

Variația costurilor în funcție de diferiți factori

În paragrafele precedente am vorbit de costurile unui atac la nivelul unei companii, dar acestea variază și în funcție de țara, dimensiunea unei organizații, industrie, tipul de atac, eficiența și experiența organizației afectate. În continuare vom prezenta în detaliu fiecare dintre aceste aspecte. Media costurilor unui atac în funcție de țară, dimensiunea organizației și industrii. În figura de mai jos este prezentată media costurilor în cazul atacurilor cibernetice în ultimii 5 ani. Se poate observa o creștere de 27,4% doar în ultimul an.

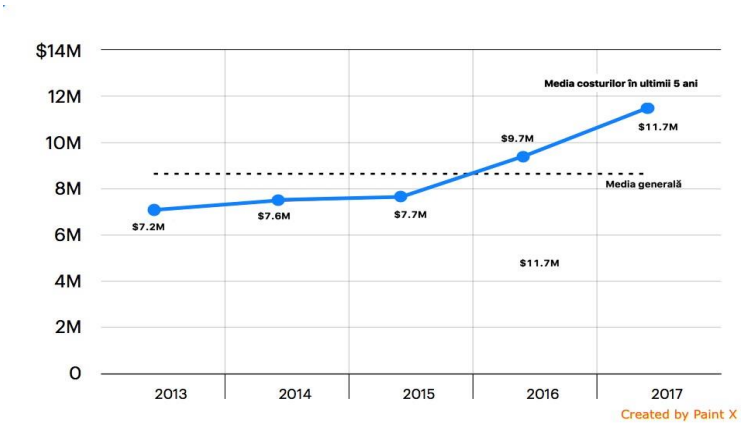

Figura 2. Media costurilor la nivel global

O prezentare mai detaliată a costurilor se regăsește în graficul următor în care studiul a fost realizat luând în considerare 254 de companii din 7 țări. Costurile raportate variază de la 5,41 milioane de dolari în Australia până la 21 milioane de dolari în Statele Unite. Pentru o analiză detaliată costurile au fost calculate având la bază raporturile companiilor pe o durată de patru săptămâni consecutive în care s-au confruntat cu atacuri cibernetice.

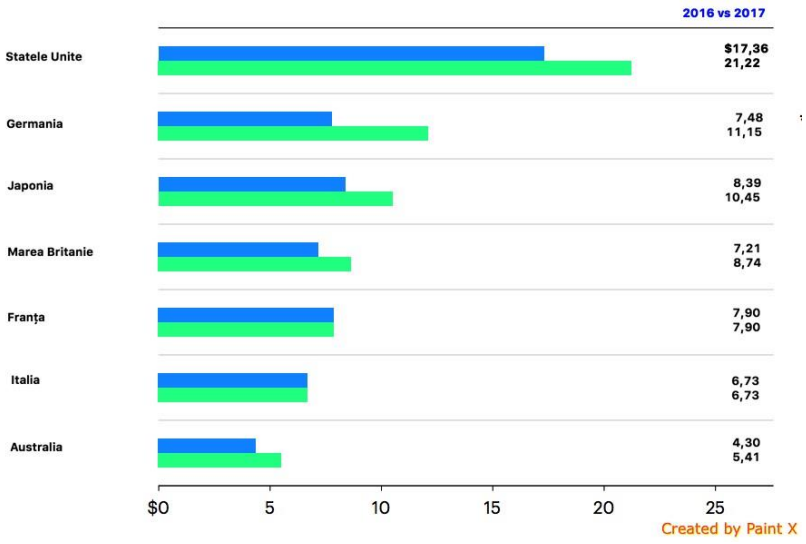

Figura 3. Analiza costurilor companiilor din șapte țări

La nivel anual distribuția costurilor pentru aceleași companii este reprezentată mai jos. Se poate observa că valoarea medie se situează la valoarea de 11,7 milioane de dolari, iar cel mai ridicat cost înregistrat are valoare de 77,1 milioane de dolari. De asemenea, 163 de organizații au o valoare a costurilor sub cea medie.

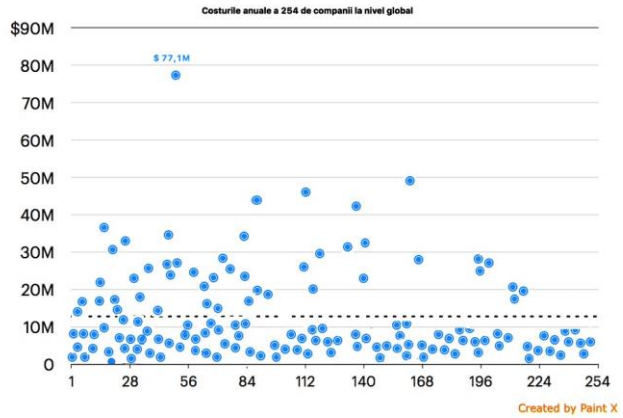

Figura 4. Costurile anuale ale companiilor celor șapte țări

Concluzii

Conform studiilor realizate [3, 5, 2] costurile atacurilor cibernetice vor atinge în anul 2021 o medie de șase trilioane de dolari pe an. Acesta reprezintă un cost enorm și pentru moment greu de imaginat. Cu toate acestea, ceea ce este cu adevărat îngrijorător, nu este numărul în sine, ci impactul atacurilor asupra dezvoltării tehnologiei și afacerilor. De aceea, la nivel mondial bugetul alocat pentru protejarea împotriva atacurilor cibernetice crește considerabil de la un an la altul, cu scopul de a împiedica eventualele catastrofe cibernetice. După cum am remarcat în paragrafele anterioare efectele colaterale ale atacurilor cibernetice sunt multiple și se vor extinde odată cu progresul tehnologic. Atenția acordată prevenirii atacurilor cibernetice nu trebuie sa fie doar din partea companiilor mari și instituțiile de stat ci mai ales din partea companiilor mici deoarece daunele provocate de un atac nu sunt doar greu de reparat ci pot conduce la dizolvarea completă a unei companii, iar riscul asumat de companii mici este unul mai mare în comparație cu cel al instituțiilor dezvoltate la scală largă.

Mulțumiri

Acest articol a fost posibil prin grija programelor de finanțate ale Ministerului Cercetării și Inovării, UEFISCDI**, proiect** 8SOL/2018 din cadrul PNCDIII, cod: PN-III-P2-2.1-SOL-2017-09-0102, nume: Sistem Informatic Integrat pentru Managementul Activităților.

BIBLIOGRAFIE

1. Hannah Kuchler. Cost of cyber crime rises rapidly as attacks increase. URL: https: //www.ft.com/content/56dae748-af79-11e7-8076-0a4bdda92ca2.
2. Nick Eubanks. The true cost of cybercrime for businesses. URL: https://www.forbes.com/ sites/theyec/2017/07/13/ the-true-cost-of-cybercrime-for-businesses/#5d0057ec4947;
3. North American enterprises and SMBs. Cyber attacks cost u.s. enterprises $1.3 million on average in 2017. URL: https://www.accenture.com/t20170926T072837Z__w__/us-en/ acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf;
4. Notpetya cyber-attack cost tnt at least $300m. URL: http://www.bbc.com/news/ technology -41336086;
5. The true cost of cybercrime for businesses. URL: https://www.forbes.com/sites/ theyec /2017/ 07/13/the-true-cost-of-cybercrime-for-businesses/ #5d0057ec4947;

Adrian Victor VEVERA este Director Tehnic, cercetător științific gradul II și membru în Consiliul Științific al Institutului Național de Cercetare-Dezvoltare în Informatică. Doctor în științe militare și informații, fiind la bază atât jurist cât și inginer specializat în fizică nucleară, deține o vastă experiență în ceea ce înseamnă securitatea națională, ocupând, de-a lungul timpului, numeroase poziții manageriale și de consiliere în diverse organisme ale statului. A publicat numeroase articole și lucrări pe teme de securitate națională și internațională, securitate energetică, criminalitate informatică, protecția infrastructurilor critice și a fost coordonatorul a numeroase proiecte de interes național.

Adrian Victor VEVERA is a Senior Researcher II, the Technical Director and a member of the Scientific Council of the National Institute for Research and Development in Informatics. Doctor of Military Sciences and Information, being both a lawyer and a nuclear physics engineer, Mr. Vevera has extensive experience in the field of national security, fulfilling various positions, over time, in numerous managerial and counseling positions in different state organisms. He has published numerous articles and papers on national and international security issues, energy security, cybercrime, critical infrastructure protection, and has been the coordinator of numerous projects of national interest.

Adriana Meda UDROIU este șeful „*Centrului de formare și pregătire profesională continuă*” din cadrul ICI București și conferențiar universitar la Facultatea de Automatică și Calculatoare din Universitatea Politehnica București și Academia Tehnică Militară. A obținut titlul de doctor în Sisteme automate la Politehnica București în anul 2003. Principalele domenii de interes pentru activitatea de cercetare sunt: securitate cibernetică, protecția infrastructurilor critice, securitatea informației, elearning, formare continuă.

Adriana Meda UDROIU is a Head of Lifelong Learning Department of ICI Bucharest and associate professor at the 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”. She received the PhD degree in Automated Systems from the University Politehnica of Bucharest in 2003. Her research interests include: cybersecurity, critical infrastructure protection, information security, elearning, lifelong learning.