BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Hafnium și dilema vulnerabilităților 0-day. Cooperarea public-privat în Cyber Threat Intelligence

Hafnium and the zero-day dilemma. Public-private cyber threat intelligence cooperation

Mihai OLTEANU*
*Student doctorand Școala Doctorală, Universitatea Națională de Apărare „Carol I", București, România
e-mail: mihaiolteanu48@yahoo.com

Abstract

Cyber Threat Intelligence (CTI) reprezintă o componentă esențială în reducerea riscurilor de securitate cibernetică, cu un focus particular asupra identificării și limitării vulnerabilităților de tip 0-day. În timp ce literatura academică, rapoartele de specialitate și documentele normative indică un sprijin larg pentru cooperarea dintre entitățile publice și private pentru dezvoltarea securității cibernetice, există câteva provocări sistemice care afectează schimbul de informații în timp real referitor la amenințări, precum cele generate de vulnerabilitățile de tip 0-day. Acest articol evaluează dinamicile colaborării public-privat în CTI, cu un focus asupra obstacolelor care previn dezvoltarea ulterioară a nivelului de cooperare, precum deficiențele de încredere, limitele legale, riscurile financiare și reputaționale și interesele strategice divergente. Printr-o analiză calitativă a literaturii existente și prin folosirea campaniei cibernetice Hafnium drept studiu de caz, articolul evidențiază dificultatea divulgării vulnerabilităților de tip 0-day și limitele formatelor de cooperare existente. Rezultatele indică faptul că, deși există mecanisme structurate de schimb de informații, colaborarea în timp real împotriva vulnerabilităților 0-day rămâne constrânsă de motivații competitive, a căror rezolvare este dificilă.

Cyber threat intelligence (CTI) plays a crucial role in limiting cybersecurity risks, with a particular focus on identifying and mitigating zero-day vulnerabilities. While academic literature, specialized reports, and normative documents widely argue in favor of cooperation between public and private entities to develop cybersecurity, significant systemic challenges hinder effective intelligence sharing when discussing real-time threats, such as zero-day vulnerabilities.
This article critically examines the dynamics of public-private collaboration in CTI, focusing on the obstacles preventing further development of the level of cooperation, such as trust deficits, legal constraints, financial and reputational risks, and diverging strategic interests. By performing a qualitative analysis on the existing literature and using the Hafnium cyberattack as a case study, the research highlights the complexities surrounding the zero-day vulnerability disclosures and the limitations of existing cooperative frameworks. The findings indicate that while structured CTI-sharing mechanisms exist, real-time collaboration on zero-day vulnerabilities remains constrained by competing incentives that are unlikely to be properly addressed.

Cuvinte-cheie:
Cyber Threat Intelligence; Hafnium; vulnerabilități 0-day; cooperare public-privat.

Keywords:
Cyber Threat Intelligence; Hafnium; Zero-day Vulnerabilities; Public-private Cooperation.

Info articol
Primit: 23 iunie 2025; Evaluat: 29 iulie 2025; Acceptat: 26 august 2025; Disponibil online: 6 octombrie 2025
Citare: Olteanu, M. 2025. „Hafnium și dilema vulnerabilităților 0-day. Cooperarea public-privat în Cyber Threat Intelligence."
Buletinul Universității Naționale de Apărare „Carol I", 14(3): 75-93. https://doi.org/10.53477/2065-8281-25-22

1. Introducere

Multiple rapoarte și studii de cyber threat intelligence evidențiază în mod constant creșterea numărului de atacuri cibernetice care excelează atât prin diversitate, cât și prin complexitate tehnică, necesitând măsuri de securitate extinse și forțând autoritățile să dezvolte cooperarea la orice nivel, fie stat-privat, internațional, național, interinstituțional sau în domeniul cercetării. Există o opinie comună, promovată atât în mediul academic, cât și în cel profesional, care afirmă că amenințările cibernetice în continuă evoluție necesită măsuri adaptive și mai multă cooperare, de orice fel. Această perspectivă există de mulți ani. Un studiu, publicat în 2007, susținea necesitatea dezvoltării cooperării internaționale dintre țări și agențiile de aplicare a legii pentru combaterea și investigarea criminalității cibernetice (Cerezo, Lopez și Patel 2007). În 2002, în urmă cu mai mult de două decenii, Lewis a argumentat nevoia unui nou cadru normativ care să implice cooperarea internațională în securitate cibernetică, având în vedere creșterea continuă a interdependenței dintre diferite sisteme (Lewis 2002). Încă din 1995, au existat autori care anticipau că dezvoltarea domeniului cibernetic va determina noi modalități de colaborare între oameni (Rheingold 1994). În prezent, cooperarea în domeniul securității cibernetice este inerentă oricărui document strategic sau programatic, fiind create și operaționalizate un număr semnificativ de formate, cum ar fi NATO Cooperative Cyber Defence Centre of Excellence, un centru axat pe cercetare și formare (Smeets 2022), sau Malware Information Sharing Platform (MISP), o platformă dedicată schimbului de rapoarte de CTI dintre mai multe categorii de actori (Wang și alții 2024).

Prin urmare, acest accent pe cooperare nu este doar teoretic, având în vedere faptul că ultimele două decenii au urmărit să crească cooperarea dintre sectoare, națiuni și actori prin diverse inițiative cu niveluri de angajament variate. Cu toate acestea, rezultatele acestor eforturi — încununate sau nu de succes — necesită o analiză suplimentară. De asemenea, nu este clar dacă mecanismele de cooperare pot beneficia de o dezvoltare suplimentară.

În prezent, impulsul continuu de a îmbunătăți mecanismele de cooperare conexe domeniului cibernetic evidențiază un punct critic: principalii actori din sfera cibernetică (în special statele și firmele) nu au reușit să găsească o abordare satisfăcătoare în această privință. Pot exista multiple motive, precum interese diferite sau constrângeri, generate de obstacole legale și de reglementare (GDPR) și preocupări legate de proprietatea intelectuală (Bechara și Schuch 2020, 353-374). Întregul proces de partajare a informațiilor conexe CTI capătă o urgență sporită atunci când este restrâns la schimbul de date legate de vulnerabilități 0-day (vulnerabilități software sau hardware care sunt exploatate înainte ca dezvoltatorii să le fi identificat și, implicit, să fi lansat un patch) (Singh, Joshi și Kanellopoulos 2019, 164-172). Impactul exploatării acestui tip de vulnerabilități este semnificativ atât din punct de vedere tehnic, cât și economic, reducând foarte mult încrederea dintre părți, având în vedere că pot fi afectate interese fundamentale, precum reputația companiei și securitatea statelor.

Acest articol analizează provocările fundamentale legate de cooperarea public-privat în partajarea informațiilor privind amenințările cibernetice, cu accent pe stimulentele structurale care determină ambele părți — de ce aleg să partajeze sau să rețină datele. Analiza va aborda în mod specific vulnerabilitățile de tip 0-day, explorând modul în care amenințări unice influențează abordarea schimbului de informații și strategiile de reducere a riscurilor pe care le implică.

2. Metodologie

Obiectivul principal al acestei cercetări este de a identifica obstacolele în partajarea informațiilor conexe CTI într-un context public-privat și de a examina modul în care aceste bariere afectează cooperarea în privința vulnerabilităților de tip 0-day. Pentru a aborda această temă, cercetarea adoptă un studiu calitativ, analizând literatura existentă dintr-o perspectivă tehnică. În plus, va fi prezentat un studiu de caz privind campania cibernetică Hafnium, bazată pe exploatarea vulnerabilităților de tip 0-day. Acest studiu de caz (1) ilustrează necesitatea analizării succesului sau eșecului mecanismelor reale de cooperare și (2) oferă perspective critice asupra provocărilor strategiilor de îmbunătățire a cooperării în domeniul vulnerabilităților de tip 0-day.

3. Cyber Threat Intelligence și vulnerabilitățile de tip 0-day

CTI este o componentă a conceptului mai larg de intelligence, având caracteristici și obiective finale similare (Sülü și Daş 2022). CTI a fost definit ca un domeniu de activitate în care datele sunt colectate, comparate, analizate și, în final, diseminate, având ca scop o mai bună înțelegere a amenințărilor, precum și a actorilor care intenționează să producă daune diferitelor componente ale ecosistemului cibernetic (Sun și alții 2023, 1748-1774). De asemenea, este considerat a fi un proces care permite organizațiilor sau statelor să obțină o înțelegere aprofundată a propriilor vulnerabilități (Shackleford 2015).

Întregul proces de CTI permite organizațiilor să planifice și să acționeze proactiv în vederea înțelegerii riscurilor și amenințărilor, precum și să profite de oportunitățile conexe spațiului cibernetic. Prin urmare, *raison d'être* al CTI este de a sprijini adoptarea unor decizii de către părțile abilitate de la diferite niveluri, de la comandanții unităților de operațiuni cibernetice până la liderii statelor și directorii executivi ai organizațiilor private (Lanzendorfer 2015). În acest sens, CTI exploatează o varietate de date technice (de exemplu, adrese IP, date de geolocalizare, analiza de trafic etc.) pentru a înțelege tipul de atac care a avut loc, măsurile de remediere necesare, capacitățile actorului cibernetic și vulnerabilitățile existente (Barnum 2014). CTI este o activitate desfășurată în scopul de a preveni amenințările prin anticiparea intențiilor atacatorului și a principalelor sale obiective, precum și a tehnicilor folosite în îndeplinirea acestora pe termen lung. În acest sens, o componentă vitală a CTI constă în identificarea vulnerabilităților existente, înainte ca atacatorul să o facă, pentru a preveni exploatarea acestora (Schlette, Böhm și alții 2021, 21-38).

În context, o categorie aparte de amenințări de nivel critic, care pot genera riscuri crescute, este cea reprezentată de vulnerabilitățile de tip 0-day, necunoscute producătorului și, implicit, exploatate silențios de către actori cibernetici până în punctul în care sunt publicate actualizări de securitate (Roumani 2021). Principala provocare conexă vulnerabilităților de tip 0-day este aceea că, prin definiție, acestea sunt cunoscute doar de către expertul care le-a identificat inițial, ceea ce înseamnă că mecanismele tradiționale de apărare – precum cele bazate pe detecția semnăturilor – tind să fie ineficiente (Ahmad și alții 2023).

Astfel, caracterul proactiv al activității de tip CTI prezintă importanță deosebită în ceea ce privește vulnerabilitățile de tip 0-day. Identificarea și mitigarea acestor vulnerabilități necesită o înțelegere profundă atât a spectrului amenințărilor, cât și a comportamentului actorilor cibernetici. Cu toate acestea, complexitatea și lipsa de cunoaștere introduc provocări semnificative pentru CTI (Albanese și alții 2013). Spre deosebire de alte amenințări, vulnerabilitățile de tip 0-day necesită deseori un răspuns imediat și coordonat deopotrivă din partea organizațiilor publice și private, ceea ce face identificarea timpurie și comunicarea lor esențiale în vederea limitării pagubelor.

Luând în calcul valoarea deosebit de ridicată a acestora din punct de vedere atât ofensiv, cât și defensiv, vulnerabilitățile de tip 0-day au devenit o resursă financiară pentru cercetătorii care decid să își dedice eforturile identificării și comercializării acestora pe piața albă, gri sau neagră. Valoarea financiară a unei vulnerabilități de tip 0-day este datorată unor factori multipli, cel mai important dintre aceștia fiind, evident, gradul de secretizare. Spre exemplu, conform unui studiu (Meakins 2018, 60-71), cercetătorii pot câștiga până la 3 milioane de dolari, dacă decid să vândă o vulnerabilitate de tip 0-day pe piața gri celor ce intenționează să le exploateze în interes propriu. Pe parcursul ultimelor două decenii, multiple vulnerabilități de tip 0-day au fost exploatate, parte dintre ele producând pagube semnificative, precum Shellshock (care afecta sisteme Unix și Linux), Heartbleed (care afecta serviciile de Internet) și F5 BIG-Ip (cereri HTTP care permiteau executarea de cod) (Teodorescu 2022). Un raport, publicat de Google și Mandiant, a evidențiat faptul că, pe parcursul anului 2023, au fost identificate 97 de vulnerabilități 0-day, dintre care 36 vizau tehnologii de tip enterprise (Google; Mandiant 2024).

4. Cooperarea în domeniul Cyber Threat Intelligence

Așa după cum a fost precizat în partea introductivă, natura activității CTI (în particular, în relație cu vulnerabilitățile 0-day) reclamă constant nevoia de a crea formate cooperative și de a continua dezvoltarea celor existente, astfel încât amenințările cibernetice să fie prevenite și limitate.
Natural, numeroase lucrări academice au susținut nevoia de cooperare prin evidențierea unor beneficii cantitative și calitative care pot fi obținute prin astfel de abordări (Pala și Zhuang 2019, 172-196). În ceea ce privește vulnerabilitățile 0-day, provocările ar putea fi chiar mai accentuate. Considerând că aceste vulnerabilități

sunt necunoscute deopotrivă pentru comercianți și pentru personalul responsabil cu securitatea cibernetică până ce nu sunt exploatate, este foarte puțin probabil ca o singură organizație să dețină toate informațiile necesare pentru a răspunde adecvat amenințării (Homburger 2019, 224-242). În absența unor formate de cooperare public-privat, potențialul de a răspunde și de a neutraliza amenințarea este foarte probabil să fie compromis.

Cel mai accesibil mecanism de cooperare este reprezentat de schimbul reciproc de rapoarte de CTI, ceea ce implică în mod direct distribuirea de informații. Astfel, schimbul de date tehnice, precum indicatori de compromitere, vectori de atac sau tactici utilizate de actori cibernetici, a fost recunoscut drept un mecanism pertinent de dezvoltare a cunoașterii colective, conexe spectrului amenințărilor cibernetice, aspect ce permite o identificare mai rapidă a incidentelor și implementarea unor măsuri proporționale (Wagner și alții 2019). Similar, în cazul vulnerabilităților 0-day, distribuirea unor rapoarte CTI este probabil să sprijine eforturile partenerilor de identificare și remediere a acestora.

Dezvoltarea unor capabilități de detecție este un rezultat direct al cooperării active dintre diverși actori, considerând că asemenea abordări permit mai multor organizații să creeze un sistem de monitorizare comprehensiv, pe baza unei cunoașteri comune, decurse din exploatarea resurselor și a expertizei existente. În timp ce guvernele pot dezvolta capabilități avansate pentru înțelegerea atacurilor cibernetice de origine statală, companiile private dețin mult mai multe date în timp real cu privire la activitatea diferitelor categorii de actori cibernetici (Purohit și alții 2023, 4273-4290). Astfel, combinarea acestor două abordări în formate cooperative este probabil să ofere sprijinul necesar îmbunătățirii prevenției și detecției atacurilor cibernetice. Această abordare este mai importantă în cazul vulnerabilităților 0-day, având în vedere că ambele categorii de entități dețin capabilități de identificare a acestora prin programe de tip *bug bounty*, susținute de proprii experți (Arshad și alții 2024, 195-216).

Mecanismele eficiente de schimb de date pot dezvolta relația dintre state și companii private, permițându-le să dezvolte încrederea și, posibil, formate de cooperare care necesită utilizarea comună a resurselor, context în care expertiza fiecărui actor ar putea fi folosită de partenerul său. Cel puțin din perspectivă defensivă, o astfel de abordare este complet dezirabilă, având în vedere că ambele părți urmăresc identificarea unor mecanisme potrivite pentru creșterea protecției propriilor rețele (Rajamäki 2017). Acest raționament este, de asemenea, complet valid în cazul vulnerabilităților 0-day, considerând că programele public-private de tip bug-bounty sunt predispuse să se dovedească a fi mai eficiente și rapide în identificarea vulnerabilităților hardware și software.

Mai mult, multiple formate de cooperare public-privat, cu diverse specificități și compuse din actori diferiți, au fost înființate cu două obiective, cel de implementare a unor măsuri de securitate și cel de încurajare a eforturilor de utilizare comună

a resurselor. Fiecare dintre aceste formate de colaborare furnizează valoare adăugată în gestionarea actorilor cibernetici și a vulnerabilităților cibernetice, dar este necunoscut dacă nivelul maxim de cooperare a fost atins. Luând în calcul că literatura academică susține dezvoltarea unor formate de cooperare, este probabil ca viziunea să fie aceea că există posibilitatea extinderii cooperării, cel puțin conform entităților care argumentează în favoarea unor acțiuni de acest tip.
Până în prezent, printre cele mai des întâlnite formate de schimb de date CTI sunt Information Sharing and Analysis Centers (ISAC), care au fost dezvoltate într-o varietate de industrii și care încurajează schimbul de date cu privire la amenințările cibernetice, Computer Security Incident Response Teams (CSIRT), precum și diferite structuri organizaționale și platforme de cooperare online (Wallis și Leszczyna 2022).

ISAC este un format creat pentru a facilita schimbul de informații cu privire la amenințări și actori cibernetici, în principal prin comunicarea voluntară dintre diverse entități. În mod natural, un ISAC nu necesită schimbul de date tehnice în timp real, precum loguri de trafic sau malware. Totuși, scopul acestui format este creșterea conștientizării dintre membrii privind amenințările cibernetice. Astfel, formatele ISAC sunt mai degrabă comune organizațiilor care nu au dezvoltat încă un nivel ridicat de încredere și care nu sunt pregătite să schimbe date cu importanță critică (Steffensen și Gnanasekaran 2024).

Un format de cooperare mai dezvoltat este CSIRT, mecanism care folosește o varietate de resurse pentru prevenirea, identificarea, investigarea și limitarea mai multor tipuri de amenințări cibernetice. Entitățile membre ale unui CSIRT, fie publice sau private, conștientizează necesitatea schimbului de resurse pentru prevenirea pagubelor asupra propriilor rețele, produse de atacurile cibernetice (Bada și alții 2014). În prezent, CSIRT reprezintă cel mai comun format de schimb de resurse, susținut de multiple entități și în mod special de Uniunea Europeană, prin mecanisme legislative, precum Directiva (UE) 2022/2555 (Directiva NIS2), care evidențiază necesitatea creării unor CSIRT-uri sectoriale, coordonate de o autoritate desemnată (nu neapărat entitate publică), cu resurse suficiente încât să fie capabilă să prevină amenințări cibernetice specifice (Parlamentul European; Consiliul Uniunii Europene 2022).

Alte agenții, precum European Union Agency for Cybersecurity (ENISA), au fost înființate pentru a oferi sprijin în gestionarea amenințărilor cibernetice și în prevenirea atacurilor cibernetice (Sklyar și Kharchenko 2019). Deși ENISA a fost obiectul mai multor schimbări pe parcursul timpului (atât ca structură, cât și ca obiective), și în prezent nu are responsabilități tehnice, reușește să coopereze cu entități publice și private pentru a crea rapoarte care evidențiază bune practici și recomandări conexe securității cibernetice (Cavelty și Smeets 2023, 1330-1352). ENISA reprezintă un reper aparte în ceea ce privește cooperarea public-privat, considerând că este o inițiativă internațională publică. În domeniul privat, au fost înființate numeroase platforme, printre care se remarcă MISP drept una dintre cele

mai populare. MISP permite membrilor și voluntarilor să schimbe constant date tehnice referitoare la amenințările cibernetice, precum indicatori de compromitere, vulnerabilități și măsuri de contracarare (Wagner și alții 2016).

Cu toate că aceste formate asigură mecanisme variate de schimb de informații CTI și o paletă largă de opțiuni pentru o entitate care este predispusă să coopereze în mitigarea și prevenirea atacurilor cibernetice identificate, literatura existentă subliniază că, în continuare, există impedimente în activitatea de cooperare, a căror dispariție este improbabilă. Modul în care acestea afectează șansele dezvoltării cooperării în contracararea multiplelor amenințări (și, în mod particular, a vulnerabilităților 0-day) va fi detaliat în secțiunile următoare. Acestea vizează evidențierea faptului că există o serie de dificultăți sistemice în extinderea oricăror formate de cooperare sau, cel puțin, a celor care au existat și au fost dezvoltate pe parcursul ultimelor decade, iar impactul acestor dificultăți asupra gestionării acestui tip de vulnerabilități este punctul principal al prezentei analize și al studiului în sine.

5. Obstacole sistemice în extinderea formatelor de cooperare

În timp ce dezvoltarea cooperării este, teoretic, previzibilă (cum a fost prezentat în secțiunile anterioare) și dezirabilă deopotrivă pentru actorii publici și privați (cel puțin la un anumit nivel, așa după cum va fi argumentat), iar rolul său defensiv și beneficiile sunt evidente, un format ideal de cooperare nu poate fi realizat în practică. Există numeroase bariere financiare, sociale, reputaționale și legislative, a căror depășire reprezintă o provocare și care vor fi descrise pe larg în această parte a studiului.

Un studiu asupra perspectivei americane cu privire la industria CTI și interacțiunea dintre entități publice și private a adresat un set de întrebări unui grup de oficiali americani, rezultând următoarele concluzii:

- 58,82% dintre participanți au fost de acord că expertiza entităților private din domeniul securității cibernetice o depășește pe cea a guvernului SUA;
- 70,59% au avut încredere că livrarea unor produse eficiente către guvernul american poate fi realizată de contractori privați;
- 58,82% au considerat că industria privată deține mai multe cunoștințe decât guvernul american pe segmentul securității cibernetice (Lanzendorfer 2015).

Cu toate că acest studiu nu prezintă o analiză comprehensivă a interacțiunii dintre organizațiile publice și cele private, el oferă câteva perspective referitoare la percepția entităților publice asupra industriei private. În acest sens, se conturează ipoteza conform căreia schimbul de informații CTI dintre cât mai multe entități ar fi soluția potrivită pentru gestionarea eficientă a atacurilor cibernetice (Fischer și alții 2023). Cu toate acestea, există numeroase contraargumente, observate pe parcursul ultimelor decenii, în privința schimbului de informații CTI dintre diferite tipuri de entități.

5.1. Lipsa de încredere

Unul dintre aspectele cele mai importante care previne schimbul uzual de rapoarte CTI este lipsa de încredere între multiple entități din spectrul activității de cyber intelligence.

În primul rând, nivelul scăzut de încredere privind schimbul de date dintre entitățile publice este determinat de riscurile operaționale asociate transmiterii de informații cu privire la campaniile aflate în derulate. Spre deosebire de alte domenii, precum contraspionajul sau contraterorismul, datele cu privire la CTI sunt cele mai valoroase în timp real, având în vedere faptul că riscul principal rezidă în potențiala expansiune a unei campanii cibernetice la nivelul mai multor entități naționale. Atunci când se produce schimbul de date dintre entitățile publice, una dintre acestea trebuie să își asume riscul că această activitate poate compromite investigații aflate în derulare. Dacă una dintre celelalte autorități începe o investigație pe cont propriu, aceasta poate alerta atacatorul. În susținerea respectivei afirmații, un studiu publicat de CCDCoE evidențiază faptul că există numeroase situații în care chiar și acorduri scrise care reglementează schimbul de informații dintre entitățile publice nu sunt respectate de toate părțile implicate (Tolga 2019). Luând în calcul aceste scenarii, entitățile publice sunt dispuse să împartă datele relevante numai cu un număr extrem de redus de parteneri cu nivel de încredere ridicat sau doar atunci când investigațiile sunt, cel puțin parțial, încheiate, iar schimbul de date nu ar genera riscuri sau amenințări operaționale suplimentare.

În al doilea rând, lipsa de încredere este o problemă în schimbul de date și printre organizațiile private, considerând problemele referitoare la competitivitate și la riscul pierderii clienților. Organizațiile private sunt deseori reticente să participe la schimburi de date cu entități competitoare, parte a aceleiași industrii, chiar și când există posibilitatea să îmbunătățească serviciile oferite propriilor clienți sau să prevină atacuri cibernetice. Astfel, deși schimbul de date ar putea preveni extinderea atacurilor cibernetice asupra mai multor sectoare și state, încrederea pe termen lung este improbabil să ajungă la un nivel suficient. Focusul principal al entităților private va rămâne asupra interesului financiar, care prevalează, în detrimentul eforturilor de colaborare (Hausken 2007, 639-688). Atunci când entitățile private operează în sectoare diferite, acestea sunt mai favorabile schimbului de date în timp real, presupunând că există acorduri semnate în acest sens și un interes financiar comun. Cu toate acestea, o astfel de abordare nu încurajează semnificativ cooperarea în domeniul CTI, având în vedere premisa că cel puțin o entitate privată operează într-un sector distinct de activitate și, implicit, nu va deține date CTI valoroase care să încurajeze un schimb de informații relevant.

În al treilea rând, schimbul de informații CTI dintre entitățile publice și private este dificil din mai multe perspective. Astfel, există nevoia unui nivel de încredere foarte ridicat, considerând că entitatea publică va oferi date sensibile, iar compania privată va transmite investigații, realizate pe baza propriilor cheltuieli. Suplimentar, schimbul de informații valoroase ar putea presupuse ca entitatea publică să ofere date privind proprii cetățeni unei entități private, acțiune care poate fi percepută

drept inacceptabilă de către societate, considerând premisa enunțată anterior, anume că interesul companiei este unul financiar. Mai mult, compania se poate supune unor reglementări care previn transmiterea de date cu privire la proprii clienți unor terțe părți care nu au fost agreate inițial (Sullivan și Burger 2017, 14-29).

5.2. Lipsa de calitate

Un mecanism permanent de schimb de date CTI este dificil de implementat, deoarece nu există nicio garanție cu privire la reciprocitate. Există autori care subliniază faptul că una dintre problemele referitoare la schimbul de date CTI este că în multe situații, acestea nu sunt de actualitate și, implicit, nu pot genera plus-valoare în cadrul investigațiilor aflate în derulare, în special având în vedere că există deja multiple date și rapoarte publice, iar mecanismele de analizare a acestora necesită timp și efort pentru a furniza o interpretare cu grad crescut de acuratețe (Schlette, Böhm și alții 2020, 21-38).

Deopotrivă actorilor publici, cât și celor privați le lipsește siguranța că informațiile furnizate vor conduce către un răspuns care să fie cu adevărat important în dezvoltarea eforturilor investigative, ceea ce face să pară nejustificate, în unele cazuri, eforturile de creștere a încrederii și de depășire a barierelor legislative. Mai mult, un mecanism de standardizare din punctul de vedere al calității este dificil și improbabil să fie implementat între mai multe părți, considerând că fiecare are resurse și mecanisme particularizate pentru desfășurarea investigațiilor. Deși aceste obstacole ar putea fi adresate în format bilateral, crearea unor mecanisme de cooperare multilaterală este improbabil să aibă succes, având în vedere că nu exisă un mod de lucru omogen deja agreat.

5.3. Riscuri reputaționale

Schimbul de date CTI riscă să deterioreze reputația entităților publice și private. Este probabil ca multe dintre organizațiile care s-au confruntat cu atacuri cibernetice majore care au generat pagube substanțiale infrastructurilor acestora să evite publicarea propriilor investigații, considerând că există o serie de riscuri: (1) clienții ar putea considera că a existat o lipsă de măsuri de securitate cibernetică, ce a permis ca datele lor să fie puse în pericol, și ar putea decide să încheie colaborarea cu entitatea privată în cauză (Perera și alții 2022); (2) organizațiile private s-ar putea confrunta cu dezavantaje competitive, dacă aceste informații ar deveni publice, considerând că rivalii economici vor încerca să demonstreze că dețin măsuri de securitate cibernetică mai avansate, care nu ar fi permis un astfel de rezultat (Lanzendorfer 2015); (3) atât entitățile publice, cât și cele private pot risca să fie țintite în viitor de actori cibernetici, având în vedere că au admis faptul că le lipsesc măsurile adecvate de securitate cibernetică (Kamiya și alții 2018). Din perspectiva entităților publice, pot exista provocări similare, dublate de faptul că un astfel de incident poate alimenta panica socială și poate eroda capacitatea de a proteja infrastructurile critice naționale.

Aceste riscuri, deși nu sunt inerente formatelor de colaborare, evidențiază o serie de motive pentru care schimbul de date în timp real, pe durata atacurilor cibernetice,

este evitat. Schimbul de informații post-factum rămâne o variantă mai sigură, deși valoarea și consistența acestora pot fi în continuare influențate din aceleași considerente. Balanța dintre transparență și riscuri reputaționale reprezintă o provocare constantă în domeniul securității cibernetice.

5.4. Lipsa standardizării

Entitățile publice și private tind să evite schimbul de informații CTI, deoarece nu există un cadru standardizat pentru realizarea rapoartelor CTI, ceea ce face dificilă utilizarea acestora în timp real, pe parcursul unui atac cibernetic. Diferiți autori argumentează faptul că lipsa de standardizare în industria CTI face procesul de schimb de date foarte ineficient (Silva și alții 2020), existând totuși propuneri de formate în acest sens (Tounsi și Rais 2017, 212-233), care însă nu au fost adoptate de suficiente entități din industrie astfel încât să fie relevante.

Întreaga problemă referitoare la lipsa de standardizare confirmă faptul că eforturile de schimb de date CTI între diferite organizații publice și private, precum și riscurile care derivă în urma acestora nu merită să fie făcute, dacă nu există o garanție că rezultatele vor fi utile în susținerea investigațiilor cibernetice și în protejarea rețelelor (Serrano, Dandurand și Brown 2014). Astfel, considerând că nu există garanția unor câștiguri pentru părțile implicate referitoare la gestionarea unor crize cibernetice sau la limitarea pagubelor, este dificilă încurajarea schimbului de date critic cu nivel ridicat de sensibilitate și cu valoare crescută.

5.5. Probleme de natură legislativă

Întregul proces de schimb de date CTI este dificil, considerând o serie de măsuri legislative care previn acest tip de activitate, în special în cazul organizațiilor private care ar transmite date tehnice ale propriilor clienți. Regulamentul General privind Protecția Datelor (GDPR) normează activitățile în cadrul UE și evidențiază o serie de limitări și condiții specifice pentru schimbul de date ale cetățenilor, parte dintre acestea incluzând indicatori relevanți pentru CTI, precum adresele IP ale utilizatorilor (Albakri, Boiten și Lemos 2018). GDPR definește datele personale drept *„orice informații privind o persoană fizică identificată sau identificabilă («persoana vizată»); o persoană fizică identificabilă este o persoană care poate fi identificată direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare,* ***un identificator online****, sau la unul ori la mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale*" (Comisia Europeană 2016). Deși GDPR a fost adoptat pentru siguranța datelor personale ale cetățenilor, reglementările limitează în mod clar posibilitatea schimbului de date cu terțe părți a unor informații care pot fi considerate date personale, reducând astfel posibilitatea schimbului de date CTI.

O analiză extinsă a impactului GDPR asupra schimbului de date CTI a fost realizată de către Albakri, Boiten și Lemos, care au concluzionat că acest schimb de date personale, conexe unui atac cibernetic poate fi efectuat doar cu anumite autorități publice și doar prin anumite mecanisme de criptare (Albakri, Boiten și Lemos 2019).

5.6. Existența unor interese divergente

Considerând că deopotrivă entitățile publice și private acționează în susținerea propriilor obiective, acestea fiind descrise absolut diferit, cooperarea în timp real în CTI este afectată; există o serie de limitări care îngreunează orice format cooperativ. În mod normal, companiile private prioritizează propriile profituri, sens în care decid să sprijine inițiative care promit încasări, cel puțin proporționale cu investițiile inițiale. Deseori, obiectivul acestora este de a se ocupa de amenințări de nivel ridicat, care pot genera pierderi financiare semnificative sau care pot afecta reputația victimelor, precum atacuri cibernetice distructive, spionaj sau campanii majore cu motivație financiară (Maschmeyer, Deibert și Lindsay 2020, 1-20). Această focalizare poate duce la o reticență în partajarea informațiilor CTI cu entitățile publice, întrucât informațiile legate de *„peștii mari"* sunt extrem de valoroase.

Spre deosebire de acestea, guvernele aleg să acorde importanță oricărei investigații care poate aduce valoare adăugată concretă în societate, prin protejarea majorității populației, precum și a organizațiilor și firmelor de orice dimensiune. De exemplu, un „pește mic", cum ar fi o campanie de phishing, poate părea neatractivă pentru actorii privați, dar esențială pentru autoritățile statului, întrucât ar putea afecta o mare parte a populației. În acest sens, guvernele sunt dispuse să finanțeze investigații care nu par a fi profitabile din punct de vedere financiar (Tropina 2015).

Această discrepanță de interese – motivațiile orientate spre profit, în contrast cu obiectivele de securitate națională – constituie o barieră importantă în cooperarea eficientă în domeniul schimbului de informații CTI. Schimbul semnificativ de date este puțin probabil în situațiile în care cele două părți abordează problema din perspective diferite și dispun de seturi distincte de măsuri. Desigur, în cazul unei campanii care prezintă interes comun, este mai probabil să asistăm la o cooperare productivă, însă astfel de situații sunt mai degrabă izolate, având în vedere perspectiva prezentată anterior.

6. Evaluarea provocărilor legate de dezvăluirea și partajarea vulnerabilităților 0-day

Deși discuția privind partajarea informațiilor CTI pare relativ clară, întrucât există un set bine definit de beneficii, dar și riscuri sau dezavantaje semnificative, asociate cooperării public-privat, acest lucru nu se aplică în mod similar în cazul schimbului de date privind vulnerabilitățile 0-day, care sunt percepute diferit, având în vedere valoarea și raritatea lor.

Avantajele partajării informațiilor CTI și îmbunătățirii cooperării, prezentate în Secțiunea 4, nu reflectă pe deplin abordarea în ceea ce privește vulnerabilitățile 0-day. Majoritatea beneficiilor cooperării se bazează pe schimbul de informații post-factum sau pe formate de colaborare preventive, în raport cu atacurile cibernetice. Prin urmare, dintr-o perspectivă defensivă, cooperarea pare o rețetă adecvată. Totuși, în cazul schimburilor de date privind vulnerabilitățile 0-day între sectorul

public și cel privat, apar două probleme majore: (1) din perspectiva entității publice, de ce ar trebui autoritățile să ofere gratuit date referitoare la o vulnerabilitate atât de valoroasă cum este cea de tipul 0-day unei entități private, sacrificând caracterul său secret și, implicit, interesul propriu? (Bilge și Dumitraş 2012); (2) din perspectiva companiei, de ce ar trebui aceasta să partajeze o vulnerabilitate 0-day și să riște ca aceasta să fie exploatată, în loc să fie remediată? Întreaga dezbatere pare a se încadra într-un joc cu sumă zero, în care niciunul dintre actori nu are motive clare să creadă că ambele părți vor avea de câștigat. Lista avantajelor, invocată de diverse entități, pentru a promova partajarea CTI nu este valabilă în cazul unei vulnerabilități unice, cel mai probabil necunoscute de ceilalți actori și care ar putea oferi avantaje strategice semnificative. Niciun nivel de încredere nu poate compensa riscul de a partaja un asemenea activ important cu un actor care, așa după cum s-a explicat anterior, are obiective și perspective diferite.

Mai mult, din perspectiva entității private, apare o altă întrebare esențială: cui ar trebui să i se partajeze date referitoare la vulnerabilitatea 0-day? Deși discuția privind cooperarea public-privat pare să implice doar doi actori, în realitate, numărul acestora este semnificativ mai mare. Marile companii își desfășoară operațiunile de securitate cibernetică și își comercializează produsele într-un număr mare de state, ceea ce înseamnă că o inițiativă de cooperare echitabilă ar presupune ca acestea să-și informeze toți partenerii (respectiv, toate statele în care activează) că au identificat o astfel de vulnerabilitate 0-day și să aștepte ca aceștia să acționeze responsabil. Această abordare depășește orice interes financiar sau strategie de afaceri, întrucât valoarea activului ar scădea considerabil, existând, totodată, riscul ca vulnerabilitatea să fie exploatată (Roumani 2021).
În plus, daunele de imagine pentru companie rămân o realitate, având în vedere că partajarea unei vulnerabilități atât de importante dintr-un produs hardware sau software, cu riscul ca aceasta să devină publică, poate afecta semnificativ încrederea clienților și, pe termen lung, interesele financiare ale companiei (Ekong și alții 2023, 123-140).

O altă problemă care decurge din argumentul expus în Secțiunea 5.2 este cea a calității și reciprocității. Este dificil (dacă nu chiar imposibil) să se construiască mecanisme de încredere care să funcționeze astfel încât atât autoritatea publică, cât și actorul privat să aibă încrederea că o situație similară va produce un rezultat echivalent și, în consecință, să decidă să partajeze date privind o vulnerabilitate 0-day recent descoperită (Schulze și Reinhold 2018).
Mai mult progres ar putea fi înregistrat din partea autorităților publice, în special a statelor membre ale unor organizații comune. UE încearcă să încurajeze eforturile către programe de Divulgare Comună a Vulnerabilităților, acestea fiind incluse în Directiva NIS2, care reglementează anumite mecanisme pentru protejarea cercetătorilor care identifică vulnerabilitățile și care încurajează statele membre să-și partajeze investigațiile în cadrul UE, ulterior cu entitățile private și, în final, public, atunci când a fost dezvoltat un patch (Parlamentul European; Consiliul Uniunii Europene 2022). Totuși, este puțin probabil ca o abordare similară să fie adoptată

de companiile private, care sunt predispuse să mențină statu-quoul, constând în identificarea vulnerabilităților 0-day și partajarea acestora (cu partenerii sau public) doar după ce o actualizare de securitate adecvată a fost creată și testată.

7. Hafnium: Studiu de caz privind exploatarea vulnerabilităților 0-day

Campania cibernetică Hafnium, identificată pentru prima dată la începutul anului 2021, reprezintă una dintre cele mai semnificative și răspândite breșe de securitate din istoria recentă, bazată pe vulnerabilități de tip 0-day. Campania a fost atribuită public unui grup de tip Advancer Persistent Threat, cu sediul în China (NATO 2021) și a constat în exploatarea unor vulnerabilități de la nivelul serverelor Microsoft Exchange, reușind să producă un impact semnificativ la nivel global. Atacatorii au obținut cu succes acces neautorizat la sisteme și servere de e-mail, au sustras date sensibile și au implementat programe malware avansate care puteau fi exploatate pe o perioadă îndelungată (Waheed și alții 2024).

Campania s-a bazat pe exploatarea complementară a patru vulnerabilități de tip 0-day, descoperite de hackeri chinezi și utilizate timp de mai multe luni la rând. Vulnerabilitățile 0-day le-au permis atacatorilor:

- să se autentifice la serverele Microsoft Exchange, ceea ce le-a dat posibilitatea să exfiltreze conținutul mailurilor prin CVE-2021-26855 (Server-Side Request Forgery);
- să obțină acces la funcționalitățile de voice mail, dacă au obținut anterior drepturi de administrator, prin CVE-2021-26858 (Insecure Deserialization);
- să scrie fișiere (potențial malware) în cadrul serverelor compromise prin CVE-2021-26858 și CVE-2021-27065 (Arbitrary File Write) (Narang 2021).

Există diferite estimări privind pagubele globale produse, însă mai multe surse publice susțin că atacul cibernetic Hafnium a reușit să compromită între 10.000 și 250.000 de clienți Microsoft, inclusiv companii și agenții guvernamentale. Mai mult, Microsoft a suferit un prejudiciu sever de imagine, în urma acestui atac cibernetic bazat pe vulnerabilități 0-day, iar relațiile dintre Statele Unite și China au fost, de asemenea, considerate ca fiind afectate (Bates 2022, 17-30).

La data de 2 martie 2021, Microsoft a publicat o știre, intitulată ”New nation-state cyberattacks”, în care a descris gruparea cibernetică denumită Hafnium, precum și faptul că aceasta a exploatat unele „vulnerabilități anterior nedescoperite” din produsele comercializate de compania americană. De asemenea, a menționat că a informat guvernul Statelor Unite ale Americii în legătură cu incidentul și că a fost sprijinită de alte companii în remedierea acestor vulnerabilități (Burt 2021). Acesta a fost primul moment în care Microsoft a recunoscut existența vulnerabilităților de tip 0-day și exploatarea lor. În aceeași zi, compania a lansat public o serie de actualizări de securitate pentru a remedia aceste vulnerabilități, care au fost ulterior adaptate constant pentru a preveni daune suplimentare (Microsoft 365 Security 2021).

Diferite surse publice subliniază faptul că Microsoft a fost avertizată cu privire la vulnerabilități, încă din ianuarie 2021, de cel puțin două ori, de către diverse companii de securitate cibernetică. Inițial, compania Volexity a observat că atacatorii exploatau în mod discret vulnerabilitățile de tip 0-day și a comunicat acest lucru către Microsoft. În februarie, înainte ca Microsoft să recunoască oficial situația, Volexity a observat o exploatare masivă a aceloraşi vulnerabilități (Krebs 2021). În plus, cel puțin încă o entitate privată a informat Microsoft, în ianuarie 2021, despre exploatarea activă a acestor vulnerabilități 0-day (Robinson 2024).

7.1. Ce a evidențiat campania Hafnium?

După analizarea detaliilor cazului Hafnium, pot fi punctate câteva idei care susțin aspectele menționate anterior referitoare la cooperarea în domeniul vulnerabilităților de tip 0-day în securitatea cibernetică.

a. A împărtășit Microsoft informațiile privind vulnerabilitățile de tip 0-day existente?

Da, însă doar după ce a dezvoltat un patch de securitate. După cum s-a evidențiat în Secțiunea 6, deși existau mai multe dovezi care indicau că Microsoft era conștientă de existența vulnerabilităților de tip 0-day înainte de a face publică situația și de a împărtăși informațiile, compania a ales să facă acest lucru abia după ce a fost dezvoltat un patch. Procedând astfel, a demonstrat că principalul său interes a fost, în primul rând, reputațional (și, implicit, financiar), deoarece Microsoft a ales să păstreze secretul cu privire la vulnerabilitățile exploatate activ, cel mai probabil în încercarea de a evita pierderea clienților prin recunoașterea problemelor, fără a avea o soluție practică disponibilă. Din perspectiva victimelor, este probabil ca o declarație publică, făcută înainte de data de 2 martie, să fi fost mai utilă în implementarea unor măsuri de atenuare și, în cele din urmă, în limitarea numărului de servere compromise. Totuși, Microsoft a acționat în propriul interes, anume protejarea obiectivelor sale financiare.

b. A existat o cooperare activă între actorii privați?

Da și nu. Pe de-o parte, mai multe entități private, precum Volexity, au ales să coopereze prin informarea Microsoft cu privire la vulnerabilitățile 0-day observate, însă acestea nu ar fi putut exploata contextul în propriul interes; așadar, nu a existat o concurență directă în această situație. Pe de altă parte, comunicarea Microsoft, din 2 martie, nu a inclus nicio mențiune privind o eventuală cooperare cu alte companii private de securitate cibernetică în dezvoltarea patch-urilor, aspect care, dacă s-ar fi materializat, este probabil să fi produs mai devreme actualizările de securitate și să limiteze pagubele. Un posibil motiv ar putea fi acela că o abordare de cooperare ar fi obligat Microsoft să admită faptul că nu a fost capabilă să gestioneze singură problema vulnerabilităților 0-day și că a avut nevoie de sprijinul unui competitor.

c. A existat o cooperare activă între actorii publici și privați?

Nu. Deși Microsoft era conștientă de vulnerabilități, a ales să informeze doar

guvernul SUA, în timp ce toate celelalte state care folosesc tehnologia sa au fost în necunoștință de cauză în privința vulnerabilităților 0-day. Așa după cum se subliniază în Secțiunea 6, partajarea în timp real a acestui tip de informații cu toate autoritățile publice este puțin probabilă, deoarece nu este în interesul companiei. Prin urmare, rețelele guvernamentale au fost compromise, deoarece niciun alt stat, în afară de SUA nu a fost capabil să implementeze măsuri de prevenție.

d. A existat o cooperare activă între actorii publici?
Nu există argumente în acest sens. Nu există dovezi publice că vreun alt stat, în afară de SUA, ar fi fost informat despre campania Hafnium. Mai mult, numărul mare de victime la nivel mondial ar putea indica faptul că statele nu au fost capabile să implementeze măsuri preventive în timp util.

8. Concluzii

Această analiză, susținută direct de studiul de caz Hafnium, evidențiază obstacolele în partajarea datelor despre vulnerabilități 0-day între diferiți actori. Deși o astfel de cooperare ar putea asigura măsuri mai rapide (așa cum evidențiază campania Hafnium), principalele argumente din spatele acestei situații sunt sistemice și puțin probabile a fi depășite pe termen lung. Diferența fundamentală în interesele de bază ale statelor și ale companiilor private conduce la lipsa unei cooperări extinse în gestionarea datelor în timp real, cu accent în mod special pe vulnerabilitățile 0-day.

Deși mai multe formate încearcă să abordeze această problemă, succesul lor este discutabil, la fel ca și perspectivele lor de îmbunătățire. Volexity demonstrează că un anumit nivel de cooperare este cu siguranță posibil atunci când nu există interese competitive. Microsoft a arătat că dezvoltarea cooperării proactive cu partenerii și promovarea intereselor financiare sunt două abordări mutual exclusive. Contradicția fundamentală dintre motivațiile actorilor publici și cele ale actorilor privați indică faptul că un model complet cooperativ în securitatea cibernetică rămâne greu de realizat. Deși inițiative, precum parteneriatele public-privat și platformele de schimb de informații, aduc un anumit progres, acestea nu abordează în totalitate problemele sistemice mai profunde, prezentate în secțiunile anterioare.
Totuși, cooperarea activă în timp real dintre Microsoft și guvernul SUA în legătură cu Hafnium trebuie analizată, deoarece creează premisele unei situații în care se pare că Microsoft a depășit interesul său financiar și a colaborat cu o autoritate oficială.

Referințe

Ahmad, Rasheed, Izzat Alsmadi, Wasim Alhamdani și Lo'ai Tawalbeh. 2023. "Zero-day attack detection: a systematic literature review." *Artif Intell Rev* 10733–10811. https://doi.org/10.1007/s10462-023-10437-z.

Albakri, Adham, Eerke Boiten și Rogério De Lemos. 2018. "Risks of Sharing Cyber Incident Information." *Proceedings of the 13th International Conference on Availability,*

Reliability and Security 1-10. https://doi.org/10.1145/3230833.3233284.

___. 2019. "Sharing Cyber Threat Intelligence Under the General Data Protection Regulation." *Privacy Technologies and Policy 7th Annual Privacy Forum, APF 2019.* Rome, Italy: Springer. 28-41. https://doi.org/10.1007/978-3-030-21752-5_3.

Albanese, Massimiliano, Sushil Jajodia, Anoop Singhal și Lingyu Wang. 2013. "An efficient approach to assessing the risk of zero-day vulnerabilities." *International Conference on Security and Cryptography (SECRYPT).* Reykjavik, Iceland: IEEE. 1-12.

Arshad, Junaid, Muhammad Talha, Bilal Saleem, Zoha Shah, Huzaifa Zaman și Zia Muhammad. 2024. "A Survey of Bug Bounty Programs in Strengthening Cybersecurity and Privacy in the Blockchain Industry." *Blockchains* 2 (3): 195-216. https://doi.org/10.3390/blockchains2030010.

Bada, Maria, Michael Goldsmith, Chris Mitchell și Elizabeth Phillips. 2014. "Improving the Effectiveness of CSIRTs." *Global Cyber Security Capacity Centre.*

Barnum, Sean. 2014. *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™).* The MITRE Corporation.

Bates, Alicia. 2022. "Prepare and Prevent, Don't Repair and Repent." *The Cyber Defense Review* 7 (3): 17-30.

Bechara, Fabio Ramazzini și Samara Bueno Schuch. 2020. "Cybersecurity and global regulatory challenges." *Journal of Financial Crime* 359-374. https://doi.org/10.1108/JFC-07-2020-0149.

Bilge, Leyla și Tudor Dumitraș. 2012. "Before we knew it: an empirical study of zero-day attacks in the real world." *CCS '12: Proceedings of the 2012 ACM conference on Computer and communications security.* North Carolina, Raleigh, USA. 833 - 844. https://doi.org/10.1145/2382196.2382284.

Burt, Tom. 2021. "New nation-state cyberattacks." https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/.

Cavelty, Myriam Dunn, și Max Smeets. 2023. „Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority." *Journal of European Public Policy* 30 (7): 1330-1352. https://doi.org/10.1080/13501763.2023.2173274.

Cerezo, Ana I., Javier Lopez și Ahmed Patel. 2007. "International Cooperation to Fight Transnational Cybercrime." *Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007).* Karlovassi, Greece: IEEE. doi:10.1109/WDFIA.2007.4299369.

Comisia Europeană. 2016. "Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434.

Ekong, Anietie P., Aniebiet Etuk, Saviour Inyang și Mary Ekere-obong. 2023. "Securing Against Zero-Day Attacks: A Machine Learning Approach for Classification and Organizations' Perception of its Impact." *Journal of Information Systems and Informatics* 5 (3): 1123-1140. doi:10.51519/journalisi.v5i3.546.

Fischer, Daniel, Clemens Sauerwein, Martin Werchan și Dirk Stelzer. 2023. "An Exploratory Study on the Use of Threat Intelligence Sharing Platforms in Germany,

Austria and Switzerland." *ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security.* New YorkNYUnited States: Association for Computing Machinery. 1-7. https://doi.org/10.1145/3600160.3600185.

Google; Mandiant. 2024. "We're All in this Together. A Year in Review of Zero-Days Exploited In-the-Wild in 2023." https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Year_in_Review_of_ZeroDays.pdf.

Hausken, Kjell. 2007. "Information sharing among firms and cyber attacks." *Journal of Accounting and Public Policy* 26 (6): 639-688. https://doi.org/10.1016/j.jaccpubpol.2007.10.001.

Homburger, Zine. 2019. "The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace." *Global Society* 33 (2): 224-242. https://doi.org/10.1080/13600826.2019.1569502.

Kamiya, Shinichi, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis și René M. Stulz. 2018. "What is the Impact of Successful Cyberattacks on Target Firms?" *National Bureau of Economic Research.* doi:10.3386/w24409.

Krebs, Brian. 2021. "At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software." https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/.

Lanzendorfer, Quinn E. 2015. *Enabling knowledge in the paradigm of international cyber intelligence.* Robert Morris University ProQuest Dissertations Publishing.

Lewis, James A. 2002. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Center for Strategic and International Studies.

Maschmeyer, Lennart, Ronald J. Deibert și Jon R. Lindsay. 2020. "A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society." *Journal of Information Technology & Politics* 18 (1): 1-20. https://doi.org/10.1080/19331681.2020.1776658.

Meakins, Joss. 2018. "A zero-sum game: the zero-day market in 2018." *Journal of Cyber Policy* 60-71. doi:10.1080/23738871.2018.1546883.

Microsoft 365 Security. 2021. "HAFNIUM targeting Exchange Servers with 0-day exploits." https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/.

Narang, Satnam. 2021. *CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065: Four Zero-Day Vulnerabilities in Microsoft Exchange Server Exploited in the Wild.* https://www.tenable.com/blog/cve-2021-26855-cve-2021-26857-cve-2021-26858-cve-2021-27065-four-microsoft-exchange-server-zero-day-vulnerabilities.

NATO. 2021. "Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise." https://www.nato.int/cps/en/natohq/news_185863.htm.

Pala, Ali, și Jun Zhuang. 2019. "Information Sharing in Cybersecurity: A Review." *Decision Analysis* 16 (3): 172-196. https://doi.org/10.1287/deca.2018.0387.

Parlamentul European; Consiliul Uniunii Europene. 2022. "Directive (EU) 2022/2555 of the European Parliament and of the Council." *Official Journal of the European Union.* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555.

Perera, Srinath, Xiaohua Jin, Alana Maurushat și De-Graft Joe Opoku. 2022. "Factors Affecting Reputational Damage to Organisations Due to Cyberattacks." *Informatics* 9 (28). https://doi.org/10.3390/informatics9010028.

Purohit, Soumya, Roshan Neupane, Naga Ramya Bhamidipati, Varsha Vakkavanthula, Songjie Wang și Matthew Rockey. 2023. „Cyber Threat Intelligence Sharing for Co-Operative Defense in Multi-Domain Entities." *IEEE Transactions on Dependable and Secure Computing* 20 (5): 4273 - 4290. doi:10.1109/TDSC.2022.3214423.

Rajamäki, Jyri. 2017. "Cyber Security, Trust-Building, and Trust-Management: As Tools for Multi-agency Cooperation Within the Functions Vital to Society." În *Cyber-Physical Security. Protecting Critical Infrastructure at the State and Local Level*, de Robert M. Clark și Simon Hakim, 233–249. Springer.

Rheingold, Howard. 1994. *The Virtual Community: Finding Connection in a Computerized World.* Secker & Warburg.

Robinson, Philip. 2024. "The Hafnium Breach – Microsoft Exchange Server Attack." https://www.lepide.com/blog/the-hafnium-breach-microsoft-exchange-server-attack/.

Roumani, Yaman. 2021. "Patching zero-day vulnerabilities: an empirical analysis." *Journal of Cybersecurity* 7 (1). https://doi.org/10.1093/cybsec/tyab023.

Schlette, Daniel, Fabian Böhm, Marco Caselli și Günther Pernul. 2020. "Measuring and visualizing cyber threat intelligence quality." *International Journal of Information Security* 20: 21-38. https://doi.org/10.1007/s10207-020-00490-y.

Schulze, Matthias și Thomas Reinhold. 2018. "Wannacry about the tragedy of the commons? Game-theory and the failure of global vulnerability disclosure." *ECCWS 2018 17th European Conference on Cyber Warfare and Security V2*. Oslo, Norway: Academic Conferences and Publishing International Limited. 454-463.

Serrano, Oscar, Luc Dandurand și Sarah Brown. 2014. "On the design of a cyber security data sharing system." *Proceedings of the 2014 ACM workshop on information sharing & collaborative security.* New York, United States: Association for Computing Machinery. 62-69. https://doi.org/10.1145/2663876.2663882.

Shackleford, Dave. 2015. "Who's Using Cyberthreat Intelligence and How?" https://cdn-cybersecurity.att.com/docs/SANS-Cyber-Threat-Intelligence-Survey-2015.pdf.

Silva, Alessandra de Melo, João José Costa Gondim, Robson de Oliveira Albuquerque și Luis Javier García Villalba. 2020. "A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence." *Future Internet.*

Singh, Umesh Kumar, Chanchala Joshi, și Dimitris Kanellopoulos. 2019. „A framework for zero-day vulnerabilities detection and prioritization." *Journal of Information Security and Applications* 164-172. https://doi.org/10.1016/j.jisa.2019.03.011.

Sklyar, Vladimir și Vyacheslav Kharchenko. 2019. "ENISA Documents in Cybersecurity Assurance for Industry 4.0: IIoT Threats and Attacks Scenarios." *IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications.* Metz, France: IEEE. doi:10.1109/IDAACS.2019.8924452.

Smeets, Max. 2022. "The Role of Military Cyber Exercises: A Case Study of Locked Shields." *2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon).* Tallinn,

Estonia: IEEE. doi:10.23919/CyCon55549.2022.9811018.

Steffensen, Vilja și Vahiny Gnanasekaran. 2024. ”Information Sharing between the Computer Security Incident Response Team and its Members: An Empirical Study.” *NIKT* 3.

Sullivan, Clare, și Eric Burger. 2017. ”«In the public interest»: The privacy implications of international business-to-business sharing of cyber-threat intelligence.” *Computer Law & Security Review* 33 (1): 14-29. https://doi.org/10.1016/j.clsr.2016.11.015.

Sülü, Mücahit și Resul Daș. 2022. ”Graph Visualization of Cyber Threat Intelligence Data for Analysis of Cyber Attacks.” *Balkan Journal of Electrical & Computer Engineering.* https://doi.org/10.17694/bajece.1090145.

Sun, Nan, Ming Ding, Jiaojiao Jiang, Weikang Xu, Xiaoxing Mo și Yonghang Tai. 2023. ”Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives.” *IEEE Communications Surveys & Tutorials* 25 (3): 1748-1774. doi:10.1109/COMST.2023.3273282.

Teodorescu, Cosmin Alexandru. 2022. ”Perspectives and Reviews in the Development and Evolution of the Zero-Day Attacks.” *Informatica Economică* 26 (2). doi:10.24818/issn14531305/26.2.2022.05.

Tolga, İhsan Burak. 2019. *Whole-of-Government Cyber Information Sharing.* Talinn: CCDCoE.

Tounsi, Wiem și Helmi Rais. 2017. ”A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attacks.” *Computers & Security* 212-233.

Tropina, Tatiana. 2015. ”Public–Private Collaboration: Cybercrime, Cybersecurity and National Security. In: Self- and Co-regulation in Cybercrime, Cybersecurity and National Security.” *SpringerBriefs in Cybersecurity* 1-41. https://doi.org/10.1007/978-3-319-16447-2_1.

Wagner, Cynthia, Alexandre Dulaunoy, Gérard Wagener și Andras Iklody. 2016. ”MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform.” *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security.* Vienna, Austria: Association for Computing Machinery. 49-56. https://doi.org/10.1145/2994539.2994542.

Wagner, Thomas D., Khaled Mahbub, Esther Palomar și Ali E. Abdallah. 2019. ”Cyber threat intelligence sharing: Survey and research directions.” *Computers & Security* 87. https://doi.org/10.1016/j.cose.2019.101589.

Waheed, Azheen, Bhavish Seegolam, Mohammad Faizaan Jowaheer, Chloe Lai Xin Sze și Ethan Teo Feng Hua. 2024. ”Zero-Day Exploits in Cybersecurity: Case Studies and Countermeasure.” *Preprints.* doi: 10.20944/preprints202407.2338.v1.

Wallis, Tania, și Rafał Leszczyna. 2022. ”EE-ISAC—Practical Cybersecurity Solution for the Energy Sector.” *Energies* 15 (6). https://doi.org/10.3390/en15062170.

Wang, Han, Alfonso Iacovazzi, Seonghyun Kim și Shahid Raza. 2024. ”CLEVER: Crafting Intelligent MISP for Cyber Threat Intelligence.” *2024 IEEE 49th Conference on Local Computer Networks (LCN).* Normandy, France: IEEE. doi:10.1109/LCN60385.2024.10639749.