EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ZPRÁVA O TYPECH OHROŽENÍ PRO ROK 2021

ŘÍJEN 2021

Duben 2020 až polovina července 2021

O AGENTUŘE ENISA

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) je agenturou Unie, která usiluje o dosažení vysoké společné úrovně kybernetické bezpečnosti v celé Evropě. Agentura Evropské unie pro kybernetickou bezpečnost, která byla zřízena v roce 2004 a následně posílena aktem EU o kybernetické bezpečnosti, se podílí na kybernetické politice EU, prostřednictvím systémů certifikace kybernetické bezpečnosti zvyšuje důvěryhodnost produktů, služeb a procesů informačních a komunikačních technologií (IKT), spolupracuje s členskými státy a útvary EU a pomáhá Evropě připravit se na budoucí kybernetické výzvy. Sdílením znalostí, budováním kapacit a zvyšováním informovanosti usiluje agentura společně s hlavními zúčastněnými stranami o posílení důvěry v propojenou ekonomiku, o podporu odolnosti infrastruktury Unie, a především o zajištění digitální bezpečnosti evropské společnosti a občanů. Více informací o agentuře ENISA a její práci naleznete zde: www.enisa.europa.eu.

KONTAKT

Autory kontaktujte na adrese etl@enisa.europa.eu.
Sdělovací prostředky se s dotazy ohledně tohoto dokumentu mohou obrátit na adresu press@enisa.europa.eu.

EDITOŘI

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – Agentura Evropské unie pro kybernetickou bezpečnost

POSKYTOVATELÉ ÚDAJŮ

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

PODĚKOVÁNÍ

Chtěli bychom poděkovat členům a pozorovatelům *ad hoc* pracovní skupiny agentury ENISA pro oblast kybernetických hrozeb za jejich cennou zpětnou vazbu a komentáře při validaci této zprávy. Také bychom chtěli poděkovat poradní skupině agentury ENISA a síti národních styčných důstojníků za jejich cennou zpětnou vazbu. Rovněž bychom chtěli poděkovat týmům agentury ENISA pro povědomí o situaci a hlášení incidentů za jejich aktivní přínos a podporu při konsolidování různých informací a jejich začleňování podle forem hrozeb.

PRÁVNÍ UPOZORNĚNÍ

Upozorňujeme, že není-li uvedeno jinak, představuje tato publikace stanoviska a názory agentury ENISA. Tato publikace by neměla být považována za právní akt agentury ENISA nebo jejích orgánů, nedojde-li ke schválení podle nařízení (EU) 2019/881. Agentura ENISA může tuto publikaci čas od času aktualizovat.

Zdroje třetích stran jsou patřičně citovány. Agentura ENISA neodpovídá za obsah externích zdrojů, mezi něž patří externí internetové stránky uvedené v této publikaci.

Tato publikace má pouze informativní charakter. Musí být dostupná zdarma. Agentura ENISA ani žádná osoba vystupující jejím jménem nenesou odpovědnost za použití informací obsažených v této publikaci.

OZNÁMENÍ TÝKAJÍCÍ SE AUTORSKÝCH PRÁV

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

OBSAH

SHRNUTÍ

Toto je deváté vydání zprávy o typech ohrožení (ETL), výroční zprávy o stavu kybernetických hrozeb, která identifikuje hlavní hrozby, závažné pozorované trendy z hlediska hrozeb, aktéry hrozeb a metody útoků a také popisuje příslušná zmírňující opatření. V procesu soustavného zlepšování naší metodiky pro vývoj v oblasti forem hrozeb podpořila letošní práci nově vytvořená *ad hoc* pracovní skupina agentury ENISA pro oblast kybernetických hrozeb (CTL).

Zpráva o typech ohrožení pro rok 2021 časově pokrývá období od dubna 2020 do července 2021, které se v této zprávě označuje jako „vykazované období“. Během vykazovaného období patří k hlavním identifikovaným hrozbám:

- **ransomware,**
- **malware,**
- **nelegální těžba kryptoměn,**
- **hrozby v souvislosti s elektronickou poštou,**
- **ohrožení údajů,**
- **ohrožení dostupnosti a integrity,**
- **dezinformace – zavádějící informace,**
- **nezáměrné hrozby,**
- **útoky na dodavatelské řetězce.**

V této zprávě se zabýváme prvními 8 kategoriemi kybernetických hrozeb. Ohrožení dodavatelských řetězců, 9. kategorie, bylo vzhledem k jeho zvláštnímu významu podrobně analyzováno v samostatné zprávě agentury ENISA „Zpráva o typech ohrožení v důsledku útoků na dodavatelské řetězce“ [1].

U každé z identifikovaných hrozeb se zabýváme metodami útoků, významnými incidenty a trendy spolu s navrhovanými zmírňujícími opatřeními. Ve vztahu k trendům během vykazovaného období zdůrazňujeme následující skutečnosti:

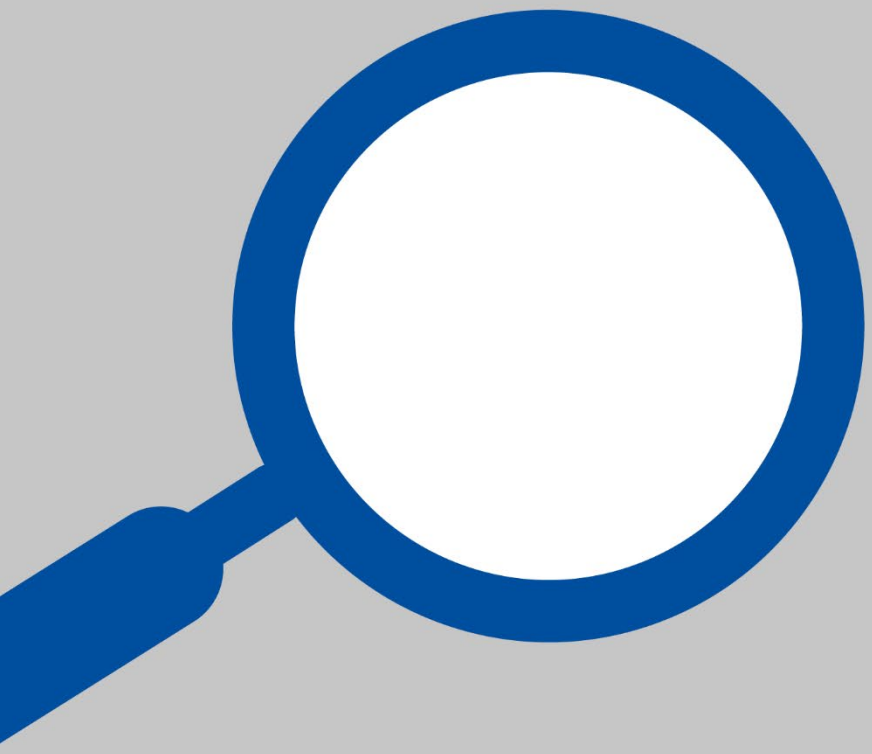
- Jako **hlavní hrozba pro období 2020–2021** je vyhodnocen **ransomware**.
- **Vládní organizace zvýšily své zapojení** na vnitrostátní i mezinárodní úrovni.
- **Pachatele kybernetické kriminality stále více motivuje zpeněžení** jejich aktivit, např. ransomwaru. Nejběžnější metodou vyplácení zůstává pro aktéry hrozeb **kryptoměna**.
- **Pokles malwaru**, který byl pozorován v roce 2020, pokračuje také během roku 2021. V roce 2021 jsme zaznamenali nárůst aktérů hrozeb, kteří se při portování svého kódu uchýlili k relativně novým nebo neobvyklým programovacím jazykům.
- Objem **infekcí v souvislosti s nelegální těžbou kryptoměn** dosáhl v prvním čtvrtletí roku 2021 **rekordní výše** ve srovnání s posledními roky. Při provádění těchto útoků sloužil jako pobídka pro aktéry hrozeb **finanční zisk** související s nelegální těžbou kryptoměn.
- **Dominantním lákadlem v kampaních** zaměřených na e-mailové útoky **je stále COVID-19**.
- **Prudce stoupl počet případů narušení bezpečnosti údajů v sektoru zdravotní péče**.
- **Tradiční kampaně DDoS (útoky distribuovaným odmítnutím služby)** jsou v roce 2021 cílenější, trvalejší a stále více multivektorové. **Internet věcí (IoT)** ve spojení s **mobilními sítěmi** vede k nové vlně útoků DDoS.
- V letech 2020 a 2021 jsme svědky **prudkého nárůstu nezáměrných incidentů**, protože pandemie COVID-19 se stala multiplikátorem **lidských chyb** a **špatných konfigurací systémů** až do té míry, že většina narušení v roce 2020 byla zaviněna chybami.

[1] Zpráva o typech ohrožení v důsledku útoků na dodavatelské řetězce, červenec 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

Při plánování obrany v oblasti kybernetické bezpečnosti a strategií pro zmírňování dopadů značně pomáhá porozumění trendům ve vztahu k aktérům hrozeb, jejich motivaci a jejich cílům. To je nedílnou součástí našeho celkového posuzování hrozeb, protože to umožňuje stanovení priorit bezpečnostních kontrol a navržení konkrétní strategie na základě potenciálního dopadu a pravděpodobnosti uskutečnění hrozby. Z tohoto pohledu připadají pro účely zprávy o typech ohrožení pro rok 2021 v úvahu následující čtyři kategorie aktérů kybernetických hrozeb:

- **státem financované subjekty,**
- **subjekty počítačové kriminality,**
- **nájemní hackeři,**
- **hacktivisté.**

Prostřednictvím průběžné analýzy odvodila agentura ENISA trendy a body zájmu pro každou ze závažných hrozeb představených ve zprávě o typech ohrožení pro rok 2021. Klíčová zjištění a názory v tomto posouzení vycházejí z četných veřejně dostupných zdrojů, které jsou uvedeny v odkazech použitých při tvorbě tohoto dokumentu. Zpráva je určena zejména pro tvůrce strategických rozhodnutí a politik, ale bude zajímat také odbornou obec v oblasti kybernetické bezpečnosti.



PŘEHLED FOREM HROZEB

Ve svém devátém vydání nabízí zpráva o typech ohrožení (ETL) obecný přehled forem kybernetických hrozeb. Zpráva o typech ohrožení je zčásti strategická a zčásti technická, s informacemi určenými pro technicky i jinak zaměřené čtenáře. Letošní práci podpořila nově vytvořená *ad hoc* pracovní skupina agentury ENISA pro oblast kybernetických hrozeb (CTL)[2].

Útoky v oblasti kybernetické bezpečnosti v letech 2020 a 2021 stále rostly, nejen z hlediska vektorů a počtů, ale také z hlediska dopadu. Na oblast kybernetických hrozeb měla – podle očekávání – dopad také pandemie COVID-19. Jedním z trvalejších důsledků, které vyplynuly z pandemie COVID-19, je trvající posun k modelu hybridní kanceláře. Proto se hrozby v oblasti kybernetické bezpečnosti související s pandemií a využívající tento „nový normální stav“ stávají běžnými. Tento trend zvýšil prostor k útokům a v důsledku toho jsme byli svědky nárůstu počtu kybernetických útoků mířících na organizace a společnosti přes domácí kanceláře[3].

Kybernetické hrozby obecně rostou. Urychlující vliv rostoucí on-line přítomnosti, přechodu tradičních infrastruktur na on-line a cloudová řešení, pokročilé vzájemné propojenosti a využívání nových vlastností vznikajících technologií, jako je umělá inteligence (AI)[4][5], rozšířil oblast kybernetických hrozeb z hlediska sofistikovanosti útoků, jejich složitosti i jejich dopadu. Nejvyššího postavení mezi závažnými hrozbami dosáhla zejména hrozba pro dodavatelské řetězce a její významnost z důvodu potenciálních katastrofických kaskádových efektů, a to natolik, že agentura ENISA vypracovala pro tuto kategorii hrozeb samostatnou zprávu o typech ohrožení[6].

Stojí za zmínku, že v této verzi zprávy o typech ohrožení se zaměřuje zvláštní pozornost na dopad kybernetických hrozeb v různých sektorech včetně sektorů uvedených ve směrnici o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů (NISD). Ze specifik každého sektoru lze získat zajímavé poznatky, pokud jde o formy hrozeb i potenciální vzájemné vztahy a důležité oblasti. Proto si formy odvětvových hrozeb zasluhují další pozornost.

V letošním roce došlo také k některým významným krokům ze strany obránců v kybernetické komunitě i ze strany tvůrců politik. Světové společenství si začalo uvědomovat význam komunikace a spolupráce při vyšetřování a sledování pachatelů kybernetické kriminality, přičemž hlavním bodem na programech schůzek předních globálních představitelů zabývajících se strategií se stává zejména ransomware (nejvýznamnější hrozba za vykazované období zprávy o typech ohrožení pro rok 2021).

Pozorní čtenáři minulých vydání zprávy o typech ohrožení pro rok 2021 si povšimnou rozdílu v mapování hlavních hrozeb. V tomto roce agentura ENISA učinila krok zpět a kategorie hrozeb sjednotila ve snaze o integraci a lepší vylíčení podobných hrozeb. Jde o součást soustavného úsilí o přepracování taxonomie hrozeb, jež pomůže při metodickém určování trendů v průběhu následujících několika let.

Zpráva o typech ohrožení pro rok 2021 vychází z volně přístupných zdrojů informací a zdrojů operativních informací o hrozbách. Identifikuje závažné hrozby, trendy a zjištění a poskytuje příslušné rámcové strategie pro zmírnění. Agentura ENISA v současnosti pracuje na posílení metodiky pro hlášení forem hrozeb s cílem podpořit transparentnost a konzistentnost této práce.

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM – Zpráva o nákladech na narušení ochrany údajů za rok 2020 – https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] Zpráva o typech ohrožení v souvislosti s umělou inteligencí: 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] Zpráva o typech ohrožení v důsledku útoků na dodavatelské řetězce, červenec 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

1.1. HLAVNÍ HROZBY

V průběhu let 2020 a 2021 se objevila a uskutečnila řada kybernetických hrozeb. Na základě analýzy předložené v této zprávě identifikuje zpráva o typech ohrožení pro rok 2021 následujících 8 hlavních skupin hrozeb a na tyto hrozby se zaměřuje (viz Obrázek 1). Těchto 8 skupin hrozeb je zdůrazněno kvůli jejich důležitosti během vykazovaného období, jejich popularitě a dopadu, který mělo naplnění těchto hrozeb.

- **Ransomware**
  Ransomware je typem úmyslného útoku, kdy útočníci zašifrují data organizace a za obnovení přístupu k nim požadují platbu. Ransomware byl během vykazovaného období hlavní hrozbou, doprovázenou několika závažnými a vysoce medializovanými incidenty. Význam a dopad hrozby ransomwaru rovněž dokládá řada souvisejících politických iniciativ v Evropské unii (EU) i ve světě.

- **Malware**
  Malware je software nebo firmware určený k provádění neoprávněného procesu, který bude mít nepříznivý dopad na důvěrnost, integritu nebo dostupnost systému. Hrozba malwarem má už řadu let soustavně vysoké postavení, ovšem ve vykazovaném období zprávy o typech ohrožení pro rok 2021 klesá. Používání nových metod útoků a některé důležité úspěchy orgánů vymáhání práva měly na operace příslušných aktérů hrozeb dopad.

- **Nelegální těžba kryptoměn**
  Nelegální nebo také skrytá těžba kryptoměn je typem kybernetické kriminality, kdy pachatel tajně používá výpočetní výkon oběti k těžbě kryptoměn. S šířením kryptoměn a jejich zvyšujícím se přijímáním širší veřejností byl zaznamenán nárůst odpovídajících kybernetických bezpečnostních incidentů.

- **Hrozby v souvislosti s elektronickou poštou**
  Útoky související s elektronickou poštou jsou skupinou hrozeb, které využívají spíše slabin v lidské psychice a každodenních zvycích než technické zranitelnosti informačních systémů. Je zajímavé, že navzdory mnoha informačním a vzdělávacím kampaním zaměřeným na tyto typy útoků jejich hrozba ve značné míře přetrvává. Zvláště pak přibývá zneužívání firemních e-mailů a pokročilých sofistikovaných metod dosahování peněžních zisků.

- **Ohrožení údajů**
  Tato kategorie zahrnuje narušení ochrany / úniky údajů. Narušení ochrany údajů nebo únik údajů je únik citlivých, důvěrných nebo chráněných údajů do nedůvěryhodného prostředí. K narušení ochrany údajů může dojít v důsledku kybernetického útoku, působení zaměstnanců, neúmyslné ztráty nebo volného zpřístupnění údajů. Hrozba je nadále vysoká, protože přístup k údajům je hlavním cílem útočníků z řady důvodů, např. kvůli vydírání, výkupnému, ublížení na cti, zavádějícím informacím atd.

- **Ohrožení dostupnosti a integrity**
  Dostupnost a integrita jsou cílem velkého množství hrozeb a útoků, mezi nimiž dominují skupiny odmítnutí služby (DoS) a webových útoků. Útoky DDoS, úzce související s webovými útoky, patří k nejkritičtějším hrozbám pro systémy IT, protože cílí na jejich dostupnost skrze vyčerpání zdrojů, v důsledku čehož dojde ke snížení výkonu, ztrátě dat a výpadkům služeb. Tato hrozba se ve zprávě o typech ohrožení soustavně drží vysoko, a to kvůli svým projevům při skutečných incidentech i kvůli potenciálním vysokým dopadům.

- **Dezinformace – zavádějící informace**
  Kampaně založené na dezinformacích a zavádějících informacích jsou na vzestupu, podporované stoupajícím využíváním platforem sociálních médií a on-line médií i v důsledku nárůstu on-line přítomnosti občanů kvůli pandemii COVID-19. Tato skupina hrozeb se ve zprávě o typech ohrožení objevuje poprvé, ovšem její význam v kybernetickém prostředí je velký. Kampaně založené na dezinformacích a zavádějících informacích se často využívají při hybridních útocích s cílem snížit celkové vnímání důvěry, důležitého faktoru kybernetické bezpečnosti.

- **Nezáměrné hrozby**
  Za hrozby jsou obvykle považovány svévolné a záměrné aktivity zahájené protivníky, kteří mají motivaci k útoku na specifický cíl. V této kategorii se zabýváme hrozbami, u nichž není úmyslný záměr zjevný. Jejich základem jsou obvykle lidské chyby a špatná konfigurace systémů, ale může se také jednat o fyzické katastrofy, které

postihnou IT infrastrukturu. Právě v důsledku své povahy mají tyto hrozby každoročně trvalé místo mezi formami hrozeb a zásadní význam pro posouzení rizik.

Obrázek 1: Zpráva o typech ohrožení 2021 – hlavní hrozby

Je třeba poznamenat, že výše uvedené hrozby zahrnují kategorie a soubor hrozeb, sjednocené do osmi výše uvedených oblastí. Každá ze skupin hrozeb je dále analyzována v samostatné kapitole této zprávy, která podrobně popisuje její specifika a uvádí konkrétnější informace, zjištění, trendy, metody útoku a vektory zmírnění.

1.2. KLÍČOVÉ TRENDY

Následující seznam shrnuje hlavní trendy pozorované v oblasti kybernetických hrozeb během vykazovaného období. Podrobně se jimi zabývají i různé kapitoly tvořící zprávu o typech ohrožení pro rok 2021.

- Šířila se **vysoce sofistikovaná a vlivná narušení dodavatelského řetězce**, jak vyzdvihla samostatná zpráva o typech ohrožení v důsledku útoků na dodavatelské řetězce. **Poskytovatelé spravovaných služeb** jsou pro pachatele kybernetické kriminality cíli s vysokou hodnotou.
- **COVID-19 se stal motivem úkolů v oblasti kybernetické špionáže** a vytvořil **příležitosti pro pachatele kybernetické kriminality**.
- **Vládní organizace zvýšily své zapojení** na vnitrostátní i mezinárodní úrovni. Bylo zaznamenáno zvýšené úsilí vlád o narušování činnosti státem financovaných aktérů hrozeb a podnikání příslušných právních kroků.
- **Pachatele kybernetické kriminality stále více motivuje zpeněžení** jejich aktivit, např. ransomwaru. Nejběžnější metodou vyplácení zůstává pro aktéry hrozeb **kryptoměna**.
- Kybernetické útoky **se stále více zaměřují a dopadají na kritickou infrastrukturu**.
- **Zneužívání formou phishingových e-mailů a útoky hrubou silou na služby vzdálené plochy (RDP)** zůstávají dvěma nejběžnějšími **vektory infekce ransomwarem**.
- Zaměření na **obchodní modely typu ransomware jako služba** (**RaaS)** se během roku 2021 zvýšilo, a ztížilo tak příslušné přiřazování jednotlivých aktérů hrozeb.
- Výskyt formy **trojitého vydírání ransomwarem** v průběhu roku 2021 výrazně vzrostl.

- **Pokles malwaru**, který byl pozorován v roce 2020, pokračuje i během roku 2021. V roce 2021 jsme zaznamenali nárůst aktérů hrozeb, kteří se při portování svého kódu uchýlili k relativně novým nebo neobvyklým programovacím jazykům.
- Začal mnohem více převládat **malware zaměřený na kontejnerová prostředí**, kdy se nové výsledky vývoje, jako je bezsouborový malware, spouštějí z paměti.
- Vývojáři malwaru neustále hledají způsoby, jak **ztížit reverzní inženýrství a dynamické analýzy**.
- Objem **infekcí v souvislosti s nelegální těžbou kryptoměn** dosáhl v prvním čtvrtletí roku 2021 **rekordní výše** v porovnání s několika posledními roky. Při provádění těchto útoků sloužil jako pobídka pro aktéry hrozeb **finanční zisk** související s nelegální těžbou kryptoměn.
- **Objem těžby kryptoměn v roce 2021 a aktivity v oblasti nelegální těžby kryptoměn jsou na rekordní výši**.
- Vidíme, že dochází k **přesunu nelegální těžby kryptoměn z prohlížeče na souborovou bázi**.
- **Dominantním lákadlem v kampaních** zaměřených na e-mailové útoky **je stále COVID-19**.
- **Zneužívání firemních e-mailů (BEC)** se **zvýšilo**, je **sofistikovanější** a začalo být **cílenější**.
- Začíná převažovat obchodní model **phishing jako služba (PhaaS)**.
- V kontextu ohrožení údajů a informací přesunuli aktéři hrozeb svoji pozornost k **informacím o vakcínách**.
- **Prudce stoupl počet případů narušení bezpečnosti údajů v sektoru zdravotní péče**.
- Tradiční útoky typu DDoS (distribuované odmítnutí služby) se přesunují na **mobilní sítě a internet věcí (IoT)**.
- Novou frontou útoků odmítnutím služby je **odmítnutí služby s požadavkem výkupného (RDoS)**.
- **Sdílení zdrojů ve virtualizovaných prostředích** funguje jako zesilovač útoků DDoS.
- **DDoS kampaně** začaly být v roce 2021 cílenější, mnohem trvalejší a stále více multivektorové.
- Útočníky při provádění útoků podporují **dezinformace využívající umělou inteligenci (AI)**.
- **Jádrem dezinformačních útoků je phishing**, který a silně využívá důvěry občanů.
- Jádrem aktivit v oblasti kybernetické kriminality jsou **zavádějící informace a dezinformace**, jež přibývají v bezprecedentní míře.
- **Obchodní model dezinformace jako služba (DaaS)** výrazně posílil, poháněn zvyšujícím se dopadem pandemie COVID-19 a potřebou mít více informací.
- V letech 2020 a 2021 jsme byli svědky **prudkého nárůstu nezáměrných incidentů**, protože pandemie COVID-19 se stala multiplikátorem **lidských chyb** a **špatných konfigurací systémů** až do té míry, že většina narušení v roce 2020 byla zavíněna chybami.
- Došlo k **prudkému nárůstu nezáměrných incidentů v oblasti cloudové bezpečnosti**.

1.3. BLÍZKOST HLAVNÍCH HROZEB PRO EU

Důležitým aspektem, který je v souvislosti se zprávou o typech ohrožení nutno brát v úvahu, je blízkost kybernetických hrozeb ve vztahu k Evropské unii (EU). Ta je pro analytiky obzvlášť důležitá, protože jim pomáhá posoudit význam kybernetických hrozeb a uvést je do souvislostí s potenciálními aktéry a vektory hrozeb, a dokonce jim slouží jako vodítko pro výběr vhodných cílených zmírňujících vektorů. V souladu s navrhovanou klasifikací pro společnou evropskou bezpečnostní a obrannou politiku (SBOP)[7] dělíme kybernetické hrozby do čtyř kategorií, které uvádí **Table 1**.

Tabulka 1: Klasifikace blízkosti kybernetických hrozeb

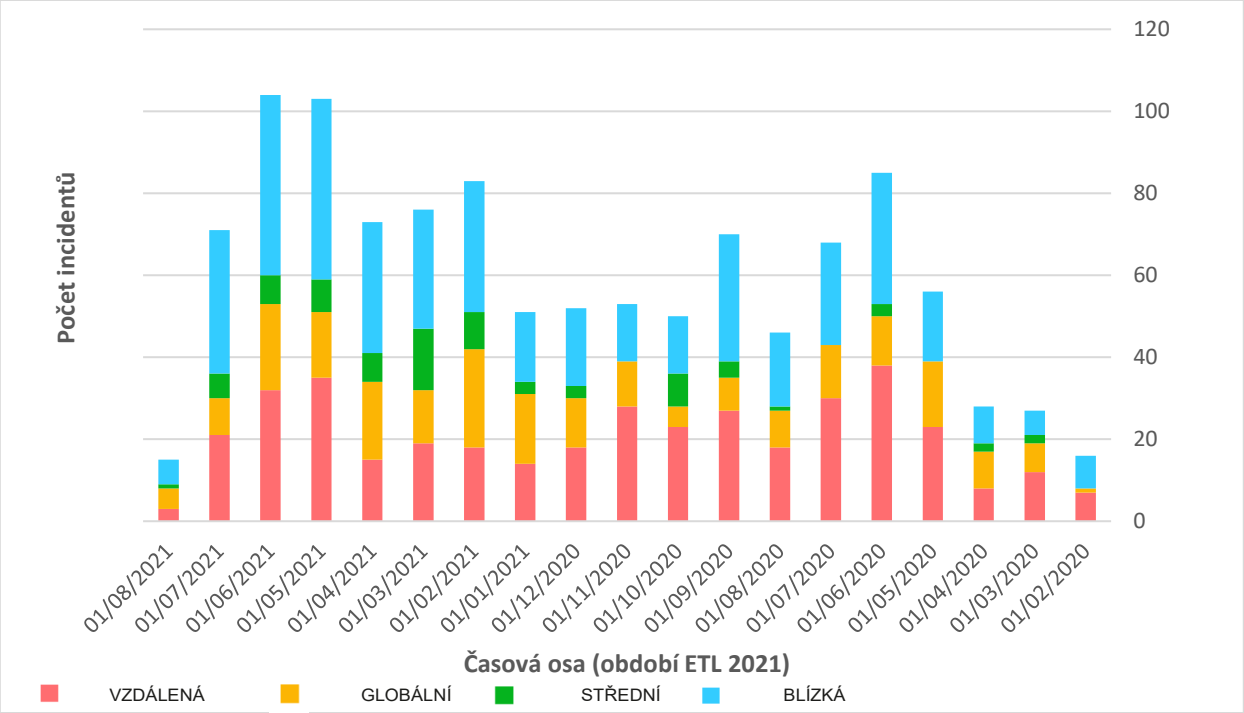
Blízkost	Koho/čeho se týká
BLÍZKÁ	Postižené sítě a systémy, kontrolované a zajišťované v rámci hranic EU. Postižené obyvatelstvo v rámci hranic EU.
STŘEDNÍ	Sítě a systémy považované za životně důležité pro provozní cíle v rámci jednotného digitálního trhu EU a sektorů podle směrnice NISD, jejichž kontrola a zajištění se spoléhají na institucionální

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

Blízkost	Koho/čeho se týká
	orgány mimo EU nebo veřejné či soukromé orgány členských států. Postižené obyvatelstvo v zeměpisných oblastech blízko hranic EU.
VZDÁLENÁ	Sítě a systémy, které v případě ovlivnění budou mít kritický dopad na provozní cíle v rámci jednotného digitálního trhu EU a sektorů podle směrnice NISD. Kontrola a zajištění těchto sítí a systémů leží mimo institucionální orgány EU nebo veřejné či soukromé orgány členských států. Postižené obyvatelstvo v zeměpisných oblastech vzdálených od EU.
GLOBÁLNÍ	Všechny výše uvedené oblasti

Obrázek 2 ilustruje časovou osu incidentů ve vztahu ke kategoriím hlavních hrozeb vykazovaným ve zprávě o typech ohrožení pro rok 2021. Je potřeba uvést, že informace v grafu vycházejí ze zpravodajských informací z otevřených zdrojů (OSINT) a jsou výsledkem práce agentury ENISA v oblasti povědomí o situaci[8].

Obrázek 2: Časová osa pozorovaných incidentů ve vztahu k závažným hrozbám podle zprávy o typech ohrožení (povědomí o situaci na bázi OSINT) z hlediska jejich blízkosti.



Jak dokládá výše uvedený obrázek, ve srovnání s rokem 2020 došlo v roce 2021 k vyššímu počtu incidentů. Zejména v kategorii BLÍZKÝCH hrozeb soustavně roste počet pozorovaných incidentů ve vztahu k hlavním hrozbám, což naznačuje jejich význam v kontextu EU. Není překvapivé, že měsíční trendy (na obrázku neznázorněné kvůli stručnosti) jsou mezi různými klasifikacemi celkem podobné, protože kybernetická bezpečnost nezná hranic a ve většině případů se mohou hrozby vyskytnout na všech úrovních blízkosti. Stojí za zmínku, že během posledních měsíců zahrnutých do zprávy o typech ohrožení pro rok 2021 bylo v kategorii BLÍZKÝCH hrozeb

[8] V souladu s aktem EU o kybernetické bezpečnosti čl. 7 odst. 6 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

pozorováno vyšší přiblížení EU. Tento trend bude agentura ENISA dále monitorovat, aby zjistila, jak se vyvíjí a jak souvisí s aktivitami aktérů hrozeb a aktuálními vektory hrozeb.

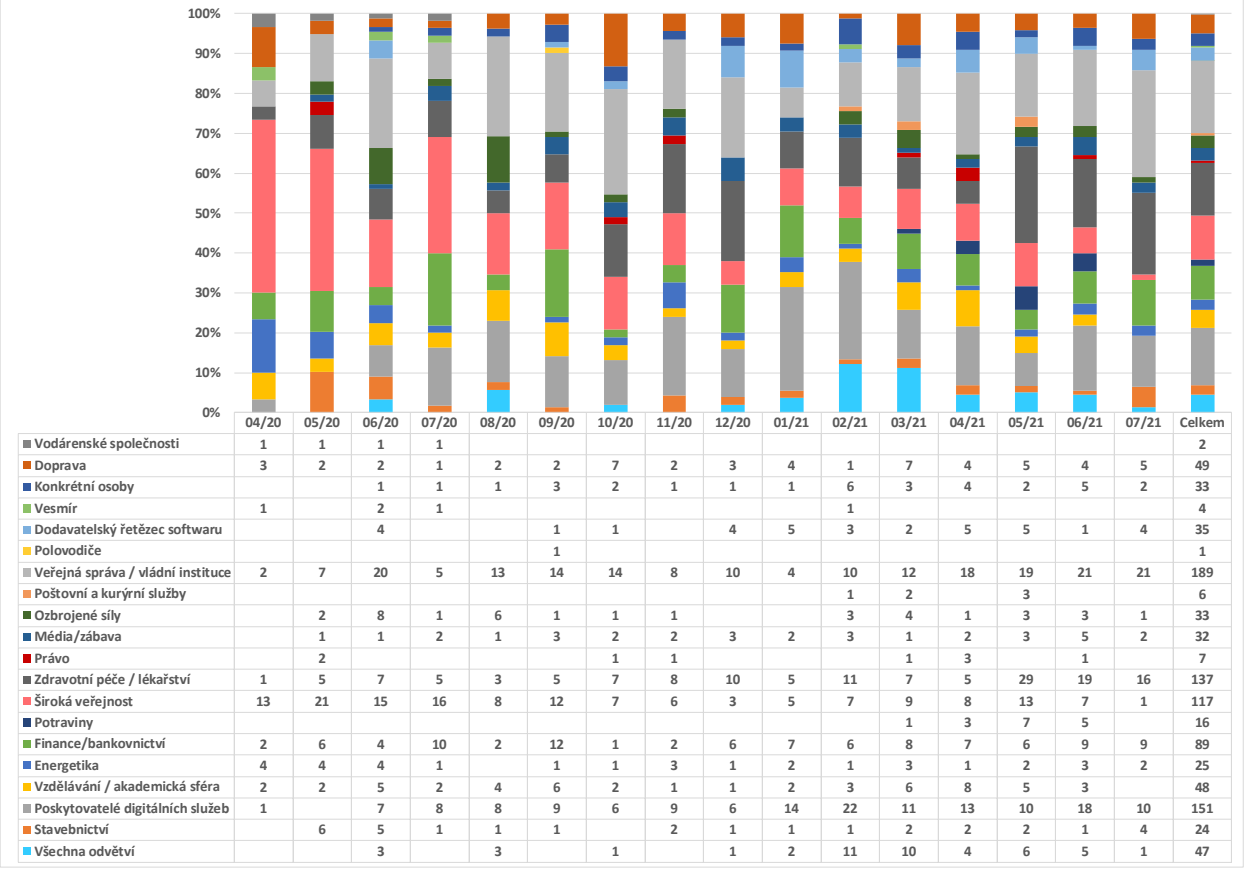
1.4. HLAVNÍ HROZBY PODLE SEKTORŮ

Kybernetické hrozby se obvykle neomezují na jeden konkrétní sektor a ve většině případů jich ovlivňují více. To je skutečně pravda, protože v mnoha případech se hrozby projevují tím, že využívají zranitelnosti v základních systémech IKT, které se využívají v různých sektorech. Je však potřeba brát v úvahu všechny faktory, jako jsou cílené útoky i útoky využívající rozdíly ve vyspělosti kybernetické bezpečnosti napříč sektory a popularitu/význam některých sektorů. Tyto faktory přispívají k hrozbám, které se projevují jako incidenty v konkrétních sektorech, a proto je důležité se důkladně podívat na sektorové aspekty pozorovaných incidentů a hrozeb. Dále lze z takové analýzy čerpat trendy zaznamenané v každém sektoru a vztahy napříč sektory.

Obrázek 3 a obrázek 4 ozřejmují postižené sektory, pokud se jedná o incidenty pozorované na základě zpravodajských informací z otevřených zdrojů (OSINT), a jsou výsledkem činnosti agentury ENISA v oblasti povědomí o situaci[9]. Uvádějí incidenty související s hlavními hrozbami ve zprávě o typech ohrožení pro rok 2021. Toto je první pokus agentury ENISA o zmapování dopadů hrozeb na konkrétní sektory. V příštích letech a v budoucích verzích zpráv o typech ohrožení se budeme snažit o sladění sektorů se sektory uvedenými ve směrnici o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů (NISD) a návrhu jejího přezkumu (NISD 2.0).

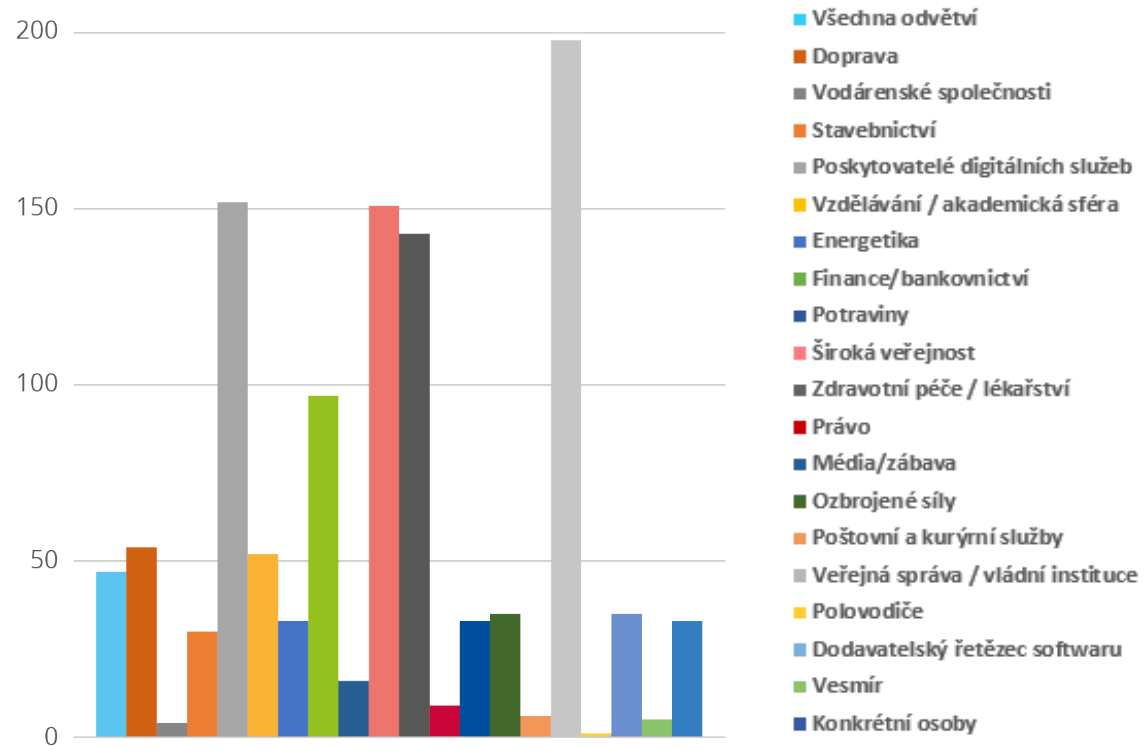
[9] V souladu s aktem EU o kybernetické bezpečnosti čl. 7 odst. 6 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN).

Obrázek 3: Časová osa pozorovaných incidentů ve vztahu k hlavním hrozbám ve zprávě o typech ohrožení z hlediska postiženého sektoru.



	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	Celkem
Vodárenské společnosti	1	1	1	1													2
Doprava	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Konkrétní osoby			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Vesmír	1		2	1							1						4
Dodavatelský řetězec softwaru			4			1	1		4	5	3	2	5	5	1	4	35
Polovodiče						1											1
Veřejná správa / vládní instituce	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Poštovní a kurýrní služby											1	2		3			6
Ozbrojené síly		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
Právo		2					1	1				1	3		1		7
Zdravotní péče / lékařství	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Široká veřejnost	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Potraviny												1	3	7	5		16
Finance/bankovnictví	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
Vzdělávání / akademická sféra	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Poskytovatelé digitálních služeb	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Stavebnictví		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Všechna odvětví			3		3		1		1	2	11	10	4	6	5	1	47

Obrázek 4: Cílené sektory podle počtu incidentů (duben 2020 – červenec 2021)



Během tohoto vykazovaného období cílil velký počet incidentů na veřejnou správu a vládní orgány a na poskytovatele digitálních služeb. Ve druhém uvedeném případě to lze očekávat vzhledem k horizontálnímu poskytování služeb pro tento sektor, a tím k dopadu na řadu jiných sektorů. Zaznamenali jsme rovněž značný počet incidentů zaměřených na koncové uživatele, nikoli nezbytně na konkrétní sektor. Významným cílem se stal také sektor zdravotnictví, přičemž tato aktivita vykazuje v posledních několika měsících vykazovaného období (květen – červenec 2021) nárůst. Zajímavé je, že sektor financí čelí konzistentnímu počtu incidentů po celý rok. Dodavatelský řetězec softwaru vykazuje během roku 2021 také zvýšený počet incidentů, což se rovněž zmiňuje ve zprávě o typech ohrožení v důsledku útoků na dodavatelské řetězce[10].

1.5. METODIKA

Zpráva o typech ohrožení (ETL) pro rok 2021 vychází z informací z otevřených zdrojů, převážně strategické povahy, a vlastních zdrojů operativních informací o hrozbách a zahrnuje více sektorů, technologií a kontextů. Zpráva se snaží být nevázaná na odvětví a prodejce a v textu v řadě poznámek pod čarou zmiňuje nebo cituje práce různých výzkumných pracovníků v oblasti bezpečnosti, bezpečnostní blogy a články ze zpravodajských médií. Zpráva o typech ohrožení pro rok 2021 časově pokrývá období od dubna 2020 do července 2021, které se v této zprávě označuje jako „vykazované období".

Při tvorbě zprávy o typech ohrožení pro rok 2021 byl použit následující přístup. Během příslušného časového období agentura ENISA, prostřednictvím povědomí o aktuální situaci, shromažďovala seznam závažných incidentů, jak se objevovaly v otevřených zdrojích. Tento seznam posloužil jako základ pro identifikaci seznamu hlavních hrozeb a jako zdrojový materiál pro několik trendů a statistik ve zprávě.

Následně byl agenturou ENISA a externími odborníky proveden důkladný výzkum dostupné literatury z otevřených zdrojů, jako jsou články ve zpravodajských médiích, odborné posudky, zpravodajská hlášení, analýzy incidentů a výzkumné zprávy z oblasti bezpečnosti. Prostřednictvím průběžné analýzy odvodila agentura ENISA trendy a body zájmu pro každou ze závažných hrozeb představených ve zprávě o typech ohrožení pro rok 2021. Klíčová

[10] Zpráva o typech ohrožení v důsledku útoků na dodavatelské řetězce, červenec 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

zjištění a názory v tomto posouzení vycházejí z četných veřejně dostupných zdrojů, které jsou uvedeny v odkazech použitých při tvorbě tohoto dokumentu.

V rámci zprávy se snažíme rozlišit mezi tím, co bylo hlášeno našimi zdroji, a naším hodnocením. (Činíme tak specificky pomocí fráze „podle našeho hodnocení“). A konečně, při provádění posouzení vyjadřujeme pravděpodobnost pomocí slov, která vyjadřují odhad pravděpodobnosti (např. pravděpodobně, velmi pravděpodobně, určitě)[11].

Ke zvýraznění taktik a metod útoků relevantních pro danou hrozbu byl v této zprávě použit rámec MITRE ATT&CK®[12] (viz příloha A). Pro každou taktiku ATT&CK® jsou uvedeny metody použité protivníkem. To může vést k seznamu zmírnění v rámci ATT&CK[13], která lze využít. MITRE ATT&CK® je znalostní databáze, společný jazyk pro taktiky a metody protivníků na základě pozorování z reálného světa. Znalostní databáze MITRE ATT&CK® slouží jako základ pro vypracování konkrétních modelů hrozeb a metodik v soukromém sektoru, ve veřejné správě a v komunitě produktů a služeb v oblasti kybernetické bezpečnosti.

Zprávu validovala *ad hoc* pracovní skupina agentury ENISA pro oblast kybernetických hrozeb[14], jež byla založena v dubnu 2021 a kterou tvoří odborníci z evropských a mezinárodních subjektů z veřejného a soukromého sektoru.

Pro budoucí vývoj forem hrozeb agentura ENISA průběžně formalizuje novou metodiku s cílem podporovat transparentnost a stanovit základy strukturovaných a sladěných procesů. V rámci tohoto úsilí bude metodika pro formy hrozeb společně s revidovanou taxonomií hrozeb v budoucnu zveřejněna.

1.6. STRUKTURA ZPRÁVY

Zpráva o typech ohrožení (ETL) za rok 2021 si zachovala strukturu předchozích zpráv o typech ohrožení tím, že využila podobnou strukturu pro zvýraznění hlavních kybernetických hrozeb v roce 2021. Čtenáři předchozích verzí si povšimnou, že kategorie hrozeb byly sjednoceny v souladu s posunem směrem k nové taxonomii kybernetických hrozeb, která se bude v budoucnu používat.

Zpráva je strukturována takto:

Kapitola 2 se zabývá trendy souvisejícími s aktéry hrozeb (tj. státem financovanými subjekty, subjekty počítačové kriminality, nájemnými hackery a hacktivisty).
Kapitola 3 pojednává o závažných zjištěních, incidentech a trendech týkajících se ransomwaru.
Kapitola 4 představuje závažná zjištění, incidenty a trendy týkající se malwaru.
Kapitola 5 popisuje závažná zjištění, incidenty a trendy týkající se nelegální těžby kryptoměn.
Kapitola 6 vyzdvihuje závažná zjištění, incidenty a trendy týkající se hrozeb v souvislosti s elektronickou poštou.
Kapitola 7 pojednává o závažných zjištěních, incidentech a trendech týkajících se ohrožení údajů.
Kapitola 8 představuje závažná zjištění, incidenty a trendy týkající se ohrožení dostupnosti a integrity.
Kapitola 9 zdůrazňuje význam hybridních hrozeb a popisuje závažná zjištění, incidenty a trendy týkající se dezinformací a zavádějících informací.
Kapitola 10 se zaměřuje na závažná zjištění, incidenty a trendy týkající se nezáměrných hrozeb.
Příloha A představuje metody obecně používané pro každou hrozbu, na základě rámce MITRE ATT&CK®.
Příloha B obsahuje významné incidenty podle hrozeb, jak byly pozorovány během vykazovaného období.

[11] CIA – Slova hodnotící pravděpodobnost https://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