Vážené čtenářky, vážení čtenáři,

tématem, které v posledních týdnech rezonuje snad ve všech oblastech, je válka na Ukrajině. Kromě lidského a geopolitického aspektu se výrazně dotkla i kyberprostoru – nejen že řada IT firem omezila své podnikání v Rusku, ale soupeření Západu s Ruskem eskalovalo i na poli informační bezpečnosti. Jak se v této situaci zachovat?

V první řadě je potřeba říci, že studená válka v on-line světě je tu už řadu let, poslední události ji pouze zvýraznily. Různé ataky hackerů, často podporovaných jednotlivými vládami, jsou dobře zdokumentované.

Objem útoků se ale za poslední týdny výrazně zvýšil – vidíme tak na jedné straně prolamování ukrajinských webů či útoky na kritickou infrastrukturu některých států, na druhé straně kompromitace vesmírných agentur, provozovatelů atomových elektráren či mediálních domů. Ne všechny průniky posledních dní jsou však skutečné – často jsou určitou propagandou či dezinformací, než že by měly reálný dopad.

Řada expertů volá po tom, aby se západní firmy odstřihly od ruských IT řešení – minimálně z morálního hlediska. Na druhou stranu by tyto produkty v zásadě neměly být méně bezpečné než třeba začátkem roku. Podobně jako jiné země i Rusko má ale zákonné normy, jak donutit své IT firmy spolupracovat s jejich tajnými službami, takže i na to je nutné vzít zřetel.

Otázka je, jak bude u ruských řešení fungovat podpora a rychlost oprav případných zranitelností, pokud tamní firmy přijdou o přístup k nejnovějším technologiím kvůli sankcím uvaleným na Rusko a jestliže se Rusové, jak se spekuluje, v nějaké míře odstřihnou od globálního internetu.

Naše rada tedy zní – nyní zbrkle neodpojovat ruské systémy z vlastní infrastruktury, ale spíše zvážit výhled ohledně jejich dalšího použití. Okamžité odstřižení od ruských produktů by mohlo ve finále znamenat pro organizaci naopak větší ohrožení, než kdyby je používala, protože implementace jiného řešení i vzhledem k obecnému nedostatku bezpečnostních expertů zabere určitý čas, po který by podnik nemusel být chráněný a nedokázal by tak čelit různým hrozbám či bezpečnostním incidentům.

Organizace by také měly zvážit, zda se u threat intelligence, tedy získávání informací o bezpečnostních hrozbách, raději než na ruské dodavatele spoléhat spíše na otevřená data, jako je třeba OSINT.

A co z toho vyplývá pro tuzemské organizace? Připravte se na zvýšený počet útoků zneužívajících různé zranitelnosti – tady bude hrát velmi důležitou roli kvalitní patch management. Měli byste také otestovat funkce svých zálohovacích systémů, oprášit plány reakce na incidenty, pokud tak nečiníte pravidelně, a zhodnotit rizika vyplývající ze vzdáleného přístupu k firemnímu IT.

Vhodné je také zvýšit úroveň logování událostí i jejich vyhodnocování, a pokud je to možné, otestovat úroveň vlastní bezpečnosti pomocí penetračních testů. A konečně byste měli zvážit možnosti, které máte při obraně proti útokům typu DDoS.

S přáním brzkého návratu klidnějšího období

Pavel Louda
vedoucí projektu

Obsah