Připravme se na nejhorší

Pandemie nám ukázala, jak důležité je hodnocení ekonomických dopadů bezpečnostních opatření. Schopnost činit rychlé a správné rozhodnutí odlišuje úspěšné od těch ostatních.

MIROSLAV NEČAS

Bezpečnostní rizika jsou vždy úzce spojena s výkonem ekonomiky a situací na trhu. Díky tomu, že se ekonomice v posledních letech dařilo a díky nízké nezaměstnanosti jsme si zvykli na relativní bezpečí ve všech oblastech. Vždy je potřeba čelit novým typům rizik, která souvisejí s vývojem technologií a novými typy útoků. V blízké době se však budeme muset vyrovnat se situací podobnou finanční krizi v roce 2009. A podle řady odhadů ovlivní pandemie COVID-19 ekonomiku ještě zásadněji. Je potřeba se připravit na zhoršení bezpečnostní situace ve všech ohledech. Potřebu uvědomit si provázanost bezpečnostních incidentů a kondice ekonomiky dokládá mimo jiné i aktuální dění v USA. Ekonomická nejistota a z ní plynoucí frustrace lidí podněcuje k násilnému řešení. Usmrcení George Floyda by nepochybně i v jiné době vyvolalo reakci, která odpovídá nesmírné závažnosti tohoto činu. Troufám si ale tvrdit, že forma protestů by byla méně násilná a stejně tak i odezva americké vlády.

Celostní přístup k hodnocení rizik

Ve společnosti TOVEK se zabýváme využitím analytických nástrojů v oblasti bezpečnosti již více než 26 let. Zažili jsme divoká devadesátá léta i krizi po roce 2009. Postupně jsme pokročili od analýzy textů a strukturovaných dat k analýzám hlasu nebo obrazu. Po celou dobu jsou naše nástroje využívány na vrcholové úrovni, kde je potřeba dávat do kontextu informace z různých zdrojů do ucelených pohledů. Naše dlouholeté zkušenosti ukazují, že je nutné přistupovat k bezpečnosti komplexně. Není možné oddělit bezpečnost kybernetickou od bezpečnosti fyzické. Je potřeba zvažovat bezpečnostní rizika spojená s vlastními zaměstnanci, dodavatelským řetězcem a zákazníky v kontextu celkové ekonomické situace na trhu. Pominout samozřejmě nelze ani aktivity konkurence nebo různých zájmových skupin. Celostní přístup k hodnocení bezpečnostních rizik vyžaduje znalost jejich širšího (procesního, technického, ekonomického, bezpečnostního, právního…) kontextu. K tomu je potřeba posilovat výměnu informací mezi „bezpečáky“ a obchodníky, ekonomy, techniky, informatiky a dalšími specialisty. To nelze bez názorné prezentace informací v souvislostech. Aby člověk dokázal pochopit podstatu určitého problému, potřebuje se v něm zorientovat. Společný obraz situace pomáhá nalézt společnou řeč lidem z různých profesí a různého zaměření. Vizuální prezentace rizik jim pomáhá uvědomit si klíčové skutečnosti a vztahy a kvalifikovaně o nich diskutovat. Pouze na základě širší diskuze lze činit účinná bezpečnostní opatření, tak aby neohrozila fungování podniku a realizaci tržních příležitostí.

Miroslav Nečas Business Develpment Manager, TOVEK

Vyhodnocení bezpečnostních incidentů v širším kontextu

Dobře nastavené systémy detekce umožňují zachytit bezpečnostní události různého druhu. Detekce problému je z celostního pohledu pouze první krok k jeho nápravě. Detekční systémy často produkují takové množství falešných poplachů, že není v lidských silách všechny detekované události zpracovat. Pro vyšetření bezpečnostní události a zjednání nápravy jsou také často potřeba doplňující informace. Může jít o údaje ze systému docházky, bankovní transakce, výpisy komunikace, externí databáze či informace dostupné na odborných fórech, blozích, sociálních sítích či v jiných otevřených zdrojích. Informace tohoto typu umožňují odhadnout cíle útoku, jeho závažnost a dopady. Na základě toho lze stanovit jeho prioritu při řešení. Získané důkazy rovněž nezbytné k vyvození konkrétní odpovědnosti, podání trestního oznámení či uplatnění pojistného plnění.

Neintegrujte systémy, syntetizujte informace! Je to rychlejší, levnější, účinnější.

Jak ale propojit informace z různorodých zdrojů do jednoho smysluplného obrazu? Integrace systémů je finančně a časově náročná. Času je málo a potřeby, které zdroje vyhodnocovat a jak se na informace dívat, se neustále mění. Řada klíčových informací není v žádném informačním systému, nachází se v šedých datech a hlavách lidí. Řešením je neintegrovat informační systémy, ale propojit v nich obsažené informace do syntetických pohledů pomocí platformy TOVEK. Tento přístup se osvědčil v řadě našich projektů. Umožňuje konsolidovat informace z ekonomických a agendových systémů, SIEM systémů, systémů řízení výroby a dalších informačních systémů uvnitř i v ně organizace. Díky tomu lze z jednoho místa snadno dohledat informace o kontextu určité bezpečnostní události, názorně je prezentovat zainteresovaným osobám a díky tomu kvalifikovaně rozhodnout, jak reagovat. Například zvolit adekvátní protiopatření či shromáždit důkazy potřebné pro vyvození interní odpovědnosti či navazující právní kroky. Naše zkušenosti ukazují, že syntézou informací lze ušetřit až 90 % času potřebného k vyšetření bezpečnostní události a zároveň dosáhnout lepších výsledků. A čas je v řadě případů cennější než peníze.