ISBN 978-9975-180-05-4, DOI: 10.53486/sstc.v1

DOI: https://doi.org/10.53486/sstc.v1.18
CZU: 330.131.7:004

RISCUL CIBERNETIC - PROVOCAREA COMPANIILOR SECOLULUI XXI. IMPACT ȘI FORME DE MANIFESTARE

CYBER RISK - THE CHALLENGE OF 21ST CENTURY COMPANIES. THE IMPACT AND FORMS OF MANIFESTATION

GÎNU Diana, Specialitatea: BA,
Academia de Studii Economice din Moldova
R. Moldova, Mun. Chișinău, str. Mitropolit Gavriil Bănulescu-Bodoni 61
e-mail autor: ginu.diana@ase.md

Abstract. *It's not easy to keep up with new technologies, cyber security trends and all information about information threats. In this article I will present as broad and concise a picture as possible of the most common types of cyber attacks, their mode of action and the impact they can create.*

Keywords: *risks, cyber risk, cyber attacks, virus, espionage*

JEL CLASSIFICATION: M15, D81, K24, O33

INTRODUCERE

În secolul XXI toate afacerile au la baza funcționării sisteme informaționale, unde fiecare dintre ele pot suferi un atac sub formă de criptare, scurgere sau preluare de date, care se va solda inevitabil cu pierdere de bani, indisponibilitate de funcționare a business-ului și sistarea temporară a funcționării afacerii. În acest context, scopul urmărit al cercetării date este de a prezenta o imagine cât mai amplă și concisă a celor mai întâlnite tipuri de atacuri cibernetice, modul lor de acționare, dar și impactul pe care acestea îl pot crea.

CONȚINUTUL DE BAZĂ

Prin intermediul surselor mass-media și a articolelor oferite de diferite comapnii a căror activitate este bazată pe domeniul IT, am realizat o cercetare științifică prin metoda documentării, efectuând observarea și analiza surselor secundare, cum ar fi: știri, statistici, ghiduri și articole referitoare la tipurile de atacuri cibernetice, autorii acestora, formele lor de manifestare și impactul.

Securitatea cibernetică reprezintă practica de a proteja informațiile, dispozitivele și activele digitale ce cuprind informațiile personale, conturile, fișierele, fotografiile și chiar banii. Atacurile cibernetice au scopul de a deteriora, obține control sau acces la documente și sisteme importante dintr-o rețea de calculatoare de firmă sau personală. Motivele atacatorului pot include furtul de informații, câștigul financiar, spionajul sau sabotajul. [1]

Se cunosc o serie de tipuri de atacuri cibernetice dintre care cele mai întâlnite sunt:

Malware, cel mai comun tip de atac cibernetic. Programele malware se infiltrează într-un sistem, de obicei prin solicitarea utilizatorilor de a accesa un link pe un site web dubios, prin e-mail prin descărcarea unui atașament infectat sau printr-o descărcare de software nedorit. Odată instalat malware-ul, poate monitoriza activitățile utilizatorilor, poate trimite date confidențiale atacatorului, poate ajuta atacatorul să pătrundă în alte ținte din rețea și chiar poate perturba o întreagă rețea IT. De asemenea, atacatorul poate distruge datele sau închide complet sistemul. Exemple de malware sunt troienii, spyware-ul, viermii, virușii, ransomware, etc. De exemplu ransomware împiedică accesul la datele victimei și amenință că le șterge sau le publică dacă nu se plătește o răscumpărare. Spyware, malware tip spion, permite obținerea accesului neautorizat la date, inclusiv la informații sensibile, cum ar fi detaliile de plată și credențiale. [2]

ISBN 978-9975-180-05-4, DOI: 10.53486/sstc.v1

Atacurile de inginerie socială au la bază manipularea psihologică a utilizatorilor în scopul efectuării unor acțiuni dezirabile unui atacator sau pentru a divulga informații sensibile. Cele mai răspândite tipuri de astfel de atacuri cibernetice sunt phishing-ul, spear pshishing-ul şi malvertising-ul. Prin phishing atacatorii trimit corespondență frauduloasă care pare să provină din surse legitime, de obicei prin e-mail. Spear phishing-ul vizează în mod special persoane cu influență, cum ar fi administratorii de sistem sau directorii superiori. Malvertising-ul este o publicitate online controlată de hackeri, care conține un cod rău intenționat ce infectează calculatorul utilizatorului atunci când acesta face click sau chiar dacă doar vizualizează anunțul. A fost depistat malvertising în multe publicații online de top. (Yahoo.com, Spotify, London Stock Exchange, MySpace, The New York Times).

Atacuri la software supply chain (atacurile lanțului de aprovizionare) au scopul de a infecta aplicații legitime. Într-un atac al lanțului de aprovizionare, furnizorul de software nu este conștient de faptul că aplicațiile sau actualizările sale sunt infectate. Virusul rulează cu aceeași încredere și privilegii ca aplicația compromisă. [3]

Distributed denial of Service (DDoS). Obiectivul unui astfel de atac este de a copleși resursele unui sistem țintă și de a-l determina să nu mai funcționeze, interzicând accesul utilizatorilor săi. Aceste atacuri pot crea întreruperea rulării serviciului pentru a capta atenția personalului de securitate și a crea confuzie, în timp ce acestea efectuează alte atacuri mai subtile care vizează furtul de date sau cauzarea altor daune. Primul atac cunoscut DDoS a fost efectuat în anul 2000 de un băiat de 15 ani pe nume Michael Calce, care doborât temporar site-uri uriașe precum Yahoo, CNN și eBay. [4]

Atacul omului din mijloc (MitM). Un atac Man-in-the-Middle implică interceptarea comunicării dintre două puncte finale, cum ar fi un utilizator și o aplicație. Atacatorul poate asculta comunicarea, poate fura date sensibile și poate uzurpa identitatea fiecărei părți care participă la comunicare.

Atacurile cu parole, când hacker-ul obține acces la informațiile despre parolele unei persoane. [3] [4]

Cele mai des întâlnite tipuri de atacatori cibernetici sunt:

Atacatori sponsorizaţi de stat care pot perturba comunicațiile, activitățile militare sau alte servicii pe care cetățenii le folosesc zilnic.

Teroriști, ce pot ataca ținte guvernamentale sau militare, dar uneori pot viza şi site-uri web civile pentru a perturba şi provoca daune de durată. Cele mai elocvente exemple provin din spaţiile actuale de conflict, şi anume: din Afganistan, din Orientul Mijlociu, din Africa etc.

Spioni industriali, a căror scop principal este de ordin financiar.

Grupuri criminale organizate folosesc phishing, spam și programe malware pentru a comite furturi de identitate sau vând și altora servicii de hacking. În 1994, un grup de infractori, condus de un tânăr programator din Rusia au spart sistemele electronice ale unei mari bănci din SUA și au început în secret să fure bani. Hackerii au atacat sistemul informatic de gestionare a numerarului și au compromis numele de utilizator și parolele, ceea ce le-a permis să mute banii din conturile clienților băncii în alte bănci din întreaga lume.

Hackeri, persoană care încearcă să obțină, în mod ilegal, controlul unui sistem de securitate, computer sau rețea, cu scopul de a avea acces la informații confidențiale.

Hacktiviști, hackeri care pătrund sau perturbă sistemele din motive politice sau ideologice. Un exemplu este și grupul *Anonymous,* care a desfășurat un șir de atacuri cibernetice asupra mai multor site-uri guvernamentale și mass-media din Rusia precum site-urile Kremlinului, Dumei, Ministerului Apărării, Serviciului Federal de Securitate din Rusia – FSB, site-urile agenţiilor de presă de stat TASS şi RIA Novosti, al cotidianului Kommersant, al ziarului pro-Kremlin Izvestia şi al revistei Forbes Russia.

Insideri, persoane din interiorul companiilor. [2] [3]

ISBN 978-9975-180-05-4, DOI: 10.53486/sstc.v1

Conform raportului ,,Data Breach Investigations Report 2022" jumătate dintre atacurile cibernetice vizează întreprinderile mici și mijlocii, iar cele mai frecvente atacuri cibernetice cu care se confruntă companiile sunt cele prezentate în figura 1.

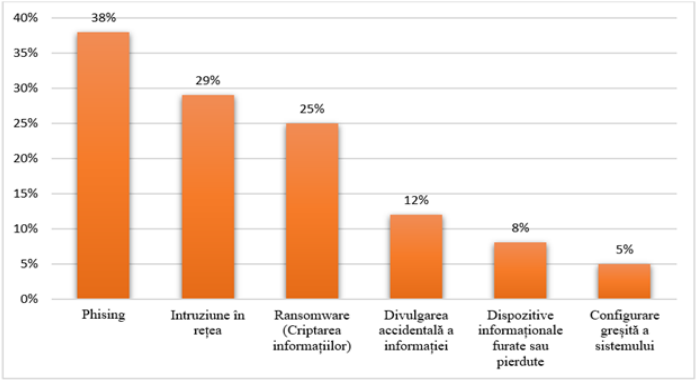

Figura 1. Cele mai răspândite tipuri de atacuri cibernetice 2022

Sursa: *Raportul ,,Data Breach Investigation Report" 2022*

Analizând tabelul de mai sus se observă că cel mai întâlnit tip de atac cibernetic este **"**phishing-ul", răspândit în special prin intermediul mail-urilor.

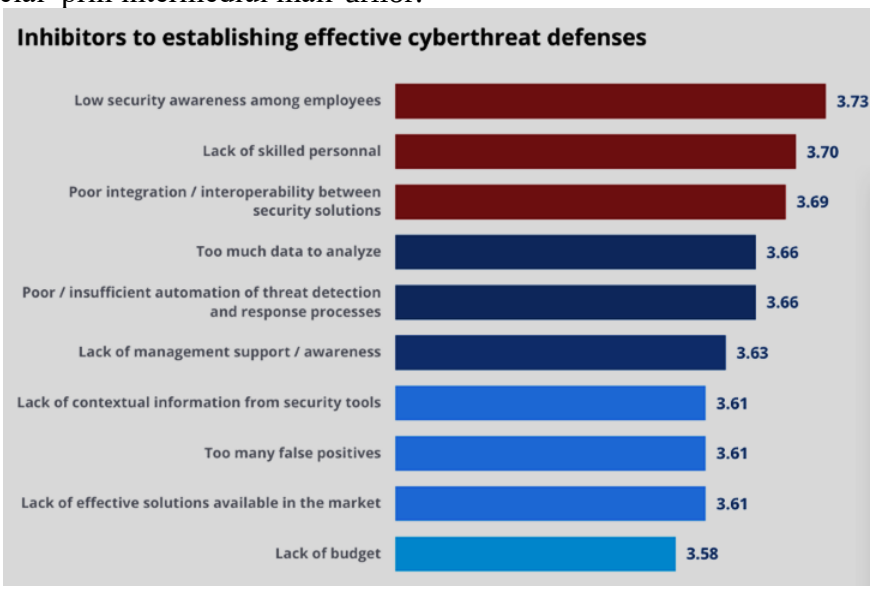

Figura 2. Inhibitori ai stabilirii unei protecții eficiente împotriva amenințărilor cibernetice

Sursa: Cyberthreat Defense Report. Cyber Edge Group

Raportul ,,Cyberthreat Defense Report (CDR) 2021" de la CyberEdge Group a evaluat opiniile a 1.200 de profesioniști în securitatea IT, reprezentând 17 țări și 19 industrii. În urma intervievării, s-au obținut rezultatele din Figura 2, ce arată că principala cauză a lipsei unei protecții eficiente față de atacurile cibernetice este gradul scăzut de conștientizare și informare despre securitatea cibernetică în rândul angajaților.

În Republica Moldova, accesul ilegal la informaţia computerizată se pedepsește conform art. 259 Cod Penal, în dependență de amploarea și nivelul daunei provocate, cu amendă în mărime de la 550 la 1350 unităţi convenţionale sau cu muncă neremunerată în folosul comunității de la 150 la 240 de ore, sau cu închisoare de până la 3 ani, cu amendă, aplicată persoanei juridice, în mărime de la 2000 la 7000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea persoanei juridice. [5]

În calitate de operator al serviciilor electronice guvernamentale în Moldova activează I.P. "Serviciul Tehnologia Informației și Securitate Cibernetică" (STISC). La 25 august 2022, STISC informa că, în ultimele 72 de ore, au fost contracarate mai multe tentative de atacuri cibernetice asupra sistemelor informaționale de importanță statală. Scopul acestor tentative de atac cibernetic a

ISBN 978-9975-180-05-4, DOI: 10.53486/sstc.v1

fost de a cauza indisponibilitatea resurselor informaționale ale statului, având obiectivul de a suprasolicita resursele de procesare ale sistemelor informaționale. Atacurile au fost efectuate din afara Republicii Moldova, de pe adrese IP localizate în diferite țări, de pe echipamente și rețele compromise. [6]

În acest context, STICS a elaborat un Ghid de bune practici privind comportamentul securității informaționale și dezvoltarea culturii sociale în spațiul informațional. Ghidul sintetizează o serie de informaţii cu privire la riscurile existente în spațiul online și prezintă recomandări utile în vederea utilizării în siguranță a sistemelor informatice precum efectuarea de backup-uri periodice și păstrarea lor separate de calculator, instalarea și pornirea software-urilor antivirus, activarea protecției prin parolă, interzicerea personalului să descarce aplicații rău intenționate, etc. Cel mai important este ca atacurile să fie imediat raportate. Acest lucru poate fi făcut la CERT-GOV-MD printr-un mesaj pe poșta electronica: incidents@cert.gov.md sau apelând la numărul de telefon: +373 22 820 921. [7]

CONCLUZII

O serie de sectoare critice precum transporturile, energia, sănătatea și finanțele au devenit tot mai dependente de tehnologiile digitale pentru a-și desfășura activitățile de bază. Digitalizarea oferă oportunități enorme și asigură soluții pentru multe dintre provocările cu care se confruntă diversele companii, dar si oamenii simpli, dar în același timp, expune economia și societatea la amenințări cibernetice.

Atacurile cibernetice și criminalitatea informatică sunt tot mai numeroase și mai sofisticate în întreaga lume, iar această tendință va continua să crească în viitor. Astfel, devine clar că organizațiile ar trebui să își orienteze bugetele IT spre achiziția sistemelor de securitate minim recomandate și necesare. Prevenirea este mai bună decât rezolvarea unei probleme deja existente. Din moment ce atacul a fost produs și este în curs, revenirea la normal poate fi costisitoare deoarece timpul de reglare al sistemului infectat poate afecta atât activitatea afacerii la nivelul tuturor funcțiilor ei de management, cât și a reputației.

BIBLIOGRAFIE:

1. Microsoft. *Ce este securitatea cibernetică?* [online]. [accesat 20 Martie 2023]. Disponibil: https://support.microsoft.com/ro-ro/topic/ce-este-securitatea-cibernetic%C4%83-8b6efd59-41ff-4743-87c8-0850a352a390
2. Microsoft. *Ce este un atac cibernetic?* [online]. [accesat 20 Martie 2023]. Disponibil: https://www.microsoft.com/ro-ro/security/business/security-101/what-is-a-cyberattack
3. Compania Xontech Systems. *Ce tipuri de amenințări cibernetice există și cum să evaluați care sunt șansele să deveniți victima unui atac cibernetic?* [online]. [accesat 20 Martie 2023]. Disponibil: https://xontech.md/news/ce-tipuri-de-amenintari-cibernetice-exista-si-cum-sa-evaluati-care-sunt-sansele-sa-deveniti-victima-unui-atac-cibernetic/
4. Evan, Porter. *Ce este un atac DDos și cum să previi unul în 2023* [online]. [accesat 21 Martie 2023]. Disponibil: https://ro.safetydetectives.com/blog/ce-este-un-atac-ddos/#:~:text=Primul%20atac%20cunoscut%20DDoS%20a,din%20imaginea%20afi%C8%99at%C4%83%20mai%20sus.
5. Articolul 259 Cod Penal RM. Accesul ilegal la informația computerizată [online]. [accesat 23 Martie 2023]. Disponibil: https://www.legis.md/cautare/getResults?doc_id=135678&lang=ro#
6. Serviciul Tehnologia Informației și Securitate Cibernetică. [accesat 23 Martie 2023]. Disponibil: https://stisc.gov.md/ro
7. I.P. Serviciul Tehnologia Informației și Securitate Cibernetică. *Securitatea cibernetică. Ghid de bune practici* [online]. [accesat 25 Martie 2023]. Disponibil: https://stisc.gov.md/sites/default/files/ghid_securitatea_cibernetica_modificat.pdf

Coordonator ştiinţific: CĂLUGĂREANU Irina,conf. univ., dr.
Academia de Studii Economice din Moldova
R. Moldova, Mun. Chișinău, str. Mitropolit Gavriil Bănulescu-Bodoni 61
e-mail: calugareanu.irina@ase.md