**Hackeři mohou díky Ripple20 ovládat řadu zařízení, například tiskárny, ale i medicínské přístroje**

**Praha, 27. listopadu 2020 –** **Nedávno objevené zranitelnosti, o nichž se mluví jako o Ripple20, umožňují útočníkům zneužít nebo vyřadit z provozu širokou škálu koncových zařízení, například tiskáren, síťových prvků nebo různých čidel a kontrolérů. Problém se týká milionů přístrojů od renomovaných výrobců a může ohrozit společnosti z mnoha oborů – od výroby, přes kancelářské provozy, energetiku, až po zdravotnická zařízení.**

**Co je Ripple20**

Sada zranitelnostíoznačovaná jako Ripple20(Vlna 20) je soubor 19 zranitelností vycházejícíchz chyb softwarové knihovny systému, který se nachází v milionech zařízení renomovaných výrobců. Jedná se tedy o problém, který zasahuje firmy z mnoha oborů podnikání po celém světě.

„Sada zranitelností Ripple20 vychází z chyb softwaru společnosti Treck Inc., jejíž jméno běžnému člověku moc neřekne. Ale její programové knihovny se nacházejí v milionech zařízení renomovaných výrobců jako například HP, Dell, Cisco, Intel, Xerox, Cat, ABB, Schneider Electric a dalších,“ upřesňuje Michael Grafnetter, odborník na IT bezpečnost Počítačové školy GOPAS.

**Na co umožňuje útočit**

Děravá knihovna se vyskytuje v systémech využívaných v průmyslu, maloobchodu, dopravě i energetice. Útočníci mohou získat plnou kontrolu nad napadenými zařízeními, takže jsou schopní upravit jejich chování nebo je úplně vyřadit z provozu.

„Odhalené chyby implementace protokolu TCP/IP umožňují nejen na dálku zcela ovládnout napadené přístroje, ale také proniknout do firemních počítačových sítí, v nichž jsou zapojená. Jedná se o velmi široké spektrum zařízení – od tiskáren, přes napájecí a záložní zdroje, síťové prvky, medicínské přístroje, až po průmyslové kontroléry a čidla, například i pro sledování úniku radiace,“ říká Michael Grafnetter.

**Co s tím?**

Řešení situace není jednoduché. Jednak jde o velmi široké spektrum zařízení, která přicházejí v úvahu. Navíc jde o systémy, které často bývají pod správou externích dodavatelů. Firmy by tedy v první řadě měly zmapovat, jakých z jejich zařízení se tato zranitelnost může týkat a kdo se o ně stará. Pak je třeba udělat preventivní opatření.

„V první řadě je třeba zajistit plošnou aktualizaci firmwaru potenciálně zranitelných zařízení. V tom je ale problém, protože softwarová chyba sahá až 20 let dozadu, mnohé stále funkční přístroje už nejsou výrobci podporovány, takže aktualizace pro ně nejsou k dispozici. Pak nezbývá než taková zařízení v síti izolovat, monitorovat, a ideálně časem nahradit novými. To ale může vyžadovat nemalé finanční prostředky. Proto je pravděpodobné, že o Ripple20 ještě uslyšíme,“ uzavírá Michael Grafnetter.

O společnosti GOPAS, a. s.

Počítačová škola GOPAS je největším poskytovatelem školení v oblasti informačních technologií na českém i slovenském trhu. Ročně absolvuje odborné kurzy téměř 30 tisíc studentů, z nichž většinu tvoří specialisté IT. I přesto, že působí na poměrně malém trhu, patří GOPAS k jedněm z největších poskytovatelů IT školení v Evropě.