**Největším bezpečnostním rizikem pro firmy jsou vlastní zaměstnanci ale i další vnitřní hrozby, třeba brigádníci nebo uklízečky**

**Praha, 22. listopadu 2022** – Česká policie letos od začátku roku do konce srpna zaznamenala téměř 14 tisíc skutků spáchaných v kybernetickém prostoru. Počet případů roste nejenom u občanů, ale i firem. Výrazný nárůst kybernetických útoků zaznamenal také bezpečnostní tým O2, který řeší denně okolo 500 útoků na firmy připojené přes jeho síť. To představuje v meziročním porovnání dvojnásobný nárůst.

Podle nejnovější zprávy Microsoft Insider Risk Report mnoho zaměstnanců, kteří způsobují svým organizacím škody, tak činí nevědomky. Nejčastější příčinou úniku dat jsou laxní a nedostatečně proškolení zaměstnanci, kteří nevědomky provádějí nebezpečné akce. Ti, kteří kradou data cíleně pro konkurenci jsou méně častým jevem, ale jejich nebezpečí není menší, pracují totiž na objednávku a jdou na jisto.

**Klikají na odkazy bez ověření**

Faktem je, že počty kybernetických hrozeb v České republice neustále rostou. Jsme nyní již pátým nejčastějším terčem útoků v Evropě. Zaměstnanci jsou celkově nejslabším článkem zabezpečení firmy. Jejich zranitelnost ještě umocňuje růst nutnosti hybridní práce.

„Simulované útoky v rámci testování odolnosti firem ukazují, že řádově pětina zaměstnanců klikne na odkaz ve zprávě, aniž by prověřovali, kam směřuje. Phishingové útoky vedené přes zaměstnance jsou velmi účinné, jejich edukace v základních pravidlech bezpečného chování ve virtuálním prostředí pokulhává na celém světě,“ upozorňuje Michal Merta, ředitel Cyber Fusion centra společnosti Accenture.

**Hybridní práce bezpečnosti nepřidá**

V současném hybridním světě pracovníci nejenže používají své osobní přístroje, ale navíc řeší pracovní úkoly na svých cestách. Firmy přitom mají technologické rezervy ve způsobu, jakým dovolí vzdáleným pracovníkům přistupovat k datům a aplikacím. Podle průzkumu Cisco jen u 32 % společností vyžadují firemní aplikace přístup přes virtuální privátní síť (VPN) a jen u přibližně pětiny společností se pro vstup k firemnímu IT používá vícefaktorová autentizace. Zhruba 20 % pak vyžaduje, aby veškerá komunikace vzdáleného pracovníka do internetu probíhala přes VPN a firemní firewall.

„Kombinace slabšího zabezpečení zařízení používaných pro práci z domova, vzdálené komunikace a podceňování důkladného školení v otázkách bezpečnosti může představovat bezpečnostní rizika pro firemní data,“ říká Ondřej Ševeček, odborník na bezpečnost a etický hacking z Počítačové školy GOPAS.

Nepřehlednost ve větších organizacích zejména v době hybridní práce dává prostor i zcela primitivním metodám, kdy se podvodník představí jako nový pracovník IT oddělení, který má za úkol pomocí vzdáleného přístupu provést nějaký zásah na počítači.

**Staré dobré metody**

Staré dobré metody přímé fyzické infiltrace do pracovních systému, stažení citlivých dat a jejich předání konkurenci je sice co do počtu událostí méně častým rizikem, ale to nesnižuje jejich nebezpečí. Naopak. Jedná se zde o velmi nebezpečnou formu průmyslové špionáže a její zacílení a přímé využití nekalou konkurencí firmy ohrožuje v maximální míře.

Aktérem krádeže dat může být uplacený neloajální zaměstnanec, cíleně dosazený nováček ale i třeba často v noci v prázdných kancelářích pracující uklízečka. Ta může buď zcizit volně ležící externí paměťový disk nebo pomocí speciální flashky rychle stáhnout data z počítače. Obranou proti těmto hrozbám je jedině holistický přístup k zabezpečení napříč celou organizací a také školení a vzdělávání jsou životně důležité pro proaktivní řešení a snižování vnitřních rizik.