Ranní Plus

Publikováno: 9. 4. 2026, 8:08
Zdroj: Ranní Plus (ČRo Plus)

---

*Tolik tedy mluvčí Vojenského zpravodajství Jan Pejšek a já už zvu do vysílání **Ondřeje Filipa**, ředitele **CZ.NIC**. Dobrý den.*

Dobré ráno.

O jaký typ hackerských útoků v tomto případě vlastně šlo?

*No tak jak už bylo řečeno, byly právě napadeny ty domácí routery. Princip byl takový, že dokázali změnit konfiguraci toho routeru, že začal využívat jiné takzvané **DNS servery**. To jsou servery, které se starají o to, aby se internetová jména přeložila na čísla. Tedy například když napíšu plus tečka rozhlas tečka cz, tak se dostanu na, tak dostanu číslo, což už je číslo serveru vaší stanice a právě vidím ty vaše webové stránky. Takže ve chvíli, kdy napadnete tuhletu službu, tak můžete uživatele takového routeru přesměrovat třeba na nějaké jiné servery, které pak právě mohou analyzovat to, co tam posíláte nebo snažit se vám ukrást hesla a nějaké další vlastně informace o vás.*

No a proč se zaměřili na malé a domácí kanceláře?

Tak já myslím, že to je hlavně proto, že tyto routery jsou často nebo tato zařízení jsou často poměrně špatně zabezpečené. Zatímco v práci nebo v kancelářích máme obvykle nějaké, někoho profesionálního, kdo se o ta zařízení stará a ta úroveň zabezpečení je samozřejmě vyšší, tak pochopitelně doma nikoho takového obvykle nemáme a to zabezpečení těchto domácích zařízení je slabší. Často lidé třeba zapomínají i takové banální věci, jako změnit si, eh, to tovární nastavení, továrně nastavené heslo nebo, nebo něco takového. Takže tyto routery jsou zranitelnější. A přesto dnes z domova poměrně běžně komunikujeme právě třeba do, do práce nebo posíláme si e-maily s nějakými, řekněme aspoň trochu citlivými informacemi.

A podařilo se zjistit, k jakým datům se hackeři dostali?

Tak bylo řečeno, že se především zaměřili na e-mailovou komunikaci. Jednak na zprávy, které byly posílány, zároveň na nějaká jména, hesla. Samozřejmě dalším nešvarem některých lidí je, že používají stejná hesla do více služeb, takže i to mohlo potom ty útočníky dál navést. Nicméně úplně konkrétní nebylo, nebylo ta zpráva. Nicméně víme, že se, že se snažili zaměřit především na lidi, kteří se pohybují, řekněme, v nějakých citlivých oblastech toho státu.

K čemuž se tedy vztahuje ta otázka, k čemu jim ty údaje mohly sloužit?

Tak ve chvíli, kdy monitorujete, byť třeba i soukromou korespondenci takových lidí, tak můžete samozřejmě postupovat dál. Můžete jejich jménem poslat nějakou zprávu. Můžete se možná třeba někdy dostat i do těch firemních systémů v případě, že jsou třeba slaběji zabezpečené. Takže těch možností je celá řada. Tato skupina se asi zaměřuje spíše na citlivé informace, ale kdybych to měl říct obecně, tak ve chvíli, kdy nějaký útočník ovládá váš e-mail, tak samozřejmě může třeba posílat vaším jménem zprávy vašim blízkým, vyvolat u nich nějakou akci, nechat si poslat peníze, což jak říkám, nebyl tento případ, a může udělat zkrátka celou řadu věcí. A pomocí e-mailu se vlastně můžete dostávat i do dalších služeb, když si třeba resetujete heslo a necháte si ho poslat e-mailem.

A dá se takovým útokům předcházet? Dají se nějak lépe zabezpečit ty domácí routery?

No, především je třeba si uvědomit, že ten domácí router je poměrně důležitý prvek, že přes něj chodí veškerá vaše komunikace, jste-li doma. Takže nepodcenit výběr toho routeru, zvolit značky,

které mají nějakou dlouhodobější podporu, které prostě mají nějaké renomé, že se starají o ty bezpečnostní problémy. Určitě změnit okamžitě ta hesla, ať už heslo na Wi-Fi, heslo do toho přístroje. A také myslet na to, že je to přístroj jako každý jiný a ta podpora někdy končí. Takže sledovat, kdy končí podpora toho routeru, kdy už se nevydávají nové verze firmwaru a v takovém případě samozřejmě to zařízení měnit. Tak, jak jsme zvyklí měnit telefon nebo počítač, tak nezapomínat, že i ty routery mají jenom omezenou životnost. A nejde o hardwarovou, ale o tu softwarovou podporu.

I přesto, když se to zabezpečení routeru překoná nebo když ho hacker překoná, mohou být moje data chráněna, mám-li dobře vytvořená hesla v počítači?

Vlastně tak trochu ano. Důležité je samozřejmě sledovat to, co se děje, jestli se neobjeví nějaká anomálie. Obvykle ta komunikace dnes je již šifrovaná, zabezpečená, a pokud se třeba objeví vám na vašem počítači hláška, že ten certifikát je neplatný, tak v tu chvíli to je taková indikace, že se děje něco špatného. Může to být samozřejmě technická chyba, ale rozhodně v tu chvíli nepokračovat třeba v přihlašování do té dané stránky, protože to je jasná indikace, že se děje něco nestandardního. Může jít o technickou chybu, ale je velice pravděpodobné, že může jít právě o nějaký takovýto typ útoku. Takže to jsou taková varování, která bychom měli brát vážně a okamžitě vlastně zjistit, třeba poradit se s nějakým odborníkem, co se mohlo stát.

*Varuje ředitel **CZ.NIC Ondřej Filip**, který byl hostem Ranního Plusu. Děkuji, na slyšenou.*

Děkuji za pozvání, na shledanou.