Vyčkávanie by nás zničilo

Ani v zdravotníctve sa kyberbezpečnosť nezaobíde bez spolupráce - Dominik Procházka AGEL, Július Selecký ESET, Jozef Zoričák organizátor kongresu, Tomáš Hettych Kompetenčné a certifikačné centrum kybernetickej bezpečnosti, Jaroslav Ďurovka Národné centrum kybernetickej bezpečnosti.

Podujatie sprevádzajú prezentácie, diskusie, praktické ukážky a výmena skúseností na všetkých úrovniach. FOTO: LUBOS PITONAK

REPORTÁŽ

Na Kongrese Nemocničné informačné systémy sa stretávajú informatici, manažéri kybernetickej bezpečnosti zo zdravotníckych zariadení a v neposlednom rade aj riaditelia a lekári.

Digitalizácia zdravotníctva priamo ovplyvňuje kvalitu zdravotnej starostlivosti, efektívnosť zdravotníckeho systému a bezpečnosť pacientov. Vzdelávanie a prehľad trendov sú preto nevyhnutnou podmienkou prevádzkovania nemocničných informačných systémov. IT profesionáli si uvedomujú, že nemôžu čakať iba na pokyny zhora, a vzdelávanie organizujú vlastnými silami.

„V slovenskom zdravotníctve hľadáme riešenia a možnosti financovania aj v oblasti informatiky a pracujeme na tom, aby sme rozširovali komunikáciu a spoluprácu zdravotníckych zariadení," vysvetľuje Jozef Zoričák, organizátor kongresu.

Ak sa prvé ročníky Kongresu NIS zamerali na výber a prevádzkovanie nemocničných informačných systémov, neskôr sa podujatie zameralo na prevádzku a aktuálne témy informatizácie zdravotníctva. S nariadením o ochrane osobných údajov a zákonom o kybernetickej bezpečnosti sa stala nosnou témou aj kybernetická a informačná bezpečnosť.

„Ochrana zdravotníckych dát je nevyhnutná pre zachovanie dôvery medzi pacientmi a poskytovateľmi zdravotnej starostlivosti, zároveň je investíciou do budúcnosti," uviedol riaditeľ Národného centra zdravotníckych informácií Pavol Vršanský.

Úlohou pre všetkých zamestnancov v zdravotníctve a aj pre sám kongres je nestratiť schopnosť reagovať na aktuálne témy a trendy v zdravotníckej informatike a kybernetickej bezpečnosti.

Keďže elektronické zdravotné záznamy umožňujú lepší prístup k informáciám o pacientoch v reálnom čase, lekári môžu lepšie diagnostikovať a rozhodovať. Automatizácia a digitalizácia procesov znižujú administratívne časy a umožňujú rýchlejší prístup k liečbe. Digitalizácia podporuje aj komunikáciu medzi zariadeniami a odborníkmi či s pacientmi a využívanie telemedicíny. Úlohou informatizácie je efektívne riadenie zdravotných systémov, udržateľnosť a zníženie nákladov a s tým všetkým neoddeliteľne spojená kybernetická bezpečnosť.

To, že témy reflektujú potreby praxe a informatici v zdravotníctve vyžadujú čoraz viac vzdelávania, potvrdzuje aj každoročný rast počtu účastníkov. V roku 2024 bolo na Kongrese NIS registrovaných viac ako dvestodvadsať účastníkov a dvadsať odborných partnerov.

Kongres NIS organizuje od roku 1996 Národný ústav tuberkulózy, pľúcnych chorôb a hrudníkovej chirurgie Vyšné Hágy, v súčasnosti v spolupráci s Národným ústavom detskej tuberkulózy a respiračných chorôb Dolný Smokovec, spoločnosťou Info consult a s odbornou záštitou Národného centra zdravotníckych informácií.

PORADŇA

Desatoro kybernetickej bezpečnosti. Aj pre vás

Malé, stredné, veľké firmy, živnostníci, školy, nemocnice, inštitúcie aj domácnosti. Ak ide o kybernetickú bezpečnosť, manuál je pozoruhodne rovnaký.

Aktualizácie softvéru
Neodkladajte reštarty na dokončenie aktualizácií.

Pri kritických systémoch vopred otestujte aktualizácie.

Prístup pre neoverené osoby
Útočníci sa môžu vydávať za technikov alebo iných pracovníkov, aby získali prístup do systémov.

Vždy overte identitu osoby a skontrolujte, či je návšteva vopred nahlásená a schválená objednávateľom výkonu.

Opatrné zdieľanie informácií na sociálnych sieťach
Útočníci zbierajú informácie z príspevkov na sociálnych sieťach.

Informácie slúžia na generovanie wordlistov na prelomenie hesiel alebo na cielené kampane.

Bezpečná správa pracovného prostredia
Zamykajte obrazovky vždy pri odchode od počítačov.

Nie, už ozaj nelepte heslá na monitory. Aj keď je to stále realitou.

Phishing
Phishingové útoky sú lacné, efektívne a ľahko sa šíria.

Podvodné e-maily často obsahujú podozrivé odkazy, naliehavé požiadavky alebo neobvykle formulované správy.

Pravidelne trénujte odolnosť voči phishingu a využite automatizované nástroje na opakovanie.

Používanie USB kľúčov a iných zariadení
Nikdy nepripájajte nájdené USB kľúče a nepovolené zariadenia.

USB kľúče môžu byť napadnuté malvérom, ktorý infikuje systém alebo zlikviduje zariadenie.

Pripájajte iba zariadenia, ktoré sú schválené a skontrolované IT tímom.

Verejné WiFi siete
Minimalizujte riziko použitím VPN, ideálne tej firemnej.

Namiesto verejnej Wi-Fi siete použite mobilný internet, napríklad LTE.

Šifrovanie a zálohovanie citlivých údajov
Aj keď dôjde k úniku, šifrované dáta sú lepšie chránené.

Ak potrebujete niečo poslať, použite aspoň heslovaný 7zip.

Nezabúdajte na zálohy a testovanie ich obnovy, pravidelné zálohovanie je kľúčové pre ochranu údajov.

Predvolené heslá a úvodné správy
Nastavte si svoje heslo do služieb a zariadení. Úvodné heslá zostávajú v emailoch

Predvolené heslá sú známe a často verejne dostupné.

Kyberbezpečnosť je tímová práca
Pri ochrane systému hrá kľúčovú rolu každý zamestnanec.

Jednoduché chyby môžu viesť k vážnym bezpečnostným incidentom.

Ak nevytrénujeme kolegov my, tak to za nás spraví niekto iný a bude to podstatne drahšie.

Dominik Procházka, riaditeľ odboru kybernetickej bezpečnosti AGEL

Všetky zariadenia a všetci ľudia, tak sa buduje odolnosť. FOTO: DREAMSTIME

SKÚSENOSTI

Nemocnice majú traumatologický plán. Máte taký plán aj pre IT?

Ako štatutár či riaditeľ firmy zodpovedáte za to, aby vaša organizácia fungovala nepretržite, bez ohľadu na neočakávané krízové situácie.

Traumatologický plán slúži v nemocnici na zabezpečenie vlastného fungovania v krízových situáciách. Keď treba plniť úlohy vyplývajúce z krízového plánu, poskytuje niečo ako manuál. Jeho súčasťou sú napríklad aj dôležité inštrukcie na poskytovanie rýchlej prvej pomoci zraneným.

V súčasnej digitálnej dobe sa preto logicky ponúka otázka, prečo nemať podobný traumatologický plán pre IT prevádzku. Tieto plány slúžia na riadenie kontinuity činností (Business Continuity Planning – BCM).

Bez dôkladného plánu riskujete, že vaše IT systémy, služby či procesy sa zastavia práve vtedy, keď ich najviac potrebujete – či už kvôli kybernetickému útoku, technickému zlyhaniu, alebo prírodnej katastrofe.

Prevencia straty údajov a zlyhania systémov
Predstavte si, že dôležitý informačný systém v nemocnici zlyhá. V tomto momente ide o minúty, možno sekundy. Každá oneskorená diagnóza alebo liečba môže mať fatálne následky. BCM pripravuje organizáciu na tieto situácie tak, aby pracovníci vedeli, čo robiť. V rámci BCM sú definované kľúčové procesy a technológie, ktoré musia byť obnovené ako prvé, a zároveň zabezpečuje, aby boli chránené a dostupné kritické dáta.

Zabezpečenie nepretržitých služieb aj v kríze
Riadenie kontinuity IT služieb v rámci BCM zabezpečuje, že aj počas výpadku alebo krízy budú systémy fungovať na akceptovateľnej úrovni. Pre nemocnice to znamená, že lekári budú mať prístup k zdravotným záznamom pacientov, a pre firmy, že dôležité obchodné operácie nebudú paralyzované.

Rýchla obnova po incidente
Bez ohľadu na to, či ide o kybernetický útok alebo zlyhanie IT infraštruktúry, BCM poskytne jasný plán, ako reagovať pri krízových situáciách. Rýchle rozhodovanie a realizácia plánu obnovy po havárii môžu byť kľúčové pre minimalizáciu strát. BCM definuje maximálny tolerovateľný čas výpadku, ktorý určuje, ako dlho môže vaša organizácia fungovať v krízovom režime bez závažných dosahov.

Reakcie v kríze sú často pokrivené stresom, preto sú príprava a plán kľúčové. FOTO: DREAMSTIME

Ochrana reputácie
Rýchla a efektívna reakcia na krízu výrazne ovplyvňuje, ako vás vnímajú pacienti, zákazníci či obchodní partneri. Ak nie ste pripravení, vaše meno môže utrpieť. BCM vám pomôže reagovať profesionálne a udržať si dôveru verejnosti aj v náročných situáciách.

Príprava na ransomvér a ďalšie hrozby
Kybernetické útoky sú na vzostupe, a preto musíte byť pripravení čeliť napríklad aj ransomvérovým útokom. BCM zabezpečí, že viete, ktoré systémy priorizovať a ako obnoviť prístup k dátam bez platenia výkupného. Včasné zálohy a ich správne využitie môžu byť kľúčové pre minimalizáciu škôd.

Testovanie a neustále zlepšovanie
BCM nie je len o vytvorení plánu, ale aj o jeho pravidelnom testovaní a aktualizácii. Cvičenia, ako sú „table-top" simulácie, pomáhajú identifikovať slabé miesta a zlepšiť plány na základe skutočných scenárov. Tréningy pripravujú organizáciu zvládnuť aj tie najneočakávanejšie krízy.

Kľúč k nepretržitému fungovaniu
V dnešnom svete je plán na riadenie kontinuity činností nevyhnutnosťou pre každú nemocnicu či firmu, ktorá sa chce efektívne brániť krízovým situáciám. Cieľom je nielen rýchlo a efektívne reagovať, ale aj ochrániť životy, reputáciu a finančné zdroje organizácie. Ak ste o krok vpred, máte veľkú šancu, že žiadna kríza neohrozí vašu každodennú prevádzku informačných systémov.

Michal Ďorda, partner pre expertné služby, Cyllium