ALISON

Až tretina členských štátov EÚ zažila v roku 2017 ohrozenie kritickej infraštruktúry v dôsledku kybernetického útoku.

Kyberútoky spôsobujú astronomické škody, naša pripravenosť je nedostatočná.

Ocitli sme sa v ére masívnych a bezprecedentných kyberútokov, ktoré spôsobujú astronomické škody súkromným spoločnostiam aj verejným inštitúciám.

Ako konštatuje Európska agentúra pre spoluprácu v oblasti presadzovania práva vo svojej výročnej štúdii za rok 2017: *Najznámejšie ransomwary roka ako WannaCry, Bad Rabbit, či NotPetya priniesli celosvetové straty v hodnote viac ako 5 miliárd dolárov. Destabilizáciu kritickej infraštruktúry kybernetickým útokom zaznamenala až tretina členských štátov EÚ. Útoky smerujú na kritické priemyselné odvetvia, zdravotníctvo, dopravu a telekomunikácie, pričom najčastejšie využívali zločinci malwary a DDoS útoky.*

Zároveň však prieskum o využívaní digitálnych technológií na Slovensku v roku 2018 potvrdil, že len necelých 40 percent našich podnikov má pokročilé bezpečnostné nástroje pre odhaľovanie vydieračských a škodlivých softvérov, či iných hrozieb.

Podľa prieskumu agentúry GfK väčšina slovenských firiem – až 93 percent – využíva štandardné preventívne systémy, napríklad antivírusy a firewally. Sofistikovanejšie bezpečnostné nástroje zamerané na nové hrozby, ako sú napr. Ransomvéry, nástroje pre šifrovanie dát a prediktívny monitoring počítačových sietí, využíva iba 38 percent spoločností. A len 20 percent firiem plánuje v najbližších 3 až 5 rokoch investovať do nadštandardných systémov pre IT bezpečnosť. Pritom útoky na firmy, obchodníkov, infraštruktúru a verejné služby majú obrovské dopady.

„Kybernetická hrozba je hrozbou pre biznis a tak ju treba aj chápať," povedal 12. septembra Martin Ciaran, výkonný riaditeľ britského Národného centra kybernetickej bezpečnosti (The National Cyber Security Centre) na konferencii Konfederácie britského priemyslu. „Existuje oveľa viac výziev pre kybernetickú bezpečnosť, než je iba Rusko, akokoľvek je aj táto hrozba vážna a trvalá."

Podľa Ciarana sa na Britániu môžu zamerať ruskí hackeri, no dáta zákazníkov môžu byť rovnako ohrozené inými krajinami, alebo zločincami. Útoky na internetových ale aj fyzických obchodníkov, viedli len v posledných mesiacoch ku krádežiam miliónov osobných údajov. Vzniknuté škody sú obrovské.

Náklady spojené s hackerskými útokmi zahŕňajú

- Reálne ukradnuté peniaze
- Náklady na nákup nových IT zariadení
- Pokuty za porušenie predpisov
- Straty spojené s výpadkom produkcie.

„Zarátať treba aj nepriame náklady od klesajúcej ceny akcií spoločnosti až po nárast nákladov na poistenie, nehovoriac o nefinančných stratách, ako je povedzme poškodenie dobrej povesti," dodáva Martin Ciaran. Medzi najviac poškodenými bola spoločnosť, ktorá bola vystavená útoku malwarom NotPetya.

Účet za vzniknuté škody obsahoval

- 4 000 nových serverov,
- 4 5000 nových počítačov,
- 2 500 nových aplikácií.

Celkové náklady v dôsledku útoku na firmu sa odhadovali na 150 až 250 miliónov libier(160 až 280 miliónov eur).

Až tretina členských štátov EÚ zažila ohrozenie kritickej infraštruktúry v dôsledku kybernetického útoku. V Nemecku bola napríklad masívnemu útoku ransomverom WannaCry vystavená železničná spoločnosť Deutsche Bahn a spoločnosť O2, v Španielsku Telefonica, v Maďarsku Telenor Hungary, v Rumunsku ministerstvo zahraničných vecí a v Spojenom kráľovstve Veľkej Británie a Severného Írska sa stal obeťou zdravotný systém NHS. Na Slovensku bola v súvislosti s WannaCry poškodená napríklad Fakultná nemocnica v Nitre.

Poslanci Európskeho parlamentu prijali ešte 13. júna 2018 uznesenia, ktorými žiadajú posilnenie kybernetickej obrany EÚ a užšiu spoluprácu EÚ s NATO. Inštitúcie aj firmy sa však musia spoliehať i na vlastné riešenia.

Svet sa ocitol v ére bezprecedentných a ničivých kyberútokov s obrovským rozsahom škôd. V porovnaní s ich výškou je účinná ochrana oveľa lacnejším a výhodnejším riešením.