INFORMAČNÍ BEZPEČNOST A POSKYTOVATELÉ PRÁVNÍCH SLUŽEB

Pokladnice s informacemi

Když byl známý bankovní lupič Willie Sutton dotázán, proč vykrádal banky, odpověděl: „Protože to je místo, kde jsou peníze.“ Z pohledu kyberútočníka poskytovatelé právních služeb nemají mnoho peněz, které by bylo možno zcizit, ale mají pokladnici plnou informací – univerzální měnu 21. století.

Tradiční představa kyberútočníka spočívá v tom, že jde o jednotlivce nebo malou skupinu, která je motivovaná instalací malware nebo získáním informace jenom pro informaci samotnou. Toto již dlouho neplatí. Podle odhadů FBI je obchod s informacemi výnosnější než obchod s drogami nebo zbraněmi.

Jaké informace jsou cílem?

Podle vyšetřování incidentů jsou nejčastějším cílem:

- privátní obchodní informace klienta;
- patentové a autorským právem chráněné informace, duševní vlastnictví;
- informace o případu a/nebo informace o strategii, včetně parametrů případné dohody nebo identifikace slabých bodů obhajoby;
- komunikace advokáta s klientem nebo jiné privilegované informace;
- osobní údaje zaměstnanců, klientů a třetích stran (zdravotní údaje, účetní podklady).

Data ve vzdálených úložištích

Podle rozhodnutí soudce pražského městského soudu Stanislava Králika v kauze Františka Savova může policie přistupovat k datům uloženým na vzdálených uložištích – cloud storage. Podle konstatování soudce cloudové úložiště není místem, kde advokát vykonává advokacii. Z naší praxe víme, že množství advokátů i celých právnických firem využívá veřejné datové úložiště jako je Dropbox, Google Drive, Office 365 a podobně. Toto rozhodnutí přináší riziko, že se policie prostřednictvím obecně formulovaného příkazu k prohlídce dostane i k informacím, které patří k jiným případům. Jedním ze způsobů, jak se ochránit technologickými prostředky, je šifrování a ochrana komunikačních kanálů, což ale obnáší další komplikace a workflow činí složitějším.

Státem sponzorované útoky

Zatím přehlíženým problémem jsou i státem sponzorované útoky na zařízení, počítače nebo i celé sítě. Kupříkladu v Austrálii bylo na poskytovatele právních služeb namířeno minimálně třináct identifikovaných malware kampaní v průběhu roku 2013.

Odhaduje se, že se podařilo identifikovat nanejvýš pět procent těchto útoků, vzhledem k sofistikovanosti a cílenosti útočných kampaní. Podle analýz za útoky v Austrálii byly Čínou sponzorované vojenské skupiny zaměřené na získávání citlivých informací a průmyslovou špionáž.

V roce 2012 se společnost Gipson Hoffman & Pancione stala obětí cílené útočné kampaně. Zaměstnanci společnosti dostali e-mail, který se jevil jako zaslaný od ostatních zaměstnanců firmy, ale ve skutečnosti obsahoval škodlivý kód s cílem zcizit informace z počítačů společnosti. Na základě analýzy malware bylo zjištěno, že stopy je možné vysledovat na čínské servery.

Útočníkem nejsou jenom represivní režimy, tendence k nákupu malware vyvinutého speciálně pro vedení kyberválky mají i státy v Evropě.

Dne 6. 8. 2014 došlo k úniku dat, ze kterých je možné usuzovat, že společnost Gamma International dodala svůj software FinFisher pro použití v České a/nebo Slovenské republice. Užívání tohoto typu software policií a/nebo rozvědkou zakládá pochybnosti o možnosti ochránit komunikaci mezi klientem a advokátem, a to hlavně v prostředí, ve kterém jedním z prostředků boje jsou uniklé odposlechy.

Co s tím?

Každá situace je řešitelná, i když neexistuje univerzální a jednoduchá metoda, která odstraní všechny problémy okamžitě a bezbolestně.

Na prvním místě je třeba provést analýzu současného stavu, definovat aktiva a zvolit úrovně ochrany. Tato analýza je podkladem, na kterém je možné vystavět modely ochrany komunikačních kanálů, datových úložišť a eliminovat slabá místa.

Informační bezpečnost je potřeba řešit nepřetržitě, erudovaně a koncepčně, bez ad hoc výdajů na nákup hardware a software.