Ing. Miroslav Čermák
Policejní akademie České republiky v Praze
student doktorského studia

Úskalí zajišťování digitálních stop v případě podezření na trestný čin neoprávněného přístupu k počítačovému systému

Na prvním místě je třeba uvést, že tento příspěvek vznikl na základě pozorování chování zaměstnanců ve vybraných organizacích a praktických zkušeností s vyšetřováním několika desítek případů týkajících se neoprávněného přístupu k počítačovým systémům a nosiči informací dle § 230 Zákona č. 40/2009 Sb., trestní zákoník, zkr. TZ ze strany ze strany zaměstnanců organizací působících v soukromém sektoru. Příspěvek se snaží poukázat především na některé sporné momenty v dosavadní kriminalistické praxi, kdy může dojít přílišným lpěním na stávajících a neaktualizovaných postupech k pochybení, neboť některé tradiční způsoby zajištění digitálních stop selhávají, a je třeba učinit závažná rozhodnutí, aby nevznikla další škoda nebo nebyly zničeny důkazy. Ambicí tohoto příspěvku není, a ani nemůže být vzhledem k jeho omezenému rozsahu popis detailního postupu policisty provádějícího trestní řízení, který se navíc případ od případu liší a musí se i aktualizovat s ohledem na vývoj situace v kyberprostoru.

Trestné činy, při kterých dochází k neoprávněnému přístupu do informačního systému, mají jedno společné: vše zpravidla začíná oznámením na podezření ze zneužití přístupu k počítačovému systému a nosiči informací, kdy v informačním systému společnosti byly zjištěny neautorizované operace, a zaměstnanec, pod jehož profilem byly tyto operace provedeny, tvrdí, že on je neprovedl, že to musel udělat někdo jiný, nejspíš hacker, který jeho přihlašovací údaje získal a následně zneužil. V takových případech **je nutné prověřit hned několik kriminalistických verzí**, především zda dané operace v systému nemohl provést:

1. samotný zaměstnanec, protože teprve až když se na to přišlo, tak začal tvrdit, že on to neudělal;
2. někdo z jeho kolegů, který odpozoroval jeho přihlašovací údaje a pak je zneužil;
3. někdo blízký danému zaměstnanci, např. manžel, přítel, syn, dcera apod. za předpokladu, že by zaměstnanec do systému přistupoval i z domova;
4. klient či jiná osoba, se kterou zaměstnanec přichází do styku, a to aniž by si to zaměstnanec uvědomoval, např. když se připojuje do systému na veřejnosti;
5. útočník z internetu, který nějakým způsobem získal přihlašovací údaje zaměstnance a pak se do systému přihlásil.

Všechny tyto kriminalistické verze je nutné prověřit. Jediné, co je na samém počátku vedení trestního řízení zpravidla známo, že údajně došlo k neoprávněnému přístupu do systému, ale není už známo, jakým způsobem. To, zda došlo k překonání nějakých bezpečnostních opatření organizační a technické povahy, a dále zda došlo k následnému narušení:

- důvěrnosti dat, kdy k nim získala přístup neoprávněná osoba;
- integrity dat, kdy došlo k jejich nežádoucí změně;

- dostupnosti systému, kdy byl oprávněné osobě odepřen přístup;
- užitečnosti systému, kdy systém nereagoval tak, jak by měl;
- nepopiratelnosti, kdy se uživatel mohl vzdát odpovědnosti;
- vlastnictví, resp. získání výhradní kontroly nad provozovaným systémem;

je nutné prověřit. Ve výše uvedených případech se jedná v zásadě o narušení základních atributů bezpečnosti tak, jak je definuje Parkerian hexad model[1] přičemž k onomu získání přihlašovacích údajů mohlo dojít několika různými způsoby:

- prostému odpozorování přihlašovacích údajů oběti (zde by se pachatel musel dostat do bezprostřední blízkosti oběti), ale opět je zde několika možných technik typu shoulder surfing,[2] které pachatel mohl použít;
- zaznamenání přihlašovacích údajů pomocí HW keyloggeru[3] (zde by se pachatel muset dostat osobně přímo k samotnému zařízení);
- instalací SW keyloggeru[4] (kterýžto mohl být obsažen v příloze e-mailu anebo stažen z internetu uživatelem ve formě trojanizované aplikace[5] anebo při surfování po napadených webových stránkách, na kterých byl umístěn škodlivý kód, jedná se o tzv. základní vektory útoku);
- hackingu, kdy útočník zneužil známé nebo zcela nové zranitelnosti, odchytil heslo přenášené po síti, zadávané do aplikace, uložené v paměti nebo v databázi.

Ve všech případech je nutné tuto hypotézu podporující danou kriminalistickou verzi prověřit, aby ji bylo možné buď potvrdit anebo vyvrátit. Vzhledem k tomu, že dvě z posledně uvedených kriminalistických verzí připouští, že k získání přihlašovacích údajů může dojít prostřednictvím škodlivého kódu, či hackingu, tak **je nutné zjistit, zda útok dále neprobíhá a nemůže dojít k dalšímu narušení bezpečnosti a vzniknout ještě větší škoda**. Zde je třeba si uvědomit, že proti sobě často stojí dva zcela protichůdné požadavky a to požadavek na:

- okamžité zajištění kontinuity podnikání z důvodu škody plynoucí ze ztráty produktivity a obchodní příležitosti, kdy zpravidla dochází k okamžitému zásahu ze strany IT[6] oddělení společnosti nebo třetí strany, se kterou je uzavřena smlouva k obnově systému ze záloh a tím nevratnému zničení digitálních stop;
- vyšetření toho, co se stalo a jak se to stalo, aby se této situaci dalo předcházet, a aby se v budoucnu neopakovala. To ovšem vyžaduje zajištění prostředků výpočetní techniky, jejich prohlídku a zajištění digitálních stop. S tím je však spojeno odpojení těchto prostředků od sítě a ty se stávají pro zaměstnance dané společnosti a jejich klienty dočasně nedostupné.

---

[1] PENDER-BEY, Georgie. *The parkerian hexad* [online]. 4. květen 2012. Získáno z: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

[2] WINKLER, Ira. The threat of shoulder surfing should not be underestimated. *CSO Online* [online]. 13. leden 2016 [vid. 27. květen 2019]. Získáno z: https://www.csoonline.com/article/3021882/the-threat-of-shoulder-surfing-should-not-be-underestimated.html

[3] Zařízení připojené na konektor klávesnice nebo vložené přímo do klávesnice, které zachytává stisknuté klávesy.

[4] Aplikace, která zachytává stisknuté klávesy a ukládá je do souboru na počítači.

[5] Aplikace, která na pozadí vykonává bez vědomí uživatele škodlivou činnost.

[6] Informační technologie, zkr. IT někdy též informační a komunikační technologie, zkr. ICT.

Policista provádějící trestní řízení by měl proto vždy zvážit, dle povahy útoku, jaké prostředky výpočetní techniky je třeba zajistit, a jakým způsobem z nich digitální stopy získat. Jde o to, aby nezajišťoval větší než nezbytně nutné množství prostředků výpočetní techniky a dat. Je třeba si uvědomit, že **jen pořízení bitové kopie disku znamená pro napadenou organizaci nedostupnost v řádu několika hodin a to u některých typů organizací, kde se průměrný denní obrat pohybuje v řádu miliónů korun**, může znamenat podstatný výpadek v příjmech.

Spolupráce s experty

Policista provádějící trestní řízení, dále jen policista, byť je při svém šetření veden snahou vyšetřit, jak k trestnému činu došlo, a dopadnout pachatele, tak **by měl zároveň brát v úvahu i aktuální výši škody a rovněž i potenciální škodu, která může jeho konáním/nekonáním vzniknout**, a s tím i související poškození dobrého jména policie ČR. To, když bude postupovat neadekvátně dané situaci, a způsobí organizaci ještě větší škodu. Vzhledem k tomu, že situace v kyberprostoru se neustále mění a techniky útoků se zdokonalují, tak policista nebude vždy disponovat takovými znalostmi z oboru kybernetické bezpečnosti, aby se obešel bez spolupráce ostatních expertů, proto by měl v mnoha případech využít znalostí:

- útvaru IT dané organizace nebo třetí strany, protože útvar IT systém ví, resp. měl by vědět, jakým způsobem napadený systém funguje, jaká technická bezpečnostní opatření obsahuje, a jaká je jejich účinnost. Zde je třeba si dát pozor na to, že IT, ať už interní nebo externí, si může být vědomo určitého pochybení při správě informačního systému, neadekvátních bezpečnostních opatření a dalších selhání a může o této skutečnosti taktně pomlčet a nemusí kriminalistovi poskytnout úplné a pravdivé informace, a v některých případech se může pokusit i zničit digitální stopy.
- CSIRT týmu,[1] který má zpravidla velice dobrý přehled o situaci v kyberprostoru, aktuálních hrozbách, zranitelnostech a používaných vektorech útoku, škodlivých kódech a tzv. indikátorech kompromitace, a může tak svým expertním názorem podstatně přispět k sestavení kriminalistických verzí, jejich zpřesnění a stanovení nejpravděpodobnějších scénářů útoku.
- Expertů – forenzních analytiků, kteří jsou schopni provést forenzní analýzu počítače a odhalit či vyloučit přítomnost škodlivého kódu a popsat jeho fungování, což opět umožňuje potvrdit či vyloučit danou kriminalistickou verzi.

Zajištění digitálních stop a minimalizace dalších škod

Vzhledem k tomu, že ze všeho nejdůležitější je vyloučení přítomnosti škodlivého kódu v systému, a v případě, že je nalezen, tak jeho izolaci a zabránění dalšímu šíření, je nutné začít jako první prověřovat tyto kriminalistické verze. A protože se **v kyberprostoru stále více setkáváme s tzv. bezsouborovým škodlivým kódem**

[1] Computer Security Incident Response tým je organizovaná skupina osob v organizaci, která jako první reaguje na incident nebo útok, kdy došlo nebo hrozí narušení bezpečnosti a tedy i zájmu chráněného TZ.

(fileless malware[1]), který se zpravidla nachází jen ve volatilní paměti počítače a v okamžiku, kdy dojde k jeho vypnutí, což je zase nezbytné pro pořízení bitové kopie disku, tak je tento kód nenávratně ztracen, tak se jako první nabízí pořízení dumpu paměti.[2] Ovšem ani to není zcela bez rizika, protože zde existují v zásadě jen dvě možnosti:

- zmrazení paměti, vyjmutí a bezprostřední připojení do speciálního zařízení a zkopírování jejího obsahu, což je velice riziková aktivita, která byť byla mnohokrát demonstrována na nejrůznějších hackerských konferencích, tak v reálné praxi selhává, neboť hrozí poškození samotné paměti a především ztráta dat, takže ji nelze doporučit,
- spuštění speciální aplikace, která provede tzv. dump paměti. Jinými slovy zapíše její obsah na externí paměťové médium a umožní její pozdější analýzu. Tato operace je sice podstatně méně riziková než předchozí, ovšem také není zcela bez rizika, neboť ona aplikace musí v paměti též vytvořit proces, a v tu chvíli může být škodlivým kódem, rovněž běžícím v paměti, detekována a proces pořizování dumpu paměti tak může být negativně ovlivněn, např. část paměti se nemusí zkopírovat, škodlivý kód se může ukončit apod.

Poté, co je pořízen dump paměti, tak by měl být pořízen obraz disku, neboť se na něm mohou nacházet smazané soubory, malware a logy, pomocí kterých lze zpětně rekonstruovat činnost uživatele v systému. **Jako první je třeba zjistit, zda k útoku došlo prostřednictvím malware, anebo nikoliv, protože v okamžiku, kdy by tomu tak bylo, tak by pachatel mohl ve své činnosti pokračovat a napadat další stroje v síti**.

Vyslovení závěru, zda s určitou jistotou došlo k napadení koncového zařízení malwarem a zda se na něm nenachází škodlivý kód, by mělo být možné nejdříve po analýze dumpu paměti a s jistotou pak po analýze image disku,[3] neboť malware nemusí být v paměti přítomen. To však musí provádět zkušený forenzní analytik, protože vyžaduje hluboké znalosti operačního systému a jeho detailního fungování. (**Komerční firmy specializující se na analýzou malware jsou schopny poskytnout informaci ohledně přítomnosti malware za ideálních podmínek nejdříve za 24 hodin.** Alespoň to vyplynulo z výsledku RFP,[4] kdy byly autorem této práce v rámci výzkumu osloveny největší antivirové společnosti působící v ČR.)

Další naprosto zásadní problém, který musí policista na místě vyřešit, je zda odpojit počítač od počítačové sítě či nikoliv. Zatímco odpojení počítače od zdroje napájení není doporučováno a správný postup má již policista šetřící kybernetickou kriminalitu zažitý, tak **zde není rozhodnutí ohledně odpojení, či neodpojení tak jednoznačné a není ani součástí běžně používaných metodik a postupů**. Je tomu tak proto, že

[1] ČERMÁK, Miroslav. Fileless neboli bezsouborový malware - CleverAndSmart [online]. 14. duben 2019 [vid. 13. květen 2019]. Získáno z: https://www.cleverandsmart.cz/fileless-neboli-bezsouborovy-malware/

[2] Dump paměti je specifický postup, při kterém dochází k pořízení bitově shodné kopie volatilní paměti, jež k uchování informací musí být připojená ke zdroji energie.

[3] Image disku je přesná bitová kopie disku, která může být při dodržení postupů použita jako důkaz.

[4] Request for Proposal neboli žádost o nabídku.

- se objevují škodlivé kódy, které sledují, zda je na daném stroji dostupná síť, např. Google, O365, Wikipedie a další služby, které běžně dostupné jsou a jejichž absence zpravidla znamená, že **počítač není připojen v síti anebo se nachází v nějakém izolovaném testovacím prostředí a pro malware je to jasný pokyn, aby se nijak neprojevoval**, a nadále zůstal v latentní fázi,
- hrozí, že pokud **k odpojení od datové sítě nedojde, tak mohou být z daného počítače napadány další stroje v síti anebo z něj mohou odcházet citlivá data**, osobní údaje, informace, které jsou součástí obchodního tajemství a informace zajišťující dané organizaci strategickou konkurenční výhodu.

Jako řešení se nabízí přepojit PC na dobu nezbytně nutnou do tzv. karanténní VLANy. Ta se však běžně nedělá, taková VLAN[1] není k dispozici a není to součástí běžných postupů. Tím by měl být malware, pokud se na daném PC skutečně nachází, zůstat nadále aktivní, takže by mělo být možné jej detekovat a zároveň zde nehrozí vznik další škody. Po pořízení dumpu paměti je možné počítač regulérním způsobem vypnout. I zde však hrozí riziko, že:

- **při regulérním vypnutí dojde k aktivaci rutiny, která nevratně smaže data**. Jako řešení se tak nabízí ukončit regulérně pouze běžící aplikace a následně počítač vypnout natvrdo. Tímto nečekaným vypnutím nebude moci být aktivována rutina likvidující data,
- **v okamžiku, kdy bude počítač opět zapnut, tak se stejně tak může spustit rutina, která zjistí, že počítač nebyl regulérně vypnut a provede smazání příslušných dat**. Proto by měl být po vypnutí počítače disk vymontován a pořízena jeho bitová kopie.

Byť může být v počítači umístěn kód pověšený na události open, close nebo startup a shutdown,[2] tak stejně tak je nutné počítat i s HW zařízením, které může rovněž v okamžiku odpojení zařízení od zdroje elektrického napětí aktivovat ochranu vedoucí k naprosté likvidaci veškerých dat na samotném zařízení za použití tzv. degausseru,[3] který může mít podobu HW karty nebo samostatného modulu umístěného uvnitř počítače, přičemž tento modul může být aktivován i na dálku. Nutno podotknout, že tyto moduly byly nalezeny jen u vysoce organizovaných skupin páchajících kybernetickou kriminalitu a operujících v různých částech světa, a rozhodně se nejedná o nějakou masivně používanou záležitost. Nicméně i s tímto by měl policista vyšetřující závažnou kybernetickou kriminalitu počítat, neboť tato technologie je dostupná, není finančně náročná a není používána spíš proto, že o této možnosti pachatelé páchající trestnou činnost moc nevědí.

Ohledání místa činu

Z výše uvedeného důvodu a nejen proto, je vhodné provést i klasické ohledání místa činu a samotných PC. Ohledání je vhodné provádět koncentricky tak, jak jej

[1] Virtuální síť oddělená od zbytku sítě, ale disponující určitou nezbytnou konektivitou.
[2] Jedná se o kontrolu stavu např. otevření a zavření konkrétního souboru nebo spuštění a vypnutí počítače.
[3] Degausser generuje silné magnetické pole, které zničí veškerá data v paměti a na disku.

doporučuje Němec,[1] a dostatečnou pozornost věnovat i uspořádání a vybavení jednotlivých pracovišť, možnostem pohybu osob na pracovišti a v nejbližším okolí, především pak možnostem manipulace s prostředky výpočetní techniky za účelem získání přihlašovacích údajů a jejich možného pozdějšího zneužití. Pokud je pracoviště vybaveno kamerovým systémem, je vhodné zajistit i záznamy z daného kamerového systému. Poté by měl následovat i výslech svědků.

Je vhodné pořídit fotografické snímky místa činu, a to orientační, přehledové, polodetailní a detailní a provést náčrtek rozmístění jednotlivých pracovišť, které může hrát významnou roli, obzvláště pak v moderních kancelářských budovách organizací, kde zaměstnanci nemají samostatné kanceláře, ale sedí v tzv. open spacech, kdy jednotlivá pracoviště od sebe nejsou fyzicky oddělena a dost často se mezi nimi nachází jen sklo a žaluzie, takže i počet možných pachatelů z řad kolegů je výrazně vyšší, neboť v open spacech, které jsou volně přístupné, jsou umístěny stovky až tisíce počítačů, které jsou obsluhovány přibližně stejným počtem zaměstnanců.

V případech kancelářských budov pak zpravidla bývá minimálně celá jedna stěna několika patrové budovy prosklená a dostupná z ulice. Horizontálně se zatahující vnitřní žaluzie, které bývají umístěny na prosklené vnitřní stěně, jsou zpravidla pootočeny tak, aby dovnitř pronikalo maximum denního světla, a nezabraňují pohledu dovnitř pobočky z prostor ulice přístupné veřejnosti. S těmito žaluziemi se rovněž nemanipuluje, a bývají ponechány v poloze, v jaké se nacházejí v okamžiku prvotního ohledávání místa činu.

Výše uvedenou skutečnost lze potvrdit opakovaným ohledání místa činu, kdy lze zjistit, že se žaluzie nachází ve stále stejné poloze. Toto zjištění je důležité, neboť výše uvedená skutečnost **umožňuje neoprávněné osobě odpozorovat přihlašovací údaje zadávané zaměstnancem pobočky anebo si celou přihlašovací sekvenci nahrát a později analyzovat**. Odpozorovat přihlašovací sekvenci zaměstnance tak může jak klient, tak i samotný zaměstnanec, který pak tyto údaje může i později zneužít. Experimentálně bylo ověřeno, že videosekvence zachycující přihlášení do Windows lze snadno pořídit a stejně tak i přihlašovací sekvence do mobilních zařízení.

Klientská zóna bývá běžně vybavená standardním kancelářským nábytkem (stůl, kolečkové křeslo a židle pro klienta, nacházející se přes stůl, takže klientský pracovník a klient sedí naproti sobě. **Klient nevidí na obrazovku monitoru klientského pracovníka, ovšem vidí na klávesnici, takže má možnost zachytit, jaké heslo je použito pro přihlášení.** (Zde je třeba si uvědomit a pozorování na místě tuto domněnku opět potvrzuje, že v okamžiku, kdy klientský pracovník odchází od počítače a jde tisknout např. smlouvy, tak obrazovku počítače uzamyká a stejně tak ji odemyká, v případě, že dojde k jejímu uzamčení po určité době nečinnosti, cca 15 minut. K tomu dochází, když na počítači nepracuje a komunikuje s klientem, kterému např. něco vysvětluje a ukazuje na tabletu. Klientský pracovník tak opakovaně před klientem zadává své heslo do systému, a klient tak má možnost heslo odpozorovat.)

Každé klientské pracoviště bývá vybaveno standardní výpočetní technikou (PC nebo notebook, dokovací zařízení, externí monitor, klávesnice a myš) a nachází se v otevřeném prostoru, tzv. openspace, kdy jednotlivá pracoviště od sebe nejsou

[1] NĚMEC, Miroslav. *Kriminalistická taktika pro policisty a studenty Policejní akademie České republiky v Praze*. Praha, ABOOK, s. r. o., 2017. ISBN 978-80-906974-09.

fyzicky oddělena a to ani skříněmi nebo paravanem a jen jedno pracoviště, kde sedí manažer pobočky, se zpravidla nachází v samostatné místnosti, která je od okolního prostoru oddělena skleněnou přepážkou s dveřmi a vertikálně stahovacími mezi-okenními žaluziemi, které byly v okamžiku ohledání místa činu vytažené. V mnoha případech z výslechů později vyplynulo, že tak jsou vytaženy trvale a není s nimi manipulováno. To potvrdilo i opakované ohledání místa činu. Existuje zde tak možnost odpozorovat heslo a to jak ze strany klienta, tak i ze strany jiného zaměstnance.

Při ohledání výpočetní techniky je nutné prověřit jak hmotné stopy (neautorizovaný zásah do HW), tak i stopy nehmotné (neautorizovaný zásah do SW a dat.), tak jak uvádí Němec.[1] Výpočetní technika (desktopy, notebooky, tiskárny) bývá do sítě zpravidla připojena prostřednictvím ethernet kabelu CAT 5, který je zpravidla veden podlahou do/z raku umístěného v technické místnosti pobočky. Kromě metalické sítě se na pobočce nachází rovněž i bezdrátová Wi-Fi síť, využívaná především pro přístup do sítě z firemních tabletů, notebooků a chytrých telefonů využívaných zaměstnanci.

Na místě je vhodné zjistit, zda kromě firemní sítě není dostupná i jiná **bezdrátová síť**, ke které by se mohl zaměstnanec připojit. Téměř vždy lze detekovat větší počet bezdrátových sítí provozovaných ostatními organizacemi sídlícími na stejné adrese a v nejbližším okolí. **Ohledáním chytrých telefonů, tabletů a notebooků na místě lze zjistit, k jaké síti jsou tato zařízení aktuálně připojena a rovněž k jakým sítím se zaměstnanci připojují a využívají je**, především v okamžiku, kdy si potřebují vyřídit nějakou soukromou záležitost, což jim zaměstnavatel umožňuje. Nelze totiž vyloučit, že by k jejich napadení mohlo dojít i z těchto sítí.

Vzhledem k tomu, že zaměstnanci se mohou hlásit z jakéhokoliv počítače, a není možné zajistit všechny počítače, **musí policista nejprve zjistit, z jakých počítačů se zaměstnanec s daným uživatelským profilem hlásil**. Tyto informace lze dohledat v logu doménového kontroléru[2] (domain controller, zkr. DC), těch může být několik. A pokud nejsou záznamy posílány do řešení centrálního monitoringu, je nutné je všechny prohledat. **Následně pak je nutné zajistit všechny počítače, ze kterých se uživatel přihlašoval. Tyto počítače by pak měl policista zajistit a provést jejich ohledání, dump paměti a image disku.**

Zde je nutné ověřit, zda mohla neoprávněná osoba, bez toho aniž by si toho někdo všiml, s danými PC manipulovat, tj. zda jsou zařízení pevně spojena např. lankem se stolem, a kde jsou umístěna. Prověrkou na místě je možné zjistit, zda je manipulace s prostředky výpočetní techniky možná. Např. pokud by to bylo možné jen přemístěním se pod stůl, což je natolik velká změna v poloze těla, tak by tuto aktivitu měla např. kamera pokrývající celý prostor, zaznamenat. Stejně tak v případě, kdy by se útočník pokusil dané zařízení odnést, např. v době polední přestávky, po pracovní době či o víkendu a zasáhnout do jeho konfigurace.

Stejně tak by mohl být připojen **HW keylogger** přímo na USB sběrnici a vzhledem k tomu, že zařízení zpravidla bývá umístěno pod stolem, tak by si tohoto HW

[1] NĚMEC, Miroslav. *Teorie a metodologie kriminalistiky pro magisterské studium. I. díl*. Praha: ABOOK, s. r. o., 2018. ISBN 978-80-906974-1-6.

[2] Server v prostředí Windows, na kterém jsou uložena jména a hesla a vůči kterému probíhá přihlašování a vytváří se auditní logy.

keyloggeru nemusel ani nikdo všimnout. Obzvlášť v případě použití miniaturního HW keyloggeru[1] o velikosti cca 2 cm umístěného mezi male (samčí) USB konektor klávesnice a female (samičí) konektor PC kdykoliv v minulosti, který navenek vypadá jako nedílná součást stávajícího konektoru, a který po sobě nezanechává žádné digitální stopy. Tuto verzi je možné potvrdit jedině analýzou záznamů z kamer, pokud jsou k dispozici.

Pokud zaměstnanci kromě PC, na kterém běží zpravidla OS Microsoft Windows a balíku MS Office, přístupu do cloudu O365 a používají i telefon a tablet s operačním systémem Google Android či iOS a do něj se přihlašují stejným heslem jako do počítače, tak je teoreticky možné vést na toto zařízení tzv. šmouhový útok,[2] ale tento vektor útoku není moc pravděpodobný, protože vzhledem k použití komplexního hesla by tento útok neměl moc velkou šanci na úspěch. Policista by se proto měl zajímat o platnou politiku hesel v dané organizaci, jeho délku, komplexitu, dobu platnosti a možnosti použití stejného hesla na dalších systémech. Nicméně i přes restriktivní politiku zde existuje **možnost zadávané heslo odpozorovat,**[3] a pokud je stejné jako do PC, pak jej útočník může použít k přihlášení.

Dále je vhodné prověřit, jaké jsou u jednotlivých počítačů klávesnice a jaké jeví známky opotřebení. Byly zaznamenány případy, kdy klávesnice byla vyměněna za stejný model, ovšem s integrovaným HW keyloggerem. Pokud jsou použity na první pohled již dlouho používané klávesnice, tak je tato pravděpodobnost nižší. V rámci průzkumu jsme zjistili, že zaměstnanci si všimnou, když jim klávesnici někdo vymění a to dokonce i když je použitá. V každém případě je třeba provést ohledání a prověřit, zda klávesnice byla rozšroubována, zda je na šroubech zřetelná známka po šroubováku či nikoliv.

Manipulaci s elektronikou klávesnice a zvedení cizorodého prvku pak lze vyloučit i díky souvislé a ničím neporušené vrstvě prachu, která by byla v případě umístění HW keyloggeru narušena. Obdobné zjištění lze učinit i se samotným PC, do kterého by rovněž mohl být umístěn HW keylogger. Tímto způsobem je možné tyto kriminalistické verze vyloučit. Analýzou dumpu paměti a image disku by pak mělo dojít i k vyloučení přítomnosti škodlivého kódu na zařízení a jedinou verzí, se kterou je nutné pak dále pracovat, by mělo být odpozorování a zneužití hesla.

Zde je nutné detailně prověřit logy všech zařízení a sestavit časovou osu, aby bylo zřejmé, kdo a kdy na nich pracoval a provést korelaci s ostatními logy, sestavit psychobehaviorální profil všech uživatelů daných počítačů, kteří na nich pracovali, provést korelaci s ostatními událostmi a přiřadit záznamy v logu konkrétní osobě, což je časově nejnáročnější část forenzní počítačové analýzy.

---

[1] HW Keylogger: nejsnadnější způsob získání hesla - SOOM.cz [online]. [vid. 15. duben 2019]. Získáno z: https://www.soom.cz/clanky/1166--HW-Keylogger-nejsnadnejsi-zpusob-ziskani-hesla

[2] ČERMÁK, Miroslav. Chytré telefony a smudge attack - CleverAndSmart [online]. 10. únor 2011 [vid. 15. duben 2019]. Získáno z: https://www.cleverandsmart.cz/chytre-telefony-a-smudge-attack/

[3] ČERMÁK, Miroslav. Chytré telefony a shoulder surfing attack. *CleverAndSmart* [online]. 14. červenec 2011 [vid. 1. květen 2019]. Získáno z: https://www.cleverandsmart.cz/chytre-telefony-a-shoulder-surfing-attack/

Závěr

Při šetření trestných činů neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 TZ musí policista prověřovat především digitální stopy. V okamžiku, kdy je pachatel neznámý, tak ani jiné stopy nemá.

Policista by měl **vždy zvážit, jaké prostředky výpočetní techniky je nutné zajistit, zda provede jejich odpojení od datové sítě, jakým způsobem provede pořízení obrazu paměti a disku** s cílem co nejrychleji zajistit digitální stopy, minimalizovat škody a vyloučit či potvrdit přítomnost malware. Neměl by však ignorovat ani klasické stopy, které mu mohou pomoci vyloučit některé kriminalistické verze.

V dalším výzkumu by bylo vhodné se zaměřit na:

- možnost neinvazivního získávání dumpu paměti a to oběma metodami zmíněnými v článku;
- připravení karanténní VLAN s limitovanou konektivitou do internetu a monitorováním datového toku od třetí vrstvy výše, aby případný pokus o únik citlivých informací mohl být detekován a zároveň bylo možné sledovat chování malware, pokud by se na daném zařízení nacházel;
- výběr nástroje pro automatické generování časové osy zachycující práci více uživatelů na jednom a více strojích.

Literatura

ČERMÁK, Miroslav. Chytré telefony a shoulder surfing attack. *CleverAndSmart* [online]. 14. červenec 2011 [vid. 1. květen 2019]. Získáno z: https://www.cleverandsmart.cz/chytre-telefony-a-shoulder-surfing-attack/

ČERMÁK, Miroslav. Chytré telefony a smudge attack - CleverAndSmart [online]. 10. únor 2011 [vid. 15. duben 2019]. Získáno z: https://www.cleverandsmart.cz/chytre-telefony-a-smudge-attack/

ČERMÁK, Miroslav. Fileless neboli bezsouborový malware - CleverAndSmart [online]. 14. duben 2019 [vid. 13. květen 2019]. Získáno z: https://www.cleverandsmart.cz/fileless-neboli-bezsouborovy-malware/

HW Keylogger: nejsnadnější způsob získání hesla - SOOM.cz [online]. [vid. 15. duben 2019]. Získáno z: https://www.soom.cz/clanky/1166--HW-Keylogger-nejsnadnejsi-zpusob-ziskani-hesla

NĚMEC, Miroslav. *Kriminalistická taktika pro policisty a studenty Policejní akademie České republiky v Praze*. Praha: ABOOK, s.r.o., 2017. ISBN 978-80-906974-09.

NĚMEC, Miroslav. *Teorie a metodologie kriminalistiky pro magisterské studium. I. díl*. Praha: ABOOK, s.r.o., 2018. ISBN 978-80-906974-1-6.

PENDER-BEY, Georgie. *The parkerian hexad* [online]. 4. květen 2012. Získáno z: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

WINKLER, Ira. The threat of shoulder surfing should not be underestimated. *CSO Online* [online]. 13. leden 2016 [vid. 27. květen 2019]. Získáno z: https://www.csoonline.com/article/3021882/the-threat-of-shoulder-surfing-should-not-be-underestimated.html

R E S U M É

Tento příspěvek popisuje, na co si dát pozor při zajišťování digitálních stop v případě spáchání trestného činu spočívajícím v neoprávněném přístupu k počítačovému systému a nosiči informací dle § 230 Zákona č. 40/2009 Sb. ve velké organizaci, kdy zaměstnanci pracují ve velkoprostorových kancelářích, nemají své stálé pracoviště a mohou se do sítě přihlásit na jakémkoliv aktuálně volně přístupném počítači anebo i ze svého soukromého zařízení prakticky kdykoliv a odkudkoliv. Jak v takovém případě efektivně provést ohledání na místě činu, identifikovat prostředky výpočetní techniky, které je nutné rovněž na místě ohledat a zajistit relevantní digitální stopy k usvědčení pachatele.

Klíčová slova: digitální stopy, obraz paměti, kopie disku.

S U M M A R Y

ČERMÁK, Miroslav: PITFALL OF TRACING DIGITAL FOOTPRINTS IN CASE OF SUSPECTED CRIME OF UNAUTHORIZED ACCESS TO THE COMPUTER SYSTEM

This paper describes to what it is necessary to pay extra attention in the course of tracing and securing digital footprints when an offense of unauthorized access to a computer system and information carrier according to § 230 of Act No. 40/2009 Coll. has been committed. This practice is common in a large organization where employees work in open spaces, have no permanent offices, and can access the network from any accessible computer or even from their private devices anytime and anywhere. This article practically gives advice how in such case effectively conduct a crime scene investigation, identify IT resources that need to be scanned on site, and ensure relevant digital footprints to convict the offender.

Keywords: digital footprints, memory dump, disk image.