ESET
ENJOY SAFER TECHNOLOGY™

Cílené útoky a hacking jako součást konkurenčního boje firem

Velké zahraniční společnosti označily cílené útoky a hacking jako jednu z největších bezpečnostních výzev. Vyplývá tak z průzkumu ESET.

Jde o specifické typy útoků zaměřených na byznys dané organizace použitím spear phishingu (cílené sociální inženýrství) nebo zneužití bezpečnostních zranitelností v neaktuálních operačních systémech.

Proč jsou firmy oblíbeným terčem útoků?

Na účtech mají více finančních zdrojů než běžní lidé.

Disponují citlivými a zajímavými údaji, které lze dále zpeněžit na černém trhu.

Cílené útoky se dají použít také jako forma konkurenčního boje mezi firmami.

Konkurenční boj

Firmy se často bojí přiznat, že se staly terčem cíleného útoku, a vytváří mylný dojem, že jsou útoky jen občasnou záležitostí.

Oblíbené jsou DDoS útoky, které si může firma zajistit na černém trhu a směřovat je na webové stránky jiné firmy s cílem je vyřadit z provozu nebo přesměrovat jejich zákazníky k sobě.

Pro konkurenční boj se také využívá Data Hunting - získávání citlivých informací nebo intelektuálního vlastnictví často spojené s vydíráním za jejich vrácení.

Ohrožení „CEO Fraud“

1. **Útočník** podle automatické odpovědi **zjistí, že je CEO** společnosti **na dovolené.**
2. **Jeho jménem zašle podvržený e-mail** nebo SMS zprávu s urgencí uhrazení faktury.
3. **Finanční oddělení** nebo zástupce CEO obratem **zadá platební příkaz** na cizí účet.
4. **Vylákanou sumu** potom z účtu nastrčené firmy **vybere bílý kůň** a transakce se ztratí v džungli zahraničních účtů.

Jak se bránit sociálnímu inženýrství?

- Školte své zaměstnance na všech úrovních.
- Nasaďte nástroje s funkcí antispamu.
- Budujte u zaměstnanců kritické myšlení a dbejte na ověřování informací.
- Proveďte fingovaný test sociálního inženýrství uvnitř firmy, abyste poukázali na slabiny.

Podle FBI bylo od napadených firem vylákáno během tří let až 2,3 miliardy dolarů.

Těžba kryptoměn bez vědomí uživatele

- Pro firmu to znamená plné vytížení infikovaných stanic, mobilů nebo serverů.
- Hardwaru se zvyšuje jeho opotřebení a roste účet za elektřinu.
- Škodlivý kód otevírá cestu dalšímu malwaru s jinými funkcemi.

Když se firma stane obětí takového útoku, nastává zjišťování toho, co se stalo, a jak se infikovala.

Podle průzkumů firmám trvá

150 – 200 dní objevit infikaci.

Samotné forenzní vyšetřování je nákladné a časově náročné, tudíž může trvat klidně více než jeden rok.