

JAK SE RODILA
INTEGRA TŘETÍ

STR. 2-3

PROSINEC 2010

UZAVŘENÝ TELEVIZNÍ
OKRUH NEBO
POČÍTAČOVÁ SÍŤ
S KAMERAMI?

STR. 4

ROZPOZNÁVÁNÍ
OBLIČEJŮ NA
STADIONU V KRAKOVĚ

STR. 5

O TRENDCH
V PODNIKOVÉ
BEZPEČNOSTI
S NADHLEDEM

STR. 6-7



BULLETIN INTEGOO

O podnikové bezpečnosti, počítačích, zabezpečovacích technologiích a projektech.
Ale především pro lidi a o lidech.

Vážení čtenáři,

vítám Vás na stránkách prvního čísla bulletinu zákazníků, partnerů a přátel společnosti INTEGOO. To, že se dostal na Vaši obrazovku nebo do Vaší ruky, vypovídá o dvou věcech – především o tom, že jste pro nás důležití, a také o tom, že začínáme s profesionálnější marketingovou komunikací.

Pokračování na str. 2

JAK SE RODILA INTEGRA TŘETÍ

V České republice vznikl jeden z nejpokročilejších systémů pro řízení podnikové bezpečnosti



Pod označením INTEGRA 3 se skrývá mnohem více než „jen“ nová verze softwarového produktu. Výsledkem téměř tříleté práce týmu odborníků na bezpečnost, softwarových architektů a vývojářů je systém, který se sice opírá o zkušenosti ze stovek nasazení předchozích verzí, ale technologicky je na zcela nové úrovni. Systém, který vychází z porozumění, že v kritické situaci záleží na konkrétních lidech a že tito lidé potřebují špičkovou podporu.

Rozhodnutí nespokojit se s postupným drobným vylepšováním dosavadního, ale pustit se do vývoje nového jádra systému padlo na jaře 2008. O několik měsíců později zahájil práci samostatný tým, který působil paralelně s kolegy zaměřenými na rozvoj a podporu systému INTEGRA 2. „Nejsme korporací o tisících zaměstnanců. Vyčlenit samostatný tým na vývoj něčeho, co bude možné nabídnout zákazníkům až za dva roky, nebylo úplně snadné rozhodnutí.

Ale dnes je nesporné, že se rozhodnutí vyplatilo. Vznikla úplně nová kvalita, produkt schopný konkurovat nejlepším a nejdražším produktům na světovém trhu,“ říká manažer produktu INTEGRA Radim Matěja. Pomohlo i to, že společnost INTEGRO získala na vývoj finanční podporu z evropských fondů.

Jde o otázky bezpečnosti, spolehlivost musí být absolutní. Nemůžeme si dovolit přijít k zákazníkovi a zjistit, že něco nefunguje.

Vývoj probíhal podle metodiky TDD (Test Driven Development), která vyžaduje, aby kromě hlavního produktu byly vyvíjeny i testovací programy zaměřené na různé oblasti funkcí. Jak Radim Matěja vysvětluje, je to postup pracný a zdlouhavý, ale dává daleko vyšší jistotu, že výsledný produkt nevykazuje chybovost. Řešení umožňuje při zavedení každé změny nebo dodatečné

funkce rychle zjistit dopady na předchozí funkce, a to bez závislosti na lidském faktoru. Ale kromě toho byl součástí týmu i živý tester – uživatel. „Jde o otázky bezpečnosti, spolehlivost musí být absolutní. Nemůžeme si dovolit přijít k zákazníkovi a zjistit, že něco nefunguje.“

Uživatel na jediné obrazovce vidí, v jakém stavu se nachází jednotlivá čidla nebo celý systém.

15 let zkušeností

Historie systému INTEGRA 3 však začala mnohem dříve než v roce 2008. Sahá až do 90. let, kdy v České republice vznikl systém Graviss, jenž může být označen za jakéhosi pradědečka dnešní INTEGRY. Základní funkce byly stejné – integrace a vizualizace. To znamená, že představoval určité rozhraní mezi technologiemi a bezpečnostním personálem. „Bez podobného software byste v bezpečnostní centrále našli několik různých

bezpečnostních ústředí. Ke každé z těchto ústředí jsou připojena čidla nebo jiná bezpečnostní zařízení v areálu. Když klávesnice začne pípat, strážný zjistí, že má poplach v zóně Kancelář 123, vytáhne manuál a zjišťuje, co má vlastně dělat.“ S programem pro řízení podnikové bezpečnosti vidí pracovník ostrahy na obrazovce mapku areálu a na ní vyznačené místo poplachu. Pomocí jiné obrazovky téhož programu zase vidí, která čidla a zařízení jsou momentálně v jakém stavu. Která jsou aktivní, která vypnutá, kde došlo k poškození apod. Ale nejen to. „Skutečná integrace jde i opačným směrem. Je možné z jednoho bodu ovládat všechna bezpečnostní zařízení a zajistit, aby tato zařízení komunikovala mezi sebou.“

Z pohledu roku 2011 by mohl být Graviss označen za primitivní. Nicméně na svou dobu to byl velmi vyspělý systém a tomu odpovídaly prodejní úspěchy v řadě evropských zemí. Měl vlastně jediný limit – bylo k němu možné připojit

Dokončení ze str. 1



Víme, že skutečný společný úspěch musí být založen na tom, že vše bude dodáno profesionálně a že za projektem zůstane i lidsky dobrý pocit.

Poté, co jsme vyrostli nejen co do počtu zaměstnanců, ale zejména do rozsahu znalostí a úrovně zkušeností a jsou za námi velké úspěšné projekty, rádi bychom Vám více přiblížili naši společnost a její zaměření. Snad to bylo vidět i na naší prezentaci na veletrhu Fire&Security Days a na dalších akcích.

Ale navzdory všem marketingovým poučkám víme, že skutečný společný úspěch je založen na tom, že se s námi bude dobře spolupracovat, že vše bude dodáno profesionálně a za projektem

zůstane lidsky dobrý pocit. To je něco, co nenahradí žádná reklamní kampaň.

Snažíme se, aby něco z našeho přístupu bylo vidět i v tomto magazínu, který je o našich produktech, o projektech a především je pro Vás. Najdete v něm vedle historie a současnosti systému INTEGRA i případovou studii ze stadionu v Krakově nebo trendové články o kamerových systémech a bezpečnostních technologiích obecně.

Pokusili jsme se připravit časopis, který pro Vás bude

zajímavý a užitečný. Pokud Vás cokoliv z jeho obsahu zaujme nebo Vám v něm naopak něco chybí, neváhejte nás kontaktovat. Rádi se budeme společně s Vámi zamýšlet nad bezpečnostními a provozními výzvami, které řešíte, a třeba to bude právě taková debata, která Vás posune k nalezení optimální varianty.

Přeji Vám klidné prožití vánočních svátků a úspěšný rok 2011.

Josef Sikyta

pouze bezpečnostní ústředny Alarmcom / Siemens. Dalším logickým krokem tedy byl vývoj obdobného systému použitelného i tam, kde organizace používá bezpečnostní zařízení různých výrobců.

Pro velkého, pro malého...

Přes několik generací takových informačních systémů se dostáváme do roku 2008, kdy společnost INTEGRO nabízela systém INTEGRA 2. I „dvojka“ byla velmi úspěšná, měla stovky instalací a zákazníci s ní jsou spokojeni. Pohled do budoucnosti řešení však obvykle říká, že dříve či později přestane systém stačit. To byl i případ INTEGRY. Hlavní výzvu představovaly rozsáhlé areály s několika budovami a více řídicími pracovišti. „Představte si, že chcete centrálně řídit areál nebo několik propojených areálů stejné organizace. Nejde vám jen o otázky narušení, ale třeba o to, kdo má mít přístup do které oblasti. Uživatel objektů potřebuje, aby strážník v každém řídicím středisku měli k dispozici všechny informace, které právě oni potřebují. A zároveň chce všechny tyto uživatele podporovat z jednoho místa. V rámci tehdejší INTEGRY by to bylo možné, ale komplikované,“ říká produktový manažer. Tomuto požadavku odpovídá i centralizovaná (serverová) IT architektura nového systému s označením INTEGRA 3.

Systém INTEGRA 3 umožňuje jednotnou správu rozsáhlých areálů s mnoha budovami a několika řídicími středisky. Systém je však dosažitelný i pro toho, kdo chce zabezpečit třeba provozovnu s jedním vchodem a třemi okny.

To ovšem neznamená, že by „trojka“ byla vhodná jen pro rozsáhlé areály. Jednou z novinek je zavedení bezplatných OEM licencí, jež budou dodávány společně

s některými bezpečnostními zařízeními. Systém INTEGRA 3 je tak k dispozici i tomu, kdo chce zabezpečit třeba provozovnu s jedním vchodem a třemi okny.

Pokročilost řešení se projevuje i v jiných rysech systému. Jak Radim Matěja vysvětluje, v INTEGRO si pozorně všímali bezpečnostních problémů, jaké zákazníci řeší, a stavěli systém, který tomu odpovídá. Inspirovat se nechali zkušenostmi a požadavky svých klientů v různých evropských zemích. „Snažili jsme se pochopit, proč výrobci různých bezpečnostních systémů zařazují různé nové funkce, umožnit jejich využití a najít elegantní řešení komplexního bezpečnostního systému.“

Konzultace v ceně

Jednou ze změn je další zjednodušení pro uživatele, kterému nyní stačí jediný letmý pohled, aby viděl, v jakém stavu je systém, nebo pár kliknutí myši k zapnutí oblasti popř. zobrazení živého obrazu kamery. Lze zmínit i robustnější zabezpečení a centrální vytváření provozních deníků, včetně záznamu historie každého připojeného zařízení.

Je zapotřebí projít se zákazníkem různé situace, které mohou nastat, připravit nejlepší možnou reakci a zanést ji do systému.

Ale, jak si v INTEGRO dobře uvědomují, sebedokonalejší informační systém neznamená, že lidé obsluhující systémy nejsou důležití. Naopak jde o to, vybavit je správnými informacemi a dát jim instrukce, co je potřeba v dané chvíli dělat, jak postupovat např. při řešení alarmových událostí. „Řada nasazení je realizována s poskytnutím konzultací k celkovému řešení bezpečnostních systémů. Je zapotřebí projít se zákazníkem různé situace, které mohou nastat, připravit nejlepší možnou reakci a zanést ji do



Systém INTEGRA 3 vzbudil při svém uvedení živý zájem.

systému.“ A právě tady se čerpá z bohatých zkušeností již zmíněných stovek nasazení předchozích verzí. Dodavatel může přinést koncentrované

zkušenosti, postřehy a nápady. To je často stejně důležité stejně jako bezchybně fungující technologie.

NĚKTERÉ ZAJÍMAVÉ RYSY A FUNKCE SYSTÉMU INTEGRA 3

Bookmark server umožňuje ukládání různých značek k videozáznamu (např. průjezd vozidla s určitou SPZ, neplatná přístupová karta, apod.). Uživatel při hledání události nemusí očima procházet dlouhé videozáznamy, ale pouze zadá vyhledávání značky. Výsledkem je seznam videosekvencí patřících ke značce a odpovídající kameře.

Modul Manažer pokrývá většinu funkcí, kvůli kterým bývají nasazovány aplikace pro řízení údržby. Je v něm evidována historie zařízení, opravy a revize, které na něm proběhly, jaká další údržba má být realizována, a kdy. Umožňuje vytvářet pohledy nejen podle typu zařízení, ale také podle zón, částí areálu apod. Výstupem jsou různé tabulkové a tiskové sestavy. Systém sám upozorňuje odpovědné osoby e-mailem na blížící se termíny údržby.

Integrace s informačními systémy je dalším klíčovým rysem, který zákazníky často zajímá. Systém INTEGRA 3 má připravené rozhraní pro export dat do SAP, personalistického systému Elanor a několika dalších systémů často používaných na českém trhu. Je však schopen komunikovat s jakýmkoliv informačním systémem, který pracuje s všeobecně akceptovanými standardy.

UZAVŘENÝ TELEVIZNÍ OKRUH NEBO POČÍTAČOVÁ SÍŤ S KAMERAMI?

Současné trendy v bezpečnostních a průmyslových kamerových systémech podle analytika společnosti INTEGEO Filipa Šelemberka



Svět bezpečnosti a kamerových systémů je se světem IT úzce provázán. Tak úzce, že dnešní kamerové systémy mají blíže k počítačové síti než k televiznímu okruhu. Kamery mají vlastní IP adresu a v centru systému nenajdete videorekordér nýbrž server. To má dopad na podobu a rychlost instalace, možnost provazování s dalšími prvky a systémy, vytváření analýz, bezpečnost celého systému a konec konců i optimální rozlišení, píše Filip Šelemberk v magazínu Security.

Jak připomíná – instalace, přemístování kamer a rozšiřování systémů je dnes záležitostí daleko jednodušší, než tomu bylo ještě před 10 lety. Vybudování datové sítě je v zásadě rutinní záležitostí a připojení další kamery není obtížnější než připojení jakéhokoliv jiného síťového prvku.

Cílem systému není dosažení maximálního rozlišení, ale maximální úroveň ochrany nebo optimálního poměru mezi bezpečností a souvisejícími náklady.

S přechodem k datovým sítím souvisí i optimální rozlišení. V dnešní nabídce můžete běžně najít kamery s rozlišením 5 Mpix, což je o třetinu více než populární Full HD. Jenže data z kamer jsou přenášena po sítích, jejichž kapacita není neomezená. I když jsou k dispozici stále účinnější metody komprese obrazu (snížení datového objemu bez ztráty informace), je často zapotřebí volit mezi rozlišením přenášeného obrazu, rychlostí přenosu a dodatečnými investicemi do kapacity sítí. Filip Šelemberk v této souvislosti upozorňuje na jedno velmi důležité slovo – optimalizace. Cílem systému není dosažení maximálního rozlišení, ale maximální úroveň ochrany nebo optimálního poměru mezi bezpečností a souvisejícími pořizovacími a provozními náklady.

Fyzická a počítačová bezpečnost

S přechodem na počítačové sítě je také zapotřebí řešit veškeré záležitosti spojené s tím, čemu se tradičně říká informační bezpečnost – od záložních zdrojů napájení přes zálohování dat a obrazu až po zdvojená síťová připojení, záložní servery, zabezpečená

datová centra, šifrování, přístupové certifikáty... To vše v závislosti na rozpočtu a významu systému.

Výrobci kamerových systémů tím jasně směřují k jediné základní myšlence – omezit úlohu člověka jen na reakci na potenciální nebezpečí.

Spojení kamer a informačních technologií také usnadňuje další, dnes již v podstatě standardní součást řešení kamerových systémů – videoanalýzy. Bezpečnost už nemusí záviset na tom, zda si pracovníci ostražiny všimnou podezřelého dění. Systém vyhodnocuje situace automaticky. V areálech, kde jsou umístěny stovky a tisíce kamer, by to ostatně ani nebylo možné jinak. Díky inteligentní analýze obrazu najdete ve velínu takového areálu třeba čtyři monitory, kam se promítají ty záběry, které souvisí s narušením pravidel. „Výrobci systémů tím jasně směřují k jediné základní myšlence – omezit úlohu člověka jen na reakci na potenciální nebezpečí,“ píše Filip Šelemberk.

Dalším trendem je propojování kamerových systémů s dalšími bezpečnostními technologiemi, jako jsou požární a zabezpečovací ústředny, systémy kontroly vstupu nebo perimetru, což je opět usnadněno tím, že všechna zařízení jsou propojena stejnou datovou sítí.

A jak tedy bude vypadat nejbližší budoucnost? – Analogové kamery budou používány jen pro specializované aplikace (např. termokamery) nebo v systémech, které tak byly historicky koncipovány. Kamerové systémy budou stále častěji doplňovány o videodetekci a logika a vyhodnocování situací bude řešena na úrovni aplikace. Role lidské obsluhy se omezí jen na řešení krizových situací. Přibudou videoanalýzy, které nespádají do oblasti bezpečnosti, a kamerové systémy budou využívány i pro čistě komerční aplikace. Tlaky na cenu a technické pokroky rozšíří kamerové systémy i do soukromého sektoru a je možné, že některý ze silných telekomunikačních hráčů na trhu nabídne IP CCTV jako doplněk k datovým službám.



ROZPOZNÁVÁNÍ FANOUŠKŮ V KRAKOVĚ

Díky chytrému bezpečnostnímu řešení a bezchybně provedenému projektu má dnes Cracovia Krakow jeden z nejlépe zabezpečených stadionů v Evropě

Pokud budete v Krakově a rozhodnete se zajít na zápas nejstaršího polského fotbalového klubu, prostě přijdete ke vchodu na stadion, vložíte vstupenku do turniketu, projdete otáčivou kovovou konstrukcí a nejspíš si ani nevšimnete, že probíhá automatická kontrola, zda jste skutečně tou osobou, která si koupila lístek. Nevšimnete si, pokud je všechno v pořádku. V opačném případě vás turniket nepustí dovnitř a jsou přivoláni pořadatelé, kteří vám zkontrolují osobní doklady a ujistí se, že nejste výtržník se zákazem vstupu.

Zkrátka, téměř žádné obtěžování běžných fanoušků a zároveň vysoká bezpečnost. Uspořádání je méně náročné i pro pořadatele. Nehrozí jim bitky s výtržníky, protože vyhlášení chuligáni se na stadion prostě nedostanou. Případné pokusy skončí hned u brány a budou se řešit s každým narušitelem jednotlivě. Sřetenutí s agresivním davem nehrozí. To všechno zajišťuje systém, který vyrobila společnost INTEGEO.

Pořadatelům nehrozí bitky s výtržníky, protože vyhlášení chuligáni se na stadion prostě nedostanou. Případné pokusy skončí hned u brány a budou se řešit s každým narušitelem jednotlivě.

Jakmile návštěvník vloží lístek do turniketu, systém vyhledá v databázi jeho fotografii, která byla pořízena při vystavení klubové karty nebo při koupi vstupenky. V příštím okamžiku probíhá analýza záběru z kamery s vysokým rozlišením, která návštěvníka snímá. Pokud podoba souhlasí, je

vše v pořádku. Pokud systém odhalí rozdíl, je vstup zablokovan a zároveň jsou upozorněni pořadatelé.

Kamery, integrace a řízení složitého projektu

Systém je v provozu od začátku podzimní fotbalové sezóny a první měsíce potvrdily, že splňuje vše, co se od něj očekávalo. Výtržníci se zákazem vstupu se na stadion nedostávají, falešných poplachů je minimum, a navíc i roste zájem o klubové karty (pokud nemáte klubovou kartu, musíte se při koupi vstupenky legitimovat). Za zmínku určitě ale stojí i to, že kompletní řešení včetně infrastruktury bylo vybudováno za pouhé tři měsíce, a to ve velmi obtížných podmínkách. Stadion procházel rekonstrukcí, vrcholily stavební práce, docházelo ke změnám harmonogramu, bylo třeba koordinovat práci několika firem a řešit i takové záležitosti, které s bezpečností obvykle příliš nesouvisí. Třeba takový „technický detail“, jakým je fotografování lidí, kteří si přicházejí koupit vstupenku. Vstupenky se prodávají v prosklených kioscích, kde není dost místa, světelné podmínky jsou všelijaké a od prodavačů nelze očekávat schopnosti profesionálních fotografů. INTEGEO do kiosků instalovalo fotopracoviště obsahující nejen fotoaparát a napojení na informační systém, ale i sadu „deštníků“ zajišťujících správné osvětlení a dostatečně ostrý snímek za každé situace.

Ale to hlavní pochopitelně spočívalo v instalaci softwarového systému pro rozpoznávání tváří a potřebných zařízení – kamer s vysokým rozlišením, vybudováním datových sítí, dodávce serverů apod. A ve spoustě integrační práce, která z těchto technologií vytvořila řešení na



míru krakovskému stadionu a propojila je s dalšími nasazenými zařízeními, jako jsou turnikety rakouské firmy Skidata.

...spoustě integrační práce, která z těchto technologií vytvořila řešení na míru krakovskému stadionu a propojila je s dalšími nasazenými zařízeními, jako jsou turnikety rakouské firmy Skidata.

Pro lidi z firmy INTEGEO to znamenalo spoustu nervů a pro některé z nich také nutnost přestěhovat se na pár týdnů do Polska. Ale dopadlo to jako vždycky – systém byl hotový včas, tedy do zahájení dalšího ročníku polské nejvyšší fotbalové soutěže.

Ale nemusí jít jen o zápasy polské extraligy. Stadion v Krakově je také jedním z uvažovaných dějišť mistrovství Evropy 2012. Takže kdo ví, třeba si na něm zahraje i česká reprezentace.

Systém Face Recognition umožňuje porovnávat tváře snímání „živě“ z kamery s tvářemi uloženými v databázi tzv. referenčních snímků. Na základě výsledků tohoto porovnání je umožněn nebo zamezen vstup do chráněného objektu, a to tím, že systém ovládá vstupní zařízení (dveřní zámky, turnikety apod.). Systém je možné rozšířit o řadu dalších volitelných funkcí, jako automatické zaznamenávání všech průchodů nebo pokusů o průchod, možnost strážného vpustit i osobu, která při kontrole nevyhověla, nebo třeba vyhledávání obličejů v databázi.

Řešení nasazené v Krakově pracuje s kamerami Mobotix M12 a softwarovým nástrojem Verilook.

SPRÁVA PODNIKOVÉ BEZPEČNOSTI – BĚŽNÁ REALITA ZAČÍNÁ PŘEKONÁVAT VĚDECKOFANTASTICKÉ PŘEDSTAVY

Přehledový článek Josefa Sikyty pro čtvrtletník Biz

Inteligentní kamerové systémy, které automaticky vyhodnocují situace a vyvolávají poplachy. Automatizace řady činností ostrahy. Řízení všech zabezpečovacích technologií centrálním informačním systémem. Pečlivé řízení přístupu k obrazu z kamer a dalším citlivým informacím. Tak by se daly shrnout hlavní rysy současných bezpečnostních řešení.

Možná si tu scénu z bondovky Zítřek nikdy neumíte vybavit. Zločinný magnát v podání Jonathana Pryceho se během porady se svými kumpány v podstatě náhodou podívá na obrazovku, na kterou se promítá záznam z bezpečnostní kamery. Má štěstí. Zrovna v tu chvíli před kamerou probíhá čínská agentka. „*Za co vás platím!*“ rozkřikne se zlosyn. „*Když je tu ona, je tu i Bond!*“



Ani agent 007 by neproklouzl Vzhledem ke skutečnému vývoji technologií působí taková scéna stejně směšně jako monochromatické monitory na kosmické lodi budoucnosti v prvním díle Vetřelce. Kdyby byl magnátův neviditelný

bojový koráb vybaven aspoň na takové úrovni, jako dnešní pokročilejší banky, univerzity či průmyslové celky (nemluvíme o vojenských základnách nebo jaderných elektrárnách), vypadal by poplach úplně jinak. Kamera by zachytila pohyb, informační systém podle velikosti objektu vyhodnotil, že se může jednat o člověka (nechceme přece, aby poplach spouštěl každý racek) a další systém provedl porovnání s údajem ze vstupní kontroly, takže by okamžitě věděl, že nikdo z posádky se momentálně nenachází ve střežené oblasti. Během několika sekund by se automaticky spustil poplach a koordinátorům na velínu by byl na obrazovku předáván vždy obraz z té kamery, v jejímž dosahu se agent 007 nachází.

Po zjištění potenciálního narušitele systém namíří na podezřelé místo dvojicí kamer (běžnou optickou i infračervenou) a pohyb narušitele je automaticky sledován. Dvojicí agentů na gumovém plavidle by čekalo nepřijemné přivítání.

Kdyby byl zlosyn technicky pokročilejší, tak by se k jeho plavidlu Bond se svou kolegyní vůbec nedokázali přiblížit. Tak například širokopásmové radary, které v současné době nasazujeme pro jednoho zahraničního zákazníka, dokáží zachytit i plavce na vodní hladině. Po zjištění potenciálního narušitele systém namíří na podezřelé místo dvojicí kamer (běžnou optickou i infračervenou) a pohyb narušitele je automaticky sledován. Dvojicí agentů na gumovém plavidle by čekalo nepřijemné přivítání.

Střežení prostor i plynulosti provozu

Takový je převládající trend posledních let, který byl naposledy potvrzen před pár týdny na veletrhu bezpečnostních technologií v Essenu, kam se sjela světová špička oboru. Je-li možné vyzdvihnout jen jednu záležitost, kolem níž se podniková bezpečnost stále častěji točí, pak jsou to právě tzv. „analýzy a detekce v obraze“. Už se nepředpokládá, že ochranka dokáže sledovat desítky nebo stovky kamer a že si všimne případného narušení. Místo toho je nasazen chytrý systém, který v obraze z kamer dokáže rozpoznat člověka, osobní automobil, dodávku, balík, zvíře nebo cokoliv jiného, na co je nastaven. Důvodem nemusí být jen ochrana proti vloupání či přepadení ale i řešení běžných provozních stavů. Systém může stejně dobře vyhodnocovat, že u stroje dochází zásoba materiálu nebo že hromada výrobků je už tak vysoká, že je třeba část rychle odvézt. Třeba v tunelech nově otevřeného Pražského dálničního okruhu, kde je takový inteligentní systém instalován, řeší systém nejen bezpečnost, ale také plynulost provozu.

Systém může stejně dobře vyhodnocovat, že u stroje dochází zásoba materiálu nebo že hromada výrobků je už tak vysoká, že je třeba část rychle odvézt.

Bezpečnostní systémy dokáží nejen rozpoznávat objekty v obraze, ale také vyhodnocovat změny. Zmizela bedna, která tu ještě před minutou byla a která podle údajů z logistického systému neměla být dnes odvážena? V takovém případě stačí několik sekund

k upozornění bezpečnostního personálu u brány. Vyhodnocují se i situace jako příliš dlouhá fronta, pád člověka, odhození zavazadla apod. – to všechno může být důvodem, proč vyburcovat ochranku. Není divu, že se mění i role firem, které taková řešení nasazují – tam, kde ještě před třemi čtyřmi lety stačilo namontovat kamery, tam dnes přicházejí konzultanti, kteří se zákazníkům debatují o nejrůznějších událostech, jaké mohou nastat a jak je řešit. A stejně jako ekonomické systémy vycházejí z optimální podoby určitých procesů (nejlepší praktiky), bezpečnostní systémy pracují s podobnými nejlepšími praktikami – na jaké události se připravovat a jak na ně případně reagovat.

Střežení bez narušení soukromí

I pro lidi působící v oboru je někdy až udivující, jak rychle se rozšiřují možnosti běžně dostupných komerčních produktů. Jestliže ještě před pár lety spouštěly systémy falešný poplach pokaždé, když před kamerou proběhlo zvíře, dnes dokáží rozlišit kočku od narušitele zcela spolehlivě. Dokonce i od takového narušitele, který se krčí nebo pokouší plížit. K tomu přibývají funkce jako čtení poznávacích značek na automobilech nebo rozlišování obličejů. Záběry z bezpečnostních kamer jsou tak porovnatelné s databází příliš agresivních fotbalových fanoušků či třeba nežádoucích návštěvníků... A na louisianské univerzitě, v jejímž areálu bydlí 5000 studentů, systém kontroluje, zda jste osoba, která do konkrétní budovy patří. Takové technologie, které byly ještě donedávna exkluzivní těžko dostupnou záležitostí, se nasazují stále častěji.



Centrální řízení umožňuje pečlivě nastavit přístupy, včetně toho, že obraz z některých kamer bude zpřístupněn pouze tehdy, pokud systém vyhodnotí situaci jako narušení bezpečnosti.

Rozpoznávání v obraze spolu s centralizací dohledu nemusí vést ke ztrátě soukromí, ale naopak soukromí chrání. K tradičním bezpečnostním řešením patřilo i to, že k záběrům z kamer měli v podstatě nekontrolovaný přístup všichni pracovníci ochranky, vrátní a mnozí další. Centrální řízení umožňuje pečlivě nastavit přístupy, včetně toho, že obraz z některých kamer bude

zpřístupněn pouze tehdy, pokud systém vyhodnotí situaci jako narušení bezpečnosti, nebo zpětně při vyšetřování určité události.

Práce pro podnikovou informatiku

Je-li prvním dlouhodobým trendem automatická identifikace objektů a situací, je druhým takovým trendem integrace technologií. Pokud čidlo zachytí zvuk o frekvenci odpovídající tříštění skla, systém nejen, že upozorní ochranku, ale také jí poskytne obraz z nejbližší kamery nebo informaci, že právě došlo k poškození této kamery. Obranná akce může začít. Podobně jsou propojovány body ze vstupních kontrol, požárních hlásičů či dalších systémů a detektorů.

Třetím trendem je spojování bezpečnostních technologií a informačních systémů, které jsme již zmínili. Kamerový systém se čtením poznávacích značek vozidel může být propojen se systémem pro správu vozového parku. Systém, který kontroluje sklady, může být propojen s objednávkovým systémem. Možností je neřeberně. Sbližování má i technologický základ – řada bezpečnostních zařízení komunikuje na protokolu IP (Internet Protokol – běžná norma pro propojení počítačů a digitálních telefonů), využívá běžné datové sítě, vyhodnocovací systémy běží na unixových nebo windowsovských serverech a v běžných osobních počítačích. Různá bezpečnostní zařízení se tak postupně stávají jednou z položek, které má na starosti správce podnikové informatiky.

Konec nočních vrátných?

Na závěr to nejdůležitější. Technologické změny také radikálně mění způsob podnikového bezpečnostního personálu. Obraz důchodce, který civí do obrazovek a každých 30 minut obejde areál, postupně mizí a za pár let

se s ním nesetkáme již vůbec. Ochranka současnosti a budoucnosti, to jsou především vycvičení chlapi, kteří čekají na poplach a poté vyrážejí do akce. A protože vyráží jen tam, kde je jich opravdu zapotřebí, mohou obsáhnout větší areály nebo více objektů. Takže výsledkem změny není jen snížení personálních nákladů, ale zároveň také posílení bezpečnosti!!! A o to jde především.

Technologické změny také radikálně mění způsob práce podnikového bezpečnostního personálu. Obraz důchodce, který civí do obrazovek a každých 30 minut obejde areál, postupně mizí a za pár let se s ním nesetkáme již vůbec.

Přetištěno z listopadového čísla magazínu Biz (www.casopis.biz)



Dobrou cestu rokem 2011
Josef Sikyta a tým INTEGOO