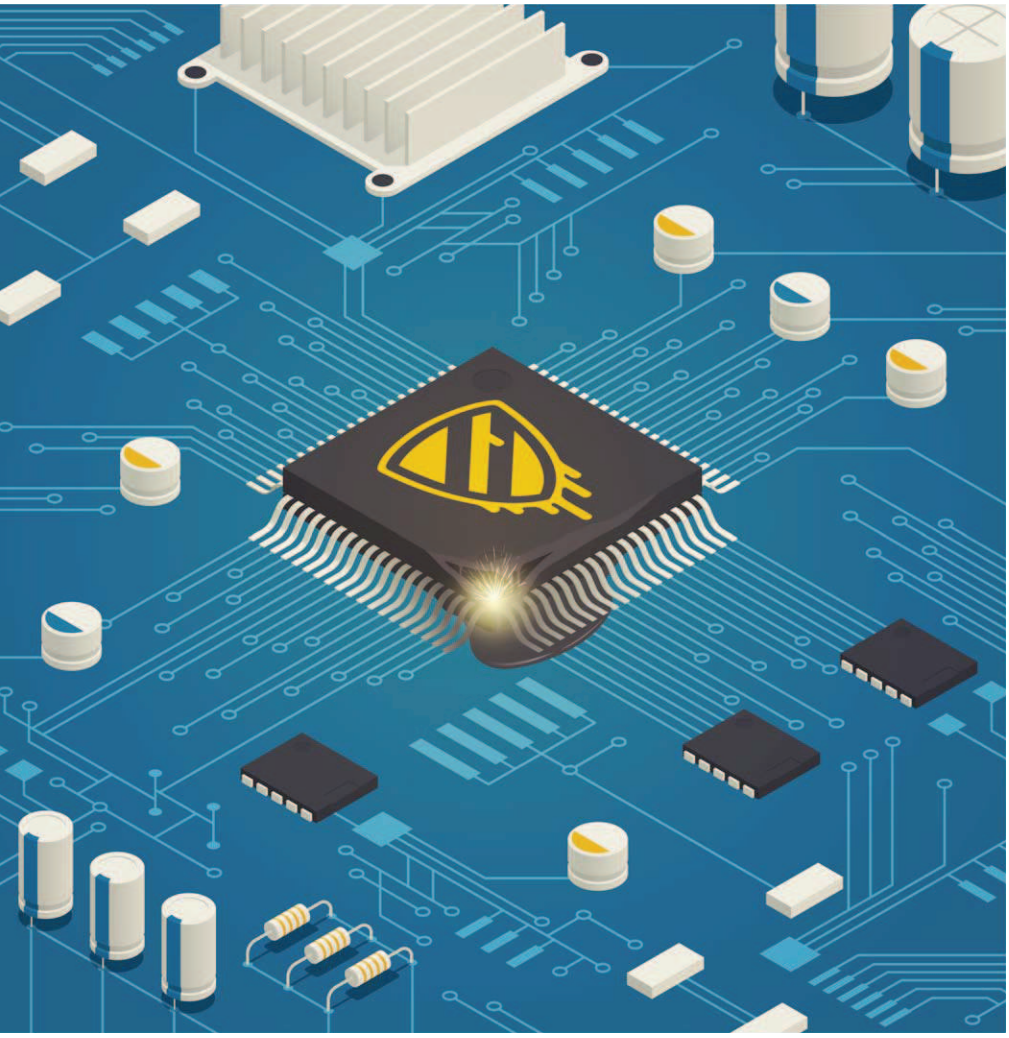
Jak řídit zranitelnosti lépe a efektivněji...

Petr Nádeníček

Už jste si pořídili nějaký Vulnerability Management System (VMS) nebo Vulnerability Risk Management (VRM)? Používáte ho a zlepšujete díky němu bezpečnost vaší organizace? Využíváte ho opravdu efektivně a tam, kde je to nejvíce třeba nebo máte o způsobu jeho využití pochybnosti? Dokážete nalezené zranitelnosti eliminovat dostatečně rychle? Zahrnujete nalezené zranitelnosti do výpočtu rizik, která vás ohrožují? A dokážete z toho vytěžit i další benefity, než „jenom" identifikaci zranitelností? V tomto článku se vám pokusíme na tyto a i některé další otázky odpovědět.



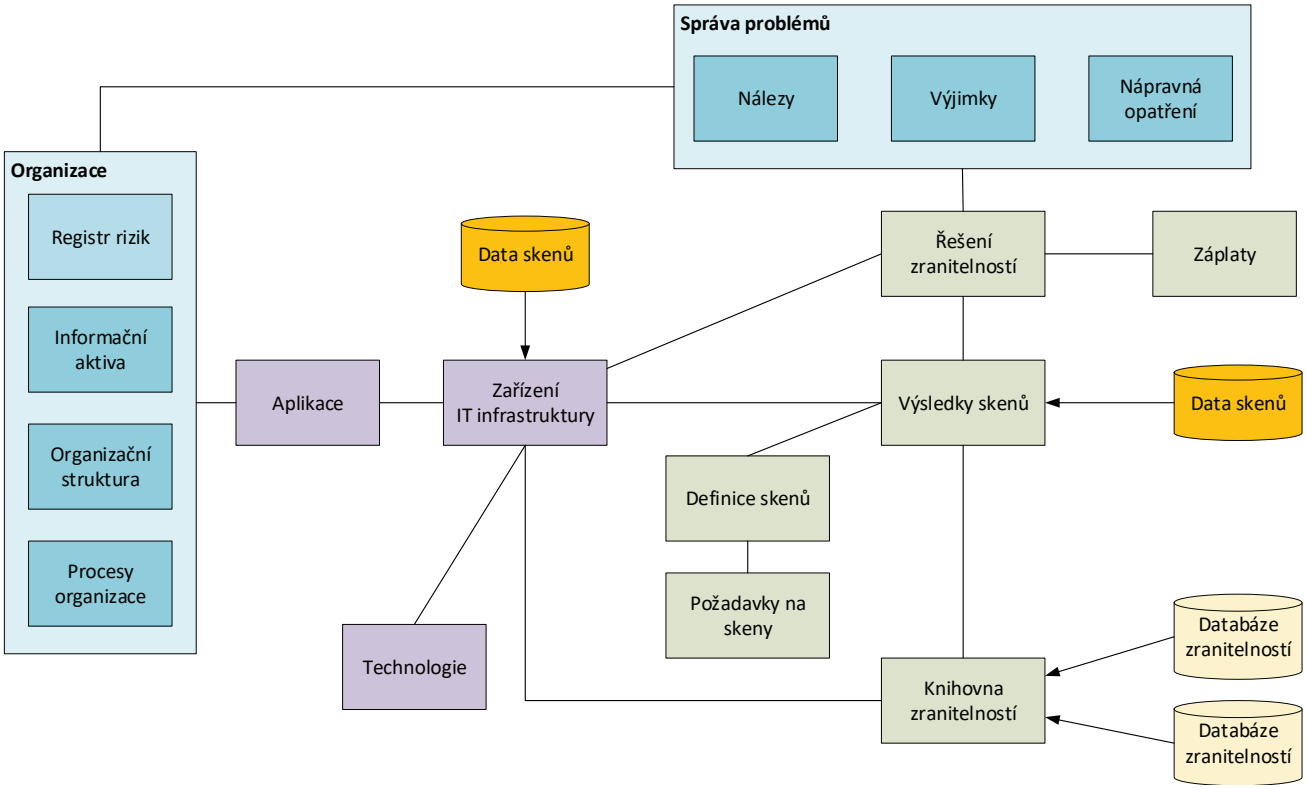
Máme nástroj. A stačí nám to?

Myslím, že nikdo, kdo se pohybuje v oblasti ICT bezpečnosti, se mnou nebude polemizovat o tom, že je přinejmenším vhodné, ne-li přímo žádoucí, jednou za čas zkontrolovat stav technického zabezpečení své infrastruktury. Jedná se o prověřování výskytu existujících zranitelností v rámci používaných operačních systémů, Middleware i samotných aplikací.

Jedním ze způsobů, jak tuto potřebu pokrýt, jsou penetrační testy, které je možné realizovat interními silami či prostřednictvím vybraného externího dodavatele. Pokud se na penetrační testy díváme z pohledu samotného procesu řízení zranitelností, jde především o definici jejich rozsahu. Penetrační testy sice ve svých prvních fázích typicky používají metody skenování a identifikace existujících zranitelností, které pak často i manuálně ověřují (zda se nejedná o false-positive detekci). Jejich primárním cílem je ale spíše celkové ověření (ne)kompromitovatelnosti daných systémů a řešení jako celku, nikoliv sestavení plnohodnotného výčtu všech existujících zranitelností v rámci testované infrastruktury. Navíc periodicita provádění penetračních testů se i ve velkých organizacích, které dbají na bezpečnost svých systémů, pohybuje spíše v řádech jednotek testů za rok, což vzhledem k tomu, jakou rychlostí dnes nové zranitelnosti vznikají, není dostatečné. Penetrační testy nám sice s řízením zranitelností dokáží určitým způsobem pomoci, ale nelze je jimi plně nahradit.

Pokud chceme držet krok s aktuální dynamikou vzniku a objevování nových zranitelností, a chceme se dostatečně chránit před jejich zneužíváním v rámci reálných útoků, zpravidla dojdeme k závěru, že se bez pořízení vlastního řešení pro řízení zranitelností neobejdeme. Cílem tohoto článku není zabývat se problémy při jeho výběru. Dejme tomu, že jsme dospěli k závěru, že nástroj potřebujeme, našli jsme na něj v rozpočtu prostředky a pořídili jsme si jej. Máme ho nainstalovaný a můžeme ho libovolně, tedy v rámci omezení dané licence, využívat.

Zde však ve většině případů nastává první zádrhel. Musíme nalézt způsob, jak toto řešení efektivně využívat. Začne to většinou tím, že dojdeme k závěru, že musíme mít ve svém týmu zaměstnance nebo rovnou celý tým, který bude pro obsluhu řešení dedikován. Pokud totiž necháme nástroj „bezprizorní", nenajdeme zpravidla způsob, jak by si ho mezi sebou jednotliví zájemci o skenování zranitelností jednoduše předávali. Dalším hlediskem je, že abychom byli schopni skener použít, musíme mít určité technické znalosti. Minimálně musíme vědět, co přesně chceme skenovat, co chceme zjistit („jen" existující zranitelnosti,



Obr. 1: Schéma řízení zranitelností v rámci GRC. Pod každým prvkem schématu se skrývá určitý webový formulář, který eviduje daný typ informací. Pro lepší znázornění si jej můžete představit jako tabulku, kde každý řádek představuje jeden záznam, sloupce jsou pak jednotlivá pole – položky formuláře.

soulad s určitou specifickou hardeningovou politikou, a další) a jakým způsobem si můžeme dovolit skeny provádět (zda můžeme použít i poněkud hrubší metody, které mohou ve svém důsledku vést k omezení funkcí nebo celkové nedostupnosti cílových systémů). A nakonec samozřejmě musíme být schopni pochopit výsledky skenů (posoudit nebo ověřit, zda určité nalezené zranitelnosti nejsou jen false-positive a zda úroveň zranitelnosti je v našem specifickém případě reálně taková, jak říká nástroj).

Když už máme dedikovanou obsluhu, musíme definovat pravidla, jakým způsobem budou jednotlivé skeny zadávány. Zpravidla je to řešeno tak, že se veškeré požadavky o provedení skenů sbíhají buď přímo u obsluhy, která určuje jejich prioritu a definuje výsledný rozvrh, nebo je tímto bodem např. vedoucí oddělení bezpečnosti, který rozhoduje a pověřuje obsluhu jejich provedením. V rozsáhlejších a stabilních infrastrukturách se zpravidla stanovuje rozvrh, podle kterého jsou periodicky prověřovány definované části infrastruktury dle jejich priority. Obě varianty řešení však v sobě skrývají řadu nedokonalostí. První je náchylná na vznikání sporů a k tomu, že se obsluha často ani nedozví, co vše by si v rámci infrastruktury zasloužilo prověřit. Druhá varianta zase často lehce sklouzne do rutiny, kdy jsou pořád dokola skenovány ty samé části infrastruktury a rozvrh není schopen reagovat na potřeby nahodilých skenů ani na důležité změny v dohlížené infrastruktuře.

Dalším nezanedbatelným aspektem je, jakým způsobem se dále nakládá s identifikovanými a potvrzenými zranitelnostmi. Jednak musíme zajistit, že tyto zranitelnosti budou adresovány personálu, který je odpovědný za jejich pokrytí (tzn., např. instalaci potřebné záplaty nebo provedení upgrade), dále bychom také měli existující zranitelnost zohlednit v aktuální úrovni sledovaných rizik. To zahrnuje dát tuto informaci do potřebného kontextu a v případě potřeby daná rizika komunikovat i mimo IT a bezpečnostní oddělení, tzn. řešit s business vlastníky možné dopady momentálně zvýšeného rizika na systémy a informace organizace.

GRC je zkratka pro Governance, Risk (Management) and Compliance. Představuje soustavu postupů a procesů organizace v oblastech správy (řízení) organizace, řízení rizik a řízení souladu (s předpisy) včetně vzájemných interakcí a propojení těchto oblastí. Používá se pro označování nástrojů, které tyto procesy komplexně podporují a umožňují jejich integrované fungování.

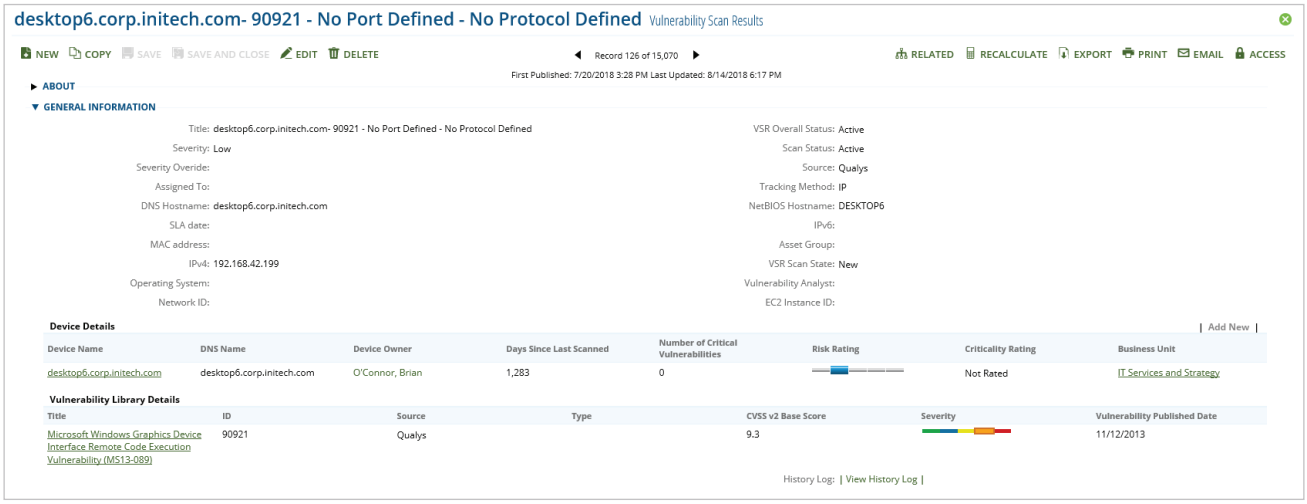
Termín „GRC“ se poprvé objevil kolem roku 2003 a přesněji definován byl o několik let později. Nyní se začíná objevovat také termín IRM – Integrated Risk Management, který však není vnímaný jako komplexní náhrada termínu GRC, ale spíše pokrývá řízení rizik v rámci tzv. „risk-aware kultury“ organizace. Zdroj: OCEG a Gartner

Řízení zranitelností v rámci GRC

Vhodným řešením popsaných úskalí je zavedení procesů adekvátních dané organizaci a jejich provázání s procesy IT provozu, IT bezpečnosti a Řízení rizik. Ideálním způsobem je pokrytí těchto procesů v rámci podpůrného GRC nástroje. Samozřejmě, že je možné tyto procesy zvládnout i bez něj, ale vzhledem už třeba jen k potřebě předávání relativně velkého objemu informací mezi různými odděleními se jeví zavedení podpůrného nástroje jako žádoucí. Samotný VMS/VRM nástroj naše komplexní potřeby bohužel zcela nepokryje.

Začlenění řízení zranitelností do GRC nástroje má řadu nezpochybnitelných výhod. Jedná se zejména o:

- Jednodušší zapojení většího množství lidí v rámci organizace – rozsah uživatelů GRC nástroje bývá daleko širší, než jejich zapojení do VMS/VRM nástroje. Zatímco



Obr. 2: Ukázka záznamu výsledku skenu (Vulnerability Scan Result) v GRC nástroji RSA Archer

nástroje používané pro řízení zranitelností jsou zpravidla používány pouze v rámci bezpečnostních oddělení, maximálně v rámci IT oddělení. GRC nástroje jsou používané v rámci celé organizace. Výhodou tedy je, že můžeme do procesů řízení zranitelností zahrnout také např. business vlastníky daných aktiv, na kterých je např. nalezena určitá zranitelnost, nebo se kterými tato zranitelnost souvisí v širším kontextu (např. vzhledem k možnému dopadu).

- Větší možnosti definice a přizpůsobení – aby mohly být GRC nástroje přizpůsobeny specifickým potřebám každé organizace, bývají zpravidla vybaveny širokými možnostmi customizace. Nástroje VMS/VRM, byť jsou třeba i vybaveny určitými workflow pro zvládání identifikovaných zranitelností, neposkytují tak široké možnosti přizpůsobení.
- Řízení zranitelnosti v širším (business) kontextu – aby mohl GRC nástroj pokrýt potřeby všech oblastí řízení, musí zejména obsahovat evidenci všech druhů aktiv organizace (od aktiv v rámci IT infrastruktury, přes informační aktiva, až po produkty a služby poskytované organizací např. klientům). Pokud jsou identifikované zranitelnosti řešené v rámci GRC, můžeme je vztahovat nejen na samotná zařízení, na kterých se vyskytují, ale můžeme je promítat třeba i vůči aplikacím, které jsou na těchto zařízení provozovány, nebo ještě dále do procesů, jež jsou těmito aplikacemi podporovány. Také jsme schopni konkrétní zranitelnosti přímo či nepřímo promítnout i vůči stávajícím rizikům. Můžeme tak vidět jednak zranitelnosti, jejich důsledky na různých aktivech, ale i působení různých zranitelností na dané aktivum nebo riziko.
- Jednodušší (automatizovaná) návaznost na další procesy – vzhledem k tomu, že procesy, jako je např. řízení výjimek, bývají standardně řešeny v rámci GRC, bývá bezproblémové se na ně napojit a obohatit je o výstupy procesu řízení zranitelností.

V rámci procesu řízení zranitelností bychom měli mít jednoznačně definovaná workflow minimálně pro:

- sběr požadavků na skenování;
- evidenci a zvládání nalezených zranitelností;
- definici a řízení výjimek;
- definici rizika a návaznost na proces řízení rizik;
- zavedení zařízení nově detekovaných v rámci infrastruktury;
- případně další workflow specifická pro danou organizaci.

Schéma možného řešení pro řízení zranitelností v rámci GRC je znázorněno na následujícím obrázku. Je nutné zdůraznit, že jsou v něm obsaženy pouze základní komponenty a vazby.

Nyní si pojďme uvedené schéma řešení vysvětlit mj. i v kontextu výše nastíněných problémů, které bychom měli v rámci realizace řízení zranitelností zahrnutého v GRC nástroji vyřešit...

Co potřebujeme prověřit?

Abychom mohli VMS/VRM efektivně používat, musíme především vědět, co (jaké zařízení, aplikaci apod.) a s jakou prioritou potřebujeme prověřit. Je rovněž třeba zajistit, aby každý, kdo má či bude mít potřebu VMS/VRM použít, tak mohl učinit. Toto je realizováno zprostředkovaně prostřednictvím obsluhy skeneru. Je tudíž nezbytné, aby se příslušné informace o požadavku na testování dostali k této obsluze, případně k dalším rolím, které disponují potřebnou plánovací a rozhodovací pravomocí.

Výchozím bodem nastíněného řešení jsou tedy „Požadavky na skeny“, ve kterých může každý oprávněný uživatel zadat, co chce skenovat, jakým způsobem, v jakém termínu, jaká je priorita tohoto úkolu atd. Požadavek následně absolvuje definované schvalovací kolečko, a pokud je schválen, vznikne na jeho základě „Definice skenu“. V rámci definice je uvedena specifikace skenu a jeho účelu, v případě periodicky opakovaného skenu je uvedena perioda, použitý skenovací nástroj, rozsah skenu a další parametry, dle typu daného skenu.

Máme tu zranitelnost – co s tím?

Po provedení skenu jsou všechny nalezené zranitelnosti zapsány do formuláře „Výsledky skenů“. Záznam obsahuje informace o zařízeních, kde byla daná zranitelnost identifikována. Dále obsahuje také odkaz na podrobný popis zranitelnosti v „Knihovně zranitelností“, která je synchronizována s online dostupnými zdroji informací o zranitelnostech, jako je například NVD databáze (National Vulnerability Database provozovaná americkým National Institute of Standards and Technology) nebo databáze výrobců skenerů (Qualys, Tenable a jiné).

Na základě daného výsledku skenu může být vytvořen záznam v „Řešení zranitelností“. Typicky jsou zakládány tikety na ty zranitelnosti, které chceme odstranit. Tiket je přiřazen konkrétnímu pracovníkovi, který za jeho vyřešení zodpovídá, případně jsou určeni i pracovníci v dalších rolích, jako je např. analytik, schvalovatel apod. Je určen konkrétní termín pro uzavření tiketu. V případě jeho překročení je workflow nastaveno

tak, že dochází k automatickým eskalacím na definované role v organizaci. Tiket může obsahovat i vazbu na příslušnou záplatu, která je evidována v rámci samostatného formuláře „Záplaty".

Uděláme výjimku, nebo nápravné opatření?

Pokud je zranitelnost úspěšně vyřešena, je tiket po schválení uzavřen. Pokud zranitelnost z jakéhokoliv důvodu vyřešit nelze, je možné na jeho základě vytvořit „Nález", který může následně vyústit ve vytvoření výjimky nebo nápravného opatření. Workflow řešení nálezu je již poněkud komplexnější a zahrnuje např. i vyjádření zástupců byznysu. Má také přímou návaznost na rizika evidovaná v „Registru rizik", tzn., že nevyřešená zranitelnost zvyšuje konkrétní sledované riziko. Pokud je z nálezu vytvořeno konkrétní nápravné opatření, je řešeno v rámci svého definovaného workflow, které končí v okamžiku implementace opatření. Poté je uzavřen tiket i související nález, což posléze ovlivňuje i návazná rizika. Pokud není možné nález vyřešit pomocí nápravného opatření, je vytvořena výjimka, která má rovněž svoje specifické workflow – výjimka je navržena, schválena a po uplynutí své platnosti je buď prodloužena (opětovně schválena) nebo zrušena. Existence výjimky pouze odkládá vyřešení souvisejícího nálezu a sama o sobě nijak nesnižuje související hodnoty rizik.

A co je to za zařízení?

Integrace výsledků skenování zranitelností může organizaci přinášet i další benefity, než jen samotnou identifikaci zranitelností. Každý, kdo se někdy potkal s nástroji pro evidenci prvků IT infrastruktury (konfigurační databází), ví, že žádný takový nástroj není dokonalý a informace, které přebíráme do GRC, často nebývají dostatečně detailní. Integrace výstupů ze skenerů zranitelností nám ale mohou významně pomoci zkvalitňovat záznamy v „Zařízení IT infrastruktury". Pokud skener objeví dosud neznámé zařízení, je relativně jednoduché pro něj automaticky vytvořit záznam a iniciovat speciální workflow pro jeho identifikaci. V rámci workflow pak můžeme existenci nového aktiva potvrdit a provést jeho posouzení z různých hledisek, která nás zajímají (např. posouzení bezpečnosti zařízení, analýza dopadů na byznys a jiné).

A můžeme ještě více...

GRC ale můžeme kromě řízení zranitelností využít i ke zkvalitnění řady dalších oblastí bezpečnosti organizace. GRC je např. ideální platformou pro veškerá posouzení bezpečnosti, ať už na úrovni aplikací, zařízení infrastruktury nebo jiných jednotlivých aktiv (informační aktiva, procesy, ...). V oblasti řízení rizik můžeme GRC využít jako univerzální platformu pro hodnocení a reporting rizik od nejnižších úrovní operačních rizik až po vyšší agregované úrovně.

V oblasti compliance můžeme GRC využít jako ideální základ pro fungování Systému řízení informační bezpečnosti (ISMS) – lze zde např. kompletně řídit veškerou systémovou dokumentaci (bezpečnostní politiky, směrnice aj.) i záznamy (prohlášení o aplikovatelnosti, kontrolní opatření apod.), sledovat aktuální vyspělost našeho systému a definované metriky i další klíčové oblasti. A tímto možnosti GRC zdaleka nekončí...

Závěrem – už je pravý čas na GRC

Ukázali jsme si, jaké výhody může organizaci přinášet integrace řízení IT zranitelností do prostředí GRC a naznačili, k čemu dalšímu je možné toto řešení využít. V rámci řízení zranitelností nám GRC může významně pomoci zejména v procesu zadávání a časování skenů, vyhodnocení jejich výsledků a mapování na různá aktiva organizace, řízeného odstraňování zranitelností a vyhodnocení stavu infrastruktury po implementaci záplat. V neposlední řadě přináší GRC organizaci i celkově lepší řízení (nejen) včetně podrobného reportingu. Nenastal tedy i pro vás už vhodný čas opustit sdílené tabulky a dokumenty a posunout se někam dále? ■

Ing. Petr Nádeníček

Autor článku působí jako Senior Security Specialist ve společnosti AEC.