accenture

KYBERÚTOK ANI NEPOSTŘEHNETE...

VIDEO TRANSCRIPT

Intro

Do pěti let bude vaše auto, dům, kávovar, květináč - prostě téměř všechno online. A bude jen otázkou času, než se i vy stanete cílem kybernetického útoku. Jsem Michal Merta, z Accenture a jsem si jistý, že i vy jste se setkali s kybernetickým útokem. Jenom o tom nevíte.

Co je vlastně kybernetický útok

Kybernetický útok je dlouhodobý, pečlivě plánovaný proces, který využívá slabých míst a momentu překvapení. Po úspěšném prvotním prolomení se útok přesouvá do další fáze - blíže k vytyčeným cílům – třeba k účtu vašeho firemního administrátora.

Útoky, se kterými se patrně většina z nás někdy v minulosti setkala, jsou bezesporu z rodiny Ransomware. Jde o druh škodlivého programu, který zašifruje vaše data a vy s nimi nemůžete pracovat. Hackeři stojící za těmito útoky tímto vyřadí obvykle systémy z provozu a požadují peníze nebo kryptoměnu výměnou za obnovení dat.

Ransomware jako takový je proto hlediska monetizace velmi zajímavý a pro mnohé hackery se z něj stává velký byznys. Stačí jen najít slabé místo, kterým jsou obvykle důvěřiví zaměstnanci nebo uživatelé. Stačí, abyste otevřeli nebezpečný odkaz v e-mailu nebo na sociálních sítích a máte problém.

Kdo profituje?

Útočníci obvykle nejsou těmi, kdo vaše data zpronevěří. Obchoduje se s nimi na černých trzích, takzvaných dark nets. Objem obchodů tam velmi nebezpečně roste a láká tak stále více jedinců i organizovaných skupin.

A protože je pro poškozenou stranu často levnější zaplatit výkupné, než riskovat ztrátu nebo zveřejnění dat, je celý tento černý trh stimulován a kyberkriminalita nebezpečně rychle roste.

Problémem je samozřejmě i neomezená dostupnost obrovského množství nástrojů, školících materiálů a online dokumentace, které téměř z každého jedince ovládajícího angličtinu mohou udělat potenciální kybernetickou hrozbu.

Každý další útok je něčím nový

Ne vždy za kybernetickým útokem stojí selhání lidského faktoru. Útočníci aktivně vyhledávají slabá místa nejenom v aplikacích, ale i na každém zařízení připojeném do sítě. S tím vším máme zkušenosti a můžeme vám v Accenture pomoci.

Existují mechanismy, které útočníka mohou detekovat, či dokonce zastavit, případně samotný útok predikovat. Mezi obranné mechanismy patří např. funkční SIEM řešení, simulování útoků, threat hunting, správa privilegovaných účtů či bezpečný vývoj aplikací.

Nicméně je potřeba si uvědomit, že pokud jste pro útočníka atraktivní, bude zkoušet nové techniky, na které ani vaše stávající zabezpečení nemusí stačit, a které nemusí být ani obranným týmům známé. Zvláště organizované skupiny mívají ve svých řadách experty na vývoj zero day exploitů či specialisty na phishing a vishing.

Právě proto jsme vybudovali Cyber Fusion Center, ve kterém jsou ti nejlepší bezpečnostní experti. Díky nim se budete moci věnovat více svému byznysu a méně jeho ochraně. Protože o bezpečnost se postaráme v Accenture.