28.6.2023 08:00 | Bezpečnosť

EXKLUZÍVNE Štát dal preskúmať kyberbezpečnosť nemocníc. Výsledky: Každá jedna mala bota, pätina ransomvér

Zdroj: istock

Filip Hanker

Lukáš Kosno

Analýza odhalila znepokojujúce zistenia. Podľa NBÚ je pozitívnou správou aspoň to, že sa zdravotníctvo zo suverénne najhoršieho sektora posunulo aspoň trochu dopredu.

Minister zdravotníctva Michal Palkovič v nedávnom rozhovore pre Živé.sk **otvorene povedal**, že si z hľadiska kybernetickej bezpečnosti uvedomujú zraniteľnosť celého systému a je pred nimi veľa práce. Avizoval, že riešenie si vyžaduje metodiku či centralizáciu agendy.

V posledných mesiacoch začal štát mapovať situáciu okolo IT prostredí v medicínskych

zariadeniach, ktoré spadajú pod rezort zdravotníctva. Projekt realizuje spoločnosť Kreston Slovakia Technology ako subdodávateľ firmy Stengl. Tá do projektu poskytla vybraných expertov. Ide o súčasť väčšieho projektu „Analýza rizík a nedostatkov v správe informačných technológií verejnej správy v MZ SR“.

Prvé zistenia auditu firma Kreston Slovakia stručne prezentovala na konferencii pre zástupcov zo zdravotníckeho sektora, na ktorom nechýbalo ani Živé.sk. Niektoré ďalšie závery sme sa dozvedeli, keď sme sa rozprávali so spolumajiteľom spoločnosti a jej technickým riaditeľom Andrejom Aleksievom a väčšinovým majiteľom Júliusom Činčalom.

V článku sa dozviete:

- Ako je na tom kyberbezpečnosť najdôležitejších slovenských štátnych nemocníc.
- Aké sú najvýznamnejšie slabiny z pohľadu IT bezpečnosti.
- Nakoľko je problémom ransomvér či boty, čakajúce na príkazy útočníka.
- Na aké aspekty sa analýza rizík a nedostatkov zameriavala.
- Čo má byť cieľom celej analýzy.
- Čo treba vyriešiť, aby malo ministerstvo z dát väčší úžitok.
- Prečo monitoring bezpečnosti neprebiehal u prevádzkovateľa eZdravia a ako je na tom s bezpečnosťou podľa vlastného kyberauditu

108 otázok a skúška, či zaplátali známe chyby

Štát analyzuje IT bezpečnosť konkrétne v štátnych nemocniciach, regionálnych úradoch verejného zdravotníctva, ale i ďalších organizáciách, ktoré má rezort vnútra „pod sebou“ – kúpeľoch, liečebniach pre závislých či ubytovniach. Celkovo je ich 108. Výsledky posudzovania majú poslúžiť na nastavenie stratégie a priorít pre riešenie kybernetickej bezpečnosti v sektore štátneho zdravotníctva.

Čítajte aj
Minister zdravotníctva: Ako vidím budúcnosť eZdravia a aké IT vylepšenia prídu...

Cieľom je zistiť situáciu v minimálne 90 percentách organizácií. Analýzy sú zatiaľ ukončené vo viac ako troch štvrtinách z nich. Niektoré sa odmietli zapojiť, inde vraj ešte sondáž prebieha a skončí v priebehu leta, zrejme v júli.

Aleksiev zdôvodnil, že v niektorých prípadoch odmietali externé posudzovanie outsourcovaní manažéri kyberbezpečnosti. Popisuje, že to vnímali ako hodnotenie ich práce. Niekedy sa ich napokon podarilo presvedčiť. Medzi analyzovanými subjektami chýba aj Národné centrum zdravotníckych informácií (NCZI) – *dôvody, prečo, prinášame v závere článku.*

Ako sa analýza realizuje: Najskôr sa zbierajú odpovede na 100 otázok, ktoré sa zameriavajú na uplatňovanie konceptu nulovej dôvery (zero trust), využívanie automatizovaných bezpečnostných nástrojov a bezpečnosť týkajúcu sa správania koncového používateľa. Následne bezpečnostní experti umiestňujú do preverovanej organizácie hardvérové a softvérové sondy. Napríklad na oskenovanie, či je systém napadnuteľný cez známe bezpečnostné chyby, ktoré nie sú dosiaľ zaplátané. Jednotlivým aspektom boli pridelené rôzne váhy – niektorým bola kladená vyššia a iným nižšia dôležitosť.

Audit však nezahŕňal penetračné testy – teda pokusy etických hackerov nájsť slabé miesta a preniknúť do infraštruktúry.

Čítajte aj
Akým kyberhrozbám čelila SR v roku 2022? NBÚ spravilo sumár, za riadenie...

Ransomvér i príkazy na diaľku

Ako sú teda na tom v kyberbezpečnosti nemocnice? Aleksiev pre Živé.sk uviedol, že spomedzi všetkých typov posudzovaných organizácií sú práve nemocnice na tom najhoršie. Paradoxom je, že najhorší stav je vraj v takých, ktoré sú po medicínskej stránke „výkladnou skriňou slovenského zdravotníctva“.

Aleksieva z Kreston Technology Slovakia sme na stretnutí požiadali, aby aspoň všeobecne zosumarizoval, ako sú na tom nemocnice s bezpečnosťou. Dozvedeli sme sa, že:

- každá nemocnica zaznamenala kyberbezpečnostný incident – to ale nie je prekvapivé, keďže nejde len o úspešný pokus, ale hocijaký detegovaný pokus o útok,
- každá nemocnica mala vo svojej infraštruktúre bota schopného vykonávať príkazy na diaľku, priemerne malo ísť o každý druhý počítač
- v každej piatej nemocnici sa našiel ransomvér, aj keď sa nie vždy musel prejaviť škodlivou činnosťou.

„Sú v katastrofálnom stave. Peniaze idú na medicínske prístroje či personál, ale nie na kyberbezpečnosť," opisuje situáciu v slovenských nemocniciach Aleksiev pre Živé.sk.

Riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT Rastislav Janota našiel pri téme bezpečnosti v zdravotníckych zariadeniach i pozitíva. Nevychádzajú však z aktuálnych analýz v nich, ale z auditných správ kybernetickej bezpečnosti. Tie sú pre určitú skupinu inštitúcií povinné a odovzdávajú sa Národnému bezpečnostnému úradu (NBÚ). SK-CERT je jedným z jeho útvarov a zistenia z kyberauditov **pravidelne sumarizuje** vo výročných správach.

Čítajte aj
Štát varuje pred hackerskou skupinou, zameriava sa najmä na školy. Odstaví...

„V rámci zdravotníctva vidíme zmenu – zo suverénne najhoršieho sektora sa prepracovalo, už najhorším nie je. Je tretie od konca. V tých ďalších dvoch sektoroch nevidím svetlo na konci tunela, v jednom vôbec, v druhom kus od kusu," konštatoval Janota.

Správa o kybernetickej bezpečnosti v SR za rok 2022 konkrétne **na základe 61 auditných správ hovorila**, že miera súladu prijatých bezpečnostných opatrení s požiadavkami zákona o kybernetickej bezpečnosti a súvisiacich predpisov bola 42 percent, čiastočný súlad bol v 15 percentách a nesúlad sa týkal 35 percent.

Starý hardvér, používatelia nevedia základy

Detaily o výsledkoch bezpečnostných analýz firma Kreston Slovakia nezverejňuje, keďže má s nemocnicami podpísané dohody o mlčanlivosti. „Majú takú silnú NDA (zmluvu o mlčanlivosti a ochrane dôverných informácií, pozn. red.), že sa s niektorými detailmi nemôžeme podeliť ani s ministerstvom," vraví Aleksiev. Výstupy sú teda anonymizované.

Tému súhlasov nemocníc so šírením dát aktuálne firma podľa svojich slov rieši aj s rezortom zdravotníctva. Napríklad, aby mohol vzniknúť rebríček nemocníc podľa miery ochrany. Okrem toho štát potrebuje údaje aj preto, aby mohol vypracovať spomínanú stratégiu. Zároveň má ministerstvo schvaľovať každý jeden IT projekt a bezpečnostný projekt.

Čítajte aj
Na Wi-Fi sa počas dovolenky nepripájajte, môžete prísť o heslá aj číslo karty...

Aleksiev však aspoň vo všeobecnosti uviedol, že investičný dlh v kybernetickej bezpečnosti v zdravotníctve je obrovský a extrémne ďalej rastie. Za problém označil „prehistorickú“ infraštruktúru.

Na žalostný stav hardvéru aj pri samotnom systéme eZdravie, do ktorého doktori zapisujú textové záznamy z vyšetrení a kam chodia lekárske predpisy, upozornili v našich rozhovoroch **šéf NCZI Peter Lukáč** či **samotný minister zdravotníctva Michal Palkovič**.

Ďalšie slabé miesto vidí Aleksiev v nedostatku špecialistov. „Množstvo nemocníc ich nemá. ITčkár nie je bezpečák. Sú to dve odlišné roly, je to úplne iný pohlaď na problematiku,“ poukázal. Dodal, že nemocnice navyše ani nevedia, v akom stave majú svoju infraštruktúru, na čo podľa jeho slov prišli porovnaním dotazníka a skúmaním reálneho stavu.

Nedostatok vidí aj v malej spolupráci medzi zariadeniami, keďže podľa neho neexistuje platforma pre zdieľanie informácií a skúseností.

Z používateľského pohľadu spočívajú nedostatky v neznalosti základov kyberbezpečnosti, takže sa zamestnanci ľahko nachytajú na podvodné e-maily či phishing v rôznych iných firmách. Okrem toho skoro žiadna nemocnica nemá zavedený manažment správy hesiel, uviedol Aleksiev.

Čítajte aj
Slovákov varujú pred hackermi, ktorých podporuje Severná Kórea. Majú jasný cieľ...

Útoky na nemocnice rastú, potvrdili sondy

Riziko napadnutia zdravotníckych inštitúcií narastá, odhalil monitorovací projekt. Uplynulé dva mesiace sondy firmy zaznamenali o 20 až 30 percent viac útokov oproti tým, ktoré boli v nemocniciach nasadené na prelome rokov.

Za pozornosť tiež stojí, že Aleksiev pre ministerstvo zdravotníctva aj priamo pracoval – do apríla, ako externý poradca. Skúmanie bezpečnosti zdravotníckeho sektora pritom štát zazmluvnil s firmou Stengl už 19. októbra 2022 a oznámenie o doplnení subdodávateľa – Kreston Slovakia Technology – prišlo 1. novembra 2022. Na projekte sa ešte v minulom roku začalo aj pracovať. Aleksiev je spolumajiteľom realizujúcej firmy Kreston Slovakia Technology od konca januára tohto roka.

Aktualizácia o 16:55: Podľa Aleksieva v tomto článku nesúhlasí pozícia, na ktorej pre rezort pracoval, ani časové obdobie. Detaily svojho pôsobenia na ministerstve nám ale nespresnil.

Hodnota celej zmluvy so Stengl je skoro 1,5 milióna eur s DPH. Kreston Slovakia je subdodávateľom, ale s deklarovanou subdodávkou nad polovicu hodnoty zákazky.

NCZI sa nezapojí. V čom vidí problém

Národné centrum zdravotníckych informácií (NCZI) prevádzkujúce napríklad celé elektronické zdravotníctvo eZdravie (eHealth) experti neskúmali. Aleksiev pre Živé.sk uviedol, že sa do projektu nezapojilo.

Šéf NCZI Peter Lukáč to pre Živé.sk zdôvodňuje tým, že neexistovala záruka dodržiavania primeraných bezpečnostných opatrení treťou stranou podľa zákona o kybernetickej bezpečnosti pri prístupe do ich infraštruktúry. „Nemôžeme reálne poskytnúť súčinnosť pri činnostiach, o ktoré nás ministerstvo zdravotníctva žiadalo v súvislosti s aktivitami spoločností Stengl a Kreston," reagoval.

Žiadosť ministerstva má pochádzať z konca mája. NCZI pre Živé.sk potvrdilo, že sa do projektu definitívne nezapojí. Bezpečnosť si podľa svojich slov stráži cez vlastné bezpečnostné operačné centrum (SOC – monitoruje prevádzku v infraštruktúre a hľadá potenciálne problémy).

Minister Palkovič aspoň nedávno pre Živé.sk prezradil, že predbežné výsledky auditu kyberbezpečnosti NCZI sú o tridsať percent lepšie ako tie z predchádzajúceho auditu v

roku 2021 a percento zhody s požiadavkami na kybernetickú bezpečnosť predstavovalo 41 percent. Podľa NCZI ale nešlo o finálne percento. Organizácia predpokladá, že v schválenej správe si oproti nemu nakoniec ešte o štvrtinu „polepší“. Správa by mala byť hotová v horizonte dní.

Viac článkov ku kyberbezpečnosti nájdete v tejto rubrike >>>

28.6.2023 08:00 | Autori: **Filip Hanker, Lukáš Kosno** | Zdroj: Zive.sk | Nahlásiť chybu

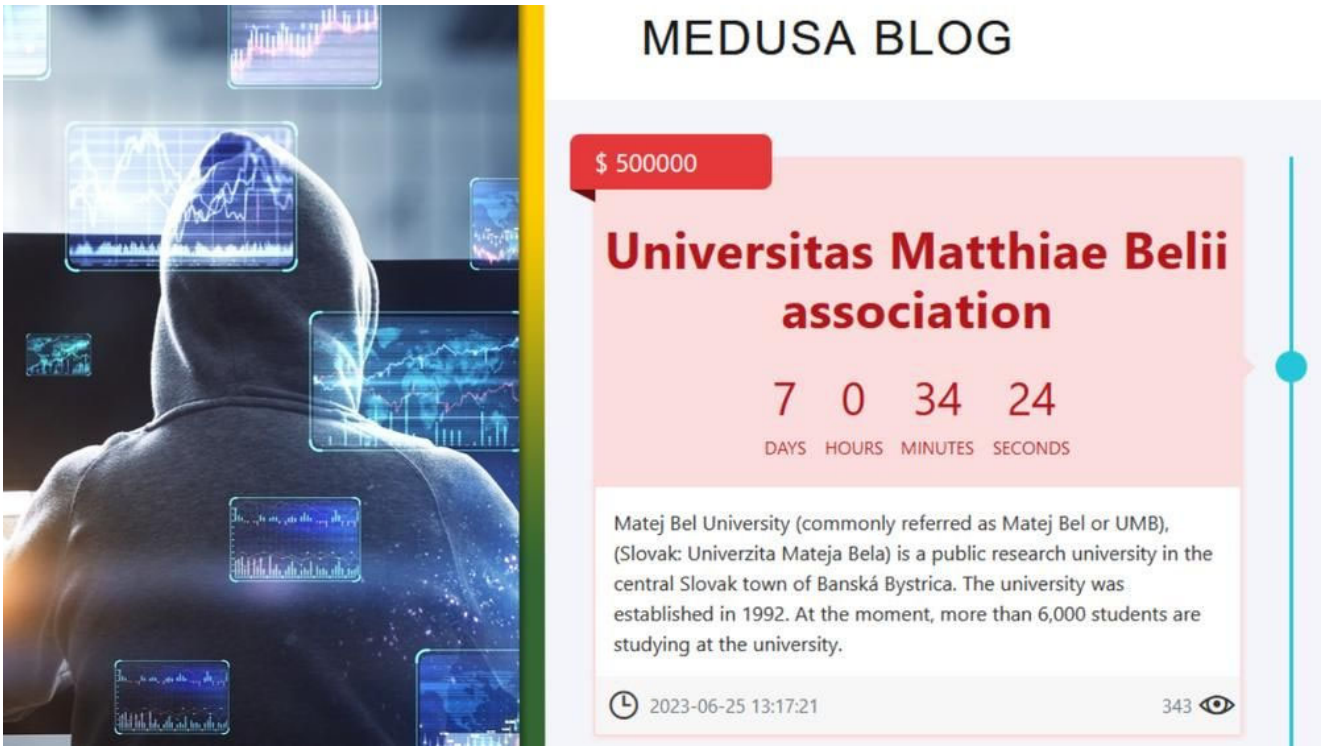
SÚVISIACE ČLÁNKY

Z čoho sú nadšení a sklamaní: Kyberbezpečnostní špecialisti hodnotia prvý polrok na Slovensku

Najväčšia databáza softvéru pre JavaScript má bezpečnostnú chybu. Odborníci radia, na čo dávať pozor

Ktorým firmám najviac hrozí kyberútok a kedy si riziko uvedomia? Pozrite si zistenia zo slovenského prieskumu

NAJČÍTANEJŠIE



1. **Hackeri vydierajú Univerzitu Mateja Bela: Za nezverejnenie dát si pýtajú obrovskú sumu**
2. Na Slovensku budú Telekom a O2 zdieľať siete. Sú pred podpisom zmluvy, vieme viac
3. Inštalovali ste si fotovoltiku do zásuvky bez povolenia? Poisťovňa vás môže hodiť cez palubu
4. Na Slovensku chce spustiť satelitnú a internetovú TV ďalšia spoločnosť
5. YouTube zaviedol automatické dabovanie videí. Táto funkcia je už spustená a je ohromujúca

6. Dohoda na poslednú chvíľu: Markíza v ponuke UPC neskončí. Pridá nový kanál
7. Antik opäť zvýši cenu TV služby. Za Markízu a JOJ si bude pýtať až 7 eur
8. Spotrebu energií znížime aj bez odopierania si komfortu. Takéto riešenia navrhuje vedec (rozhovor)
9. Telekom dnes výrazne zhoršil svoju predplatenú kartu. Čo všetko sa zmenilo?
10. Štát dal preskúmať kyberbezpečnosť nemocníc. Výsledky: Každá jedna mala bota, pätina ransomvér

TIP NA VIDEO

PREHRAŤ VIDEO

Počítač Atari Falcon bol „posledný svojho druhu“. Týmto najviac zaujal