EUROPEAN UNION AGENCY
FOR CYBERSECURITY

IZVJEŠĆE ENISA-E O PRIJETNJAMA 2021.

travanj 2020. – sredina srpnja 2021.

LISTOPAD 2021.

O ENISA-I

Agencija Europske unije za kibersigurnost, ENISA, agencija je Unije osnovana s ciljem postizanja visoke zajedničke razine kibersigurnosti u cijeloj Europi. Agencija Europske unije za kibersigurnost osnovana je 2004. na temelju Akta o kibersigurnosti EU-a i odonda pridonosi kiberpolitici EU-a, poboljšava pouzdanost proizvoda, usluga i postupaka IKT-a s pomoću programa kibersigurnosne certifikacije, surađuje s državama članicama i tijelima EU-a te pomaže Europi da se pripremi na kiberizazove koji je očekuju u budućnosti. Razmjenom znanja, izgradnjom kapaciteta i informiranjem Agencija zajedno sa svojim ključnim dionicima radi na jačanju povjerenja u povezano gospodarstvo kako bi se povećala otpornost infrastrukture Unije te kako bi se u konačnici zajamčila sigurnost europskog društva i građana. Više informacija o ENISA-i i njezinu radu možete pronaći ovdje: www.enisa.europa.eu.

KONTAKT

E-adresa za kontakt s autorima: etl@enisa.europa.eu.
E-adresa za medijske upite o ovom dokumentu: press@enisa.europa.eu.

UREDNICI

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – Agencija Europske unije za kibersigurnost

SURADNICI

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

ZAHVALE

Željeli bismo zahvaliti članovima i promatračima *ad hoc* Radne skupine ENISA-e za kiberprijetnje na njihovim korisnim povratnim informacijama i komentarima u vrednovanju ovog izvješća. Također bismo željeli zahvaliti Savjetodavnoj skupini ENISA-e i mreži nacionalnih časnika za vezu na njihovim korisnim povratnim informacijama.
Također bismo željeli zahvaliti i timovima ENISA-e za svijest o situaciji i obavješćivanje o incidentima na njihovu aktivnom doprinosu i podršci u konsolidaciji različitih informacija u izvješće o prijetnjama.

PRAVNA OBAVIJEST

OBAVIJEST O AUTORSKOM PRAVU

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

SADRŽAJ

SAŽETAK

Ovo je deveto izdanje godišnjeg izvješća ENISA-e o prijetnjama (engl. *ENISA Threat Landscape*, ETL) o stanju kiberprijetnji, u kojemu se utvrđuju glavne prijetnje, glavni trendovi zabilježeni u pogledu prijetnji, akteri prijetnji i tehnike napada, a u njemu se opisuju i relevantne mjere za ublažavanje posljedica. Tijekom procesa stalnog unaprjeđenja naše metodologije za razvoj prijetnji, ove godine naš je rad poduprla novoosnovana *ad hoc* Radna skupina ENISA-e za kiberprijetnje (engl. *Cybersecurity Threat Landscapes*, CTL).

Vremenski raspon izvješća ETL 2021. obuhvaća razdoblje od travnja 2020. do srpnja 2021. i u cijelom se izvješću naziva „razdoblje izvješćivanja". Tijekom razdoblja izvješćivanja, glavne utvrđene prijetnje obuhvaćale su:

- **programe za ucjenjivanje (ransomware)**
- **zlonamjerne softvere**
- ***cryptojacking* napade**
- **prijetnje povezane s e-poštom**
- **prijetnje usmjerene na podatke**
- **prijetnje usmjerene na dostupnost i cjelovitost**
- **dezinformacije – pogrešne informacije**
- **prijetnje koje nisu zlonamjerne**
- **napade u lancu opskrbe.**

U ovom izvješću raspravljamo o prvih osam kategorija kiberprijetnji. Deveta kategorija, prijetnje u lancu opskrbe, detaljno je analizirana, zbog njihove posebne istaknutosti, u namjenskom izvješću ENISA-e pod nazivom „Izvješće ENISA-e o prijetnjama u obliku napada u lancu opskrbe" (engl. *ENISA Threat landscape for Supply Chain Attacks*)[1].

U slučaju svake od utvrđenih prijetnji raspravlja se o tehnikama napada, važnim incidentima i trendovima, zajedno s predloženim mjerama za ublažavanje posljedica. Što se tiče trendova, tijekom razdoblja izvješćivanja ističemo sljedeće:

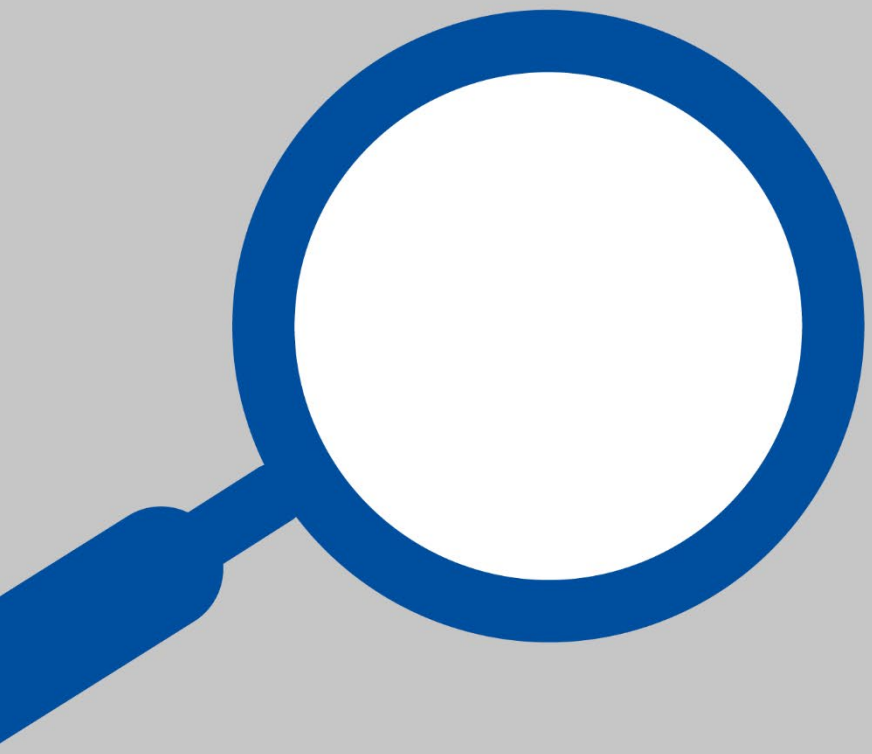
- **Programi za ucjenjivanje (ransomware)** ocijenjeni su kao **glavna prijetnja za 2020. – 2021.**
- **Vladine organizacije povećale su napore** na državnoj i međunarodnoj razini.
- **Kiberkriminalci su sve više motivirani monetizacijom** svojih aktivnosti, kao što su npr. programi ucjenjivanja **Kriptovaluta** je i dalje najčešća metoda isplate aktera prijetnje.
- **Pad broja zlonamjernih softvera** koji je zabilježen 2020. nastavlja se bilježiti i u 2021. Tijekom 2021. svjedočili smo tome da sve veći broj aktera prijetnje pribjegava relativno novim ili neuobičajenim programskim jezicima za prijenos svojeg koda.
- Količina **zaraza *cryptojacking* napadima** dosegnula je **rekordnu razinu** u prvom tromjesečju 2021. u usporedbi s prethodnih nekoliko godina. **Financijska dobit** povezana s *cryptojacking* napadima potaknula je aktere prijetnje da izvrše takve napade.
- **COVID-19 i dalje je prevladavajući mamac u kampanjama** za napade e-poštom.
- Došlo je do **porasta broja povreda podataka u vezi sa zdravstvenim sektorom**.
- Primjećuje se da su 2021. **tradicionalne kampanje DDoS (distribuirani napad uskraćivanjem usluga, engl. *Distributed Denial of Service*)** ciljanije, trajnije i povećano viševektorske. **Internet stvari** zajedno s **mobilnim mrežama** uzrokuje novi val distribuiranih napada uskraćivanjem usluga.
- Tijekom 2020. i 2021. zabilježen je **nagli porast incidenata koji nisu zlonamjerni**, jer je pandemija bolesti COVID-19 postala čimbenik za **ljudske pogreške** i **pogrešne konfiguracije sustava**, do te mjere da je većina povreda 2020. bila uzrokovana pogreškama.

[1] Izvješće ENISA-e o prijetnjama u obliku napada u lancu opskrbe, srpanj 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

Razumijevanje trendova povezanih s akterima prijetnje, njihovim motivacijama i ciljevima uvelike pomaže u planiranju obrana u području kibersigurnosti i strategija ublažavanja posljedica. To čini sastavni dio naše cjelokupne procjene prijetnji jer omogućuje davanje prioriteta zaštitnim kontrolama i osmišljavanje namjenske strategije na temelju mogućeg utjecaja i vjerojatnosti ostvarenja prijetnje. Imajući to na umu, za potrebe izvješća ETL 2021. razmatraju se sljedeće četiri kategorije aktera kiberprijetnje:

- **akteri pod pokroviteljstvom države**
- **akteri kiberkriminaliteta**
- **akteri koji pripadaju skupini „hakera za najam”**
- **hakeri-aktivisti.**

Kontinuiranom analizom ENISA je izvela trendove i zanimljivosti za svaku od glavnih prijetnji predstavljenih u izvješću ETL 2021. Ključni rezultati i prosudbe u ovoj procjeni temelje se na višestrukim javno dostupnim resursima koji su navedeni u referencama korištenim za izradu ovog dokumenta. Izvješće je uglavnom namijenjeno donositeljima strateških odluka i tvorcima politika, ali bit će zanimljivo i stručnoj zajednici u području kibersigurnosti.



1. PREGLED PRIJETNJI

U devetom izdanju izvješće ENISA-e o prijetnjama (ETL) daje se opći pregled kiberprijetnji. Izvješće ETL djelomično je strateško, a djelomično tehničko, te sadržava informacije relevantne za čitatelje s tehničkim znanjem i bez njega. Ove godine naš je rad poduprla novoosnovana *ad hoc* Radna skupina ENISA-e za kiberprijetnje (CTL)[2].

Tijekom 2020. i 2021. napadi u području kibersigurnosti nastavili su rasti, i to ne samo u pogledu vektora i brojeva, već i njihova utjecaja. Očekivano, na kiberprijetnje je utjecala i pandemija bolesti COVID-19. Jedna od trajnijih promjena koja je proizašla iz pandemije bolesti COVID-19 jest dugoročan prijelaz na hibridni model rada u uredu. Stoga kiberprijetnje povezane s pandemijom i iskorištavanjem „novog normalnog" postaju sve uobičajenije. Taj trend povećao je površinu napada i, shodno tome, svjedočili smo porastu broja kibernapada usmjerenih na organizacije i poduzeća zbog rada od kuće[3].

Općenito, kiberprijetnje su u porastu. Potaknuto stalno rastućom prisutnosti na internetu, prelaskom tradicionalnih infrastruktura na internetska rješenja i rješenja u oblaku, naprednim međusobnim povezivanjem i iskorištavanjem novih značajki novih tehnologija kao što je umjetna inteligencija[4][5], područje kibersigurnosti razvilo se s obzirom na sofisticiranost napada, njihovu složenost i njihov utjecaj. Prijetnja usmjerena na lance opskrbe, kao i na njihov značaj zbog potencijalno katastrofalnih kaskadnih učinaka, dosegla je najviše mjesto među glavnim prijetnjama, u toj mjeri da je ENISA osmislila posebnu prijetnju za tu kategoriju prijetnje.[6]

Vrijedi napomenuti da je u ovom izdanju ETL-a poseban naglasak stavljen na utjecaj kiberprijetnji u raznim sektorima, uključujući one navedene u Direktivi o mrežnoj i informacijskoj sigurnosti. Mogu se steći zanimljiva saznanja na temelju posebnosti svakog sektora s obzirom na prijetnje te potencijalne međuovisnosti i područja od značaja. U skladu s time, sektorske prijetnje zahtijevaju dodatnu pozornost.

Također, subjekti zaduženi za obranu u kiberzajednici i tvorci politika ove su godine poduzeli neke važnije mjere. Globalna zajednica počela je shvaćati važnost komunikacije i suradnje u ispitivanju i praćenju kiberkriminalaca, pri čemu su ransomware programi (najistaknutija prijetnja za razdoblje obuhvaćeno izvješćem ETL 2021.) postali glavna točka na dnevnom redu sastanaka o strategiji svjetskih čelnika.

Vjerni čitatelji prošlih izdanja izvješća ETL 2021. primijetit će razliku u mapiranju glavnih prijetnji. Ove se godine ENISA odmaknula od svega i konsolidirala kategorije prijetnji u cilju pomaka prema integraciji i boljem predstavljanju sličnih prijetnji. To je dio trajnih napora prema izmjenama taksonomije prijetnji, što će pomoći u metodološkom utvrđivanju trendova tijekom sljedećih nekoliko godina.

Izvješće ETL 2021. temelji se na raznim dostupnim izvorima informacija i saznanja o kiberprijetnjama. U njemu se utvrđuju glavne prijetnje, trendovi i rezultati te navode relevantne strategije na visokoj razini za ublažavanje posljedica. ENISA trenutačno radi na učvršćivanju metodologije za izvješćivanje o prijetnjama kako bi se promicala transparentnost i dosljednost u radu.

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM – Izvješće o troškovima povrede podataka 2020. – https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] Izvješće ENISA-e o prijetnjama u području umjetne inteligencije: 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] Izvješće ENISA-e o prijetnjama u obliku napada u lancu opskrbe, srpanj 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

1.1. GLAVNE PRIJETNJE

Tijekom 2020. i 2021. pojavio se i ostvario niz kiberprijetnji. Na temelju analize predstavljene u ovom izvješću, u izvješću ENISA-e o prijetnjama za 2021. utvrđuje se sljedećih osam glavnih skupina prijetnji na koje se stavlja naglasak (vidjeti Slika 1). Tih osam skupina prijetnji istaknuto je zbog njihova značaja tijekom razdoblja izvješćivanja, njihove popularnosti i utjecaja koji su imale.

- **Program za ucjenjivanje (ransomware)**
  Programi za ucjenjivanje vrsta su zlonamjernog napada u kojemu napadači šifriraju podatke organizacije i zahtijevaju plaćanje kako bi ponovno omogućili pristup tim podacima. Programi za ucjenjivanje predstavljali su glavnu prijetnju tijekom razdoblja izvješćivanja, uz nekoliko istaknutih incidenata o kojima se puno izvještavalo. O značaju i utjecaju prijetnje koja proizlazi iz programa za ucjenjivanje svjedoči i niz političkih inicijativa koje su u vezi s tim pokrenute u Europskoj uniji (EU) i diljem svijeta.

- **Zlonamjerni softver („malware")**
  Zlonamjerni softver je računalni program ili oprema namijenjena izvršavanju neovlaštenog procesa koji će negativno utjecati na povjerljivost, cjelovitost ili dostupnost sustava. Prijetnja zlonamjernog softvera već dugi niz godina zauzima visoko mjesto, iako je tijekom razdoblja obuhvaćenog izvješćem ETL 2021. zabilježen pad broja slučajeva. Upotreba novih tehnika dodavanja privitaka i neke velike pobjede zajednice za izvršavanje zakonodavstva utjecali su na rad relevantnih aktera prijetnje.

- ***Cryptojacking* napadi**
  Cryptojacking ili skriveno rudarenje kriptovaluta („cryptomining") vrsta je kiberkriminaliteta u kojemu se kriminalac potajno koristi računalnom snagom žrtve za generiranje kriptovalute. Potaknut naglim širenjem kriptovaluta i sve većim brojem osoba koje se njima koriste, zabilježen je porast takvih incidenata u području kibersigurnosti.

- **Prijetnje povezane s e-poštom**
  Napadi povezani s e-poštom odnose se na skup prijetnji kojima se iskorištavaju slabosti ljudske psihe i svakodnevnih navika, a ne tehničke ranjivosti informacijskih sustava. Zanimljivo je da je unatoč brojnim kampanjama podizanja razine svijesti i edukacije protiv tih vrsta napada, ta prijetnja i dalje vrlo prisutna. Konkretno, u porastu su ugrožavanje poslovne e-pošte i napredne, sofisticirane tehnike izvlačenja novčanih dobitaka.

- **Prijetnje usmjerene na podatke**
  Ova kategorija obuhvaća povrede/curenje podataka. Povreda podataka ili curenje podataka odnosi se na otkrivanje osjetljivih, povjerljivih ili zaštićenih podataka u nepouzdanom okruženju. Do povrede podataka može doći kao posljedica kibernapada, napada iznutra, nenamjernog gubitka ili otkrivanja podataka. Razina prijetnje i dalje je visoka jer je pristup podacima glavni cilj napadača iz nekoliko razloga, npr. iznuda, otkupnina, kleveta, dezinformacije itd.

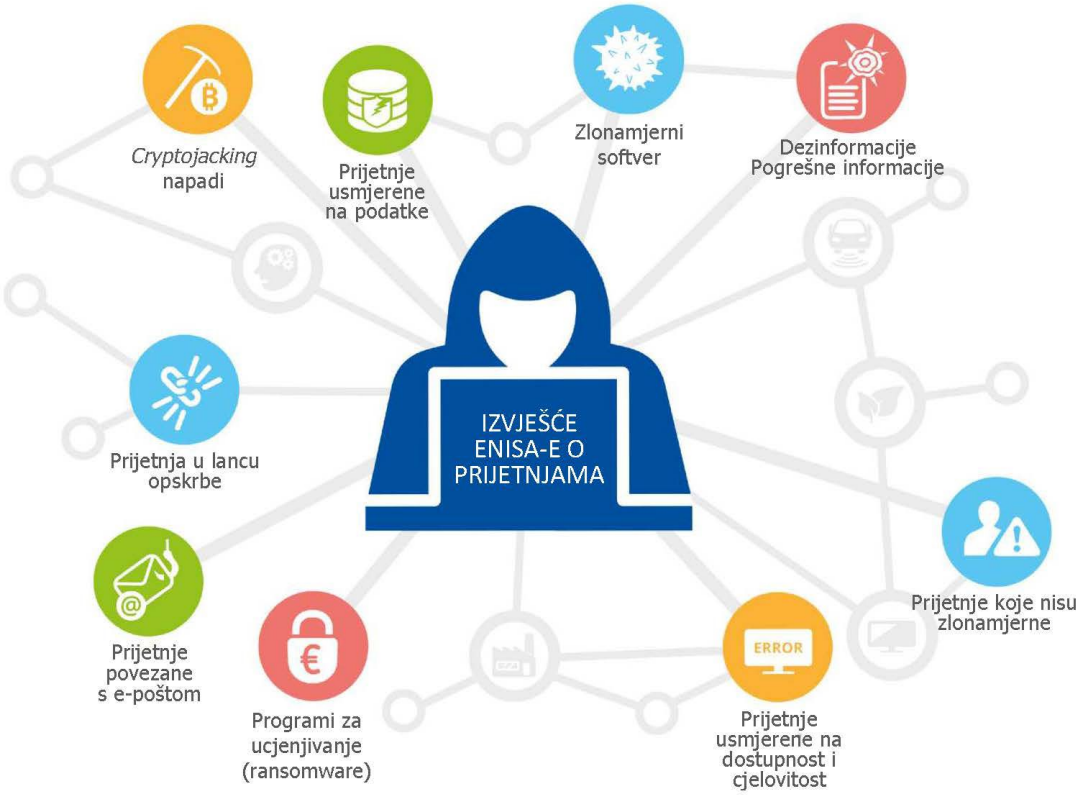
- **Prijetnje usmjerene na dostupnost i cjelovitost**
  Mnoge prijetnje i napadi usmjereni su na dostupnost i cjelovitost, a među njima se ističu uskraćivanje usluge (DoS) i mrežni napadi. Distribuirani napadi uskraćivanjem usluga usko su povezani s mrežnim napadima, a čine jednu od najopasnijih prijetnji informacijskim sustavima, ciljajući njihovu dostupnost iscrpljivanjem resursa, što uzrokuje pad performansi, gubitak podataka i prekide pružanja usluga. Ta prijetnja kontinuirano zauzima visoko mjesto među prijetnjama koje procjenjuje ENISA-e jer se očituje u stvarnim incidentima te ima potencijal uzrokovati velike probleme.

- **Dezinformacije – pogrešne informacije**
  Kampanje dezinformiranja i širenja pogrešnih informacija su u porastu, potaknute povećanom upotrebom platforma društvenih medija i mrežnih medija, ali i kao rezultat povećane prisutnosti ljudi na internetu zbog pandemije bolesti COVID-19. Ova skupina prijetnji prvi je put uključenja u izvješće ETL, no njezina je važnost u kibersvijetu velika. Kampanje dezinformiranja i širenja pogrešnih informacija često se koriste u hibridnim napadima u cilju smanjenja ukupne percepcije povjerenja, glavnog pokretača kibersigurnosti.

- **Prijetnje koje nisu zlonamjerne**
  Prijetnje se obično smatraju dobrovoljnim i zlonamjernim aktivnostima protivnika koji imaju razloga napasti određenu metu. Ova kategorija sadržava prijetnje u kojima zle namjere nisu očite. One se uglavnom temelje na

ljudskim pogreškama i pogrešnim konfiguracijama sustava, ali mogu se odnositi i na katastrofe koje imaju fizičke posljedice po IT infrastrukturu. Također, zbog svoje prirode te su prijetnje neprestano prisutne u godišnjem izvješću o prijetnjama i ozbiljan su razlog za zabrinutost u pogledu procjena rizika.

Slika 1.: Izvješće ENISA-e o prijetnjama 2021. – glavne prijetnje



Potrebno je napomenuti da spomenute prijetnje obuhvaćaju kategorije i skup prijetnji objedinjene u osam prethodno navedenih područja. Svaka skupina prijetnji dodatno se analizira u odgovarajućem poglavlju ovog izvješća, u kojemu se razrađuju njezine posebnosti i pružaju konkretnije informacije, rezultati, trendovi, tehnike napada i vektori ublažavanja posljedica.

1.2. KLJUČNI TRENDOVI

U popisu u nastavku sažimaju se glavni trendovi zabilježeni u području kiberprijetnji tijekom razdoblja izvješćivanja. U različitim poglavljima izvješća ENISA-e o prijetnjama za 2021. ti se trendovi detaljno opisuju.

- Došlo je do povećanja slučajeva **visoko sofisticiranog ugrožavanja lanaca opskrbe koje ima snažan utjecaj**, kako je istaknuto u posebnom izvješću ENISA-e o prijetnjama u lancu opskrbe. **Pružatelji usluga upravljanja** važne su mete kiberkriminalaca.
- **COVID-19 je potaknuo kibernetičku špijunažu** i stvorio **mogućnosti za kiberkriminalce**.
- **Vladine organizacije povećale su napore** na državnoj i međunarodnoj razini. Zabilježeni su povećani napori vlada da poduzmu pravne mjere protiv aktera prijetnje pod pokroviteljstvom države i poremete njihovo djelovanje.
- **Kiberkriminalci su sve više motivirani monetizacijom** svojih aktivnosti, kao što su npr. programi ucjenjivanja **Kriptovaluta** je i dalje najčešća metoda isplate aktera prijetnje.
- Napadi u području kiberkriminaliteta **sve su više usmjereni i utječu na kritičnu infrastrukturu**.
- **Ugrožavanje putem *phishing* e-poruka (za krađu identiteta) i *brute forcing* napadi (napadi uzastopnim pokušavanjem) na servisima udaljene radne površine (RDP)** i dalje su dva najčešća **vektora zaraze programima ucjenjivanja**.

- Usredotočenost na **poslovne modele vrste RaaS (engl. *ransomware as a service*)** povećala se tijekom 2021., što otežava točno pripisivanje odgovornosti pojedinačnim akterima prijetnje.
- Učestalost planova **programa za ucjenjivanje za trostruku iznudu** snažno se povećala tijekom 2021.
- **Pad broja zlonamjernih softvera** koji je zabilježen 2020. nastavlja se i u 2021. Tijekom 2021. svjedočili smo tome da sve veći broj aktera prijetnje pribjegava relativno novim ili neuobičajenim programskim jezicima za prijenos svojeg koda.
- **Zlonamjerni softveri kojima se napadaju spremišna okruženja** postali su raširениji, uz nove verzije poput zlonamjernog softvera bez datoteka koji se izvršava iz memorije.
- Razvojni programeri zlonamjernih softvera neprestano pronalaze načine da **otežaju obrnuti inženjering i dinamičku analizu**.
- Količina **zaraza *cryptojacking* napadima** dosegnula je **rekordnu razinu** u prvom tromjesečju 2021. u usporedbi s posljednjih nekoliko godina. **Financijska dobit** povezana s *cryptojacking* napadima poticaj je akterima prijetnje da izvrše takve napade.
- **Količina rudarenja kriptovaluta 2021. i *cryptojacking* aktivnosti na rekordno su visokoj razini**.
- Vidimo da se događa **prijelaz na *cryptojacking* napade na temelju datoteka, a ne preglednika.**
- **COVID-19 i dalje je prevladavajući mamac u kampanjama** za napade e-poštom.
- **Ugrožavanje poslovne e-pošte (engl. *business e-mail compromise*, BEC)** je **u porastu**, a postalo je **sofisticiranije** i **usmjerenije**.
- Poslovni model **PhaaS (engl. *phishing-as-a-service*)** postaje sve raširениji.
- Akteri prijetnje svoju su pozornost usmjerili na **informacije o cjepivima** u kontekstu prijetnji prema podacima i informacijama.
- Došlo je do **porasta broja povreda podataka u vezi sa zdravstvenim sektorom**.
- Tradicionalni napadi DDoS postaju usmjereni na **mobilne mreže i internet stvari**.
- **Uskraćivanje usluge do plaćanja otkupnine (engl. *ransom denial of service*, RDoS)** novo je područje napada uskraćivanjem usluge.
- **Dijeljenje resursa u virtualiziranim okruženjima** pojačava distribuirane napade uskraćivanjem usluga.
- **Kampanje DDoS** 2021. postale su usmjerenije i mnogo trajnije te povećano viševektorske.
- **Dezinformacije omogućene umjetnom inteligencijom** omogućuju napadačima izvršavanje njihovih napada.
- ***Phishing* je u središtu napada dezinformiranja** i njime se snažno iskorištavaju uvjerenja ljudi.
- **Pogrešne informacije i dezinformacije** u samom su središtu aktivnosti kiberkriminaliteta i njihov broj raste neviđenom brzinom.
- Učestalost **poslovnog modela DaaS (engl. *Disinformation-as-a-service*)** znatno je porasla, potaknuta sve većim utjecajem pandemije bolesti COVID-19 i potrebom za više informacija.
- 2020. i 2021. zabilježen je **porast incidenata koji nisu zlonamjerni**, jer je pandemija bolesti COVID-19 postala čimbenik za **ljudske pogreške** i **pogrešne konfiguracije sustava**, do te mjere da je većina povreda 2020. bila uzrokovana pogreškama.
- Došlo je do **porasta incidenata sigurnosti u oblaku koji nisu zlonamjerni**.

1.3. BLIZINA EU-A U ODNOSU NA GLAVNE PRIJETNJE

Važni aspekt koji je potrebno razmotriti u kontekstu izvješća ENISA-e o prijetnjama odnosi se na blizinu kiberprijetnje Europskoj uniji (EU). To je posebice važno kako bi se analitičarima pomoglo u procjeni važnosti kiberprijetnji, njihovu povezivanju s mogućim akterima i vektorima prijetnje, pa čak i za usmjeravanje odabira odgovarajućih ciljnih vektora ublažavanja posljedica. U skladu s predloženom klasifikacijom za zajedničku sigurnosnu i obrambenu politiku EU-a[7], klasificiramo kiberprijetnje u četiri kategorije, kako je prikazano u Tablica 1.

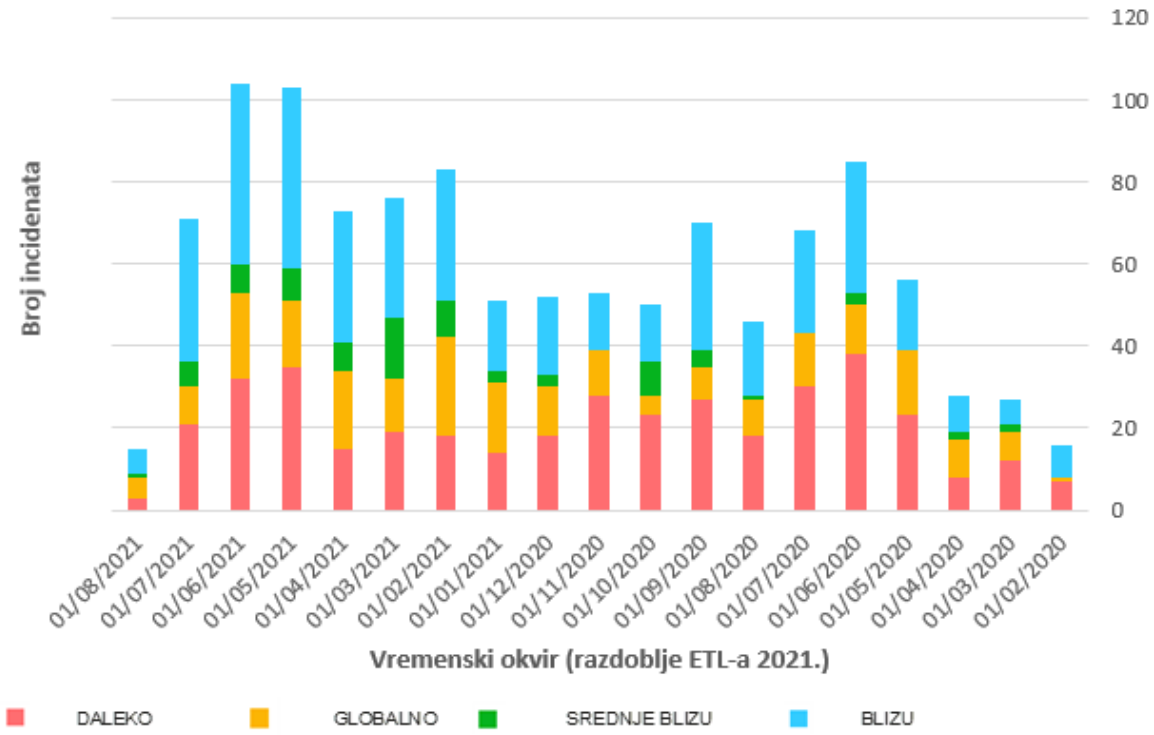
[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf

Tablica 1.: Klasifikacija blizine kiberprijetnji

Blizina	Razlozi za zabrinutost
BLIZU	Pogođene mreže i sustavi kojima se upravlja i koji su osigurani unutar granica EU-a. Pogođeno stanovništvo unutar granica EU-a.
SREDNJE BLIZU	Mreže i sustavi koji se smatraju ključnima za operativne ciljeve u okviru digitalnog jedinstvenog tržišta EU-a i sektora iz Direktive o mrežnoj i informacijskoj sigurnosti, no njihova kontrola i osiguravanje ovise o javnim ili privatnim tijelima država članica koja ne pripadaju institucijama EU-a. Pogođeno stanovništvo u zemljopisnim područjima koja su blizu granica EU-a.
DALEKO	Mreže i sustavi koji će, ako se na njih utječe, imati odlučujući utjecaj na operativne ciljeve o okviru digitalnog jedinstvenog tržišta EU-a i sektora iz Direktive o mrežnoj i informacijskoj sigurnosti. Kontrola i osiguravanje tih mreža i sustava nije pod kontrolom javnih ili privatnih tijela institucija EU-a ili država članica. Pogođeno stanovništvo u zemljopisnim područjima koja su daleko od EU-a.
GLOBALNO	Sva prethodno navedena područja.

Slika 2 pokazuje vremenski okvir incidenata povezanih s kategorijama glavnih prijetnji navedenima u izvješću ETL 2021. Treba napomenuti da se informacije na grafikonu temelje na obavještavanju iz otvorenih izvora (engl. *open source intelligence*, OSINT) i rezultat su rada ENISA-e u području svijesti o situaciji[8].

Slika 2.: Vremenski okvir zabilježenih incidenata povezanih s glavnim prijetnjama iz ETL-a (svijest o situaciji temeljena na OSINT-u) s obzirom na njihovu blizinu.



[8] U skladu s člankom 7. stavkom 6. Akta o kibersigurnosti EU-a https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

Kako je vidljivo na prethodnoj slici, 2021. zabilježen je veći broj incidenata u usporedbi s 2020. Konkretno, u kategoriji „BLIZU" primjećuje se stalan porast broja zabilježenih incidenata povezanih s glavnim prijetnjama, što upućuje na njihovu važnost u kontekstu EU-a. Nije iznenađujuće da su mjesečni trendovi (koji nisu prikazani na slici radi sažetosti) prilično slični među različitim klasifikacijama jer kibersigurnost ne poznaje granice i u većini se slučajeva prijetnje ostvaruju na svim razinama blizine. Važno je napomenuti da je, tijekom posljednjih nekoliko mjeseci obuhvaćenih izvješćem ETL 2021. u EU-u zabilježen veći broj slučajeva koji pripadaju kategoriji „BLIZU", što je trend koji će ENISA nastaviti pratiti kako bi vidjela na koji se način razvija i kako je povezan s aktivnostima aktera prijetnje i aktualnim vektorima prijetnje.

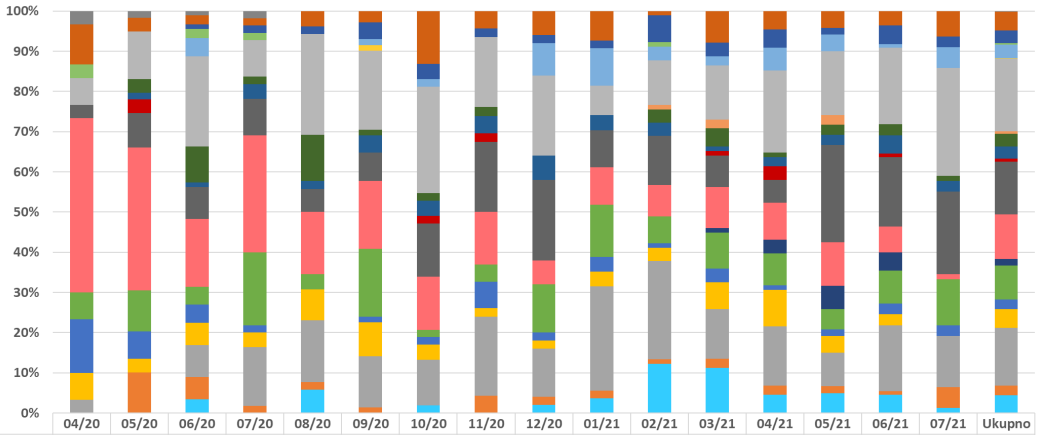
1.4. GLAVNE PRIJETNJE PO SEKTORU

Kiberprijetnje uglavnom nisu ograničene na jedan određeni sektor i u većini slučajeva pogađaju više njih. To je doista točno jer se u mnogo slučajeva prijetnje očituju iskorištavanjem ranjivosti u temeljnim IKT sustavima koji se koriste u raznim sektorima. Međutim, ciljani napadi, te napadi u kojima se iskorištavaju razlike u zrelosti kibersigurnosti diljem sektora i popularnost/važnost određenih sektora, predstavljaju čimbenike koje je potrebno uzeti u obzir. Ti čimbenici pridonose tome da se prijetnje očituju kao incidenti u određenim sektorima, stoga je važno dobro sagledati sektorske aspekte zabilježenih incidenata i prijetnji. Osim toga, trendovi zabilježeni u svakom sektoru i međusektorske ovisnosti zapažanja su koja se mogu utvrditi na temelju takve analize.

Na slikama 3. i 4. istaknuti su pogođeni sektori u vezi s incidentima zabilježenim na temelju obavještavanja iz otvorenih izvora (OSINT), a rezultat su rada ENISA-e u području svijesti o situaciji[9]. Odnose se na incidente povezane s glavnim prijetnjama iz izvješća ETL 2021. Ovo je prvi pokušaj ENISA-e da mapira utjecaj tih prijetnji na određene sektore. U nadolazećim godinama i budućim verzijama izvješća o prijetnjama nastojat će se uskladiti sektori s onima navedenim u Direktivi o mrežnoj i informacijskoj sigurnosti (NISD) i prijedlogu za njezinu reviziju (NISD 2.0).

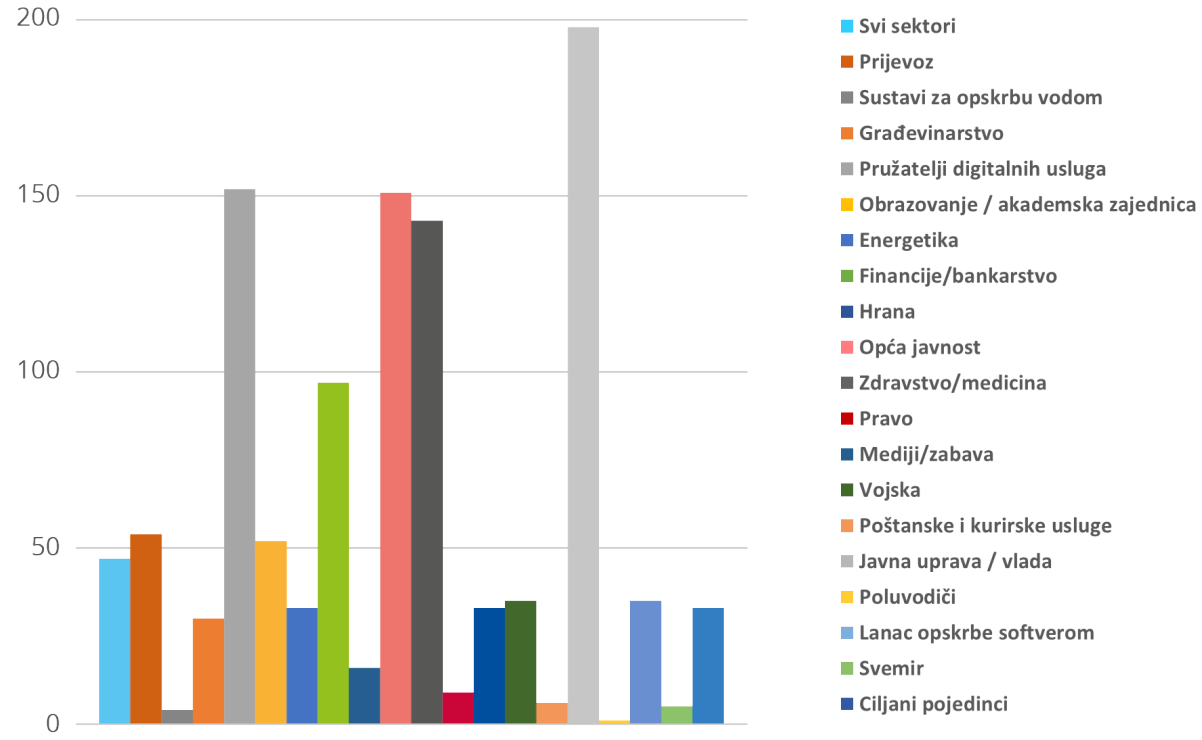
[9] U skladu s člankom 7. stavkom 6. Akta o kibersigurnosti EU-a (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

Slika 3.: Vremenski okvir zabilježenih incidenata povezanih s glavnim prijetnjama iz ETL-a s obzirom na pogođeni sektor.



	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	Ukupno
Sustavi za opskrbu vodom	1	1	1	1													2
Prijevoz	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Ciljani pojedinci			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Svemir	1		2	1							1						4
Lanac opskrbe softverom			4			1	1		4	5	3	2	5	5	1	4	35
Poluvodiči						1											1
Javna uprava / vlada	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Poštanske i kurirske usluge											1	2		3			6
Vojska		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Mediji/zabava		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Pravo		2					1	1				1	3		1		7
Zdravstvo/medicina	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Opća javnost	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Hrana												1	3	7	5		16
Financije/bankarstvo	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
Obrazovanje / akademska zajednica	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Pružatelji digitalnih usluga	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Građevinarstvo		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Svi sektori			3		3		1		1	2	11	10	4	6	5	1	47

Slika 4.: Ciljani sektori prema broju incidenata (travanj 2020. – srpanj 2021.)



Tijekom ovog razdoblja izvješćivanja velik broj incidenata bio je usmjeren na sektor javne uprave i vlade te pružatelje digitalnih usluga. Potonje je očekivano s obzirom na vodoravno pružanje usluga za taj sektor, a time i njegov utjecaj na mnoge druge sektore. Također smo primijetili da je znatan broj incidenata usmjeren na krajnje korisnike, a ne nužno na određeni sektor. Zdravstveni sektor također je bio znatno pogođen, a tijekom posljednjih nekoliko mjeseci razdoblja izvješćivanja (svibanj – srpanj 2021.) primijećeni su znakovi porasta takvih aktivnosti. Zanimljivo je da se financijski sektor suočava s konstantnim brojem incidenata tijekom cijele godine. U lancu opskrbe softverom također je došlo do porasta broja incidenata tijekom 2021., što je isto tako zabilježeno u izvješću ENISA-e o prijetnjama u lancu opskrbe[10].

1.5. METODOLOGIJA

Izvješće ENISA-e o prijetnjama (ETL) 2021. temelji se na informacijama dostupnim iz otvorenih izvora, koje su uglavnom strateške prirode i temeljene na vlastitim kapacitetima ENISA-e u pogledu saznanja o kiberprijetnjama, a obuhvaća više sektora, tehnologija i konteksta. U izvješću se pokušava postići objektivnost s obzirom na industrije i dobavljače, a u njemu se u više fusnota navode ili citiraju radovi različitih istraživača u području sigurnosti. Vremenski raspon izvješća ETL 2021. obuhvaća razdoblje od travnja 2020. do srpnja 2021. i u cijelom se izvješću naziva „razdoblje izvješćivanja".

U izradi izvješća ETL 2021. primijenjen je sljedeći pristup. Tijekom relevantnog vremenskog razdoblja ENISA je, s pomoću svijesti o situaciji, prikupila popis velikih incidenata kako su se pojavljivali u otvorenim izvorima. Taj je popis služio kao osnova za utvrđivanje popisa glavnih prijetnji, ali i kao izvorni materijal za nekoliko trendova i statističkih podataka u izvješću.

Potom su ENISA i vanjski stručnjaci proveli dubinsko uredsko istraživanje dostupne literature iz otvorenih izvora, kao što su novinski članci, mišljenja stručnjaka, obavještajna izvješća, analiza incidenta i izvješća iz područja sigurnosti. Kontinuiranom analizom ENISA je izvela trendove i zanimljivosti za svaku od glavnih prijetnji predstavljenih u

[10] Izvješće ENISA-e o prijetnjama u obliku napada u lancu opskrbe, srpanj 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

izvješću ETL 2021. Ključni rezultati i prosudbe u ovoj procjeni temelje se na višestrukim javno dostupnim resursima koji su navedeni u referencama korištenim za izradu ovog dokumenta.

U samom izvješću nastojimo razlikovati ono što je zabilježeno u našim izvorima i ono što je naša procjena. (To činimo tako da izričito upotrebljavamo izraz „prema našoj procjeni"). Konačno, pri provedbi procjene vjerojatnost izražavamo riječima kojima se iskazuje procjena vjerojatnosti (npr. vjerojatno, vrlo vjerojatno, sigurno)[11].

U ovom izvješću upotrijebljen je okvir MITRE ATT&CK®[12] kako bi se istaknule taktike i tehnike napada relevantne za određenu prijetnju (vidjeti Prilog A). Za svaku taktiku ATT&CK® predstavljene su tehnike kojima se koristio protivnik. Na taj način može nastati popis tehnika ATT&CK za ublažavanje, koje se mogu primijeniti.[13] MITRE ATT&CK® je baza znanja, zajednički jezik za protivničke taktike i tehnike temeljene na opažanjima iz stvarnog svijeta. Baza znanja MITRE ATT&CK® koristi se kao osnova za razvoj konkretnih modela i metodologija prijetnji u privatnom sektoru, vladi i u zajednici proizvoda i usluga za kibersigurnost.

Izvješće je potvrdila *ad hoc* Radna skupina ENISA-e za kiberprijetnje[14] koja je uspostavljena u travnju 2021., a riječ je o skupini stručnjaka iz europskih i međunarodnih subjekata javnog i privatnog sektora.

Što se tiče buduće izrade izvješća o prijetnjama, ENISA je u postupku formaliziranja nove metodologije kako bi se promicala transparentnost i postavili temelji za strukturirane i dobro usklađene procese. U tom će pothvatu, zajedno s revidiranom taksonomijom prijetnji, metodologija za prijetnje u budućnosti biti stavljena na raspolaganje javnosti.

1.6. STRUKTURA IZVJEŠĆA

Izvješće ENISA-e o prijetnjama (ETL) 2021. zadržalo je strukturu prethodnih izvješća ETL koristeći se sličnom strukturom za isticanje glavnih kiberprijetnji u 2021. Osobe koje su čitale prošle verzije primijetit će da su kategorije prijetnji konsolidirane u skladu s pomakom prema novoj taksonomiji kiberprijetnji koja će se koristiti u budućnosti.

Ovo izvješće čine sljedeći dijelovi:

U **2. poglavlju** istražuju se trendovi u vezi s akterima prijetnje (tj. akteri pod pokroviteljstvom države, akteri kiberkriminaliteta, akteri koji pripadaju skupini „hakera za najam" i hakeri-aktivisti).
U **3. poglavlju** raspravlja se o važnim saznanjima, incidentima i trendovima u vezi s programima za ucjenjivanje.
U **4. poglavlju** predstavljena su važna saznanja, kao i važni incidenti i trendovi u vezi sa zlonamjernim softverima.
U **5. poglavlju** opisana su važna saznanja, kao i važni incidenti i trendovi u vezi s *cryptojacking* napadima.
U **6. poglavlju** istaknuta su važna saznanja, kao i važni incidenti i trendovi u vezi s prijetnjama povezanim s e-poštom.
U **7. poglavlju** raspravlja se o važnim saznanjima, incidentima i trendovima u vezi s prijetnjama prema podacima.
U **8. poglavlju** predstavljena su važna saznanja, kao i važni incidenti i trendovi u vezi s prijetnjama usmjerenim na dostupnost i cjelovitost.
U **9. poglavlju** istaknuta je važnost hibridnih prijetnji i u njemu se opisuju važna saznanja, kao i važni incidenti i trendovi u vezi s dezinformacijama i pogrešnim informacijama.
U **10. poglavlju** stavljen je naglasak na važna saznanja, kao i važne incidente i trendove u vezi s prijetnjama koje nisu zlonamjerne.
U **Prilogu A** predstavljene su tehnike koje se često koriste za svaku prijetnju, u skladu s okvirom MITRE ATT&CK®.
U **Prilogu B** navode se važni incidenti po prijetnji, kako su zabilježeni tijekom razdoblja izvješćivanja.

[11] CIA – riječi za procjenu vjerojatnosti 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