Doba se mění, **nahrává hackerům,** říká šéf AEC

Už déle než třicet let patří společnost AEC s pobočkami v Praze, Brně a Bratislavě k nejvýznamnějším poskytovatelům kybernetické ochrany na trhu.

Podle výkonného ředitele společnosti AEC Tomáše Strýčka je však tempo, jakým dnes útočníci zdokonalují své nástroje a postupy, alarmující.

NOVÉ VÝZVY MASIVNÍ PŘESUN LIDÍ NA HOME OFFICE ZNAMENAL PRO FIRMY ZAJIŠŤUJÍCÍ BEZPEČNOST POČÍTAČŮ NOVÉ VÝZVY, ŘÍKÁ ŘEDITEL SPOLEČNOSTI AEC TOMÁŠ STRÝČEK. FOTO: AEC

Na svém webu uvádíte, že nejste anonymní, ale běžný člověk toho o vaší práci asi moc neví...

Je pravda, že o své práci nemůžeme mluvit tolik, jako je to běžné v jiných oborech, ale jinak nic neskrýváme. Jsme ti, kdo navrhují procesy, technologie i celé bezpečnostní architektury. Diskrétnost přitom nechápeme jenom jako jednu z přirozených součástí poskytovaných bezpečnostních řešení. Pro nás je to hlavní předpoklad vztahu s klientem. Nenápadnost je důležitá i pro kolegy, kteří v roli etických hackerů prověřují odolnost systémů proti kybernetickým útokům anebo zasahují v případech incidentů. Určitou výjimku představovala jen nedávná medializace našich zákroků v tuzemských nemocnicích, které čelily rozsáhlým kybernetickým útokům.

Změnila se nějak v průběhu let, během nichž AEC působí na trhu, vaše role?

Ta se nemění, stále pracujeme na zajištění bezpečnosti informačních systémů a děláme všechno pro to, aby útok nenastal. Ale doba se změnila. Digitalizace pokročila a technologie a možnosti útočníků jsou dnes obrovské. Musíme počítat s tím, že k napadení systému dříve či později dojde. Klíčové jsou první kroky, jde o každou sekundu. Naši lidé jsou zkušení, dokážou rozpoznat, že útočník získal přístup do systému, umí v něm monitorovat jeho další aktivity a jsou schopni jeho snahy v síti eliminovat. Pracujeme ve velmi dynamickém prostředí, konfrontujeme se s útočníkem a často přitom musíme reagovat na úplně nové hrozby. Rozhodující je, že našim klientům, kteří se ocitli pod útokem, dokážeme okamžitě pomoci.

Co tedy dnes představuje pro uživatele největší hrozbu?

Alarmující je, jak výrazné zdokonalování na straně útočníků každoročně registrujeme. Útoky nyní bývají mnohem přesněji zacílené. Dříve šlo obvykle o nějakou plošnou phishingovou kampaň a její autoři vyčkávali, jestli se někdo nachytá. V současnosti si vytipují cíl, zjistí si maximum informací a přizpůsobí podmínky, aby úder vyšel najisto. Podvodné e-maily jsou psané bezchybnou češtinou a tak, aby budily důvěru. Útočníci už umí zfalšovat dokonce i hlas nebo obraz – připojí se na videohovor a budou se vydávat za vašeho kolegu. To, co nám loni stačilo k rozpoznání útoku, už letos stačit nemusí. Pro hackery jde o úspěšný byznys, takže jim stojí za to ho vylepšovat.

Jak se z vašeho pohledu promítla do kybernetických hrozeb pandemie koronaviru?

Koronavirus přinesl nové výzvy. Tou první je přechod celé řady společností do online módu. Home office znamenal změny v IT struktuře, včetně přechodu zaměstnanců mimo chráněný perimetr firmy. Naší úlohou je zajistit, aby to pro naše klienty neznamenalo bezpečnostní slabinu. Určitou komplikací je, že firemní zařízení nyní často využívá více členů domácnosti, včetně dětí, takže je náročnější ten systém ochránit. Musíme mít na paměti, že pro útočníky platí čím hůře, tím lépe. Takže právě chaos spojený s nejrůznějšími opatřeními týkajícími se koronavirové epidemie pro ně vytváří ideální podmínky. Ke zvýšení intenzity a závažnosti útoků dochází pravidelně i před Vánoci. Útočníci se teď například vydávají za zástupce spedičních firem nebo e-shopů.

Lze vůbec nějak minimalizovat nebezpečí kybernetického napadení?

Rozeznat, že jsem cílem útoku, není vždy snadné. Klíčová je obezřetnost, takže sledujte odchylky od toho, co znáte, všímejte si nepřesností. Před rozkliknutím e-mailu se zamyslete nad tím, jestli nevybízí k něčemu, co není úplně běžné. Jestli vaše banka nebo třeba e-shopy takto normálně komunikují a naléhají přitom na poskytnutí osobních údajů, ověření PINu nebo na otevření nějaké přílohy. Pro firmy je to ještě náročnější. Řada z nich nedisponuje odpovídající kapacitou, díky níž by si mohla potřebná řešení zajistit vlastními silami. Trendem je outsourcing bezpečnosti u zkušené firmy, pro kterou je ochrana klientů posláním a boj s kyberzločinem výzvou.