



Tlačová správa

16.03.2020

Bratislava 16. marca 2020 – Varovanie pre prevádzkovateľov základnej služby v sektore zdravotníctvo pred kybernetickými hrozbami a útokmi

Národné centrum kybernetickej bezpečnosti SK-CERT varuje prevádzkovateľov základných služieb v sektore zdravotníctvo (nemocnice, poskytovateľov zdravotnej starostlivosti, testovacie laboratória a ďalšie zdravotnícke zariadenia) ale aj všetky ostatné organizácie verejnej správy a prevádzkovateľov základnej služby v ostatných sektoroch pred možným zvýšením kybernetických hrozieb a útokov na ich systémy a siete.

Nakoľko zdravotnícke zariadenia v tejto dobe zažívajú nielen nápor pacientov, ale aj zavádzajú špeciálne bezpečnostné opatrenia z dôvodu vírusu COVID-19, môže u nich dôjsť k zníženej schopnosti detegovať a riešiť kybernetické bezpečnostné incidenty. SK-CERT pozoruje výrazne rastúci trend útokov, priživujúcich sa na tejto situácii.

13. marca 2020 ráno fakultná nemocnica v českom Brne – Bohunicích nahlásila kybernetický bezpečnostný incident¹. Aj napriek tomu, že momentálne nie je verejne známe, o aký incident išlo a ani aké škody spôsobil, ide o precedens, na ktorý musia byť jednotlivé zdravotnícke zariadenia pripravené. Správa spoločnosti CheckPoint² zároveň uvádza prípad jednej konkrétnej APT skupiny, ktorá sa v súčasnosti zameriava na organizácie verejného sektora s využitím údajných „informácií o rozšírení nových infekcií koronavírusom“ ako vstupného dokumentu, ktorým začína útok. SK-CERT tiež eviduje nárast objemu DDoS útokov v období medzi 17. februárom a 15. marcom 2020, vrátane útokov na weby so zdravotníckym obsahom na Slovensku.

Očakávame ransomvérové útoky alebo DoS útoky; šírenie malvéru, alebo phishingové kampane s využitím krádeže identity a falošných dokumentov pojednávajúcich o novom koronavíruse; nie sú však vylúčené aj iné typy útokov, zamerané na krádež citlivých údajov alebo deštrukciu systémov.

Národné centrum kybernetickej bezpečnosti SK-CERT preto odporúča všetkým zdravotníckym zariadeniam (ale aj všetkým ostatným organizáciám verejnej správy a prevádzkovateľom základnej služby):

- **Preverte** funkčnosť záloh a to, či dokážu spoľahlivo udržať záložnú kópiu dát v prípade útoku.
- **Monitorujte** svoje systémy a siete – zamerajte sa najmä na výpadky a neštandardné správanie.
- **Preskúšajte** svoje plány kontinuity činností a aktualizujte ich, ak ste zistili akékoľvek nedostatky.
- **Aktualizujte** si informácie o technológii, procesoch a IT personáli – či všetky technické nástroje fungujú a sú aktualizované, či sú zavedené procesy dobre nastavené a či je personál pripravený na detekciu a riešenie kybernetických bezpečnostných incidentov
- **Vykonajte** rýchle poučenie všetkých zamestnancov o bezpečnej práci za počítačom, najmä o tom, že nemajú otvárať prílohy v mailoch, klikať na linky a podobne a to ani vtedy, ak mail príde od známej resp. dôveryhodnej osoby.

¹ <https://nukib.cz/cs/informacni-servis/aktuality/1417-fn-v-brne-bohunicich-dnes-nahlasila-nukibu-kyberneticky-bezpecnostni-incident/>

² <https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/>

- **Zverejnite** pre zamestnancov kontaktnú e-mailovú adresu vášho manažéra kybernetickej bezpečnosti a poučte ich, aby na ňu nahlasovali akékoľvek podozrenie na kybernetický bezpečnostný incident, prijaté škodlivé súbory, pokus o získanie prístupov do systémov organizácie, k mailu a pod alebo pokus o získanie ľubovoľných osobných údajov.
- Bezodkladne **hláste** akýkoľvek kybernetický bezpečnostný incident Národnému centru kybernetickej bezpečnosti SK-CERT na Národnom bezpečnostnom úrade na adrese <https://www.sk-cert.sk> .
- V prípade, že potrebujete akúkoľvek pomoc v oblasti kybernetickej bezpečnosti, okamžite **kontaktujte** Národné centrum kybernetickej bezpečnosti SK-CERT.

Všetky varovania a odporúčania Národného centra kybernetickej bezpečnosti SK-CERT v súvislosti s oronavírusom a ochorením COVID-19 nájdete aj na stránke <https://www.korona.gov.sk/varovania-narodneho-centra-kybernetickej-bezpecnosti-sk-cert/> .

* * *

Národný bezpečnostný úrad (www.nbu.gov.sk) je ústredný orgán štátnej správy pre ochranu utajovaných skutočností, šifrovú službu, kybernetickú bezpečnosť a dôveryhodné služby. Úrad je národným kontaktným bodom pre kybernetickú bezpečnosť pre EÚ, NATO a OBSE.

Národné centrum kybernetickej bezpečnosti SK-CERT (www.sk-cert.sk), zriadené na Národnom bezpečnostnom úrade 1. septembra 2019 transformáciou Národnej jednotky SK-CERT, je akreditovaným členom organizácie Trusted Introducer a zároveň aj členom v organizácii FIRST (Forum of Incident Response Security Teams) s globálnym členstvom 490 tímov z 92 štátov. V rámci úradu zodpovedá za tému bezpečnosti 5G technológií.