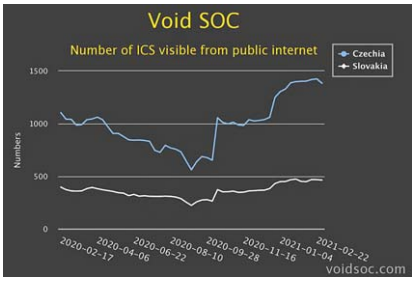
Průmyslové řídicí systémy veřejně dostupné z internetu jsou pozvánkou pro hackery

-soitron-

České firmy stále nechrání své řídicí systémy a přes veškerou osvětu se v tomto ohledu stav zabezpečení dokonce zhoršuje. Počet řídicích systémů (ICS) veřejně dostupných z internetu totiž stoupl od začátku roku o 40 %. Vyplývá to z dat společnosti Soitron a jejího bezpečnostního oddělení Void SOC. Průmyslové systémy se přitom stávají lákadlem pro hackery, kteří mohou zneužít slabin jejich nedostatečného zabezpečení, získat firemní data a omezit provoz podniku.

České průmyslové firmy ve velkém přecházejí na automatizované řídicí systémy a vzdálený přístup je dnes běžně využívanou metodou pro sledování nejen výrobních technologií nebo logistiky, ale například i malých vodních či solárních elektráren. Zabezpečení těchto systémů však pokulhává.

První průzkum společnosti Soitron provedený týmem analytiků Void SOC (Security Operations Center) ukázal, že až 1580 průmyslových podniků v České republice a 509 na Slovensku má svoje průmyslové řídicí systémy (tzv. ICS) dostupné na internetu bez jakéhokoliv zabezpečení. Společnost Soitron identifikované firmy na toto bezpečnostní riziko ihned po odhalení upozornila. Ani po roce ale většina firem problém nevyřešila a jejich systémy jsou stále volně dostupné. Celkový počet „otevřených" ICS se v České republice od začátku roku 2021 dokonce zvýšil o 40 %.



Graf ukazuje, kolik ICS na území ČR a SR je veřejně dostupných z internetu. Zdroj: Void SOC

„Sednout si k počítači a napadnout takhle nezabezpečenou vodní elektrárnu či automatizovaný řídicí systém není nic složitého. V současné chvíli evidujeme například jeden pivovar, který dokonce přešel na novější verzi průmyslového systému, ale stále není zabezpečený. Výrobní linku tak lze z internetu například úplně zastavit," popisuje Martin Lohnert ze Soitronu.

Někdy jde jen o peníze, někdy může jít o život

Útoky na průmyslové systémy mohou způsobit velké škody, ale ve hře nejsou jen peníze. Médii nedávno prošla informace o útoku v americkém městě Oldsmar na Floridě. Ukázal, že ohrožené mohou být i zdroje pitné vody. Hackeři se nabouráním do systému pokusili otrávit louhem zásobárnu vody pro 15 tisíc lidí žijících nedaleko Tampy Bay. *„Automatizovaný systém zde měli velmi špatně zabezpečený. Hackeři se připojili do počítače na regulaci vody, bez jakéhokoliv složitého know-how. Stačilo jim použít běžnou aplikaci a heslo, které v minulosti uniklo a nebylo změněno.,"* podotýká Martin Lohnert a pokračuje: *„Případ z USA je ale jen špičkou ledovce. Situace je v realitě mnohem horší – co se týče zabezpečení i počtu incidentů. Pochopitelně, ne každý napadený subjekt se chce hackerským útokem „vytahovat." A naše průzkumy ukazují, že průmyslné řešení často nemají ani jen to zabezpečení heslem. Netroufnu si ani odhadnout, kolik řídicích systémů na světě lze ovládat přes webovou stránku".*

Jak se chránit před útokem? Podstatný je aktivní přístup firem k otázce ochrany jejích systémů před kybernetickými hrozbami. Nezbytné je také nastavit a pravidelně kontrolovat procesy zaměřené na zajištění kybernetické bezpečnosti ve firmě. *„Stejně důležitý je reakční čas, pokud monitoring kybernetické bezpečnosti zachytí průnik do systémů firmy. Ne každý incident musí skončit špatně, tedy pokud se začne situace řešit okamžitě, jak vznikne. Minimálně tím, že se pokusíte minimalizovat škody, například odpojením napadeného zařízení v provozu. Jednoduše řečeno by všichni měli začít brát bezpečnost vážně,"* říká závěrem Martin Lohnert. ■

Řídicí systém výrobní linky v pivovaru přístupný z internetu. Zdroj: Void SOC