Hackeři využili karantény a útočí, zaměstnanci na home office se neumí bránit

Hackeři začínají využívat možností, které jim otevřela nařízená karanténa. Řada českých firem je teď proti počítačovým útokům zranitelnější. Musela v rychlosti přejít do režimu práce z domova, aniž stačila připravit zabezpečení svých informačních systémů.

Jiné společnosti, aby umožnily svým zaměstnancům přístup z domova, dokonce část bezpečnostních prvků vypnuly.

„Dalším problémem je sehnat dostatek pracovních notebooků. Ty vhodné byly dle naší zkušenosti během prvního týdne vykoupeny. Takže řada zaměstnanců pracuje z domácích počítačů, které nemusí být vhodně nastavené a adekvátně zabezpečené, takže skrze ně mohou uniknout hesla nebo data,“ řekl MF DNES Martin Haller, expert na kyberbezpečnost z firmy Patron-It.

Útoky na nemocnice

Zvýšenou aktivitu hackerů v poslední době potvrzuje i Národní centrála proti organizovanému zločinu (NCOZ). *„Za období, kdy je vyhlášen nouzový stav, registrujeme mírný nárůst zejména takzvaných ransomwarových útoků* (útočníci zašifrují data v počítačích a za jejich opětovné dešifrování požadují výkupné – pozn. red.), *zejména v oblasti IT systémů zdravotnických zařízení. Lze předpokládat, že tento typ kybernetického útoku přichází do České republiky ve druhé vlně, kdy lze dohledat, že obdobné útoky proběhly i v jiných státech, a to nejen v Evropě,“* uvedl mluvčí protimafiánské centrály Jaroslav Ibehej.

Vyšší výskyt vyděračských virů eviduje také Národní kyberbezpečnostní úřad (NÚKIB). Ten kvůli tomu preventivně začal s větší koordinací s podobnými úřady v rámci Evropské unie. Jen v uplynulých měsících musely v Česku útokům hackerů čelit nemocnice v Brně, Benešově a Kosmonosech. Fakultní nemocnice v brněnských Bohunicích, která mimo jiné prováděla testy na koronavir, kvůli útoku musela odložit operace a převézt pacienty jinam.

Stát příliš nehlídá IT systémy nemocnic. Hackeři cílí na menší špitály

Nemocnice a úřady jsou nejen v době koronavirové krize nejcitlivějším místem každého státu a také oblíbeným terčem vyděračských kampaní hackerů. Například včera neznámí útočníci napadli portál italské správy sociálního zabezpečení a vyřadili jej z provozu.

Stalo se to jen krátce poté, co tamní vláda vyhlásila příspěvek ve výši v přepočtu šestnáct a půl tisíce korun pro sezonní pracovníky. O příspěvek se prostřednictvím portálu přihlásilo přes 300 tisíc lidí, dalším to však zmíněný útok znemožnil.

Sliby hackerů

Česká policie zatím útoky na tuzemské nemocnice stále vyšetřuje. *„Nemají úplně stejný modus operandi a při provedení útoku hackeři využívají šifrovací systémy, které se obtížně dešifrují. Vývoj zneužívaných šifrovacích nástrojů je velmi dynamický a jeho progresivita je pro běžnou IT komunitu těžko řešitelná,“* popsal mluvčí NCOZ Ibehej.

Podle zjištění MF DNES několik tuzemských nemocnic již dříve útočníkům výkupné vyplatilo. Podle zdrojů redakce šlo o částky v řádech jednotek tisíc amerických dolarů.

V době, kdy naplno propukla koronavirová krize, se objevily i zprávy, že hackeři nebudou situaci zneužívat a útočit nebudou. A podle expertů tomu řada lidí uvěřila.

„Teze o neútočení je strašně nebezpečná. Setkáváme se s tím dnes a denně. Spousta klientů nám říká, že přece hackeři slíbili, že nebudou útočit. Tenhle nesmysl se roznesl rychlostí blesku,“ varuje Martin Uher, vedoucí analytik v bezpečnostní platformě Securo Pro.

Podle něj se útoky soustředí především na nepozornost lidí pracujících v home office. Hackeři využívají také toho, že část zaměstnanců nebyla zvyklá používat technologie umožňující vzdálenou práci. *„Tím, jak se na to spěchalo, hrozí, že se při nasazení něco přehlédlo, nastavilo špatně nebo se použila ne úplně bezpečná technologie. Právě po takovýchto chybách část hackerů jde a jejich prostřednictvím firmy napadá,“* řekl MF DNES Martin Haller z Patron-It.

Kromě sofistikovaných útoků na firmy nebo státní zařízení se však množí i pokusy podvodníků, jak vytáhnout peníze z důvěřivých lidí. Často lidem nabízejí informace o lidech infikovaných koronavirem v jejich okolí za drobný poplatek. Platební brána však slouží jen ktomu, aby se k útočníkům dostaly informace o platební kartě podvedeného člověka. MF DNES už dříve informovala například o podvodných e-shopech nabízejících respirátory a roušky.
Hrad se stal terčem kybernetického útoku. Data šla k hackerům do zahraničí

„V souvislosti s koronavirem bychom chtěli varovat před možnými phishingovými útoky (získávání citlivých údajů) , kdy by mohlo být využito obav běžných uživatelů například pod záminkou předání „spolehlivých“ informací o koronaviru. Dále bychom chtěli varovat před možnými podvody přes e-shopy o nákupu ochranných prostředků, kdy by mohlo dojít k nedodání zaplaceného zboží,“ dodal mluvčí NCOZ Ibehej.

Autor: Karel Hrubeš

Celý článek naleznete zde.