dek opět záleží primárně na druhu příslušného robota a jak se využívá.

Podobně jako u jiných průmyslových systémů spočívá riziko autonomních strojů v neopravených zranitelnostech a přístupu ke kritickým a tajným informacím v pracovním prostředí, dodává Atwood.

Jerry Irvine, šéf IT u outsourcingového poskytovatele Prescient Solutions, tvrdí, že tyto zranitelnosti dávají přístup ke kritickým podnikovým systémům a duševnímu vlastnictví.

Organizacím, které implementují bezpečný přístup a autorizaci, doporučuje, aby přístup omezily pouze na ty pracovníky, kteří jej nezbytně potřebují k výkonu činnosti.

Dalším dobrým zvykem je oddělit autonomní systémy od jiných sítí, což limituje jejich digitální stopu a přístup k jiným systémům a aplikacím.

Jedním z důležitých kroků k zajištění vysoké bezpečnosti robotů je pečlivě je hlídat. „Správa protokolů a operačních postupů robota člověkem a celkově dohled lidí nad roboty musí být v blízké budoucnosti vždy co nejdůkladnější," vysvětluje Atwood.

Pečlivý dohled výrazně sníží riziko nehod v prostředích, kde roboti pracují, např. v hotelech, továrnách nebo nemocnicích.

Rozhodnutí, kdo ve firmě bude zodpovědný za bezpečnost robotů, závisí na příslušné organizaci. Protože však mohou roboti přesahovat mnoho oblastí, měla by se zodpovědnost rozprostřít přes vícero pracovních skupin včetně IT, bezpečnostního managementu a toho nejvyššího vedení.

V mnoha firmách mají klíčovou roli nejvyšší IT a bezpečnostní manažeři, obzvláště pokud je robotika v daném prostředí úzce spjata s IT prostředím, jako jsou cloudové služby, mobilní aplikace nebo analytika big dat.

„Hlavní bezpečnostní IT manažer a jeho tým by měli mít největší zodpovědnost za jakákoli propojená zařízení včetně robotů," vysvětluje Curran.

„Neměl by být rozdíl mezi robotem s přístupem na síť a routerem."

Důležité jsou samozřejmě také různé kontrolní a monitorovací mechanismy, standardy a procedury, které minimalizují rizika spojená s nasazením robotických technologií do firem, dodává.

Samotní roboti by případně mohli hrát roli v bezpečnostním týmu.

„Roboty pro detekci fyzických narušení již vyvinulo mnoho společností. Obvykle jde o skupiny malých mobilních robotů s kamerami a detektory pohybu, kteří se pohybují po budově a hledají možná narušení," popisuje Curran.

Tyto stroje využívají technologie typu kamer s vysokým rozlišením, snímače nebo mikrofony. „Vždy existuje šance na hacknutí robotů – dodatečné bezpečnostní prvky by tedy měly hrát určitou roli – například rozpoznání obličeje správce robotů," dodává Curran.

Podle něj existuje skutečné nebezpečí z narušení soukromí, obzvláště pokud má robot možnost zcela volně se v budově pohybovat.

„Je tedy nutné zajistit, že se příslušné nahrávky budou i bezpečně ukládat." ■

Co ukázala analýza domácího routeru?

SoHo (Small office/Home office) je v angličtině používaná zkratka pro „malé" domácí routery a modemy. Avšak v dnešní době se častěji přezdívají jako SoHopeless vzhledem k trvajícímu nezájmu o jejich bezpečnost ze strany výrobců.

MARTIN KUNC

Možná si vzpomenete na 900 tisíc routerů napadených koncem loňského roku v Německu. Počet zranitelných zařízení se dokonce odhadoval na pět milionů. Jak může vypadat analýza takového zařízení? Jedna taková analýza se uskutečnila nedávno v Národním bezpečnostním týmu CSIRT.CZ.

I zařízení zajišťující provoz domácí sítě s přístupem k internetu se stále vyvíjejí. Dnes už bývá standardem USB port pro sdílení souborů či připojení tiskárny a Wi-Fi už je prakticky samozřejmostí.

[Běžný router by neměl mít z vnějšku dostupné prakticky vůbec nic.]

Nazývání takového zařízení routerem je poněkud nepřesné, protože zpravidla obsahuje i switch, bezdrátový přístupový bod a často i jiné funkcionality jako například VPN server.

Je dobré také rozlišovat zařízení určené pro prodej koncovým uživatelům (např. v e-shopu) a zařízení, které výrobce typicky prodá poskytovali připojení k internetu (ISP) a ten je pak nasadí u svých zákazníků.

Do druhé kategorie, často označované zkratkou CPE (Customer Premise Equipment), pak spadají například ADSL modemy. CPE pak většinou zůstávají ve správě ISP a uživateli zůstane jen malý prostor pro případnou konfiguraci své vlastní sítě.

Právě pro vzdálenou správu těchto zařízení ISP používá protokol TR-069, který standardně využívá TCP port 7547, případně nově objevující se port 5555.

Následující analýza jednoho takového zařízení se uskutečnila na základě automatického hlášení jed-