Celkové množství strojů určených pro robotický sběr ovoce využívaných v praxi je zatím velmi malé. Z technického hlediska jejich většímu rozšíření nic podstatného nebrání, je však nutné zvyšovat jejich robustnost a spolehlivost, snižovat náklady na jejich pořízení i provoz a zkracovat návratnost. Stále je prostor k postupnému zlepšování produktivity a využitelnosti těchto robotů. Zvyšování jejich podílu na trhu je tedy jen otázkou času.

Bezpilotní letouny – drony

Drony jsou stále běžnější součástí zemědělské praxe. V současné době jsou nejčastěji využívány pro letecké snímkování porostů. Pomáhají zlevnit sběr dat a zlepšit rozlišení leteckých snímků. Technika je zemědělcům stále dostupnější, ať jako koncovým uživatelům, nebo formou služby (*obr. 4*).

Základem dronu je jeho univerzální hardwarová platforma. Trh v této oblasti nyní prochází dosti výraznou konsolidací, na jejímž konci jej pravděpodobně ovládne jen několik etablovaných výrobců. Platformy dronů budou běžně dostupné za přijatelnou cenu.

Více pozornosti je třeba věnovat softwaru pro sběr dat a jejich analýzu a souvisejícím službám. Mnoho firem nabízí letecké snímkování jako službu, včetně analýzy dat, od jednoduchého indexování (např. NDVI – *Normalized Difference Vegetation Index*) po zpracování komplexnějších analýz.

Počítá se také s tím, že se rozšíří postřikové drony. Například v Japonsku se k postřikování rýžových polí používají už od začátku 90. let minulého století na dálku řízené helikoptéry. Ty se sice osvědčily, ale jejich využití se mimo Japonsko zatím nerozšířilo. Zde je zatím mezera na trhu.

Obr. 5. Robotizovaný systém dojení DairyProQ (foto: GEA DairyRobot)

Roboty v mléčných farmách

Mléčné farmy se zabývají chovem dojeného skotu. Automatizované dojení se v mléčných farmách používá už 25 let. Jde o osvědčenou techniku rozšířenou po celém světě a trh s ní neustále roste. Pro další rozvoj dojicích robotů je zapotřebí vyřešit dva problémy: robotické rameno musí být tak robustní, aby vydrželo i v nepříznivých podmínkách, např. když je zvíře nakopne, a za druhé je třeba zdokonalit mechanismus lokalizace struků, často založený na měření změn vzoru promítaného na vemeno.

Kromě pevných dojicích robotizovaných stanovišť (*obr. 5*) získávají v živočišné výrobě na oblibě též mobilní roboty pro automatické krmení.

Další informace

Kompletní studie s názvem *Agricultural Robots, Drones, and AI: 2020-2040: Technologies, Markets, and Players* je dostupná u společnosti IDTechEx a lze si ji objednat na research@IDTechEx.com.

Khasha Ghaffarzadeh, IDTechEx

S Linuxem jste v bezpečí?

V průmyslové automatizaci se z mnoha důvodů často používají operační systémy Linux. Linux nezřídka bývá součástí nejen podnikových serverů, ale i kritických řídicích systémů průmyslových provozů. Kromě flexibility a schopnosti zajistit práci v reálném čase je argumentem i to, že Linux je považován za bezpečnější a méně náchylný ke kyberhrozbám než operační systémy Windows. Platí to opravdu? Odborníci z firmy Kaspersky v poslední době pozorují trend, kdy stále více kyberzločinců cíleně útočí na systémy s Linuxem a zároveň vyvíjí nástroje zaměřené na tento operační systém v rámci tzv. APT – *Advanced Persistent Threat*.

Za posledních osm let odborníci zaznamenali asi dvanáct kyberzločinců či skupin, kteří používali malware APT zaměřený na Linux. Patří mezi ně skupiny Barium, Sofacy, Lamberts, Equation nebo nedávné kampaně LightSpy z dílny TwoSail Junk a WellMess. Díky diverzifikaci svého arzenálu a jeho rozšíření o linuxové nástroje jsou kyberzločinci schopni útočit efektivněji a s větším dosahem.

„Spousta velkých korporací napříč všemi světadíly začíná v posledních letech častěji používat Linux jako hlavní operační systém na svých počítačích. Tento trend se týká i počítačů vládních subjektů, a proto se častěji setkáváme s hrozbami zacílenými na tuto platformu. Mýtus, že je velmi malá pravděpodobnost, že by hackeři útočili na Linux vzhledem k jeho malému rozšíření, jen dává prostor dalším kyberhrozbám. I když jsou zacílené útoky na Linux stále raritou, malware určený pro tento druh útoků existuje, a to včetně webshellů, backdoorů, rootkitů, a dokonce i na míru vyvinutých exploitů. Úspěšná infekce Linuxu mívá navíc dalekosáhlé následky, protože hackeři mohou získat přístup nejen do napadeného zařízení, ale i do zařízení běžících na Windows nebo macOS," uvádí tisková zpráva firmy Kaspersky. Jako příklad jmenuje Kaspersky ruskojazyčnou skupina Turla a novou verzi linuxového backdooru Penguin_x64, která byla poprvé detekována z kraje tohoto roku a podle telemetrie společnosti Kaspersky do července infikovala desítky serverů v Evropě a v USA.

Firma Kaspersky proto dává uživatelům Linuxu tato doporučení:

- vytvořte seznam důvěryhodných zdrojů softwaru a nepoužívejte nezašifrované kanály pro aktualizace,
- nespouštějte binární soubory a skripty z nedůvěryhodných zdrojů,
- ujistěte se, že pravidelně provádíte aktualizace a instalujete bezpečnostní záplaty,
- věnujte čas správnému nastavení firewallu – ujistěte se, že zaznamenává aktivitu v síti, blokuje všechny nepoužívané porty a minimalizuje vaši síťovou stopu,
- používejte klíče k SSH autentifikaci a klíče chraňte hesly,
- používejte dvoufaktorovou autentifikaci a důležité přístupové klíče mějte uložené na externích tokenech (např. Yubikey),
- používejte out-of-bound síťový tap k nezávislému monitorování a analýze síťové komunikace vašich linuxových systémů,
- udržujte systémovou integritu spustitelného souboru a pravidelně kontrolujte změny konfiguračních souborů,
- buďte připraveni na útoky zevnitř organizace – proto používejte šifrování celého disku a důležitý hardware opatřete bezpečnostní páskou, která indikuje neoprávněnou manipulaci,
- provádějte audit systému a kontrolujte protokoly, zda neobsahují indikátory útoku,
- používejte speciální bezpečnostní řešení s ochranou pro Linux, jako je Integrated Endpoint Security od firmy Kaspersky.

[Kaspersky: *Pokročilé trvalé hrozby častěji útočí na Linux*. Tisková zpráva, 23. září 2020.]

(*Bk*)