EUROPEAN UNION AGENCY
FOR CYBERSECURITY

POROČILO O NARAVI GROŽENJ ZA LETO 2021

Od aprila 2020 do sredine julija 2021

OKTOBER 2021

O AGENCIJI ENISA

Agencija Evropske unije za kibernetsko varnost, ENISA, je agencija Unije, katere cilj je dosegati visoko skupno raven kibernetske varnosti po vsej Evropi. Ustanovljena je bila leta 2004, njene pristojnosti pa so bile okrepljene z uredbo EU o kibernetski varnosti. Prispeva h kibernetski politiki EU, povečuje zaupanje v produkte, storitve in procese IKT s certifikacijskimi shemami za kibernetsko varnost, sodeluje z državami članicami in organi EU ter pomaga Evropi, da bo pripravljena na kibernetske izzive prihodnosti. Z izmenjavo znanja, krepitvijo zmogljivosti in ozaveščanjem sodeluje s svojimi ključnimi deležniki, da bi okrepila zaupanje v povezano gospodarstvo, povečala odpornost infrastrukture Unije ter navsezadnje zagotovila digitalno varnost evropske družbe in državljanov. Več informacij o agenciji ENISA in njenem delu je na voljo tu: www.enisa.europa.eu..

STIK

Če želite stopiti v stik z avtorji, pišite na etl@enisa.europa.eu.
Če imate novinarsko vprašanje v zvezi s tem dokumentom, pišite na press@enisa.europa.eu.

UREDNIKI

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – Agencija Evropske unije za kibernetsko varnost

SODELUJOČI

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

ZAHVALA

Zahvaljujemo se članom in opazovalcem ad hoc delovne skupine agencije ENISA za kibernetske grožnje za njihove dragocene povratne informacije in pripombe pri potrjevanju tega poročila. Zahvaljujemo se tudi svetovalni skupini agencije ENISA in mreži nacionalnih uradnikov za zvezo za njihove dragocene povratne informacije. Prav tako se zahvaljujemo skupinama agencije ENISA za situacijsko zavedanje in priglasitev incidentov za njune aktivne prispevke ter podporo pri sestavljanju okolja groženj na podlagi različnih informacij.

PRAVNO OBVESTILO

OBVESTILO O AVTORSKIH PRAVICAH

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

KAZALO

PREGLED OKOLJA GROŽENJ 6

1.1. GLAVNE GROŽNJE 7

1.2. KLJUČNI TRENDI 8

1.3. EU IN BLIŽINA GLAVNIH GROŽENJ 9

1.4. GLAVNE GROŽNJE PO SEKTORJIH 11

1.5. METODOLOGIJA 13

1.6. ZGRADBA POROČILA 14

POVZETEK

To je deveta izdaja poročila o naravi groženj, tj. letnega poročila o stanju kibernetskih groženj, ki prinaša informacije o glavnih grožnjah, glavnih trendih, opaženih v zvezi z grožnjami, akterjih groženj in tehnikah napadanja ter opisuje ustrezne blažilne ukrepe. V okviru nenehnih izboljšav naše metodologije za opredelitev okolij groženj je letošnje delo podprla novooblikovana ad hoc delovna skupina agencije ENISA za kibernetske grožnje.

Poročilo o naravi groženj za leto 2021 se nanaša na obdobje od aprila 2020 do julija 2021, ki se v poročilu omenja kot „poročevalsko obdobje“. V poročevalskem obdobju so bile ugotovljene naslednje glavne grožnje:

- **izsiljevalsko programje,**
- **zlonamerna programska oprema,**
- **kraja procesorske zmogljivosti,**
- **grožnje v zvezi z e-pošto,**
- **grožnje zoper podatke,**
- **grožnje zoper razpoložljivost in celovitost,**
- **dezinformiranje – napačno informiranje,**
- **nezlonamerne grožnje,**
- **napadi na dobavne verige.**

V tem poročilu je obravnavanih prvih 8 kategorij kibernetskih groženj. Grožnje za dobavne verige iz 9. kategorije so bile zaradi posebnega pomena podrobno proučene v namenskem poročilu agencije ENISA z naslovom ENISA Threat Landscape for Supply Chain Attacks (Poročilo o naravi groženj za napade na dobavne verige) ([1]).

Pri vsaki ugotovljeni grožnji in tehniki napadanja so obravnavani pomembni incidenti in trendi skupaj s predlaganimi blažilnimi ukrepi. Kar zadeva trende v poročevalskem obdobju, poudarjamo naslednje:

- **izsiljevalsko programje** je bilo ocenjeno kot **glavna grožnja v obdobju 2020–2021**;
- **vladne organizacije so pospešile izboljšave** na nacionalni in mednarodni ravni;
- **storilce kaznivih dejanj v kibernetskem prostoru vse bolj spodbuja monetizacija** njihovih dejavnosti, npr. z izsiljevalskim programjem; **kriptovaluta** je še vedno najbolj pogost način izplačila pri akterjih groženj;
- **upad zlonamerne programske opreme**, ki je bil opažen leta 2020, se leta 2021 nadaljuje. Leta 2021 smo opazili večje zatekanje akterjev groženj k razmeroma novim ali redkim programskim jezikom za prenos svojih kod;
- število **okužb za krajo procesorske zmogljivosti** je v primerjavi s preteklimi leti v prvem četrtletju leta 2021 doseglo **rekordno vrednost**. K izvedbi teh napadov je akterje groženj spodbudila **finančna korist**, povezana s krajo procesorske zmogljivosti;
- **covid-19 je še vedno prevladujoča vaba v kampanjah** za napade po e-pošti;
- število **kršitev varnosti podatkov, povezanih z zdravstvenim sektorjem, se je povečalo**;
- **tradicionalni porazdeljeni napadi za zavrnitev storitve** so leta 2021 bolj ciljno usmerjeni, vztrajnejši in vse bolj večvektorski. **Internet stvari** v povezavi z **mobilnimi omrežji** povzroča nov val porazdeljenih napadov za zavrnitev storitve;
- v letih 2020 in 2021 smo opazili **porast nezlonamernih incidentov**, saj je pandemija covida-19 pomnožila število **človeških napak** in **napačnih sistemskih konfiguracij** do točke, da so večino kršitev leta 2020 povzročile napake.

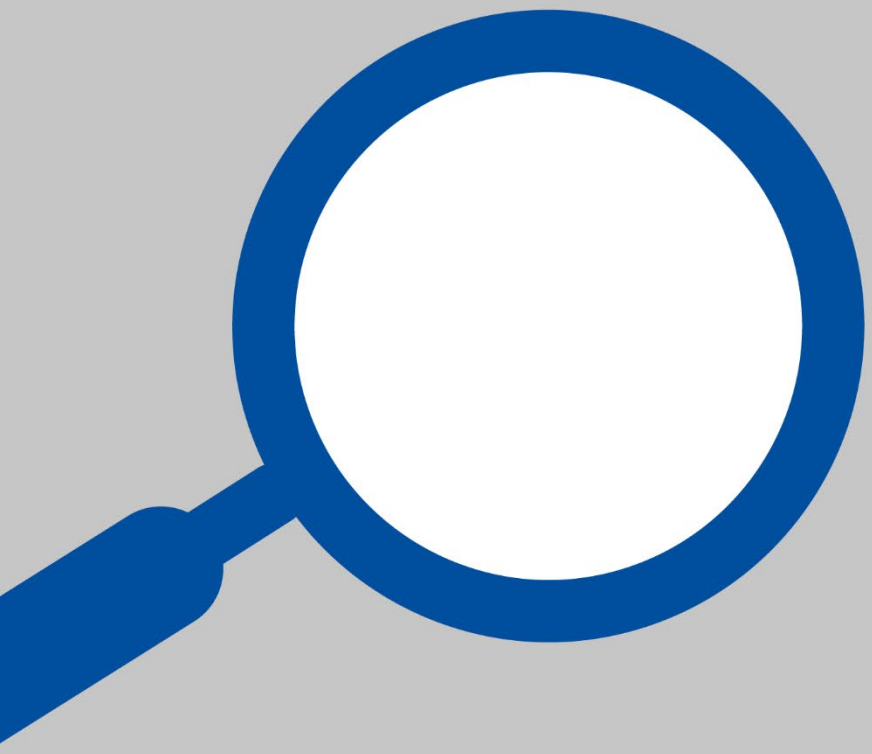
Razumevanje trendov glede akterjev groženj, njihovih nagibov in tarč zelo pomaga pri načrtovanju obrambe kibernetske varnosti in blažilnih strategij. To je sestavni del naše celovite ocene groženj, ker omogoča prednostno

[1] ENISA Threat Landscape for Supply Chain Attacks, julij 2021: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks..

razvrščanje varnostnih kontrol in oblikovanje namenske strategije na podlagi potencialnega vpliva in verjetnosti uresničitve grožnje. Ob upoštevanju tega so za potrebe Poročila o naravi groženj za leto 2021 obravnavane naslednje štiri kategorije akterjev kibernetskih groženj:

- **akterji, ki jih podpira država,**
- **akterji kibernetske kriminalitete,**
- **akterji, ki so hekerji najemniki,**
- **hektivisti.**

Na podlagi stalnega proučevanja je agencija ENISA izpeljala trende in pomembne točke za posamezne pomembne grožnje, predstavljene v Poročilu o naravi groženj za leto 2021. Ključne ugotovitve in presoje v tej oceni temeljijo na več javno dostopnih virih, navedenih v referencah, uporabljenih za izdelavo tega dokumenta. Poročilo je večinoma namenjeno strateškim odločevalcem in oblikovalcem politik, zanimivo pa bo tudi za tehnično skupnost, ki se ukvarja s kibernetsko varnostjo.



1. PREGLED OKOLJA GROŽENJ

Deveta izdaja poročila o naravi groženj prinaša splošen pregled kibernetskih groženj. Poročilo o naravi groženj vsebuje informacije za tehnične in netehnične bralce ter je tako deloma strateško, deloma pa tehnično. Letošnje delo je podprla novooblikovana ad hoc delovna skupina agencije ENISA za kibernetske grožnje ([2]).

Napadi na kibernetsko varnost so v letih 2020 in 2021 še naprej naraščali ne le z vidika vektorjev in števila, temveč tudi njihovega vpliva. Tudi pandemija covida-19 je, kot je bilo pričakovano, vplivala na kibernetske grožnje. Eden dolgotrajnejših trendov, ki ga je povzročila pandemija covida-19, je trajen prehod na hibridni pisarniški model. Zato kibernetske grožnje, povezane s pandemijo, in izkoriščanje „nove normalnosti“ postajajo prevladujoči. Ta trend je povečal površino napadov, zato smo posledično videli porast števila kibernetskih napadov na organizacije in gospodarske družbe prek domačih pisarn ([3]).

Kibernetske grožnje so v splošnem v porastu. Zaradi vse večje prisotnosti na spletu, prehoda tradicionalnih infrastruktur na spletne rešitve in rešitve v oblaku, napredne medpovezljivosti in izrabe novih lastnosti nastajajočih tehnologij, kot je umetna inteligenca ([4]) ([5]), postajajo napadi v kibernetskem okolju bolj prefinjeni in zapletenejši ter vplivnejši. Tako so se zaradi svoje pomembnosti ter mogočih katastrofalnih kaskadnih učinkov najvišje med glavnimi grožnjami uvrstile predvsem grožnje za dobavne verige, in sicer tako visoko, da je agencija ENISA izdelala namensko poročilo o naravi groženj te kategorije ([6]).

Treba je poudariti, da je v tej različici poročila o naravi groženj posebej poudarjen vpliv kibernetskih groženj v različnih sektorjih, vključno s tistimi iz direktive o varnosti omrežij in informacijskih sistemov. Zanimiv vpogled prinašajo posebnosti posameznega sektorja, ko gre za okolje groženj, in potencialne soodvisnosti ter področja pomembnosti. V skladu s tem bi bilo treba sektorskim okoljem groženj nameniti dodatno pozornost.

Tudi na strani obrambe v kibernetski skupnosti in oblikovalcev politik so bili storjeni nekateri pomembni koraki. Globalna skupnost začenja prepoznavati pomen komunikacije in sodelovanja pri proučevanju storilcev kaznivih dejanj v kibernetskem prostoru in njihovem sledenju, zlasti izsiljevalsko programje (najvidnejša grožnja v poročevalskem obdobju Poročila o naravi groženj za leto 2021) pa postaja glavna točka dnevnih redov sestankov globalnih voditeljev o strategiji.

Predani bralci prejšnjih izdaj poročila o naravi groženj bodo opazili razliko pri razporejanju glavnih groženj. Letos je agencija ENISA naredila korak nazaj ter prečistila kategorije groženj, zato da bi podobne grožnje združili in bolje predstavili. Gre za stalna prizadevanja za prenovljeno taksonomijo groženj, kar bo pomagalo pri metodološkem določanju trendov v naslednjih nekaj letih.

Poročilo o naravi groženj za leto 2021 temelji na različnih informacijah iz javnih virov in virov obveščevalnih podatkov o kibernetskih grožnjah. Prinaša glavne grožnje, trende in ugotovitve ter ustrezne blažilne strategije na visoki ravni. Agencija ENISA trenutno utrjuje metodologijo poročanja o naravi groženj, s čimer spodbuja preglednost in doslednost pri delu.

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM – Cost of a Data Breach Report 2020 (Poročilo o stroških kršitev varnosti podatkov za leto 2020) – https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/.
[4] ENISA AI Threat Landscape (Poročilo o naravi groženj umetne inteligence): 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] ENISA Threat Landscape for Supply Chain Attacks (Poročilo o naravi groženj za napade na dobavne verige), julij 2021: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

1.1. GLAVNE GROŽNJE

V obdobju 2020–2021 so se pojavile in uresničile številne kibernetske grožnje. Na podlagi tu predstavljene analize je v Poročilu o naravi groženj za leto 2021 opredeljenih in izpostavljenih naslednjih 8 skupin glavnih groženj (glej Slika 1). Teh 8 skupin groženj je poudarjenih zaradi svojega pomena v poročevalskem obdobju, svoje razširjenosti in vpliva svoje uresničitve.

- **Izsiljevalsko programje**
  Izsiljevalsko programje je vrsta zlonamernega napada, pri katerem napadalci zakodirajo podatke organizacije in zahtevajo plačilo za povrnitev dostopa. Izsiljevalsko programje je bilo v poročevalskem obdobju glavna grožnja, ki jo je spremljalo več zelo odmevnih in močno medijsko izpostavljenih incidentov. Pomembnost in vpliv grožnje izsiljevalskega programja dokazujejo tudi številne povezane politične pobude v Evropski uniji in drugje po svetu.

- **Zlonamerna programska oprema**
  Zlonamerna programska oprema je programska oprema ali strojna programska oprema, namenjena izvajanju nepooblaščenega procesa, ki škodljivo vpliva na zaupnost, celovitost in razpoložljivost sistema. Grožnje, povezane z zlonamerno programsko opremo, se že vrsto let uvrščajo visoko, čeprav je v poročevalskem obdobju Poročila o naravi groženj za leto 2021 prišlo do njihovega zmanjšanja. Uporaba novih tehnik napadanja in nekatere velike zmage skupnosti organov pregona so vplivale na delovanje pomembnih akterjev groženj.

- **Kraja procesorske zmogljivosti**
  Kraja procesorske zmogljivosti ali prikrito rudarjenje kriptovalut je vrsta kibernetske kriminalitete, pri kateri storilec kaznivega dejanja prikrito uporablja računalniško zmogljivost žrtve za ustvarjanje kriptovalute. S širitvijo kriptovalut in njihovo vse večjo uporabo v širši javnosti je bilo opaženo povečano število s tem povezanih kibernetskih incidentov.

- **Grožnje v zvezi z e-pošto**
  Napadi v zvezi z e-pošto zajemajo sveženj groženj, ki predvsem izkoriščajo slabosti človeške duševnosti in vsakodnevnih navad, in ne tehnične ranljivosti informacijskih sistemov. Zanimivo je, da je grožnja kljub številnim ozaveščevalnim in izobraževalnim kampanjam zoper tovrstne napade še vedno precej prisotna. Zlasti so v porastu vrivanje v poslovno elektronsko komunikacijo in napredne prefinjene tehnike pridobivanja finančnih koristi.

- **Grožnje zoper podatke**
  Ta kategorija zajema kršitve varnosti podatkov/uhajanje podatkov. Kršitev varnosti podatkov ali uhajanje podatkov je izdaja občutljivih, zaupnih ali zaščitenih podatkov v zaupanja nevredno okolje. Kršitev varnosti podatkov je lahko posledica kibernetskega napada, dela osebe z notranjimi informacijami, nenamerne izgube ali razkritja podatkov. Grožnja je še vedno visoka, saj je dostop do podatkov glavna tarča napadalcev iz številnih razlogov, kot so izsiljevanje, odkupnina, obrekovanje, napačno informiranje itd.

- **Grožnje zoper razpoložljivost in celovitost**
  Razpoložljivost in celovitost sta tarči kopice groženj in napadov, med katerimi izstopata družini napadov za zavrnitev storitve in spletnih napadov. Strogo gledano v povezavi s spletnimi napadi je porazdeljeni napad za zavrnitev storitve ena najbolj kritičnih groženj za IT-sisteme, saj z izčrpavanjem sredstev, povzročanjem slabšega delovanja, izgubo podatkov in izpadi storitev napada njihovo razpoložljivost. Grožnja je v poročilih o naravi groženj stalno uvrščena visoko zaradi pojavljanja v dejanskih incidentih in potenciala za velik vpliv.

- **Dezinformiranje – napačno informiranje**
  Kampanje dezinformiranja in napačnega informiranja so v porastu zaradi vse večje uporabe spletnih medijev in platform družbenih medijev ter večje prisotnosti ljudi na spletu zaradi pandemije covida-19. Čeprav se ta skupina groženj prvič pojavlja v poročilu o naravi groženj, je zelo pomembna v kibernetskem svetu. Kampanje dezinformiranja in napačnega informiranja se pogosto uporabljajo pri hibridnih napadih, katerih namen je zmanjšati splošno dojemanje zaupanja, ki je pomemben zagovornik kibernetske varnosti.

- **Nezlonamerne grožnje**
  Grožnje so običajno razumljene kot prostovoljne in zlonamerne dejavnosti, ki jih ustvarjajo nasprotniki, ki v napadu na konkretno tarčo vidijo neko spodbudo. V okviru te kategorije obravnavamo grožnje, pri katerih zlonamernost ni očitna. Gre zlasti za grožnje na podlagi človeških napak in napačnih sistemskih konfiguracij,

nanašajo pa se lahko tudi na fizične nesreče, usmerjene na IT-infrastrukture. Te grožnje so po svoji naravi stalno prisotne v letnih poročilih o naravi groženj in vzbujajo resno zaskrbljenost pri ocenah tveganj.

Slika 1: Poročilo o naravi groženj za leto 2021 – glavne grožnje

Treba je poudariti, da navedene grožnje zajemajo kategorije in zbiranje groženj, razporejenih po zgoraj omenjenih osmih področjih. Vsaka skupina groženj je dodatno obravnavana v namenskem poglavju tega poročila, ki podrobneje opisuje njene posebnosti ter prinaša podrobnejše informacije, ugotovitve, trende, tehnike napadanja in blažilne vektorje.

1.2. KLJUČNI TRENDI

Spodnji seznam povzema glavne trende, opažene pri kibernetskih grožnjah v poročevalskem obdobju. Poleg tega je njihov podrobnejši pregled podan v različnih poglavjih Poročila o naravi groženj za leto 2021.

- Širjenje **zelo prefinjenega in vplivnega ogrožanja dobavnih verig**, kot poudarja namensko poročilo o naravi groženj za dobavne verige. **Ponudniki upravljanih storitev** so med storilci kaznivih dejanj v kibernetskem prostoru zelo iskane tarče.
- **Covid-19 je spodbudil določanje nalog na področju kibernetskega vohunjenja** in ustvaril **priložnosti za storilce kaznivih dejanj v kibernetskem prostoru**.
- **Vladne organizacije so pospešile izboljšave** na nacionalni in mednarodni ravni. Opažena so močnejša prizadevanja držav, da preprečijo delovanje akterjev groženj, ki jih podpira država, in zoper njih sprožijo sodne postopke.
- **Storilce kaznivih dejanj v kibernetskem prostoru vse bolj spodbuja monetizacija** njihovih dejavnosti, npr. z izsiljevalskim programjem. **Kriptovaluta** je še vedno najbolj pogost način izplačila pri akterjih groženj.
- Kibernetski napadi **so vse bolj usmerjeni in vplivajo na kritično infrastrukturo**.

- **Ogrožanje prek ribarjenja z e-sporočili in napad na storitev oddaljenega namizja (Remote Desktop Services – RDP) s surovo silo** spadata še vedno med najpogostejša **vektorja okužbe z izsiljevalskim programjem**.
- Leta 2021 se je povečala osredotočenost na **poslovne modele izsiljevalske storitve (Ransomware as a Service – RaaS)**, zaradi česar je bilo težje opredeliti posamezne akterje groženj.
- Leta 2021 se je močno povečal pojav shem, ki vključujejo **programje s trojnim izsiljevanjem**.
- **Upad zlonamerne programske opreme**, ki je bil opažen leta 2020, se leta 2021 nadaljuje. Leta 2021 smo opazili večje zatekanje akterjev groženj k razmeroma novim ali redkim programskim jezikom za prenos svojih kod.
- **Zlonamerna programska oprema, ki napada vsebniška okolja**, je veliko bolj prisotna, pri čemer se pojavljajo novosti, kot je brezdatotečna zlonamerna programska oprema, ki se izvaja iz pomnilnika.
- Razvijalcem zlonamerne programske opreme uspeva **otežiti izvajanje obratnega inženiringa in dinamične analize**.
- Število **okužb za krajo procesorske zmogljivosti** je v primerjavi z zadnjimi nekaj leti v prvem četrtletju leta 2021 doseglo **rekordno vrednost**. K izvedbi teh napadov je akterje groženj spodbudila **finančna korist**, povezana s krajo procesorske zmogljivosti.
- **Rudarjenje kriptovalut leta 2021 in dejavnosti kraje procesorske zmogljivosti so dosegli rekordne vrednosti**.
- Lahko vidimo, da prihaja do **premika kraje procesorske zmogljivosti z brskalnika na datoteke**.
- **Covid-19 je še vedno prevladujoča vaba v kampanjah** za napade po e-pošti.
- **Vrivanje v poslovno elektronsko komunikacijo** se je **povečalo**, postaja bolj **prefinjeno** in **ciljno usmerjeno**.
- Poslovni model **ribarjenja kot storitve (Phishing as a Service – PhaaS)** je vse bolj prisoten.
- Akterji groženj so pozornost preusmerili na **informacije o cepivih** v okviru groženj za podatke in informacije.
- Število **kršitev varnosti podatkov, povezanih z zdravstvenim sektorjem, se je povečalo**.
- Tradicionalni porazdeljeni napadi za zavrnitev storitve se preusmerjajo na **mobilna omrežja in internet stvari**.
- **Izsiljevalski napadi za zavrnitev storitve (Ransom Denial of Service – RDoS)** so nova vrsta napadov za zavrnitev storitve.
- **Skupna raba virov v virtualiziranih okoljih** krepi porazdeljene napade za zavrnitev storitve.
- **Kampanje porazdeljenih napadov za zavrnitev storitve** so leta 2021 postale bolj ciljno usmerjene, precej vztrajnejše in vse bolj večvektorske.
- **Z umetno inteligenco podprto dezinformiranje** napadalcem pomaga izvesti napade.
- **Osrednji del dezinformacijskih napadov je ribarjenje**, ki močno izkorišča prepričanja ljudi.
- **Napačno informiranje in dezinformiranje** sta ključna dela dejavnosti kibernetske kriminalitete in sta v izrednem porastu.
- Uporaba **poslovnega modela dezinformiranja kot storitve (Disinformation as a Service – DaaS)** močno narašča zaradi vse večjega vpliva pandemije covida-19 in potrebe po več informacij.
- V letih 2020 in 2021 smo opazili **porast nezlonamernih incidentov**, saj je pandemija covida-19 število **človeških napak** in **napačnih sistemskih konfiguracij** pomnožila do točke, da so večino kršitev leta 2020 povzročile napake.
- Prišlo je do **porasta nezlonamernih incidentov na področju varnosti oblaka**.

1.3. EU IN BLIŽINA GLAVNIH GROŽENJ

Pomemben vidik, ki ga je treba upoštevati v okviru poročila o naravi groženj, zajema bližino kibernetskih groženj glede na Evropsko unijo (EU). To je zlasti pomembno z vidika pomoči analitikom pri oceni pomembnosti kibernetskih groženj, njihovem povezovanju s potencialnimi akterji in vektorji groženj ter celo usmerjanju izbire ustreznih ciljno usmerjenih blažilnih vektorjev. V skladu s predlagano razvrstitvijo za skupno varnostno in obrambno politiko EU (SVOP) ([7]) kibernetske grožnje razvrščamo v štiri kategorije, ki jih ponazarja Preglednica 1.

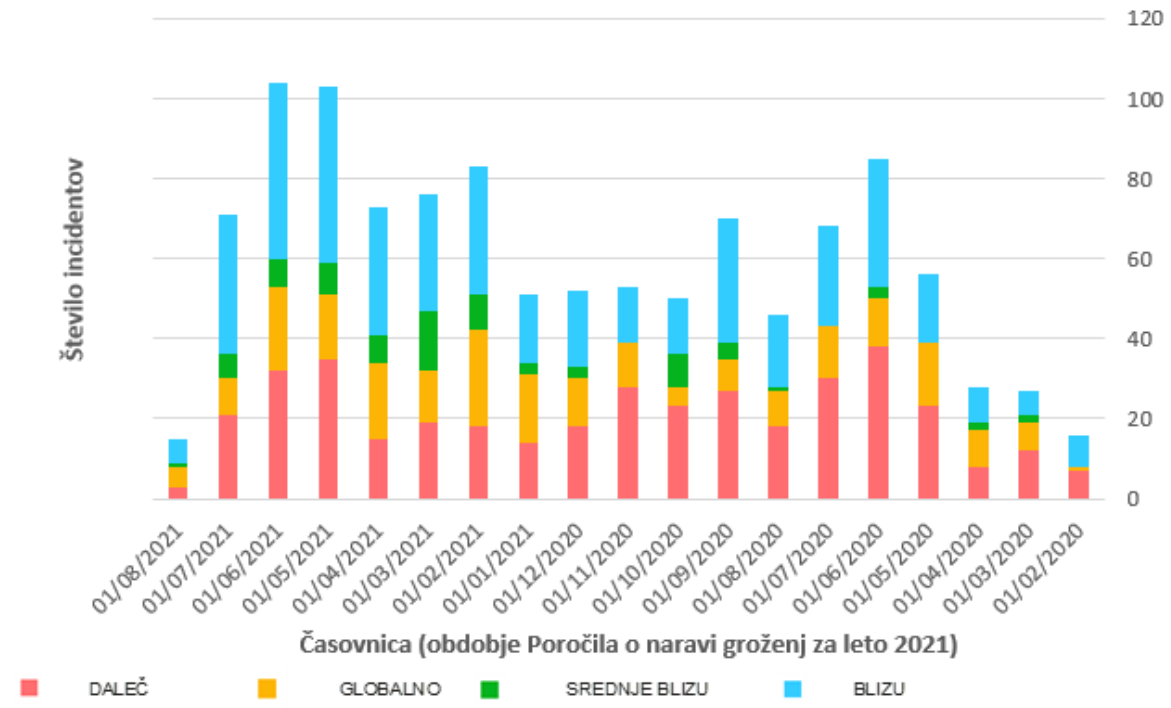
[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf

Preglednica 1: Razvrstitev bližine kibernetskih groženj

Bližina	Zaskrbljenost
BLIZU	Prizadeta omrežja, sistemi, nadzorovani in zagotavljani znotraj meja EU. Prizadeto prebivalstvo znotraj meja EU.
SREDNJE BLIZU	Omrežja in sistemi, ki veljajo za ključne za operativne cilje znotraj digitalnega enotnega trga EU in sektorjev, na katere se nanaša direktiva o varnosti omrežij in informacijskih sistemov, vendar se njihov nadzor in zagotavljanje opirata na institucionalne organe iz tretjih držav ali javne in zasebne organe držav članic. Prizadeto prebivalstvo na geografskih območjih blizu meja EU.
DALEČ	Omrežja in sistemi, katerih prizadetost bi kritično vplivala na operativne cilje znotraj digitalnega enotnega trga EU in sektorjev, na katere se nanaša direktiva o varnosti omrežij in informacijskih sistemov. Nadzor in zagotavljanje navedenih omrežij in sistemov sta zunaj institucionalnih organov EU ali javnih ali zasebnih organov držav članic. Prizadeto prebivalstvo na geografskih območjih daleč od EU.
GLOBALNO	Vsa navedena območja.

Slika 2 ponazarja časovnico incidentov, povezanih s kategorijami glavnih groženj, na katere se nanaša Poročilo o naravi groženj za leto 2021. Poudariti je treba, da informacije v diagramu temeljijo na OSINT (obveščevalnih podatkih iz javnih virov) in so rezultat dela agencije ENISA na področju situacijskega zavedanja ([8]).

Slika 2: Časovnica opaženih incidentov, povezanih s pomembnimi grožnjami iz poročila o naravi groženj (situacijsko zavedanje na podlagi OSINT) z vidika njihove bližine



Kot kaže zgornja slika, je bilo leta 2021 več incidentov kot leta 2020. Zlasti v kategoriji BLIZU nenehno raste število opaženih incidentov, povezanih z glavnimi grožnjami, kar kaže na njihovo pomembnost za EU. Ni presenetljivo, da

[8] V skladu s členom 7(6) uredbe EU o kibernetski varnosti: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.

so mesečni trendi (na sliki niso prikazani zaradi zgoščenosti) precej podobni pri različnih razvrstitvah, saj kibernetska varnost ne pozna meja, grožnje pa se v večini primerov uresničujejo na vseh ravneh bližine. Upoštevati je treba, da je bilo v zadnjih mesecih, na katere se nanaša Poročilo o naravi groženj za leto 2021, opaženih več groženj BLIZU EU, agencija ENISA pa bo še naprej spremljala ta trend, da ugotovi, kako se giblje in kako je povezan z dejavnostmi akterjev groženj in tekočih vektorjev groženj.

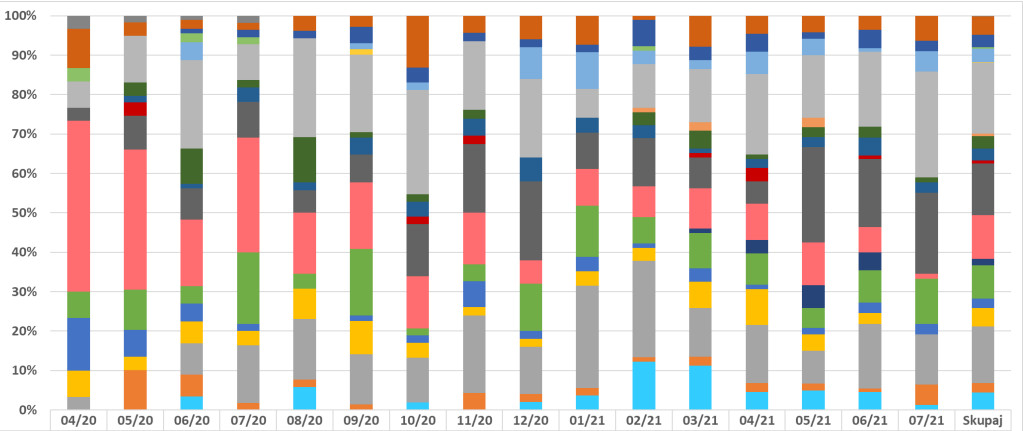
1.4. GLAVNE GROŽNJE PO SEKTORJIH

Kibernetske grožnje običajno niso omejene na posamezen sektor, v večini primerov pa prizadenejo več kot enega. To je dejansko res, saj se v številnih primerih grožnje kažejo skozi izkoriščanje ranljivosti osnovnih sistemov IKT, ki se uporabljajo v različnih sektorjih. Kljub temu so tarčni napadi in napadi, ki izkoriščajo razlike v zrelosti kibernetske varnosti po sektorjih ter razširjenost/pomen nekaterih sektorjev, tudi dejavniki, ki jih je treba upoštevati. Ti dejavniki prispevajo h grožnjam, ki se kažejo kot incidenti v konkretnih sektorjih, zato je pomembno temeljito proučiti sektorske vidike opaženih incidentov in groženj. Poleg tega se lahko s tako analizo ugotovijo trendi v posameznih sektorjih in medsektorska odvisnost.

Sliki 3 in 4 kažeta sektorje, ki so jih prizadeli incidenti, opaženi na podlagi OSINT (obveščevalnih podatkov iz javnih virov), ki so rezultat dela agencije ENISA na področju situacijskega zavedanja ([9]). Nanašata se na incidente, povezane z glavnimi grožnjami iz Poročila o naravi groženj za leto 2021. To je prvi poskus agencije ENISA, da razporedi vpliv groženj na konkretne sektorje. V naslednjih letih in naslednjih različicah poročil o naravi groženj bodo prizadevanja usmerjena v usklajevanje sektorjev s tistimi iz direktive o varnosti omrežij in informacijskih sistemov ter izdelavo predloga za njen pregled (direktiva o varnosti omrežij in informacijskih sistemov 2.0).

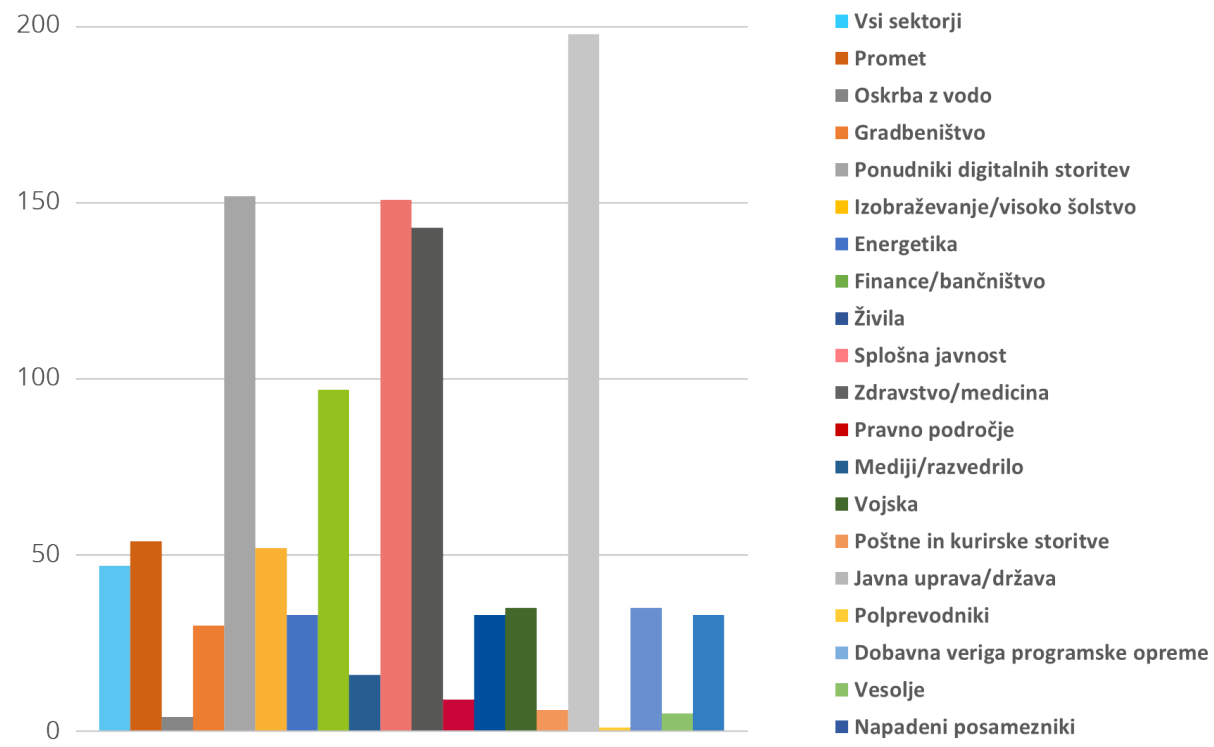
[9] V skladu s členom 7(6) uredbe EU o kibernetski varnosti (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN).

Slika 3: Časovnica opaženih incidentov, povezanih z glavnimi grožnjami iz poročila o naravi groženj, z vidika prizadetega sektorja



	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	Skupaj
Oskrba z vodo	1	1	1	1													2
Promet	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Napadeni posamezniki			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Vesolje	1		2	1							1						4
Dobavna veriga programske opreme			4			1	1		4	5	3	2	5	5	1	4	35
Polprevodniki						1											1
Javna uprava/država	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Poštne in kurirske storitve											1	2		3			6
Vojska		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Mediji/razvedrilo		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Pravno področje		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
Splošna javnost	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Živila												1	3	7	5		16
Finance/bančništvo	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
Izobraževanje/visoko šolstvo	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Ponudniki digitalnih storitev	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Gradbeništvo		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Vsi sektorji			3		3		1		1	2	11	10	4	6	5	1	47

Slika 4: Napadeni sektorji po številu incidentov (april 2020–julij 2021)



V tem poročevalskem obdobju je veliko incidentov prizadelo javno upravo in državo ter ponudnike digitalnih storitev. Slednje je pričakovano glede na vodoravno opravljanje storitev, kar vpliva na številne druge sektorje. Opazili smo tudi precejšnje število incidentov, ki so prizadeli končne uporabnike in ne nujno konkretni sektor. Tudi zdravstveni sektor je bil deležen velikega števila napadov, v zadnjih nekaj mesecih poročevalskega obdobja (maj–julij 2021) pa so se pokazali znaki naraščanja te dejavnosti. Zanimivo je, da je število incidentov čez leto v finančnem sektorju enakomerno. Tudi dobavna veriga programske opreme kaže porast števila incidentov v letu 2021, kar je ugotovljeno tudi v poročilu o naravi groženj za dobavne verige ([10]).

1.5. METODOLOGIJA

Poročilo o naravi groženj za leto 2021 temelji na informacijah iz javnih virov, ki so predvsem strateške narave, in lastnih zmogljivostih agencije ENISA za pridobivanje obveščevalnih podatkov o kibernetskih grožnjah, nanaša pa se na več sektorjev, tehnologij in področij. Poročilo skuša biti nevtralno z vidika panoge in dobaviteljev, pri čemer se v besedilu in sprotnih opombah sklicuje na dela različnih varnostnih raziskovalcev, varnostne spletne dnevnike in članke iz novičarskih medijev ali jih navaja. Poročilo o naravi groženj za leto 2021 se nanaša na obdobje od aprila 2020 do julija 2021, ki se v poročilu omenja kot „poročevalsko obdobje“.

Pri izdelavi Poročila o naravi groženj za leto 2021 je bil uporabljen naslednji pristop. Agencija ENISA je s situacijskim zavedanjem v ustreznem obdobju oblikovala seznam pomembnih incidentov, o katerih so poročali javni viri. Seznam je bil uporabljen kot podlaga za pripravo seznama glavnih groženj ter izvornega gradiva za različne trende in statistične podatke v poročilu.

Agencija ENISA in zunanji strokovnjaki so nato opravili poglobljen pregled razpoložljive literature iz javnih virov, kot so članki novičarskih medijev, strokovna mnenja, obveščevalna poročila ter poročila o analizah incidentov in varnostnih raziskavah. Na podlagi stalnega proučevanja je agencija ENISA izpeljala trende in pomembne točke za posamezne pomembne grožnje, predstavljene v Poročilu o naravi groženj za leto 2021. Ključne ugotovitve in

[10] ENISA Threat Landscape for Supply Chain Attacks, julij 2021: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

presoje v tej oceni temeljijo na več javno dostopnih virih, navedenih v referencah, uporabljenih za izdelavo tega dokumenta.

V poročilu skušamo razlikovati med tistim, o čemer so poročali naši viri, in tistim, kar je naša ocena (pri tem konkretno uporabljamo besedno zvezo „po naši oceni“). Nazadnje, pri ocenjevanju sporočamo verjetnost z besedami, ki izražajo oceno verjetnosti (npr. verjetno, zelo verjetno, zagotovo) ([11]).

V tem poročilu smo uporabili okvir MITRE ATT&CK® ([12]), s katerim smo poudarili napadalne taktike in tehnike, ki se nanašajo na zadevne grožnje (glej Prilogo A). Za vsako taktiko ATT&CK® so predstavljene tehnike, ki jih je uporabil nasprotnik. To lahko privede do seznama blažitev ATT&CK ([13]), ki se lahko uporabijo. MITRE ATT&CK® je zbirka znanja oziroma skupni jezik za nasprotne taktike in tehnike, ki temeljijo na opažanjih iz resničnega sveta. Zbirka znanja MITRE ATT&CK® se uporablja kot podlaga za oblikovanje konkretnih modelov groženj in z njimi povezanih metodologij v zasebnem sektorju, državi in skupnosti proizvodov in storitev za kibernetsko varnost.

Poročilo je potrdila ad hoc delovna skupina agencije ENISA za kibernetske grožnje ([14]), ki je bila ustanovljena aprila 2021, gre pa za skupino, ki jo sestavljajo strokovnjaki iz evropskih in mednarodnih subjektov javnega in zasebnega sektorja.

Glede nadaljnje opredelitve okolij groženj agencija ENISA trenutno pripravlja novo metodologijo, ki bo spodbujala preglednost ter zagotovila podlago za organizirane in usklajene postopke. V okviru teh prizadevanj bo metodologija za okolja groženj skupaj z revidirano taksonomijo groženj v prihodnje javno objavljena.

1.6. ZGRADBA POROČILA

Poročilo o naravi groženj za leto 2021 ohranja zgradbo predhodnih poročil o naravi groženj, pri čemer uporablja podobno zgradbo za poudarjanje glavnih kibernetskih groženj leta 2021. Bralci prejšnjih različic bodo opazili, da so kategorije groženj prečiščene, zato da se oblikuje nova taksonomija kibernetskih groženj, ki se bo uporabljala v prihodnje.

To poročilo je sestavljeno na naslednji način:

poglavje 2 obravnava trende, povezane z akterji groženj (t. i. akterji, ki jih podpira država, akterji kibernetske kriminalitete, akterji, ki so hekerji najemniki, in hektivisti);
poglavje 3 obravnava pomembne ugotovitve, incidente in trende glede izsiljevalskega programja;
poglavje 4 prinaša pomembne ugotovitve, incidente in trende glede zlonamerne programske opreme;
poglavje 5 opisuje pomembne ugotovitve, incidente in trende glede kraje procesorske zmogljivosti;
poglavje 6 podaja pomembne ugotovitve, incidente in trende glede groženj v zvezi z e-pošto;
poglavje 7 obravnava pomembne ugotovitve, incidente in trende glede groženj za podatke;
poglavje 8 prinaša pomembne ugotovitve, incidente in trende glede groženj zoper razpoložljivost in celovitost;
poglavje 9 opisuje pomembne ugotovitve, incidente in trende glede dezinformiranja in napačnega informiranja;
poglavje 10 obravnava pomembne ugotovitve, incidente in trende glede nezlonamernih groženj;
Priloga A prinaša tehnike, ki se pogosto uporabljajo pri posameznih grožnjah, na podlagi okvira MITRE ATT&CK®;
Priloga B zajema pomembne incidente po grožnjah, ki so bili opaženi v poročevalskem obdobju.

[11] CIA – besede ocenjevalne verjetnosti: 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