visních prohlídek a naléhavých oprav. V případě neočekávané události firmy rychle obnoví výrobu díky servisu a náhradním dílům z globální distributorské sítě UR. Služba Service360 tak zákazníkům přináší klid, který potřebují pro své podnikání.

Služba je dostupná ve dvou balíčcích. *UR Basic Warranty* je součástí dodávky každého robotu, pokrývá záruku po dvanáct měsíců a zaručuje průměrnou dobu odezvy do 4 h. Součástí je řešení požadavků prostřednictvím techniků firmy UR a její globální sítě partnerů. K dispozici je také zákaznický portál myUR – online platforma pro správu servisních požadavků, komunikaci s odborníky, zobrazování případů z minulosti a vyhledávání informací a návodů v databázích. Náklady jsou kryté zárukou. Tento balíček je v pořizovací ceně robotu.

UR Service360 Basic lze dokoupit kdykoliv během záruční doby zařízení a přizpůsobit se tak každému firemnímu rozpočtu. Nabízí opakované rozšíření záruky o dvanáct měsíců, průměrnou dobu odezvy do 4 h a zákaznický portál myUR. Mezi hlavní výhody patří předvídatelnost výroby díky jistotě provozuschopnosti robotu: 60 % problémů je vyřešeno obratem. Všechny díly a náklady na servis jsou již obsaženy ve službě. Zákazník má přímý kontakt na odborníky UR. Služba se přizpůsobuje potřebám zákazníka – jde o týmový proces zákaznické podpory ze strany UR společně s lokálním distributorem.

Prevence místo opravy

Společnost Universal Robots chce, aby zákazníci za své investice do kolaborativních robotů dostali co nejlepší služby. Všechny produkty UR Service360 zahrnují opravy prováděné zkušenými inženýry UR přímo na místě nebo na dálku. To zajišťuje, že robot bude pracovat optimálně, a pomáhá zkrátit dobu návratnosti investice do jeho pořízení. Plány provedení servisních prohlídek je možné přizpůsobit plánům zákazníků.

Podrobnosti o službě Service360 zájemci najdou na webu Universal Robots: https://www.universal-robots.com/cs/produkty/ur-service360/.

(*Universal Robots*)

Průzkum Acronis k World Cyber Protection Week: již 42 % firem zažilo výpadky v důsledku ztráty dat

Společnost Acronis uvedla u příležitosti World Cyber Protection Weeku, který je pokračováním Světového dne zálohování (31. března), že opět narostl počet uživatelů, kteří zažili ztrátu dat či zařízení s daty. V oblasti firemních informačních systémů se více firem setkalo s výpadky provozu v důsledku ztráty dat a administrátoři IT v důsledku toho zvyšují frekvenci zálohování.

Průzkum společnosti Acronis je již v pořadí pátý, který od roku 2016 pravidelně provádí u příležitosti Světového dne zálohování. Letos jej společnost rozšířila i na skupinu administrátorů IT, kteří zodpovídají za firemní komunikační infrastruktury. Bylo dotázáno na tři tisíce respondentů z celého světa: běžných uživatelů i firemních profesionálů na IT. Není překvapením, že podle výsledků zpracovaných na základě průzkumu se obě skupiny výrazně liší, jak zodpovědností k ochraně dat, tak i způsobem zabezpečení.

Nejzajímavější údaje z letošního průzkumu:

- 68 % běžných uživatelů již zažilo ztrátu dat či zařízení, ať již svých, či rodinných příslušníků, což je o 3 procentní body více než při loňském dotazování,
- 42 % firem zažilo výpadky provozu v důsledku ztráty podnikových dat, což je o 12 procentních bodů více než vloni,
- i když většina (51 %) běžných uživatelů stále zálohuje lokálně, 31 % již zálohuje do cloudu (o 5 procentních bodů více než loni) a 17 % kombinovaně (o 7 procentních bodů více než vloni),
- administrátoři firemních informačních systémů zálohují z 25 % lokálně, 35 % jich zálohuje do cloudu, 20 % kombinovaně a zbylých 20 % replikuje data do jiných datových center,
- výrazně narostly obavy běžných uživatelů z ransomwarových útoků (o 29 %), cryptojackingu (o 31 %) a sociálního inženýrství (o 34 % bodů),
- na firemní úrovni se zvyšuje frekvence zálohování: významně přibylo administrátorů IT, kteří zálohují alespoň jednou denně (nyní 27 %) nebo vícekrát za den (nyní 15 %), naopak rychle ubývá těch, kteří zálohují pouze jednou či dvakrát za měsíc (nyní 20 %).

„Povědomí o kybernetických hrozbách mezi běžnými uživateli rychle roste, což je důsledek osobní zkušenosti se ztrátou dat a také množících se zpráv o kybernetických útocích," uvedl Zdeněk Bínek, zodpovědný za prodej řešení Acronis v ČR a na Slovensku. „Avšak z průzkumu je patrné, že stále existuje velký rozdíl v přístupu mezi běžnými uživateli a IT profesionály. U těch oceňujeme zejména trend častějšího podnikového zálohování, protože čím je frekvence nižší, tím se zvyšuje i riziko ztráty většího množství dat a náklady na jejich obnovu."

Více informací o průzkumu lze nalézt na https://www.acronis.com/en-us/blog/posts/how-cyber-protection-trends-are-evolving-2020.

[Tisková zpráva Acronis, 2. dubna 2020.]

(*ed*)

Ransomware

Ransomware je vyděračský software, který zamyká přístup k infikovanému zařízení nebo šifruje jeho obsah. Po uživateli požaduje výpalné s tím, že po zaplacení bude zpřístupněno zařízení nebo budou odšifrována data. Obnovení přístupu k datům po zaplacení výpalného však není zaručeno.

Cryptojacking

Cryptojacking je parazitická těžba kryptoměn, při níž útočník využívá zdroje napadeného počítače (popř. routeru, IP kamery nebo zařízení IoT) pro vlastní obohacení. Výrazně tak snižuje výpočetní výkon dostupný pro skutečného vlastníka zařízení. Aktivita tohoto malwaru narůstá zejména v době růstu kurzu kryptoměn.

Sociální inženýrství

V oblasti zabezpečení dat a informací se jako sociální inženýrství označuje snaha od uživatelů podvodem vylákat jejich hesla, bankovní údaje nebo jiné informace. Nejběžnější formou je e-mailový phishing: rozesílání e-mailových zpráv, které se tváří jako zpráva z banky, informace spediční služby, letecké společnosti apod. Útočník často zneužívá osobní údaje, k nimž se dostal jinou cestou (odchycené rodné číslo, číslo účtu, číslo letenky, informace o zásilce, informace o technickém problému s počítačem, který oběť řešila s technickou podporou, apod.).