EUROPEAN UNION AGENCY
FOR CYBERSECURITY

PANORÁMA HROZIEB ENISA 2021

Apríl 2020 až polovica júla 2021

OKTÓBER 2021

O AGENTÚRE ENISA

Agentúra Európskej únie pre kybernetickú bezpečnosť, ENISA, je agentúra Únie, ktorej úlohou je zabezpečovať vysokú spoločnú úroveň kybernetickej bezpečnosti v Európe. Agentúra EÚ, ktorá bola zriadená v roku 2004 a ktorej postavenie posilnil akt EÚ o kybernetickej bezpečnosti, prispieva k vytváraniu kybernetickobezpečnostnej politiky EÚ a pomocou systémov certifikácie kybernetickej bezpečnosti zvyšuje dôveryhodnosť produktov, služieb a procesov IKT, spolupracuje s členskými štátmi a orgánmi EÚ a pomáha Európe pripraviť sa na kybernetické výzvy v budúcnosti. Agentúra prostredníctvom spoločného využívania vedomostí, budovania kapacít a zvyšovania informovanosti spolupracuje s kľúčovými zainteresovanými stranami s cieľom posilniť dôveru v rámci prepojenej ekonomiky, zvýšiť odolnosť infraštruktúry Únie a v konečnom dôsledku zachovať digitálnu bezpečnosť európskej spoločnosti a občanov Európy. Ďalšie informácie o agentúre ENISA a jej práci nájdete tu: www.enisa.europa.eu.

KONTAKT

Autorov môžete kontaktovať na adrese etl@enisa.europa.eu.
Na otázky médií týkajúce sa tohto dokumentu použite adresu press@enisa.europa.eu.

EDITORI

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – Agentúra Európskej únie pre kybernetickú bezpečnosť

PRISPIEVATELIA

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

POĎAKOVANIE

Radi by sme sa poďakovali členom a pozorovateľom ad hoc pracovnej skupiny agentúry ENISA pre panorámu kybernetických hrozieb za cenné pripomienky a komentáre pri hodnotení tejto správy. Radi by sme sa tiež poďakovali poradnej skupine agentúry ENISA a sieti národných styčných úradníkov za ich cenné pripomienky. Chceli by sme tiež poďakovať tímu pre situačnú informovanosť a tímu pre oznamovanie incidentov agentúry ENISA za ich aktívny príspevok a podporu pri konsolidácii rôznych informácií do panorámy hrozieb.

PRÁVNE UPOZORNENIE

Upozorňujeme, že tento dokument predstavuje názory a interpretácie agentúry ENISA, pokiaľ nie je uvedené inak. Tento dokument sa nemá považovať za právny krok agentúry ENISA alebo jej orgánov, pokiaľ nie je prijatý v súlade s nariadením (EÚ) č. 2019/881. Agentúra ENISA môže z času na čas tento dokument aktualizovať.

Zdroje tretích strán sú príslušným spôsobom uvedené. Agentúra ENISA nie je zodpovedná za obsah externých zdrojov vrátane externých webových stránok, na ktoré tento dokument odkazuje.

Tento dokument je určený len na informačné účely. Musí byť dostupný bezplatne. Agentúra ENISA ani iná osoba, ktorá koná v jej mene, nenesú zodpovednosť za využitie informácií uvedených v tomto dokumente.

OZNÁMENIE O AUTORSKÝCH PRÁVACH

ISBN: 978-92-9204-536-4 – DOI: 10.2824/324797 – ISSN: 2363-3050

OBSAH

ZHRNUTIE

Toto je deviate vydanie správy agentúry ENISA Panoráma hrozieb (ETL), výročnej správy o stave prostredia kybernetickobezpečnostných hrozieb, ktorá identifikuje hlavné hrozby, hlavné trendy pozorované v súvislosti s hrozbami, aktérov hrozieb a techniky útokov a tiež popisuje príslušné opatrenia na zmiernenie. V procese neustáleho zlepšovania našej metodológie rozvoja panorámy hrozieb bola tohtoročná práca podporovaná novozostavenou ad hoc pracovnou skupinou agentúry ENISA pre panorámu kybernetickobezpečnostných hrozieb (CTL).

Správa ETL 2021 sa týka časového obdobia od apríla 2020 až do júla 2021, ktoré sa v správe označuje ako „sledované obdobie“. Medzi hlavné hrozby identifikované počas sledovaného obdobia patria:

- **ransomvér,**
- **malvér,**
- **kryptojacking,**
- **hrozby súvisiace s e-mailmi,**
- **ohrozenie údajov,**
- **ohrozenie dostupnosti a integrity,**
- **dezinformácie – neúmyselne nepravdivé informácie,**
- **neškodlivé hrozby,**
- **útoky na dodávateľský reťazec.**

V tejto správe budeme diskutovať o prvých 8 kategóriách kybernetickobezpečnostných hrozieb. Ohrozenia dodávateľského reťazca, 9. kategória, bola kvôli osobitnej významnosti podrobne analyzovaná v osobitnej správe agentúry ENISA „Panoráma hrozieb pre dodávateľský reťazec ENISA“[1].

Pre každú z identifikovaných hrozieb sa diskutuje o technikách útoku, významných incidentoch a trendoch spolu s navrhovanými opatreniami na zmiernenie. Pokiaľ ide o trendy, počas sledovaného obdobia zdôrazňujeme nasledovné:

- **Pre roky 2020 – 2021** bol ako **hlavná hrozba** vyhodnotený **ransomvér.**
- **Vládne organizácie rozšírili svoju činnosť** na vnútroštátnej aj medzinárodnej úrovni.
- **Páchatelia počítačovej trestnej činnosti sú čoraz viac motivovaní speňažovaním** svojich aktivít, napríklad ransomvér. **Kryptomena** zostáva najbežnejšou metódou vyplácania pre aktérov hrozieb.
- **Pokles výskytu malvéru** pozorovaný v roku 2020 pokračoval aj počas roku 2021. V roku 2021 sme videli nárast aktérov hrozieb, ktorí sa uchyľujú k relatívne novým alebo nezvyčajným programovacím jazykom na portovanie svojho kódu.
- Objem tzv. **kryptojackingových infekcií** v prvom štvrťroku 2021 **dosiahol rekord** v porovnaní s poslednými rokmi. Aktérov týchto hrozieb motivoval k útokom **finančný zisk** spojený s kryptojackingom.
- **COVID-19 je stále dominantnou návnadou v kampaniach** e-mailových útokov.
- **V zdravotníctve došlo k prudkému nárastu úniku údajov**.
- **Tradičné kampane DDoS (distribuované útoky na vyradenie služby)** sú v roku 2021 cielenejšie, vytrvalejšie a viac multivektorové. **IoT (internet vecí)** v spojení s **mobilnými sieťami** má za následok novú vlnu útokov DDoS.
- V rokoch 2020 a 2021 pozorujeme **prudký nárast neškodlivých incidentov**, keďže pandémia COVID-19 sa stala multiplikátorom **ľudských chýb** a **nesprávnej konfigurácie systému** až do takej miery, že väčšina porušení v roku 2020 bola spôsobená chybami.

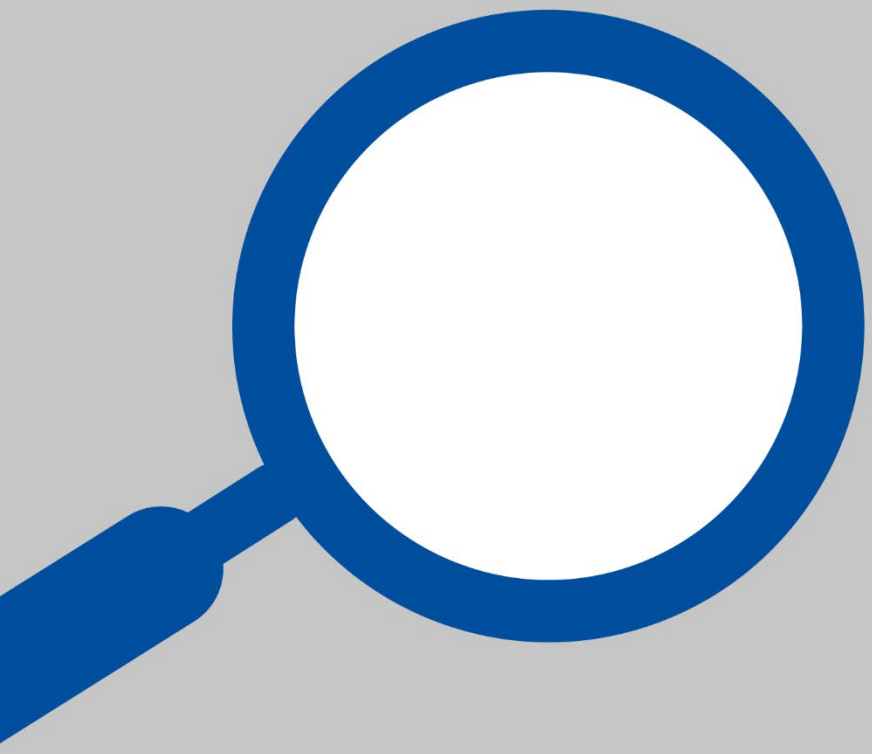
Pochopenie trendov súvisiacich s aktérmi hrozieb, ich motiváciami a cieľmi výrazne pomáha pri plánovaní kybernetickobezpečnostnej obrany a stratégií na zmiernenie. Toto je neoddeliteľnou súčasťou nášho celkového

[1] Panoráma hrozieb pre dodávateľský reťazec ENISA, júl 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

posúdenia hrozieb, pretože to umožňuje stanoviť priority bezpečnostných kontrol a navrhnúť špecializovanú stratégiu založenú na potenciálnych následkoch a pravdepodobnosti naplnenia hrozby. S ohľadom na túto skutočnosť sa na účely správy ETL 2021 berú do úvahy tieto štyri kategórie aktérov kybernetickobezpečnostnej hrozby:

- **aktéri podporovaní štátom,**
- **aktéri z prostredia počítačovej kriminality,**
- **nájomní hakeri,**
- **hacktivisti.**

Pomocou nepretržitej analýzy agentúra ENISA odvodila trendy a body záujmu pre každú z hlavných hrozieb prezentovaných v správe ETL 2021. Kľúčové zistenia a názory v tomto hodnotení sú založené na viacerých a verejne dostupných zdrojoch, ktoré sú uvedené v odkazoch použitých na vypracovanie tohto dokumentu. Správa je určená hlavne tvorcom strategických rozhodnutí a tvorcov politík, ale bude zaujímať aj technickú komunitu kybernetickej bezpečnosti.



PREHĽAD PANORÁMY HROZIEB

Deviate vydanie správy Panoráma hrozieb ENISA (ETL) poskytuje všeobecný prehľad o panoráme kybernetickobezpečnostných hrozieb. Správa ETL je čiastočne strategická a čiastočne technická s informáciami relevantnými pre technických aj netechnických čitateľov. Tohtoročnú prácu podporovala novozostavená ad hoc pracovná skupina agentúry ENISA pre panorámu kybernetickobezpečnostných hrozieb (CTL)[2].

Kybernetickobezpečnostné útoky v rokoch 2020 a 2021 naďalej pribúdali, a to nielen z hľadiska vektorov a počtu, ale aj z hľadiska ich následkov. Podľa očakávania mala na panorámu kybernetickobezpečnostných hrozieb vplyv aj pandémia COVID-19. Jedným z trvalejších trendov vývoja, ktoré vyplynuli z pandémie COVID-19, je pretrvávajúci prechod na hybridný model práce. Preto sa kybernetickobezpečnostné hrozby súvisiace s pandémiou a využívaním „nového normálu“ stávajú hlavným prúdom. Tento trend zvýšil rozsah útokov a v dôsledku toho sme zaznamenali nárast počtu kybernetickobezpečnostných útokov zameraných na organizácie a spoločnosti prostredníctvom práce z domu[3].

Vo všeobecnosti sú kybernetickobezpečnostné hrozby na vzostupe. Vďaka neustále rastúcej online prítomnosti, prechodu tradičných infraštruktúr do režimu online a využívaniu cloudových riešení, rozvinutej vzájomnej prepojenosti a využívaniu nových funkcií vznikajúcich technológií, ako je umelá inteligencia (AI)[4][5], sa panoráma kybernetickej bezpečnosti rozrástla z hľadiska sofistikovanosti útokov, ich zložitosť a následkov. Najvyššiu pozíciu medzi hlavnými hrozbami dosiahli predovšetkým hrozby pre dodávateľské reťazce a ich význam v dôsledku potenciálne katastrofických kaskádových účinkov, a to natoľko že agentúra ENISA vytvorila špeciálnu panorámu hrozieb pre túto kategóriu hrozieb[6].

Stojí za zmienku, že v tejto iterácii správy ETL sa osobitný dôraz kládol na vplyv kybernetickobezpečnostných hrozieb v rôznych odvetviach vrátane odvetví uvedených v smernici o sieťovej a informačnej bezpečnosti (NISD). Zaujímavý pohľad možno získať na základe osobitostí každého odvetvia, pokiaľ ide o panorámu hrozieb, ako aj z potenciálnych vzájomných závislostí a oblastí významu. V súlade s tým si panoráma odvetvových hrozieb zaslúži ďalšiu pozornosť.

Tento rok sa tiež uskutočnilo niekoľko pozoruhodných krokov zo strany obrancov v kybernetickej komunite, ako aj zo strany tvorcov politík. Globálna komunita si začala uvedomovať dôležitosť komunikácie a spolupráce pri vyšetrovaní a sledovaní páchateľov počítačovej trestnej činnosti, pričom ransomvér (najvýraznejšia hrozba za obdobie sledované v správe ETL 2021) sa stal hlavným bodom programov stretnutí o stratégii medzi globálnymi lídrami.

Verní čitatelia predošlých vydaní správy ETL 2021 si všimnú rozdiel v mapovaní hlavných hrozieb. Tento rok agentúra ENISA urobila krok späť a konsolidovala kategórie hrozieb smerom k integrácii a lepšiemu zastúpeniu podobných hrozieb. Je to súčasť prebiehajúceho úsilia o prepracovanú taxonómiu hrozieb a pomôže to metodologicky stanoviť trendy v priebehu niekoľkých nasledujúcich rokov.

Správa ETL 2021 je založená na rôznych informáciách z otvorených zdrojov a zdrojov spravodajských informácií o kybernetických hrozbách. Identifikuje hlavné hrozby, trendy a zistenia a poskytuje relevantné stratégie na zmiernenie rizika na vysokej úrovni. Agentúra ENISA v súčasnosti pracuje na konsolidácii metodiky podávania správ o panoráme hrozieb s cieľom podporiť transparentnosť a konzistentnosť práce.

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM – správa Cena úniku údajov 2020 – https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] Panoráma hrozieb AI ENISA: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
[5] https://www.stealthlabs.com/blog/top-10-cybersecurity-trends-in-2021-and-beyond/
[6] Panoráma hrozieb pre útoky na dodávateľský reťazec ENISA, júl 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

1.1. HLAVNÉ HROZBY

V priebehu rokov 2020 a 2021 sa objavila a realizovala séria kybernetickobezpečnostných hrozieb. Na základe prezentovanej analýzy sa v správe Panoráma hrozieb ENISA 2021 identifikuje nasledujúcich 8 hlavných skupín hrozieb, na ktoré sa správa zameriava (pozrite si Obrázok 1). Týchto 8 skupín hrozieb je zvýraznených z dôvodu ich dôležitosti počas sledovaného obdobia, ich popularity a následkom, ktorý mala realizácia týchto hrozieb.

- **Ransomvér**
  Ransomvér je typ škodlivého útoku, pri ktorom útočníci zašifrujú údaje organizácie a požadujú platbu za obnovenie prístupu. Ransomvér bol hlavnou hrozbou počas sledovaného obdobia s niekoľkými významnými a vysoko medializovanými incidentmi. O význame a dopade hrozby ransomvéru svedčí aj séria súvisiacich politických iniciatív v Európskej únii (EÚ) a vo svete.

- **Malvér**
  Malvér je softvér alebo firmvér určený na vykonávanie neoprávnených procesov, ktoré majú nepriaznivý účinok na dôvernosť, integritu alebo dostupnosť systému. Malvérové hrozby sú už mnoho rokov neustále vysoko hodnotené, aj keď počas obdobia sledovaného v správe ETL 2021 klesajú. Používanie nových techník pripojenia a niektoré významné úspechy pre komunitu presadzovania práva ovplyvnili operácie relevantných aktérov hrozieb.

- **Kryptojacking**
  Kryptojacking alebo skrytá ťažba kryptomeny je typ počítačovej kriminality, pri ktorej zločinec tajne využíva výpočtovú kapacitu obete na generovanie kryptomeny. S rozširovaním kryptomien a ich stále rastúcim využívaním širšou verejnosťou bol pozorovaný nárast zodpovedajúcich kybernetickobezpečnostných incidentov.

- **Hrozby súvisiace s e-mailmi**
  Útoky súvisiace s e-mailom sú zväzkom hrozieb, ktoré využívajú slabé miesta v ľudskej psychike a každodenných návykoch, a nie technickú zraniteľnosť informačných systémov. Je zaujímavé, že napriek mnohým osvetovým a vzdelávacím kampaniam proti týmto typom útokov hrozba do značnej miery pretrváva. Na vzostupe sú najmä ohrozenia obchodných e-mailov a vyspelé sofistikované techniky pri získavaní peňažných príjmov.

- **Ohrozenie údajov**
  Táto kategória zahŕňa porušenia dôvernosti/únik údajov. Porušenia dôvernosti údajov alebo únik údajov je uvoľnenie citlivých, dôverných alebo chránených údajov do nedôveryhodného prostredia. Porušenie dôvernosti údajov môže nastať v dôsledku kybernetického útoku, vnútorného porušenia, neúmyselnej straty alebo vystavenia údajov. Hrozba je naďalej vysoká, keďže prístup k údajom je hlavným cieľom útočníkov z mnohých dôvodov, ako napríklad vydieranie, výkupné, ohováranie, neúmyselne nepravdivé informácie atď.

- **Ohrozenie dostupnosti a integrity**
  Dostupnosť a integrita sú terčom množstva hrozieb a útokov, medzi ktorými vynikajú skupiny vyradenia služby (DoS) a webových útokov. Útok DDoS, ktorý úzko súvisí s webovými útokmi, je jednou z najkritickejších hrozieb pre IT systémy. Zameriava sa na dostupnosť IT systémov vyčerpávaním zdrojov, čo spôsobuje zníženie výkonu, stratu údajov a výpadky služieb. V rámci hrozieb hodnotených agentúrou ENISA sa neustále umiestňuje na popredných miestach, a to z dôvodu prejavu v skutočných incidentoch a potenciálneho dosahu.

- **Dezinformácie – neúmyselne nepravdivé informácie**
  Dezinformačné kampane a kampane neúmyselne nepravdivých informácií sú na vzostupe, ktorý vyvoláva zvýšené využívanie platforiem sociálnych médií a online médií, ako aj v dôsledku nárastu online prítomnosti ľudí v dôsledku pandémie COVID-19. Táto skupina hrozieb sa prvýkrát objavuje v správe ETL, jej význam v kybernetickom svete je však vysoký. Dezinformačné kampane a kampane neúmyselne nepravdivých informácií sa často používajú v hybridných útokoch na zníženie celkového vnímania dôvery, ktorá je hlavným pilierom kybernetickej bezpečnosti.

- **Neškodlivé hrozby**
  Hrozby sa bežne považujú za zámerné a zlomyseľné aktivity zo strany protivníkov, ktorí majú nejaké stimuly na útok na konkrétny cieľ. V tejto kategórii sú zaradené hrozby, pri ktorých nie je zjavný úmysel škodiť. Väčšinou sú založené na ľudských chybách a nesprávnej konfigurácii systému, ale môžu sa vzťahovať aj na reálne katastrofy postihujúce IT infraštruktúru. Tieto hrozby sú aj vzhľadom na svoju povahu neustále prítomné v ročnej panoráme hrozieb a sú hlavným problémom pri hodnotení rizík.

Obrázok 1: Panoráma HROZIEB ENISA 2021 – hlavné hrozby

Je potrebné poznamenať, že vyššie uvedené hrozby zahŕňajú kategórie a súbor hrozieb konsolidovaných do ôsmich vyššie uvedených oblastí. Každá zo skupín hrozieb je ďalej analyzovaná v osobitnej kapitole tejto správy, ktorá rozvádza jej špecifiká a poskytuje konkrétnejšie informácie, zistenia, trendy, techniky útokov a vektory zmierňovania.

1.2. KĽÚČOVÉ TRENDY

V nižšie uvedenom zozname sú zhrnuté hlavné trendy pozorované v panoráme kybernetických hrozieb počas sledovaného obdobia. Aj tieto trendy sú podrobne preskúmané v jednotlivých kapitolách zahŕňajúcich panorámu hrozieb ENISA z roku 2021.

- Rozšírili sa **vysoko sofistikované a účinné ohrozenia dodávateľských reťazcov**, ako to zdôrazňuje špecializovaná panoráma hrozieb pre dodávateľský reťazec. Vysokohodnotnými cieľmi páchateľov počítačovej trestnej činnosti sú **poskytovatelia riadených služieb**.
- Epidémia **COVID-19 podnietila úlohy v oblasti kybernetickej špionáže** a vytvorila **príležitosti pre páchateľov počítačovej trestnej činnosti**.
- **Vládne organizácie rozšírili svoju činnosť** na národnej aj medzinárodnej úrovni. Pozoruje sa zvýšené úsilie vlád rozložiť štátom sponzorovaných aktérov hrozieb a podniknúť proti nim právne kroky.
- **Páchatelia počítačovej trestnej činnosti sú čoraz viac motivovaní speňažovaním** svojich aktivít, napríklad ransomvér. **Kryptomena** zostáva najbežnejšou metódou vyplácania pre aktérov hrozieb.
- Útoky počítačovej kriminality **sa čoraz viac zameriavajú na kritickú infraštruktúru a ovplyvňujú ju.**

- **Ohrozenie prostredníctvom phishingových e-mailov a hrubého vynútenia služieb vzdialenej pracovnej plochy (RDP)** zostávajú dvomi najčastejšími **vektormi ransomvérovej infekcie**.
- Zameranie na **obchodné modely typu RaaS (ransomvér ako služba)** sa v priebehu roku 2021 zvýšilo, čo sťažuje správne pripísanie zodpovednosti jednotlivým aktérom hrozieb.
- Výskyt schémy **trojnásobného vydieračského ransomvéru** sa v priebehu roku 2021 výrazne zvýšil.
- **Pokles výskytu malvéru** pozorovaný v roku 2020 pokračoval aj počas roku 2021. V roku 2021 sme videli nárast aktérov hrozieb, ktorí sa uchyľujú k relatívne novým alebo nezvyčajným programovacím jazykom na portovanie svojho kódu.
- **Malvér zacielený na kontajnerizované prostredia** sa stal oveľa rozšírenejším, pričom nové evolúcie, ako napríklad malvér bez súborov, sa spúšťajú z pamäte.
- Vývojári malvéru neustále hľadajú spôsoby**, ako sťažiť reverzné inžinierstvo a dynamickú analýzu.**
- Objem **kryptojackingových infekcií** v prvom štvrťroku 2021 dosiahol **rekordnú výšku** v porovnaní s poslednými rokmi. Aktérov týchto hrozieb motivoval k útokom **finančný zisk** spojený s kryptojackingom.
- **Objem ťažby kryptomien a aktivity kryptojackingu sú v roku 2021 rekordne vysoké.**
- Vidíme, že dochádza k **posunu od kryptojackingu v prehliadačoch ku kryptojackingu založenému na súboroch**.
- **COVID-19 je stále dominantnou návnadou v kampaniach** e-mailových útokov.
- **Ohrozenie obchodných e-mailov (BEC)** sa **rozšírilo**, zvýšila sa **dômyselnosť** a stalo sa **zacielenejšie**.
- Obchodný model **PhaaS (phishing ako služba)** získava prevahu.
- Aktéri hrozieb presunuli svoju pozornosť na **informácie o vakcínach** v súvislosti s ohrozením údajov a informácií.
- **V zdravotníctve došlo k prudkému nárastu úniku údajov**.
- Tradičné útoky DDoS (distribuované útoky na vyradenie služby) smerujú na **mobilné siete a IoT (internet vecí)**.
- **Ransomové útoky na vyradenie služby (RDoS)** je novou métou útokov na vyradenie služby.
- **Zdieľanie zdrojov vo virtualizovaných prostrediach** pôsobí ako zosilňovač útokov DDoS.
- **Kampane DDoS** sa v roku 2021 stali cielenejšie a omnoho vytrvalejšie a čoraz viac multivektorové.
- **Dezinformácie s podporou umelej inteligencie (AI)** podporujú útočníkov pri ich útokoch.
- **Phishing je jadrom dezinformačných útokov** a silne využíva dôveru ľudí.
- **Neúmyselne nepravdivé informácie a dezinformácie** sú jadrom aktivít v oblasti počítačovej kriminality a nebývalým tempom sa rozširujú.
- **Obchodný model DaaS (dezinformácie ako služba)** sa výrazne rozrástol v dôsledku rastúceho vplyvu pandémie COVID-19 a potreby mať viac informácií.
- V rokoch 2020 a 2021 sme pozorovali **prudký nárast neškodlivých incidentov**, keďže pandémia COVID-19 sa stala multiplikátorom **ľudských chýb** a **nesprávnej konfigurácie systému** až do takej miery, že väčšina porušení v roku 2020 bola spôsobená chybami.
- Došlo k **prudkému nárastu neškodlivých incidentov v oblasti zabezpečenia cloudov**.

1.3. BLÍZKOSŤ HROZIEB PRE EÚ

Dôležitým aspektom, ktorý treba zvážiť v súvislosti s panorámou hrozieb ENISA, je blízkosť kybernetickej hrozby vzhľadom na Európsku úniu (EÚ). Toto je obzvlášť dôležité z hľadiska pomoci analytikom pri hodnotení významnosti kybernetických hrozieb, na ich koreláciu s potenciálnymi aktérmi a vektormi hrozieb a dokonca na usmernenie výberu vhodných cielených vektorov zmierňovania. V súlade s navrhovanou klasifikáciou pre spoločnú bezpečnostnú a obrannú politiku EÚ (SBOP)[7] klasifikujeme kybernetickobezpečnostné hrozby do štyroch kategórií, ako znázorňuje Tabuľka 1.

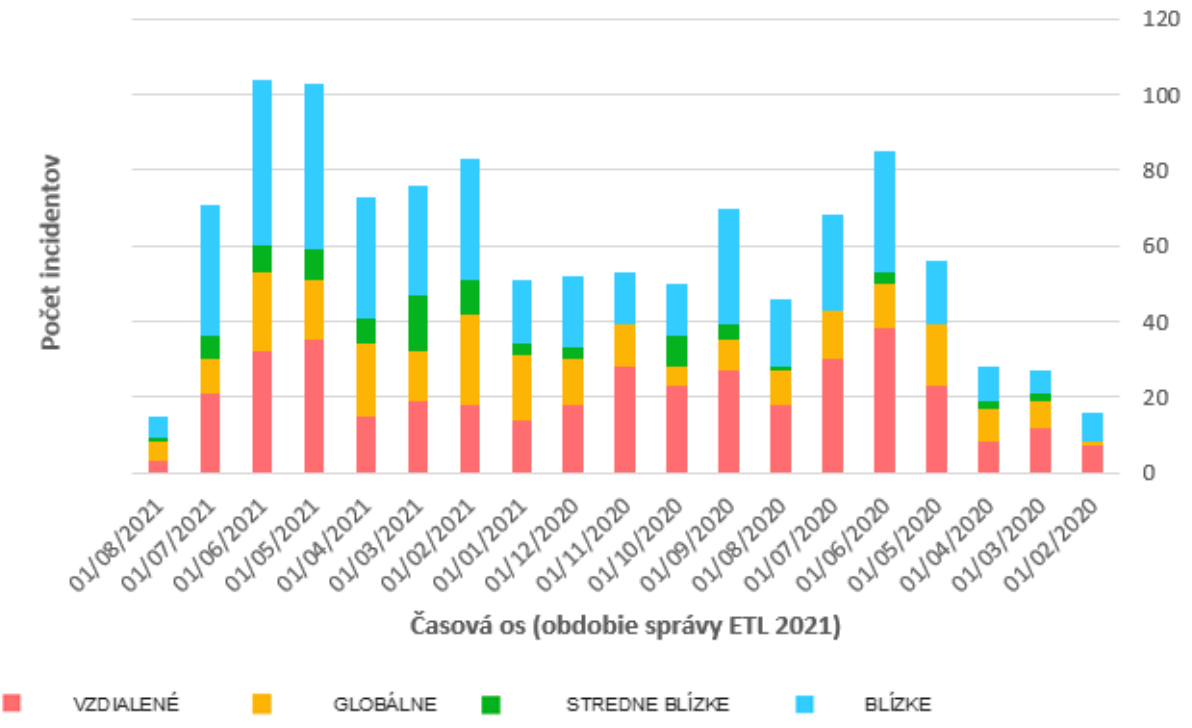
[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf

Tabuľka 1: Klasifikácia blízkosti kybernetickobezpečnostných hrozieb

Blízkosť hrozieb	Obavy
BLÍZKE	Ovplyvnenie sietí a systémov kontrolovaných a zabezpečovaných v rámci hraníc EÚ. Postihnutie obyvateľstva v rámci hraníc EÚ.
STREDNE BLÍZKE	Siete a systémy považované za nevyhnutné pre operačné ciele v rámci jednotného digitálneho trhu EÚ a odvetví podľa smernice NISD, ale ich kontrola a zabezpečenie sa spoliehajú na neinštitucionálne orgány mimo EÚ alebo verejné či súkromné orgány členských štátov. Postihnutie obyvateľstva v geografických oblastiach blízko hraníc EÚ.
VZDIALENÉ	Siete a systémy, ktoré, ak budú zasiahnuté, budú mať rozhodujúci vplyv na operačné ciele v rámci jednotného digitálneho trhu EÚ a odvetví podľa smernice NISD. Na kontrolu a zabezpečenie týchto sietí a systémov nemajú inštitúcie EÚ alebo verejné alebo súkromné orgány členských štátov (ČŠ) dosah. Postihnutie obyvateľstva v geografických oblastiach vzdialených od EÚ.
GLOBÁLNE	Všetky vyššie uvedené oblasti

Obrázok 2 zobrazuje časovú os incidentov súvisiacich s kategóriami hlavných hrozieb uvedených v správe ETL 2021. Je potrebné poznamenať, že informácie v grafe sú založené na spravodajských informáciách z otvorených zdrojov (OSINT) a sú výsledkom práce agentúry ENISA v oblasti situačnej informovanosti[8].

Obrázok 2: Časová os pozorovaných incidentov súvisiacich s hlavnými hrozbami v správe ETL (situačná informovanosť založená na OSINT) z hľadiska ich blízkosti.



[8] V súlade s aktom o kybernetickej bezpečnosti EÚ čl. 7 ods. 6 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

Ako dokazuje obrázok vyššie, v roku 2021 sa zaznamenal vyšší počet incidentov v porovnaní s rokom 2020. Najmä v kategórii BLÍZKE neustále rastie počet pozorovaných incidentov súvisiacich s hlavnými hrozbami, z čoho vyplýva ich význam pre EÚ. Nie je prekvapením, že mesačné trendy (pre stručnosť nie sú na obrázku zobrazené) sú medzi rôznymi klasifikáciami dosť podobné, pretože kybernetická bezpečnosť nepozná hranice a vo väčšine prípadov sa hrozby realizujú na všetkých úrovniach blízkosti. Je pozoruhodné, že počas posledných mesiacov, ktorých sa týka správa ETL 2021, sa v EÚ pozoroval vyšší výskyt hrozieb kategórie BLÍZKE, čo je trend, ktorý bude agentúra ENISA naďalej monitorovať, aby zistila, ako sa vyvíja a ako súvisí s aktivitami aktérov hrozieb a pretrvávajúcimi vektormi hrozieb.

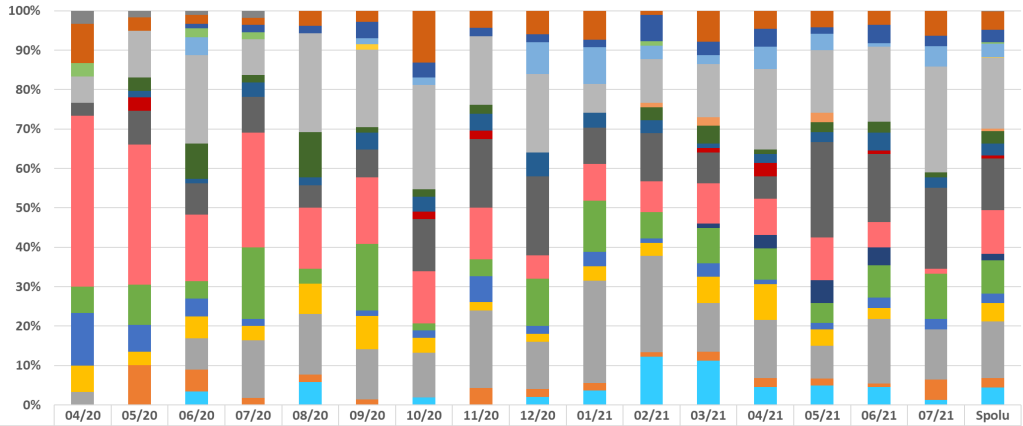
1.4. HLAVNÉ HROZBY PODĽA ODVETVÍ

Kybernetickobezpečnostné hrozby sa zvyčajne neobmedzujú na jedno konkrétne odvetvie a vo väčšine prípadov ovplyvňujú viac ako jedno z nich. To je skutočne pravda, pretože v mnohých prípadoch sa hrozby prejavujú využívaním slabých miest v základných systémoch IKT, ktoré sa používajú v rôznych odvetviach. Cielené útoky, ako aj útoky využívajúce rozdiely vo vyspelosti kybernetickej bezpečnosti medzi odvetviami a popularitu/významnosť určitých odvetví, to všetko sú faktory, ktoré je potrebné zvážiť. Tieto faktory prispievajú k tomu, že hrozby sa prejavujú ako incidenty v konkrétnych odvetviach, a preto je dôležité dôkladne preskúmať aspekty pozorovaných incidentov a hrozieb v odvetviach. Okrem toho trendy zaznamenané v každom odvetví a závislosti medzi odvetviami sú postrehy, ktoré možno z takejto analýzy vyvodiť.

Na obrázku 3 a obrázku 4 sú zdôraznené odvetvia zasiahnuté incidentmi zaznamenanými na základe spravodajských informácií z otvorených zdrojov (OSINT) a sú výsledkom práce agentúry ENISA v oblasti situačnej informovanosti[9]. Týkajú sa incidentov súvisiacich s hlavnými hrozbami v správe ETL 2021. Ide o prvý pokus agentúry ENISA zmapovať vplyv hrozieb na konkrétne odvetvia. V nadchádzajúcich rokoch a v budúcich iteráciách panorámy hrozieb sa vyvinie úsilie na zosúladenie odvetví s odvetviami uvedenými v správe o sieťovej a informačnej bezpečnosti (NISD) a návrhu na jej preskúmanie (NISD 2.0).

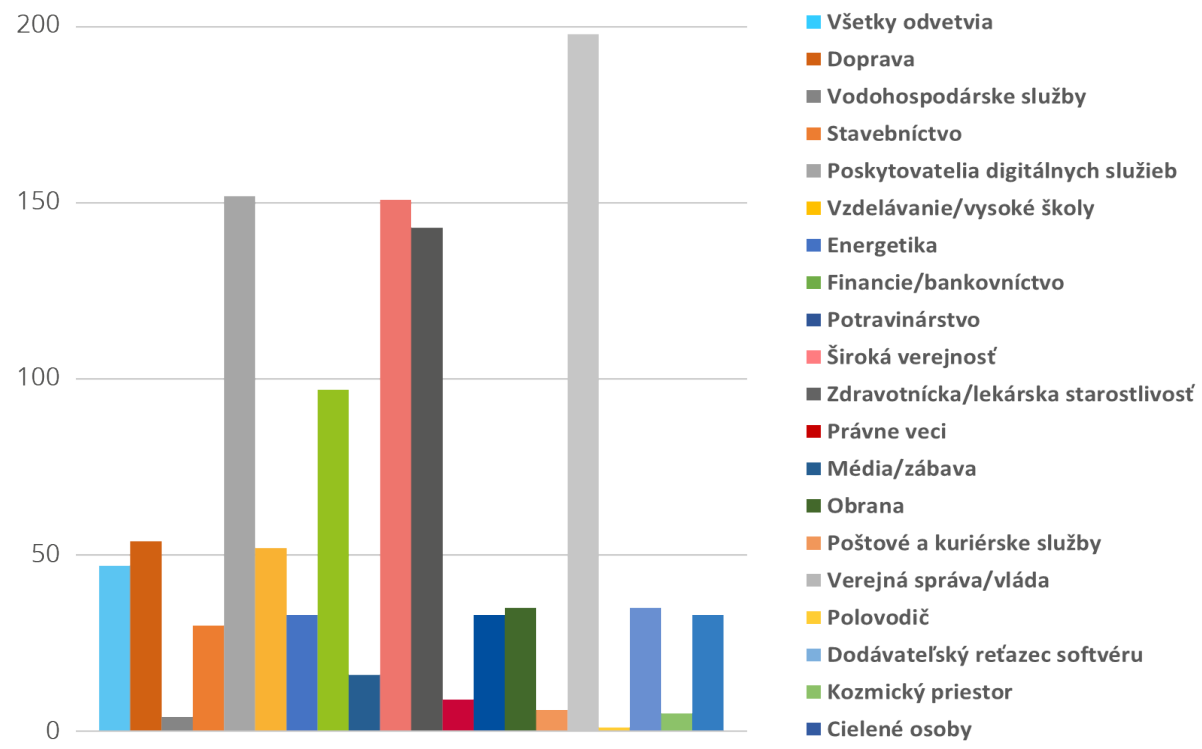
[9] V súlade s aktom o kybernetickej bezpečnosti EÚ čl. 7 ods. 6 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

Obrázok 3: Časová os pozorovaných incidentov súvisiacich s hlavnými hrozbami správy ETL z hľadiska postihnutého odvetvia.



	04/20	05/20	06/20	07/20	08/20	09/20	10/20	11/20	12/20	01/21	02/21	03/21	04/21	05/21	06/21	07/21	Spolu
Vodohospodárske služby	1	1	1	1													2
Doprava	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Cielené osoby			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Kozmický priestor	1		2	1							1						4
Dodávateľský reťazec softvéru			4			1	1		4	5	3	2	5	5	1	4	35
Polovodič						1											1
Verejná správa/vláda	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Poštové a kuriérske služby											1	2		3			6
Obrana		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Média/zábava		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Právne veci		2					1	1				1	3		1		7
Zdravotnícka/lekárska starostlivosť	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Široká verejnosť	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Potravinárstvo												1	3	7	5		16
Financie/bankovníctvo	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Energetika	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Vzdelávanie/vysoké školy	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Poskytovatelia digitálnych služieb	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Stavebníctvo		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Všetky odvetvia			3		3		1		1	2	11	10	4	6	5	1	47

Obrázok 4: Cieľové odvetvia podľa počtu incidentov (apríl 2020 – júl 2021)



Počas tohto sledovaného obdobia sa veľký počet incidentov zameral na verejnú správu a vládu a poskytovateľov digitálnych služieb. To sa dá očakávať vzhľadom na horizontálne poskytovanie služieb pre toto odvetvie, a teda jeho vplyv na mnohé ďalšie odvetvia. Zaznamenali sme tiež značný počet incidentov zameraných na koncových používateľov a nie nevyhnutne na konkrétne odvetvie. Výrazne bolo zasiahnuté aj zdravotníctvo a táto aktivita vykazuje známky nárastu počas posledných mesiacov sledovaného obdobia (máj – júl 2021). Je zaujímavé, že finančné odvetvie čelí počas roka nemeniacemu sa počtu incidentov. Dodávateľský reťazec softvéru tiež vykazuje zvýšený počet incidentov počas roku 2021, čo je tiež zistením v správe Panoráma hrozieb pre dodávateľský reťaze ENISA[10].

1.5. METODIKA

Správa Panoráma hrozieb ENISA (ETL) 2021 je založená na informáciách dostupných z otvorených zdrojov, najmä informácií strategického charakteru, a vlastných spravodajských informáciách o kybernetických hrozbách (CTI) agentúry ENISA a pokrýva viac ako jedno odvetvie, technológiu a kontext. Správa sa usiluje byť nezávislou od odvetví a dodávateľov a v celom texte vo viacerých poznámkach pod čiarou odkazuje alebo cituje práce rôznych výskumníkov v oblasti bezpečnosti, blogov o bezpečnosti a článkov v spravodajských médiách. Správa ETL 2021 sa týka časového obdobia apríl 2020 až júl 2021, ktoré sa v správe označuje ako „sledované obdobie“.

Pri vypracovaní správy ETL 2021 bol použitý nasledujúci prístup. Počas príslušného časového obdobia agentúra ENISA prostredníctvom situačnej informovanosti zhromaždila zoznam hlavných incidentov, ktoré sa objavili v otvorených zdrojoch. Tento zoznam slúžil ako základ pre identifikáciu zoznamu hlavných hrozieb, ako aj zdrojový materiál pre viaceré trendy a štatistických údajov v správe.

Agentúra ENISA a externí experti potom vykonali dôkladný teoretický prieskum dostupnej literatúry z otvorených zdrojov, ako sú články v médiách, názory odborníkov, spravodajské správy, analýzy incidentov a správy o výskume bezpečnosti. Pomocou nepretržitej analýzy agentúra ENISA odvodila trendy a body záujmu pre každú z hlavných

[10] Panoráma hrozieb pre dodávateľský reťazec agentúry ENISA, júl 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

hrozieb prezentovaných v správe ETL 2021. Kľúčové zistenia a názory v tomto hodnotení sú založené na viacerých a verejne dostupných zdrojoch, ktoré sú uvedené v odkazoch použitých na vypracovanie tohto dokumentu.

V správe sa snažíme rozlišovať medzi tým, čo uviedli naše zdroje, a tým, čo je naším hodnotením. (Robíme tak špecificky používaním frázy „v našom hodnotení“). Nakoniec, pri hodnotení vyjadrujeme pravdepodobnosť pomocou slov, ktoré vyjadrujú odhad pravdepodobnosti (napr. pravdepodobné, veľmi pravdepodobné, určite)[11].

V tejto správe bol na zdôraznenie taktiky a techniky útokov relevantných pre danú hrozbu použitý rámec MITRE ATT&CK®[12] (pozrite si prílohu A). Pre každú taktiku ATT&CK® sú uvedené techniky, ktoré protivník použil. To môže viesť k zoznamu zmiernení ATT&CK[13], ktoré sa môžu použiť. MITRE ATT&CK® je vedomostná základňa, spoločný jazyk pre taktiky a techniky protivníka založené na pozorovaniach v reálnom svete. Vedomostná základňa MITRE ATT&CK® sa používa ako základ pre vývoj špecifických modelov hrozieb a metodológií v súkromnom sektore, vo verejnom sektore a v komunite produktov a služieb kybernetickej bezpečnosti.

Správa bola validovaná ad hoc pracovnou skupinou agentúry ENISA pre panorámu kybernetických hrozieb[14], ktorá bola založená v apríli 2021. Táto skupina pozostávala z odborníkov z európskych a medzinárodných subjektov verejného a súkromného sektora.

Pokiaľ ide o budúci rozvoj panorámy hrozieb, agentúra ENISA je v procese formalizácie novej metodológie s cieľom podporiť transparentnosť a vytvoriť základy pre štruktúrované a dobre zosúladené procesy. V rámci tohto úsilia sa spolu s revidovanou taxonómiou hrozieb v budúcnosti zverejní metodika pre panorámy hrozieb.

1.6. ŠTRUKTÚRA SPRÁVY

V Panoráme hrozieb ENISA (ETL) 2021 sa zachovala štruktúra predchádzajúcich správ ETL a použila sa podobná štruktúra na zdôraznenie hlavných kybernetickobezpečnostných hrozieb v roku 2021. Čitatelia minulých správ si všimnú, že kategórie hrozieb boli konsolidované v súlade s posunom k novej taxonómii kybernetickobezpečnostných hrozieb, ktorá sa má používať v budúcnosti.

Správa má túto štruktúru:

V **kapitole 2** sa skúmajú trendy súvisiace s aktérmi hrozieb (t. j. štátom sponzorovanými aktéri, aktérmi počítačovej kriminality, aktérmi najatými hackermi a hacktivistami).
V **kapitole 3** sa diskutujú hlavné zistenia, incidenty a trendy týkajúce sa ransomvéru.
V **kapitole 4** sa uvádzajú hlavné zistenia, incidenty a trendy týkajúce sa malvéru.
V **kapitole 5** sa opisujú hlavné zistenia, incidenty a trendy týkajúce sa kryptojackingu.
V **kapitole 6** sú zdôraznené hlavné zistenia, incidenty a trendy týkajúce sa hrozieb súvisiacich s e-mailmi.
V **kapitole 7** sa diskutujú hlavné zistenia, incidenty a trendy týkajúce sa ohrozenia údajov.
V **kapitole 8** sa uvádzajú hlavné zistenia, incidenty a trendy týkajúce sa ohrozenia dostupnosti a integrity.
V **kapitole 9** sa zdôrazňuje význam hybridných hrozieb a opisujú sa hlavné zistenia, incidenty a trendy týkajúce sa dezinformácií a neúmyselne nepravdivých informácií.
Kapitola 10 sa sústreďuje na hlavné zistenia, incidenty a trendy týkajúce sa neškodných hrozieb.
V **prílohe A** sa na základe rámca MITRE ATT&CK® uvádzajú techniky bežne používané pre jednotlivé hrozby.
V **prílohe B** sú uvedené významné incidenty pre jednotlivé hrozby, ako boli pozorované počas sledovaného obdobia.

[11] CIA – Slová na odhad pravdepodobnostihttps://www.cia.gov/static/0aae8f84700a256abf63f7aad73b0a7d/Words-of-Estimative-Probability.pdf
[12] MITRE ATT&CK®, https://attack.mitre.org/
[13] https://attack.mitre.org/mitigations/enterprise /
[14] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes