Vítejte v kyberprostorové džungli

Klíčem k úspěšnému tažení proti kyberzločinu nemusí být nutně sofistikované ochranné či monitorovací systémy, ale větší empatie a pochopení chování a mentality člověka, který si do kyberprostoru přenáší vzorce chování z běžného života.

Technologické a softwarové firmy na rozdíl od všech ostatních sektorů sdílejí mnohem více potenciálně citlivých informací na on-linových skupinových fórech a v diskusních skupinách.

Jeden z nejrozšířenějších omylů, jehož se firmy i jednotlivci při budování obrany proti kybernetickému zločinu dopouštějí, by se dal shrnout do věty: „Když investujeme do špičkových technických nástrojů, jsme v bezpečí."

Ve skutečnosti efektivní kybernetická bezpečnost závisí na technologiích mnohem méně, než by se na první pohled mohlo zdát. Stejně jako u jiných komplikovaných systémů totiž platí, že nejslabším článkem je lidský faktor. Proto se lidé neustále musí učit žít v novém prostředí a adaptovat se na jeho pravidla.

Další mylnou představou je, že nesmíme dělat kompromisy a musíme dosáhnout stoprocentní bezpečnosti. To však není reálně možné, a ani vhodné. Stejně tak neplatí vize, že musíme disponovat kvalitnější ochranou než potenciální útočníci. Bezpečnostní strategie a taktika by totiž měla primárně reflektovat cíle organizace, nikoliv schopnosti útočníka.

Efektivní obrana znamená především efektivní monitoring? Ani to dnes už úplně neplatí. Neméně důležité jsou schopnosti učit se a vnímat aktuální hrozby. Ale ani snaha najmout si nejlepší profesionály, aby nás chránili před kybernetickými útoky, však nemusí stačit. Kybernetická bezpečnost totiž není odpovědností jednoho oddělení, ale všech zaměstnanců a oddělení ve firmě. ■

Jan Krob
poradenství v oblasti IT, KPMG Česká republika

> Stále častěji se setkáváme se skupinami sponzorovanými vládou, které do prostoru přinášejí geopolitické ambice států.

Kyberprostor se neustále rozpíná a pohlcuje naše životy. Penetrace chytrých telefonů, na něž přesouváme své osobní a pracovní aktivity, za poslední tři roky rapidně vzrostla. Digitální stopy našeho reálného života čím dál častěji ukládáme na vzdálené cloudy.

Kyberprostor nemá reálné hranice, střetávají se v něm zájmy jednotlivců, velkých korporací i států. A výlučně na stát se v kyberprostoru spoléhat nemůžeme, protože nedisponuje dostatečnými prostředky. Státy totiž mají co dělat, aby dokázaly před kyberzločinem ubránit svou klíčovou infrastrukturu, jež je navázaná na internet a virtuální prostor. Jednotlivci nebo soukromé firmy se tak musí v první řadě spolehnout sami na sebe.

Kybernetičtí loupežníci

Pochopit motivaci útočníka je další důležitou podmínkou efektivní obrany proti kybernetickým útokům.

V životopisu kyberzločinců zaujímá důležité místo hacker, tedy jedinec motivovaný tím, že může předvést své schopnosti, a způsobit tak značné škody. Materiální zisk nemusí být nutně jeho primárním motivem, což se ovšem nedá říci o organizované zločinecké skupině.

Za novodobého Robina Hooda můžeme považovat všechny (h)aktivisty, kteří touto cestou chtějí zviditelnit určité ideologie nebo prosadit své politické postoje a zájmy. Stále častěji se můžeme setkat i se skupinami sponzorovanými vládou, které do kyberprostoru přenášejí geopolitické ambice států a proměňují jej v alternativu mezistátních „bitevních polí".

K nejčastějším důvodům kybernetických útoků patří oportunismus – kyberzločinec jednoduše využije příležitosti, kterou mu lehkovážný uživatel nabídne. Dalšími populárními důvody jsou cílená špionáž, terorismus, finanční zločin a krádeže dat. Svou roli hraje mimo jiné i nespokojenost se zaměstnavatelem.

Značné bezpečnostní trhliny

Podle průzkumu KPMG Vulnerability Index obsahuje 15 % firemních webů dotazovaných společností zneužitelné testovací funkce a privátní přístup k portálům s potenciální možností nahrávat soubory. 16 % firemních webových serverů je zranitelných kvůli chybějícím bezpečnostním záplatám nebo neaktuálnímu serverovému softwaru. 78 % firemních webů pak obsahuje citlivé informace v podobě metadat dokumentů.