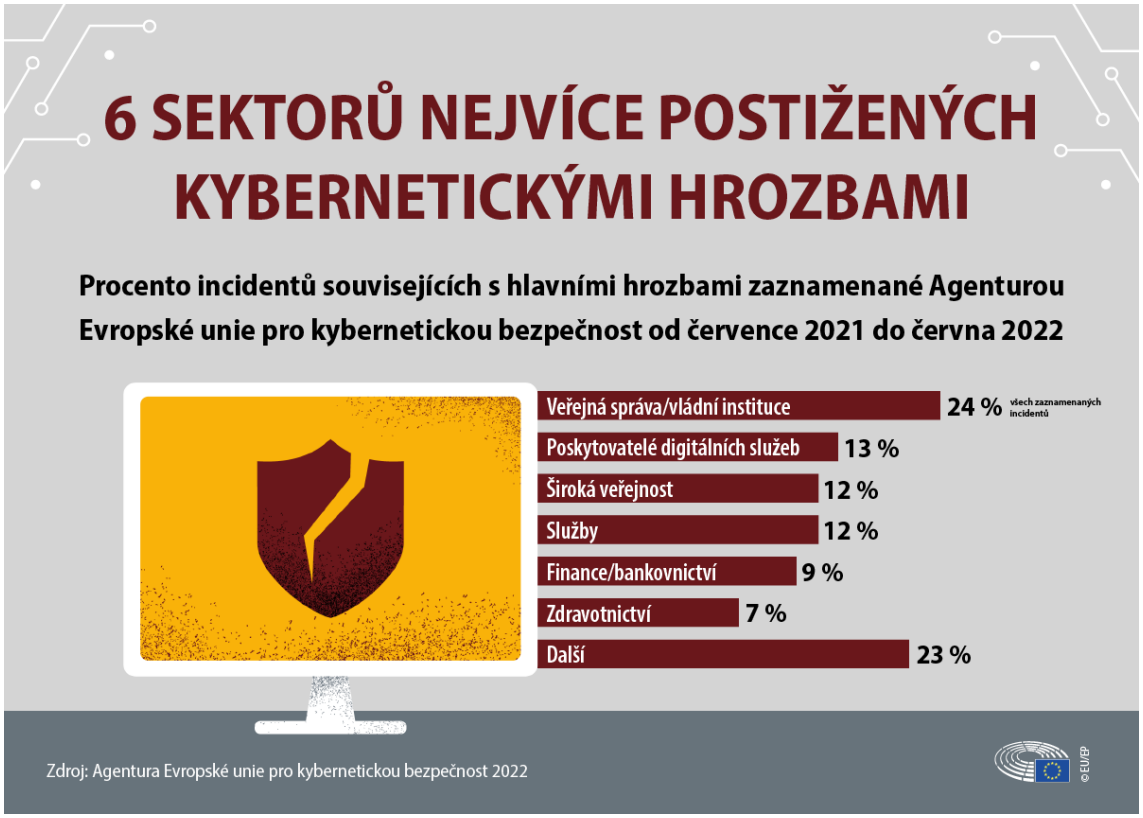
Článek

21-03-2023 - 10:50
20220120ST021428

Evropský parlament

Kybernetická bezpečnost: Hlavní a nově se objevující hrozby

S kterými kybernetickými hrozbami jsme se v roce 2022 potýkali nejvíce? Které sektory byly postiženy nejčastěji? A jaký dopad má válka na Ukrajině?

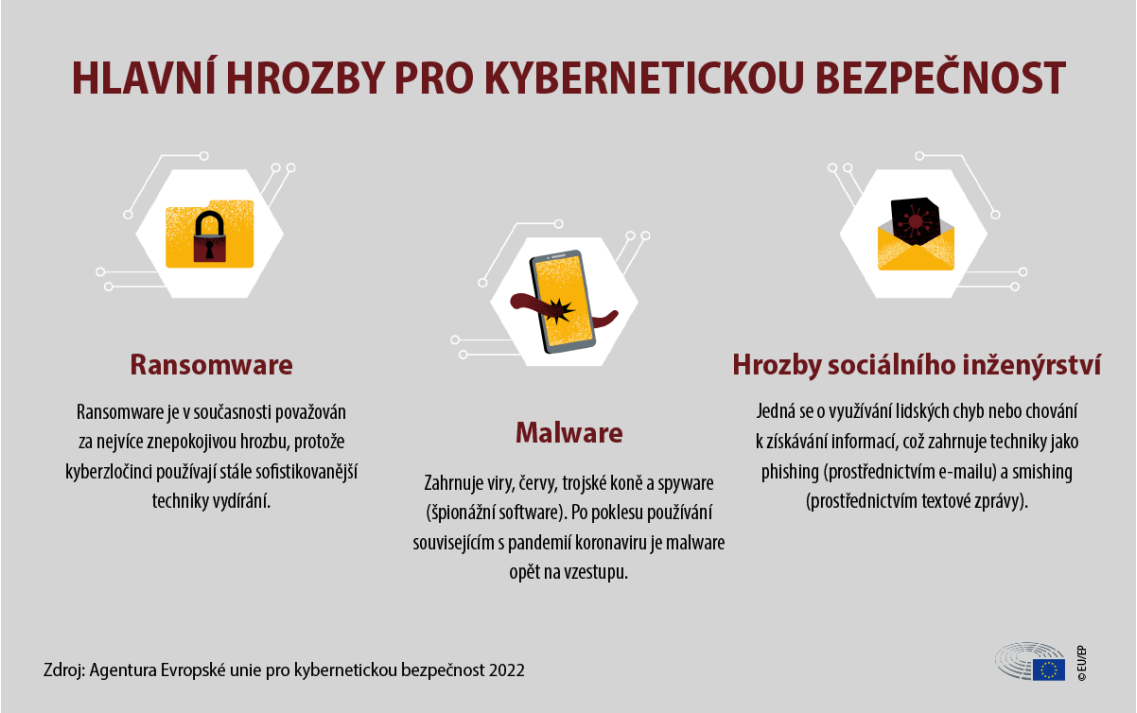


Které sektory jsou kybernetickými hrozbami postižené nejvíce?

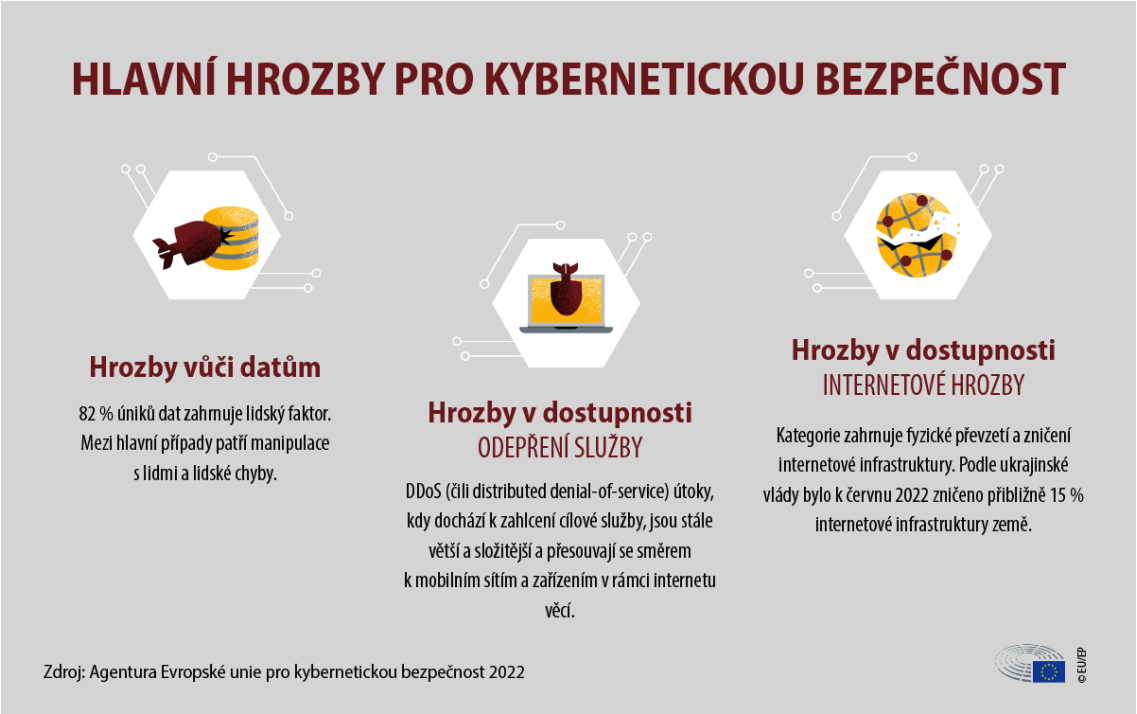
Pokrok v oblasti digitální transformace nevyhnutelně vedl k tomu, že se vynořily nové hrozby pro kybernetickou bezpečnost. Během pandemie koronaviru se mnoho společností muselo rychle přizpůsobit novým pracovním podmínkám – práce na dálku a z domu otevřela nové přístupové body a možnosti pro kybernetické útoky. Nejčastěji využívané hrozby změnila také válka na Ukrajině.

Parlament přijal svůj postoj ke směrnici, která změnu situace na poli kybernetické bezpečnosti a nově se objevujících hrozeb bere v potaz a zavádí harmonizovaná opatření v celé EU, včetně ochrany základních sektorů.

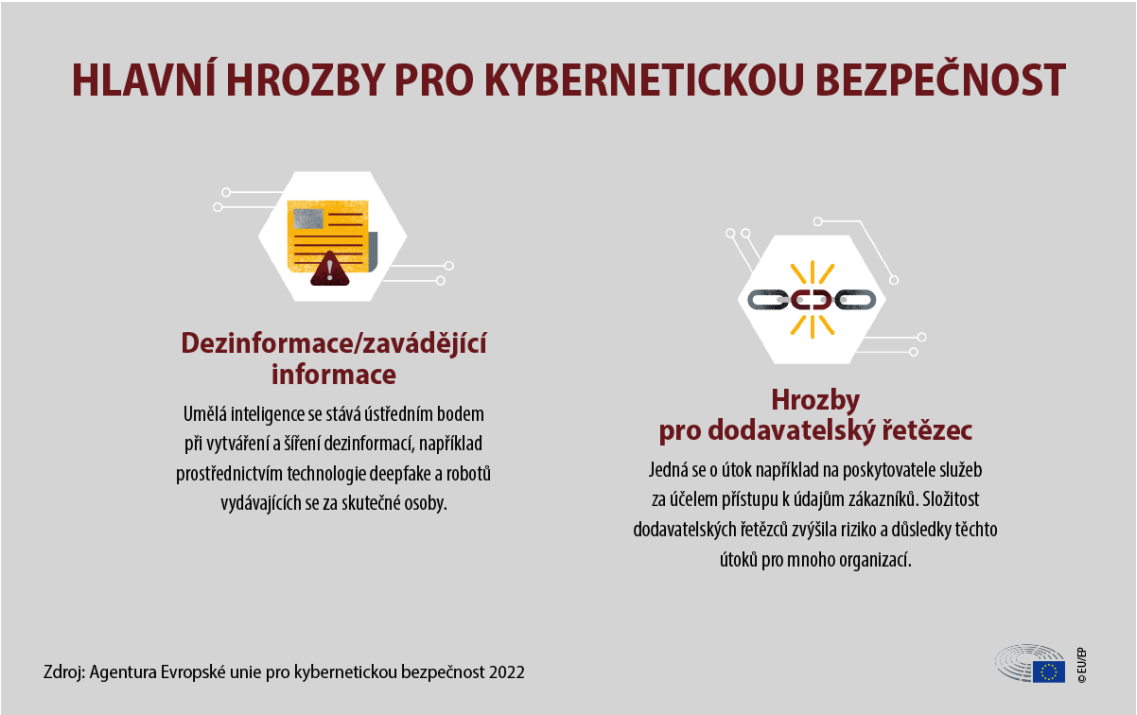
Přečtěte si více o tom, jak chce Parlament posílit kybernetickou bezpečnost v EU.



Hlavní hrozby pro kybernetickou bezpečnost



Hlavní hrozby pro kybernetickou bezpečnost



Hlavní hrozby pro kybernetickou bezpečnost

Osm hlavních hrozeb pro kybernetickou bezpečnost (nejen v roce 2022)

Podle Agentury Evropské unie pro kybernetickou bezpečnost (ENISA) existuje osm hlavních skupin hrozeb:

1. Ransomware – útočníci se zmocní cizích dat a za obnovení přístupu vyžadují zaplacení výkupného

V roce 2022 byly útoky ransomwaru i nadále jednou z hlavních kybernetických hrozeb. Jsou rovněž stále komplikovanější. Podle průzkumu citovaného agenturou Enisa, který byl proveden na konci roku 2021 a v roce 2022, se více než polovina respondentů nebo jejich zaměstnanců s útoky ransomwaru osobně setkala.

Podle údajů Agentury EU pro kybernetickou bezpečnost vzrostla průměrná výše požadovaného výkupného z 13 milionů eur v roce 2019 na 62 milionů eur v roce 2021 a průměrná hodnota vyplaceného výkupného se zdvojnásobila ze 71 tisíc eur v roce 2019 na 150 tisíc eur v roce 2020. Odhaduje se, že globální výše škod způsobených ransomwarem v roce 2021 dosáhla 18 miliard eur, což je 57krát více než v roce 2015.

2. Malware – software, který spouští proces poškozující systém

Pod pojmen malware si lze představit viry, červy, trojské koně a spyware (špionážní software). Po celosvětovém poklesu malwaru souvisejícím s pandemií (v roce 2020 a na začátku roku 2021) se jeho používání koncem roku 2021 opět výrazně zvýšilo, protože se lidé začali vracet do kanceláří.

Nárůst malwaru se připisuje také cryptojackingu (tajnému využívání počítače oběti k nelegálnímu generování kryptoměn) a malwaru souvisejícímu s internetem věcí (malwaru zaměřenému na zařízení připojená k internetu, jako jsou routery nebo kamery).

Podle agentury Enisa bylo v prvních šesti měsících roku 2022 zaznamenáno více útoků na internet věcí než v předchozích čtyřech letech.

3. Hrozby sociálního inženýrství – zneužití lidské chyby k získání přístupu k informacím nebo službám

Jedná se o systém navádění a podvedení oběti k tomu, aby otevřela škodlivé dokumenty, soubory nebo e-maily či navštívila webové stránky, a tím poskytla útočníkům neoprávněný přístup k systémům nebo službám. Nejčastějším útokem tohoto druhu je phishing (prostřednictvím e-mailu); nebo smishing (prostřednictvím textových zpráv).

Podle průzkumu, který citovala Enisa, obsahuje téměř 60 % případů narušení bezpečnosti v Evropě, na Blízkém východě a v Africe prvek sociálního inženýrství.

Nejčastěji se útočníci využívající phishingu vydávali za organizace z finančního a technologického sektoru. Zločinci se také stále častěji zaměřují na kryptografické burzy a majitele kryptoměn.

4. Hrozby vůči datům – cílení na zdroje dat za účelem získání neoprávněného přístupu a jejich zveřejnění

V současné době žijeme v ekonomice založené na datech, která produkuje obrovské množství údajů, jež jsou nesmírně důležité mimo jiné pro podniky a umělou inteligenci, což z nich činí hlavní cíl kyberzločinců. Hrozby vůči datům lze klasifikovat především jako narušení dat (úmyslné útoky kyberzločince) a úniky dat (neúmyslné zveřejnění dat).

Nejčastější motivací pro tyto útoky jsou peníze. Pouze v 10 % případů je motivem špionáž.

Přečtěte si více o tom, jak chce EU podpořit sdílení dat a regulovat umělou inteligenci.

5. Hrozby v dostupnosti: odepření služby – útoky, které uživatelům brání v přístupu k datům nebo službám

Jedná se o jedny z nejkritičtějších hrozeb pro IT systémy. Jejich rozsah a složitost se zvyšuje. Běžnou formou útoku je například přetížení síťové infrastruktury a znepřístupnění systému.

Útoky související s odmítnutím služeb stále častěji zasahují mobilní sítě a připojená zařízení. Jsou hojně využívány v rusko-ukrajinské kybernetické válce. Terčem útoků se staly také webové stránky související s koronavirem, například web s informacemi pro získání očkování.

6. Hrozby v dostupnosti: internetové hrozby – hrozby v dostupnosti internetu

Patří k nim fyzické převzetí a zničení internetové infrastruktury, čehož jsme byli svědky na okupovaných ukrajinských územích po invazi, a také aktivní cenzura zpravodajských webových stránek nebo sociálních médií.

7. Dezinformace/misinformace – šíření zavádějících informací

Rostoucí využívání platforem sociálních a online médií vedlo k nárůstu kampaní šířících dezinformace (záměrně zfalšované informace) a misinformace (sdílení nesprávných údajů). Cílem je vyvolat strach a nejistotu.

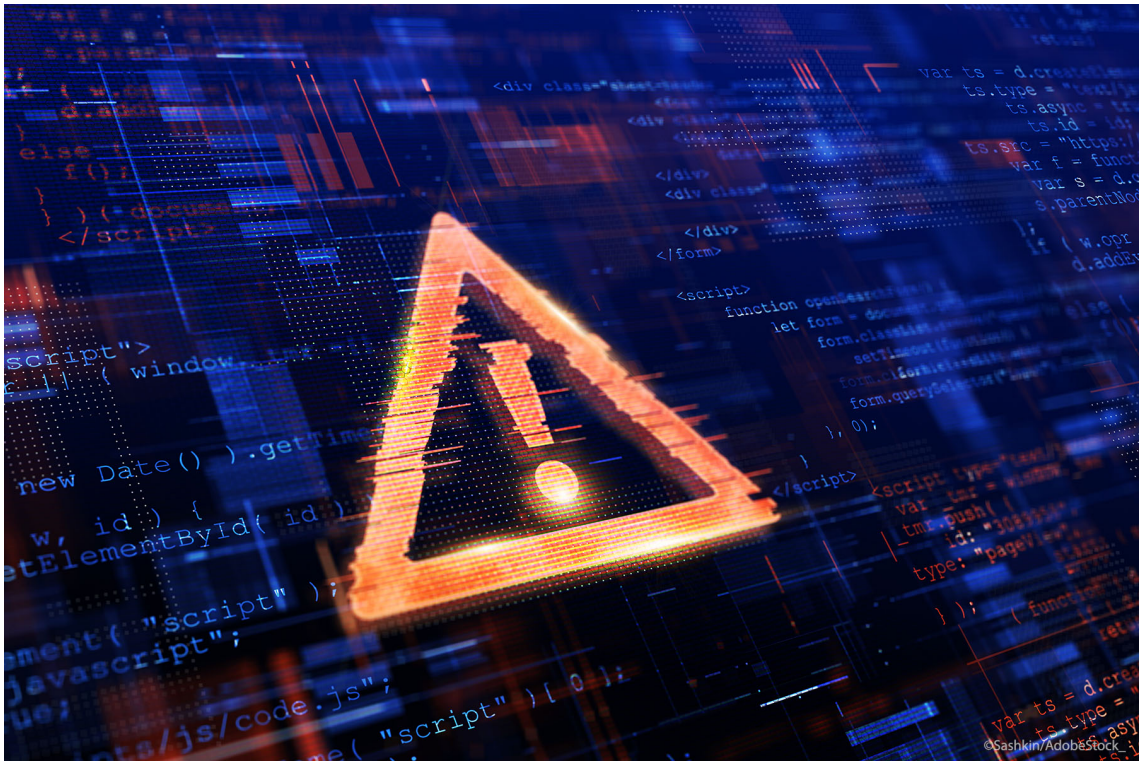
Rusko tuto technologii využilo k cílenému vnímání války.

Technologie deepfake znamená, že je nyní možné vytvářet falešné zvuky, videa nebo obrázky, které jsou téměř k nerozeznání od skutečných. Boti, kteří se vydávají za skutečné lidi, mohou narušovat online komunity tím, že je zaplavují falešnými komentáři.

Přečtěte si více o sankcích proti dezinformacím, které požaduje Parlament.

8. Útoky na dodavatelský řetězec – zaměřené na vztahy mezi organizacemi a dodavateli

Jedná se o kombinaci dvou útoků – na dodavatele a na zákazníka. Organizace jsou vůči takovým útokům stále zranitelnější, a to kvůli stále složitějším systémům a velkému množství dodavatelů, na které je obtížnější dohlížet.



Které hlavní hrozby se objevují v oblasti kybernetické bezpečnosti?

Hlavní sektory zasažené kybernetickými hrozbami

Kybernetické hrozby v Evropské unii ovlivňují celou řadu odvětví – mnoho z nich navíc platí za životně důležité sektory pro fungování společnosti. Mezi šest sektorů, které jsou postižené nejvíce, patří podle pozorování Agentury Evropské unie pro kybernetickou bezpečnost mezi červnem 2021 a červnem 2022:

1. veřejná správa/vládní instituce (24% podíl na celkovém počtu hlášených incidentů)
2. poskytovatelé digitálních služeb (13 %)
3. široká veřejnost (12,4 %)
4. služby (11,8 %)
5. finance/bankovnictví (8,6 %)
6. zdravotnictví/lékařství (7,2 %)

Přečtěte si více o tom, kolik nás kybernetické útoky stojí.

Dopad války na Ukrajině na kybernetické hrozby

Válka Ruska na Ukrajině ovlivnila kybernetickou sféru v mnoha ohledech. Kybernetické operace jsou využívány ruku v ruce s tradičními vojenskými akcemi. Podle agentury Enisa provádějí aktéři sponzorovaní ruským státem kybernetické operace proti subjektům a organizacím na Ukrajině a v zemích, které ji podporují.

Zvýšila se také aktivita hacktivistů (hackerů pro politicky nebo sociálně motivované účely), přičemž mnozí z nich provádějí útoky na podporu vybrané strany konfliktu.

Dezinformace byly nástrojem kybernetické války již před zahájením invaze a využívají je obě strany. Ruské dezinformace se zaměřily na hledání ospravedlnění pro invazi, zatímco Ukrajina dezinformace používá k motivaci vojáků. Využívány byly také deepfakes s ruskými a ukrajinskými představiteli, kteří vyjadřovali názory podporující druhou stranu konfliktu.

Kyberzločinci se snažili vylákat peníze od lidí, kteří chtěli podpořit Ukrajinu, prostřednictvím falešných charitativních organizací

Další informace

Enisa: Hrozby kybernetické bezpečnosti do roku 2030
Europol: Kybernetická kriminalita