REVIEW SCIENTIFIC PAPER
DOI: 10.63395/STEDConf14022025935K187
Submitted: 22.08.2025.
Accepted: 19.11.2025.

„OČI ŠIROM OTVORENE" – JEDAN OD POSTULATA INFORMACIONE SIGURNOSTI

Alen Kamiš[1], Aleksandar Zakić[2], Marko Zakić[3], Nemanja Deretić[4]

[1]Visoka škola za uslužni biznis Istočno Sarajevo – Sokolac, Cara Lazara bb, 71350 Sokolac – Istočno Sarajevo, Bosna i Hercegovina, alen@vub.edu.ba
[2]Alfa BK Univerzitet, Fakultet informacionih tehnologija, Bulevar maršala Tolbuhina 8, 11000, Beograd, Republika Srbija, aleksandar.zakic@alfa.edu.rs
[3]Toplička akademija strukovnih studija, Ćirilo i Metodije br. 1, 18400 Prokuplje, Republika Srbija, marko.zakic@vpskp.edu.rs
[4]Beogradska akademija poslovnih i umetničkih strukovnih studija, Kraljice Marije 73, 11000 Beograd, Republika Srbija, nemanja.deretic@bpa.edu.rs

Coresponding author: Alen Kamiš, The College of Service Business, Cara Lazara bb, 71350 Sokolac, East Sarajevo, Bosnia and Herzegovina, alen@vub.edu.ba

SAŽETAK

Ovaj rad predstavlja originalni naučni doprinos kroz sveobuhvatnu primjenu metodologije studije slučaja u analizi evoluirajućih cyber prijetnji koje oblikuju informacionu sigurnost u 21. vijeku. Umjesto deskriptivnog ili preglednog pristupa, rad uvodi jasnu naučnu strukturu, definisane kriterijume odabira studija slučaja, metodološki okvir i transverzalnu analizu između različitih tipova napada. Cilj je pružiti dublji uvid u obrazac ponašanja modernih napadača, identifikovati kritične ranjivosti i formulisati preporuke koje se mogu praktično primijeniti u organizacijama svih veličina. Rad uključuje četiri proširene studije slučaja, zasnovane na kombinaciji naučne literature, industrijskih izvještaja i aktuelnih izvora.

Ključne riječi: informaciona sigurnost, sajber napadi, prijetnje, malver, praktični primjeri

UVOD

Digitalna transformacija i globalna povezanost donijele su bez presedana nivo zavisnosti od informacionih sistema. Međutim, ova zavisnost stvorila je i novu vrstu ranjivosti – sisteme koji su istovremeno kompleksni, distribuirani i kontinuirano izloženi sofisticiranim napadima. Tradicionalni modeli zaštite zasnovani na perimetarskoj sigurnosti više nisu dovoljni. Prema izvještaju ENISA-e (2024), broj napada koji uključuju lanac snabdijevanja porastao je za 68%, dok je broj napada koji iskorištavaju zero-day ranjivosti porastao za 45% u posljednje tri godine.

Iako se u literaturi često sreću radovi koji opisuju pojedinačne incidente, mali broj njih uspostavlja jasnu metodologiju koja omogućava poređenje, generalizaciju i dublje razumijevanje. Ovaj rad zato uvodi case-study pristup, koji omogućava strukturisanu i naučno validnu analizu kompleksnih cyber incidenata. Kroz analizu četiri reprezentativna slučaja, rad daje sveobuhvatnu sliku trendova, alata i tehnika koje oblikuju savremeni cyber prostor.

METODOLOGIJA

Metodologija studije slučaja korištena u ovom radu zasniva se na principima Roberta Yina (2014), jednog od najznačajnijih autora u ovoj oblasti. Primijenjeni su sljedeći koraci:

- Definisanje cilja istraživanja – identifikovati obrasce ponašanja modernih napada, njihove efekte i dominantne ranjivosti koje su eksploatisane u organizacijama.
- Kriterijumi za izbor slučajeva: raznovrsnost tipova napada (ransomware, ICS napad, supply-chain, napad na maloprodajni sektor), međunarodni uticaj i značaj, pouzdani izvori koji omogućavaju rekonstrukciju napada.
- Izvori podataka – korišteni su zvanični izvještaji ENISA, CISA, CrowdStrike, Microsoft Threat Intelligence, akademske studije, te relevantni novinski članci.

- Analitički okvir – svaki slučaj je analiziran prema četiri kriterijuma: (1) vektor napada, (2) ranjivosti, (3) efekti napada, (4) naučene lekcije.
- Uporedna analiza slučajeva – identifikovani su zajednički obrasci i specifične razlike, što je poslužilo za formulisanje zaključaka i preporuka.

Primjena ove metodologije omogućila je dubinsku analizu incidenata uz visok nivo naučne pouzdanosti.

NAPADI, UPADI I MALVER – NEVIDLJIVE PRIJETNJE DIGITALNOG SVIJETA

U savremenom digitalnom okruženju, informaciona sigurnost suočava se sa sve sofisticiranijim prijetnjama koje dolaze iz raznih izvora – od pojedinaca sa osnovnim tehničkim znanjem do dobro organizovanih kriminalnih grupa ili čak državnih aktera. Među najčešćim i najopasnijim oblicima ugrožavanja informacione sigurnosti nalaze se napadi, neovlašćeni upadi u sisteme i maliciozni softver, poznat kao malver. Razumijevanje ovih prijetnji ključno je za razvijanje efikasnih strategija zaštite i jačanje otpornosti informacionih sistema.

Napadi: Ciljani i masovni pristupi kompromitovanju sistema

Napad na informacioni sistem predstavlja svaku radnju čiji je cilj ugrožavanje povjerljivosti, integriteta ili dostupnosti podataka. Ovi napadi mogu biti ciljani, kada napadač želi kompromitovati konkretan sistem, organizaciju ili osobu, ili masovni, gdje napadač nasumično napada veliki broj sistema u nadi da će pronaći ranjivosti.

Jedan od najraširenijih oblika je DoS (Denial of Service) i njegov sofisticiraniji oblik DDoS (Distributed Denial of Service). Ovi napadi imaju za cilj preopterećenje resursa sistema kako bi onemogućili pristup legitimnim korisnicima. Posebno su opasni za organizacije koje zavise od dostupnosti svojih usluga u realnom vremenu, poput banaka, e-trgovine i zdravstvenih ustanova.

Brute-force su napadi pri kojim napadač pokušava da pogodi lozinku ili enkripcijski ključ isprobavanjem velikog broja kombinacija. Phishing su napadi u kojim se korisnici socijalnim inženjeringom navode da otkriju povjerljive informacije, a spadaju u svakodnevne izazove bezbjednosnih timova. Razvoj generativnih AI alata dodatno komplikuje odbranu, jer lažne poruke i web-stranice izgledaju autentičnije nego ikada.

Upadi: Dan kad napadač uđe u sistem

Neovlašćeni upad podrazumijeva pristup informacijama ili sistemima bez dozvole. On može biti rezultat ranjivosti u softveru, neadekvatne konfiguracije mrežnih uređaja, loših lozinki ili krađe legitimnih pristupnih podataka.

Napadači koji uspiju ostvariti pristup često ne ostaju pasivni. Umjesto toga, oni mogu:

- eksfiltrovati podatke,
- instalirati backdoor za kasniji ponovni ulazak,
- širiti se lateralno unutar mreže u potrazi za dodatnim osjetljivim informacijama ili boljim pozicijama ili
- šifrovati podatke s ciljem iznude (ransomware).

Upadi su često teško uočljivi jer napadači koriste tehnike prikrivanja poput enkripcije komunikacije, tunelovanja kroz dozvoljene servise (npr. DNS ili HTTPS) i manipulacije logovima. Detekcija takvih aktivnosti zahtijeva napredne SIEM (Security Information and Event Management) alate i pažljivo osmišljene politike nadzora i reagovanja.

Malver: Nevidljivi napadač unutar sistema

Maliciozni softver, poznat kao malver, predstavlja jednu od najefikasnijih metoda za kompromitovanje sistema. Razlikujemo više vrsta malvera, u zavisnosti od funkcionalnosti:

- Virus – samoreplicirajući kod koji se vezuje za druge fajlove ili programe i aktivira se kada se oni pokrenu.

- Trojanac (Trojan) – maskira se kao legitimni program, ali u pozadini obavlja zlonamjerne aktivnosti.
- Ransomware – šifruje podatke korisnika i traži otkupninu za dešifrovanje.
- Spyware – tajno prikuplja informacije o korisniku bez njegovog znanja.
- Rootkit – omogućava napadaču administratorski pristup i često je nevidljiv konvencionalnim metodama detekcije.

Distribucija malvera može se odvijati putem e-mail priloga, malicioznih web-stranica, kompromitovanih softverskih paketa ili preko USB uređaja. Jedan od ključnih izazova u borbi protiv malvera je njegova sposobnost da se neprestano mijenja, koristeći tehnike poput polimorfizma i metamorfizma kako bi izbjegao antivirusne sisteme.

TRENDOVI INFORMACIONE SIGURNOSTI U 2025. GODINI

Kako digitalno poslovanje i tehnologija nastavljaju ubrzano da se razvijaju, tako i prijetnje po informacionu sigurnost postaju sve kompleksnije, dinamičnije i teže predvidive. Godina 2025. donosi niz sigurnosnih izazova i trendova koji značajno utiču na strategije zaštite podataka i infrastrukture u privatnom i javnom sektoru. U nastavku se ističe šest ključnih trendova koji obilježavaju informacionu bezbjednost u 2025. godini.

Vještačka inteligencija kao okosnica moderne cyber sigurnosti

Ipak, vještačka inteligencija nije isključivo prijetnja – ona istovremeno postaje stub moderne odbrane. Savremeni sistemi za detekciju prijetnji koriste mašinsko učenje i analitiku ponašanja korisnika (UEBA) kako bi u realnom vremenu prepoznali anomalije koje mogu ukazivati na upad. AI takođe omogućava bržu analizu incidenata, automatsko reagovanje (SOAR sistemi) i predikciju potencijalnih rizika. Budućnost informacione sigurnosti oslanjaće se na simbiotski odnos između čovjeka i mašine, gdje AI pruža skalabilnost i brzinu, a ljudi kontekstualno razumijevanje i donošenje odluka.

Balansiranje između sigurnosti i korisničkog iskustva

Rast svijesti o bezbjednosti često dolazi u konflikt sa potrebom za jednostavnim i fluidnim korisničkim iskustvom. Korisnici žele brz pristup podacima i servisima, s minimalnim brojem prepreka, dok sigurnosni timovi insistiraju na višefaktorskoj autentifikaciji, segmentaciji mreže i strožim pravilima pristupa. U 2025. godini fokus se pomjera ka "security by design" pristupu, gdje se sigurnost ugrađuje u rješenja bez narušavanja korisničkog komfora. Primjeri uključuju biometrijsku autentifikaciju, behavioral passwordless pristup i kontekstualno upravljanje pristupom.

Sigurnost u oblaku i rizik od pogrešne konfiguracije

Migracija u cloud je nezaustavljiva, ali s njom dolaze i novi sigurnosni izazovi. Najveći među njima u 2025. godini ostaje pogrešna konfiguracija servisa u oblaku, koja često omogućava neovlašćeni pristup podacima. Zbog složenosti cloud okruženja (više dobavljača, mikrousluge, kontejneri), čak i male greške u podešavanjima mogu imati ozbiljne posljedice. Edukacija DevOps timova, implementacija Infrastructure-as-Code pristupa sa sigurnosnim politikama i kontinuirani cloud security posture management (CSPM) alati postaju nezaobilazan dio modernog sigurnosnog arsenala.

PROŠIRENE STUDIJE SLUČAJA

Studija slučaja 1: Stuxnet (2010) – Prvo digitalno oružje

Stuxnet predstavlja najpoznatiji primjer cyber oružja kreiranog s ciljem sabotiranja industrijskih procesa. Napad je kompromitovao SCADA sisteme i PLC kontrolere u iranskim nuklearnim postrojenjima.

- Vektor napada: četiri zero-day ranjivosti u Windows OS-u i fizički unašanje USB uređaja.
- Ranjivosti: nedostatak segmentacije ICS mreže, mogućnost manipulacije PLC logikom.

- Posljedice: uništenje postrojenja i značajno usporavanje nuklearnog programa Irana; globalni šok u industriji.
- Naučene lekcije: važnost air-gap politika, verifikacije firmware integriteta i forenzičkog nadzora ICS-a.

Kao što ističe Langner (2013), Stuxnet je promijenio shvatanje cyber sigurnosti u industriji jer je pokazao da digitalni napad može izazvati fizičku destrukciju.

Studija slučaja 2: WannaCry (2017) – Globalni ransomware talas

WannaCry je bio jedan od najbrže širećih ransomware incidenata. Iskoristio je SMB ranjivost EternalBlue koju je NSA godinama koristila, a kasnije je procurela u javnost.

- Vektor napada: exploit EternalBlue (CVE-2017-0144).
- Ranjivosti: neprimijenjeni sigurnosni patchovi i zastarjeli sistemi.
- Posljedice: više od 230.000 kompromitovanih računara u 150 država.
- Najpogođeniji sektor: britanske zdravstvene ustanove (NHS).

Prema Microsoft Security Report (2018), čak 98% pogođenih sistema bilo je bez zakrpe starije od dva mjeseca.

Studija slučaja 3: SolarWinds (2020) – Supply-chain napad

SolarWinds napad je paradigma modernih supply-chain prijetnji. Napadači, pripisani APT29 grupi, uspeli su kompromitovati build proces kompanije SolarWinds i ubaciti zlonamjerni kod u legitimno ažuriranje.

- Vektor napada: kompromitovana CI/CD infrastruktura.
- Ranjivosti: nedovoljno kontrolisan pristup kod signing sertifikatima.
- Posljedice: kompromitacija više od 18.000 organizacija, uključujući američke vladine institucije.
- Naučene lekcije: važnost zero-trust modela i verifikacije integriteta build procesa.
- Sinha & Bernroider (2022) navode da je SolarWinds najkompleksniji supply-chain napad u istoriji.

Studija slučaja 4: Marks & Spencer (2025) – Napad na maloprodajni sektor

Napad grupe Scattered Spider na britanski lanac Marks & Spencer pokazao je ranjivost maloprodajnog sektora, posebno u pogledu third-party integracija.

- Vektor napada: kompromitacija partnerske firme i krađa pristupnih podataka.
- Ranjivosti: slab nadzor eksternih dobavljača i zastarjeli IAM sistemi.
- Posljedice: prekid online prodaje, krađa ličnih podataka i procijenjena šteta od 300 miliona funti.

Izvještaj The Times (2025) navodi da će operativni poremećaji od ovog napada trajati mjesecima.

ZAKLJUČCI

Uporedna analiza četiri studije slučaja pokazala je da savremeni cyber napadi, bez obzira na kontekst ili ciljnu organizaciju, dijele niz strukturnih i operativnih sličnosti. U svim analiziranim incidentima ključnu ulogu imala je eksploatacija ranjivosti koje nisu bile pravovremeno zakrpljene, što potvrđuje da neadekvatan patch menadžment i dalje predstavlja jednu od najkritičnijih slabih tačaka u informacionim sistemima. Napadači su se, osim toga, oslanjali na zloupotrebu legitimnih administrativnih alata, čime su uspijevali izbjeći detekciju i zadržati dugotrajan pristup kompromitovanim okruženjima. Uočen je i visok stepen tehničke i organizacione sofisticiranosti, uključujući napredne tehnike prikrivanja tragova, upotrebu modularne maliciozne infrastrukture i koordinirano djelovanje unutar dobro strukturiranih kriminalnih grupa.

Posebno značajan nalaz odnosi se na supply-chain napade, koji se potvrđuju kao jedna od najvećih prijetnji modernim organizacijama. Njihova sposobnost da kompromituju širi ekosistem kroz jednog dobavljača čini ih izuzetno opasnim i teško detektabilnim. Istovremeno, ransomware ostaje najrasprostranjeniji oblik napada s direktnim i mjerljivim uticajem na kontinuitet poslovanja, što ga i dalje svrstava u prioritetne izazove za sve vrste organizacija.

Rezultati istraživanja ukazuju na to da odgovor na savremene cyber prijetnje zahtijeva holistički i proaktivan pristup. Ključne preporuke obuhvataju implementaciju zero-trust arhitekture, ubrzanje procesa zakrpa, primjenu višefaktorske autentifikacije, kontinuirani nadzor anomalija putem UEBA i SIEM sistema, unapređenje sigurnosnih kontrola kod eksternih partnera, te primjenu naprednih i redovno testiranih strategija backup-a i oporavka.

Ovaj rad potvrđuje da strukturiran case-study pristup omogućava dublje razumijevanje obrazaca savremenih napada i pruža čvrstu osnovu za definisanje praktičnih i primjenjivih sigurnosnih preporuka. Dobijeni uvidi mogu značajno doprinijeti unapređenju sigurnosnih politika i jačanju otpornosti organizacija u realnom poslovnom okruženju.

DECLARATIONS OF INTEREST STATEMENT

The authors affirm that there are no conflicts of interest to declare in relation to the research presented in this paper.

LITERATURA

Boffey, D. (2025). Russia accused of trying to hack border security cameras to disrupt Ukraine aid. *The Guardian*. Retrieved July 13, 2025 from https://www.theguardian.com/world/2025/may/21/russia-accused-trying-disrupt-aid-ukraine-hacking-border-crossings?utm_source=chatgpt.com

CrowdStrike. (2023). Global Threat Report 2023, CrowdStrike Inc.

ENISA. (2024). Threat Landscape Report 2024, European Union Agency for Cybersecurity.

Fish, I., & Witherow, T. (2025). Marks & Spencer faces £300m hit from cyberattack. *The Times*. Retrieved July 13, 2025 from https://www.thetimes.com/business-money/companies/article/marks-and-spencer-300m-cost-cyberattack-9gln92jd9?utm_source=chatgpt.com®ion=global

Kushner, D. (2024). The real story of Stuxnet. IEEE Spectrum. Report. Retrieved July 13, 2025 from https://spectrum.ieee.org/the-real-story-of-stuxnet

Langner, R. (2013). To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve, The Langner Group.

Malwarebytes. (2024, July 26). What was WannaCry? | WannaCry Ransomware | Malwarebytes. Retrieved July 13, 2025 from https://www.malwarebytes.com/wannacry

Microsoft. (2018), Security Intelligence Report, Microsoft Corporation.

Official journal of the European Union. (2022). Report. Retrieved July 13, 2025 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

Owda, A. (2025). Major cyber attacks in review: February 2025 - SOCRadar® Cyber Intelligence Inc. *SOCRadar® Cyber Intelligence Inc*. Report. Retrieved July 13, 2025 from https://socradar.io/major-cyber-attacks-in-review-february-2025/?utm_source=chatgpt.com

Sinha, S., & Bernroider, E. (2022). Supply chain attacks and software integrity: Lessons from SolarWinds. *Journal of Cybersecurity, 8*(2), 112–130.

Yin, R. K. (2014). *Case Study Research: Design and Methods, (5th ed.)*. SAGE Publications.

Zscaler. (n.d.). What is the SolarWinds cyberattack? *In Zscaler.* Retrieved July 13, 2025 from https://www.zscaler.com/resources/security-terms-glossary/what-is-the-solarwinds-cyberattack

Kamiš, A. i sar. (2025). "Oči širom otvorene" – jedan od rezultata informacione sigurnosti. *STED Conference 14*(2), 187-192.

"EYES WIDE OPEN" – ONE OF THE FUNDAMENTALS OF INFORMATION SECURITY

Alen Kamiš[1], Aleksandar Zakić[2], Marko Zakić[3], Nemanja Deretic[4]

[1]The College of Service Business, Cara Lazara bb, 71350 Sokolac, East Sarajevo, Bosnia and Herzegovina, alen@vub.edu.ba
[2]Alfa BK University, Faculty of Information Technologies, Bulevar maršala Tolbuhina 8, 11000, Belgrade, Republic of Serbia, aleksandar.zakic@alfa.edu.rs
[3]Toplica Academy of Professional Studies, Cyril and Methodius No. 1, 18400 Prokuplje, Republic of Serbia, marko.zakic@vpskp.edu.rs
[4]Belgrade Business and Arts Academy of Applied Studies, Kraljice Marije 73, 11000, Belgrade, Republic of Serbia, nemanja.deretic@bpa.edu.rs

ABSTRACT

This paper presents an original scientific contribution through the comprehensive application of the case study methodology in analyzing the evolving cyber threats that shape information security in the 21st century. Rather than relying on a descriptive or review-based approach, the paper introduces a clear scientific structure with defined criteria for selecting case studies, a methodological framework, and a transversal analysis across different types of attacks. The objective is to provide deeper insight into the behavioral patterns of modern threat actors, identify critical vulnerabilities, and formulate recommendations that can be practically applied within organizations of all sizes. The paper includes four extended case studies based on a combination of academic literature, industry reports, and contemporary sources.

Keywords: information security, cyberattacks, threats, malware, practical examples.