HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

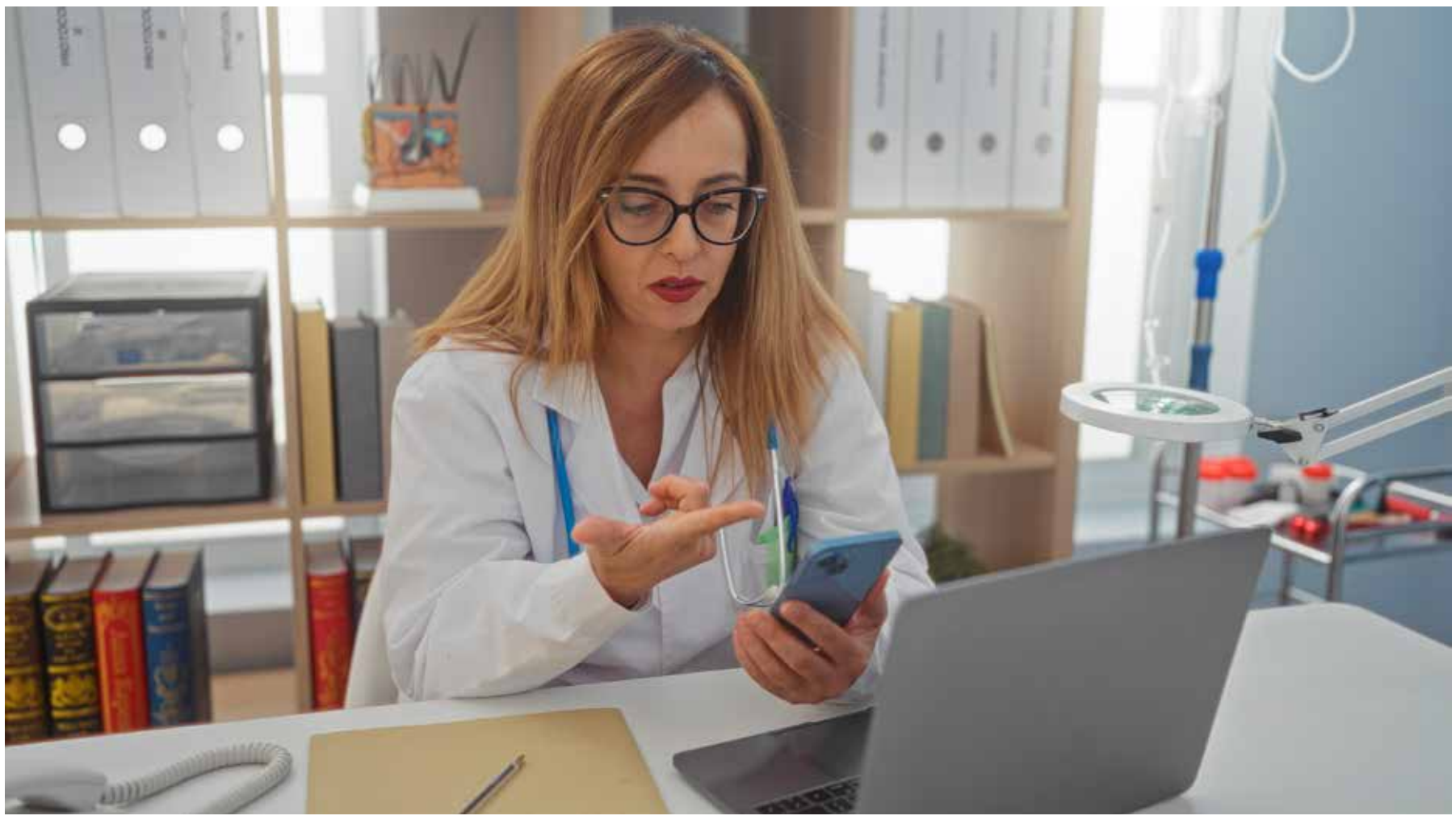
PIATOK – NEDEĽA
25. – 27. OKTÓBRA 2024

Odborná spolupráca
NBÚ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Cítite sa bezpečne v zdravotníctve?

TÉMA

Ani špičkové technológie nás neobránia, ak nie sú vzdelaní a opatrní používatelia a zodpovední štatutári. Lebo kybercunami sa blíži. Fakty a skúsenosti sú neľútostné.



Zdravotníctvo je lákavým cieľom útokov. Je zlatou baňou citlivých údajov a má množstvo nechránených a zraniteľných miest. FOTO: DREAMSTIME

Kybernetická kriminalita svojím finančným objemom prekonáva aj ropný priemysel. Aj zisky z kávy sú iba zanedbateľné v porovnaní so ziskami kybernetických zločineckých gangov.

Ohromujúce čísla

Podľa analytického tímu Cybersecurity Ventures boli globálne škody spôsobené kyberkriminalitou v minulom roku na úrovni osem až desať biliónov USD. Zahŕňajú priame finančné straty, straty z narušenia biznisu, náklady na obnovenie systémov a reputačné škody spôsobené ransomvérom, phishingom a ďalšími kybernetickými útokmi.

Trojnásobná akcelerácia

Globálne sa odhaduje, že približne 60 percent finančných strát kriminálneho pôvodu spôsobili práve kybernetické útoky. Kyberkriminalita sa tak stáva dominantným typom trestnej činnosti. Zahŕňa podvody, neoprávnené prieniky do systémov, zmeny v dátach a krádeže identity. Od roku 2015 sa objem škôd trojnásobne zvýšil. Vzhľadom na tento trend sa očakáva, že podiel kyberkriminality na celkovej kriminalite bude naďalej rásť.

Slovensko nie je výnimka

Hoci sa počítačová kriminalita často spája s veľkými korporáciami, postihuje firmy bez rozdielu veľkosti aj jednotlivcov. Či už je útočník individuálny, alebo to je organizovaná skupina, využívajú útoky prostredníctvom sociálneho inžinierstva.

„Najčastejšie metódy kybernetického útoku sú phishing, smishing alebo vishing," upozorňuje skúsený súdny znalec Jaroslav Oster. Čiže podvodné maily, telefonáty a správy, alebo ich kombinácia. Na konci väčšiny scenárov je snaha útočníkov získať citlivé informácie použiteľné pre ďalšiu manipuláciu, prístup k bankovým účtom či vybudovať falošnú dôveru vedúcu k zaslaniu finančných prostriedkov.

Zločin na prenájom

Model „phishing ako služba" sprístupňuje phishing aj menej skúseným zločincom. Za malý poplatok môžu spustiť škodlivé kampane bez rozsiahlych technickými znalostí. Pre organizácie to znamená zvýšené riziko, že ich zamestnanci budú čeliť čoraz viac a častejšie sofistikovaným phishingovým pokusom.

Jaroslav Oster upozorňuje aj na fakt, že vek páchateľov v tejto oblasti klesá a takzvané scripting kids majú 13-14 rokov. A ak by sme pokračovali tým, ako umelá inteligencia uľahčuje programovanie a písanie, prepadneme sa do veľmi chmúrnych úvah.

Kde to najviac bolí

Čo sa týka cieľov, najväčší počet útokov na Slovensko smeruje dlhodobo na seniorné skupiny. Štatistika je o to hrozivejšia, že táto zraniteľná a neskúsená veková skupina má významné zastúpenie medzi lekármi a učiteľmi.

V zdravotníctve je až 95 percent kybernetických útokov spôsobených ľudskou chybou. „Aj keď nemocnice investujú veľa zdrojov do technickej ochrany, najzraniteľnejší článok ostáva človek," varuje Dominik Procházka, riaditeľ odboru bezpečnosti AGEL SK.

Kde to bolí dvojnásobne

„Zdravotnícke zariadenia majú prepracovaný a slabo vyškolený personál v oblasti kybernetickej bezpečnosti, ktorý je najčastejším adresátom kybernetických útokov," hovorí Marian Daníšek, manažér IT infraštruktúry Penta Hospitals.

EURÓPSKY MESIAC KYBERNETICKEJ BEZPEČNOSTI

Tento fakt sa týka nielen Slovenska, ale celého sveta, a kybernetický zločin to bezohľadne využíva. My pacienti sa stávame rukojemníkmi krehkej bezpečnosti v zdravotníctve.

„Roky sa čaká na koncepciu vzdelávania v kybernetickej bezpečnosti v zdravotníctve. Aktivity jednotlivcov a úzkych skupín z radov rôznych združení a súkromného sektora suplujú štát. Vzdelávacie aktivity v jednej sieti nepotiahnu celý systém, lebo ten je navzájom previazaný," dopĺňa svojho kolegu manažér kybernetickej bezpečnosti Peter Dufek.

Ešte sme neskončili

Jozef Zoričák, vedúci oddelenia informatiky Národného ústavu pľúcnych chorôb, poukazuje na kritický rozdiel, kde nemocničné siete majú silné a profesionálne kyberbezpečnostné tímy. Zároveň dokážu zdieľať náklady na technológie aj na ľudí. Menšie zariadenia len veľmi ťažko so svojím rozpočtom siahajú na tento štandard.

Zdravotníctvo je totiž z hľadiska bezpečnosti náročná oblasť. IT oddelenia spravujú rôznorodé koncové body a obrovské množstvo dát a ich klientmi sú zamestnanci aj pacienti. Jedno však Jozef Zoričák zvlášť zdôrazňuje: „Vek používateľov je kritický bezpečnostný prvok pri pacientoch aj zamestnancoch."

Osvietený manažment

Pre riaditeľov zdravotníckych zariadení, tak ako pre všetkých štatutárov, zo zákona vyplýva, že zodpovedajú za kyberbezpečnosť.

A ako sa prejavuje osvietený manažment? „Nepodceňuje školenie zamestnancov na všetkých úrovniach. Má odvahu podpísať nepopulárne opatrenia v kybernetickej bezpečnosti, ako sú zložité heslá a viacfaktorová autentifikácia," okamžite odpovedá Jozef Zoričák.

Zároveň s platnosťou novelizácie kyberbezpečnostného zákona bude mať osvietený manažment menej práce. Aby splnili prísne požiadavky, organizácie budú musieť investovať do školenia zamestnancov a často aj do nových technológií.

Dvojnásobný výkon

Nič nové, že IT oddelenia v nemocniciach sú poddimenzované. IT tímy v štátnych nemocniciach však majú často iba polovičné obsadenie, prípadne správca je manažérom širokej a rôznorodej skupiny dodávateľov. Za ostatné roky im pribudla aj kyberbezpečnosť podľa zákona. A žiadni noví bezpečáci na obzore.

Zamestnanci aj pacienti očakávajú používateľsky príjemné prostredie, takže správcovia sietí hľadajú multifunkčné riešenia. Uplatnenie tu nachádzajú inteligentné autentifikátory, ktoré majú bezheslové prihlásenie a automatické odhlásenie cez biometrické overovanie a umožňujú prístup k zariadeniam, aplikáciám a fyzickým priestorom. A žiadne zdržovanie a jeden bezpečnostný report.

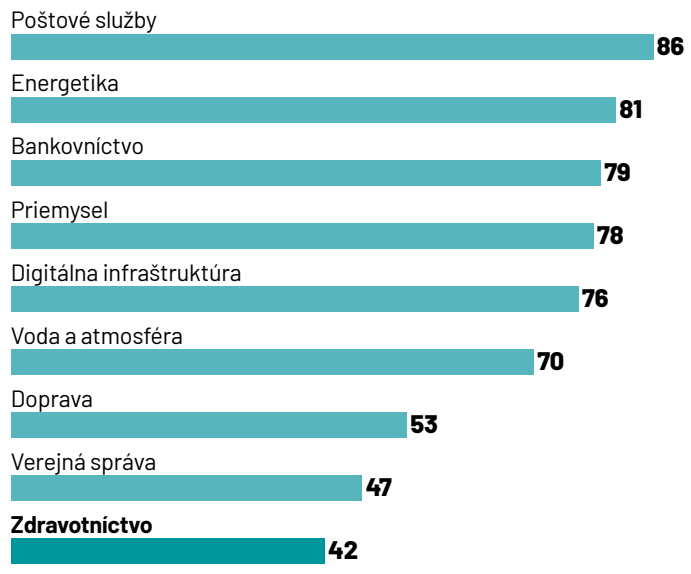
Podpora od dodávateľov

Európska smernica NIS prináša do zákona aj priamu povinnosť pre organizácie znižovať riziká a zvyšovať celkovú kyberodolnosť. „Sústreďujeme sa na produkty, ktoré majú plne integrované hodnotenie zraniteľnosti a automatizovanú správu opráv," potvrdzuje Július Selecký zo spoločnosti Eset.

Producenti bezpečnostného hardvéru a softvéru kladú dôraz na automatizáciu a jednoduchosť použitia, čím reflektujú legislatívne požiadavky aj nedostatok profesionálov. V každom prípade, odpočítavanie do príchodu nového zákona v januári 2025 sa už začalo.

Stav súladu kyberbezpečnosti podľa odvetví

auditované subjekty podľa zákona (percentuálny podiel v odvetví)



Zdroj: Správa o kyberbezpečnosti v Slovenskej republike v roku 2023, NBU, spracovanie do grafu KCCKB.