Lidský faktor

Náš časopis je mnoho let plný nejrůznějších návodů, jak zvyšovat bezpečnost IS/IT. Před útoky v kyberprostoru nás mají chránit stále rozsáhlejší právní úpravy s drakonickými sankcemi, stále důmyslnější softwarové nástroje, stále komplexnější systémy řízení bezpečnosti a stále spolehlivější zálohovací a kontinuitu udržující mechanismy. Přesto celý svět mnohdy marně bojuje s útoky, které zahlcují servery, vydírají uživatele, kradou identity a provádějí další ošklivosti. Kde je tedy slabé místo?

Jak řekl bývalý ruský premiér Černomyrdin: „Mysleli jsme to dobře a dopadlo to jako obvykle.“ Můžeme mít sebesofistikovanější nástroje, ale pokud bude ten, kdo je má používat či dodržovat, slabým článkem, vždy budeme tahat za kratší konec sirky proti útočníkům, kteří mají znalosti, příležitost a motivaci.

Kdysi jsme dělali audit bezpečnosti IS velké banky. Po přečtení více než 1 000 stránek bezpečnostní dokumentace to vypadalo, že naše činnost je zbytečná. Až do spatření dveří do výpočetního centra, které byly místo zamčení dokořán

Jiří Slíva & DSM

otevřeny a ještě zajištěny klínem, aby si zaměstnanci, chodící kouřit, nezabouchli. Když jsem pracoval na odhalení podvodu, který stál jinou banku 30 mil. Kč, zjistilo se, že administrátorské heslo znali všichni zaměstnanci útvaru IT a pro jistotu bylo ještě vyvěšené na nástěnce na chodbě. Před několika lety nespokojený zaměstnanec sbalil všechny projekty uložené na serveru do souboru ZIP a opatřil heslem, které nikdy neprozradil a ani šifrová služba tohoto státu si s ním neporadila. Běžně se setkávám s tím, že vedoucí pracovníci, ale třeba i advokáti, svěřují své podepisovací certifikáty a hesla do datové schránky svým asistentkám, takže tyto jednají, jako by jednali oni sami. Ve firmách je běžné vzájemné sdělování hesel, odcházení od neodhlášených systémů, vytváření stínového IT na vlastním hardware a software pod pomýleným heslem BYOD, používání neschválených externích služeb (od soukromých mailů obsahujících firemní dokumenty až po veřejná úložiště typu Dropbox nebo Disk Google). A to uvádím příklady ze sféry znalé či přinejmenším poučené. Pak se již nemůžeme divit běžným uživatelům, kteří vytrvale používají hesla typu „123456“, nerozlišují, zda jsou na linku „www.mojebanka.cz“ nebo „www.jehobanka.cz“ případně klikají na všechno, co jim vyskočí na obrazovce, protože chtějí vidět nějakou nahou celebritu.

Z kriminologie je známo, že výše trestu není odstrašujícím faktorem, protože pachatel buď v daném momentu o tom vůbec nepřemýšlí, případně je přesvědčen, že se na něj nikdy nepřijde. Naopak vliv má rychlost zjištění trestného činu, a ještě více neprodlené potrestání pachatele. V kyberprostoru to je složitější nežli v kontaktním fyzickém světě, protože pachatel se může vydávat za někoho jiného, skrývat se za anonymizátory a proxy servery, jakož i využívat rozporu mezi globalitou kyberprostoru a teritorialitou práva. Důkazy mohou být snadno vymazány či modifikovány a míra latence (skrytosti) trestné činnosti je vysoká. Má to tedy nějaké řešení?

Jako u všech druhů zločinnosti, i u kyberzločinů je třeba se zaměřit více na prevenci a proaktivní jednání než represi. Prevence nespočívá v tom, že každému, kdo se byť jen uklepne na klávesnici „vyšpulí“ nějaký orgán, nejlépe přímo z EU, pokutu 100 mil. EUR. Prevence spočívá ve vytvoření takového systému řízení bezpečnosti, v němž bude hrát významnou roli bezpečnostní vědomí v organizaci, správné nastavení řídících struktur (viz stále přežívající nebezpečné slučování správy IS/IT a správy bezpečnosti IS/IT), jejich komunikace (bezpečnost je věcí všech, nikoliv jen bezpečnostního manažera, který je často vnímán jako utráceč peněz akcionářů), ale také zajištění, aby byla každá operace v IS/IT zadokumentovaná, dohledatelná a zejména, abychom mohli přiřadit, kdo za ni odpovídá. Protože za většinou úspěšných útoků zvenčí stojí nedbalost či úmysl někoho zevnitř – dodavatelem počínaje a uživatelem konče.

Proto je namístě znovu připomenout Demingovo pravidlo PDCA, které v oblasti bezpečnosti IS/IT může mít podobu např. Naplánuj (čeho chceš dosáhnout, tj. co chceš zabezpečit) – Udělej (realizuj bezpečnostní projekty a opatření) – Kontroluj (přezkoumej, ověř, monitoruj a promítej zpětnou vazbu, např. o incidentech) – Jednej (rozhodni o dalších krocích za účelem udržování a zlepšování bezpečnostního systému). Typickou chybou je zaměření se na jeden krok, obvykle „Udělej“, jako by tím bylo hotovo. Ale bez kontroly a monitorování nebude žádný systém, natož bezpečnostní správně fungovat déle než maximálně v okamžiku jeho spuštění. Protože lidé jsou nejslabším článkem řetězu definujícího celkovou úroveň informační bezpečnosti organizace, měla by být kontrola zaměřena především tímto směrem. A jednou z nejméně realizovaných zásad je starý římský princip Quis custodiet ipsos custodes? neboli Kdo bude hlídat hlídače samotné?

Možná nám v tom pomůže další vývoj nástrojů na bázi umělé inteligence, možná by to chtělo méně mechanického alibismu a více zdravého rozumu a osobní odpovědnosti. Nejspíše vhodná kombinace obojího.

Prof. Vladimír Smejkal
soudní znalec