Sledování pohybu osob a zařízení pro zabezpečovací úlohy

Společnost SECURITAS ČR vyvinula v České republice unikátní službu Securitas Device Motion Monitoring (DMM), která umožňuje sledovat přítomnost a pohyb mobilních a jiných zařízení a osob ve střeženém prostoru, sbírat a vyhodnocovat data a vizualizovat je s pomocí digitálního 3D modelu. Společnost službu nabízí jako součást konceptu zabezpečení, avšak možnosti jejího využití jsou velmi široké. Podmínkou konkrétní instalace je vždy soulad s nařízením GDPR a dalšími normami souvisejícími s ochranou soukromí.

Bezpečnostní agentura Securitas ČR představila novou službu, která je v segmentu komerčních systémů pro zabezpečení objektů unikátní. Securitas Device Motion Monitoring (DMM) díky kombinaci několika metod dovoluje sledovat a vizualizovat pohyb zařízení a osob ve střeženém prostoru.

Obr. 1. Jan Peroutka, technický ředitel SECURITAS ČR

Původně byla určena k použití všude tam, kde fyzická ostraha není dostatečně efektivní, kde by instalace kamerového systému byla příliš nákladná a kde je třeba ochránit rozsáhlý prostor před vstupem nepovolaných osob. „Securitas je firma s dlouhou tradicí a konzervativním myšlením," říká Jan Peroutka, technický ředitel firmy Securitas ČR. „Tradiční přístup znamená opevnit a chránit hradby objektu. Náš nový systém DMM ale zjišťuje, co se děje uvnitř hradu."

Systém, který vznikl na základě spolupráce agentury Securitas ČR s několika dalšími firmami a start-upy, má široké možnosti použití, i mimo zabezpečovací systémy. „Securitas poskytuje svým zákazníkům zabezpečení objektů, aktiv a osob. Když bude chtít zákazník instalovanou infrastrukturu využít i k jiným účelům, nebudeme mu v tom bránit, nenaruší-li to naše bezpečnostní funkce." Instalovaný systém tak může být využit také k řízení podnikové logistiky, sledování toku materiálu, plánování údržby nebo k řízení technického vybavení budov.

Obr. 2. Digitální dvojče objektu vytvořené v systému od firmy Twinzo

Princip funkce

Základem systému DMM jsou lokátory umístěné v monitorovaném prostoru, které dokážou v závislosti na potřebách konkrétní instalace detekovat přítomná zařízení se signálem Bluetooth LE (BLE, *Bluetooth Low Energy*), RFID nebo WiFi. V praxi může jít např. o detekci zaměstnaneckých čipů nebo přístupových karet s BLE a RFID. Data získaná z lokátorů lze následně v reálném čase zobrazovat v přehledném digitálním 3D modelu daného prostoru (tzv. digitální dvojče), který se vytváří při instalaci jako součást systému DMM.

Zatímco metody sledování pohybu zařízení (RTLS – *Real-Time Locating System*) nejsou na trhu novinkou, Securitas ČR přináší jako první tuto službu v rámci konceptu zabezpečení. Nabízí možnost integrace s kamerovým nebo přístupovým systémem nebo napojení na dispečink Securitas Operation Center, který zajistí okamžitou reakci na definované stavy (např. přítomnost cizího mobilního zařízení ve střeženém prostoru), včetně výjezdu mobilní jednotky a propojení s dalšími službami bezpečnostní agentury.

Možnosti využití služby DMM jsou nesmírně široké: sledování přítomnosti a pohybu zařízení (popř. spolu s osobami, které tato zařízení nosí) v definovaných zónách, měření obsazenosti místností, řízení parkovišť, sledování pohybu v nouzových situacích nebo po zmáčknutí tísňového tlačítka, navigace v objektu či monitorování technologických zařízení.

Ochrana soukromí na prvním místě

Vzhledem k možnostem současné techniky klade Securitas při navrhování a instalaci bezpečnostních systémů dlouhodobě důraz na ochranu osobních údajů. To se týká i služby DMM, u níž v závislosti na typu instalace a způsobu používání může hrozit porušení souladu s GDPR, se zákoníkem práce a dalšími normami. „Data ze systému DMM mohou být buď z principu anonymní, anonymizovaná, nebo spojená s konkrétními osobami, například zaměstnanci či držiteli přístupových karet. Ve všech případech je však soulad s GDPR, zákoníkem práce a dalšími normami už součástí prvotního návrhu každé konkrétní instalace. To je pro společnost Securitas naprosto zásadní," doplňuje Jan Peroutka.

Pilotní projekt v kancelářské budově

První pilotní projekt realizovala firma Securitas ve svém sídle v Kateřinské ulici v Praze. Jde o kancelářskou budovu, do níž přichází množství zaměstnanců i návštěv. Přicházející osoby se sice hlásí ve vrátnici, ale je těžké sledovat, zda jdou skutečně tam, kam udávají. Jediným řešením, ovšem nepohodlným, je to, že si každou návštěvu zajde příslušný pra-

covník k vrátnici vyzvednout a potom ji zase k vrátnici dovede.

Novým řešením situace jsou však čipové karty s komunikací BLE. Jejich pohyb sledují lokátory v jednotlivých místnostech. Jan Peroutka popisuje základní kroky návrhu pilotního projektu: „Nejprve jsme si stanovili střežený prostor, ten jsme si rozdělili na zóny a pro jednotlivé zóny jsme stanovili pravidla a směrnice, co se má stát při detekci narušení. Našim zaměstnancům jsme rozdali karty, které v sobě mají čip pro bezdrátovou komunikaci, nouzové tlačítko a detektor pádu. Je to tedy trochu chytřejší karta než běžná přístupová karta, ale je možné do ní nahrát i standardní přístupový systém."

Připomeňme, že jde o pilotní projekt. V kancelářské budově se nepočítá s tím, že by detektor pádu nebo nouzové tlačítko našly časté uplatnění, ale jde o to, aby se ověřila jejich funkce.

Do jednotlivých místností byly nainstalovány lokátory od finské firmy Quuppa. Jejich výhodou je skutečnost, že kromě síly signálu detekují i směr, z něhož signál přichází. Díky tomu je přesnost lokalizace lepší než 1 m.

Další, velmi podstatnou součástí projektu je vizualizace. Firma Securitas se obrátila na slovenskou firmu Twinzo, která se zabývá tvorbou virtuálních dvojčat např. pro podnikovou logistiku, údržbu nebo řízení budov. Digitální dvojče je potom vizualizováno na mobilním telefonu, tabletu nebo počítači. Primární je přitom vizualizace v 3D aplikaci na mobilních zařízeních – zde je ovládání nejpohodlnější a zobrazení nejpřehlednější.

Příklad vizualizace je na *obr. 2*. Sledované čipy jsou zde znázorněny oranžovými kuličkami.

V pilotním projektu si firma Securitas vyzkoušela nejen přístupové karty, ale i čipy instalované např. v notebookoch. U notebooku je možné sledovat, zda se vyskytuje ve střeženém prostoru, nebo zda si jej někdo odnesl domů. V případě, že se notebook nevrátí, je možné zpětně na základě záznamu z vrátnice identifikovat, kdo si ho mohl odnést.

Po kliknutí na jednotlivé kuličky ve vizualizaci se zobrazí, komu karta nebo čip patří. Potom záleží na přístupových právech, jaké informace se zobrazí dále. Může to být záznam, kde se osoba nebo sledovaný předmět toho dne pohybovaly, kolik lidí a jak dlouho pobývalo v dané zasedací místnosti apod.

V praxi je tak možné např. sledovat, kolik času tráví zaměstnanci na svém pracovišti u výrobní linky a kolik intenzivním teambuildingem v kuchyňce nebo kuřárně. Je jednoduché nechat během přestávky ležet kartu na pracovním stole. Potom je otázkou přístupového systému, zda se pracovník bez karty bude moci vrátit zpátky na pracoviště. Opět je třeba myslet, hned od počátku plánování projektu, na GDPR a zákoník práce. Počítá se s tím, že v objektu budou zamaskované zóny, kde zaměstnanci nebudou sledováni.

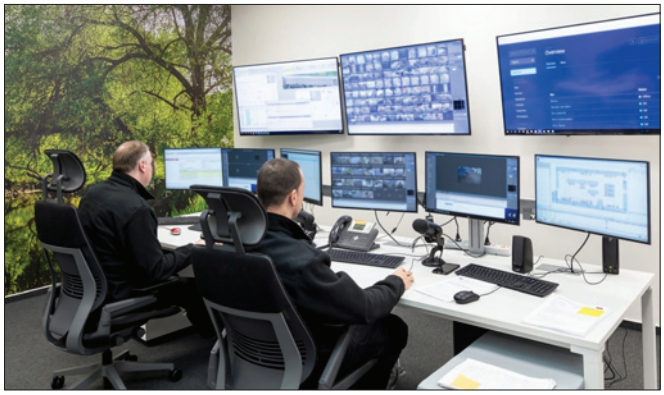
Stejně je možné sledovat např. vysokozdvižné a manipulační vozíky. Systém umožňuje zjistit, kde právě jsou, ale i to, kudy jezdily. Tyto informace potom mohou být využity k optimalizaci vnitropodnikové dopravy.

Zde je dobré připomenout, že systém není možné použít k zajištění bezpečnosti vozíků. K zamezení kolize vozíku s osobou nebo překážkou je nutné použít bezpečnostní snímače. Požadavky na bezpečnost a zabezpečení jsou různé.

Obr. 3. Digitalizace strážní služby: strážní mohou při své práci využívat vizualizaci DMM v mobilních zařízeních

Povolení k vjezdu

Druhý pilotní projekt byl vytvořen pro správu národního parku. Do chráněných zón je zakázán vjezd motorovými vozidly. Výjimku mají stálí obyvatelé, hosté penzionů a dopravní obsluha. Ti musí mít povolení k vjezdu. Dosud to byly papírové kartičky umísťované za sklo. Jenže chráněné zóny jsou rozsáhlé a kontrola byla jen namátková. Zákaz vjezdu byl proto často porušován.



Obr. 4. Alarmy generované v DMM je možné integrovat do systémů kamerového dohledu, aby se strážní mohli soustředit na podezřelé události

Povolení není vázáno na registrační značku vozidla, sledování vjezdu kamerovým systémem podle registračních značek proto není možné.

V pilotním projektu byly papírové kartičky nahrazeny čipovými a na hranici chráněné zóny byly umístěny jejich čtečky. Výhodou je, že BLE má dosah několik stovek metrů. Čtečky mohou být vybaveny kamerou, která zaznamená registrační značky automobilů, jež projedou bez karty s povolením. Data jsou potom předávána správě parku, která situaci dále řeší.

Sledování chování návštěvníků a cestujících

Další pilotní projekt byl realizován ve středisku Magenta Experience Center společnosti T-Mobile v Praze na Pankráci. Jde o místo, kde je kromě prodejny coworkingový prostor, kavárna, galerie a přednáškové sály. Cílem je sledovat chování zákazníků – nejen jejich počet, ale také to, kde a jak dlouho se ve středisku zdržují a zda se do něj vracejí opakovaně. K tomu se využívají jejich vlastní mobilní telefony s rozhraním Bluetooth a lokátory Quuppa.

Uvažuje se rovněž o využití WiFi. Technicky je to možné, ale firma Securitas v tomto případě začala velmi podrobným rozborem shody s pravidly GDPR. Telefon totiž o sobě prostřednictvím WiFi prozradí mnohem více informací, včetně osobních údajů, než prostřednictvím BTE a je třeba zajistit jejich důslednou anonymizaci. Výhodou by bylo, že prostřednictvím WiFi je telefon detekovatelný i při vypnutém rozhraní Bluetooth, dokonce i když je přepnutý do letového režimu.

Ve čtvrtém pilotním projektu je zadáním sledovat počet cestujících a jejich pohyb v nádražní hale. Opět se využívají jejich mobilní telefony, protože umožňují sledovat i to, kolik cestujících se na nádraží vrací opakovaně, např. jezdí každý den do zaměstnání, a kolik je náhodných cestujících. Alternativní systém s kamerami a rozpoznáváním obličejů je nejen nákladný, ale též problematický z hlediska GDPR.

Vyvinuto v Česku, ambice jsou globální

„Technické řešení DMM jsme navrhli v Česku a na jeho vývoji pracujeme už rok a půl," uvádí Jan Peroutka. „Zatím jsme v České republice úspěšně realizovali uvedené čtyři pilotní projekty a službu budeme dále rozvíjet ve spolupráci s klienty a na míru jejich potřebám. Náš vývoj ale sleduje i mateřská společnost Securitas AB s vyhlídkou na to, že se z DMM stane globální produkt v nabídce naší mezinárodní bezpečnostní agentury."

[Tiskové zprávy společnosti SECURITAS ČR.]
(*Foto a grafika: SECURITAS ČR*)

Petr Bartošík