Článok
21-03-2023 - 14:26
20220120ST021428

Európsky parlament

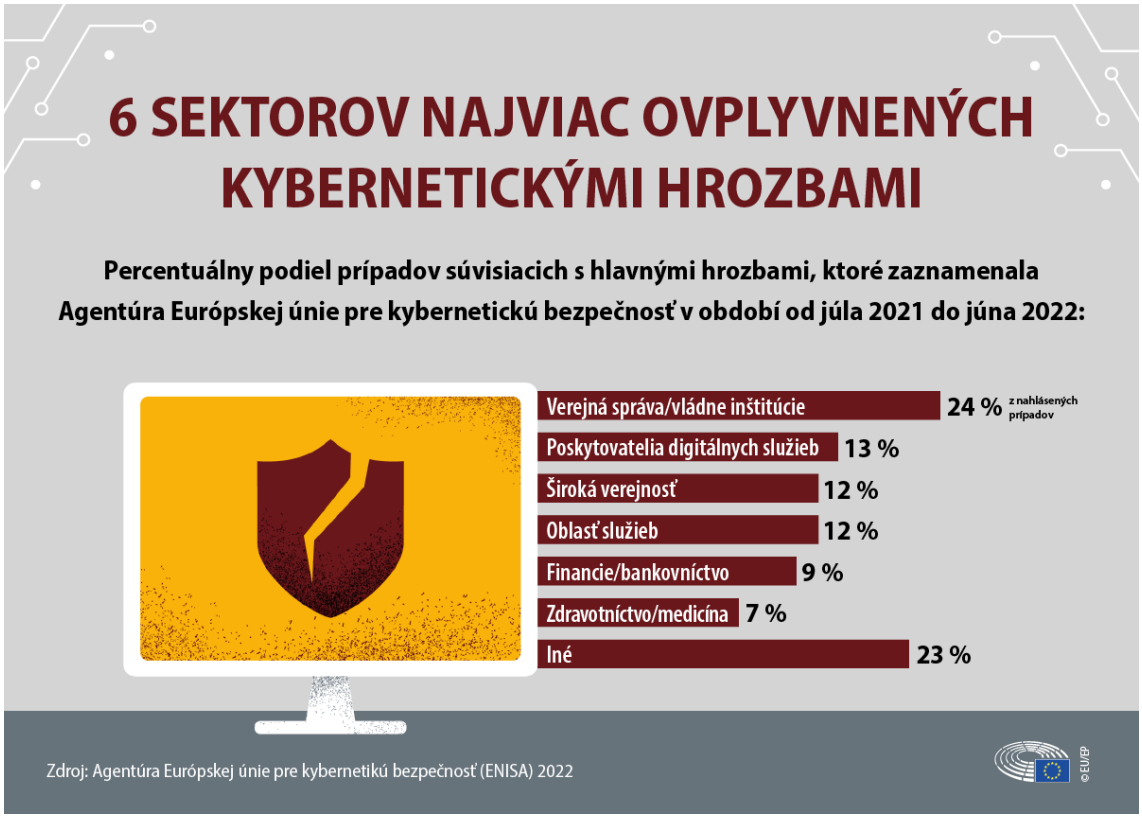
Kybernetická bezpečnosť: hlavné hrozby v roku 2021 (infografika)

Prečítajte si o hlavných kybernetických hrozbách v roku 2022, najviac postihnutých odvetviach a vplyve vojny na Ukrajine.

Pokrok v oblasti digitálnej transormácie so sebou nevyhnutne prináša aj riziko kybernetických hrozieb. Počas pandémie boli spoločnosti nútené sa rýchlo adaptovať na nové pracovné podmienky, čo tiež otvorilo dvere príležitostí pre kybernetických zločincov.

Parlament prijal novú smernicu, ktorá reflektuje zmeny na poli kybernetickej bezpečnosť a prináša jednotné opatrenia naprieč EÚ, vrátane ochrany sektorov nevyhnutných na chod spoločnosti.

Zistite viac o opatreniach EÚ na boj proti kybernetickým zločinom.



Sektory najviac ovplyvnené kybernetickými hrozbami

8 najväčších kybernetických hrozieb

Podľa správy o kybernetických hrozbách za rok 2022 vypracovanej Európskou agentúrou pre kybernetickú bezpečnosť (ENISA) medzi hlavnými skupinami hrozieb patria nasledovné:

1. Ransomvér: útočníci zamedzia prístup k dátam spoločnosti a požadujú výkupné za znovu umožnenie prístupu

V roku 2022 boli útoky ransomvéru naďalej jednou z hlavných kybernetických hrozieb. Zároveň sú čoraz zložitejšie. Podľa prieskumu citovaného agentúrou ENISA, ktorý sa uskutočnil koncom roka 2021 a v roku 2022, bola viac ako polovica respondentov alebo ich zamestnancov oslovená pri útokoch ransomvéru.

Z údajov, ktoré citovala Agentúra pre kybernetickú bezpečnosť, vyplýva, že najvyššia požiadavka na výkupné vzrástla z 13 miliónov eur v roku 2019 na 62 miliónov eur v roku 2021 a priemerné zaplatené výkupné sa zdvojnásobilo zo 71 000 eur v roku 2019 na 150 000 eur v roku 2020. Odhaduje sa, že v roku 2021 dosiahne celosvetová škoda spôsobená ransomvérom

hodnotu 18 miliárd eur, čo je 57-krát viac ako v roku 2015.

2. Malvér – škodlivý softvér, ktorý napáda operačný systém užívateľa

Malvér zahŕňa vírusy, červy, trójske kone a spyware. Po globálnom poklese malvéru spojeného s pandémiou v roku 2020 a začiatkom roka 2021 sa jeho používanie výrazne zvýšilo koncom roka 2021, keď sa ľudia začali vracať do kancelárií.

Nárast malvéru sa pripisuje aj tzv. crypto-jackingu (tajnému použitiu počítača obete na nelegálnu ťažbu kryptomien) a malvéru tzv. internetu vecí (malvér zameraný na zariadenia pripojené k internetu, ako sú routre alebo kamery).

Podľa agentúry ENISA bolo v prvých šiestich mesiacoch roku 2022 zaznamenaných viac útokov v súvislosti z internetom vecí (z anglického Internet-of-Things) ako za predchádzajúce štyri roky.

3. Hrozby sociálneho inžinierstva - využitie ľudskej chyby na získanie prístupu k informáciám alebo službám

Podvod voči obetiam, aby otvorili škodlivé dokumenty, súbory alebo e-maily, navštívili webové stránky, a tak získali neoprávnený prístup k systémom alebo službám. Najbežnejším útokom tohto druhu je tzv. **phishing** (prostredníctvom e-mailu); alebo **smishing** (prostredníctvom textových správ). Podľa prieskumu, ktorý citovala agentúra ENISA, takmer 60 % prípadov narušenia bezpečnosti v Európe, na Blízkom východe a v Afrike obsahuje prvok sociálneho inžinierstva. Najčastejšie organizácie, za ktoré sa vydávali phisheri, boli z finančného a technologického sektora. Zločinci sa čoraz častejšie zameriavajú aj na krypto burzy a vlastníkov kryptomien.

4. Hrozby spojené s prístupom k údajom

Zameranie sa na zdroje údajov s cieľom získať neoprávnený prístup a ich zverejnenie (H3)Žijeme v ekonomike založenej na údajoch, ktorá produkuje obrovské množstvo údajov, ktoré sú okrem iného mimoriadne dôležité pre podniky a umelú inteligenciu, čo z nich robí hlavný cieľ kyberzločincov. Hrozby voči údajom možno klasifikovať najmä ako narušenia údajov (úmyselné útoky kyberzločinca) a úniky údajov (neúmyselné zverejnenie údajov).Najčastejšou motiváciou takýchto útokov zostávajú peniaze. Len v 10 % prípadov je motívom špionáž.

5. Hrozby obmedzujúce prístup k údajom

Útoky brániace používateľom v prístupe k údajom alebo službám (H3)Ide o jedny z najkritickejších hrozieb pre IT systémy. Ich rozsah a zložitosť narastá. Jednou z bežných foriem

útoku je preťaženie sieťovej infraštruktúry a zneprístupnenie systému.Útoky typu Denial of Service čoraz častejšie zasahujú mobilné siete a pripojené zariadenia. Často sa používajú v rusko-ukrajinskej kybernetickej vojne. Terčom útokov sa stali aj webové stránky súvisiace s Covid-19, ako napríklad stránky na získanie očkovania.

6. Hrozby spojené s dostupnosťou internetu

Patrí k nim fyzické prevzatie a zničenie internetovej infraštruktúry, ako to bolo vidieť na okupovaných ukrajinských územiach od invázie, ako aj aktívna cenzúra spravodajských webových stránok alebo webových stránok sociálnych médií.

7. Dezinformácie/dezinformácie - šírenie zavádzajúcich informácií

Čoraz častejšie využívanie platforiem sociálnych médií a online médií viedlo k nárastu kampaní šíriacich dezinformácie (zámerne falšované informácie) a dezinformácie (zdieľanie nesprávnych údajov). Cieľom je vyvolať strach a neistotu. Rusko využilo túto technológiu na cielené vnímanie vojny. Technológia Deepfake znamená, že v súčasnosti je možné vytvárať falošné zvuky, videá alebo obrázky, ktoré sú takmer na nerozoznanie od skutočných. Boti, ktorí sa vydávajú za skutočných ľudí, môžu narúšať online komunity tým, že ich zaplavia falošnými komentármi.

Prečítajte si viac o sankciách proti dezinformáciám, ktoré požaduje Parlament.

8. Útoky na dodávateľský reťazec

Tieto útoky sa zameriavajú na vzťahy medzi organizáciami a dodávateľmi. Ide o kombináciu dvoch útokov - na dodávateľa a zákazníka. Organizácie sú voči takýmto útokom čoraz zraniteľnejšie, pretože majú čoraz zložitejšie systémy a množstvo dodávateľov, na ktorých je ťažšie dohliadať.

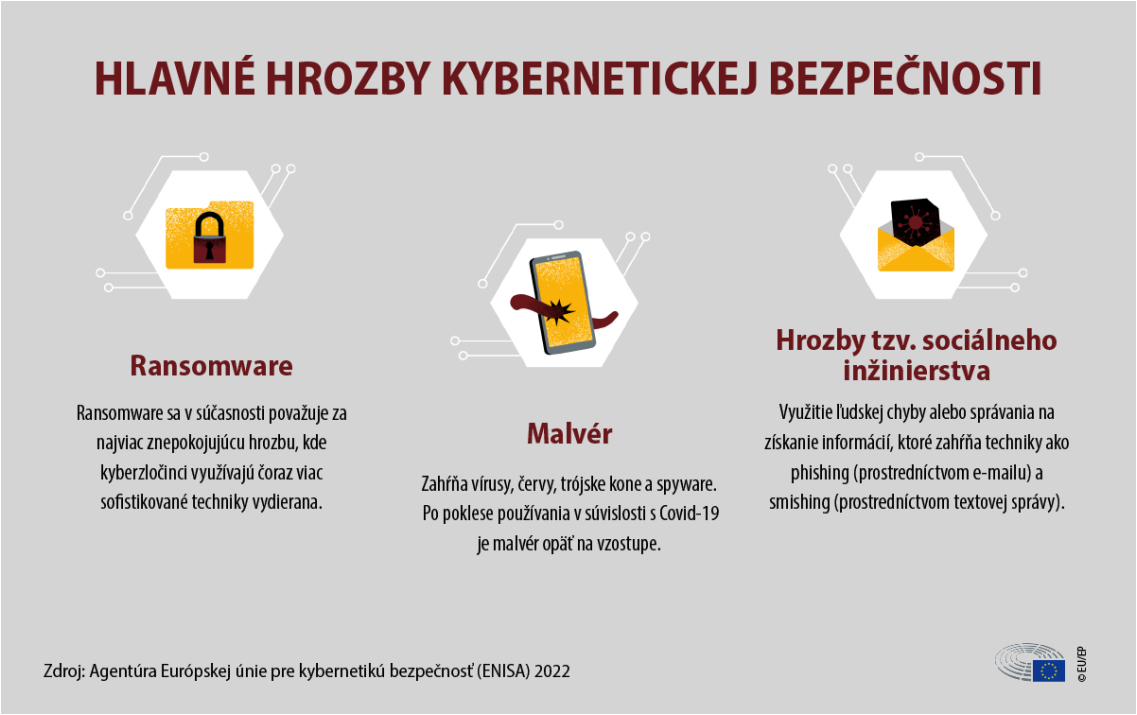
Sektory najviac zasiahnuté kybernetickými hrozbami

Kybernetické hrozby v Európskej únii ovplyvňujú životne dôležité sektory nevyhnutné pre chod spoločnosti. Medzi sektory najviac ovplyvnené hrozbami podľa Európskej agentúry pre kybernetickú bezpečnosť (ENISA) patrili v období jún 2021 až jún 2022:

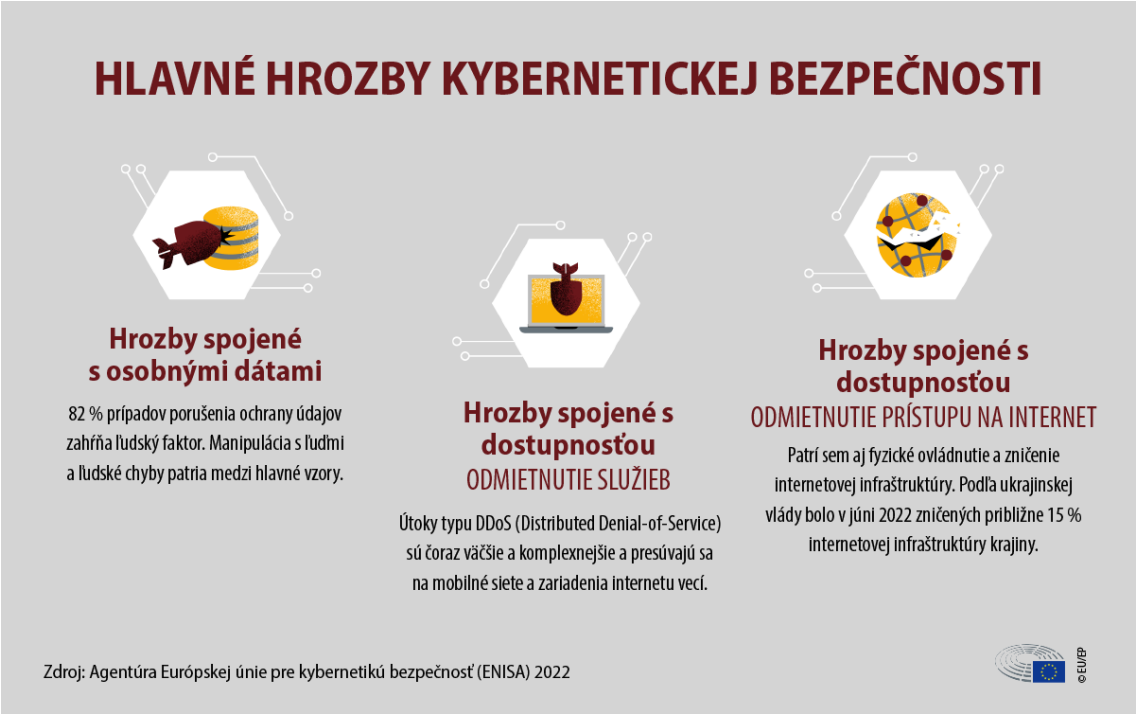
1. verejná správa a štátne inštitúcie (24 % zaznamenaných hrozieb),
2. poskytovatelia digitálnych služieb (13 % zaznamenaných hrozieb),
3. široká verejnosť (12,4 % zaznamenaných hrozieb),
4. služby (11,8 % zaznamenaných hrozieb),

5. finančníctvo/bankovníctvo (8,6% zaznamenaných hrozieb) a
6. zdravotníctvo (7,2 % zaznamenaných hrozieb).

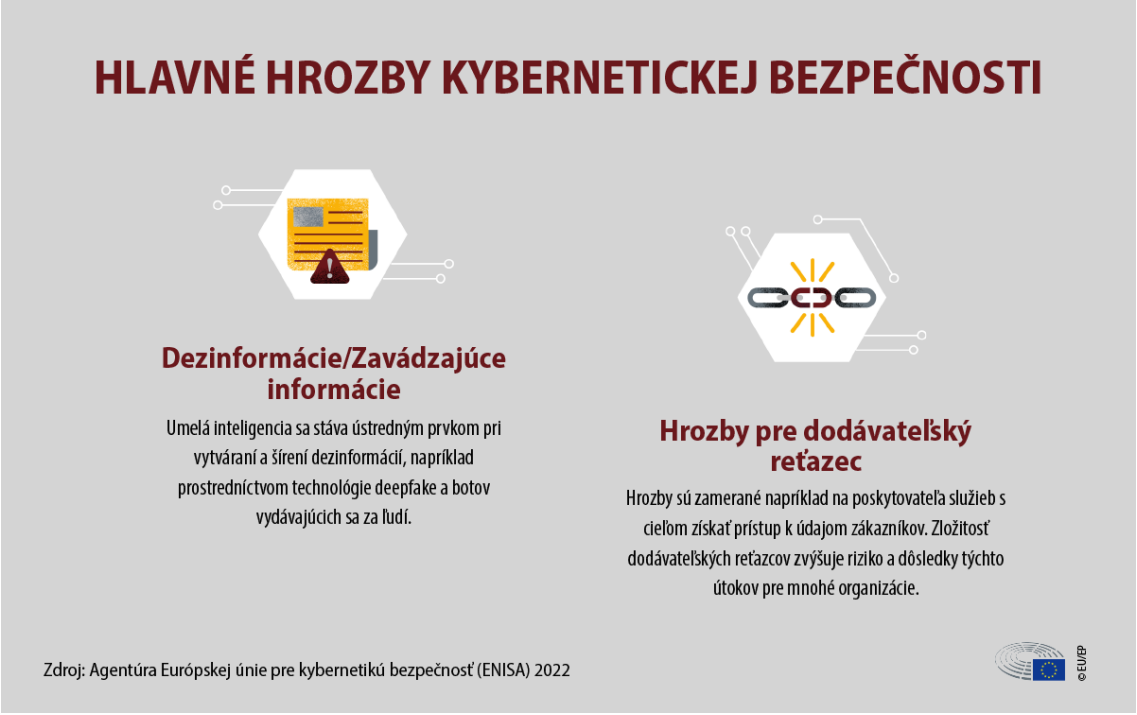
Prečítajte si viac o nákladoch spojených s kybernetickými útokmi.



SK_IFG cybersecurity_2023_cybersecurity2-1.png



SK_IFG cybersecurity_2023_cybersecurity2-2.png



Hlavné hrozby kybernetickej bezpečnosti

Vojna na Ukrajine a kybernetické hrozby

Vojna Ruska na Ukrajine ovplyvnila kybernetickú sféru mnohými spôsobmi. Kybernetické operácie sa používajú ruka v ruke s tradičnými vojenskými akciami. Podľa agentúry Enisa aktéri sponzorovaní ruským štátom uskutočnili **kybernetické operácie** proti subjektom a organizáciám na Ukrajine a v krajinách, ktoré ju podporujú.

Zvýšila sa aj tzv. **hacktivistov** (hackerov na politicky alebo sociálne motivované účely), pričom mnohí z nich vykonávajú útoky na podporu vybranej strany konfliktu.

Dezinformácie boli nástrojom kybernetickej vojny už pred začiatkom invázie a využívajú ich obe strany. Ruské dezinformácie sa zameriavajú na hľadanie ospravedlnení pre inváziu, zatiaľ čo Ukrajina používa dezinformácie na motiváciu vojakov. Používali sa aj deepfake videá s ruskými a ukrajinskými lídrami, ktorí vyjadrovali názory podporujúce druhú stranu konfliktu.

Kyberzločinci sa pokúšali **vylákať peniaze** od ľudí, ktorí chceli podporiť Ukrajinu, prostredníctvom falošných charitatívnych organizácií.

Viac informácií o tom, ako chce EÚ posilniť zdieľanie údajov a regulovať umelú inteligenciu.

Ďalšie informácie (v anglickom jazyku)

Agentúra ENISA: Kybernetické hrozby v roku 2030
Europol: Kybernetické zločiny