ALISON

Europol a Agentúra EÚ pre kybernetickú bezpečnosť hlásia červené čísla

- Kybernetická kriminalita v štátoch EÚ
- Nárast bezpečnostných incidentov dôveryhodných služieb
- Slovenské korelácie

Trendy potvrdené v roku 2020

Okrem horúčav zhoršujú ťažkú situáciu „bezpečákov“ v lete výročné správy bezpečnostných organizácií a agentúr za predchádzajúci rok. Žiaľ, je to tak v roku 2020, keď Europol vydal *Hodnotenie hrozieb internetovej organizovanej trestnej činnosti za rok 2019*.

Odborníci na kybernetickú kriminalitu sa zhodli na dvoch hlavných fenoménoch novej dekády kybernetického sveta, ktoré sú príznačné pre Európsku úniu.

1. **Dáta.** Dáta a opäť dáta, finančné aj všeobecné údaje, sú stredobodom záujmu kybernetických zločincov.
2. **Kybernetická kriminalita sa neustále vyvíja a je čoraz odvážnejšia.** Zameriava sa na väčšie a najmä ziskovejšie ciele.

Existujú prípady, keď spoločnosti v roku 2019 zaplatili za šifrované súbory výkupné viac ako milión eur. Už tento rok tento trend potvrdil a výška výkupného je vždy predmetom dohadov a poloprávd aj v solídnych médiách. Bezpečnostné reporty sa však vykonávajú nad anonymizovanými dátami, aby nedošlo k strate reputácie, panike alebo ohrozeniu súvisiacich informačných systémov a služieb.

ALISON

Prečo je zraniteľnosť dôveryhodných služieb kritická

Lebo na nich funguje komerčný svet aj štát. Medzi dôveryhodné služby patrí online banking, daňové podanie online, elektronické zdravotníctvo, elektronické doručovanie, časové pečiatky, elektronické pečate a podpisy, ale aj procesy, akými sú elektronické obstarávanie alebo autentifikácia webových sídel a služby súvisiace s elektronickou identifikáciou podľa občianskeho preukazu.

Agentúra EÚ pre kybernetickú bezpečnosť (The European Union Agency for Cybersecurity – ENISA) hodnotí ich bezpečnosť v samostatnej Výročnej správe o incidentoch v oblasti dôveryhodných služieb za rok 2019. Bezpečnostným incidentom rozumie úmyselné využitie zraniteľnosti na spôsobenie škody alebo straty na aktívach informačného systému alebo neúmyselné vykonanie akcie, ktorej výsledkom je škoda na aktívach. Je to akékoľvek narušenie bezpečnosti informačných systémov a sietí subjektu a porušenie bezpečnostnej politiky a súvisiacich pravidiel.

Takže v roku 2019 počet bezpečnostných incidentov narástol o 80 percent. Už štvrtý rok po sebe bol najčastejšou príčinou výpadok hardvéru alebo chýbajúce softvérové záplaty a až 87 percent incidentov sa týkalo elektronických podpisov. **32 incidentov** malo významný vplyv na dôveryhodné služby EÚ. Odborníci však vyzývajú členské štáty a prevádzkovateľov dôveryhodných služieb, aby nahlasovali nielen incidenty, ale aj zraniteľnosť a útoky, čo môže prispieť k odhaleniu útočníkov a predchádzaniu škodám.

Pre zaujímavosť – ENISA začala používať v komunikácii zaujímavý infografický nástroj, slovenskú verziu nájdete na portáli Živе.sk.

Záverom – slovenské čísla

V medzinárodne uznávanom rebríčku National Cyber Security Index (NCSI) bolo Slovensko zaradené na siedme miesto. Správa o kybernetickej bezpečnosti SR za rok 2019 podľa SK CERT hovorí stručne:

- Najčastejšie riešeným typom incidentov bol botnet.
- Na vzostupe je najmä phishing.
- Počet detegovaných a nahlásených incidentov vzrástol v porovnaní s rokom 2018 o 14,3 percenta.
- Počet riešených incidentov vzrástol oproti roku 2018 o 60,2 percenta.
- Nežiaduci obsah bol najviac detegovaným a nahláseným typom incidentov.

https://www.nbu.gov.sk/wp-content/uploads/urad/Sprava-o-kybernetickej-bezpecnosti-SR-2019.pdf