Těžko na cvičišti – lehko na bojišti!

Význam vzdělávání IT profesionálů pro zajištění kybernetické bezpečnosti

Milan Balážik

Bezpečnost dnešního digitálního světa se v posledních létech změnila, bohužel k horšímu. Na jedné straně se zvýšila jeho zranitelnost, na straně druhé se zvýšily hrozby. Jaké jsou příčiny? Dnešní digitální svět je čím dál víc vzájemně propojen. Služby, které spoléhají na výpočetní, úložní a komunikační schopnosti systémů, jsou všude. Na jedné straně nám umožňují využívat neustále nové, lepší, užitečnější, a zejména efektivnější služby, dělá nás nezávislými. Na straně druhé nás všechny dělají zranitelnějšími. Je to tím, že na tyto služby pochopitelně spoléháme a očekáváme, že budou neustále a bez přerušení fungovat. Přitom se nejedná pouze o služby, které nám život ulehčují, případně ho dělají příjemnějším a pohodlnějším, ale zejména o služby tzv. kritické infrastruktury, na jejímž fungování závisí nejenom naše pohodlí, ale také ty nejcennější věci, které máme, jako jsou finance, zdraví a lidské životy.

K tomu, aby tyto systémy fungovaly tak, jak mají, je nutné udržovat je ve „zdravém" stavu, tj. aby byly funkční a bezpečné. Bohužel, v popředí úsilí bývá často právě hledisko funkčnosti. To, že nějaký systém nebo služba nad ním postavená nejsou funkční, je totiž vidět na první pohled. Jiný je stav v bezpečnosti, a to zejména v bezpečnosti kybernetické. Bezpečnost není na první pohled vidět, zpomaluje vývoj a omezuje používání nových funkčností a je drahá. Z teoretického hlediska je bezpečnost tím vyšší, čím nižší jsou bezpečnostní rizika. Kybernetické bezpečnostní riziko je dáno především:

- stavem využitelných zranitelností (slabin)
- závažností dopadu na chráněná aktiva
- úrovní hrozby (útočník)

Čím vyšší je kterýkoliv z uvedených faktorů, tím horší je stav bezpečnosti konkrétního aktiva (služby, data, hardware, software, infrastruktura...).

V čem se tedy situace zhoršila?

Bohužel ve všech třech faktorech. Využitelných zranitelností přibývá velmi rychle. Růst nových a rozšiřování stávajících funkčností roste neustále vyšším tempem, přičemž na jejich zabezpečení není dost času, prostředků, lidí ani schopností. Jako příklad si uveďme trendy IoT, Industry 4.0 nebo chytrá či autonomní auta. Dopady, které můžou zasáhnout důležitá aktiva, jsou v důsledku jejich závislosti na digitálním světě stále více kritické až fatální.

Nejvíce se ale změnily hrozby. Kybernetický prostor se v posledních létech stal bojištěm. Dávno jsou za námi časy, kdy útočníci (hackeři) byli lidé, kteří se snažili proniknout do systémů pro vzrušení, či zábavu, případně se jednalo o politické aktivisty. Tito lidé pracovali zejména z osobního přesvědčení či ideologické motivace a jejich schopnosti byly omezené. Dnešní útočníci jsou nájemní profesionálové, jejichž cílem je odcizení firemních informačních, finančních a jiných aktiv, případně jejich zničení (např. finanční sektor, obchod, služby...). Ještě výše v hierarchii se nacházejí kyberbojovníci silových složek států, jejichž cílem je kybernetická válka, která sahá od šíření dezinformací až po úroveň destabilizace ekonomik států (např. masové sdělovací prostředky, kritická infrastruktura, obrana nebo vláda států).

Kyberbojovníci mají racionální cíle, na které se soustřeďují, jsou zkušení a výborně trénovaní, pracují koordinovaně, mají strategické a taktické vedení, téměř neomezené časové a finanční možnosti. Porovnejme si to se schopnostmi a možnostmi dnešních IT profesionálů, kteří mají za úkol bránit aktiva proti uvedeným útočníkům: Naši obránci musí chránit všechna aktiva najednou (nevědí, na které bude útočeno), přičemž nemají téměř žádné zkušenosti s kybernetickými útoky a jejich projevy.

Spoléhání na bezpečnostní technologie

Dalším velkým problémem je, že bezpečnost je příliš orientována na technologie. Dnešní bezpečnostní IT profesionál má implementované všechny moderní bezpečnostní technologie. Jejich množství neustále narůstá a v „bezpečnostním ekosystému" dochází k jejich hromadění a vrstvení. To má za následek, že bezpečnostní systémy jsou hodně komplikované, nepřehledné, jejich funkčnost se často překrývá.

Dnešní svět bezpečnosti je bohužel často definován až diktován výrobci bezpečnostních technologií. IT profesionálové jsou pak vzděláváni s ohledem na konkrétní technologie a často „pro stromy nevidí les". Soustředí se na správnou konfiguraci každé technologie, ale nejsou schopni vidět věci v souvislostech.

Kromě toho má každá – i bezpečnostní – technologie své nedostatky i zranitelnosti a často generuje falešné poplachy, což ztěžuje netrénovaným lidem rozpoznat možný kybernetický útok ve kterékoliv jeho fázi.

Dnešní stav kybernetické obrany spoléhá zejména na správné nastavení bezpečnostních technologií a na jejich automatické

možnosti rozpoznat kyberneticky útok. Toto je mnohdy, vzhledem ke komplexitě systémů a rychlosti vývoje v kybernetickém prostoru, chybný předpoklad. V případě, že tato automatizovaná kaskáda selže (a v praxi se ukazuje, že selhává velice často), má netrénovaný IT profesionál velmi omezené možnosti rozpoznání útoku a nedostačující zkušenosti pro adekvátní reakci.

Moderní bezpečnostní technologie vyžadují neustálé vysoce dynamické ladění ze strany lidí, v opačném případě buďto ztrácejí účinnost, nebo co je případ horší, vytváří pocit falešné jistoty. Schopnost sledovat a vyhodnocovat výstupy těchto technologií je vysoce netriviální. Rozpoznat v takovém případě útok samo o sobě vyžaduje vysoce schopné operátory. Bohužel se často stává, že je útok jako takový „identifikován", teprve když se exfiltrovaná „chráněná" data začnou nabízet k prodeji na internetu.

Přístup spoléhání pouze na bezpečnostní technologie je velmi nebezpečný. Útočníci velmi dobře znají všechny platformy technologické bezpečnosti a jejich nedostatky či zranitelnosti (vzhledem na výše uvedené mnohdy lépe než obránci). Proto je potřebné, aby IT profesionálové kromě identifikace probíhajícího útoku byli schopni v ideálním případě takovému útoku čelit, tj. aktivně se podílet na jeho odvrácení, případně podniknout kroky k zmírnění dopadů na aktiva.

Trénink kybernetické obrany

Natrénování postupů detekce a následné reakce, vedoucí k odvrácení útoku, je v běžném životě a na produkčních systémech nemožné. Ačkoli by teoreticky šlo vést sofistikovaný kybernetický útok na produkční prostředí, není to obvykle přijatelná možnost – zejména z důvodu možných negativních až fatálních dopadů na aktiva, které mohou být ještě umocněny použitím neadekvátních způsobů na zastavení útoku ze strany personálu, který není připraven čelit takovým situacím.

Kybernetický trénink se odehrává na kybernetickém cvičišti, kde se IT profesionálové můžou naživo potkat a utkat s útočníky, jejich taktikou, strategií. Je to jediná příležitost, jak bez následků zažít různé fáze kybernetických útoků a naučit se je ne jenom rozpoznat, ale i účinně se bránit.

V kybernetickém tréninku se IT profesionálové nemusí bát dělat pod útokem chyby. Nevadí, když nastane situace, kde se pod tlakem zvolí neadekvátní (nevhodné/neúčelné) řešení, jehož důsledkem je narušení či ztráta aktiv. Učí se zejména principy obrany – nezáleží na konkrétních výrobcích a použitých technologiích.

Kybernetický výcvik umožňuje účastníkům pochopit způsoby a principy, jakými se připravují, koncipují a vedou kybernetické útoky ze strany profesionálních hackerů, a naučit se volit optimální způsoby detekce a reakce na ně.

Kybernetický výcvik učí a nutí lidi koordinovaně pracovat v týmu, naučit se vhodně formulovat problémy a popisovat stav problémů v jazyce srozumitelném pro management. Management tak získává informace v potřebném rozsahu, kvalitě i úrovni pro rychlá a správná rozhodnutí.

Správný kybernetický výcvik musí mít následující charakteristiky:

- musí se řídit ověřenou metodologií a útoky musí probíhat na pozadí realistických scénářů
- dává možnost zažít projevy skutečných živých útoků na různé cíle a různými vektory
- získávání praktických zkušeností v detekci různých fází útoků a jejich odvrácení, příp. zmírnění
- realistické technické útoky musí být kombinovány se sociálním inženýrstvím
- možnost zpětné vazby, korekce, poučení z chyb a praktické otestování nabytých dovedností
- možnost forenzní analýzy proběhlého útoku
- výcvik musí být přizpůsoben konkrétním schopnostem obranného týmu
- získání zkušenosti a návyků s prací pod tlakem
- možnost bez nebezpečí vyzkoušet, vytrénovat a zkonsolidovat své detekční, reakční, komunikační a rozhodovací schopnosti

Milan Balážik

Autor článku je manažerem vzdělávacího centra CyberGym Europe, a. s.