HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
29. – 31. JANUÁRA 2021

Partneri špeciálnej prílohy:
ALISON
ALITER TECHNOLOGIES

Zlomový rok na Slovensku?

Ekonomika, vzdelávanie a komunikácia sa preklápajú do digitálneho modelu. Sme pripravení?

ILUSTRAČNÁ SNÍMKA: DREAMSTIME

HROZBY A ZRANITEĽNOSTI

Typy hrozieb a zraniteľností, ktorých neriešenie môže mať vážny dosah na systém kybernetickej bezpečnosti

- Neustály rozvoj nových techník a spôsobov útokov
- Zraniteľní používatelia
- Útoky zamerané na bežných používateľov s veľkými finančnými stratami
- Narastajúci počet technologických zraniteľností
- Nedostatok odborného personálu
- Laxný prístup k požiadavkám vyplývajúcim z legislatívy alebo zo štandardov
- Nízka úroveň bezpečnostného povedomia
- Zneužívanie nových technológií na vykonávanie útokov
- Slabá detekcia
- Pomalý výkon trestného práva v oblasti počítačovej kriminality s neistým výsledkom
- Útoky na kritickú infraštruktúru štátu, orgány štátu a obranné mechanizmy s mocensko-politickým pozadím
- Nelegálne aktivity presahujúce kybernetický priestor

Zdroj: Stratégia kybernetickej bezpečnosti SR 2021-2025

TÉMA

Kybernetický priestor nemá hranice. Nech sme kdekoľvek, týkajú sa nás všetky výhody aj hrozby tohto sveta.

Dostupnosť informácií, online komunikácia a množstvo zariadení pripojených na internet nám ukazujú fascinujúce možnosti kybernetického priestoru. Komerčný sektor, akademická sféra, moderné médiá a interpersonálna komunikácia nadobudli nečakané možnosti, zatiaľ čo klasické mocenské, štátne a geopolitické formácie prechádzajú ťažkou skúškou hodnôt a princípov. Digitalizácia nám viac ako čokoľvek iné pripomína, že sme súčasťou svetového spoločenstva. V januári slovenská vláda schválila Národnú stratégiu kybernetickej bezpečnosti na roky 2021 až 2025. Presahuje volebné obdobia aj rezorty, ovplyvňuje obchodné aj trestné právo, ochranu informačných aktív či sociálnych sietí a vývoj občianskej spoločnosti.

Kto by si mal prečítať stratégiu

Stratégia je východiskovým dokumentom, ktorý komplexne stanovuje prístup Slovenskej republiky k zaručeniu kybernetickej bezpečnosti. Národný bezpečnostný úrad musí pripraviť a do troch mesiacov oznámiť akčný plán Európskej komisii, tak ako nás zaväzuje smernica o bezpečnosti sietí a informačných systémov. Konkrétny plán čiastkových úloh a zdrojov by mal zaujímať ministerstvá, špecializované úrady, samosprávu a – teraz nasleduje všeobjímajúca formulácia – všetkých prevádzkovateľov základných služieb.

Základná služba je totiž komerčná alebo štátom poskytovaná služba podstatná pre chod spoločnosti. Viete o niečom, čo by nebolo pre chod spoločnosti podstatné? Tak to tam nepatrí, všetko ostatné áno. Takže energetika a všetci dodávatelia energií, doprava, elektronické komunikácie, bankovníctvo a finančné služby, pošta, priemysel, zdravotníctvo a, samozrejme, verejná správa.

Novelizácia kľúčového zákona

Už teraz je mimoriadne diskutovanou a očakávanou novelizácia zákona o kybernetickej bezpečnosti, ktorá by mala byť predložená vláde. Dôvodom novelizácie sú najmä skúsenosti z implementácie požiadaviek zákona od roku 2018, spätná väzba z trhu, prichádzajúce nové technológie a nutnosť úpravy v súlade s novými európskymi pravidlami.

V tomto procese vládny kabinet presadzuje posilnenie kompetencií NBÚ s dôrazom aj na ochranu všetkých sektorov kybernetického priestoru krajiny a zároveň apeluje aj na jednotnejšiu reguláciu v tejto oblasti. Piliermi novelizácie sú úpravy definície základných pojmov, postavenie manažéra kybernetickej bezpečnosti či certifikácie v tejto oblasti. Novela zavádza aj takzvaný inštitút blokovania.

K dosahu na podnikateľské prostredie a verejnú správu Peter Habara, hovorca Národného bezpečnostného úradu, uvádza: „Novelizácia zákona o kybernetickej bezpečnosti pozitívne ovplyvní rozpočet verejnej správy aj podnikateľské prostredie zvyšovaním efektivity.“ Národné centrum kybernetickej bezpečnosti SK CERT už teraz zdokonaľuje systém detekcie, reakcie a ochrany, predovšetkým rýchlosť a všestrannosť týchto procesov.

> Audit kybernetickej bezpečnosti je správnym krokom, ktorý vytvára tlak a prebúdza sebareflexiu manažérov.
>
> **Igor Straka,** manažér kybernetickej bezpečnosti

Ďalší rozmer kvality

Európsky parlament prijal v roku 2020 Nariadenie o kybernetickej bezpečnosti, populárne označované ako Cyber Act, a jeho priamym dôsledkom je úprava kompetencií európskych inštitúcií. V tejto súvislosti Európska agentúra pre kybernetickú bezpečnosť (ENISA) pripravuje návrh na certifikácie výrobkov, procesov a služieb kybernetickej bezpečnosti. Na Slovensku by túto certifikačnú schému mal prevziať Národný bezpečnostný úrad a následne budú môcť o akreditáciu na posudzovanie zhody požiadať aj iné slovenské certifikačné orgány.

Ak rozmýšľate, prečo stále opakujeme posudzovanie zhody a certifikácia, povedzme si, čo je ich prínosom pre občiansky život, riadenie štátu aj biznis. Digitalizácia a pripojiteľnosť sú mantrou súčasnosti. Na internet je pripojených čoraz viac zariadení, ale bezpečnosť a odolnosť proti kybernetickým hrozbám neboli v nich dostatočne zabudované v čase, keď boli navrhnuté.

„Certifikované výrobky a služby vo všeobecnosti garantujú kvalitu a zvyšujú dôveryhodnosť produktu v očiach zákazníka. A týka sa to nielen oblasti kybernetickej bezpečnosti, a nielen počítačov či mobilov,“ prízvukuje Ivan Makatura, generálny riaditeľ Kompetenčného a certifikačného centra kybernetickej bezpečnosti. Takže ak sa budete rozhodovať pri kúpe zubnej kefky s mobilnou aplikáciou, máte pri tej certifikovanej vyššiu záruku, že vám nikto nehekne osobné údaje. O energetike a zdravotníctve nehovoriac. Zariadenia v priemysle komunikujúce cez internet by si počtom a vplyvom zaslúžili vlastnú prílohu.

To, čo nás najviac páli

Vráťme sa však k prevádzkovateľom základných služieb. November 2021 je prvým termínom, keď musia prevádzkovatelia odovzdať na Národný bezpečnostný úrad záverečné správy auditu kybernetickej bezpečnosti. Takže už teraz by stovky miest, obcí, firiem a inštitúcií mali mať za sebou implementáciu bezpečnostných opatrení s cieľom chrániť dáta a informácie, ktoré spracúvajú. Účelom následného auditu je overiť plnenie povinností a posúdenie zhody prijatých bezpečnostných opatrení s požiadavkami zákona a inými súvisiacimi právnymi predpismi.

Rozdiely v pripravenosti sú obrovské. „Spoločnosti, ktoré sú riadené reguláciami v oblasti bezpečnosti, sú pripravené až ukážkovo. Zvyšok Slovenska sa zatiaľ hľadá,“ sumarizuje Igor Straka, manažér kybernetickej bezpečnosti TÜV SÜD Slovakia, s. r. o.

Podľa skúseností profesionálov z praxe prevádzkovatelia často neodlišujú fakt, že informačná a kybernetická bezpečnosť je niečím iným ako prevádzka infokomunikačných technológií. „Chýbajú ľudia, peniaze a skúsenosti. V každom prípade audit kybernetickej bezpečnosti je správny krok, ktorý vytvára tlak a prebúdza sebareflexiu manažérov,“ uzatvára Straka.

Nevídaná finančná kapitola

Nový program financovania Digitálna Európa na roky 2021 až 2027 podporuje digitalizáciu ekonomík a spoločností Únie. Predstavuje rozsiahlu implementáciu kľúčových digitálnych technológií, akými sú napríklad aplikácie umelej inteligencie a najmodernejšie nástroje kybernetickej bezpečnosti. Európskym podnikom, najmä malým a stredným, pomôže využívať obrovské príležitosti digitálnej transformácie, rozšíriť činnosti a získať konkurenčnú výhodu.

Program investícií Európskej únie na roky 2021 až 2027 s názvom Horizont Európa je deviaty rámcový program pre výskum a inovácie. Plynulo nadväže na Horizont 2020, ktorý bol najväčší a najvýznamnejší program financujúci projekty vedy, výskumu a inovácií v programovom období 2014 až 2020. Pre program Horizont Európa navrhuje Komisia prideliť astronomický rozpočet 100 miliárd eur, čo môže iniciovať vznik nového trhového segmentu a odvetvia.

Ak sa Slovensko nezačne pripravovať na tieto možnosti už dnes, nebudeme schopní spracovať projekty v krátkom čase a čerpať finančné stimuly. Príležitosť v kybernetickej bezpečnosti tak vzniká pre výskumné centrá, softvérové domy, tvorcov aplikácií či inovatívne technológie a výrobky úplne novej generácie.

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

CYBERARK · Flowmon A Kemp Company · MICRO FOCUS · SYNAPSA · paloalto NETWORKS