Forensic Readiness je hudbou budoucnosti

Jsme dostatečně připraveni na forenzní šetření? Proč nejsou incidenty důkladně šetřeny a nejsou z nich vyvozovány důsledné závěry? Kde hledat příčiny takové situace?

Původně bylo úmyslem popsat základní cíle a principy implementace oblasti, o které se hojně diskutuje v určité komunitě odborníků na informační bezpečnosti, oblasti Forensic Readiness. Realita je však obecně taková, že Forensic Readiness je v našich podmínkách realizovatelná jen s obtížemi, přestože její přínosy jsou, jak uvidíme dále, zřejmé. Problematika Forensic Readiness tedy bude popsána spíše způsobem, který dá informaci nejenom o jejím přínosu, ale zejména o podmínkách její implementace, které jsou klíčové k tomu, aby přinášela deklarované přínosy.

Forensic Readiness

Forensic Readiness v překladu znamená „připravenost na forenzní šetření“. V tomto smyslu by se mohlo zdát, že je to celé o něčem, co je v našich podmínkách spíše výjimečné, neboť forenzní šetření je aktivita, ke které se přistupuje pouze velice ojediněle. Jen ty větší společnosti se někdy, v případě velkých nebo medializovaných kauz, zaštitují „forenzními audity“ a pouze ojediněle jsou forenzní šetření ve větším rozsahu realizována externími subjekty (policií, protimonopolním úřadem, případně jinými státními orgány). Proč se tedy vůbec zabývat záležitostí, která je výjimečná, a tedy není zřejmě efektivní se vůbec zabývat její implementací?

Odpověď na tuto otázku je potřeba hledat ve správné interpretaci toho, co Forensic Readiness znamená reálně, aniž bychom se omezovali na výše uvedená zjednodušující vysvětlení. Vychází-je z klíčového dokumentu o Forensic Readiness [1] lze za základní definici považovat schopnost organizace maximalizovat potenciální využití digitálních důkazů při současné minimalizaci ceny šetření, nehledě na zvýšení účinnosti preventivních opatření a zvýšení schopnosti organizace zotavit se z mimořádných událostí. Forensic Readiness lze také chápat jako preventivní opatření, které je nutné realizovat s tím, že incidenty určitě vzniknou, v kontrastu přípravy konkrétních reaktivních opatření na již vzniklý incident.

Forensic Readiness vychází z následujících, objektivně existujících skutečností:

- Bezpečnostní incidenty (nebo obecněji problémy) objektivně v organizacích vznikají, nejen v oblasti, která je definována v rámci „úzkého“ chápání ICT a informačních systémů (můžeme je nazvat počítačové systémy), ale i v jiných oblastech činnosti organizace – od obyčejných krádeží materiálu a zařízení (ne nutně pouze počítačového) až po krádeže know-how, zcizování identity, vydírání, šikanu, zneužívání pravomocí, ale i jiné případy obchodně-právních a občansko-právních sporů a další problémy zdánlivě nesouvisející s digitálními daty.
- Převážná většina těchto incidentů a problémů zanechává různé druhy digitálních důkazů – od klasických logů v počítačích přes cíleně sbírané další počítačová (meta)data, záznamy digitálních kamer v hlídaných prostorách, záznamy ACS, EZS, EPS a podobných dohledových systémů nebo i digitální provozní záznamy o chodu výrobních prostředků až po potenciální záznamy GPS systémů ve služebních automobilech.
- Každý závažný incident musí být vyšetřen, musí být zjištěna příčina, ohodnocen důsledek, a když to je možné, tak i zjištěn a potrestán viník.

Z pohledu stávajících standardů a doporučení týkajících se bezpečnostních incidentů (např. ISO/IEC 27035) je primárním úkolem systému reakcí na bezpečnostní incidenty co nejrychlejší obnovení funkčnosti tak, aby výpadky

byly minimální, a tím se minimalizovaly dopady na chod organizace. Problematika bezpečnosti informací a pohled na řešení bezpečnostních incidentů tak, jak se uvádí v těchto normách, je celkem logický a přirozený, zorný úhel informační bezpečnosti ani neumožňuje jiné interpretace. Pro širší pochopení dopadů bezpečnostních incidentů na management organizace to je však nedostačující pohled.

Každý incident, ať už detekovaný nebo i takový, který ani zjištěný není, přináší organizaci škody. U zjištěného incidentu lze spočíst (nebo alespoň odhadnout) jeho dopady, u nezjištěného jsou dopady zpravidla ještě horší. Může způsobit opakování, může mít dopady na morálku organizace, na její dobré jméno, na plnění regulatorních podmínek apod. A jelikož o něm nevíme, nemůžeme tyto negativní dopady nijak ovlivnit.

Z pohledu managementu je i přístup k řešení zjištěných incidentů, kdy primární snaha je napřímena na obnovení funkčnosti, nedostatečný. Každý incident způsobuje škody a je nanejvýš nezbytné dopátrat se příčin a původce těchto škod. Problém však je v tom, že šetření incidentu z jedné strany a snaha o zotavení organizace po incidentu z druhé strany jdou většinou proti sobě, protože šetření vyžaduje sbírání stop a jejich analýzy. Ttyto činnosti komplikují postup obnovení a zdržují veškeré obnovovací činnosti.

Tento rozpor řeší právě Forensic Readiness. Když to zjednodušíme, je to cílené získávání a uchovávání klíčových informací organizace (digitálních důkazů) předem tak, aby byly okamžitě k dispozici pro případy šetření, ať už se jedná o právní spory, soudní líčení nebo o případy šetření bezpečnostních incidentů. Tento předvídavý přístup umožní:

- mít připravené důkazy pro ochranu organizace v jakýchkoli případech sporů;
- efektivně a rychle šetřit případy interních incidentů, včetně trestné činnosti zaměstnanců;
- systematické a systémové ukládání digitálních důkazů může výrazně zefektivnit interní šetření;
- strukturované ukládání digitálních důkazů výrazně ulehčí v případech nutnosti poskytnutí důkazů třetím stranám (např. soudům, policii apod.);
- rozšířit záběr oblasti bezpečnosti informací i na opatření proti dalším externím a zejména interním hrozbám;
- demonstrovat due-diligence a perfektní správu informačních aktiv organizace, soulad s regulatorními požadavky, zlepšit vyhlídky na úspěch interních nebo externích šetření a právních sporů;
- výrazně zvýšit úspěch při hledání interních, ale i externích pachatelů incidentů a řešení náhrad způsobených škod.

Podmínky implementace Forensic Readiness

Obecně pojmenované skutečnosti však nijak nepomohou dosáhnout toho, co je uvedeno v definici Forensic Readiness – maximalizace využití digitálních důkazů při minimalizaci ceny šetření. Hledat důkazy až v momentě potřeby, až v případě incidentu je také možné, avšak značně neefektivní. Zdržuje to práce na obnově, nezřídka už bývá pozdě a důkazy jsou nenávratně ztracené.

Zejména to jsou důvody, aby byly v organizaci potenciální digitální důkazy sbírány a uchovávány předem. V případě potřeby by byly k dispozici, nebylo by nutné je pracně získávat a dohledávat. Tyto důkazy by byly získány a uloženy způsobem, který znemožní jejich zpochybnění (tj. byla by zachována jejich integrita). Zjevné také je, že implementace Forensic Readiness obnáší určité dodatečné náklady. V organizacích, kde je vysoká úroveň bezpečnostního povědomí a je tam dobře implementován ISMS (systém řízení bezpečnosti informací), jsou dodatečné náklady na implementaci Forensic Readiness výrazně nižší než v organizacích, kde jsou s informační bezpečností problémy.

Implementace Forensic Readiness ovlivňuje i spektrum lidí, kterých se může potenciálně týkat. Z těch interních se může jednat zejména o interní vyšetřovací tým, interní audit nebo jeho speciální útvary, HR útvar, PR útvar, vlastníky informačních aktiv, liniové manažery, bezpečnostní útvary, IT, právní útvar, ale také o řadové zaměstnance apod. Široké spektrum potenciálně šetřených incidentů také logicky může způsobit, že bude nutná komunikace s různými externími subjekty, např. s policií (nejen místně příslušnou), ale i s dalšími subjekty na národní i mezinárodní úrovni, s dalšími státními institucemi, jako jsou antimonopolní úřad, ČNB, finanční úřady, odbory, externí auditoři, celníci, partnerské organizace a v neposlední řadě např. i média.

Od obecných proklamací ke konkrétním krokům

Obecné povídání o Forensic Readiness je potřeba doplnit o konkrétní kroky vedoucí k efektivní implementaci. Vytyčme tedy konkrétní cíle a definujme konkrétní činnosti, které povedou k naplnění takových cílů.

Cíle:

- Získávat digitální důkazy legálně tak, aby nebyly ovlivněny business procesy.
- Získávat takové digitální důkazy, které se týkají potenciálně nejzávažnějších incidentů nebo sporů.

- Digitální důkazy by se měly sbírat a používat pouze v těch případech, jejichž závažnost odpovídá nákladům na šetření.
- Šetření za použití digitálních důkazů by mělo minimálně ovlivňovat ostatní standardní business procesy.
- Použití digitálních důkazů by mělo být vždy ve prospěch organizace, mělo by chránit její zájmy.

Pro efektivní dosažení vytyčených cílů lze navrhnout následující kroky:

- Definice scénářů, které mohou vyžadovat digitální důkazy.
- Identifikace potenciálních zdrojů a druhů digitálních důkazů.
- Stanovení požadavků na konkrétní digitální důkazy.
- Určení požadavků na prostředky pro uchování digitálních důkazů.
- Stanovení politik a předpisů pro správnou manipulaci a ukládání digitálních důkazů.
- Zajištění cíleného monitoringu pro efektivní odhalení závažných incidentů.
- Specifikace podmínek pro iniciaci formálních vyšetřovacích postupů (s využitím digitálních důkazů).
- Školení všech zainteresovaných s cílem zajištění odborné manipulace a využití digitálních důkazů s důrazem na citlivost takových dat.
- Nastavení pravidel podrobné dokumentace všech případů použití digitálních důkazů.
- Zajištění právní podpory ve všech případech použití/využití digitálních důkazů.

Příklad problémů při interním šetření **BOX 1**

Jedna přední česká společnost v rámci svého strategického plánu zahájila důvěrná jednání o akvizici jiné společnosti s cílem získat důležitý segment trhu, zvýšit tím svoji konkurenceschopnost, rozšířit portfolio svých činností a stát se výhodnějším partnerem pro získávání lukrativnějších zahraničních zakázek. Pro takto důvěrná jednání byl vyčleněn tým prověřených pracovníků, jednání byla průběžně hodnocena na úrovni top managementu a jejich průběh nasvědčoval brzkému úspěchu. Byly dohodnuty i detaily smluv, avšak těsně před podpisem druhá strana od předběžných dohod najednou bez udání důvodů ustoupila. Bylo zřejmé, že protistraně se dostaly k dispozici citlivé interní informace, které ji odradily od dokončení smluvních jednání.
Následovalo interní šetření, avšak stávající situace v organizaci neumožnila předložit jediný hodnověrný důkaz o tom, kdo způsobil krach zdárně se vyvíjejícího obchodu. Absence jakékoli evidence zařízení, která byla k dispozici podezřelým osobám, produktů a aplikací, které mohly tyto osoby používat, evidence toho, co a kdy využívaly, monitoring aktivit, logování událostí apod. Interní šetření tedy nepřineslo nic konkrétního. A přesto, že jedna z podezřelých osob nedlouho po incidentu rozvázala pracovní poměr a navíc nastoupila na vysokou pozici v (teď už konkurenční) společnosti, nebylo možné nalézt jediný solidní důkaz o tom, že svým jednáním hrubě poškodila svoji (teď už bývalou) společnost.

Na tomto místě by mohl následovat podrobnější popis výše navržených kroků, rozbor podmínek a východisek, praktická doporučení ke každému navrženému kroku. Zastavme se však nad jinou, mnohem důležitější otázkou. Je Forensic Readiness pro mne? Co mi to přinese? Stojí za tu námahu? A jestli ano, dá se to vůbec efektivně realizovat?

Odpovědi na tyto otázky si musí dát každý sám. Jako návod uvedu na tomto místě jeden jediný konkrétní příklad (viz Box 1).

Jistě si dovedete představit množství dalších, třeba i méně závažných incidentů, které u vás v organizaci nikdy nebyly průkazně objasněny jen proto, že nebyly důkladně vyšetřeny nebo pro jejich šetření nebyl nalezen dostatek důkazů. Přitom takových důkazů je již ve většině organizací dostatek, jen nejsou jako důkazy chápány, nejsou cíleně sbírány, ukládány a využívány.

Forensic Readiness – hudba budoucnosti

Proč nejsou incidenty důkladně šetřeny a nejsou z nich vyvozovány důsledné závěry? Kde hledat příčiny takové situace? Pokusím se pojmenovat alespoň ty, které jsou z mého pohledu nejdůležitější, aniž bych je dával do nějakého pořadí nebo je generalizoval na všechny organizace.

- Naše současné právní prostředí nevytváří příliš vhodné podmínky pro precizní dodržování všech procesně-právních postupů. Vyplývá z toho např. i skutečnost, že pro konání právních úkonů (např. propuštění zaměstnance na hodinu) nejsou vždy exaktně vyžadovány nezvratitelné důkazy, resp. jejich nezvratitelnost se neposuzuje příliš přísně. Proč se tedy „namáhat nějakými důkazy“, když lze to samé provést i na základě méně průkazných faktů? Z druhé strany existuje málo nástrojů, jak postihnout zaměstnance, který způsobí zaměstnavateli škodu. Domoci se náhrady takové škody je procesně tak náročné, že je často jednodušší od formálních postupů upustit a situaci řešit (decentně řečeno) jinými, interními prostředky. Přitom existence nezvratitelných důkazů by tuto situaci mohla výrazně posunout dopředu a způsobené škody efektivně vymoci.
- Výše uvedené způsobuje, že u nás jsou pojmy forenzní, forenzní postupy, důkazy apod. chápány tak, že patří výlučně do soudní síně. V případech trestních šetření (vyšetřování policií)

se navíc jaksi předpokládá, že to je čistě věcí policie, očekává se tedy výlučně pasivní přístup. Nelze se potom divit, že takové vyšetřování se může táhnout dlouhou dobu, že může způsobit výrazné zásahy do chodu organizace, a tím i dodatečné škody, nebo to policii neumožní získat dostatek důkazů a věc se nedořeší.

- Dalším problémem je to, že z jedné strany jsou na organizace kladeny různé regulatorní požadavky na ukládání a uchovávání informací (např. požadavky na implementaci log managementu), z druhé strany jiné regulatorní požadavky omezují organizace v uchovávání a využití jiných druhů informací (např. požadavky na ochranu osobních údajů) a neexistují jednoznačně definované hranice a pravidla, co je ještě možné a co ne. Nejasnosti a někdy i nekompetentnosti v této oblasti způsobují, že je mnohdy jednodušší nepouštět se za hranice určitého, obecně přípustného minimálního rozsahu toho, co je v organizacích ukládáno a využíváno, jinak řečeno nezadávat příčiny k potenciálním problémům. Navíc u nás neexistuje kompetentní instituce nebo autorita, která by problematice dat zpracovávaných v rámci business procesů organizace,dala v tomto smyslu jednoznačné hranice a řád.

- Existuje velké množství informací, které jsou v organizaci nějakým způsobem zpracovávány, avšak jen minimum z nich se využívá efektivně. Příkladem mohou být logy. Ty jsou standardně někde ukládány, ale je velký problém s jejich využitím. Log management je ještě pořád ve většině organizací velkou neznámou, logy se využívají pouze částečně, nesystematicky, nesystémově, používají se téměř výhradně pouze některé systémové logy a pouze k provozním účelům. Jejich ukládání a uchovávání není systematicky řešeno. Při vývoji aplikací nejsou kladeny žádné požadavky na aplikační logy, na jejich vypovídající hodnotu, a vývojáři tudíž tyto neaplikují vůbec nebo pouze v minimální míře, nanejvýš pro provozní účely. O SIEM (Security Information Event Management) systémech ani nemluvím, jejich implementace je obecně v našem prostředí v plenkách, přestože jejich ohromná síla a efektivnost se už i při počátečních implementačních pokusech výrazně projevila.

- Nedostatečné je povědomí interních vyšetřovacích týmů o použitelnosti a síle digitálních důkazů. Všichni dobře víme, že je (až na výjimky) většina speciálních týmů interní bezpečnosti orientována „klasicky“ – na problematiku fyzické bezpečnosti. Komplexnost interních informací, jejich využitelnost a vysoký potenciál právě pro účely interních šetření, schopnost komplexního posouzení různých zdrojů informací, digitální nevyjímaje, bývá často za hranicemi možností těchto týmů. Tyto nedostatky vyplývají mimo jiného z toho, jak se např. chápou a využívají logy v organizaci – viz výše.

- Mnohaletá zkušenost s realizací bezpečnostních projektů a analýz informačních rizik potvrzuje, že pouze některé organizace mají představu o svých klíčových informačních aktivech, o dalších zdrojích informací, které by mohly sloužit jako digitální důkazy nemluvě. I v případech, kdy takový podrobný asset management existuje, je pouze málo organizací, které jsou schopny dávat veškeré své informace efektivně do souvislostí, např. spojit záznamy z logů, kamerových systémů, ACS a EZS do jedné klíčové informace – např. důkazu o přítomnosti konkrétního zaměstnance na konkrétním pracovním místě.

V podobném výčtu můžeme pokračovat i dále a rozebírat problém do větších a větších detailů. V každé organizaci je situace jiná a jednotlivosti j potřeba posuzovat přísně individuálně.

Závěr

Přes výše uvedené výhody a přínosy se může stát, že Forensic Readiness někoho nemusí vůbec oslovit. Reálná situace v dané organizaci může být taky taková, že není v současné době efektivní se touto problematikou zabývat. Vše skutečně závisí na konkrétní situaci, interních potřebách a možnostech a na externích podmínkách, které nejsou vždy jednoduché.

Jedno bychom si však měli určitě uvědomit. Digitální data, která ve většině organizací již v současné době existují a jsou zpracovávána a ukládána, obsahují nesmírné množství informací o každodenním chodu organizace a o pracovní (a často i mimopracovní) činnosti každého jejího zaměstnance. Je v nich nesmírný potenciál a nevyužité možnosti pro nasazení ještě přesnějších a efektivnějších způsobů řízení organizace. Forensic Readiness je jednou z oblastí, která se účelným využitím takových informací zabývá.

Marián Svetlík
svetlik@rac.cz

Ing. Marián Svetlík

Od ukončení vysokoškolského studia pracoval v různých oblastech IT/IS. Od roku 2000 je vedoucím konzultantem a vedoucím Znaleckého ústavu digitálních forenzních analýz společnosti Risk Analysis Consultants, s.r.o.

POUŽITÉ ZDROJE

[1] ROWLINGSON, R. *A Ten Steps for Forensic Readiness*. International Journal of Digital Evidence, Winter 2004, Volume 2, Issue 3.