Kibernetska grožnja okolje nevladnih organizacij v EU

in zahteve za izmenjavo obveščevalnih podatkov o grožnjah z organi kazenskega pregona

UnderServed

OKTOBER 2024

CyberPeace Institute

UCD Centre for Cybersecurity and Cybercrime Investigation
Lárionad um Chibearshlándáil agus Imscrúdú Cibearchoireachta UCD

Avtorji

Adrien Ogée, Murielle Abi Akar, Miles Collins (CyberPeace Institute),
Dr. Cormac Doherty (University College Dublin Center for Cybersecurity
and Cybercrime Investigation).

Sofinancira
Evropska unija

Ta projekt je bil financiran iz sklada ISF 2022 Evropske unije v okviru sporazuma o nepovratnih sredstvih št. 101111844. Izražena stališča in mnenja so izključno mnenja avtorja(-ev) in ne odražajo nujno stališč in mnenj Evropske unije ali Evropske komisije. Evropska unija in organ, ki dodeli pomoč, za njih nista odgovorna.

Izjava o omejitvi odgovornosti

Sofinancira Evropska unija Izražena stališča in mnenja so izključno mnenja avtorja(-ev) in ne odražajo nujno stališč in mnenj Evropske unije ali organa, ki dodeljuje pomoč, Evropske komisije. Evropska unija in organ, ki dodeli pomoč, za njih nista odgovorna.

Čeprav se informacije v dokumentih zdijo točne, avtorji ali kateri koli drug udeleženec konzorcija UnderServed v zvezi s tem gradivom ne dajejo nikakršnega jamstva, vključno z domnevnimi jamstvi o prodajnosti in primernosti za določen namen, vendar ne omejeno nanje.

Niti konzorcij UnderServed niti kateri koli od njegovih članov, njihovih uradnikov, zaposlenih ali zastopnikov ni odgovoren za kakršno koli netočnost ali opustitev v tem dokumentu, če gre za malomarnost ali kako drugače.

Ne glede na splošnost zgoraj navedenega niti konzorcij UnderServed niti kateri koli od
njegovih članov, njihovih uradnikov, zaposlenih ali zastopnikov ni odgovoren za kakršno koli neposredno ali posredno ali posledično
izgubo ali škodo, ki bi nastala zaradi kakršnega koli informacijskega nasveta ali netočnosti ali opustitve v tem dokumentu.

GPT-4 je bil uporabljen v uredniške namene.

Obvestilo o avtorskih pravicah

Kazalo vsebine

Seznam tabel

Seznam slik

Povzetek

V dobi hitre digitalizacije družbe imajo **nevladne organizacije (NVO)** ključno vlogo pri reševanju številnih humanitarnih kriz, vprašanj človekovih pravic in pobud za socialno kohezijo v **Evropski uniji (EU)** in zunaj nje. Vendar so te organizacije zaradi večje odvisnosti od digitalnih tehnologij izpostavljene **številnim kibernetskim grožnjam**, zato se morajo nujno in ciljno odzvati, da zaščitijo svoje delovanje in občutljive podatke, s katerimi ravnajo.

Projekt UnderServed, ki ga financira Evropska komisija, se kaže kot ključni ukrep, namenjen krepitvi kibernetske varnosti nevladnih organizacij. Ta pobuda temelji na ugotovitvi Evropske komisije, da so nevladne organizacije zelo ranljive za kibernetske napade, kar so nazorno pokazale **nedavne odmevne kršitve**, med drugim ogrožanje podatkov Mednarodnega odbora Rdečega križa. Po Microsoftovih podatkih je sektor nevladnih organizacij za sektorjem informacijske tehnologije drugi sektor, ki ga nacionalne države najpogosteje napadajo. To poudarja potrebo po izboljšanih ukrepih kibernetske varnosti, prilagojenih potrebam in omejitvam sektorja nevladnih organizacij.

Cilj **platforme UnderServed platform** je zagotoviti celovit nabor orodij in virov, ki bodo nevladnim organizacijam pomagali pri njihovih prizadevanjih na področju kibernetske varnosti.. To vključuje lažjo **prijavo incidentov**, **pomoč** in **dostop do podpornih mrež.**. Platforma je zasnovana kot tehnološka rešitev in strateška podpora nevladnim organizacijam za učinkovitejše upravljanje informacijske varnosti in ohranjanje njihovih **ključnih humanitarnih misij** v varnem digitalnem okolju.

To poročilo z raziskavo, anketami, intervjuji in tehničnimi analizami predstavlja trenutno stanje kibernetske varnosti nevladnih organizacij, razkriva različne stopnje pripravljenosti in opredeljuje prevladujoče ranljivosti. Na primer, le 19 % nevladnih organizacij, ki so sodelovale v raziskavi v EU, ima uradni načrt odzivanja na incidente in obnove po nesreči, kar kaže na kritično vrzel pri pripravljenosti na kibernetske incidente. Od 56 analiziranih nevladnih organizacij **so vse pokazale napačno konfiguracijo in varnostne pomanjkljivosti ali** ranljivosti v programski opremi, ki jo uporabljajo, kar kaže na **nujno potrebo** po izboljšanih praksah digitalne higiene. Na primer, 93 % od 56 nevladnih organizacij ni imelo ustreznih varnostnih razširitev sistema domenskih imen (DNSSEC), kar je znatno povečalo njihovo dovzetnost za napade s ponarejanjem domen.

Nevladne organizacije so na milost in nemilost prepuščene kibernetskim kriminalcem in državnim akterjem; med januarjem 2023 in januarjem 2024 je bilo v 70 % analiziranih nevladnih organizacij v EU ogrožen vsaj en uporabniški račun, kar poudarja potrebo po zanesljivem upravljanju dostopa in uvedbi večfaktorskega preverjanja pristnosti (MFA). Če lahko zlonamerni akterji izkoristijo ta pooblastila za napade na nevladne organizacije, so lahko posledice res hude.

Čeprav nevladne organizacije običajno ne razkrivajo kibernetskih napadov in o njih ne poročajo, je v tem poročilu obravnavanih več primerov, vključno z napadom z lažno elektronsko pošto, napredno trajno grožnjo in napadom z izsiljevalsko programsko opremo.

Ugotovitve tega poročila poudarjajo, da je platforma UnderServed nujno potrebna in da je treba v nevladnem sektorju sprejeti proaktiven in ozaveščen pristop h kibernetski varnosti. Ta projekt je **pomemben korak** k izboljšanju kibernetske varnosti nevladnih organizacij v EU.. Z zagotavljanjem prilagojene **platforme za poročanje o incidentih in izmenjavo informacij**, projekt ne rešuje le neposrednih potreb nevladnih organizacij na področju kibernetske varnosti, temveč prispeva tudi k razvoju **varnejšega**u **kibernetskega ekosistema** za sodelovanje teh pomembnih organizacij. Izvajanje programa UnderServed je tako ključna pobuda za zaščito nepogrešljivega prispevka nevladnih organizacij k družbeni blaginji pred razvijajočimi se kibernetskimi grožnjami.

Uvod

Nevladne organizacije (NVO) imajo ključno vlogo in pomembno prispevajo k različnim vidikom družbe. **V Evropski uniji (EU) deluje več kot tisoč nevladnih organizacij, ki so ključnega pomena pri reševanju humanitarnih kriz, spodbujanju človekovih pravic in krepitvi socialne kohezije**[1]. Evropske nevladne organizacije so v ospredju pri odzivanju na naravne nesreče, spopade in izredne razmere ter prizadetim prebivalcem nudijo pomoč pri reševanju življenj, kot so pomoč v hrani, zdravstvena oskrba in zatočišče[1]. Humanitarne nevladne organizacije v EU s svojo predanostjo, inovativnostjo in sodelovanjem pomembno prispevajo k lajšanju trpljenja, zaščiti ranljivega prebivalstva in spodbujanju globalne solidarnosti.

Digitalna doba je nedvomno izboljšala delo nevladnih organizacij na številnih ravneh, vendar je prinesla tudi številne negativne, pogosto nepriznane zunanje učinke. **Kibernetske grožnje, ki vplivajo na posameznike in organizacije po vsem svetu, so tveganje, ki predstavlja resen izziv in zahteva nujne odzive**. Skupno raziskovalno središče Evropske komisije in strategija EU za varnostno unijo (2020-2025) priznavata razširjenost teh kibernetskih groženj. Priznavajo, da kibernetska varnost ni več nišno vprašanje, temveč zadeva vse sektorje – od vladnih ustanov do podjetij in celo nevladnih organizacij. Evropska komisija je v odgovor na to uvedla ključne ukrepe za okrepitev kibernetske varnosti[2]. Te vključujejo znatne naložbe v krepitev kibernetske infrastrukture in povečanje kibernetske odpornosti. Na primer **Na primer Evropska agencija za varnost omrežij in informacij (ENISA), Zakon o kibernetski varnosti, Zakon o kibernetski odpornosti** in številni drugi[2].

Prizadevanja za vzpostavitev močnejših kibernetskih zmogljivosti in infrastruktur napredujejo, vendar je postalo očitno, da vlade, organizacije civilne družbe ali zasebni sektor pogosto spregledajo neprofitni sektor.[3]. Študija, ki jo je izvedla Univerza Združenih narodov, je pokazala, da je le 30 % nevladnih organizacij po vsem svetu prejelo vladno podporo za izpolnjevanje predpisov in zakonskih zahtev o kibernetski varnosti[3].

Microsoftovi podatki razkrivajo, da kibernetski kriminalci pogosto ciljajo na nevladne organizacije in miselne centre, ki so **drugi najbolj ciljani sektor**. Ti subjekti predstavljajo 31 % vseh obvestil o napadih nacionalnih držav na organizacijske domene[4]. Leta 2022 se je Mednarodni odbor Rdečega križa (ICRC), priznana nevladna organizacija, soočil s kibernetskimi napadi, ki so v prefinjenem kibernetskem napadu ogrozili osebne podatke več kot 515.000 posameznikov po vsem svetu[5]. Tudi dobrodelna organizacija Philabundance je doživela kibernetski napad, ki je povzročil izgubo v višini 1 milijona dolarjev[6].

Kljub svoji ključni vlogi so nevladne organizacije

1 Evropske operacije civilne zaščite in humanitarne pomoči. »Humanitarni partnerji«. 1. februar 2024. [Na spletu]. Na voljo : **https://civil-protection-humanitarian-aid.ec.europa.eu/partnerships/humanitarian-partners_en**

2 Oblikovanje digitalne prihodnosti Evrope. »Politike kibernetske varnosti«, 20. marec 2024. [Na spletu]. Na voljo : **https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies**

3 United Nations University, Institute of Macau., »Civil society organizations' cyber resilience« (Kibernetska odpornost organizacij civilne družbe). 2021. [Na spletu]. Na voljo : **https://collections.unu.edu/eserv/UNU : 8262/Civil_Society_Organizations_Cyber_Resilience.pdf**

4 Spelhaug, Justin. »Krepitev kibernetske obrambe za neprofitne organizacije.« Microsoft o vprašanjih, 13. december 2021. **https://blogs.microsoft.com/on-the-issues/2021/10/21/cyber-defenses-security-program-nonprofits/**

5 Mednarodni odbor Rdečega križa (ICRC), »Kibernetski napad na Mednarodni odbor Rdečega križa : Kaj vemo«. 22. junij 2022 [Na spletu]. Na voljo : **https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know**

6 Pat Ralph, »Fundacija Philabundance postala žrtev kibernetskega napada in izgubila skoraj milijon dolarjev.«, PhillyVoice, 1. december 2020, **https://www.phillyvoice.com/philabundance-cyberattack-theft-1-million-dollars/**

še vedno zelo dovzetne za kibernetska tveganja. Te organizacije so zaradi **proračunskih omejitev**, ki jim preprečujejo, da bi namenile dovolj sredstev za upravljanje IT in kibernetske varnosti, še **posebej ranljive**. Njihovi odnosi s številnimi bogatimi donatorji in vse večji digitalni odtis so odlične priložnosti za kibernetske kriminalce, da izkoristijo vrzeli v kibernetski varnosti. Zato se **nevladne organizacije soočajo s precejšnjimi tveganji**, vključno z grožnjami njihovim finančnim virom, operativni učinkovitosti in celo političnim stališčem. Ta ranljivost poudarja potrebo po bolj vključujočih strategijah kibernetske varnosti, ki ščitijo vse sektorje, vključno te.

V podporo tem prizadevanjem je nastal projekt UnderServed, ki ga financira EU. **Cilj projekta je rešiti te težave z vzpostavitvijo platforme za izmenjavo informacij in poročanje o incidentih, ki je posebej zasnovana za izpolnjevanje zahtev ranljivega sektorja**. V okviru projekta bo ta platforma osredotočena predvsem na humanitarni sektor, vendar bo zasnovana tako, da jo bo v prihodnosti mogoče razširiti na druge sektorje.

To poročilo je prvi rezultat v delovnem sklopu 2 »Pokrajina groženj NVO« projekta UnderServed. V njem sta podrobno opisana in analizirana ogroženost 30 humanitarnih nevladnih organizacij s sedežem v EU.

1.1 Preslikava izhodov UnderServed

Namen tega poglavja je prikazati zaveze sporazuma o nepovratnih sredstvih UnderServed, tako v okviru formalnega rezultata kot opisa naloge, glede na ustrezne rezultate projekta in opravljeno delo.

UnderServed GA Component Title	UnderServed GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			
D2.1 Report on NGO Threat Landscape	Final fact-based pdf report in English and executive summary translated in 24 EU languages.	All	This report presents the threat landscape of NGOs based in the EU and Switzerland. Translation at a later stage.
TASKS			
T2.2. Research	The research will focus on collecting raw incidents data and conducting survey and interviews with NGOs, CERTs and LEAs	2 & 3	We conducted surveys and Interviews with NGOs and CERTs/LEAs
T2.3. Interim analysis	Conduct an initial analysis of the data to establish how the data needs to be presented in the platform. Develop case studies.	4, 5 & 6	In the following sections, we provide several case studies along with an analysis of the data gathered and the requirements suggested for the plateform.

Tabela 1 : Upoštevanje opisov rezultatov in nalog programa UnderServed GA

1.2 Zakaj to poročilo?

Cilj tega poročila je **izboljšati razumevanje področja kibernetskih groženj, ki vplivajo na nevladne organizacije** v EU, da bi lahko na podlagi tega razvili platformo UnderServed. Poročilo prikazuje vprašanja kibernetske varnosti, ki zadevajo nevladne organizacije EU, in obravnava njihovo stopnjo **razvitosti kibernetske varnosti**, **slabosti** in **ranljivosti** njihove digitalne infrastrukture ter **kibernetske incidente**, ki so vplivali nanje. Poleg tega smo izvedli ankete z organi LEA in CERT o njihovih interakcijah z nevladnimi organizacijami ter o njihovih zahtevah glede platforme. To poročilo vsebuje tudi **primerjalno analizo z nevladnimi organizacijami s sedežem v Švici**, **ki ponuja primerjalno perspektivo iz države, ki je v preteklosti gostila humanitarne nevladne organizacije in se zavzemala za njihovo zaščito**[7].

7 Ville De Genève – Uradna spletna stran. »Mednarodne institucije, stalne misije in nevladne organizacije«, 5. februar 2024. [Na spletu]. Na voljo : **https://www.geneve.ch/en/themes/international-geneva/international-institutions-permanent-missions-non-governmental-organisations**.

1.3 Pregled rezultatov in struktura poročila

To poročilo je prvi rezultat v delovnem sklopu 2 »Pokrajina groženj NVO« projekta UnderServed. Vsebuje podroben opis in analizo groženj, s katerimi se soočajo nevladne organizacije s sedežem v EU, in sicer v treh glavnih razdelkih. V prvem razdelku je obravnavana stopnja zrelosti nevladnih organizacij na vseh področjih kibernetske varnosti, ki temelji na vprašalnikih in intervjujih s 30 nevladnimi organizacijami v EU in 30 v Švici. Drugo poglavje temelji na pregledih ranljivosti in ocenjuje ranljivosti digitalnega odtisa vseh teh nevladnih organizacij. V tretjem delu so obravnavani incidenti, s katerimi so se soočile nevladne organizacije, pri čemer so uporabljeni podatki iz odprtih in zaprtih obveščevalnih virov, pasivnega pregledovanja in spremljanja temnih spletnih strani ter raziskav, izvedenih za agencije LEA in skupine CERT. Na podlagi tega pregleda okolja kibernetskih groženj, ki vplivajo na nevladne organizacije v EU, je v četrtem razdelku podan vpogled, zlasti na podlagi raziskav, v module, ki bi jih lahko zahtevala platforma UnderServed.

1.4 Raziskovalna metodologija

To poročilo temelji na podatkih, ki jih je Inštitut za kibernetski mir pridobil in analiziral iz dveh kanalov :

· **Primarni podatki** z neposrednim sodelovanjem z nevladnimi organizacijami, pristojnimi organi oblasti in skupinami CERT z anketami in intervjuji, pridobljeni iz vodilnih storitev Inštituta za kibernetski mir, vključno s programom CyberPeace Builders in Cyber Incident Tracers.[8/9]. Podatki so bili združeni in anonimizirani zaradi spoštovanja zasebnosti in varnosti sodelujočih nevladnih organizacij.

· **Sekundarni viri** iz odprtih virov, zbrani s tehnikami obveščevalnih podatkov iz odprtih virov, pasivno pregledovanje digitalnih sredstev za ugotavljanje morebitnih tveganj ali ranljivosti. Prav tako so zbrani iz zaupanja vredne mreže partnerskih podjetij za kibernetsko varnost, kar zagotavlja dodatne vpoglede, ki izhajajo iz sekundarnih zbirk podatkov, kot so telemetrijski podatki, kršitve in uhajanje podatkov ter ocene kibernetske varnosti.

Za ugotavljanje ravni pripravljenosti nevladnih organizacij in kibernetske odpornosti je v metodologiji uporabljen pristop mešanih metod. **Pristop kombiniranih metod** je postopek zbiranja, analiziranja in mešanja kvalitativnih in kvantitativnih metod ter podatkov v eni študiji, da se zagotovi celovitejša, na dejstvih temelječa rešitev teme analize.

Za to poročilo je 30 nevladnih organizacij EU izpolnilo vprašalnik o varnostni zrelosti, ki je vseboval različna vprašanja iz devetih kategorij informacijske varnosti. Izpolnilo ga je še 30 nevladnih organizacij v Švici, rezultati pa so bili analizirani, da bi ponudili primerjalno perspektivo.

8 Inštitut CyberPeace. »CyberPeace Builders.« CyberPeace Builders, n.d. **https://cpb.ngo/**
9 Inštitut CyberPeace. »Cyber Incident Tracers | CyberPeace Institute,« 10. oktober 2023. **https://cyberpeaceinstitute.org/cyber-incident-tracers**

Inštitut CyberPeace Institute je razvil **General Splošno oceno kibernetske varnosti (GCSA),** da bi racionaliziral in poenostavil oceno kibernetske varnosti nevladnih organizacij[10]. GCSA je celovito **orodje za samoocenjevanje**, ki je namenjeno nevladnim organizacijam, **da ocenijo svojo stopnjo zrelosti na področju kibernetske varnosti**, ki temelji na industrijskih standardih, kot je **okvir kibernetske varnosti NIST[11]**. Samoocenjevanje je napisano v angleščini in traja manj kot 20 minut. Ker nevladne organizacije pogosto nimajo enotne kontaktne točke za kibernetsko varnost, je bilo orodje zasnovano tako, da so lahko vanj prispevali različni člani osebja organizacije. Po zaključku organizacija prejme **dvostransko poročilo** o trenutnem stanju kibernetske varnosti s predlaganimi naslednjimi koraki.

10 CyberPeace Institute, »Ukrepanje za izboljšanje : Vloga GCSA pri kibernetski odpornosti neprofitnih organizacij«. 30. januar 2024. [Na spletu]. Na voljo : **https://cyberpeaceinstitute.org/news/measure-to-improve-the-gcsas-role-in-nonprofit-cyber-resilience/**

11 NIST. »Okvir kibernetske varnosti | NIST,« 8. marec 2024. **https://www.nist.gov/cyberframework**

Raziskava je sestavljena iz 30 vprašanj, ki zajemajo 9 kategorij dejavnosti informacijske varnosti :

- **Varstvo sredstev in podatkov :** Ta kategorija se osredotoča na prepoznavanje kritičnih sredstev in podatkov, urejanje dostopa do sistemov in omrežij ter izvajanje ciljno usmerjenih zaščitnih ukrepov za občutljive informacije.
- **Varnostno kopiranje in obnovitev po nesreči :** v tej kategoriji je opisan pomen rednega varnostnega kopiranja in preverjanja podatkov, pri čemer je poudarjena metoda 3-2-1.
- **Načrt odzivanja na incidente in obnovitve po nesreči :** ta kategorija se razlikuje od prejšnje kategorije in preučuje odpornost organizacije, da se po nesreči čim hitreje vrne na površje.
- **Digitalno varovanje oboda :** zajema varovanje virtualnih računov in digitalnih platform, kot so spletna mesta, e-pošta in družabni mediji, ki so namenjeni javnosti, pred kibernetskimi napadi, vključno s strategijami za preprečevanje uhajanja podatkov.
- **Zaščita končne točke naslednje generacije :** osredotoča se na napredna varnostna orodja, ki se proaktivno učijo in preprečujejo zlonamerno programsko opremo v realnem času, ter dvomi o namestitvi takšnih protivirusnih rešitev v organizacijskih napravah.
- **Prakse preverjanja pristnosti :** Obravnava uvedbo dodatne varnostne ravni, pogosto s kombinacijo tega, kar uporabniki imajo, poznajo in so, kot je dvo- ali večfaktorsko preverjanje pristnosti, vključno z biometričnimi podatki, na ključnih organizacijskih platformah.
- **Simulirano lažno predstavljanje in usposabljanje :** V tej kategoriji se ocenjuje stopnja ozaveščenosti o kibernetski varnosti v organizaciji s poudarkom na rednem usposabljanju uporabnikov, izvajanju simulacij lažnega predstavljanja in uvajanju opozorilnih pasic za zunanja e-poštna sporočila.
- **Upravljanje gesel :** v zvezi z uporabo programske opreme ali strojne naprave, ki se uporablja za shranjevanje in upravljanje gesel zaposlenih.
- **Ozaveščanje o grožnjah in spremljanje :** osredotoča se na spremljanje dejavnosti v temnem spletu za odkrivanje sumljivih dejanj ali kraje identitete, na primer uhajanja uporabniških poverilnic, da se izboljša organizacijska varnost.

Ciljne organizacije so registrirane, apolitične in neodvisne nevladne organizacije, ki si prizadevajo za izboljšanje življenja in zmanjšanje trpljenja, s poudarkom na humanitarno-razvojnih in mirovnih prizadevanjih. Vsi delujejo v EU ali Švici in svoje dejavnosti izvajajo na nacionalni, evropski ali svetovni ravni.

Približno 65 % analiziranih nevladnih organizacij je bilo razvrščenih med majhne organizacije. Majhne organizacije so opredeljene kot organizacije s 50 ali manj zaposlenimi, medtem ko so velike organizacije tiste z 51 ali več zaposlenimi.

Interna ekipa inštituta CyberPeace Institute je opravila pogovore s 60 nevladnimi organizacijami. S temi intervjuji smo pridobili kvalitativne vpoglede v zvezi s človeško usmerjenim razumevanjem njihove prakse kibernetske varnosti. Intervjuji so potekali v francoščini in angleščini.

Vzorec 30 nevladnih organizacij EU je omogočil podrobno preučitev vsake sodelujoče nevladne organizacije, kar je omogočilo razumevanje njihovih edinstvenih okoliščin, izzivov in praks. Tako poglobljena analiza lahko prinese podrobna spoznanja, ki so lahko pri večjih vzorcih nejasna. Vendar velikost vzorca morda ne zajema celotnega obsega pripravljenosti na kibernetsko varnost in ozaveščenosti o grožnjah v celotni skupnosti humanitarnih nevladnih organizacij v EU.

Poleg anketiranja nevladnih organizacij je Inštitut za kibernetski mir izvedel tudi raziskavo o sodelovanju med **nevladnimi organizacijami**, **organi kazenskega pregona (LEA)** in **skupinami za odzivanje na računalniške grožnje (CERT)**. Ta raziskava je bila izvedena zaradi vse pogostejših in zahtevnejših kibernetskih napadov na neprofitne organizacije. V zvezi s tem je bila izvedena raziskava, katere namen je bil pridobiti vpogled v to, kako skupine CERT/LEA za odzivanje na kibernetske napade sodelujejo z nevladnimi organizacijami, s kakšnimi izzivi se soočajo in kakšne so možne rešitve, ki bi lahko okrepile ta partnerstva.

Ta raziskava je bila namenjena strokovnjakom, ki delajo v skupinah CERT in LEA, izpolnilo pa jo je osem udeležencev. Ti anketiranci so imeli različne vloge, med drugim so bili **svetovalci za informacijsko varnost**, **detektivski inšpektorji in višji svetovalci na področju digitalne forenzike in odzivanja na incidente (DFIR)**. Cilj je bil oceniti trenutno stanje sodelovanja med skupinami CERT/LEA in nevladnimi organizacijami, s poudarkom na odzivanju na incidente, obvladovanju kibernetskih groženj in področjih, na katerih bi bilo mogoče sodelovanje izboljšati.

Spoznanja, pridobljena v tej raziskavi, zagotavljajo dragocene poglede na operativno realnost spopadanja s kibernetskimi grožnjami in poudarjajo potrebo po boljši komunikaciji, izmenjavi virov in platformah za tehnično podporo med skupinami CERT, LEA in nevladnimi organizacijami.

1.5 Omejitve

Čeprav ugotovitve te študije ponujajo dragocen vpogled v okolje groženj humanitarnih nevladnih organizacij s sedežem v EU, je treba priznati nekatere omejitve, ki so morda vplivale na rezultate.

Glede na velikost vzorca smo ocenili 30 nevladnih organizacij samo v humanitarnem ekosistemu. To število nevladnih organizacij lahko vnese nekaj pristranskosti. Druge nevladne organizacije imajo morda drugačne izkušnje in znanje glede nadzora kibernetske varnosti, ranljivosti in groženj.

Nevladne organizacije na splošno nerade delijo podrobne informacije o incidentih na področju kibernetske varnosti : nimajo praktično nobenih zakonskih obveznosti, da bi to storile, nimajo spodbud za to in na splošno niso dovolj zrele, da bi razumele tveganja in koristi, povezane z oblikovanjem zgodbe o kibernetskem incidentu. Prav to so razlogi za nastanek projekta UnderServed.

Čeprav se je digitalni odtis nevladnih organizacij v zadnjem desetletju povečal[12], jim omejeni viri IT omejujejo zmožnost vzpostavitve in vzdrževanja lastne digitalne infrastrukture, kot so avtonomni sistemi, zaradi česar je težko celovito oceniti njihovo kibernetsko varnost brez bolj neposrednih ali aktivnih metod sodelovanja, ki pa niso bile vključene v to raziskavo.

Nazadnje, majhen vzorec skupin CERT in LEA, vključenih v raziskavo, morda ne bo v celoti zajel raznolikosti izkušenj in operativnih kontekstov v različnih regijah in organizacijah.

12 Al Achkar, »Doseganje varnega delovanja s sprejemanjem : Izzivi in priložnosti za upravljanje varnostnih tveganj«. [Na spletu]. Na voljo : **https://gisf.ngo/wp-content/uploads/2021/12/Digital_Risk_how_new_technologies_impact_acceptance_and_raise_new_challenges_for_NGOs.pdf**

2. Kibernetska zrelost nevladnih organizacij

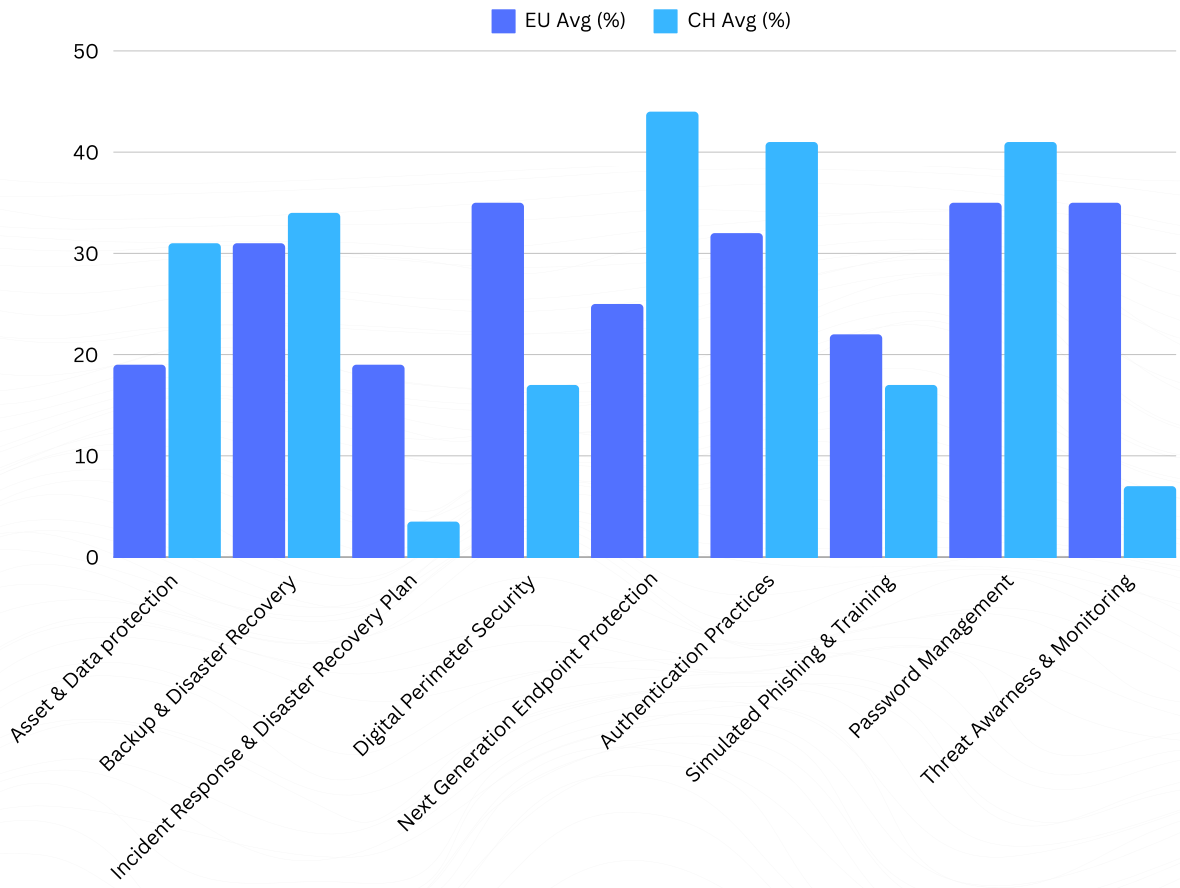
Humanitarne nevladne organizacije v EU se srečujejo z različnimi izzivi, ki vplivajo na njihovo delovanje. Glede na to, da je bilo ocenjenih **30 nevladnih organizacij**, spodnja analiza ni izčrpna. Pomembno je tudi omeniti, da so podrobne informacije o sodelujočih nevladnih organizacijah izpuščene zaradi varovanja njihove zasebnosti in varnosti.

Da bi bolje ocenili stopnjo zrelosti nevladnih organizacij EU na področju kibernetske varnosti, so bili opravljeni intervjuji, v katerih je bil izpolnjen vprašalnik GCSA, bodisi neposredno s strani nevladne organizacije bodisi s strani izvajalca intervjuja.

V naslednjih podpoglavjih so predstavljeni rezultati ankete za vsako vprašanje po vrstnem redu.

2.1 Povprečne ocene zrelosti kibernetske varnosti

Po ocenjevanju nevladnih organizacij in glede na oceno so bili **rezultati razdeljeni v 9 kategorij**. Na spodnji sliki so prikazane ocene za vsako kategorijo.



Slika 1 : Povprečna ocena razvitosti kibernetske varnosti humanitarnih nevladnih organizacij v EU in Švici

Zrelost nevladnih organizacij EU na področju kibernetske varnosti kaže na **mešane razmere**. Precejšnje število nevladnih organizacij se je ukvarjalo s postopki varnostnega kopiranja, upravljanjem gesel, praksami avtentikacije in izvajanjem digitalne varnosti. Prav tako aktivno spremljajo grožnje in kibernetska tveganja ter tako izboljšujejo splošne ukrepe za kibernetsko varnost. Vendar jih večina nima bistvenih ukrepov kibernetske varnosti, kot so varnost v oblaku, odzivanje na incidente in druge kategorije, ki so potrebni za ohranjanje njihovega delovanja. Čeprav ima na primer **19 % nevladnih organizacij načrte za odzivanje na incidente in obnovitve po nesreči, medtem ko jih ima švicarske nevladne organizacije le 3,5 %**, bi bilo treba tej kategoriji nameniti več pozornosti. Skoraj polovica anketiranih švicarskih nevladnih organizacij aktivno izvaja ukrepe za zaščito končnih točk naslednje generacije in preverjanje pristnosti, v nasprotju z nižjo stopnjo sprejemanja med nevladnimi organizacijami v EU. Poglobimo se v vsako kategorijo.

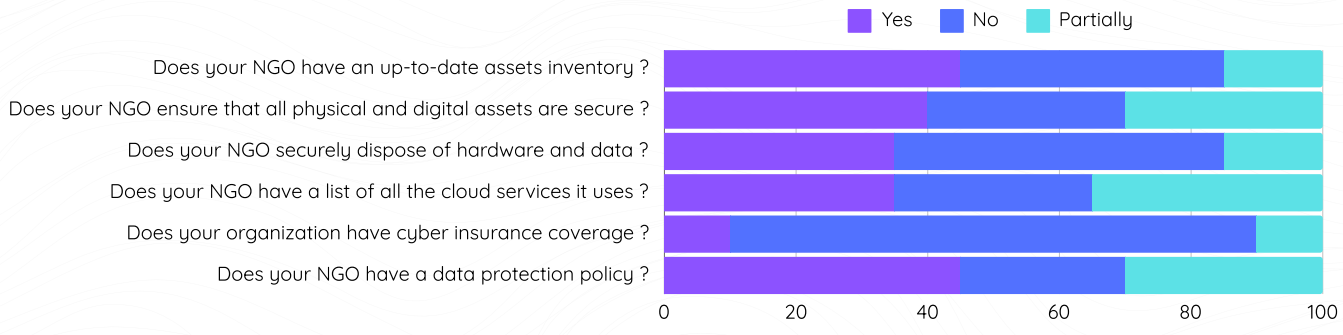
2.2 Sredstva in varstvo podatkov

Na področju premoženja in varstva podatkov so razmere v nevladnih organizacijah EU zaskrbljujoče. **Le 29 % jih ima posodobljene in pravilno konfigurirane tako fizične kot digitalne vire**. Ta nizek odstotek je zaskrbljujoč glede na pomen vzdrževanja strojne opreme in licenc programske opreme za varnost.

Le 16 % jih ima posodobljen popis teh sredstev.. Ta korak je ključnega pomena za prepoznavanje in obvladovanje morebitnih varnostnih tveganj, vendar je pogosto zanemarjen. Samo **32 % jih izvaja učinkovito upravljanje popravkov**, ki je bistveno za preprečevanje izkoriščanja ranljivosti.

Poleg tega obstaja precejšnja vrzel pri kibernetskem zavarovanju, saj **84 % nevladnih organizacij v EU nima te zaščite**, **v primerjavi z 31 % švicarskih nevladnih organizacij, katerih splošno zavarovanje vključuje tudi kibernetsko kritje v primeru kibernetskega incidenta**. Kibernetsko zavarovanje je ključnega pomena za zmanjšanje finančnih izgub po kibernetskem napadu, vendar pogosto zahteva dokumentirane politike, ki jih v številnih nevladnih organizacijah ni.

In **le 27 % jih ima uradno politiko o varstvu podatkov**.



Slika 2 : Odgovori na raziskavo : vpogledi GSA v nevladne organizacije EU

2.3 Varnostno kopiranje in obnovitev po nesreči

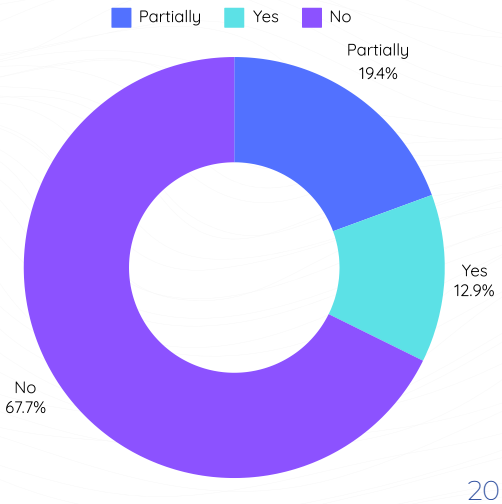
v tej kategoriji je opisan pomen rednega varnostnega kopiranja in preverjanja podatkov, pri čemer je poudarjena **metoda varnostnega kopiranja 3-2-1** : Tri kopije podatkov, ki so shranjene na dveh različnih vrstah medijev, in ena kopija zunaj lokacije. Tako nevladne organizacije EU kot švicarske nevladne organizacije imajo podobne ocene zrelosti glede strategij varnostnega kopiranja in obnovitve po nesreči : **le 29 % jih je poročalo o varnostnih kopijah svojih podatkov in njihovem varnem shranjevanju.**, da se lahko takoj obnovijo po incidentu. Kar pomeni, **da je 79 % nevladnih organizacij EU poročalo, da so opredelile svoje kritične funkcije, povezane z zagotavljanjem bistvenih storitev ranljivim skupinam prebivalstva**. To je dober začetek. Na žalost jih več kot polovica poroča, da ne ustvarjajo varnostnih kopij podatkov, povezanih s temi ključnimi storitvami.

2.4 Načrt odzivanja na incidente in obnovitve po nesreči

Kar zadeva načrtovanje odzivanja na incidente in obnovitve po nesreči, **ga ima vzpostavljenega le 3,2 % nevladnih organizacij s sedežem v Švici in 19 % nevladnih organizacij s sedežem v EU**. Ta zaskrbljujoča statistika opozarja na kritično vrzel : omejeno izvajanje načrtov za odzivanje na incidente in obnovitve po nesrečah v nevladnih organizacijah. Te razmere poudarjajo, da je nujno potrebna dostopna platforma za poročanje o incidentih.

2.5 Digitalno varovanje oboda

Digitalna varnost oboda je ključnega pomena za zaščito virtualnih sredstev organizacije, namenjenih javnosti, kot so spletna mesta, e-pošta in platforme družabnih medijev, pred kibernetskimi napadi. To vključuje strategije za preprečevanje uhajanja podatkov. Čeprav **je 35 % nevladnih organizacij EU poročalo o zavarovanju svojih omrežij, kar je dvakrat več kot pri švicarskih nevladnih organizacijah**, ostaja precejšnje področje, ki vzbuja skrb. V EU kar **68 % nevladnih organizacij ne izvaja pregledov ranljivosti spletnih strani**. Nasprotno pa v Švici **le 17 % nevladnih organizacij zanemarja izvajanje pregledov ranljivosti spletnih strani**. Ta očitna razlika kaže na kritično vrzel v praksah digitalne varnosti nevladnih organizacij EU in poudarja potrebo po strožjih in doslednejših ukrepih za kibernetsko varnost.



Slika 3 : Rezultati GCSA nevladnih organizacij o uvajanju ocene ranljivosti spletnih strani

2.6 Zaščita končne točke naslednje generacije

Protivirusne rešitve, vključno z zaščito končne točke naslednje generacije, so ključnega pomena pri odkrivanju, zajemanju in odstranjevanju potencialno škodljivih aplikacij v računalnikih. Takšna zaščita je še posebej pomembna, saj sledi vedenjskim kazalnikom, povezanim z aktivnimi okužbami z zlonamerno programsko opremo, kar zagotavlja večjo varnost v organizacijskih okoljih. Vendar je zaskrbljujoče, da je **le 35 % končnih točk nevladnih organizacij v EU zaščitenih pred zlonamerno programsko opremo in drugimi kibernetskimi grožnjami s posodobljeno varnostno programsko opremo**. Ta nizek odstotek kaže na veliko vrzel v osnovnih ukrepih kibernetske obrambe, zaradi česar je večina teh organizacij nevarno izpostavljena vse bolj izpopolnjenim kibernetskim napadom.

2.7 Prakse preverjanja pristnosti

Upravljanje identitete in dostopa je osrednji del programa kibernetske varnosti. Vendar pa se prakse, kot je večfaktorsko preverjanje pristnosti, med nevladnimi organizacijami EU ne uporabljajo tako pogosto, kot bi se morale. **Le 54 % teh organizacij uporablja MFA za dostop do občutljivih podatkov ali sistemov.**. Poleg tega jih **le 45 % uporablja postopek dodeljevanja pravic dostopa na podlagi vlog in odgovornosti uporabnikov, kar je bistveno za zagotavljanje varnega in učinkovitega nadzora dostopa.** Poleg tega jih **le 42 % zagotavlja ustrezno upravljanje uporabniških računov, zlasti za posameznike, ki se pridružijo organizaciji ali jo zapustijo**. Ta pomanjkljivost v zanesljivih praksah preverjanja pristnosti kaže na pomembno področje ranljivosti.

2.8 Simulirano lažno predstavljanje in usposabljanje

V tej kategoriji se ocenjuje raven ozaveščenosti o kibernetski varnosti v organizaciji, pri čemer se poudarja pomen rednega usposabljanja uporabnikov, simulacij lažnega predstavljanja in uvedbe opozorilnih pasic za zunanja e-poštna sporočila. Zaskrbljujoče je, da **65,5 % nevladnih organizacij v obeh regijah nima pobud za simulacijo lažnega predstavljanja in usposabljanje za ozaveščanje.** To je še posebej zaskrbljujoče, saj so lažno predstavljanje (phishing) glavni vzrok kibernetskih napadov, vendar se zdi, da nevladne organizacije podcenjujejo pomen ozaveščanja in usposabljanja za preprečevanje takšnih incidentov.

Poleg tega **58 % nevladnih organizacij v EU svojim zaposlenim in prostovoljcem ne ponuja usposabljanja o kibernetski varnosti, kar 71 % pa jih ne izvaja simulacij lažnega predstavljanja za vse zaposlene.**. Zaradi pomanjkanja celovitega usposabljanja in pripravljenosti so te organizacije izpostavljene večjim tveganjem, kar kaže na nujno potrebo po izboljšanju izobraževanja in prakse na področju kibernetske varnosti.

2.9 Upravljanje gesel

Na področju sprejemanja rešitev za upravljanje gesel, bodisi s programskimi aplikacijami bodisi s strojnimi napravami za varno shranjevanje in upravljanje gesel zaposlenih, je opazna pomanjkljivost. Približno **36 % nevladnih organizacij v EU in Švici ne upravlja aktivno svojih gesel.**

Kar zadeva posebne prakse, **le 35 % nevladnih organizacij v EU uporablja upravitelja gesel za varno shranjevanje in ravnanje z gesli**. Poleg tega **le 19 % teh organizacij aktivno izobražuje svoje zaposlene o pomenu ustvarjanja edinstvenih in zapletenih gesel**.

2.10 Ozaveščanje o grožnjah in spremljanje

Na tem področju se ocenjuje spremljanje dejavnosti temnega spleta in dnevnikov za odkrivanje kršitev varnosti, anomalij ali nepooblaščenih dejavnosti. Natančneje, spremljanje temnega spleta je postopek aktivnega sledenja in analiziranja spletnih dejavnosti in vsebine v šifriranih in skritih plasteh interneta za prepoznavanje morebitnih varnostnih groženj, nezakonitih dejavnosti ali ukradenih informacij. Spremljanje dnevnikov vključuje neprekinjeno pregledovanje in analiziranje dnevnikov, ki jih ustvarja sistem in v katerih so zabeleženi dogodki in dejavnosti, da bi prepoznali varnostne incidente, anomalije ali morebitne grožnje v omrežju ali okolju IT ter se nanje odzvali. Tako razpoložljivi podatki kažejo, da **35 % nevladnih organizacij s sedežem v EU izvaja dejavnosti ozaveščanja o grožnjah in spremljanja, medtem ko je odstotek švicarskih nevladnih organizacij manjši.**. Vendar pa nadaljnja razčlenitev tega globalnega podatka pokaže, da **81 % nevladnih organizacij v EU še vedno ne spremlja temnega spleta**, medtem ko **61 % pa nima zmogljivosti za spremljanje svojih dejavnosti v dnevnikih**.

2.11 Stanje nevladnih organizacij glede groženj, o katerem so poročali organi LEA/CERT

Zaradi njihovega strokovnega znanja so ocene in komentarji o politikah organov za ukrepanje na področju varnosti in zaščite ter organov za ukrepanje na področju varnosti bistvenega pomena. Njihove ocene zagotavljajo ključne informacije o učinkovitosti varnostnih praks in priporočajo prilagoditve za zmanjšanje tveganj. Te ocene zagotavljajo celovite varnostne preglede, pravno skladnost in pripravljenost na odzivanje na varnostne incidente. V tem kontekstu in na podlagi opravljenih raziskav smo preučili naravo interakcij med temi subjekti in nevladnimi organizacijami, s posebnim poudarkom na poročanju o kibernetskih napadih in odzivanju nanje.

2.11.1 Poročanje nevladnih organizacij organom CERT/LEA

Na vprašanje, ali njihove organizacije sodelujejo z nevladnimi organizacijami v zvezi s kibernetskimi napadi, so bili anketiranci enakomerno porazdeljeni, saj jih je le polovica poročala o takšnih stikih. To kaže, da so nekateri organi CERT in LEA dejavno vključeni v podporo nevladnim organizacijam, medtem ko drugi morda niso vzpostavili uradnih kanalov sodelovanja ali pa se nevladne organizacije odločijo, da o incidentih ne bodo poročale organom CERT in LEA.

2.11.2 Pogostost interakcij

Pri organih CERT/LEA, ki so sodelovale iz nevladnimi organizacijami, je bila pogostost interakcij različna :

- **Tedenske interakcije :** 25 %
- **Mesečne interakcije :** 25 %
- **Redke interakcije (npr. enkrat ali dvakrat na leto) :** 50 %

Ta razpršenost kaže na to, da nekatere skupine CERT/upravičeni organi za delo redno vzdržujejo stike z nevladnimi organizacijami, medtem ko druge sodelujejo bolj občasno. Na to spremenljivost lahko vplivajo viri, ki so na voljo v agenciji, ali obseg prijavljenih incidentov.

2.11.3 Merjenje učinka posredovanj organov CERT/LEA

Na vprašanje, kako merijo učinek svojih posredovanj pri kibernetskih incidentih, o katerih poročajo nevladne organizacije, so anketiranci navedli različne metode :

- **Zmanjšanje pogostosti incidentov :** nekatere agencije kot ključno merilo spremljajo zmanjšanje pogostosti prijavljenih incidentov po njihovem posredovanju.
- **Hitrost obnovitve :** drugi merijo vpliv po tem, kako hitro si nevladne organizacije po incidentu opomorejo in ponovno začnejo normalno delovati.
- **Povratne informacije nevladnih organizacij :** več anketirancev je navedlo, da se pri ocenjevanju uspešnosti svojih ukrepov zanašajo na povratne informacije, ki jih posredujejo nevladne organizacije same.

2.11.4 Prejemanje podatkov o kibernetskih napadih od nevladnih organizacij

Anketirance smo vprašali, ali od nevladnih organizacij prejemajo podatke o kibernetskih napadih :

- Večina anketirancev je navedla, da prejemajo nekatere podatke, čeprav se kakovost in doslednost teh podatkov zelo razlikujeta.
- Pomanjkanje podatkov : Nekateri anketiranci so opozorili, da od nevladnih organizacij ne prejemajo dosledno ustreznih podatkov, zaradi česar jim je težko zagotoviti pravočasno in učinkovito podporo.

2.11.5 Komunikacijski kanali

Organe CERT/LEA, ki so poročali o stikih z nevladnimi organizacijami, smo vprašali tudi o kanalih, po katerih potekajo te komunikacije. Iz odgovorov je razvidno, da dajejo prednost digitalnim komunikacijskim orodjem, in sicer z naslednjo porazdelitvijo :

- **E-pošta :** 50 %
- **Več kanalov (npr. e-pošta, telefon, sestanki) :** 25 %
- **Vsi razpoložljivi kanali :** 25 %

Čeprav je elektronska pošta prevladujoče komunikacijsko sredstvo, so nekateri anketiranci navedli, da uporabljajo več metod za ohranjanje stikov z nevladnimi organizacijami, kar kaže na potrebo po prilagodljivih komunikacijskih strategijah glede na nujnost in naravo incidentov.

Avtorji tega poročila priznavajo, da zgoraj navedeni podatki niso izčrpni. Kljub temu so ustrezen povzetek omejenih kibernetskih zmogljivosti nevladnih organizacij EU v humanitarnem sektorju in poudarjajo potrebo po sistematičnem in standardiziranem zbiranju, analizi in izmenjavi informacij za zagotavljanje boljših odzivov in lažjega mednarodnega sodelovanja.

3. Ranljivosti nevladnih organizacij

Da bi sledile hitremu razvoju digitalne tehnologije, so nevladne organizacije vzpostavile močno spletno prisotnost. Čeprav jim je to nedvomno olajšalo delo in omogočilo globalno širjenje informacij, je hkrati povečalo površino za napade in jih naredilo bolj dovzetne za kibernetske napade. To dokazuje število ranljivosti, ki so bile odkrite pri raziskovanju vseh nevladnih organizacij v raziskovalni skupini. Od **60 jih je bilo analiziranih 56** (3 nevladne organizacije v EU imajo premajhen digitalni odtis, da bi bile zajete v naših pasivnih pregledih, in 1 v Švici). **Med 56 analiziranimi nevladnimi organizacijami so bile pri vseh ugotovljene napačne konfiguracije in varnostne pomanjkljivosti ter ranljivosti[13] programske opreme, ki jo uporabljajo**.

Preverili smo naslednje vrste slabosti in ranljivosti :

- Varnost omrežja in infrastrukture
- Varnost aplikacij in podatkov
- Znane ranljivosti in skladnost

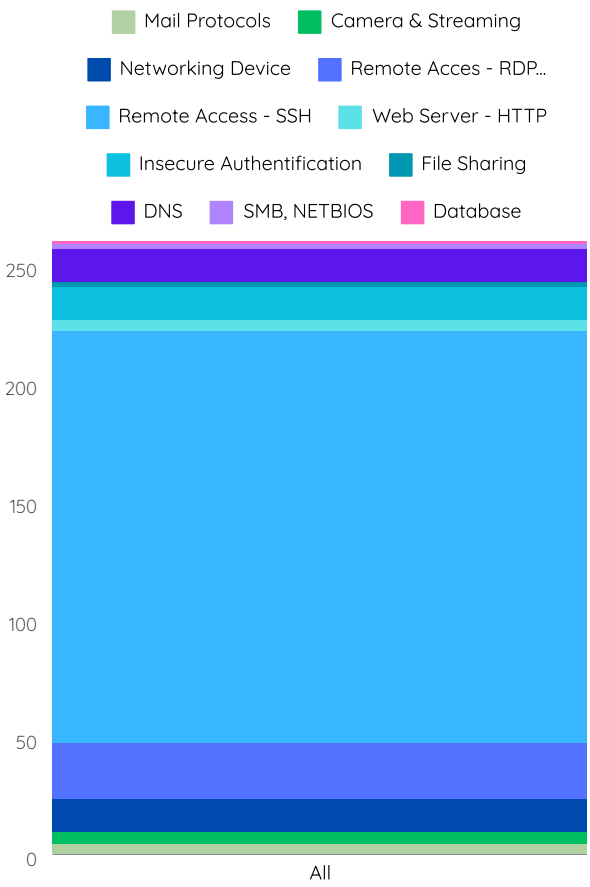
3.1 Varnost omrežja in infrastrukture

Pomanjkljivosti v konfiguraciji omrežne in infrastrukturne varnosti med nevladnimi organizacijami v EU in Švici so večplastne, od težav s šifriranjem do neustreznih varnostnih protokolov. Ugotovljeno je bilo na primer, da je izvajanje razširitev DNSSEC (Domain Name System Security Extensions) zelo pomanjkljivo, saj kar **93 % nevladnih organizacij EU in Švice ni imelo ustreznega DNSSEC zaradi napačno konfiguriranih ali manjkajočih zapisov. Zaradi tega so lahko ranljivi za napade s podtikanjem domen.**.

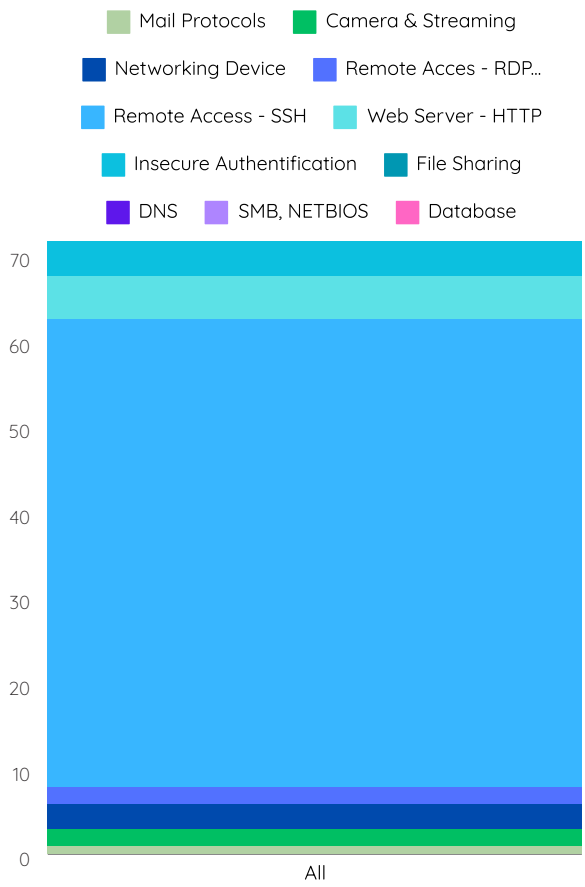
V zadnjem letu **je 8 nevladnih organizacij v EU imelo potekla potrdila SSL**, **6 pa jih je imelo samopodpisana potrdila**, kar je povzročilo ranljivosti pri prenosu podatkov in izpostavilo občutljive informacije morebitnemu prestrezanju in napadom. Poleg tega **uporaba zastarelih protokolov, kot je TLS v1.0**, **ki je bil ugotovljen v 14 nevladnih organizacijah v EU in 14 v Švici, povečuje dovzetnost za napade MiTM (npr. pudelj, zver itd.**)

Čeprav so odprta vrata morda potrebna za delovanje poslovnih aplikacij in storitev, je treba zagotoviti, da nezanesljive ali občutljive storitve niso neposredno izpostavljene, če pa že morajo, so ustrezno nadzorovane in v ozadju varnostnih naprav, kot so požarni zidovi in sistemi WAF. Na žalost **je imelo 24 % nevladnih organizacij EU in skoraj polovica švicarskih nevladnih organizacij potencialno tvegane storitve izpostavljene na odprtih vratih, kot je prikazano na slikah 4 in 5.**.

13 »Skupne ranljivosti in izpostavljenosti,« CVE, **https://cve.mitre.org/**



Slika 4 : Tvegane storitve, odkrite v nevladnih organizacijah v EU



Slika 5 : Tvegane storitve, odkrite v nevladnih organizacijah v Švici

Naše ugotovitve so pokazale, da je bila večina odprtih omrežnih vrat sicer standardnih in pogosto uporabljenih za varne internetne storitve, vendar so **v obeh skupinah izrazito prevladovala nezanesljiva vrata spletnega strežnika HTTP**. To lahko predstavlja tveganje, zlasti če se ta nezanesljiva vrata uporabljajo v povezavi s portali za preverjanje pristnosti, zaradi česar so organizacije izpostavljene napadom MitM (Man-in-the-middle).

Omeniti velja izpostavljenost vrat, ki se uporabljajo za omrežne naprave in kamere, ter pogosto izkoriščena vrata, ki se uporabljajo v kampanjah izsiljevalske programske opreme[14] :

- Protokol oddaljenega namizja (RDP)
- Protokol za prenos datotek (FTP)
- Blok strežniških sporočil (SMB)
- Virtualno omrežno računalništvo (VNC)

14 Napačne konfiguracije in slabosti, ki se uporabljajo v kampanjah izsiljevalske programske opreme | CISA,« Agencija za kibernetsko varnost in varnost infrastrukture CISA. **https://www.cisa.gov/stopransomware/mis-configurations-and-weaknesses-known-be-used-ransomware-campaigns**

3.2 Varnost aplikacij in podatkov

Nevladne organizacije se pogosto zanašajo na spletne aplikacije za bistvene funkcije, kot je izmenjava informacij. Vendar, zaradi napačno nastavljenih glave HTTP in nezanesljivih nastavitev aplikacij lahko te organizacije postanejo odprte za spletne napade. Ta težava je zelo razširjena **od 27 od 29 nevladnih organizacij EU in 25 od 27 švicarskih nevladnih organizacij je imelo manjkajoče ali napačno konfigurirane varnostne glave HTTP.**. Poleg tega **so bile slabosti spletnih aplikacij ugotovljene v 25 nevladnih organizacijah EU in vseh švicarskih nevladnih organizacijah, pri čemer je bila najpogosteje odkrita ranljivost Cross-Site Request Forgery.**. Te ugotovitve opozarjajo na nujno potrebo po boljših praksah spletne varnosti.

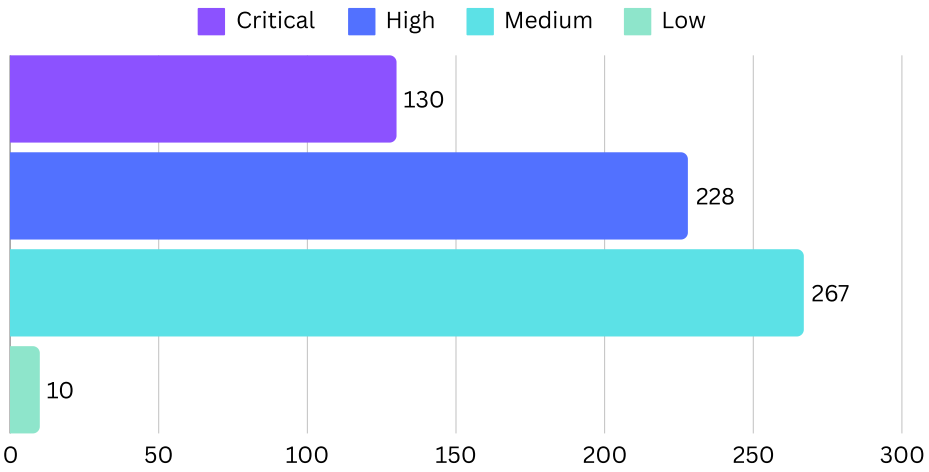
Varnost e-pošte je še eno ključno področje, ki vzbuja skrb. **Kar 83 % nevladnih organizacij v EU in 70 % švicarskih nevladnih organizacij ne izvaja bistvenih ukrepov za varnost e-pošte, kot sta SPF ali DKIM, zaradi česar so bolj dovzetne za ponarejanje e-poštnih domen..** K temu pripomore tudi problem napačno konfiguriranih potrdil, pri čemer se neujemanja gostiteljskih imen pojavljajo pri približno tretjini nevladnih organizacij v EU in skoraj polovici nevladnih organizacij v Švici. Ta neskladja, pri katerih se ime domene certifikata SSL ne ujema z domeno spletnega mesta, povzročijo varnostna opozorila v spletnih brskalnikih, zmanjšujejo verodostojnost spletnega mesta in in opozarjajo na morebitne ranljivosti.

3.3 Znane ranljivosti in skladnost

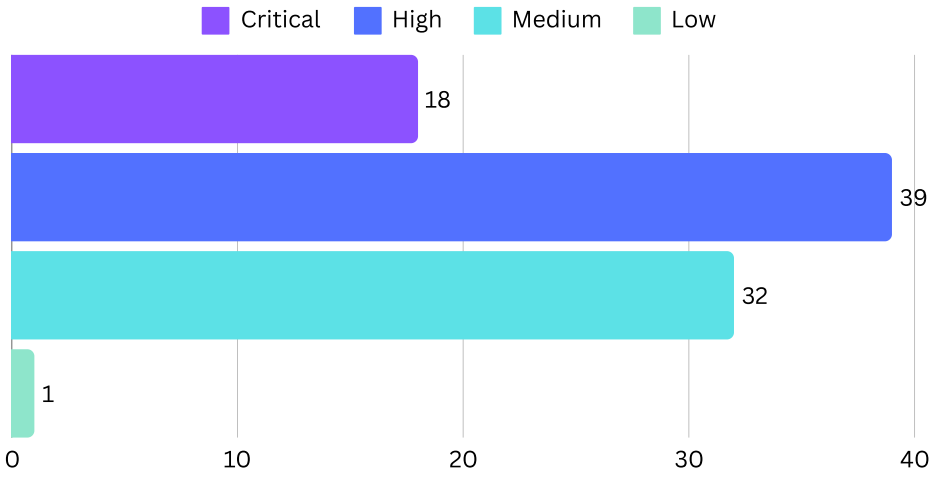
Skupne ranljivosti in izpostavljenosti (CVE)

Na podlagi zbranih podatkov o internetno izpostavljenih sredstvih nevladnih organizacij so različne organizacije za svoje delo uporabljale in še vedno uporabljajo nezanesljive naprave in storitve. Uporaba nepodprte programske opreme in nepopravljenih sistemov izpostavlja nevladne organizacije večjemu tveganju izkoriščanja

s strani akterjev groženj, ki za napade na sisteme uporabljajo skupne ranljivosti in izpostavljenosti (CVE)[15]. Med januarjem 2023 in januarjem 2024 **je bilo v regiji odkritih 637 skupnih ranljivosti in izpostavljenosti (CVE), kar dokazuje, s kakšnimi izzivi na področju kibernetske varnosti se soočajo nevladne organizacije,** pri čemer se večina nanaša na nevladne organizacije iz EU. CVE so bile ugotovljene v napravah, povezanih z internetom, pri natanko petini pregledanih nevladnih organizacij v EU in približno tretjini v Švici. Še bolj zaskrbljujoče je, da je **15 % nevladnih organizacij EU v svoji infrastrukturi potencialno imelo CVE visoke in kritične resnosti (na podlagi osnovne ocene CVSS 7 ali več)[16]**. Če pogledamo samo zadnja dva meseca, naši podatki kažejo, da je 14 % nevladnih organizacij v EU in 30 % švicarskih nevladnih organizacij trenutno potencialno prizadetih zaradi CVE.



Slika 6 : Število CVE, odkritih v nevladnih organizacijah EU, razvrščenih po resnosti.



Slika 7 : Število CVE, odkritih v nevladnih organizacijah CH, razvrščenih po resnosti

15 Spletna stran CVE (Common Vulnerabilities and Exposures). [Na spletu]. Na voljo : **https://www.cve.org/**

16 S. C. Leadership, »Kaj je CVSS - Common Vulnerability Scoring System«, 24. oktober 2023. **https://www.sans.org/blog/what-is-cvss/**

Še bolj zaskrbljujoče je, da **sta dve nevladni organizaciji v EU (in tri v Švici) imeli CVE, ki so na seznamu CISA z znanimi izkoriščanimi ranljivostmi**[17]. Gre za ranljivosti, pri katerih so bili zabeleženi primeri izkoriščanja, kar znatno povečuje tveganje za organizacije.

	EU	CH
CVE ID	CVE-2021-40438 (2 NGO's)	CVE-2021-40438 (2 NGO's)
	CVE-2019-0211 (1 NGO)	CVE-2019-0211 (1 NGO)
	CVE-2019-11043 (1 NGO)	CVE-2020-28949 (1 NGO)
	CVE-2012-1823 (1 NGO)	CVE-2020-13671 (1 NGO)

Tabela 2 : CISA KEV našteva CVE, prisotne v okoljih nevladnih organizacij

Med CVE na seznamu CISA KEV se najpogosteje pojavlja CVE-2021-40438, ki je ranljivost strežnika Apache kritične stopnje[18]. **Zadeva štiri organizacije – po dve v vsaki skupini.**. Tej sledi CVE-2019-0211, zelo resna ranljivost strežnika Apache[19].

O eni ranljivosti na tem seznamu, CVE-2019-11043, so poročali tudi, da je bila uporabljena v kampanjah izsiljevalske programske opreme[20]. To je kritična ranljivost, ki vpliva na zastarele različice PHP in jo je mogoče izkoristiti za oddaljeno izvajanje kode v ciljnih sistemih.

Ugotovljene ranljivosti in varnostni izzivi, s katerimi se soočajo nevladne organizacije, poudarjajo ključno potrebo po okrepljenih ukrepih za kibernetsko varnost. Ker se nevladne organizacije pri uresničevanju svojih nalog in širjenju globalnega vpliva vse bolj zanašajo na tehnologijo, je treba dati prednost zanesljivim varnostnim protokolom za omrežja in aplikacije, biti pozoren na znane ranljivosti in upoštevati najboljše prakse kibernetske varnosti. Odpravljanje teh ranljivosti ni ključnega pomena le za varovanje občutljivih podatkov in zagotavljanje neprekinjenega delovanja, temveč tudi za ohranjanje zaupanja deležnikov in donatorjev. **Tveganja, ki jih predstavljajo te ranljivosti, opozarjajo na možnost incidentov na področju kibernetske varnosti, ki lahko ovirajo delovanje in ogrozijo celovitost dela nevladnih organizacij**. Zato so proaktivno upravljanje tveganj, stalno spremljanje in hitra sanacija bistvene sestavine celovite strategije kibernetske varnosti za zaščito nevladnih organizacij pred razvijajočimi se grožnjami in ublažitev morebitnih vplivov na njihove ključne naloge.

17 Agencija za kibernetsko varnost in varnost infrastrukture CISA, »Known Exploited Vulnerabilities Catalog«. **https://www.cisa.gov/known-exploited-vulnerabilities-catalog?page=1**
18 NVD – cve-2021-40438.« **https://nvd.nist.gov/vuln/detail/cve-2021-40438**
19 NVD – CVE-2019-0211.« **https://nvd.nist.gov/vuln/detail/CVE-2019-0211**
20 CVE-2019-11043 podrobnost,» NIST National Vulnerability Database. [Na spletu]. Na voljo : **https://nvd.nist.gov/vuln/detail/CVE-2019-11043**

4. Kibernetski incidenti nevladnih organizacij

V tem razdelku so obravnavani kibernetski incidenti, ki so prizadeli nevladne organizacije, vključno z javno objavljenimi primeri, podatki, zbranimi v raziskovalnih skupinah, in evidentiranimi uhajanjem poverilnic. Poudarja izzive, s katerimi se soočajo nevladne organizacije, in njihove odzive na kibernetske grožnje ter želi zagotoviti celovit pregled nad kibernetsko varnostjo v tem sektorju. Da bi zagotovili podrobno in dobro raziskano oceno kibernetske varnosti v nevladnih organizacijah, smo na koncu vključili več študij primerov.

4.1 Javno prijavljeni incidenti

Spodnji incidenti temeljijo na raziskavi odprtih virov in ni nujno, da so žrtve del raziskovalne skupine, omenjene drugje v tem poročilu.

Napad na organizacijo SOS Children's Villages International, Avstrija, 2021

Globalna organizacija SOS Children's Villages International s sedežem v Avstriji je bila 18. septembra 2021 žrtev incidenta kibernetske varnosti. Organizacija je takoj ukrepala in izvedla ustrezne protiukrepe, vključno z obveščanjem ustreznih organov in iskanjem pomoči pri zunanjih strokovnjakih za kibernetsko varnost. Ti ukrepi so jim omogočili, da so hitro zaščitili svoje strežnike in do 30. septembra 2021 ponovno vzpostavili normalno delovanje vseh glavnih sistemov. Sledila je temeljita preiskava, ki na srečo ni pokazala nobenih dokazov o pridobivanju, uhajanju ali nepooblaščenem razkrivanju osebnih podatkov. Incident je poudaril pomen strogih praks kibernetske varnosti, zlasti za organizacije, ki obdelujejo občutljive podatke upravičencev, donatorjev, osebja in ponudnikov storitev. Takojšen in učinkovit odziv organizacije SOS Children's Villages International na grožnjo kibernetske varnosti poudarja njeno zavezanost k ohranjanju visokih standardov varnosti podatkov in zasebnosti[21].

Napad z izsiljevalsko programsko opremo na organizacijo Caritas, Nemčija, 2022

Caritas Nemčija je 25. septembra 2022 postala žrtev napada z izsiljevalsko programsko opremo, kar je povzročilo znatne motnje v njenih IT-sistemih. Kljub izzivom se je Caritas odločil, da ne bo plačal odkupnine, ki so jo zahtevali napadalci. Namesto tega so se osredotočili na vzpostavitev alternativne infrastrukture IT, pri čemer so uporabili obstoječe varnostne kopije podatkov. Organizacija je poudarila, da kljub težavam nadaljuje z izvajanjem svojih storitev, s čimer je dokazala odpornost in predanost svojemu namenu[22].

21 SOS Children's Villages International, »Statement on Cyber Security Incident", 6. oktober 2024. [Na spletu]. Na voljo : **https://www.sos-childrensvillages.org/news/statement-on-cyber-security-incident**

22 B2B Cyber Security, »Ransomware Victim Caritas Refuses to Pay«. 25. september 2022. [Na spletu]. Na voljo : **https://b2b-cyber-security.de/en/ransomware-opfer-caritas-will-nicht-zahlen/**

Kibernetski napad na ADAPT, Irska, marec 2022

Društvo ADAPT, služba za pomoč pri nasilju v družini s sedežem v Limericku na Irskem, je 23. marca 2022 doživelo kibernetski napad. Ta napad je povzročil precejšnje motnje v njihovih sistemih IT in delovanju storitev. Organizacija je nemudoma ukrepala in obvestila organe pregona in organe za varstvo podatkov ter poiskala zunanje strokovno znanje s področja IT, da bi odpravila kršitev. Kljub izzivom je ADAPT ostal zavezan nadaljevanju svojih bistvenih storitev za osebe, ki jih je prizadela zloraba v družini[23].

Kibernetski napad na podjetje Rehab, Irska, marec 2022

Skupina Rehab Group, irska organizacija, ki zagotavlja zdravstvene in socialne storitve, je bila marca 2022 žrtev kibernetskega napada. Ta incident je znatno vplival na njihove IT sisteme, kar je povzročilo motnje pri izvajanju storitev. Skupina Rehab je v odgovor izvedla svoj načrt kriznega upravljanja, ki je vključeval obveščanje ustreznih organov in angažiranje strokovnjakov za kibernetsko varnost. Kljub tem izzivom si je organizacija prizadevala zmanjšati vpliv napada na svoje storitve in stranke[24].

Zdravniki brez meja, februar 2022

Februarja 2022 naj bi bila organizacija Médecins Sans Frontières (MSF), znana tudi kot Zdravniki brez meja, tarča hekerjev. Prodajal se je nepooblaščen dostop do omrežja MSF, kar je pomenilo resno kršitev kibernetske varnosti. Ta incident je opozoril na ranljivost celo velikih in uveljavljenih humanitarnih organizacij za kibernetske napade. Takšne kršitve so še posebej zaskrbljujoče zaradi občutljive narave podatkov, ki jih hranijo organizacije, kot je MSF[25].

Laboratorij EU Disinfo Lab, Belgija, 2020

EU Disinfo Lab, neprofitna organizacija, ki se ukvarja z analizo dezinformacijskih kampanj proti EU, je bil 20. julija 2020 žrtev napada DDoS (Distributed Denial of Service (Distribuirana zavrnitev storitve)). Zaradi tega kibernetskega napada je bilo njihovo spletno mesto več ur brez povezave. Nevladna organizacija je incident opisala kot »kibernetski napad z grobo silo«, vendar so člani osebja domnevali, da je šlo za napad DDoS. Napad opozarja na vse večje grožnje, s katerimi se soočajo organizacije, ki se ukvarjajo z digitalno varnostjo informacij[26].

23 Limerick Leader, »Limerick Domestic Abuse Charity Targeted in Cyber Attack,« 23. marec 2020. [Na spletu]. Na voljo : **https://www.limerickleader.ie/news/home/773188/limerick-domestic-abuse-charity-targeted-in-cyber-attack.html**

24 The Irish Times, »Rehab Group Falls Victim to Cyber Attack,« 16. marec 2022. [Na spletu]. Na voljo : **https://www.irishtimes.com/business/technology/rehab-group-falls-victim-to-cyber-attack-1.4828860**

25 Forbes, »Hackers Sell Access to a $2 Billion Nonprofit, a Californian Hospital, and Michigan Government« 23. februar 2022. [Na spletu]. Na voljo : **https://www.forbes.com/sites/thomasbrewster/2022/02/23/hackers-sell-access-to-a-2-billion-nonprofit-a-californian-hospital-and-michigan-government/?sh=33a007dc5758**

26 Tech Monitor, »EU Disinfo Lab in DDoS Attack,« 20. julij 2020. [Na spletu]. Na voljo : **https://techmonitor.ai/technology/cybersecurity/eu-disinfo-lab-in-ddos-attack**

Akadem, Francija, september 2023

Akadem, digitalna platforma sklada Fonds Social Juif Unifié (FSJU), je v noči s 25. na 26. september 2023 doživela napad izsiljevalske programske opreme. Ta kibernetski napad se je zgodil na Yom Kippur, pomemben židovski praznik. Napad je povzročil nedostopnost spletišča Akadem, kar je pomenilo resno motnjo v njihovih storitvah[27].

Transparency International, Nemčija, 2019

Leta 2019 se je organizacija Transparency International soočila s šest tednov trajajočim prefinjenim napadom z lažnim predstavljanjem. Napad je bil zaznan zaradi večjega števila neuspešnih poskusov prijave v njihove račune Microsoft Office in je vključeval tako množične poskuse prijave kot tudi ciljno usmerjeno lažno predstavljanje (spear phishing). E-poštna sporočila z lažnim predstavljanjem so posnemala slog pisanja višjega vodstva, kar je vzbujalo sum, da bi si lahko napadalci ogledali notranjo komunikacijo. Microsoftova opozorila so kljub večfaktorskemu preverjanju pristnosti kazala na vdore v dva računa zaposlenih. Ekipa IT, ki ji je pomagalo podjetje za kibernetsko varnost, je ugotovila, da je napad morda izviral iz državnih virov, pri čemer je šlo za podtikanje domen in domnevno uporabo zapletene vohunske programske opreme. Napadi so se po šestih tednih nepričakovano ustavili, organizacija pa se je začela bolje zavedati groženj kibernetske varnosti. Zanimivo je, da so organizacije v času incidenta razpravljale o tem, ali naj incident prijavijo organom pregona, in se na koncu odločile, da ga ne bodo[28].

---

27 L'Informe, »Les dessous de la cyberattaque contre Akadem, le site du Fonds Social Juif Unifié,« [Na spletu]. 4. oktober 2023. Na voljo : **https://www.linforme.com/tech-telecom/article/les-dessous-de-la-cyberattaque-contre-akadem-le-site-du-fonds-social-juif-unifie_1051.html**

28 Solidarity Action Network, »Resisting Sustained Phishing Attacks,« [Na spletu]. Na voljo : **https://solidarityaction.network/wp-content/uploads/resisting-sustained-phishing-attacks.pdf**

V Švici je o kibernetskih incidentih javno razpravljalo še manj nevladnih organizacij.

ICRC, Švica, januar 2022

Mednarodni odbor Rdečega križa (ICRC) je januarja 2022 doživel prefinjen kibernetski napad, ki je ogrozil strežnike z osebnimi podatki več kot 515.000 ljudi po vsem svetu. Kršitev podatkov je vključevala občutljive podatke posameznikov, ki jim je Mednarodni odbor Rdečega križa pomagal, kot so pogrešane osebe in njihove družine, priporniki ter drugi, ki so jih prizadeli konflikti in nesreče. Napad je bil napreden, saj je uporabljal posebna hekerska orodja in tehnike, ki so se izogibale standardnemu odkrivanju. Mednarodni odbor Rdečega križa je nemudoma sprejel ukrepe za odpravo kršitve, povečanje varnosti in pomoč prizadetim posameznikom[29].

Insecurity Insight, Švica, 2022

Švicarska neprofitna organizacija Insecurity Insight je po poročanju o ruskih napadih na ukrajinske bolnišnice doživela velik incident kibernetskega nadlegovanja. Zaposleni so na svoje telefone prejeli številna ribarska sporočila in neprimerno vsebino, kar je bilo za organizacijo doslej nezaslišanega obsega. Christina Wille, direktorica filma, meni, da je bil to poskus ustrahovanja njene ekipe, da ne bi nadaljevala z dokumentiranjem posledic vojne v Ukrajini. Kljub tem poskusom kibernetski napadi niso preprečili njihovih prizadevanj za poročanje[30].

29 Mednarodni odbor Rdečega križa (ICRC), »Kibernetski napad na Mednarodni odbor Rdečega križa : Kaj vemo,« [Na spletu]. Na voljo : **https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know**

30 CNN, »Humanitarian aid to Ukraine disrupted by cyberattacks«. 23. april 2022 [Na spletu]. Na voljo : **https://edition.cnn.com/2022/04/23/politics/humanitarian-aid-ukraine-war-cyberattacks/index.html**

4.2 Zbrani podatki o incidentih v raziskovalni skupini

Če posebej preučimo **raziskovalno skupino 60 nevladnih organizacij, bi lahko nekatere kibernetske incidente odkrili s pomočjo merljivih podatkov, ki jih je mogoče najprej pridobiti prek prometa sinkholed c2**. Sinkholing je tehnika kibernetske varnosti, ki se uporablja za preusmerjanje prometa iz napadenega omrežja ali zlonamernih končnih točk na nadzorovan strežnik, t. i. »strežnik sinkhole«. Glavni namen sinkholinga je prekiniti grožnjo, ki jo predstavljajo zlonamerna programska oprema, botneti in druge zlonamerne dejavnosti. Varnostni raziskovalci ali omrežni skrbniki prepoznajo zlonamerna imena domen ali naslove IP, ki se uporabljajo za nadzor ogroženih sistemov, kot so strežniki C&C (command and control) botnetov, in nato konfigurirajo usmerjanje DNS ali IP za preusmerjanje prometa iz teh prepoznanih zlonamernih končnih točk na strežnik »sinkhole«. Strežnik »sinkhole« se na zahteve ne odzove tako, kot bi se odzval zlonamerni strežnik, s čimer učinkovito prekine komunikacijo med okuženimi napravami in nadzornimi strežniki. S tem se okuženim napravam prepreči prejemanje zlonamernih navodil, raziskovalcem pa se omogoči zbiranje podatkov o okuženih sistemih, kot so naslovi IP. Z njimi je mogoče analizirati vzorec napada, obseg okužbe in morebiti obvestiti prizadete strani. Ta metoda omogoča **identifikacijo dveh nevladnih organizacij v EU in ene v Švici, ki sta bili verjetno okuženi, in sicer s primerjavo naslovov IP in uporabniških računov teh nevladnih organizacij, ki so povezani z internetom ali zunanjim prebegom, s podatki iz platform za obveščanje o kibernetskih grožnjah. Z raziskovanjem temnega spleta smo lahko potrdili tudi, da so bile poverilnice ukradene precejšnjemu številu nevladnih organizacij**. Poglejmo si pobliže.

Naprave, okužene z zlonamerno programsko opremo

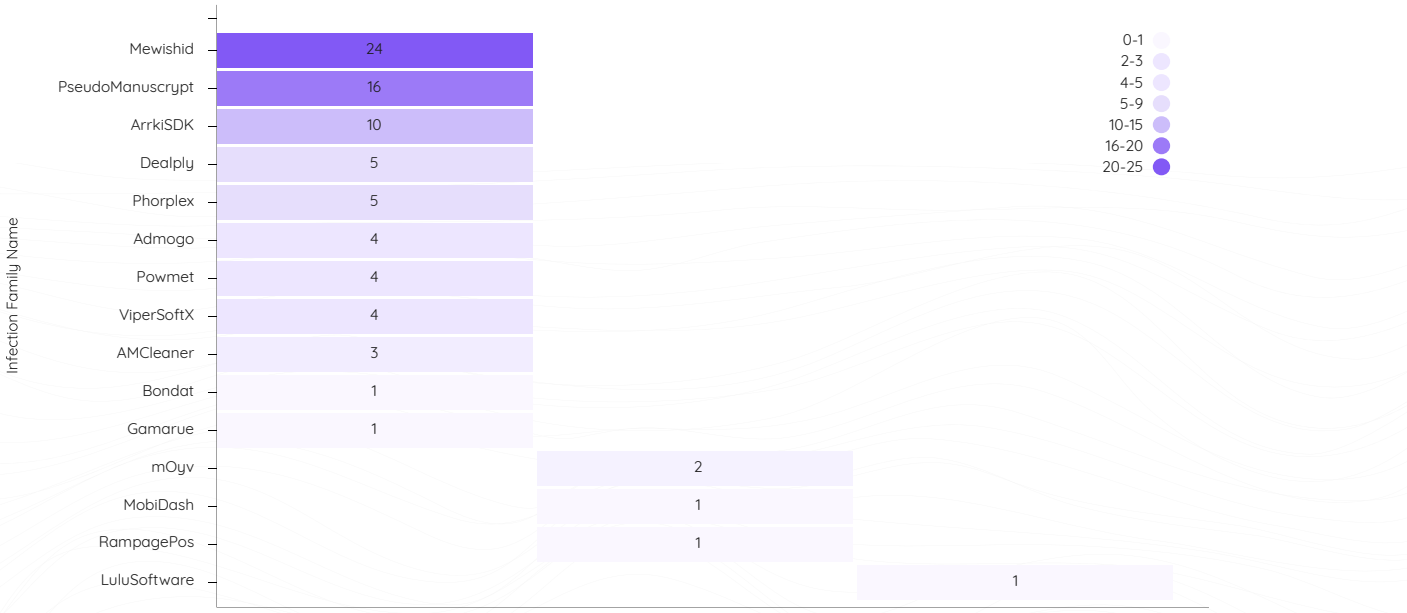
Številne oblike zlonamerne programske opreme temeljijo na domenah ali strežnikih, ki jih nadzorujejo napadalci. Te infrastrukture se običajno imenujejo infrastruktura poveljevanja in nadzora. Ko je zlonamerna programska oprema dostavljena v napravo in se izvrši, se pogosto zgodi, da vzpostavi povezavo s strežnikom ali domeno c2 za nadaljnja navodila ali za pridobitev dodatnega plačilnega bremena.

V tem primeru smo pridobili podatke o sumljivem odhodnem prometu iz okolja nevladnih organizacij na zunanje lokacije, povezane z znanimi infrastrukturami poveljevanja in nadzora, ki kažejo, da je naprava poskušala vzpostaviti komunikacijo c2 ali »poklicati domov« – ta metoda zbiranja podatkov se običajno imenuje »sinkholed c2 promet«.

V obdobju od januarja 2023 do 2024 je bil promet c2, ki je nakazoval okužene naprave, zabeležen 83-krat. **V EU sta sodelovali dve nevladni organizaciji, v Švici pa le ena. Promet je izhajal iz skupno 13 zunanjih IP-jev iz 9 držav**, kot je razvidno iz tabele 3.

	# Detected Traffic Events	#Malware Types	# NGOs	# Infected Assets	# Source Countries
EU	81	14	2	12	8
CH	1	1	1	1	1
Total	82	15	3	13	9

Ugotovljenih je bilo 15 družin zlonamerne programske opreme, kot je razvidno iz slike 8. Vsak stolpec predstavlja dogodke, ki so bili zabeleženi v organizaciji, v grafu pa ni prikazano prekrivanje sevov zlonamerne programske opreme med organizacijami. MewishID (oglaševalska programska oprema), ki mu sledi PseudoManuscrypt (vohunska programska oprema). **Mewishid je vrsta tvegane programske opreme/oglasne programske opreme, ki bi lahko potencialno izkoristila sistemske vire na moteč ali nezaželen način, kar predstavlja potencialno varnostno tveganje**[31]. **PseudoManuscrypt je vrsta vohunske programske opreme, ki napadalcu omogoča pridobitev oddaljenega dostopa do okuženega sistema in izločanje občutljivih informacij, kot so poverilnice VPN**[32]. Običajno se prenaša prek piratske programske opreme ali lažnih namestitvenih datotek. Čeprav zlonamerna programska oprema ni bila pripisana določenemu akterju, je v veliki meri prizadela industrijske in vladne organizacije ter ima značilnosti, **povezane z dejavnostjo APT 41 in zlonamerno programsko opremo Manuscrypt, ki jo je uporabljala skupina Lazarus**[33].



Slika 8 : Toplotni zemljevid : število zaznanih zlonamernih prometnih sporočil v treh žrtvah

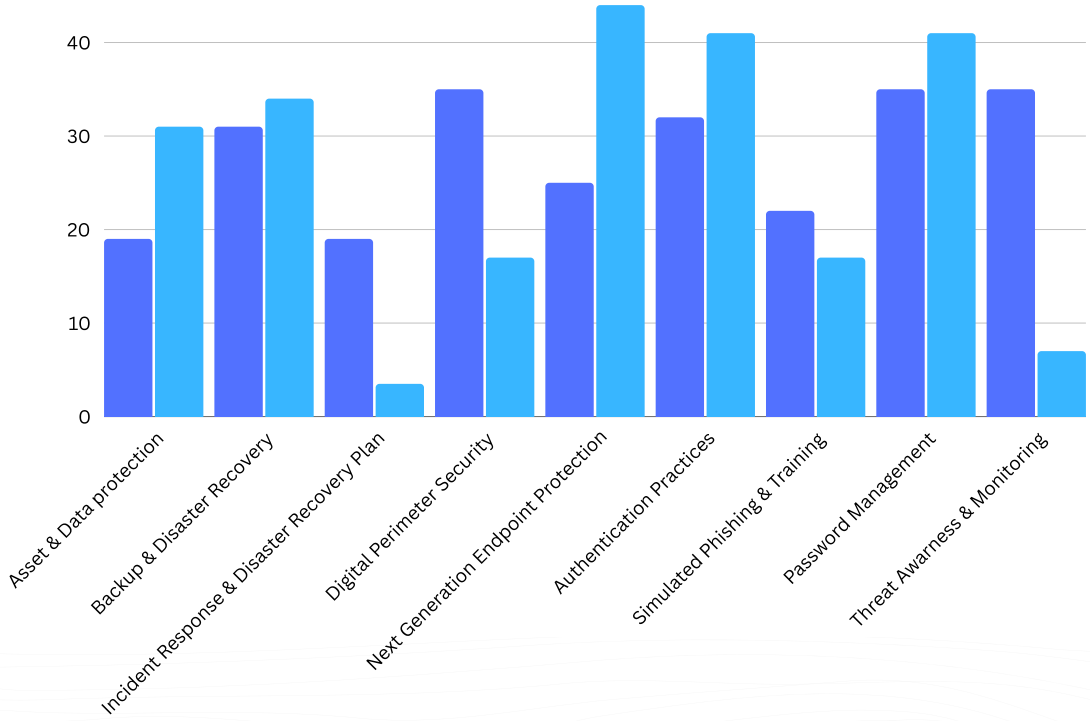
31 Fortiguard, »Riskware/Mewishid«, [Na spletu]. Na voljo : **https://www.fortiguard.com/encyclopedia/virus/7294236**

32 Malpedia, »win.pseudomanuscrpyt«, [Na spletu]. Na voljo : **https://malpedia.caad.fkie.fraunhofer.de/details/win.pseudo_manuscrypt**

33 ThreatPost, »PseudoManuscrypt' Mass Spyware Campaign Targets 35K Systems«. 16. december 2021. [Na spletu]. Na voljo : **https://threatpost.com/pseudomanuscrypt-mass-spyware-campaign/177097/**

Največ prometa, kot je prikazano na sliki 9, je ustvarila vohunska programska oprema PseudoManuscrypt. To je lahko posledica ponavljajočih se okužb ali ponavljajočih se poskusov klicanja domov iz okuženih naprav. Drugi pomembni sevi zlonamerne programske opreme so bili :

- **Gamarue :** tega črva, ki se običajno prenaša prek izmenljivih naprav, je v preteklosti že uporabila vsaj ena skupina APT za krajo informacij in namestitev dodatne zlonamerne programske opreme.[34].
- **M0yv :** čeprav sta bila odkrita le dva poskusa klica na domači računalnik, je prisotnost tega namestitvenega programa omembe vredna, ker ga je razvijalec izsiljevalske programske opreme Maze že uporabljal [35].

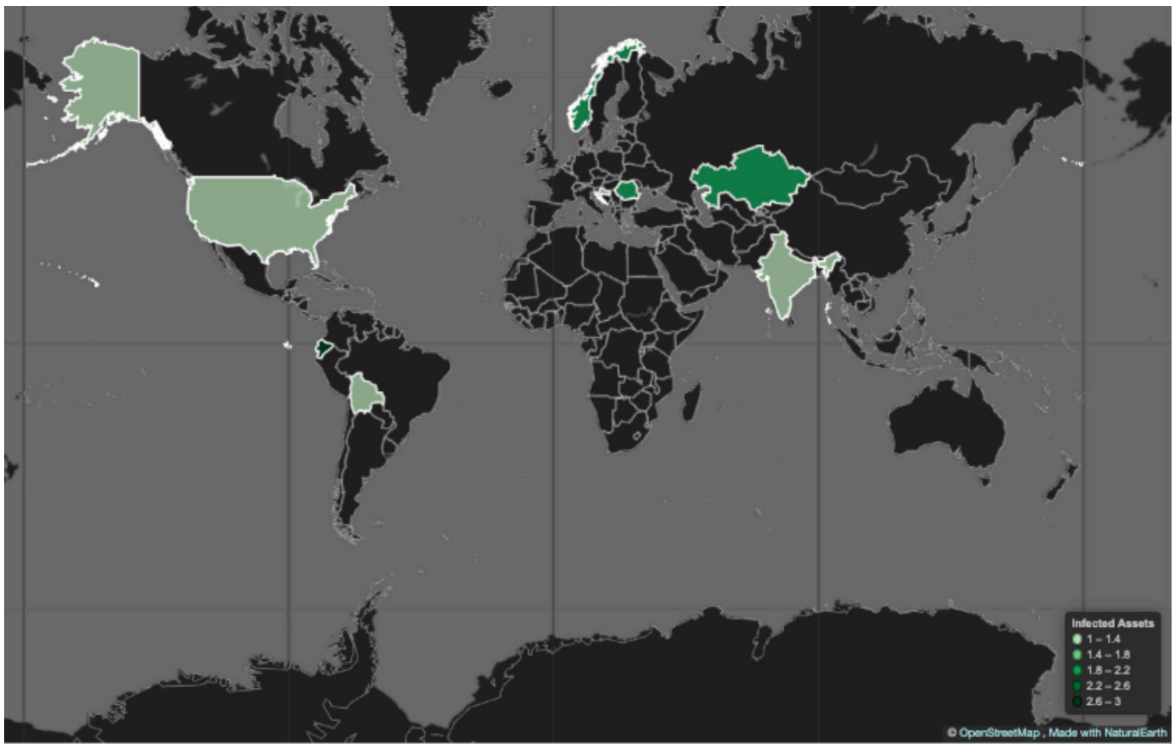


Slika 9 : EU Število prometa okužb po kategorijah

Z geolokacijskimi podatki o naslovih IP je bilo mogoče kartirati, od kod izvira promet. V skupini EU, kot je prikazano na sliki 10, **je promet, ki kaže na okužene naprave, izviral predvsem iz Ekvadorja (19,8 %), sledijo Hrvaška (13,3 %), Kazahstan (13,3 %), Norveška (13,3 %), Romunija (13,3 %), ZDA (13,3 %), Indija (6,7 %), Bolivija (6,7 %) : zlonamerni promet, povezan z nevladnimi organizacijami EU, je posledica globalnega delovanja nekaterih nevladnih organizacij**.

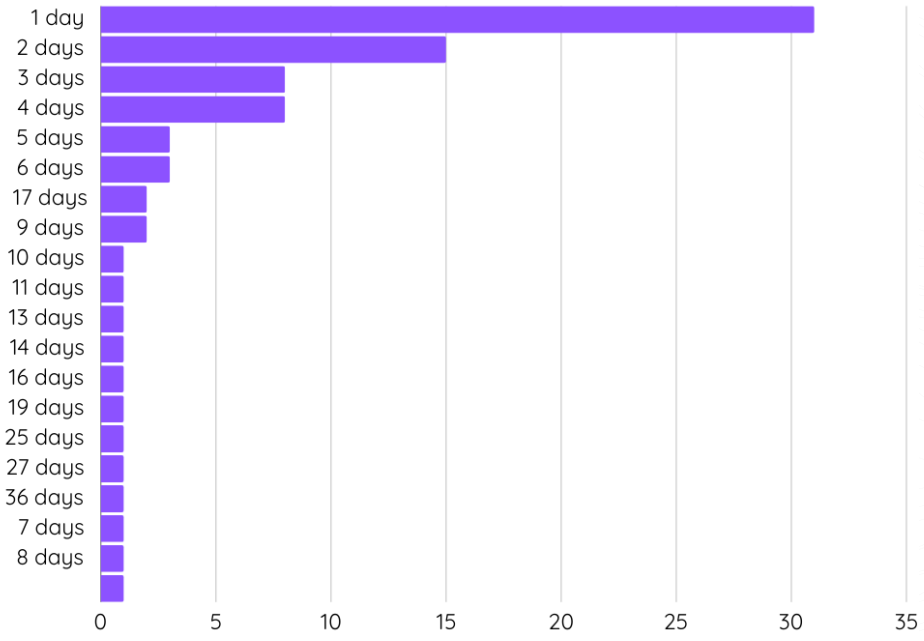
34 Red Canary, »Gamarue«, [Na spletu]. Na voljo : **https://redcanary.com/threat-detection-report/threats/gamarue/**

35 Malpedia, »win.m0yv«, [Na spletu]. Na voljo : **https://malpedia.caad.fkie.fraunhofer.de/details/win.m0yv**



Slika 10 : Lokacije izvora okužbe v EU

V zadnjem letu je večina okužb klicala domov manj kot 4 dni, vendar so se ponavljajoči poskusi povezave, ki so kazali na vztrajno okužbo, nadaljevali **do 36 dni**, kot je prikazano na sliki 11. Večina okužb se je pojavila v zadnji polovici leta 2023, največ med avgustom in novembrom 2023, kar je v veliki meri posledica prometa, ki je nastal zaradi okužbe z vohunsko programsko opremo, ki se je razširila z enega zunanjega IP v nevladni organizaciji v skupini EU.



Slika 11 : Štetje trajanja klica na dom

4.3 Razkrite poverilnice

Po podatkih raziskave družbe Verizon so bila ukradena pooblastila pomembna pri **49 % kršitev, ki so jih povzročili zunanji akterji**, zaradi česar je kraja pooblastil ena od sredstev, ki jih kibernetski kriminalci najbolj iščejo[36]. Ti uporabljajo različne taktike, vključno z usmerjenimi napadi z lažnim predstavljanjem, zlonamerno programsko opremo za krajo poverilnic in pridobivanjem poverilnic iz prosto dostopnih kombiniranih seznamov ali zbirk podatkov, kupljenih prek posrednikov začetnega dostopa. Odtekanje teh poverilnic predstavlja kritično težavo, ki zahteva nujno pozornost. Ne le, da lahko privede do nepooblaščenega dostopa, zlasti če ni večfaktorske avtentikacije, temveč lahko kibernetskim kriminalcem omogoči tudi dragocen vpogled v njihove tarče. Te informacije je mogoče izkoristiti za izogibanje varnostnim ukrepom, vključno z MFA, in dostop do drugih storitev, saj se gesla pogosto ponovno uporabljajo na različnih platformah.

Inštitut CyberPeace Institute je na podlagi podatkov iz globokih in darknetnih virov opravil analizo, da bi ugotovil vse primere, ko so bili uporabniški računi nevladnih organizacij izpostavljeni na platformah za kibernetski kriminal in visoko tvegane platforme, bodisi za izmenjavo bodisi za prodajo. Rezultati so pokazali, da so med januarjem 2023 in januarjem 2024 **nepooblaščene osebe pridobile in razkrile vsaj en uporabniški račun 70 % nevladnih organizacij EU in 82 % švicarskih nevladnih organizacij. 389 prijavnih podatkov, objavljenih na 31 razkritih seznamih, povezanih z dnevniki krajišč, je bilo povezanih z več kot polovico nevladnih organizacij v skupini EU.**

V Švici je bilo stanje še slabše, **saj je bilo v 34 razkritih zbirkah podatkov, in povezanih z dnevniki krajišč, objavljenih 557 računov, kar je zadevalo skoraj dve tretjini nevladnih organizacij v švicarski skupini**. To sicer ne pomeni, da so razkrite poverilnice izkoristili kibernetski kriminalci ali da bi jih celo lahko izkoristili, vendar je to zaskrbljujoče iz dveh razlogov. Prvič, vemo, da le približno polovica nevladnih organizacij v raziskavi uporablja večfaktorsko preverjanje pristnosti. Drugič, velika večina jih ne spremlja uhajanja poverilnic; ne le da se večinoma ne zavedajo grožnje, polovica se jih tudi ne zaščiti pred nepooblaščenim dostopom. To pomeni, da bi lahko kibernetski kriminalci pridobili dostop, ne da bi številne nevladne organizacije za to sploh vedele.

36 Verizon. »Poročilo o preiskavah kršitev podatkov«. 2023. [Na spletu]. Na voljo : **https://www.verizon.com/business/resources/reports/dbir/**

4.4 Študije primerov

V okviru programa **CyberPeace Builders program**, ki povezuje prostovoljce s področja kibernetske varnosti z nevladnimi organizacijami, je več nevladnih organizacij v EU in Švici izmenjalo informacije o preteklih ali tekočih incidentih na področju kibernetske varnosti. Dva od njih sta bila javno dokumentirana. Dodatna je bila anonimizirana in je predstavljena v nadaljevanju. Vsaka študija primera bo vsebovala informacije o primeru, obveščevalne podatke, ki so bili v tistem času na voljo in bi jih bilo mogoče deliti, če bi takrat obstajala platforma za poročanje o incidentih, ter analizo teh informacij, predstavljeno z uporabo diamantnega modela.

Diamantni model analize vdorov je konceptualni okvir, ki se v kibernetski varnosti uporablja za analizo in razumevanje kibernetskih napadov. Ta model je bil razvit, da bi zagotovil bolj strukturiran in celovit način obravnavanja kibernetskih vdorov, ki presega enostavnejše pristope, ki so se običajno uporabljali prej. Diamantni model se osredotoča na povezave med štirimi ključnimi značilnostmi vdora :

- **Nasprotnik :** predstavlja subjekt, ki je odgovoren za kibernetski napad. Razumevanje nasprotnika, njegovih zmogljivosti, namenov in virov lahko omogoči vpogled v motive napada in morebitne naslednje korake.

- **Sposobnost :** gre za orodja, tehnike in metode, ki jih nasprotnik uporablja za izvedbo napada. Analiza zmogljivosti lahko pomaga pri ugotavljanju narave grožnje in razvoju obrambnih ukrepov.

- **Infrastruktura :** to vključuje fizične in virtualne vire, ki jih nasprotnik uporablja za izvedbo napada, kot so strežniki za poveljevanje in nadzor zlonamerne programske opreme, ter omrežja, ki se uporabljajo za komunikacijo. Poznavanje infrastrukture lahko pomaga pri odkrivanju in blaženju napadov.

- **Žrtev :** to je cilj napada, ki je lahko posameznik, organizacija ali sistem. Poznavanje žrtve in razumevanje, zakaj je bila žrtev tarča, lahko pomaga pri prepoznavanju morebitnih prihodnjih tarč in krepitvi obrambe.

Diamantni model poudarja medsebojno povezanost teh štirih elementov, kar pomeni, da lahko razumevanje enega izboljša razumevanje drugih. Posebej uporaben je za obveščevalne podatke o grožnjah in varnostno analizo, saj analitikom pomaga sestavljati informacije o tem, kako in zakaj je prišlo do napada, napovedovati prihodnje grožnje in razvijati učinkovite protiukrepe.

4.4.1 Primer 1 : Napad na belgijsko nevladno organizacijo z lažnim predstavljanjem (angl. Spear-phishing)

Informacije o primeru

Laboratorij EU Disinfo Lab, ki je bil tarča napada DDoS že leta 2020, je bil leta 2022 tarča kampanje "spear-phishing", ki je izkoristila kršitev v USAID, zaupanja vrednem vladnem donatorju v ZDA. **Cilj tega napada je bilo 149 nevladnih organizacij po vsem svetu.** Kot smo poročali že leta 2022 : V e-poštnem sporočilu, prikazanem spodaj, so bili prejemniki pozvani, naj kliknejo na povezavo. Pri tem so naprave žrtev prenesle del zlonamerne kode, ki je napadalcu omogočila trajen dostop do njihovega računalnika in omogočila »doseganje ciljev, kot so bočni premik, odtujitev podatkov in pošiljanje dodatne zlonamerne programske opreme«.[37]. Microsoft je ta napad pripisal skupini Nobelium, ki stoji za napadom na SolarWinds v letu 2020[38].

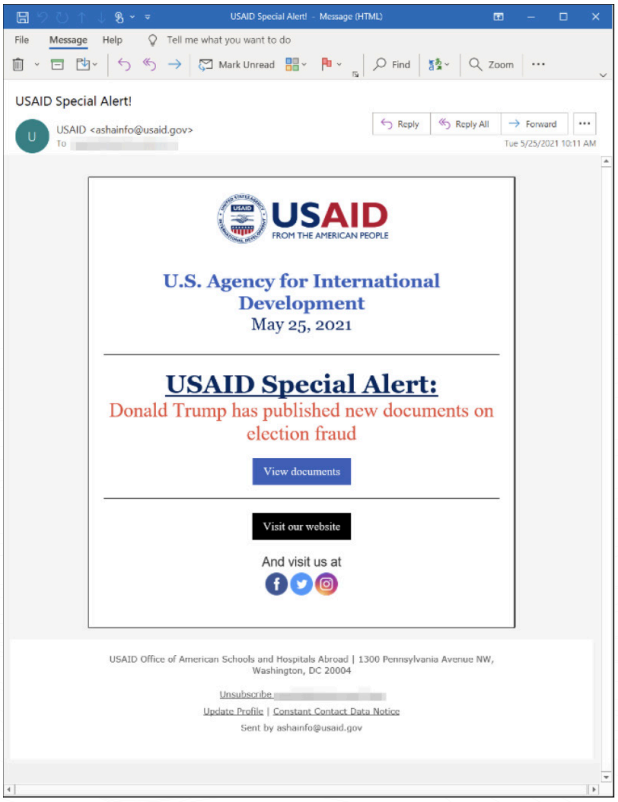
Razpoložljive obveščevalne informacije

Podrobnosti o različnih vrstah obveščevalnih podatkov, predstavljenih v nadaljevanju, so navedene v Dodatku II.

Kontekstualna inteligenca

- **Strateško obveščanje o grožnjah :** izhajajo iz izmenjave informacij z generalnim direktorjem enega od ciljne skupine kampanje »spear-phishing« – napredne prakse v zvezi s komunikacijo po elektronski pošti, visoka ozaveščenost o tveganjih za lažno predstavljanje in naprednih trajnih grožnjah, namenjenih nevladnim organizacijam, napredni varnostni postopki, vključno z močnimi politikami varnostnega kopiranja podatkov, visoka raven zrelosti kibernetske varnosti, čeprav je bila v času incidenta večinoma nedokumentirana.

- **Taktično obveščanje o grožnjah :** poznavanje prejšnjega ciljno usmerjenega napada DDoS in sumov vladnega vohunjenja.



Slika 12 : Elektronska pošta, ki jo je laboratorij EU Disinfo Lab prejel leta 2022

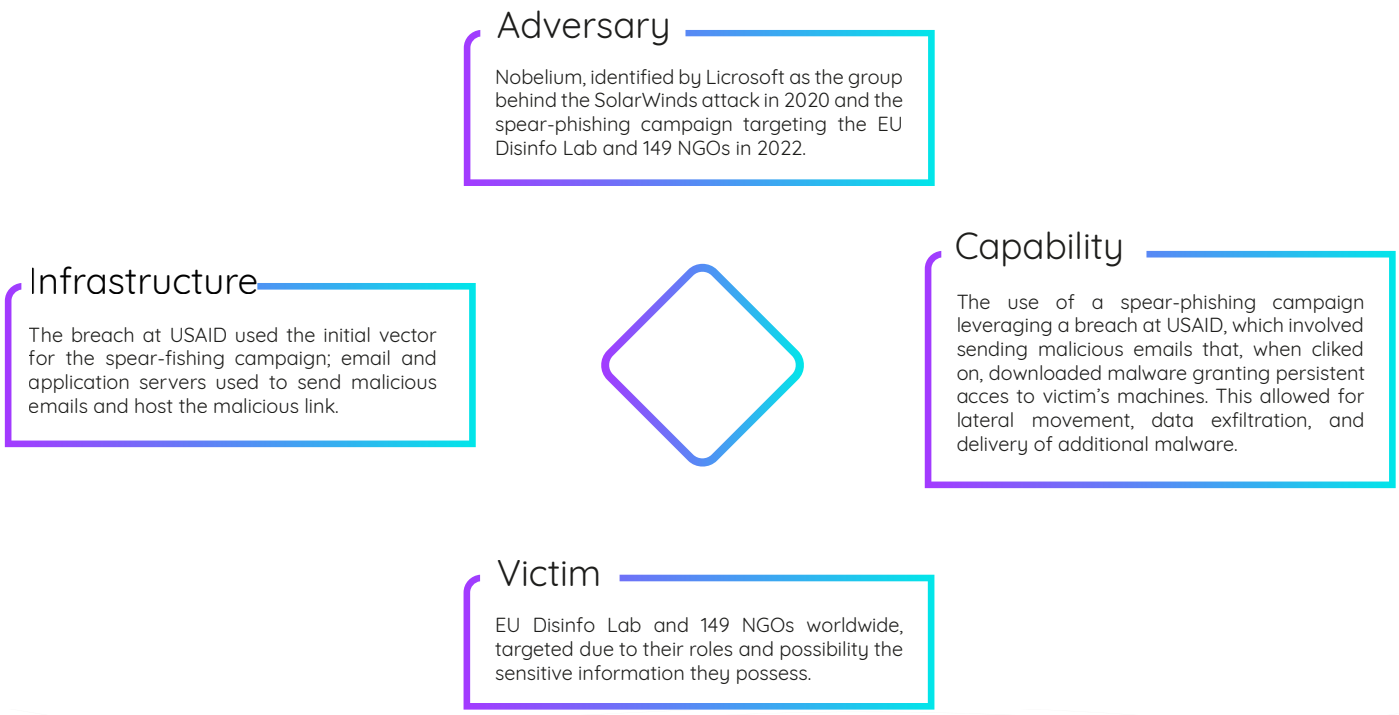
37 CyberPeace Institute, »Neprofitna organizacija tarča kibernetskega napada : Valuable Lessons for You«. 23. julij 2021. [Na spletu]. Na voljo : **https://cyberpeaceinstitute.org/news/non-profit-organization-targeted-by-cyberattack-valuable-lessons-for-you/**

38 Microsoft Security, »New sophisticated email-based attack from Nobelium«. 27. april 2021 [Na spletu]. Na voljo : **https://www.microsoft.com/en-us/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/**

Obveščevalne informacije za posamezne incidente

• **Tehnični podatki o grožnjah :** samo surovi podatki - e-poštni naslov pošiljatelja, vsebina e-poštnega sporočila in značilnosti zlonamerne povezave. Na voljo so dnevniki e-pošte in aplikacij.

• **Obveščanje o operativnih grožnjah :** v času incidenta ni bilo na voljo, vendar je bilo kmalu zatem v podrobnem poročilu Microsofta navedeno pripisovanje in TTP.

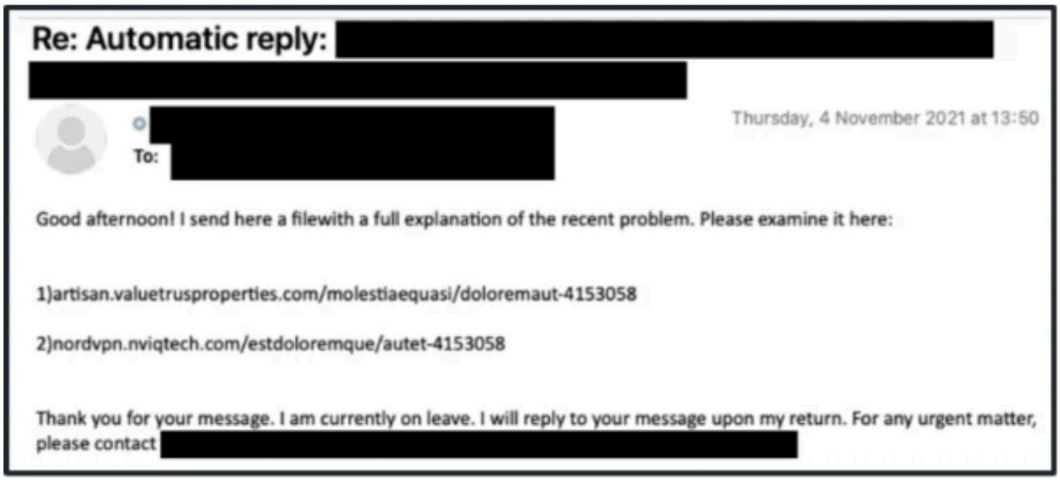


Diamantni model za posamezen primer

4.4.2 Primer 2 : Ogrožanje imenika Active v švicarski nevladni organizaciji

Informacije o primeru

Na drugi incident, ki je prizadel švicarsko nevladno organizacijo, smo bili opozorjeni leta 2021. Kot smo poročali že takrat : inštitut CyberPeace Institute je 4. novembra začel opažati nenavadna e-poštna sporočila, ki so prihajala od resničnih oseb in so jih strežniki potrdili kot pristna. Tipična vsebina teh e-sporočil je sestavljena kot odgovor na obstoječo razpravo in je običajno napisana v istem jeziku. Običajno se začne s kratkim pozdravom in usmeri na dva naslova URL. E-poštno sporočilo se konča z vsebino iz prvotne niti.



Slika 13 : Vzorec e-poštnega sporočila (prečiščeno)

Z analizo glave e-pošte je bilo mogoče ugotoviti, da so bila e-poštna sporočila poslana z legitimnih računov in s pravih strežnikov subjektov, od katerih naj bi izvirala.

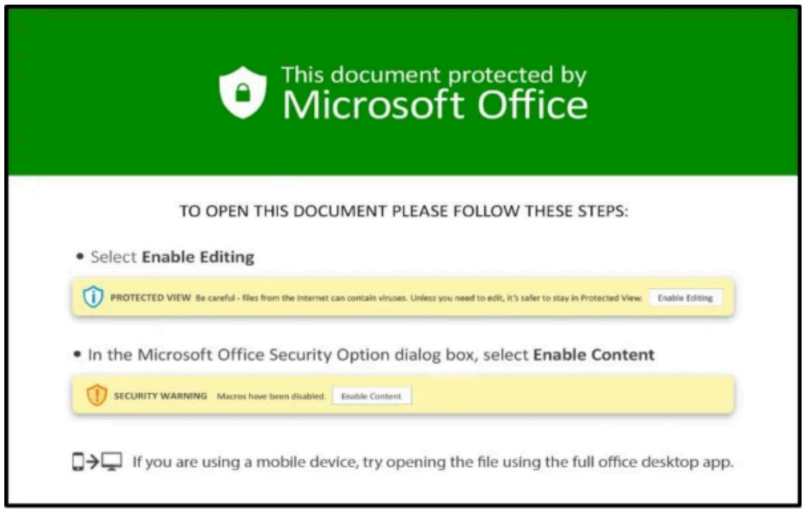
Inštitut CyberPeace Institute je prek alternativnega komunikacijskega kanala takoj stopil v stik z ogroženimi nevladnimi organizacijami, ki so potrdile, da elektronska sporočila niso bila legitimna in da so bili strežniki ogroženi. Inštitut je lahko analiziral prve korake širjenja kampanje v urah, ki so sledile prvemu zaznavanju, opozoril partnerje in zagotovil podporo ogroženim subjektom pri odpravljanju posledic nesreče, izmenjavi informacij in spremljanju razmer.

Med akterji na področju kibernetske varnosti se je splošno znanje o kampanji začelo širiti 8. novembra, 9. novembra pa je Microsoft Defender prvo stopnjo koristnega bremena označil kot zlonamerno. Vsaj ena žrtev pa je bila prizadeta že v začetku novembra.

Koristni tovor na prvi stopnji

Naša ekipa je opravila digitalno forenziko in obratno inženirstvo pri napadu. Zato je bilo mogoče podrobno razumeti, kako pride do okužbe.
Povezave v e-poštnem sporočilu vodijo do datoteke zip, ki vsebuje Excelov list (.xls). Če skripte v programu Excel niso omogočene, bo uporabnik pozvan, da jih omogoči.

Skripta nato prenese več zlonamerne vsebine z ogroženih spletnih strani tretjih oseb, datoteke spusti v mapo **C : \DATOP** *osebnem računalniku uporabnika, ki je prejel e-poštno sporočilo, in spremeni nekaj ključev registra, tako da je zlonamerna vsebina trajna ob vsakem odprtju programa Microsoft Office.. Zato lahko zlonamerna vsebina deluje samo v sistemih Windows (ključi registra so izključno v sistemu Windows). Izvajanje zlonamerne skripte je za uporabnika pregledno. Če prenos ni uspešen, se lahko prikaže pojavno okno z opozorilom, da skripta ni uspela.*



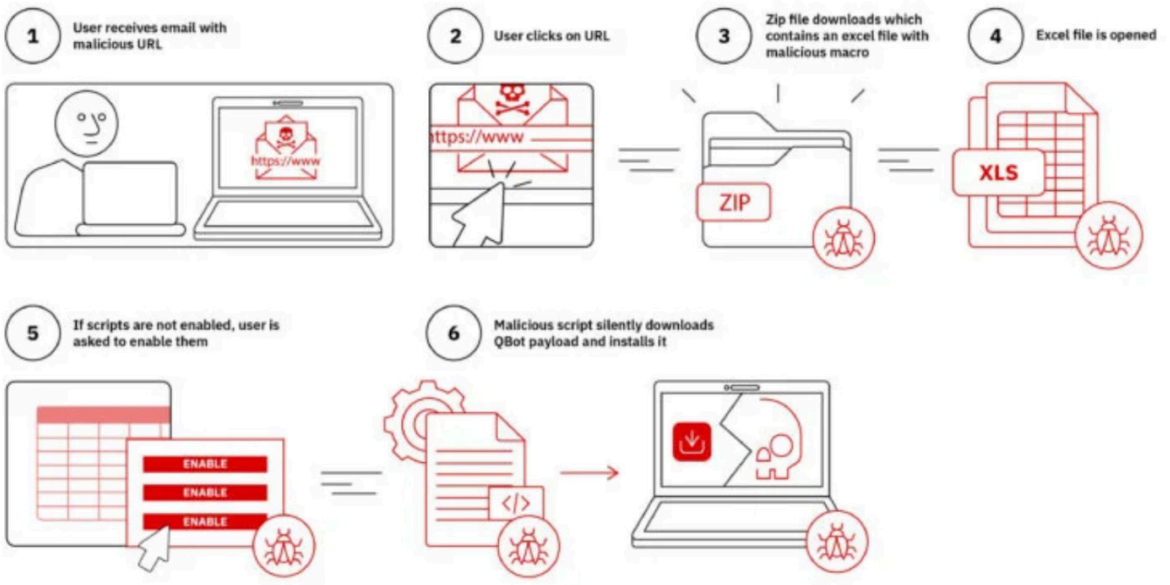
Slika 14 : Sporočilo, ki uporabnika poziva, naj omogoči izvajanje zlonamerne skripte

Podatki našega partnerja Group-IB kažejo, da je bil koristni tovor na prvi stopnji ustvarjen z orodjem SilentBuilder (znanim tudi kot EtterSilent), ki je bilo zasnovano posebej za ta namen. Zato se lahko izdelava zlonamernih dokumentov in njihova nadaljnja distribucija preneseta na druge osebe, kar otežuje identifikacijo napadalca.

Viri za drugostopenjski koristni tovor, ki jih je Inštitut CyberPeace odkril v skriptih, se ujemajo s kazalniki ogroženosti (IoC), o katerih je poročal TrendMicro.

Koristni tovor druge stopnje

Zlonamerna vsebina, ki je shranjena v **C : \DATOP** *v uporabnikovem računalniku, se prenese le, če so izpolnjeni nekateri posebni pogoji, povezave pa hitro postanejo neodzivne.. Dobavljena je v različnih oblikah, najpogosteje v obliki DLL ali izvedljivih datotek. Vsebuje elemente, ki se na videz navezujejo na SquirrelWaffle in Qakbot/QBot, dva seva zlonamerne programske opreme, ki se uporabljata v kampanjah izsiljevalske programske opreme in drugih vrstah kibernetskega izsiljevanja. Običajno se aktivirajo pozneje, ko nastopi pravi trenutek.*



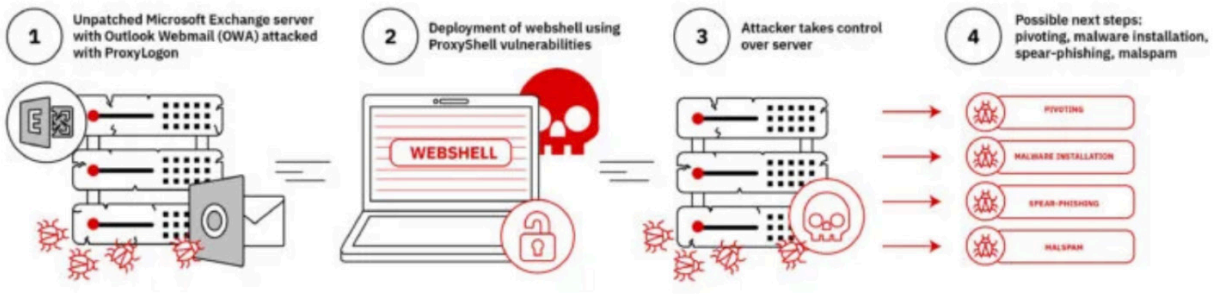
Slika 15 : Postopek okužbe z virusom QBot

Na podlagi naših dosedanjih raziskav, ki datoteke razvrščajo kot Qakbot (bančni trojanski konj), širjenja zlonamernih datotek prek kampanj malspama in ugotovitev tekoče preiskave infrastrukture, ki stoji za plačilnimi obremenitvami, ocenjujemo, da gre pri tej kampanji verjetno za kibernetski kriminal/finančno motivirano dejavnost. V nekaterih primerih so poročali tudi, da je bil Qakbot uporabljen za nalaganje Cobalt Strike, močnega orodja za ciljno usmerjene napade na infrastrukturo. [...]

Začetna ogroženosti

SCRT, s katerim smo med preiskavo tesno sodelovali, je ugotovil, da se je ta kampanja zlonamerne programske opreme začela sz ogroženostjo strežnikov Microsoft Exchange, ki niso bili posodobljeni z varnostnimi popravki. Natančneje, napadalci izkoristijo ranljivosti ProxyLogon (CVE-2021-26855) in ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207) za vstop v strežnik Exchange, namestitev svojih orodij in oddaljeno izvajanje kode.

To vpliva na Microsoft Exchange 2013, 2016 in 2019. Microsoft je leta 2021 izdal več varnostnih posodobitev za odpravo teh ranljivosti.



Slika 16 : Kako je ogrožen strežnik izmenjave

Izvirni članek vključuje tudi obrambne korake in korake za obnovitev, ki jih tukaj zaradi kratkosti nismo vključili.

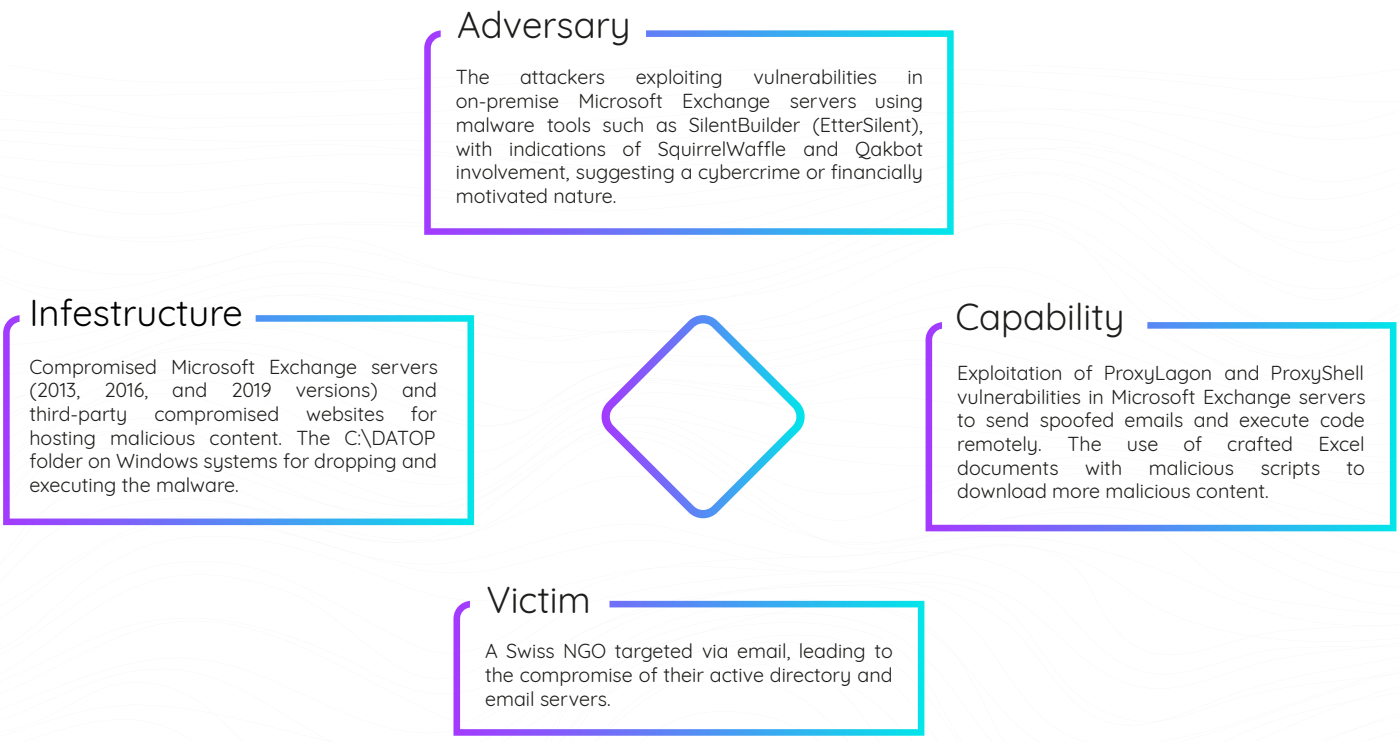
Razpoložljive obveščevalne informacije

Kontekstualna inteligenca

- **Obveščanje o strateških grožnjah :** na voljo je bilo malo informacij, vodja IT je bil na daljšem dopustu, oseba, ki je vodila odzivanje na incident, pa ni imela izkušenj na področju kibernetske varnosti ali IT. Dokumentirane politike niso bile na voljo in čeprav je nevladna organizacija delovala na občutljivem območju, je bilo zavedanje o kibernetski grožnji omejeno.
- **Taktične obveščevalne informacije o grožnjah :** ni na voljo.

Obveščevalne informacije za posamezne incidente

- **Tehnična obveščevalna služba o grožnjah :** ponarejena e-poštna sporočila, ogroženi e-poštni strežniki, zlonamerne skripte in datoteke, dnevniki dogodkov aktivnega imenika.
- **Obveščanje o operativnih grožnjah :** preiskava tretje osebe je razkrila, da je kampanja za namestitev zlonamerne vsebine izkoriščala ranljivosti v lokalnih strežnikih Microsoft Exchange (ProxyLogon in ProxyShell). Ugotovljena je bila tudi uporaba posebnih sevov zlonamerne programske opreme, kot sta SquirrelWaffle in Qakbot/QBot. Obveščevalne informacije so bile samo v človeku berljivi obliki.



Diamantni model za posamezen primer

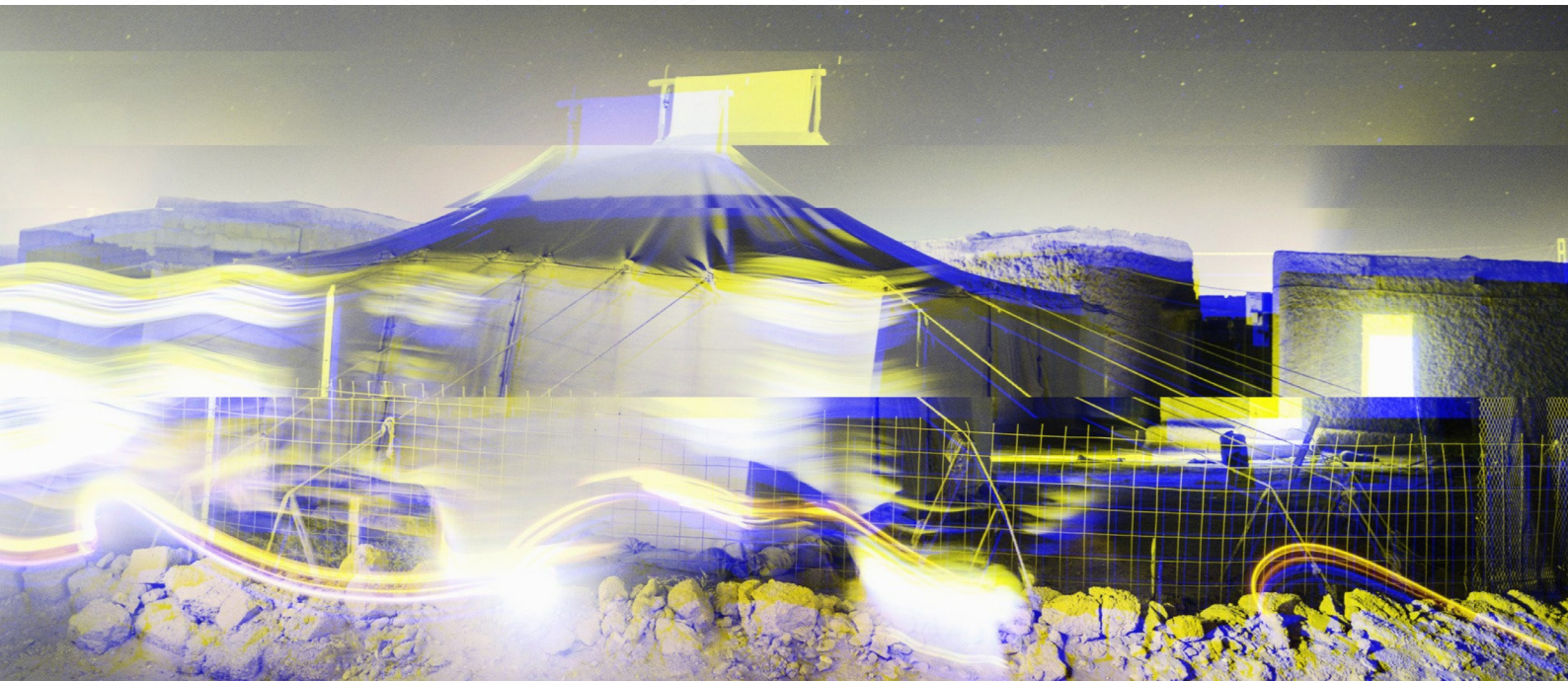
4.4.3 Primer 3 : Nevladna organizacija s sedežem v EU tarča napada izsiljevalske programske opreme

Informacije o primeru

Nevladna organizacija s sedežem v EU (država zaradi ohranjanja anonimnosti ni navedena) je leta 2023 doživela napad z izsiljevalsko programsko opremo, ki je zašifrirala podatke njenega spletnega strežnika, vključno z informacijami za več kot 10 let. Ustvarjalci grožnje so v zameno za dešifrirni ključ zahtevali odkupnino v višini 5000 EUR. Nevladna organizacija, ki ni imela varnostnih kopij in ni mogla prepoznati vrste izsiljevalske programske opreme, je za pomoč zaprosila prostovoljce iz inštituta CyberPeace Institute in organe pregona.

Časovnica :

- **Dan 0 :** Odkritje napada z izsiljevalsko programsko opremo; vse datoteke so šifrirane, razen sporočila o odkupnini.
- **Dan 2 :** Prva ocena prostovoljca; tehnični direktor nevladne organizacije je poskušal komunicirati z napadalci prek programa Jabber.
- **Dan 10 :** Prostovoljčev načrt ukrepanja je vključeval poskuse dešifriranja, sodelovanje z napadalci ter kontaktiranje ponudnikov gostovanja in organov pregona.
- **Dan 11 :** Pri razpakiranju šifriranih datotek ali vzpostavljanju stika z napadalci ni napredka; obstaja sum, da gre za vandalizem amaterskih hekerjev.
- **Dan 13 :** Začela so se pogajanja z akterji grožnje; zahtevana odkupnina je bila znižana na 300 dolarjev.
- **Dan 14 :** Preiskava legitimnosti kripto menjalnice, ki je bila uporabljena za plačilo odkupnine; identificirana je kot subjekt, registriran na Sejšelih.
- **Dan 16 :** Nevladna organizacija razmišlja o vključitvi policije; zaskrbljenost zaradi pravnih posledic.
- **Dan 17 :** Odločitev o plačilu odkupnine, ki je odvisna od testiranja orodja za dešifriranje.
- **Dan 20 :** Napadalci ne želijo dokazati zmožnosti dešifriranja; dvomi o obstoju delujočega orodja za dešifriranje.
- **Dan 21 :** Odločitev o neplačilu odkupnine zaradi pomanjkanja dokaza o dešifriranju.
- **Dan 22 :** Osredotočite se na izboljšanje varnosti spletnih mest in preprečevanje prihodnjih napadov.



Razpoložljive obveščevalne informacije

Kontekstualna inteligenca

* Razpoložljivi obveščevalni podatki o strateških grožnjah : razen območja delovanja in morebitnega motiva napadalcev na splošno niso na voljo.
* Taktična inteligenca : ni na voljo.

Obveščevalne informacije za posamezne incidente

** Tehnični podatki o grožnjah : lokacija spletnega strežnika, tehnične podrobnosti o strežniku (npr. različica Apache), vendar brez dnevnikov, podatki, za katere je bila v spletnem strežniku šifrirana izsiljevalska programska oprema, vrsta izsiljevalske programske opreme, pridobljena z analizo šifrirane datoteke na naslovu **nomoreransom.org**, , ki kaže na morebitne vrste, kot so CrySIS, XORBAT, Nemucod, MegaLocker ali Hakbit.
* Operativna obveščevalna informacija o grožnjah : obvestilo o odkupnini, ki zahteva 5000 USD, obravnava Jabber in **nowpayment.io** za plačilo odkupnine, dnevniki komunikacije žrtev/kriminalci, glejte sliki 17 in 18, korespondenca z Europolom in francoskimi organi pregona glede morebitne pomoči in pravnih premislekov, vpogledi v vedenje in zmožnosti napadalcev na podlagi njihovih odzivov in dejanj.

README (1) — Edited

```
[91m
################################
##########  WARNING ############
################################
- English -
The data on the server is encrypted.
To receive the key, pay $5000.
Payment link: https://nowpayments.io/donation/############
After payment, a decrypt.sh file will be created in the /root folder, which will allow you to
decrypt the data.
Jabber contact: #########@exploit.im, #########@jabb.im

- Русский -
Данные на сервере зашифрованы.
Для получения ключа оплатите $5000.
Ссылка для оплаты: https://nowpayments.io/donation/############
После оплаты в папке /root будет создан файла decrypt.sh, который позволит расшифровать данные.
Контакт для связи jabber: #########@exploit.im, #########@jabb.im
################################
##########  WARNING ############
################################
```

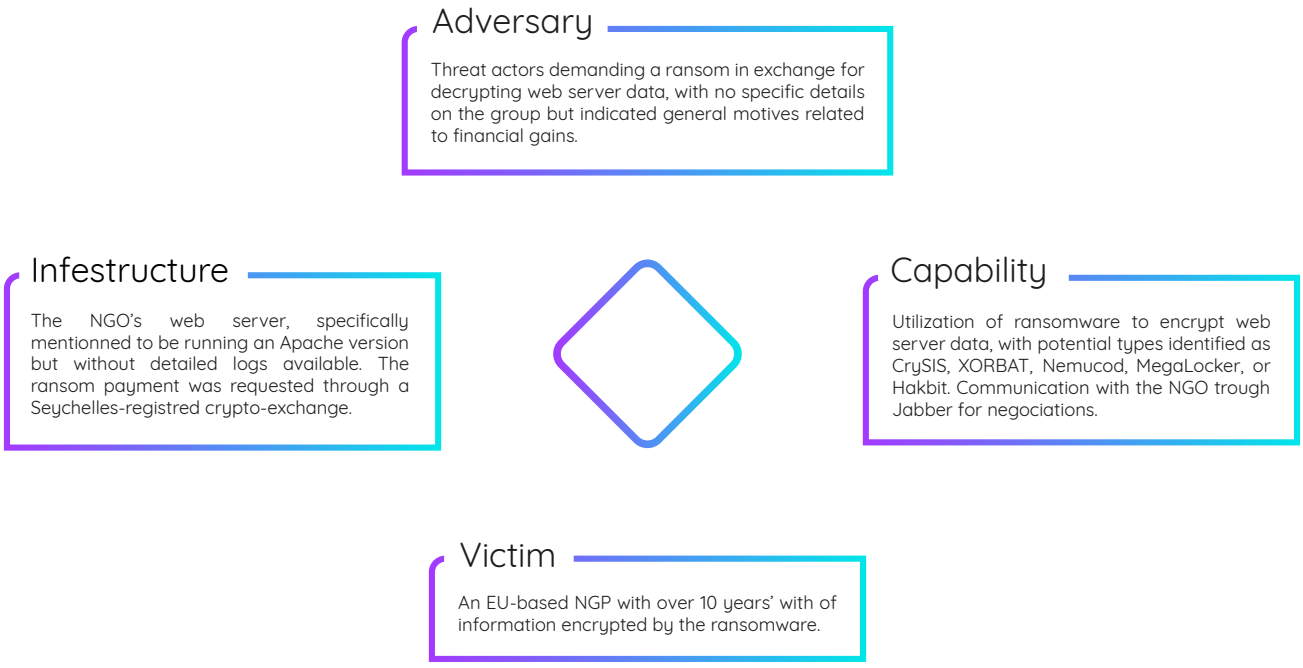
Slika 17 : Nevladna organizacija je prejela odkupnino

[redacted]@exploit.im/Psi+

(10:07:49 AM) [redacted] Hello, We do not have the ability to replace the servers either. You will see that our work is all humanitarian. We ask you to return the website to allow us to continue our community work.

(10:13:40 AM) [redacted] **@exploit.im/Psi+:** Hello. I think it would be fair if you paid $300. For your mistake, so that you will be more vigilant in the future. I don't think this amount should be a big problem. https://nowpayments.io/donation/[redacted]

Slika 18 : Komunikacijski dnevniki pogajanj



Diamantni model za posamezen primer

4.5 Ključni kibernetski incidenti, ki so prednostno obravnavani in jih upravljajo organi LEA/CERT

Organa LEA in CERT obravnavata različne kibernetske incidente, ki vplivajo na nevladne organizacije, najpogostejši pa so lažno predstavljanje, zlonamerna programska oprema in ogrožanje naprav. Poleg odzivanja na te grožnje številne agencije uporabljajo tudi preventivni pristop in pomagajo nevladnim organizacijam pri krepitvi njihove obrambe. V nadaljevanju je predstavljenih nekaj ključnih spoznanj iz njihovih izkušenj.

4.5.1 Vrste obvladovanih kibernetskih incidentov

V raziskavi, ki je bila izvedena za pristojne organe in skupine CERT, so bili udeleženci vprašani o vrstah kibernetskih incidentov, ki jih upravljajo za nevladne organizacije. Iz povratnih informacij je razvidno, da so organi LEA vključeni v obravnavo številnih incidentov, pri čemer se osredotočajo zlasti na pogoste vektorje napadov, kot sta lažno predstavljanje in zlonamerna programska oprema. Najpogosteje obravnavani incidenti so bili :

- **Lažno predstavljanje in ogrožanje poverilnic :** več anketirancev je opozorilo, da so bila najpogostejša vrsta obravnavanih incidentov lažna e-poštna sporočila, ki so vodila do kraje ali ogrožanja poverilnic.
- **Zlonamerna programska oprema :** Omenjeni so bili tudi incidenti, povezani z okužbami z zlonamerno programsko opremo, zlasti v primerih, ko so se nevladne organizacije soočale z znatnimi motnjami v delovanju.
- **Ogrožanje naprav in kršitev računov :** V nekaterih primerih so se anketiranci ukvarjali z domnevno ali potrjeno ogrožanje naprav z vdori v uporabniške račune.

Poleg odzivanja na incidente imajo nekatere agencije tudi preventivno vlogo, saj nevladnim organizacijam pomagajo vzpostaviti obrambo pred napadi. En anketiranec je kot ključno strategijo pri obvladovanju morebitnih kibernetskih incidentov izpostavil osredotočenost na preprečevanje.

4.5.2 Prednostna razvrstitev kibernetskih incidentov, o katerih poročajo nevladne organizacije

Učinkovito določanje prioritet incidentov je ključnega pomena za zagotovitev, da se nevladne organizacije pravočasno odzovejo na kibernetske grožnje. Odgovori na anketo so razkrili različne pristope k temu, kako agencije ocenjujejo prijavljene incidente in jim dajejo prednost :

- **Določanje prednostnih nalog glede na vrsto žrtve :** Nekateri anketiranci so omenili, da incidente, o katerih poročajo nevladne organizacije, obravnavajo kot dogodke »prioritete 1« (P1), ki zahtevajo takojšnjo pozornost, zlasti kadar gre za večje kršitve ali grožnje osnovnim storitvam.
- **Določanje prednostnih nalog na podlagi učinka :** Več anketirancev je navedlo, da se incidenti obravnavajo prednostno glede na možen vpliv na delovanje ali ugled nevladne organizacije, brez posebnega upoštevanja v primerjavi z drugimi žrtvami.

Čeprav je določanje prednostnih nalog na podlagi učinka še vedno običajno, se nekatere agencije vse bolj zavedajo, da je treba incidente NVO obravnavati bolj nujno, zlasti kadar gre za kritične kršitve ali grožnje bistvenim storitvam.

5. Zahteve glede platforme za poročanje nevladnih organizacij o kibernetskih incidentih organom LEA

5.1 Zahteve za platformo LEA/CERT

Med vprašanji, vključenimi v ankete, jih je bilo več namenjenih ugotavljanju izzivov, s katerimi se soočajo anketiranci. Na podlagi teh informacij lahko ekipa bolje prilagodi platformo svojim potrebam in zmanjša te izzive.

5.1.1 Izzivi, s katerimi se soočajo nevladne organizacije pri obvladovanju incidentov

Anketiranci so izpostavili več ponavljajočih se izzivov :

- **Pomanjkanje virov :** Nekatere agencije so kot glavno oviro navedle omejene vire, tako v smislu osebja kot tehnologije. To še posebej velja za hkratno obravnavo več incidentov, kar obremenjuje obstoječe zmogljivosti.
- **Komunikacijske vrzeli :** Več anketirancev je omenilo težave pri vzpostavljanju in vzdrževanju dosledne komunikacije z nevladnimi organizacijami, kar lahko povzroči zamude pri odzivanju na incidente.
- **Pomanjkanje ozaveščenosti o kibernetski varnosti v nevladnih organizacijah :** Številne nevladne organizacije niso v celoti opremljene za prepoznavanje ali ponovno sporočanje kibernetskih incidentov, zaradi česar organi oblasti težje učinkovito posredujejo. Anketiranci so kot ključni dejavnik izpostavili pomanjkanje usposabljanja o kibernetski varnosti v nevladnih organizacijah.

5.1.2 Vrste podatkov, prejetih od nevladnih organizacij

Pri tistih anketirancih, ki prejemajo podatke od nevladnih organizacij, so najpogosteje navedene naslednje vrste podatkov :

- **Dnevniki incidentov :** številne nevladne organizacije delijo dnevnike, v katerih so podrobno opisane sumljive dejavnosti, vključno s poskusi prijave, naslovi IP in poskusi lažnega predstavljanja.
- **Kazalniki ogroženosti (IOC) :** nekatere nevladne organizacije zagotavljajo IOC, kot so podpisi zlonamerne programske opreme, URL-ji ali IP-naslovi, vključeni v napad.
- **Minimalni podatki :** v nekaterih primerih nevladne organizacije zagotovijo le osnovne podatke ali poročila, ki lahko ne zadostujejo za temeljito preiskavo.

5.1.3 Zgodbe o uspehu ali pozitivni rezultati sodelovanja

Anketirance smo prosili, naj delijo zgodbe o uspehu ali pozitivne rezultate sodelovanja z nevladnimi organizacijami. Nekaj pomembnih primerov je bilo :

- **Preprečitev večjih vdorov :** eden od anketirancev je opisal primer, ko je zgodnje odkrivanje poskusov lažnega predstavljanja preprečilo veliko kršitev varnosti podatkov v veliki nevladni organizaciji.
- **Izboljšano zavedanje :** več anketirancev je izpostavilo primere, ko so nevladne organizacije po prejemu pomoči organov oblasti izvajale strožje varnostne ukrepe in izboljšale svojo notranjo ozaveščenost o tveganjih za kibernetsko varnost.

5.1.4 Platforma za poročanje o kibernetskih grožnjah

Vrzeli v podatkih, ki so jih ugotovili anketiranci (omejitve)

Anketiranci so bili pozvani, naj navedejo vse ključne podatke, ki jih ne prejemajo, vendar bi bili zanje koristni. Ugotovljenih je bilo več ključnih podatkovnih vrzeli, ki bi lahko, če bi jih odpravili, bistveno izboljšali sposobnost organov kazenskega pregona in nevladnih organizacij za učinkovitejše odzivanje na kibernetske incidente in njihovo preiskovanje :

- **Odprtokodne obveščevalne informacije o grožnjah :** eden od anketirancev je omenil, da se njihova organizacija v veliki meri zanaša na odprtokodne obveščevalne podatke o grožnjah, vendar je opozoril, da ta proces zahteva veliko virov. Koristen bi bil dostop do bolj racionaliziranih in učinkovitih virov obveščevalnih podatkov o grožnjah, kar bi omogočilo hitrejše sprejemanje odločitev brez pretiranega ročnega dela.
- **Informacije o varnostnih kontrolah, ki jih uporabljajo druge nevladne organizacije :** več anketirancev je poudarilo potrebo po vpogledu v varnostne kontrole, ki jih imajo druge nevladne organizacije. Te informacije bi lahko pomagale pri skupnem učenju in potencialno omogočile ekonomijo obsega pri naročanju orodij ali storitev kibernetske varnosti v več nevladnih organizacijah. Skupen vpogled v najboljše prakse in nadzor bi nevladnim organizacijam pomagal tudi pri primerjanju lastnih varnostnih ukrepov z industrijskimi standardi.
- **Domenske povezave :** eden od anketirancev je opozoril na pomen domenskih povezav - povezovanje domen in IP-jev z znanimi grožnjami. Ti podatki bi okrepili zmožnost organov pregona, da povežejo navidezno različne incidente in izsledijo dejavnosti kibernetskih kriminalcev v različnih nevladnih organizacijah ali na območju napada.
- **Poročila o incidentih in IOC :** anketiranci so opozorili na potrebo po bolj izčrpnih poročilih o incidentih in kazalnikih ogroženosti (IOC). IOC, kot so metode kibernetskih napadov ali določeni dokazi, so ključnega pomena za pomoč pri preiskavah. Organi LEA so poudarili, da je lahko vsak dokaz ključen za identifikacijo in prijetje storilca, zato je nujno, da nevladne organizacije v svojih poročilih navedejo čim več podrobnosti.

• **Dnevniki omrežnega prometa in podatki DNS :** več anketirancev je opozorilo na pomanjkanje podrobnih dnevnikov omrežnega prometa, zlasti prometa DNS in opozoril na visoki ravni, ki bi jih lahko prejemale nevladne organizacije. Ti podatki lahko pomagajo pri ugotavljanju izvora in obsega napadov ter odkrivanju sumljivega prometa pred incidentom, kar zagotavlja dragocen vpogled v vzorce napadov.

• **Časovni razpored dogodkov :** kot je bilo že omenjeno, pogosto manjkajo podrobni časovni razporedi incidentov. Natančno poznavanje trenutka, ko je bil napad prvič odkrit in kako se je odvijal, je bistvenega pomena za ponoven pregled dogodkov in razumevanje celotnega obsega napada. Ti podatki časovnega razporeda bi bili dragoceni za izboljšanje odzivanja na incidente in zagotavljanje boljše pripravljenosti na prihodnje incidente.

5.1.5 Uporaba podatkov, ki so jih zagotovile nevladne organizacije

Vsi anketiranci so navedli, da podatke, ki jih zagotavljajo nevladne organizacije, uporabljajo za odzivanje na kibernetske grožnje in njihovo ublažitev. Vendar pa so poudarili, da je pomembno prejeti celovite in pravočasne podatke, da se omogoči hitrejše in učinkovitejše odzivanje.

5.1.6 Prednosti namenske platforme za poročanje o grožnjah za nevladne organizacije

Anketirance smo vprašali, kako bi posebna platforma za poročanje o kibernetskih grožnjah, prilagojena posebej za nevladne organizacije, koristila njihovim agencijam. Ugotovljenih je bilo več potencialnih prednosti :

• **Centralizirano poročanje in ozaveščanje sektorja :** posebna platforma bi nevladnim organizacijam zagotovila enotno, centralizirano mesto za poročanje o kibernetskih incidentih, kar bi organom pregona omogočilo boljši pregled nad vrstami in pogostostjo napadov na neprofitni sektor. To ne bi pomagalo le pri prepoznavanju posebnih groženj, pomembnih za nevladne organizacije, temveč bi tudi olajšalo ozaveščanje celotnega sektorja. Anketiranci so opozorili, da bi izmenjava najboljših praks v neprofitnem sektorju koristila vsem organizacijam, saj bi omogočila boljše razumevanje skupnih izzivov, s katerimi se soočajo NVO.

• **Hitrejše odzivanje na incidente in obveščanje o grožnjah :** anketiranci so navedli, da bi takšna platforma lahko izboljšala odzivanje na incidente, saj bi olajšala izmenjavo informacij o grožnjah v realnem času. S povečanim obsegom telemetrije in kazalnikov kompromitacije, ki se samodejno zbirajo in izmenjujejo, bi platforma povečala hitrost in natančnost odzivov organov pregona in nevladnih organizacij na kibernetske napade. Če bi bile agencije na tekočem z dogajanjem v realnem času, bi lahko sprejemale hitrejše in bolj utemeljene odločitve.

• **Izmenjava znanja o najnovejših taktikah, tehnikah in postopkih (TTP) :** druga ključna prednost, ki so jo izpostavili anketiranci, je bila možnost izmenjave najnovejših taktik, tehnik in postopkov (TTP) kibernetskih kriminalcev. To bi izboljšalo izmenjavo znanja med nevladnimi organizacijami in organi kazenskega pregona ter zagotovilo, da se obe strani zavedata novih groženj in načinov obrambe pred njimi. Ta funkcija bi agencije obveščala tudi o najnovejših metodah kibernetskih napadov na nevladne organizacije, vključno z vrstami napadov, vzroki in vzorci, ki jih napadalci lahko uporabljajo.

• **Analiza groženj in odkrivanje vzorcev :** platforma bi uporabnikom omogočila učinkovitejše analiziranje groženj in odkrivanje vzorcev. S povezovanjem incidentov v neprofitnem sektorju bi lahko organi za zaščito okolja ugotavljali trende in sledili vedenju kibernetskih kriminalcev, vključno s skupnimi vektorji napadov in vzorci, ki jih kriminalci lahko uporabljajo. Ta zmogljivost bi podprla dolgoročne preiskave in pomagala preprečevati prihodnje napade z odkrivanjem ponavljajočih se groženj.

• **Okrepljena izmenjava podatkov in sodelovanje :** strukturiran in dosleden mehanizem za izmenjavo podatkov bi zmanjšal ročno delo, potrebno za zbiranje in obdelavo podatkov o incidentih. S funkcijami, kot so samodejno zbiranje podatkov (npr. IOC, dnevniki incidentov, časovni razporedi), bi platforma izboljšala sodelovanje med nevladnimi organizacijami in organi oblasti, zlasti pri prepoznavanju čezmejnih groženj ali incidentov, ki vplivajo na več organizacij. Anketiranci so opozorili, da bi bili ti podatki na voljo pri odzivanju na incidente in obveščanju o grožnjah v različnih regijah.

• **Analiza zgodovinskih podatkov in prepoznavanje trendov :** platforma bi omogočala tudi shranjevanje in analizo preteklih podatkov, kar bi organom oblasti in nevladnim organizacijam pomagalo pri spremljanju ponavljajočih se incidentov in ugotavljanju dolgoročnih trendov. Ta funkcija bi agencijam omogočila, da ocenijo uspešnost svojih posegov skozi čas, hkrati pa bi razkrila globlji vpogled v razvijajoče se taktike kibernetskih kriminalcev, usmerjenih v neprofitni sektor.

5.1.7 Posebni podatki, ki jih je treba prednostno obravnavati na posebni platformi za poročanje o grožnjah

Anketirance smo vprašali, kateri podatki bi morali biti na namenski platformi za poročanje o grožnjah prednostno obravnavani, da bi jih njihove agencije lahko uporabile. V povratnih informacijah je bilo izpostavljenih več ključnih vrst podatkov, ki bi povečali učinkovitost odzivov organov kazenskega pregona :

• **Kazalniki ogroženosti (IOC) :** anketiranci so nenehno poudarjali potrebo po IOC v realnem času, kot so zlonamerni IP-naslovi, URL-ji in gesla datotek. Poleg tega bi način napada (npr. ali je šlo za izkoriščevalski program ničelnega dne ali spremenjeno zlonamerno programsko opremo) organom kazenskega pregona zagotovil dodaten kontekst za hitro ocenjevanje in blokiranje trenutnih groženj ali preiskovanje njihovih virov.

• **Podrobni dnevniki incidentov :** številni anketiranci so opozorili, da bi bili izčrpni dnevniki incidentov, vključno s časovnimi oznakami, prizadetimi sistemi, prometom DNS in sprejetimi ukrepi, neprecenljivi. Ti dnevniki bi omogočili temeljitejšo analizo napada, s čimer bi dobili vpogled v naravo napada, organi oblasti pa bi se lahko učinkovito odzvali.

• **Informacije o povzročitelju grožnje :** nekateri anketiranci so izrazili potrebo po profilih akterjev groženj ali kakršnih koli obveščevalnih podatkih, povezanih z domnevnimi storilci napadov. To lahko vključuje vse informacije, ki bi lahko grožnjo povezale z organizirano kriminalno združbo (OCG) ali znano kibernetsko kriminalno združbo. Razumevanje poteka kibernetskega napada - ali je napadalec spremenil taktiko zlonamerne programske opreme ali uporabil znan vektor - bi bilo za organe pregona ključnega pomena pri preiskovanju in pregonu kibernetskih kriminalcev.

• **Prizadeti sistemi in podatki :** predlagano je bilo, da se je treba prednostno osredotočiti na posebne sisteme in podatke, ki so bili ogroženi med napadom. Če organi oblasti vedo, kateri sistemi so bili tarča napada ali vdora, lahko bolje ocenijo resnost napada in zagotovijo ustrezno podporo.

• **Časovni razpored dogodkov :** več anketirancev je navedlo, da bi bil ključnega pomena časovni potek dogodkov, ki bi prikazoval, kdaj je bil napad odkrit, kako je potekal in kakšne odzivne ukrepe je sprejela nevladna organizacija. To bi organom pregona zagotovilo bistvene informacije za rekonstrukcijo napada in razumevanje učinkovitosti odziva.

• **Učinek med organizacijami :** drugi pomemben podatek so bile informacije o tem, ali so podobni napadi prizadeli več organizacij. Tako bi lahko organi oblasti prepoznali usklajene ali razširjene kampanje in se nanje proaktivneje odzvali. Skorajšnji izidi in incidenti, ki so se jim nevladne organizacije izognile, so lahko prav tako dragoceni za izboljšanje zaščite v celotnem sektorju.

• **Sorazmerni nadzor in obramba :** anketiranci so poudarili pomen razumevanja groženj in vektorjev napadov, s katerimi se soočajo nevladne organizacije, da lahko organi kazenskega pregona ocenijo, katere sorazmerne kontrole in obrambne ukrepe je treba izvesti.

• **Učinkovitost Microsoftovih varnostnih orodij :** eden od anketirancev je opozoril na pomen razumevanja uporabe, razširjenosti in učinkovitosti varnostnih orodij, kot je Microsoft Defender, na katerega se pri konsolidaciji varnostnih kontrol zanašajo številne neprofitne organizacije. Pri oblikovanju obrambnih strategij bi bile koristne študije primerov in pregledi, kako so ta orodja pomagala ublažiti določene napade.

• **Pregled novih napadov :** anketiranci so želeli tudi pregled novih napadov s podrobnostmi o tem, kako so se zgodili in kaj bi se lahko iz teh incidentov naučili.

5.1.8 Uporabne funkcije platforme za poročanje o kibernetskih grožnjah

V odgovorih na anketo je bilo navedenih več ključnih značilnosti in zmogljivosti, zaradi katerih bi bila platforma za poročanje o kibernetskih grožnjah koristnejša za organe kazenskega pregona (LEA) in nevladne organizacije (NVO). Te funkcije se osredotočajo na izboljšanje čezmejne preglednosti, lažjo izmenjavo obveščevalnih podatkov ter izboljšanje zmožnosti prepoznavanja kibernetskih napadov in odzivanja nanje. V nadaljevanju so navedene glavne točke, ki so jih izpostavili anketiranci :

• **Vidnost prek meja :** eden od anketirancev je poudaril pomen čezmejne prepoznavnosti. Kibernetske grožnje pogosto presegajo geografske meje, zlasti v primeru globalnih nevladnih organizacij. Platforma, ki omogoča čezmejno vidnost, bi organom pregona in nevladnim organizacijam omogočila spremljanje kibernetskih groženj na mednarodni ravni, s čimer bi lahko odkrili vzorce in grožnje, ki bi sicer v lokalnem ali regionalnem okolju ostali neopaženi. To bi okrepilo sodelovanje med organi kazenskega pregona v različnih državah in izboljšalo usklajeno odzivanje na globalne kibernetske grožnje.

• **Souporaba dnevnikov in zlonamerne e-pošte za zbiranje obveščevalnih podatkov :** druga dragocena funkcija, ki je bila omenjena, je možnost, da nevladne organizacije enostavno delijo dnevnike in primere zlonamernih e-poštnih sporočil. To bi olajšalo zbiranje obveščevalnih podatkov v organizacijah ter pomagalo prepoznati trende in skupne vektorje napadov. Eden od anketirancev je predlagal, da bi se Microsoft lahko vključil v to platformo in uporabil skupne podatke za pomoč pri oblikovanju svojih zaščitnih kontrol. Ker so nevladne organizacije pogoste tarče kibernetskih napadov, bi lahko obsežna skupna obveščevalna informacija pomagala pri oblikovanju mehanizmov zaščite, ne le za nevladne organizacije, temveč tudi za širši tehnološki ekosistem.

• **Prepoznavanje zlonamernih naslovov IP :** več anketirancev je poudarilo potrebo po funkciji, ki lahko označi zlonamerne naslove IP. Ta identifikacija v realnem času bi nevladnim organizacijam in pristojnim organom omogočila hitro prepoznavanje in blokiranje prometa iz znanih zlonamernih virov. Z vključitvijo te funkcije v platformo bi lahko organizacije proaktivno preprečevale napade s prepoznavanjem in nevtraliziranjem groženj, preden povzročijo škodo.

• **Poizvedovanje po incidentu prek API-ja :** eden od predlogov je vključeval API za poizvedovanje po incidentih in kazalnikih. To bi nevladnim organizacijam in organom LEA omogočilo programski dostop do podatkov o incidentih in obveščevalnih podatkov o grožnjah, kar bi olajšalo integracijo platforme z obstoječimi varnostnimi orodji in sistemi. Tak API bi lahko omogočil hitrejše odzivanje z avtomatizacijo pridobivanja podatkov in zagotavljanjem posodobitev o novih grožnjah v realnem času.

• **Spremljanje prometa med incidenti :** kot dragocena je bila izpostavljena tudi funkcija, ki omogoča pregled omrežnega prometa pred incidentom in med njim. S spremljanjem prometa v realnem času bi lahko platforma nevladnim organizacijam in pristojnim organom omogočila odkrivanje anomalij ali sumljivih vzorcev, ki bi lahko kazali na potek kibernetskega napada. Ta funkcija bi bistveno izboljšala zavedanje o razmerah med incidenti, kar bi omogočilo hitrejše obvladovanje in ublažitev grožnje.

• **Identifikacija kibernetskega napadalca :** anketiranci so navedli, da bi morala platforma vključevati zmogljivosti za pomoč pri prepoznavanju kibernetskega napadalca ali povzročitelja grožnje, ki stoji za incidentom. Funkcija, ki zbira podatke, uporabne za pripisovanje napadov, bi bila ključnega pomena, ne glede na to, ali gre za sledenje naslovov IP, jezikovne vzorce v lažnih e-poštnih sporočilih ali opombe o izsiljevalski programski opremi. To bi organom pregona pomagalo pri iskanju in pregonu kibernetskih kriminalcev, nevladnim organizacijam pa pri razumevanju narave groženj, s katerimi se soočajo.

• **Informacije o povzročitelju grožnje :** v zvezi z identifikacijo napadalcev je še en anketiranec poudaril potrebo po vseh podatkih, ki bi lahko pomagali identificirati povzročitelja grožnje, kot so naslovi IP ali poseben jezik, uporabljen v lažnih elektronskih sporočilih ali zapisih o izsiljevalski programski opremi. Te informacije bi bile neprecenljive pri oblikovanju profilov povzročiteljev groženj in povezovanju več incidentov, ki jih je morda zagrešila ista skupina ali posameznik.

Če povzamemo, se značilnosti in zmogljivosti, ki so jih opredelili anketiranci, osredotočajo na povečanje čezmejne vidljivosti, izboljšanje izmenjave obveščevalnih podatkov ter zagotavljanje naprednih orodij za prepoznavanje kibernetskih groženj in odzivanje nanje. Mednje sodijo možnost deljenja dnevnikov in zlonamernih e-poštnih sporočil, prepoznavanje zlonamernih naslovov IP, poizvedovanje na podlagi API, spremljanje omrežnega prometa med incidenti ter orodja za prepoznavanje akterja grožnje. Zaradi teh lastnosti bi platforma za poročanje o kibernetskih grožnjah postala zelo učinkovito orodje za nevladne organizacije in organe pregona v boju proti kibernetskim grožnjam.

5.1.9 Posebna podpora in viri za nevladne organizacije

Zadnje vprašanje v raziskavi se je osredotočalo na vrste podpore ali virov, ki bi bili za nevladne organizacije najbolj koristni za izboljšanje njihove kibernetske varnosti. Iz odgovorov na anketo je razvidna široka paleta zamisli o podpori in virih, ki bi nevladnim organizacijam koristili pri krepitvi njihove kibernetske varnosti. V odgovorih se je pojavilo več skupnih tem, ki poudarjajo področja, na katerih se nevladne organizacije soočajo z največjimi izzivi, in vrste pomoči, ki bi imele največji učinek.

- **Dostop do cenovno dostopnih ali brezplačnih virov :** eden od n anketirancev je izpostavil potrebo po podpori pri iskanju ugodnih ali brezplačnih virov, ki bi pomagali ublažiti ali se braniti pred kibernetskimi grožnjami. Glede na to, da številne nevladne organizacije delujejo z omejenimi sredstvi, je dostop do stroškovno učinkovitih ali brezplačnih rešitev ključnega pomena. Takšna pomoč bi nevladnim organizacijam omogočila izvajanje potrebnih ukrepov kibernetske varnosti, ne da bi dodatno finančno obremenila njihovo delovanje.
- **Strokovno znanje in vodenje na področju kibernetske varnosti :** velik izziv za nevladne organizacije je pomanjkanje notranjega strokovnega znanja o kibernetski varnosti. Kot je navedel eden od vprašanih, bi bila lahko učinkovita rešitev zagotavljanje virtualnega glavnega varnostnega uradnika (vCSO) kot storitve. Ta pristop nevladnim organizacijam omogoča, da pridobijo vodstvo in strokovno znanje na področju varnosti na delni osnovi, brez bremena zaposlitve CSO za polni delovni čas, česar si številne nevladne organizacije ne morejo privoščiti. To prilagodljivo zunanje vodstvo bi nevladnim organizacijam pomagalo pri razvoju in vzdrževanju zanesljive strategije kibernetske varnosti.
- **Sposobnosti za napredno odkrivanje groženj in odzivanje nanje :** več anketirancev je omenilo potrebo po odkrivanju končnih točk, zmogljivostih varnostnega operativnega centra (SOC) in usposabljanju za lov na grožnje. Ti napredni ukrepi kibernetske varnosti, ki jih običajno uporabljajo večje organizacije, bi nevladnim organizacijam pomagali učinkoviteje odkrivati kibernetske grožnje in se nanje odzivati. Poleg tega sta bili kot ključni orodji, ki nevladnim organizacijam pomagata proaktivno prepoznati in ublažiti morebitne napade, preden povzročijo večjo škodo, izpostavljeni tudi obveščevalna informacija o grožnjah ter razširjeno odkrivanje in odzivanje (Extended Detection and Response - XDR).
- **Usposabljanje in orodje :** med najpogosteje omenjenimi potrebami je bilo usposabljanje, pri čemer so anketiranci poudarili, da številne nevladne organizacije nimajo temeljnega znanja za obvladovanje tveganj kibernetske varnosti. Programi usposabljanja o osnovnih praksah kibernetske varnosti, odkrivanju groženj in uporabi posebnih varnostnih orodij bi zaposlenim v nevladnih organizacijah omogočili boljšo zaščito njihovih organizacij. Poleg tega je bistvenega pomena dostop do ustreznih orodij, saj bi nevladnim organizacijam omogočila spremljanje omrežij, odkrivanje ranljivosti in učinkovitejše odzivanje na incidente.

• **Uporabniku prijazne platforme in kontaktne točke :** eden od anketirancev je poudaril, da je treba nevladnim organizacijam zagotoviti uporabniku prijazno platformo za kibernetsko varnost, ki poenostavlja odkrivanje groženj in poročanje o incidentih. Nevladne organizacije pogosto nimajo tehničnega znanja in izkušenj za navigacijo po zapletenih varnostnih sistemih, zato bi jim poenostavljen vmesnik olajšal uporabo orodij in protokolov za kibernetsko varnost. Poleg tega bi vzpostavitev jasnih kontaktnih točk z ustreznimi agencijami poenostavila komunikacijo v primeru kibernetskega incidenta, kar bi nevladnim organizacijam zagotovilo, da hitro dobijo pomoč, ki jo potrebujejo.

• **Izboljšanje infrastrukture IT :** nekateri anketiranci so predlagali tudi izboljšanje splošne informacijske infrastrukture nevladnih organizacij, da bi podprli boljše prakse kibernetske varnosti. Posodobitev zastarelih sistemov in izboljšanje varnosti omrežij bi postavila trdnejše temelje za obvladovanje kibernetskih groženj. To je mogoče združiti z nasveti o izvajanju sistema upravljanja informacijske varnosti (ISMS), strukturiranega pristopa k upravljanju občutljivih informacij in zagotavljanju izpolnjevanja standardov kibernetske varnosti.

• **Redno posodabljanje in izmenjava informacij :** eden od anketirancev je poudaril potrebo po posodobljenih informacijah o orodjih, tehnikah in najboljših praksah. Če bi nevladnim organizacijam stalno zagotavljali najnovejše informacije o najnovejših trendih, grožnjah in orodjih za kibernetsko varnost, bi bile vedno obveščene in bi se lažje odločale o svojih varnostnih strategijah na podlagi informacij.

Če povzamemo, podpora in viri, ki jih nevladne organizacije potrebujejo za izboljšanje svoje kibernetske varnosti, vključujejo dostop do cenovno dostopnih virov, strokovnega vodenja (prek storitev, kot je virtualna organizacija CSO), naprednih zmogljivosti za odkrivanje in odzivanje na grožnje, usposabljanja in uporabniku prijaznih orodij. Zagotavljanje teh virov bi nevladnim organizacijam omogočilo boljšo obrambo pred kibernetskimi grožnjami, pri čemer bi delovale v okviru svojih omejenih proračunov in tehničnega znanja.

5.2 Zahteve za platformo NVO

Incidenti, predstavljeni v razdelku 4.5, ki vključujejo laboratorij EU za dezinformacije, švicarsko nevladno organizacijo in neimenovano nevladno organizacijo s sedežem v EU, nazorno prikazujejo raznolikost kibernetskih groženj in zapletenost odzivanja na takšne incidente. Ti primeri poudarjajo izzive, s katerimi se soočajo nevladne organizacije, od ugotavljanja narave napada do obnovitve po njegovih posledicah, in opozarjajo na ključno potrebo po strukturiranem podpornem sistemu.

Nevladne organizacije pogosto delujejo v različnih delovnih področjih, velikostih in tehničnih okoljih, kar lahko bistveno vpliva na njihovo ranljivost in strategije odzivanja na kibernetske incidente. Posebnost napadov na te nevladne organizacije na primer poudarja, kako pomembno je **podrobno poznati profil in tehnično strukturo organizacije, da bi lahko učinkovito prilagodili odziv**. Zato sta **modul za organizacijske informacije in funkcija za pregled tehnične infrastrukture** v platformi bistvenega pomena, da se organom kazenskega pregona in podpornim subjektom zagotovi potrebno ozadje za učinkovito pomoč..

Podrobna dokumentacija o **vrsti napada**, njegovem **vplivu**, **časovnem razporedu** je ključna za razumevanje in učinkovito ublažitev incidenta, kot je razvidno iz teh primerov. Ne glede na to, ali gre za izsiljevalsko programsko opremo ali za »spear-phishing«, je sposobnost natančne kategorizacije incidenta in opisa njegovega razvoja ključnega pomena tako za nevladne organizacije kot za odzivne subjekte. Zaradi te potrebe je v platformo vključen **modul za obveščanje o incidentih**, ki zagotavlja, da se o incidentih natančno poroča in se po njih ukrepa.

Izziv varne izmenjave tehničnih podatkov in rezultatov pasivnega skeniranja se je pokazal v teh incidentih, kjer bi dostop do digitalnih dokazov in njihova analiza lahko bistveno vplivala na postopke odzivanja in obnove. S tem je poudarjena potreba po **modulu za prenos tehničnih podatkov**, ki omogoča varen prenos dnevnikov, forenzičnih izpisov in drugih pomembnih digitalnih dokazov ter organom pregona zagotavlja informacije, potrebne za temeljito preiskavo.

Nevladne organizacije se pri odpravljanju posledic kibernetskih incidentov soočajo s pravno negotovostjo in zapletenostjo, zlasti v zvezi z vlaganjem pritožb in upravljanjem pravne dokumentacije. Razprave nevladnih organizacij s sedežem v EU o pravnih tožbah kažejo, da je v platformi potreben **vmesniški modul za pravno podporo**, ki bi ponujal smernice, predloge in poenostavljen postopek za vlaganje pravnih pritožb.

Takojšen dostop do virov za obnovo, vključno z orodji za dešifriranje in pripomočki za forenzično analizo, je ključnega pomena za nevladne organizacije, ki nimajo dovolj virov za kibernetsko varnost, kar se je pokazalo pri boju nevladne organizacije iz EU s šifriranimi podatki. **Središče za pomoč pri obnovi** na platformi bi neposredno odgovorilo na to potrebo, saj bi omogočilo hitrejšo obnovo in krepitev odpornosti po nesreči.

V teh primerih je bila poudarjena vrednost strokovne podpore prostovoljcev, kar kaže na pomen usklajenega odzivanja. Vključitev **funkcije usklajevanja prostovoljne podpore**, vključno s povezavo z omrežji prostovoljcev in imenikom upravljanih storitev odkrivanja in odzivanja, je odziv na bistveno vlogo, ki jo ima strokovna pomoč pri odzivanju na incidente in obnovi.

Nazadnje, širši izzivi, s katerimi se soočajo nevladne organizacije v smislu skupnih obveščevalnih podatkov, dostopnosti in proaktivnih ukrepov za kibernetsko varnost, kažejo na potrebo po neobveznih zahtevah, kot so **platforma za obveščanje o kibernetskih grožnjah, modul za prevajanje**, ter funkcije za **analizo incidentov in trendov**. Ti dodatki bi izboljšali zmožnost platforme za spodbujanje sodelovalnega, informiranega in večjezičnega okolja za kibernetsko varnost v nevladnem sektorju.

Ti primeri skupaj potrjujejo potrebo po celoviti platformi, ki obravnava celoten spekter potreb, ki izhajajo iz kibernetskih incidentov v nevladnih organizacijah, od začetnega poročanja in pravne podpore do izterjave in proaktivnih obrambnih strategij.

5.3 Predlogi modulov platforme

5.3.1 Organizacijski informacijski modul

• **Profil nevladne organizacije :** oddelek za vnos podrobnosti o nevladni organizaciji, kot so dokazilo o registraciji, lokacija, obseg dela in velikost, da lahko organi kazenskega pregona celovito spoznajo subjekt.

• **Pregled tehnične infrastrukture :** funkcija za nevladne organizacije za opis njihovega tehničnega okolja, vključno z arhitekturo omrežja, kritičnimi sredstvi in veljavnimi ukrepi za kibernetsko varnost.

• **Vrednotenje digitalne odpornosti :** možnost vključevanja ocene zrelosti nevladne organizacije na področju kibernetske varnosti, ki ponuja kontekst o varnostni drži organizacije. Povezava z orodjem za splošno oceno kibernetske varnosti inštituta CyberPeace Institute [39] ali drugimi orodji.

5.3.2 Modul za obveščanje o incidentih

• **Vrsta napada :** nevladnim organizacijam omogoča, da določijo vrsto kibernetskega napada (npr. izsiljevalska programska oprema, lažno predstavljanje, DDoS) za natančno kategorizacijo incidenta.

• **Vpliv incidenta :** omogoča poročanje o zahtevah za odkupnino, vključno z zneskom, naslovi denarnic s kriptovalutami in dnevniki komunikacije z napadalci, če je to pomembno, pa tudi o operativnih učinkih itd.

• **Časovni razpored incidenta :** funkcija za dokumentiranje zaporedja dogodkov, ki omogoča jasnejše razumevanje razvoja incidenta.

• **Sistem izdajanja oznak :** dokaz za nevladno organizacijo, da je bil incident prijavljen.

39 »Ukrep za izboljšanje : Vloga GCSA pri kibernetski odpornosti neprofitnih organizacij", CyberPeace Institute, 30. januar 2024, **https://cyberpeaceinstitute.org/news/measure-to-improve-the-gcsas-role-in-nonprofit-cyber-resilience/**

5.3.3 Modul za nalaganje tehničnih podatkov

• **Varno nalaganje datotek :** možnost varnega prenosa dnevnikov, forenzičnih izpisov, šifriranih datotek, zapiskov o odkupnini in drugih digitalnih dokazov, ki lahko pomagajo pri preiskavi.

• **Rezultati pasivnega skeniranja :** možnost prenosa rezultatov pasivnega skeniranja za vpogled v morebitne ranljivosti, ki so bile izkoriščene v napadu.

5.3.4 Vmesnik za pravno podporo

• **Pravna pomoč pri pritožbah :** smernice in predloge za pomoč nevladnim organizacijam pri vložitvi pravne pritožbe v zvezi s kibernetskim incidentom neposredno prek platforme, vključno z informacijami o različnih načinih za to v posameznih državah.

• **Obstoječa pritožbena dokumentacija :** možnost nalaganja dokumentacije v zvezi s pritožbami, ki so že bile vložene pri organih pregona ali drugih organih.

5.3.5 Središče za pomoč pri obnovi

• **Repozitorij orodij za dešifriranje :** neposreden dostop do seznama najnovejših orodij za dešifriranje in vodnikov za njihovo uporabo (npr. **www.nomoreransom.org**).

• **Viri za forenzično analizo :** povezave do forenzičnih orodij in virov za pomoč nevladnim organizacijam pri izvajanju predhodnih preiskav in ohranjanju dokazov za organe pregona.

5.3.6 Usklajevanje podpore prostovoljcem

• **Zahtevek za prostovoljno pomoč :** povezava s CyberPeace Builders, ki nevladnim organizacijam omogoča, da zaprosijo za pomoč prostovoljcev.

• **Imenik MDR :** dostop do imenika podjetij za nadzorovano odkrivanje in odzivanje, ki so pripravljena pomagati nevladnim organizacijam.

5.3.7 Neobvezne zahteve

• **Platforma za obveščanje o kibernetskih grožnjah, namenjena nevladnim organizacijam :** platforma, namenjena nevladnim organizacijam, ki bi jim omogočala medsebojno izmenjavo/prevzemanje obveščevalnih podatkov o kibernetskih grožnjah, ki bi jo lahko dopolnili z informacijami partnerjev.

• **Modul za prevajanje :** platforma bi lahko bila na voljo v vseh jezikih EU.

• **Analiza incidentov in trendi :** možnost dostopa nevladnih organizacij do anonimnih podatkov o nedavnih kibernetskih grožnjah in trendih, ki vplivajo na sektor, kar spodbuja proaktiven pristop h kibernetski varnosti.

• **Mehanizem povratnih informacij :** sistem, ki nevladnim organizacijam omogoča, da posredujejo povratne informacije o svojih izkušnjah s postopkom prijave incidentov in prejeto pomočjo, kar omogoča stalno izboljševanje platforme.

Namen teh zahtev za platformo je poenostaviti postopek poročanja o incidentih za nevladne organizacije, izboljšati njihov dostop do orodij za obnovo in strokovne podpore ter spodbujati okolje sodelovanja med nevladnimi organizacijami, organi kazenskega pregona in prostovoljci na področju kibernetske varnosti. Ta celostni pristop ne pomaga le pri takojšnjem odzivanju na incidente, temveč prispeva tudi k oblikovanju bolj odpornega kibernetskega ekosistema za nevladne organizacije.

Zaključek

Celovita analiza, predstavljena v tej študiji, poudarja kompleksne izzive in ranljivosti na področju kibernetske varnosti, s katerimi se morajo soočiti nevladne organizacije v EU. Kljub **različnim stopnjam razvitosti kibernetske varnosti**, **zaskrbljujoče** : hvalevredna prizadevanja na področjih, kot so postopki varnostnega kopiranja in varnost digitalnega oboda, so izravnana z izrazitimi pomanjkljivostmi na področju zmogljivosti odzivanja na incidente in napredne zaščite končnih točk. **Razširjene ranljivosti** , ugotovljene na področjih varnosti omrežij, **aplikacij in podatkov, ter vrsta kibernetskih incidentov, od napadov z izsiljevalsko programsko opremo do uhajanja poverilnic, kažejo na nujno potrebo po kibernetski varnosti v sektorju humanitarnih nevladnih organizacij v EU.**

Raziskava je razkrila **ključne izzive in priložnosti pri sodelovanju med LEA in nevladnimi organizacijami na področju kibernetske varnosti**. Omejena interakcija in pogoste grožnje, kot je lažno predstavljanje, poudarjajo potrebo po strukturirani komunikaciji in cenovno dostopnih orodjih za kibernetsko varnost. **Enotna platforma za poročanje o kibernetskih grožnjah bi poenostavila poročanje, izboljšala odzivanje na incidente in okrepila sodelovanje med nevladnimi organizacijami.** Z odpravljanjem trenutnih ranljivosti in spodbujanjem proaktivne izmenjave podatkov bi platforma znatno okrepila odpornost nevladnih organizacij na vse večje kibernetske grožnje.

Kot odgovor na te izzive sta razvoj in izvajanje namenske platforme za poročanje o incidentih, kot je predvideno v projektu UnderServed, **postala kritična**. Ta platforma, prilagojena posebnim potrebam in ranljivostim nevladnih organizacij EU, bi bila temelj za izboljšanje upravljanja kibernetskih incidentov in obnovitvi po njih. Z omogočanjem učinkovitega poročanja, sledenja in analize incidentov na področju kibernetske varnosti **bi platforma omogočila hiter odziv in ublažitev posledic**, kar bi znatno zmanjšalo potencialni vpliv kibernetskih napadov na delovanje nevladnih organizacij EU.

Poleg tega bi takšna platforma spodbujala sodelovalno okolje, ki bi skupaj izboljšalo pripravljenost in odpornost sektorja na kibernetsko varnost. Vključitev funkcij, kot so **komunikacijski kanali realnem času, , dostop do orodij za dešifriranje, forenzični viri in podpora prostovoljcev** , še dodatno poudarja vlogo platforme pri odpravljanju kritičnih vrzeli v zmogljivostih kibernetske varnosti nevladnih organizacij EU.

Končno, to poročilo z zagovarjanjem **sistematičnega zbiranja, izmenjave in analize podatkov o kibernetskih incidentih** poudarja, da morajo nevladne organizacije EU nujno sprejeti proaktiven in sodelovalen pristop h kibernetski varnosti. S tem se lahko nevladne organizacije EU ne le branijo pred trenutnimi kibernetskimi grožnjami, temveč tudi **predvidevajo in se pripravljajo na prihodnje izzive**, kar jim zagotavlja, da bodo lahko še naprej nemoteno zagotavljale **ključne humanitarne in razvojne storitve.**

Predlagana platforma za poročanje o incidentih je pomemben korak naprej pri doseganju teh ciljev in pomeni **skupno zavezo za zaščito neprecenljivega prispevka nevladnih organizacij EU v digitalno odvisnem svetu.**

Reference

• Al Achkar, Ziad. n.d. »Doseganje varnega delovanja s sprejemanjem : Izzivi in priložnosti za upravljanje varnostnih tveganj.« [Na spletu]. Na voljo : **https://gisf.ngo/wp-content/uploads/2021/12/Digital_Risk_how_new_technologies_impact_acceptance_and_raise_new_challenges_for_NGOs.pdf**

• B2B Cyber Security, »Ransomware Victim Caritas Refuses to Pay«. 25. september 2022. [Na spletu]. Na voljo : **https://b2b-cyber-security.de/en/ransomware-opfer-caritas-will-nicht-zahlen/**

• Agencija za kibernetsko varnost in varnost infrastrukture CISA, »Known Exploited Vulnerabilities Catalog«. **https://www.cisa.gov/known-exploited-vulnerabilities-catalog?page=1**

• CNN, »Humanitarian aid to Ukraine disrupted by cyberattacks«. 23. april 2022 [Na spletu]. Na voljo : **https://edition.cnn.com/2022/04/23/politics/humanitarian-aid-ukraine-war-cyberattacks/index.html**

• CVE-2019-11043 podrobnost,« NIST National Vulnerability Database. [Na spletu]. Na voljo : **https://nvd.nist.gov/vuln/detail/CVE-2019-11043**

• Inštitut CyberPeace Institute. »Cyber Incident Tracers | CyberPeace Institute,« 10. oktober 2023. **https://cyberpeaceinstitute.org/cyber-incident-tracers**

• Inštitut CyberPeace Institute. «CyberPeace Builders.« CyberPeace Builders, n.d. **https://cpb.ngo/**

• CyberPeace Institute, »Ukrep za izboljšanje : Vloga GCSA pri kibernetski odpornosti neprofitnih organizacij«. 30. januar 2024. [Na spletu]. Na voljo : **https://cyberpeaceinstitute.org/news/measure-to-improve-the-gcsas-role-in-nonprofit-cyber-resilience/**

• Inštitut CyberPeace Institute, »Non-Profit Organization Targeted by Cyberattack : Valuable Lessons for You«. 23. julij 2021. [Na spletu]. Na voljo : **https://cyberpeaceinstitute.org/news/non-profit-organization-targeted-by-cyberattack-valuable-lessons-for-you**

• Komisija za varstvo podatkov (DPC), »Annual Report 2023,« [Na spletu]. Na voljo : **https://www.dataprotection.ie/sites/default/files/uploads/2023-03/DPC%20AR%20English_web.pdf**

· Evropske operacije civilne zaščite in humanitarne pomoči. »Humanitarni partnerji«. 1. februar 2024. [Na spletu]. Na voljo : **https://civil-protection-humanitarian-aid.ec.europa.eu/partnerships/humanitarian-partners_en**

• Forbes, »Hackers Sell Access to a $2 Billion Nonprofit, a Californian Hospital, and Michigan Government« 23. februar 2022. [Na spletu]. Na voljo : **https://www.forbes.com/sites/thomasbrewster/2022/02/23/hackers-sell-access-to-a-2-billion-nonprofit-a-californian-hospital-and-michigan-government/?sh=33a007dc5758**

• Fortiguard, »Riskware/Mewishid«, [Na spletu]. Na voljo : **https://www.fortiguard.com/encyclopedia/virus/7294236**

• Mednarodni odbor Rdečega križa (ICRC), »Kibernetski napad na Mednarodni odbor Rdečega križa : Kaj vemo«. 22. junij 2022 [Na spletu]. Na voljo : **https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know**

• L'Informe, »Les dessous de la cyberattaque contre Akadem, le site du Fonds Social Juif Unifié« [Na spletu]. 4. oktober 2023. Na voljo : **https://www.linforme.com/tech-telecom/article/les-dessous-de-la-cyberattaque-contre-akadem-le-site-du-fonds-social-juif-unifie_1051.html**

• Limerick Leader, »Limerick Domestic Abuse Charity Targeted in Cyber Attack«. 23. marec 2020 [Na spletu]. Na voljo : **https://www.limerickleader.ie/news/home/773188/limerick-domestic-abuse-charity-targeted-in-cyber-attack.html**

• Malpedia, »win.m0yv.« [Na spletu]. Na voljo : **https://malpedia.caad.fkie.fraunhofer.de/details/win.m0yv**

• Malpedia, »win.pseudomanuscrpyt«. [Na spletu]. Na voljo : **https://malpedia.caad.fkie.fraunhofer.de/details/win.pseudo_manuscrypt**

• Microsoft Security, »New sophisticated email-based attack from Nobelium«. 27. april 2021 [Na spletu]. Na voljo : **https://www.microsoft.com/en-us/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/**

• Napačne konfiguracije in slabosti, ki se uporabljajo v kampanjah izsiljevalske programske opreme | CISA« Agencija za kibernetsko varnost in varnost infrastrukture CISA **https://www.cisa.gov/stopransomware/misconfigurations-and-weaknesses-known-be-used-ransomware-campaigns**

• NIST. »Cybersecurity Framework | NIST«. [Na spletu]. Na voljo : **https://www.nist.gov/cyberframework**

• NIST – »CVE-2019-0211.« [Na spletu]. Na voljo : **https://nvd.nist.gov/vuln/detail/CVE-2019-0211**

• NIST – »CVE-2021-40438.« [Na spletu]. Na voljo : **https://nvd.nist.gov/vuln/detail/cve-2021-40438**

• Ralph, Pat. »Fundacija Philabundance postala žrtev kibernetskega napada in izgubila skoraj milijon dolarjev.« PhillyVoice, 1. december 2020. **https://www.phillyvoice.com/philabundance-cyberattack-theft-1-million-dollars/**

• Red Canary, »Gamarue«, [Na spletu]. Na voljo : **https://redcanary.com/threat-detection-report/threats/gamarue/**

• S. C. Leadership, »What is CVSS - Common Vulnerability Scoring System«. 24. oktober 2023. [Na spletu]. Na voljo : **https://www.sans.org/blog/what-is-cvss/**

• Oblikovanje digitalne prihodnosti Evrope. »Politike kibernetske varnosti«. 20. marec 2024. [Na spletu]. Na voljo : **https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies**

• Solidarnostna akcijska mreža, »Resisting Sustained Phishing Attacks«. [Na spletu]. Na voljo : **https://solidarityaction.network/wp-content/uploads/resisting-sustained-phishing-attacks.pdf**

• Mednarodne otroške vasi SOS, »Statement on Cyber Security Incident«. 6. oktober 2024. [Na spletu]. Na voljo : **https://www.sos-childrensvillages.org/news/statement-on-cyber-security-incident**

• Spelhaug, Justin. »Krepitev kibernetske obrambe za neprofitne organizacije.« Microsoft o vprašanjih, 13. december 2021. **https://blogs.microsoft.com/on-the-issues/2021/10/21/cyber-defenses-security-program-nonprofits/**

• Tech Monitor, »EU Disinfo Lab in DDoS Attack«. 20. julij 2020. [Na spletu]. Na voljo : **https://techmonitor.ai/technology/cybersecurity/eu-disinfo-lab-in-ddos-attack**

• Spletna stran CVE (Common Vulnerabilities and Exposures). [Na spletu]. Na voljo : **https://www.cve.org/**

• The Irish Times, »Rehab Group Falls Victim to Cyber Attack«. 16. marec 2022. [Na spletu]. Na voljo : **https://www.irishtimes.com/business/technology/rehab-group-falls-victim-to-cyber-attack-1.4828860**

• ThreatPost, »PseudoManuscrypt' Mass Spyware Campaign Targets 35K Systems«. 16. december 2021. [Na spletu]. Na voljo : **https://threatpost.com/pseudomanuscrypt-mass-spyware-campaign/177097/**

• United Nations University, Institute of Macau, »Civil society organizations' cyber resilience« (Kibernetska odpornost organizacij civilne družbe). 2021. [Na spletu]. **https://collections.unu.edu/eserv/UNU : 8262/Civil_Society_Organizations_Cyber_Resilience.pdf**

• Verizon. »Poročilo o preiskavah kršitev podatkov«. 2023. [Na spletu]. Na voljo : **https://www.verizon.com/business/resources/reports/dbir/**

• Ville De Genève – Uradna spletna stran. »Mednarodne institucije, stalne misije in nevladne organizacije«. 5. februar 2024. [Na spletu]. Na voljo : **https://www.geneve.ch/en/themes/international-geneva/international-institutions-permanent-missions-non-governmental-organisations**

Dodatki

Dodatek I : anketna vprašanja

Vprašanja iz ankete NGO

1. 1A. Ali ima vaša nevladna organizacija posodobljen popis vseh digitalnih in fizičnih sredstev?
2. 2A. Ali vaša nevladna organizacija zagotavlja ustrezno upravljanje uporabniških računov oseb, ki se pridružijo organizaciji ali jo zapustijo (tj. ustvarjanje, posodabljanje, ukinjanje računov)?
3. 3A. Ali vaša nevladna organizacija uporablja postopek za zagotavljanje pravic dostopa na podlagi vlog in odgovornosti uporabnikov?
4. 4A. Ali vaša nevladna organizacija zagotavlja, da so vsa fizična in digitalna sredstva posodobljena in ustrezno konfigurirana?
5. 5A. Ali vaša nevladna organizacija varno odstrani strojno in programsko opremo, ki je ne potrebujete več?
6. 1B. Ali so končne točke vaše nevladne organizacije (računalniki, prenosniki, mobilne naprave) zaščitene s posodobljeno varnostno programsko opremo proti zlonamerni programski opremi in drugim kibernetskim grožnjam (npr. protivirusni program)?
7. 2B. Ali so fizična sredstva vaše nevladne organizacije (npr. računalniki, prenosniki) opremljena z virtualnim požarnim zidom med omrežjem vaše organizacije in internetom?
8. 1C. Ali vaša nevladna organizacija uporablja navidezno zasebno omrežje (VPN), da lahko zaposleni dostopajo do delovnih virov na daljavo?
9. 2C. Ali ima vaša nevladna organizacija seznam vseh storitev v oblaku, ki jih uporablja za namene spremljanja in varnosti (npr. e-pošta, HR, finančno orodje itd.)?
10. 1D. Ali so opredeljene kritične funkcije vaše nevladne organizacije za zagotavljanje bistvenih storitev ranljivim skupinam prebivalstva?
11. 2D. Ali vaša nevladna organizacija varnostno kopira svoje ključne funkcionalne podatke?
12. 3D. Ali so varnostne kopije vaše nevladne organizacije varno shranjene in preverjene za obnovitev?
13. 4D. Ali ima vaša nevladna organizacija vzpostavljen načrt za obnovitev po nesreči v primeru incidenta s področja kibernetske varnosti?
14. 1E. Ali je vaša nevladna organizacija kdaj izvedla pregled ranljivosti spletnega mesta?
15. 2E. Ali je vaša nevladna organizacija kdaj izvedla tehnično oceno varnosti e-pošte?
16. 1F. Ali vaša nevladna organizacija za dostop do občutljivih podatkov ali sistemov (npr. e-pošta, oblak, finančno orodje, družbeni mediji itd.) uporablja večfaktorsko preverjanje pristnosti (MFA)?
17. 2F. Ali vaša nevladna organizacija uporablja upravitelja gesel za varno shranjevanje in upravljanje gesel?
18. 3F. Ali vaša nevladna organizacija izobražuje uporabnike, naj imajo edinstvena in zapletena gesla?
19. 1G. Ali vaša nevladna organizacija svojim zaposlenim in prostovoljcem zagotavlja usposabljanje o kibernetski varnosti?
20. 2G. Ali je vaša nevladna organizacija izvedla simulacije lažnega predstavljanja za vse zaposlene?
21. 1H. Ali je vaša nevladna organizacija sposobna spremljati temni splet, da bi ugotovila morebitno uhajanje podatkov?
22. 2H. Ali je vaša nevladna organizacija sposobna spremljati dejavnosti dnevnikov?
23. I1. Ali ima vaša nevladna organizacija pravilnik kibernetske varnosti?
24. I2. Ali ima vaša organizacija načrt odzivanja na incidente?
25. I3. Ali ima vaša organizacija sklenjeno kibernetsko zavarovanje?
26. I4. Ali ima vaša nevladna organizacija pravilnik o varstvu podatkov?
27. I5. Ali lahko vaša nevladna organizacija šifrira občutljive podatke?
28. I6. Ali vaša nevladna organizacija uporablja varne kanale za izmenjavo občutljivih podatkov?
29. I7. Ali ima vaša nevladna organizacija politiko razkrivanja ranljivosti?
30. I8. Ali ima vaša nevladna organizacija politiko usmerjanja umetne inteligence?

Vprašanja iz ankete LEA

1. Organizacija
2. Polno ime
3. E-pošta
4. Položaj
5. Ali vaša agencija sodeluje z nevladnimi organizacijami v zvezi s kibernetskimi napadi? (da/ne)
    a. Kako pogosto prihaja do teh sodelovanj?

i. Dnevno
ii. Tedensko
iii. Mesečno
iv. Drugo [Prosimo, navedite]

    b. Po katerih kanalih potekajo ta sodelovanja? (e-pošta, telefon, osebno, spletna platforma)
    c. Katere vrste kibernetskih incidentov upravljate za nevladne organizacije?
    d. Kako prednostno obravnavate incidente, o katerih poročajo nevladne organizacije?
    e. S kakšnimi izzivi se soočate pri upravljanju incidentov za nevladne organizacije?
    f. Ali od nevladnih organizacij prejemate podatke o kibernetskih napadih? (da/ne)
    g. Če da, katere vrste podatkov o kibernetskih napadih prejemate od nevladnih organizacij??
    h. Ali lahko delite kakšne zgodbe o uspehu ali pozitivne rezultate sodelovanja z nevladnimi organizacijami pri incidentih kibernetskih napadov?
    i. Kako merite učinek posredovanja vaše agencije pri kibernetskih incidentih, o katerih poročajo nevladne organizacije?

6. Če ne prejmete kakšnih ključnih podatkov, ki bi vam bili koristni, navedite, kateri so ti podatki.
7. Ali uporabljate podatke, ki jih zagotavljajo nevladne organizacije, za odzivanje na kibernetske grožnje in njihovo ublažitev? (da/ne)
8. Kako bi posebna platforma za poročanje o grožnjah koristila vaši agenciji?
9. Katere konkretne podatke, ki bi bili uporabni za vašo agencijo, bi želeli prednostno obravnavati na takšni platformi?
10. Katere funkcije ali prednosti bi lahko ponudila platforma za poročanje o kibernetskih grožnjah, da bi bila bolj uporabna za organe pregona?
11. Ali bi bila podpora ali viri koristni za nevladne organizacije, da bi izboljšale svojo kibernetsko varnost? (da/ne)
12. Če da, kakšna podpora ali viri bi bili koristni za nevladne organizacije, da bi izboljšale svojo kibernetsko varnost?

Dodatek II : Obveščevalni podatki o kibernetskih grožnjah, ki jih je mogoče deliti pod vodstvom nevladnih organizacij

Pri obravnavi večplastne kibernetske varnosti je ključno razumeti različne plasti obveščevalnih podatkov o grožnjah : strateški, taktični, tehnični in operativni. Vsaka od njih ima ključno vlogo pri oblikovanju celovite slike kibernetskih groženj, ki organizacijam omogoča, da se pripravijo, zaščitijo in učinkovito odzovejo na spreminjajoče se digitalne nevarnosti. Z razčlenitvijo teh plasti se poglobimo v globine strategij kibernetske varnosti, od načrtovanja politike na visoki ravni do tehničnih podrobnosti preprečevanja kibernetskih napadov.

1 Kontekstualno obveščanje

1.1 Strateško obveščanje o grožnjah

• **Vir :** Predvsem od vodstva nevladnih organizacij, dopolnjujejo pa jih vpogledi iz zunanjih nasvetov o kibernetski varnosti in obveščevalnih poročil za posamezne sektorje.
• **Opis :** Kontekstualno obveščanje zagotavlja netehnični pregled stanja kibernetske varnosti nevladne organizacije, vključno z razpoložljivostjo dokumentov o upravljanju varnosti (kot so politike varstva podatkov), ranljivostmi in preteklimi incidenti. Vključuje tudi spoznanja, pridobljena na podlagi primerjav v celotnem sektorju, in napovedne analize za predvidevanje novih groženj, na katere vplivajo dejavnosti nevladnih organizacij.
• **Oblika :** Običajno so predstavljeni v besedilni obliki, lahko pa vključujejo tudi predstavitve, poročila in druge vrste človeku berljivih dokumentov.

1.2 Taktično obveščanje o grožnjah

• **Vir :** vodja službe za informacijsko varnost (CISO), ki ga dopolnjujejo tehnično osebje in skupine za odzivanje na incidente.
• **Opis :** taktično obveščanje se nanaša na taktike, tehnike in postopke (TTP), ki so jih akterji groženj uporabili v prejšnjih primerih, usmerjenih neposredno na nevladno organizacijo ali na podobne organizacije. Upoštevani so znani profili slabih akterjev ali skupine nevarnih akterjev, ki so pomembni za nevladne organizacije.
• **Oblika :** Predstavljeno v besedilu in dokumentih. Za večjo interoperabilnost so lahko uporabljeni strukturirani formati, kot sta JSON ali XML.

2 Obveščevalne informacije za posamezne incidente

2.1 Tehnično obveščanje o grožnjah

• **Vir :** ekipa IT nevladne organizacije ali podizvajalci, vključno s prodajalci izdelkov za kibernetsko varnost, ki posredujejo informacije o grožnjah.

• **Opis :** tehnični obveščanje o grožnjah vključujejo neobdelane tehnične podatke, kot so naslovi IP, naslovi URL, podpisi zlonamerne programske opreme, vzorci lažnih elektronskih sporočil, forenzični izpisi in drugi artefakti. Vključuje lahko tudi posebne vrste dnevnikov (npr. požarni zid, omrežje, aplikacija) in priporočene oblike za deljenje.
• **Oblika :** neobdelani tehnični podatki v običajnih formatih, kot sta CSV ali PCAP za omrežni promet.

2.2 Operativno obveščanje o grožnjah

• **Vir :** CISO nevladne organizacije, strokovnjaki za informacijsko varnost ali specializirani podizvajalci, po možnosti dopolnjeni s partnerstvi z zunanjimi skupnostmi za izmenjavo kibernetskih obveščevalnih podatkov.

• **Opis :** operativni obveščevalni podatki omogočajo podroben vpogled v posamezne napade, vključno z njihovo naravo, motivom, časom in načini izvedbe. Upošteva se učinkovitost uporabljenih odzivnih ukrepov in strategij za ublažitev.

• **Oblika :** običajno se delijo v obliki STIX (Structured Threat Information eXpression), kar omogoča standardizirano izmenjavo in analizo prek protokolov, kot je TAXII (Trusted Automated Exchange of Indicator Information), in platform, kot sta MISP (Malware Information Sharing Platform) ali OpenCTI.

Dodatek III : Glosar

• **Napad in kibernetski napad :** moteči kibernetski incident, kršitev varnosti podatkov ali dezinformacijska operacija, ki jo izvede povzročitelj grožnje z uporabo računalniškega omrežja ali sistema z zlonamernim namenom, da bi povzročil škodo (tehnično, finančno, izgubo ugleda ali drugo) ali pridobil/ukradel podatke brez soglasja.

• **Varnostno kopiranje :** kopija računalniških podatkov, ki se hrani v varnem okolju in se uporabi v primeru okvare infrastrukture za ponovno vzpostavitev delujočega sistema.

• **Skupine za odzivanje na računalniške grožnje (CERT) :** skupine CERT so strokovne skupine, ki obravnavajo incidente na področju kibernetske varnosti. Rešitve v oblaku : gre za aplikacije, shranjevanje, storitve na zahtevo, računalniška omrežja ali druge vire, do katerih se dostopa z internetno povezavo prek skupnega okvira računalništva v oblaku drugega ponudnika.

• **Kibernetski mir (Cyberpeace) :** stanje, ko so v digitalnih ekosistemih zagotovljeni varnost, dostojanstvo in pravičnost ljudi..

• **Kibernetska varnost :** varovanje računalniških sistemov in omrežij pred nepooblaščenim razkritjem informacij, krajo ali poškodbo strojne in programske opreme ali elektronskih podatkov. Kibernetska varnost z uporabo tehnologij, postopkov in kontrolnih mehanizmov zmanjšuje tveganje kibernetskih napadov ter ščiti sisteme, omrežja in tehnologije.

• **Kibernetski prostor :** digitalni sistemi in spletni svet sestavljajo kibernetski prostor, ki zajema vse, kar je dostopno prek računalniških omrežij in interneta. To vključuje vse od poslovnih omrežij in platform družabnih medijev do bančnih računov in storitev v oblaku. Vključuje tudi vse povezane naprave, kot so kamere za videonadzor, igralne konzole, televizorji ali robotski sesalniki.

• **Kršitev varnosti podatkov :** izpostavljenost zaupnih, občutljivih ali zaščitenih informacij nepooblaščeni osebi.. To je lahko naključno, na primer disk USB, pozabljen na vlaku, ali priponka e-pošte, poslana napačni osebi, lahko pa je tudi namerno, na primer ko zlonamerni akterji dostopajo do omrežja in izsesajo (ciljajo, kopirajo in prenašajo) podatke.

• **Dešifriranje :** Pretvarjanje šifriranih podatkov (glej opredelitev »Šifriranje«) v prvotno obliko. To je postopek za obrnjeno šifriranje in vračanje podatkov v človeku berljivo obliko.

• **Ključ dešifriranja :** informacije, potrebne za postopek dešifriranja. Dezinformacije : lažne ali zavajajoče informacije, ki se širijo – pogosto prikrito – z namenom zavajanja.

• **Oorazdeljena zavrnitev storitve (DDoS) :** tehnika napada, s katero se omrežje, storitev ali strežnik preplavijo s prevelikim prometom, zaradi česar prenehajo normalno delovati. O porazdeljenem napadu govorimo, kadar je vir napada sestavljen iz več naprav ali sistemov.

• **Domena :** v računalniškem omrežju je domena ime za računalniški vir ali niz računalniških virov, ki jih upravlja en subjekt..

• **DomainKeys Identified Mail (DKIM) :** se uporablja za preverjanje celovitosti e-poštnega sporočila z generiranjem kriptografskih ključev in podpisovanjem odhodnih e-poštnih sporočil z digitalnim podpisom.

• **Šifriranje :** reverzibilen postopek pretvorbe informacij ali podatkov v kodirano obliko z uporabo matematičnih računskih algoritmov. Običajno se uporablja za zaščito občutljivih informacij v mirovanju ali med prenosom, tako da si jih lahko ogledajo le pooblaščene osebe.

• **Požarni zid :** del računalniškega sistema ali omrežja, ki je zasnovan tako, da onemogoča nepooblaščen dostop in hkrati omogoča zunanjo komunikacijo.

• **Haktivisti :** osebe ali skupine, ki pridobijo nepooblaščen dostop do računalniških datotek, sistemov ali omrežij za doseganje družbenih, političnih ali ideoloških ciljev.

• **Odzivanje na incidente :** dejavnosti, ki obravnavajo kratkoročne neposredne učinke incidenta in lahko podpirajo tudi kratkoročno obnovo.

• **Načrt odzivanja na incidente (IRP) :** načrt odzivanja na incidente je dokument, v katerem so opisani postopki, koraki in odgovornosti organizacije v njenem programu odzivanja na incidente..

• **Internet stvari (IoT) :** opisuje pametne naprave, ki so povezane z internetom, vendar niso osebni računalniki ali pametni telefoni.

• **Naslov IP :** v kontekstu informacijske tehnologije naslov internetnega protokola. Malware (zlonamerna programska oprema) : zlonamerna programska oprema. To so deli kode, namenjeni poškodovanju, uničenju ali spodkopavanju računalniških sistemov. Vključuje viruse, ki se lahko razmnožijo in preprečijo delovanje sistemov, izsiljevalsko programsko opremo, ki blokira sisteme, dokler se ne plača odkupnina, in vohunsko programsko opremo, ki je skrita v ciljnem sistemu in vohuni za uporabniki naprave.

• **Starejši sistemi :** zastarelo računalniško programsko in/ali strojno opremo, ki ni sposobna kljubovati sodobnim oblikam napadov in predstavlja tveganje za druge aplikacije in podatke, ki lahko uporabljajo isto infrastrukturo.

• **Napad človeka v sredini (MitM) :** kibernetski napad, pri katerem napadalec na skrivaj posreduje in po možnosti spremeni komunikacijo med dvema strankama, ki sta prepričani, da komunicirata neposredno..

• **Večfaktorosko preverjanje pristnosti (MFA) :** preverjanje pristnosti z uporabo dveh ali več dejavnikov za doseganje preverjanja pristnosti. Faktorji vključujejo : (i) nekaj, kar poznate (npr. geslo/osebna identifikacijska številka [PIN]); (ii) nekaj, kar imate (npr. kriptografska identifikacijska naprava, žeton); ali (iii) nekaj, kar ste (npr. biometrija).

• **Vrata :** navidezna točka, kjer se začnejo in končajo omrežne povezave. Vrata temeljijo na programski opremi in jih upravlja operacijski sistem računalnika. Vsaka vrata so povezana z določenim procesom ali storitvijo. Vrata omogočajo računalnikom, da enostavno razlikujejo med različnimi vrstami prometa : e-poštna sporočila na primer pridejo na druga vrata kot spletne strani, čeprav oboje pride do računalnika prek iste internetne povezave.

• **Ransomware :** vrsta zlonamerne programske opreme, namenjena izsiljevanju denarja s šifriranjem/ blokiranjem dostopa do datotek ali računalniškega sistema, dokler se ne plača odkupnina.. Okvir politike pošiljatelja (SPF) : se uporablja za preverjanje pristnosti domene pošiljatelja s preverjanjem, kateri naslovi IP so legitimni za pošto, poslano iz domene organizacije.

• **Tveganje :** verjetnost škode ali izgube zaradi ranljivosti. Kibernetsko tveganje vključuje grožnje, kot so kibernetski napadi, vdori v podatke in odpovedi sistema, zato je potrebno proaktivno upravljanje za zaščito pred morebitno škodo.

• **Strežnik :** računalnik ali naprava v omrežju, ki upravlja omrežne vire.

• **Socialni inženiring :** psihološka manipulacija z osebo, da bi jo prisilili k nekemu dejanju ali izročitvi informacij.

• **Programska oprema :** niz navodil, podatkov ali programov, ki se uporabljajo za upravljanje računalnikov in izvajanje določenih nalog. Je nasprotje strojne opreme, ki opisuje fizične vidike računalnika.

• **Podtikanje :** ponarejanje naslova pošiljatelja prenosa, da bi pridobili nepooblaščen vstop v varen sistem.

• **Plast varnih vtičnic (SSL) :** internetni varnostni protokol, ki temelji na šifriranju.đ.

• **Načelo najmanjšega privilegija (PoLP) :** koncept informacijske varnosti, ki določa, da mora imeti uporabnik ali subjekt dostop le do določenih podatkov, virov in aplikacij, ki so potrebni za izvedbo zahtevane naloge.

• **Udeleženci groženj :** znani tudi kot akterji kibernetskih groženj ali zlonamerni akterji, posamezniki ali skupine, ki namerno povzročajo škodo digitalnim napravam ali sistemom.

• **Protokol semaforja (TLP) :** protokol zahteva, da oseba, ki pošilja informacije, tem informacijam dodeli barvo z barvno kodo. Ta barva označuje, ali in na kakšen način se te informacije lahko nadalje razširjajo. Nekdo, ki prejme informacije in meni, da jih je mogoče razširjati v večjem obsegu, mora najprej zaprositi za dovoljenje pošiljatelja.

• **Navidezno zasebno omrežje (VPN) :** šifrira vašo povezavo in anonimizira vaš naslov IP. Ustvari varen predor, ki omogoča dostop do notranjih virov. Virus : programska oprema, zasnovana tako, da se razmnožuje in širi v računalniški infrastrukturi.

• **Ranljivost :** ranljivost je napaka v programski opremi, ki jo je mogoče izkoristiti za ogrožanje računalniškega sistema.

• **Požarni zid za spletne aplikacije (WAF) :** pomaga zaščititi spletne aplikacije s filtriranjem in spremljanjem prometa HTTP med spletno aplikacijo in internetom. Spletne aplikacije običajno ščiti pred napadi, kot so med drugim ponarejanje navzkrižnega spletnega mesta, navzkrižno zapisovanje na spletnem mestu (XSS), vključevanje datotek in vbrizgavanje SQL.

• **Spletni strežnik :** računalniški sistem, ki lahko končnim uporabnikom prek interneta prek spletnega brskalnika posreduje spletno vsebino.

• **Ničelno zaupanje :** pristop kibernetske varnosti, ki se osredotoča na uporabnike, sredstva in vire namesto na statične meje, ki temeljijo na omrežju. Ne predpostavlja samodejnega zaupanja na podlagi fizične lokacije ali lastništva sredstev, saj pred odobritvijo dostopa zahteva preverjanje pristnosti in avtorizacijo.