Digital Forensics v podnikové sféře

Digital Forensics in the corporate area

Ing. Marián Svetlík, Sr.

Anotace:

Digitální forenzní analýza je oblast forenzní vědy, která má široký přesah i mimo soudní budovy. Její využití v privátní sféře je jedním z mnoha důkazů univerzálnosti jejího použití. Článek se věnuje základním aspektům a důvodům použití digitální forenzní analýzy v každodenním životě organizací.

Annotation:

Digital Forensics is an area of forensic science that has a wide reach outside the courthouse. Its use in the private sphere is one of the many proofs of the universality of its use. The article deals with the basic aspects and reasons for the use of Digital Forensics in the daily life of organizations.

Klíčová slova:

digitální forenzní analýza, digitální informace

Keywords:

digital forensics analysis, digital information

Úvod

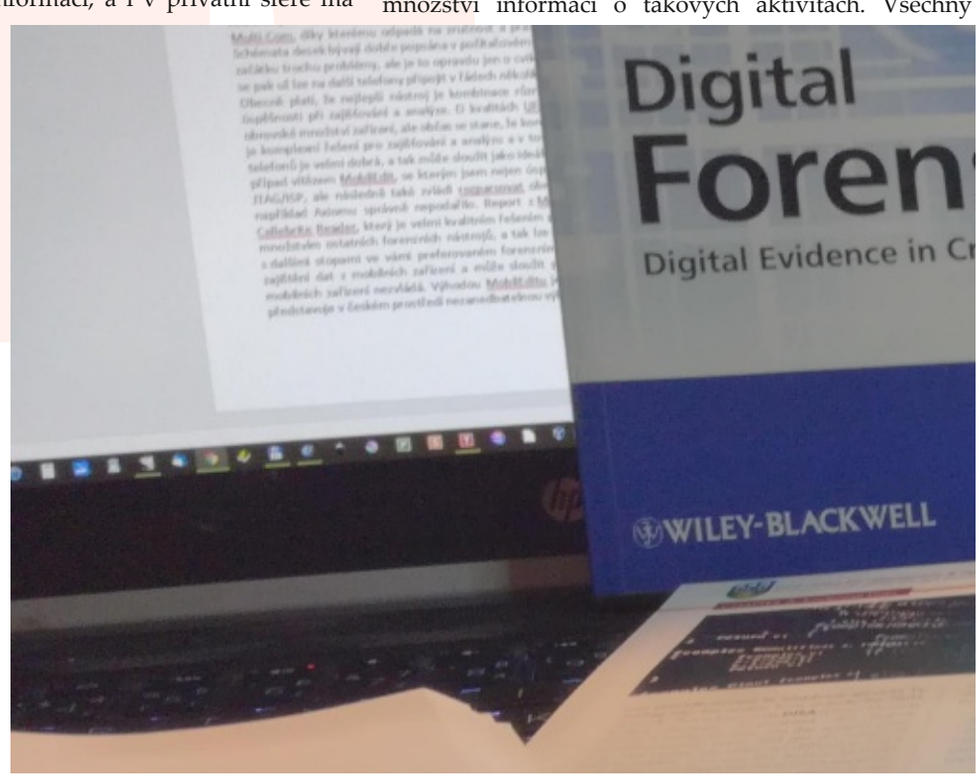
Základní otázkou je, proč a jestli vůbec se zabývat i v privátní sféře problematikou Digital Forensic, jako metodou a nástrojem pro získávání a práci s digitálními důkazy.

Jednoznačnou a jednoduchou odpovědí je skutečnost, že každý rozhodovací proces je uskutečněn na základě dostupných informací, a i v privátní sféře má prakticky každé rozhodnutí i právní dopady. Správnost každého rozhodnutí lze podložit mimo jiného i správností informací, na základě kterých bylo rozhodnutí učiněno.

Asi nejvýraznějším způsobem se to projevuje v případech rozhodnutí, které souvisí s porušením závazných bezpečnostních předpisů a vyvozování důsledků šetření bezpečnostních incidentů. To jsou oblasti, které přímo souvisí s informačními technologiemi a tedy i s digitálními důkazy.

Digitální informace a digitální důkazy

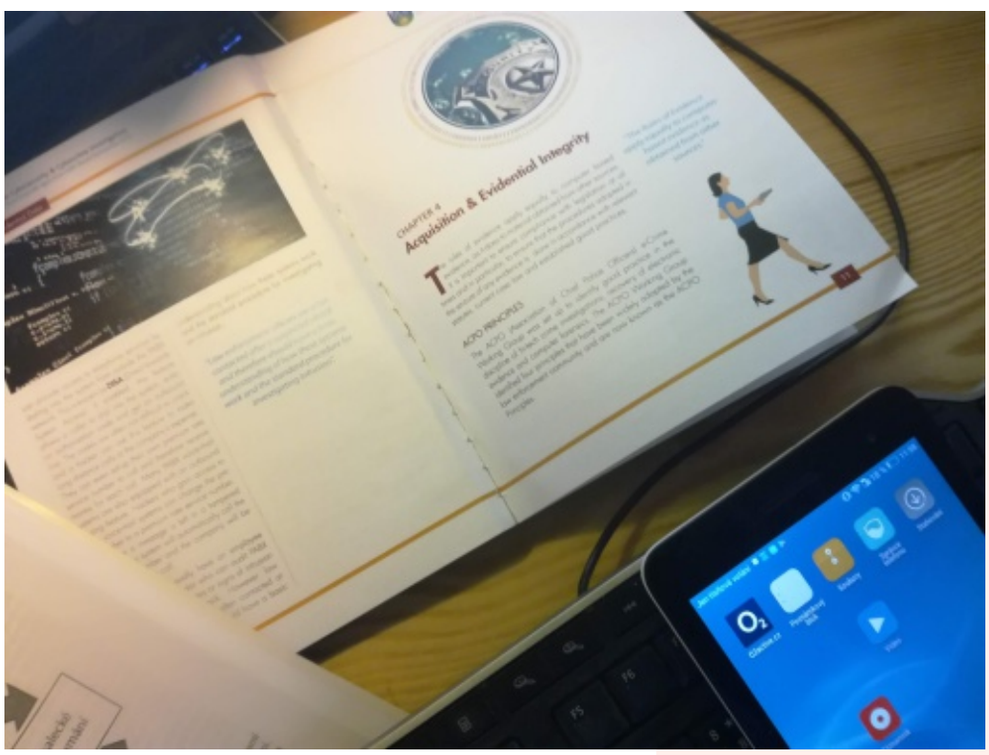
Aktivity každého subjektu společnosti vznikají na základě jeho rozhodovacích schopností. Vzhledem k penetraci elektronických informací ve společnosti vzniká o jeho rozhodnutích a následných aktivitách velké množství informací. Nezávisle na tom, zda aktivity subjektu jsou v zájmu nebo proti zájmům společnosti, v elektronické podobě existuje velké množství informací o takových aktivitách. Všechny



takové informace mohou potenciálně sloužit jako elektronické důkazy.

Jestliže na základě informací dochází k určitému rozhodovacímu procesu, který má vliv na aktivity daného subjektu, je nutné prokázat hodnověrnost takových informací a takové informace se stávají důkazem o opodstatněnosti, ale i o výsledku rozhodovacího procesu. Takové informace (v elektronické podobě) se stávají elektronickými důkazy.

Jestliže subjekt vyvíjí aktivity v souladu se zájmy společnosti, je v jeho zájmu takové aktivity dokumentovat (schraňovat o nich důkazy) pro případ



jakéhokoliv sporu (jak soukromě-právního, tak veřejně-právního charakteru). Znamená to cíleně a vědomě uchovávat (elektronické) důkazy o svých aktivitách ve svém vlastním zájmu. Nicméně při práci s důkazy může potenciálně narazit na určité nejasnosti jak z pohledu procesního (tj jaké informace/důkazy může za jakých podmínek uchovávat a následně jako důkazy použít), ale i z pohledu technologického (tj. jak takové informace/důkazy získávat, uchovávat a pracovat s nimi, aby jejich hodnověrnost, a tedy i důkazní síla byly na odpovídající úrovni).

Znamená to mino jiného, že digitální důkazy jsou podmnožinou obecnější skupiny (digitálních) informací, mající své specifické vlastnosti a specifické způsoby získávání a práce s nimi. Přestože u nás platí, že jako důkaz může být použito cokoli, co přispěje k objasnění sledované skutečnosti, váha (důkazní síla) jednotlivých důkazů se může diametrálně lišit.

Použití metod, nástrojů a postupů z oblasti Digital Forensic je nezbytné k tomu, aby bylo možné (obecné) digitální informace „proměnit" na digitální důkazy, které mají relevanci v rozhodovacích procesech a při řešení právních problémů jak soukromě-právního, tak veřejně-právního charakteru.

Využití digitálních důkazů

Primárním a tím nejlépe viditelným způsobem využití digitálních důkazů jsou reakce na bezpečnostní incidenty, které vznikají v informačním systému. Na základě výsledků šetření bezpečnostního incidentu vzniká nutnost přijmout větší nebo menší množství různých rozhodnutí. Od rozhodnutí organizačního a technického charakteru, až po případná pracovněprávní rozhodnutí nebo i rozhodnutí, která mohou vést k trestněprávním důsledkům.

Nicméně nelze opomenout, že využití digitálních důkazů, jako výsledku implementace procesů a postupů Digital Forensic, je vhodné a dobré použít i v případě řešení jiných oblastí, které nemusí být vůbec spojovány s incidenty v informačních systémech, jak bylo uvedeno výše, např. při řešení interních nebo externích fraudů, porušování závazných interních předpisů a pod.

Implementace Digital Forensic

Jak implementovat v odpovídající míře relevantní doporučení pro práci s digitálními důkazy?

Z pohledu organizačně-procesního je vhodné využít již široce akceptovaná doporučení, která lze shrnout pod pojem "Forensic Rediness". Tady můžu odkázat na dobře a podrobně zpracovanou publikaci "A Ten Step Process for Forensic Readiness, Robert Rowlingson Ph.D (https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf)". Je to základní meto-

dika, ze které pak následně vychází např. i doporučení ISACA "Importance of Forensic Readiness" (https://www.isaca.org/resources/isaca-journal/past-issues/2014/importance-of-forensic-readiness).

Z pohledu organizačně-technického se jako vhodné jeví širší implementace doporučení, které vycházejí z řady norem ISO/IEC 27 000, týkající se obecně zajištění bezpečnosti informací, pro tuto oblast specificky normy ISO/IEC 27 037.

Z obecného pohledu se jeví v této fázi jako podstatné:

- Zvýšit povědomí (napříč organizací, ale zejména v oblastech, které mají přímý vztah k IS - např. útvary informační bezpečnosti, operačních rizik, interního auditu) o rozdílech mezi obecnou digitální informací a digitálním důkazem. Přestože v našem právním řádu lze za důkaz považovat cokoli, co pomůže objasnit sledovanou skutečnost, v interním zájmu organizace je maximalizovat váhu takového důkazu. Znamená to přidat obecné digitální informaci další parametry, kterými jsou hodnověrnost, integrita, autentičnost, relevantnost, spolehlivost a další. Právě postupy a metody Digital Forensic jsou zaměřeny na zvýšení důkazní síly digitálních důkazů.
- Pravidelně proškolovat relevantní pracovníky o principech práce Digital Forensic. Odstupňovat hloubku a zaměření školících aktivit podle míry uplatnění metod Digital Forensic v jejich konkrétních náplních činnosti.
- U pracovníků, kteří přicházejí přímo do styku s digitální informací (zejména těch, kteří např. přímo řeší bezpečnostní incidenty), pomocí školení a praktických cvičení zajistit praktické dovednosti nutné pro zajišťování digitálních důkazů, a to až do úrovně získání odpovídající kvalifikace pro práci s digitálními důkazy (až na úrovni získání certifikace pro danou činnost, nejméně na úrovni certifikovaného zajištění digitálních důkazů - „Certified First Responder" např. v intencích ISO/IEC 27037).
- Implementovat principy Digital Forensic do interních předpisů organizace tak, aby se na relevantních místech předpisové základny staly integrální součástí metod a postupů práce.
- Snažit se zajistit takovou změnu v interních procesech práce s digitální informací, aby již při vzniku důležité digitální informace tato měla alespoň některé základní atributy digitálního důkazu. Jako příklad může být zajištění integrity a autentičnosti – použitím např. elektronického podpisu (nebo alespoň určitého ekvivalentu - hash a timestamp) už při vytváření a následně při práci s vybranými bezpečnostně relevantními informacemi.

Z konkrétního pohledu se jeví v této fázi jako podstatné:

Implementovat do praxe relevantních pracovníků (zejména těch, kteří přímo řeší bezpečnostní incidenty) proces samotného zajištění digitálních důkazů způsobem, který zajišťuje vysokou důkazní sílu takových důkazů. K tomu:

- Proškolit vybraný personál tak, aby získal vědomosti, znalosti a dovednosti k výkonu pozice „Digital Evidence First Responder" v intencích požadavků normy ISO/IEC 27 037.
- Pravidelně udržovat získanou kvalifikaci a rozšiřovat ji na základě nových poznatků a technologií.
- Zajistit odpovídající programové a technické vybavení tak, aby bylo možné kvalitně na odpovídající úrovni zajišťovat digitální důkazy.

Závěr

Implementace metod, procesů a prostředků Digital Forensic do bezpečnostní praxe organizace přináší významnou podporu pro rozhodovací procesy organizace a důvěru v jejich opodstatněnost.

Většina rozhodujících informací v organizaci, na základě kterých jsou přijímaná různá rozhodnutí, jsou informace digitální. Posílení hodnověrnosti takových informací jejich získáním a zpracováním ve formě digitálních důkazů, posílí důvěryhodnost a opodstatněnost takových rozhodnutí. Ať už jsou to rozhodnutí organizačně-provozního charakteru, ale zejména rozhodnutí, která mají pracovně-právní charakter nebo taková, která mohou vést až k trestněprávním důsledkům.

***Ing. Marián Svetlík, Sr.**, soudní znalec, pracuje jako specialista na digitální forenzní analýzu Czech Cybercrime Centre of Excellence na Masarykově univerzitě v Brně, přednáší informační bezpečnost a počítačovou kriminalitu na vysokých školách. Je šéfredaktorem časopisu Digital Forensic Review, členem řídícího výboru Institutu pro Digitální Forenzní Analýzu, podílí se na mezinárodních projektech spojených s problematikou Digital Forensic a Cybercrime.*


FORENSIC
IMAGE AND VIDEO
ENHANCEMENT
AMPED
FIVE
THE COMPLETE SOFTWARE SOLUTION
PROCESS AND ANALYZE DIGITAL IMAGES FROM CCTV, BODY WORN CAMS, MOBILE PHONES, DRONES, LATENT FINGERPRINTS, AND MORE
SCIENTIFIC WORKFLOW DRIVEN BY FORENSIC NEEDS
Distribuci, prodej a školení v ČR a SR zajišťuje:
FIREWIRE REVOLUTION
We Secure your World
FIREWIRE REVOLUTION EU
by forensee
Belgická 19
120 00 Praha 2
www.firewire-revolution.eu
info@firewire-revolution.eu
+420 315 55 88 70
forensee
digital forensics