Víc než polovina firem už využívá ve svém provozu AI a IoT

8.3.2024 - | PROTEXT

Propojené technologie představují rostoucí síť zařízení, systémů a aplikací připojených k internetu a k sobě navzájem. Umožňují provádět transformaci firem prostřednictvím shromažďování většího množství dat a automatizací procesů. Přinášejí však také nová rizika a problémy při zabezpečení firemních aktiv a ochraně zákazníků.

Společnost Kaspersky vypracovala studii „Connecting the future of business“, která má firmám pomoci udržet si náskok před změnami, které propojené technologie přinášejí, a klade zásadní otázky ohledně způsobu, jakým se jim musí přizpůsobit kybernetická bezpečnost. Za tímto účelem byl proveden průzkum mezi 560 vedoucími pracovníky v oboru IT bezpečnosti ze Severní Ameriky, Latinské Ameriky, Evropy, Středního východu, Afriky, Ruska a asijsko-pacifického regionu.

V tomto průzkumu se společnost Kaspersky snažila zjistit, co si respondenti myslí o následujících propojených technologiích:

Z průzkumu vyplynulo, že AI využívá již 54 % a IoT 51 % firem. Každá třetí je plánuje nasadit do dvou let. Datové prostory využívá 32 % firem a téměř polovina (49 %) je hodlá používat v blízké budoucnosti.

Další propojené technologie (digitální dvojčata, rozšířená realita, virtuální realita, web 3.0, 6G) využívá zatím pouze pětina (20–21 %) firem zapojených do průzkumu, ale více než 70 % z nich uvažuje o jejich brzké integraci do svých provozních procesů.

Rozšíření AI a IoT s sebou přináší zranitelnost novými způsoby vedení kybernetických útoků. Podle průzkumu si 16–17 % organizací myslí, že AI a IoT je „velmi obtížné“ nebo „mimořádně obtížné“ chránit, zatímco pouze 8 % uživatelů AI a 12 % provozovatelů IoT se domnívá, že jsou jejich firmy plně chráněny.

Jak je však vidět, čím méně je implementace těchto technologií rozšířená, tím složitější je pro firmy jejich ochrana a naopak. Například nejméně rozšířené technologie AR/VR a 6G jsou z hlediska kybernetické obrany nejproblematičtější a podle vyjádření 39–40 % firem je jejich zabezpečení obtížné.

„Propojené technologie přinášejí obrovské obchodní příležitosti, ale také novou éru zranitelnosti vůči závažným kybernetickým hrozbám. S rostoucím množstvím shromažďovaných a přenášených dat je nutné posílit opatření kybernetické bezpečnosti. Firmy, které integrují AI a IoT do svojí infrastruktury, by ji měly chránit pomocí řešení Container Security a Extended Detection and Response, aby odhalily kybernetické hrozby již v rané fázi a zajistily tak účinnou obranu,“ komentuje **Ivan Vassunov**, viceprezident pro firemní produkty společnosti Kaspersky.

Kaspersky doporučuje **čtyři účinné způsoby, jak zajistit, aby byly organizace připraveny na ochranu propojených technologií:**

1. Postupujte podle zásad „secure-by-design“ (bezpečné díky návrhu). Integrací kybernetické bezpečnosti do každé fáze životního cyklu vývoje softwaru se software a hardware splňující podmínky „secure-by-design“ stávají odolnými vůči kybernetickým útokům a přispívají k celkové bezpečnosti digitálních systémů. Například řešení založená na systému KasperskyOS, umožňují

firmám minimalizovat míru ohrožení a výrazně snížit schopnost kyberzločinců provést úspěšný útok.

2. Zajistěte školení a zvyšování kvalifikace zaměstnanců. Vytvoření kultury kybernetického povědomí vyžaduje komplexní strategii, která umožní zaměstnancům získávat znalosti a využívat je v praxi. Odborníci na informační bezpečnost si mohou pomocí školení Kaspersky Expert training prohloubit svoje dovednosti, aby dokázali lépe bránit firmy před útoky.

3. Upgradujte svá řešení kybernetické bezpečnosti a používejte centralizované a automatizované platformy, jako je například Kaspersky Extended Detection and Response (XDR). Spolu se zaváděním propojených technologií potřebují firmy také řešení kybernetické bezpečnosti s pokročilejšími funkcemi, které jim umožní shromažďovat a korelovat telemetrii z různých zdrojů a provádět účinnou detekci hrozeb s rychlou automatickou reakcí.

4. Dodržujte příslušné směrnice, abyste se vyhnuli právním problémům nebo poškození pověsti, a zajistěte, aby vaše postupy v oblasti kybernetické bezpečnosti splňovaly měnící se normy a právní požadavky.

ČTK ke zprávě vydává obrazovou přílohu, která je k dispozici na adrese https://www.protext.cz.

https://www.ceskenoviny.cz/tiskove/zpravy/vic-nez-polovina-firem-uz-vyuziva-ve-svem-provozu-ai-a-iot/2490122