Buďme opatrní. Obrana před kyber špiony záleží na každém z nás

cetin.cz/-/budme-opatrni-obrana-pred-kyber-spiony-zalezi-na-kazdem-z-nas

První díl seriálu o bezpečnosti kritické infrastruktury

Současná geopolitická nestabilita způsobila, že témata, která mnoho lidí dlouho nebralo zcela vážně, vystoupila na povrch. Jedním z nich je ochrana kritické infrastruktury státu.

Když poslední dobou čtete články z oblasti bezpečnosti, často objevíte zmínky o hackerech nebo ruských a čínských agentech. Jedno mívají společné. Snaží se získat informace a lidi, které by mohli využít ke kybernetické sabotáži nebo až k rozvratu společnosti dané země.

Tyto útoky jsou směřované na subjekty kritické infrastruktury zemí NATO nebo na cíle zajišťující obranu některého státu. S tím souvisí také bezpečnost dodavatelských řetězců a s tím spojená odolnost kritické infrastruktury evropských zemí.

Jak se obecně kryjí špioni?

Špioni a agenti tu byli samozřejmě od nepaměti. Špionáži se taky někdy přezdívá „druhé nejstarší řemeslo na světě“. Nicméně pro někoho může být překvapení, že si špioni dělají profily o lidech z firem, které se starají o kritickou infrastrukturu – podobně jako obchodní zástupci o svých partnerech.

Špioni a agenti mají dobré důvody pro to, aby se skrývali pod identitou konzultantů a obchodních zástupců. Proč? Na první pohled je těžko odhalíte. Skutečně může jít o vnímavého obchodního zástupce, který poznatky využívá jen k prohlubování vzájemných dobrých vztahů. Networking je totiž pro každý byznys důležitý. I v této vypjaté době tak není potřeba se plašit a očekávat, že každý zástupce zahraničního dodavatele je špion nebo agent.

A kdo tedy vlastně ti špioni a agenti jsou? V evropských i asijských regionech je agent člověk, který pracuje ve prospěch zpravodajské služby, která ho získala, aby jí pomáhal dosahovat určité cíle. Není to tedy zpravodajsky důstojník, který je naopak zaměstnanec zpravodajské služby a vytváří svou agenturní síť ze zmíněných zverbovaných agentů, které řídí ke stanoveným zpravodajským cílům. Nicméně mezi špiony lze obecně zařadit obě skupiny – agenty i jejich řídící důstojníky.

Cíl mají společný – a to využít různé kombinace motivů špionáže zvaných PINE (peníze, ideologie, nenávist a ego) k tomu, aby získali potřebné firemní tajemství – v našem případě – o kritické infrastruktuře. Tajemství zdánlivě neškodné, které však v pravou chvíli může pomoci nepřátelské straně narušit národní bezpečnost skrze fyzickou či kybernetickou sabotáž kritické infrastruktury. I zdánlivě nepodstatná informace o infrastruktuře může být důležitým střípkem pro odhalení zranitelnosti – třeba v podobě mezery v zabezpečení nebo kvůli lidskému faktoru. Hrozbou může být člověk, který se cítí nedoceněný, potřebuje peníze na hypotéku nebo se chce firmě pomstít. Zranitelnosti technologií i lidí jsou branou k mnohým pokladům, které vedou k úspěšné misi špionů a agentů – tedy k získání potřebné informace, k úspěšné sabotáži, či k získání potřebných finančních prostředků pro další kybernetické operace.

Pozor, aby se z bonbonu nestala bomba

Od mala mi rodiče říkali, abych se s nikým cizím nebavil, nevyzrazoval tajemství a nebral si od cizích lidí bonbony. Stačí se držet těchto rad a být obezřetný. Tím špionům ztížíme práci a kritická infrastruktura státu bude tím spíše v bezpečí.

Je dobré více zvažovat, co komu říkáme, a nedělit se o citlivé firemní tajemství jen proto, abychom byli zajímavější. Je potřeba si dát pozor i na takové věci jako USB disky darované na konferencích. Neměli bychom je používat ve firemní informační síti, abychom pomohli darovanému „bonbonu“ proměnit se v „bombu“ v naší síti. Protože zde určitě neplatí heslo „darovanému koni na zuby nehleď“.

Pavel Rivola
Ředitel, bezpečnost a IMS