Vážené čtenářky, vážení čtenáři,

průmyslové řídicí systémy (ICS) jsou, jak ukazují nedávné studie, pro hackery relativně snadné cíle, a to kvůli špatným návykům spojeným s kyberbezpečností.

Například více než třetina lokalit s ICS má podle studie firmy CyberX minimálně jedno přímé propojení s veřejným internetem. Kdyby tomu tak nebylo, museli by hackeři, aby mohli své nekalé operace vykonat, být přímo na místě. Vyhledávací nástroje, jako je třeba Shodan, přitom výrazně usnadňují nalezení zařízení, která nejsou řádně zajištěná, což útočníkům usnadňuje přístup do průmyslových sítí.

Dalším kritickým bodem jsou bezdrátové přístupové body Wi-Fi – 16 % míst, kde se ICS využívají, má aktivní alespoň jeden bezdrátový přístupový bod a 84 procent má nejméně jedno zařízení přístupné vzdáleně – obě možnosti opět útočníkům usnadňují přístup.

Průmyslové řídicí systémy také často obsahují zabudované operační systémy, které je obtížné aktualizovat, natož změnit operační systém. Polovina systémů má podle CyberX zastaralé a nepodporované verze systému Windows – pro Vista se ukončila podpora v roce 2017, pro XP v roce 2014, pro Windows 7 se má ukončit v roce 2020.

Sedm z deseti lokalit s ICS pak využívá ve svých sítích nezašifrovaná hesla. Jsou obvykle spojené se staršími zařízeními, která nepodporují zabezpečené protokoly jako SNMP v3 nebo SFTP. A více než polovina míst s ICS nemá automatickou aktualizaci antivirových systémů, což zvětšuje příležitost útoku, jak ukázala analýza společnosti Kaspersky Lab.

Nejhorší ale je, že se situace okolo ICS nijak nelepší. Jedinou hmatatelnou změnou od loňské studie bylo snížení počtu lokalit využívajících starší systémy Windows – ze 76 % na 53 %.

ICS je totiž obtížné a nákladné nahradit, takže se nedotčené využívají celé roky. To přináší také další problémy, kdy ICS například využívají protokoly jako třeba Modbus TCP, které nové monitorovací systémy už nepodporují. Podle průzkumu Kaspersky Lab tak prý téměř polovina průmyslových podniků nedokáže detekovat útoky na zařízení ICS.

Zdá se tedy, že ICS představují poměrně závažnou skrytou hrozbu. Abyste ji co možná nejlépe eliminovali, přinášíme v tomto vydání podrobný návod, jak systémy ICS náležitě zabezpečit.

A protože se blíží Vánoce, připravili jsme pro vás i přehled toho, jaká rizika mohou svým nositelům přinést chytré hodinky – o ně je totiž v posledních měsících enormní zájem, a nebude tedy překvapením, když je pod stromečkem najdete i vy.

S přáním příjemně stráveného zbytku roku třeba i nad stránkami SecurityWorldu

Pavel Louda
vedoucí projektu

Obsah