Co všechno lze najít na nesmazaných discích?

Ochrana dat se netýká jen firemní sítě. Vyřazená paměťová média mohou obsahovat důležité i citlivé údaje o firmě a jejích zaměstnancích.

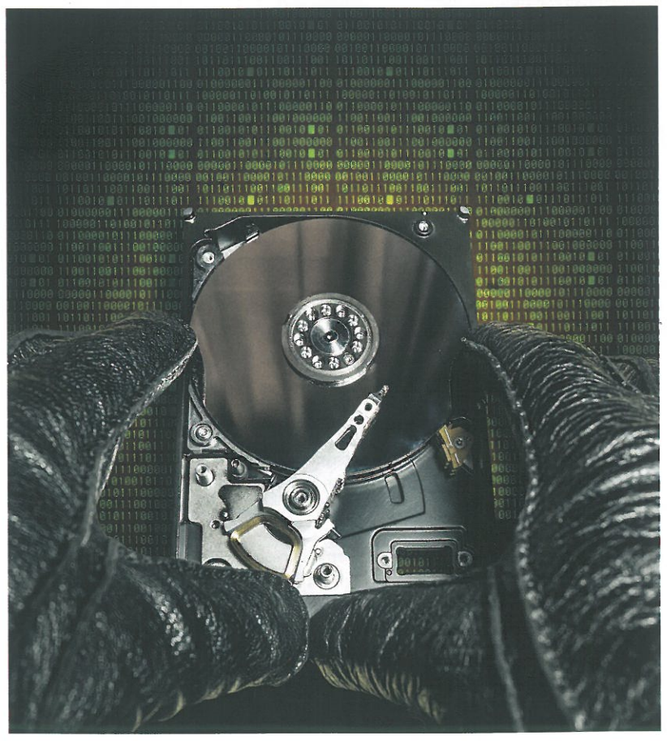
JAN KOPŘIVA

Většina organizací, jejichž procesy jsou závislé na IT, dnes v rámci své infrastruktury implementuje ochranné mechanismy pro zajištění důvěrnosti, integrity a dostupnosti dat, sítí nebo dalších kritických systémů.

Zabezpečení dat v produkčních systémech se tradičně věnuje značná pozornost. Jedním z aspektů, který však obvykle bývá opomíjený, je bezpečnost dat spojená s vyřazovanými paměťovými médii.

Ta jsou tak velmi často odprodávaná specializovaným společnostem a bazarům, aniž na nich obsažená data jsou korektně zlikvidovaná. V rámci výzkumu zaměřeného na zjištění složitosti získání důvěrných dat neoprávněnou osobou analyzovali bezpečnostní specialisté ze společnosti Alef Nula několik pevných disků původně užívaných v infrastruktuře jisté nadnárodní společnosti.

[Z obsahu pevných disků je pochopitelně velmi jednoduché identifikovat organizaci, ve které se užívaly.]



Podařilo se jim při tom nalézt velké množství uživatelských i firemních dat, která by pro potenciálního útočníka nebo konkurenční společnost mohla mít extrémně vysokou hodnotu.

Úroveň bezpečnostního povědomí ve společnosti se neustále zvyšuje. Jedním z důvodů jsou legislativní požadavky, které na některé organizace klade zákon o kybernetické bezpečnosti. Dalšími faktory jsou snahy některých firem o získání bezpečnostní certifikace podle určitého standardu i zvýšená publicita, které se dostává kybernetickým útokům.

V neposlední řadě hraje důležitou úlohu také skutečnost, že organizace jsou si dostatečně vědomy nezbytnosti korektně fungujícího IT pro zajištění svých činností.

Procesní i technická bezpečnostní opatření se tak dnes stávají běžnou součástí informačního prostředí většiny organizací a jen výjimečně je možné se setkat s korporátní infrastrukturou, ve které není na úrovni sítě implementovaná ochrana firewallem nebo v níž na koncových zařízeních není instalované nějaké antimalwarové řešení.

Kromě zajištění fungování systémů kritických pro podporu hlavních procesů dané organizace je při zavádění bezpečnostních opatření zpravidla primárním zájmem ochrana jejích dat. Ať už jde o informace o organizační struktuře, obchodní či výrobní tajemství nebo o smlouvy s dodavateli a odběrateli, zachování důvěrnosti (a samozřejmě i integrity a dostupnosti) těchto dat je z pochopitelných důvodů pro danou organizaci nezbytné.

V produkčním prostředí je za tímto účelem standardně implementována široká škála bezpečnostních opatření. Mimo něj – v rámci testovacích prostředí nebo u zařízení z produkčního prostředí vyřazených – však často není bezpečnost dat zohledněná vůbec.

Můžeme se tak setkat s de facto nezabezpečeným testovacím prostředím, které obsahuje provozní data, nebo s vyřazeným zařízením, na němž se buď „ostrá" data stále nacházejí, nebo z nějž byla smazána způsobem, který umožňuje jejich obnovení.

Smazat data nestačí

Při běžném smazání dat, které vykonávají například uživatelé při odstraňování souborů, nedochází k fyzickému přepsání původních dat, ale jen k označení paměťového prostoru, kde se daný soubor nacházel, za volný, resp. k dispozici pro zápis jiných dat.

Pomocí volně dostupných nástrojů je tak často možné jednoduchým způsobem takto „smazané" soubory obnovit.

Nejčastěji užívaný postup pro rychlou likvidaci všech dat na paměťových médiích je principiálně velmi podobný – dochází při něm k likvidaci informací o umístění souborů na disku, o diskových oddílech a souborovém systému, ale vlastní data obsažená v jednotlivých souborech jím v podstatě nejsou nijak dotčená.

Existují nástroje, které umožňují přepsat (i vícenásobně) celé paměťové médium náhodnými nebo uživatelem nastavenými daty, a zajistit tak neobnovitelnost původního obsahu. Popsaný postup je poměrně bezpečný, nicméně časově velmi náročný, a proto se v praxi používá pouze zřídka.

Vzhledem k relativně nízké ceně paměťových médií některé organizace při jejich vyřazování z aktivního užívání přistupují k fyzické likvidaci. Značný počet organizací však paměťová média po smazání dat odprodává specializovaným firmám a bazarům k dalšímu použití.

Přestože v některých případech jsou užité výše popsané techniky bezpečné likvidace dat, v mnoha případech se média odprodávají pouze po smazání/přepsání informací o diskových oddílech.

V podstatě výjimečně je ale možné setkat se s paměťovým médiem, na němž se před prodejem neaplikoval ani jeden z výše uvedených postupů a po jehož připojení jsou na něm obsažená data volně čitelná bez jakýchkoli specializovaných nástrojů.

Co se našlo?

V rámci výzkumného projektu s cílem zjistit složitost získání citlivých organizačních dat analyzovala společnost Alef Nula několik pevných disků odprodaných jistou nadnárodní společností se zastoupením v České republice specializovanému bazaru.

Zmíněné disky se mazaly pomocí výše uvedené, ne zcela bezpečné metody.

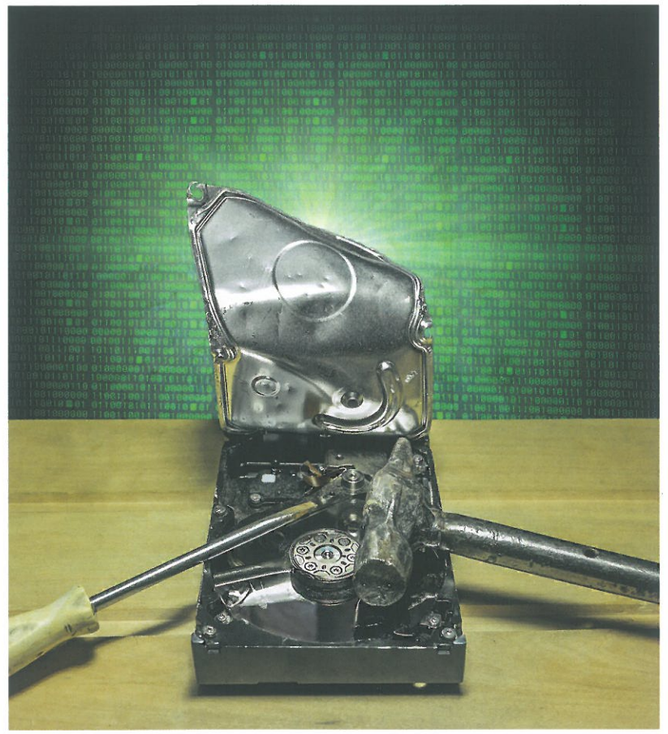
V jednom případě se data na pevném disku ponechala ve zcela čitelné podobě. Získání přístupu k datům z těchto médií pomocí specializovaných nástrojů bylo relativně jednoduché. Jak dokládají následující odstavce, obsažené informace byly citlivé jak z pohledu uživatelů systémů, z nichž disky pocházely, tak z pohledu dané organizace.

Z obsahu pevných disků bylo pochopitelně velmi jednoduché určit organizaci, v rámci níž se užívaly. Vzhledem k tomu, že se na nich nacházely mimo jiné i kopie obsahu e-mailových schránek, určení identity původních uživatelů i jejich zařazení v rámci organizace bylo obdobně triviální, stejně jako zjištění značné části organizační struktury.

Díky záznamům komunikace s externími subjekty a kopiím pracovních kalendářů bylo možné také odvodit pravděpodobnou provázanost dané organizace s externími společnostmi, vnitrofiremní i soukromé aktivity a vztahy jednotlivých uživatelů.

Mezi nejcitlivější objevená korporátní data, nalezená na pevném disku původně užívaném zástupcem středního managementu dané organizace, patřily finanční nabídky a smlouvy se zákazníky a dodavateli nebo technická dokumentace a informace o výrobních postupech a plánech.

Kromě nich se na discích nacházely též faktury, reklamační protokoly a informace o SW i HW systémech užívaných v rámci infrastruktury zmíněné organizace. Mezi daty byly i životopisy žadatelů o zaměst-



[Při běžném smazání dat nedochází k fyzickému přepsání původních dat, ale jen k označení paměťového prostoru, kde se daný soubor nacházel, za volný.]

nání v organizaci. Za zmínku stojí, že analyzovaná data dohromady pokrývala dobu deseti let.

Nejcitlivější soukromá data tvořily osobní údaje uživatelů (které navíc podléhají zákonné ochraně podle zákona č. 101/2000 Sb., o ochraně osobních údajů), smlouvy a informace o bankovních účtech.

V rámci e-mailové schránky jednoho z uživatelů se dokonce nacházela zpráva se záznamem výplatní pásky. Uvedený záznam byl sice zašifrovaný, v těle doprovodného e-mailu byl však popsán postup generování hesla.

Libovolný útočník, který by znal uživatelské jméno dané osoby, by tak díky uvedenému návodu musel pro dešifrování vyzkoušet maximálně tisíc různých hesel, a uvedené opatření tak de facto pozbývalo smyslu.

Obecně lze říci, že data z analyzovaných pevných disků by mohla být vysoce hodnotná jak pro potenciálního útočníka, tak pro libovolnou konkurenční organizaci. Uvedená problematika úzce souvisí s ochranou osobních údajů (viz výše uvedený zákon), zejména pokud jde o povinnosti správce osobních údajů při jejich likvidaci.

Nedodržení povinností správce osobních údajů v rámci likvidace osobních údajů může mj. vyústit v uložení sankcí, které citovaný zákon upravuje.

Zjištění specialistů společnosti Alef Nula by tak měla sloužit jako doklad potřeby vhodným způsobem chránit firemní data nejen v produkčním prostředí, ale i mimo něj, a to včetně nutnosti fyzicky likvidovat paměťová média při jejich vyřazování nebo zajistit skutečně bezpečné smazání na nich obsažených dat. ■

Autor pracuje jako bezpečnostní expert ve společnosti Alef Nula.