SECURITY magazín

ročník XX | květen / červen 2014 www.securitymagazin.cz | 89 Kč

Ochrana datových center

- BEZPEČNOST NA STADIONECH
- MECHANICKÉ ZÁBRANNÉ SYSTÉMY
- KAMEROVÉ SYSTÉMY

ISSN 1210-8723
03 >
9 771210 872008

NEWSLETTER ASOCIACE TECHNICKÝCH BEZPEČNOSTNÍCH SLUŽEB GRÉMIUM ALARM

Ztracené děti, o.s. je nevládní nezisková organizace založena v roce 2008 zaměřující se na problematiku jak dlouhodobě, tak právě aktuálně ztracených dětí a mladistvých do 18 let věku. V rámci našich projektů se snažíme předcházet dočasné ztrátě dítěte a to jak se zaměřením na děti, tak na rodiče. Naši pomoc soustředíme i na rodinné příslušníky, kterých se daná problematika týká. V současné době probíhá mimo jiné projekt „S Denisem bezpečně“, jež obsahuje přednášky s tématy vztahujícími se k bezpečnosti dětí a je určen pro školky a školy.

Více informaci naleznete na www.ztracene-deti.cz nebo na FB - Ztracené děti o.s.

sbírkový účet: 2700297/0100

Uplynulé týdny se nesly ve znamení hrozeb v oblasti informačních technologií. Alespoň tak by se mohlo zdát při sledování našich médií. Premiér Sobotka splnil povinnost a otevřel novou budovu Národního kybernetického centra a neopomněl zmínit, že tím plní programový závazek vlády. Při stříhání stuhy si před fotoaparáty čechral mediální peří. Kybernetická bezpečnost je prostě mediálně „cool". Zato otázce zákona o soukromých bezpečnostních službách se před eurovolbami raději všichni vyhýbají jako čert kříži. Respektive před každými volbami, přestože jde o zákon, který je důležitý i pro bezpečnost státu a jeho občanů. Stát sice již dávno zjistil, že nemůže zajistit ochranu všude a všem, nicméně jasně přiznat to veřejnosti nechce – byť jde o normální stav, ve kterém byla již první republika. Občan, protože absolutně netuší, co by měl zákon řešit, si pod ním představuje jediné – privatizaci policie. A jakýkoli politik, který by jen vypadal, že něco takového chystá, může zapomenout na hlasy. Proto návrh zákona jen leží, občas na něm někdo utře prach a pak ho po chvilce zase odloží. Jak ukázala konference KBM 2014, všichni si na tento stav tak nějak zvykli a už se o něm ani nemluví. Přitom sektor zaměstnává přes 1 % zaměstnanců v ČR, zaměstnanců, kteří jsou zároveň voliči …

Tomáš Jirásko

Z OBSAHU ČÍSLA VYBÍRÁME:

SECURITY MAGAZÍN

Odborný dvouměsíčník o zabezpečovací technice, ochraně majetku, osob a informací
Vychází od října 1994
Ročník XX
Vydání číslo 118-3/2014 květen – červen

Vydává © Security Media, s.r.o.
www.securitymagazin.cz
Registrace MK ČR 6826, ISSN 1210-8723
Veslařský ostrov 62, 147 00 Praha 4

Šéfredaktor
Tomáš Jirásko
tomas.jirasko@securitymedia.cz

Redaktoři
Kamil Pittner
kamil.pittner@securitymedia.cz

Václav Maletínský
vaclav.maletinsky@securitymedia.cz

Marketing, inzerce, předplatné
Kateřina Škarková, + 420 725 931 693
katerina.skarkova@securitymedia.cz

Miroslav Krčil, + 420 605 974 304
miroslav.krcil@securitymedia.cz

Produkce, grafické zpracování, tisk:
SMART POINT, s. r. o.
C&COM Advertising, s. r. o.

Rozšiřuje: PNS, a. s.

Předplatné: A.L.L. Production s. r. o.
P.O.Box 732, 111 21 Praha 1
telefon : 840 30 60 90
email : security@predplatne.cz

Předplatné v SR:
L. K. Permanent Slovakia, spol. s. r. o.
Poštový priecinok 4, 834 14 Bratislava 34
+ 421-02-44453711, herslova@lkpermanent.sk

Cena výtisku 89 Kč
Roční předplatné 480 Kč

Podávání novinových zásilek povoleno:
Česká pošta, OZSeČ Ústí nad Labem,
dne 21. 1. 1998 j. zn. P-352/98.

Rodina Bosch Amax roste

Bosch Security Systems doplnil portfolio zabezpečovacích systémů pro domácnosti a malé firmy o dva modely panelů Amax s bezdrátovým příslušenstvím. Nové panely EZS Amax 3000 a Amax 2100 spolu s již dříve uvedeným Amax 4000 pokrývají širokou škálu potřeb jednotlivých uživatelů. Amax 2100 je vhodný pro malé prostory s maximálně osmi zónami, Amax 3000 si poradí až s 32zónovým řešením a AMAX 4000 dokáže pokrýt až 64 zón. Amax 3000 a 4000 mohou být provozovány v hybridním režimu s detektory řady Bosch Blue Line Gen2, či stejně tak s bezdrátovými typu Radion. Zařízení mají certifikaci EN 50131 třídy 2.

www.boschsecurity.com

2 000 000 zabezpečených automobilů

První mechanické zabezpečení Construct bylo vyrobeno v roce 1991 na vůz Škoda Favorit. Byl to relativně jednoduchý, přesto velmi účinný systém, jehož principy jsou v současném provedení produktů Construct dodnes zachovány. Výrobu miliónténo kusu slavila společnost v roce 2007. Na přelomu března a dubna, v roce 20. výročí schválení produktu mechanického zabezpečení Construct jako originálního příslušenství pro vozy značky Škoda, vyrobila společnost již dvoumiliónty kus na Škodu Roomster a Fabii (CF 016).

www.construct.cz

Nové sídlo Národního centra kybernetické bezpečnosti

Premiér Sobotka slavnostně otevřel 13. května nové sídlo NCKB. Společně s ním se otevření zúčastnil také ředitel Národního bezpečnostního úřadu Dušan Navrátil, náměstek generálního tajemníka NATO Sorin Ducaru a ředitel Evropské agentury ENISA Udo Helmbrecht. Současný vládní kabinet se zavázal ve svém programovém prohlášení ke zlepšení bezpečnosti a obranné politiky ve spolupráci s EU a NATO. Otevření brněnské pobočky tak deklaruje plnění těchto vládních závazků. Sídlo Národního centra kybernetické bezpečnosti bylo zřízeno v gesci Národního bezpečnostního úřadu. Vybudováno bylo v bývalých prostorách budovy ministerstva obrany, které objekt převedlo do správy NBÚ v roce 2011. Náklady na rekonstrukci a vybavení sídla byly vyčísleny na 82 milionů korun. Úlohou centra je zejména koordinace spolupráce při předcházení kybernetickým útokům a řešení aktuálních problémů jak na státní, tak na mezinárodní úrovni. Pracoviště má také úlohu zastupovat Českou republiku v Severoatlantické alianci.

www.vlada.cz

Panoramatická kamera Axis M3027-PVE

Kompaktní a cenově zajímavou kameru M3027-PVE představil Axis. Jedná se o fixní kopulovou kameru s 5megapixelovým senzorem, která umožňuje 360° nebo 180° panoramatické záběry. Síťová kamera je odolná vůči vandalům (krytí IK10), má denní i noční režim a je určena pro vnitřní i venkovní instalace zejména v buticích, hotelech, restauracích nebo kancelářích. Kamery v řadě M30 jsou navrženy tak, aby jejich instalace byla co nejjednodušší. Podporují proto napájení přes datovou síť (Power over Ethernet – IEEE 802.3af), čímž se eliminuje potřeba napájecích kabelů a snižují se náklady na instalaci.

www.axis.com/cs

Synology Surveillance Station 6.3

Od května je dostupná beta verze aplikace Surveillance Station 6.3. Novinka díky rozšířené podpoře různých scénářů nasazení zvyšuje efektivitu monitoringu, jeho jednoduchost a spolehlivost. Surveillance Station 6.3 mimo jiné nyní umožňuje uživatelům sledovat v živém zobrazení zároveň až 64 kanálů v rozlišení 720 p v rámci jednoho uživatelského rozhraní a nabízí webový plug-in, který kvůli výkonu nahradil Javu v prohlížečích Internet Explorer, Firefox a Chrome, nyní i pro Safari nebo novou podporu joysticků.

www.synology.com

G4S využívá SuMo pro Salesforce

Britská G4S Security Services UK nasadila v rámci snahy o zefektivnění prodejního kanálu službu SuMo určenou pro prostředí Salesforce. SuMo se zaměřuje na zvýšení výkonu změnou pracovních návyků a chování zaměstnanců. Aplikace využívá herní mechanizmy a sociální techniky (bodování, dosažení odznaků, správcovství témat) a ve výsledku slouží k lepšímu využívání i shromažďování CRM dat. Podle G4S od nasazení SuMo došlo k 60procentnímu nárůstu „aktivního“ prodejního kanálu (obchodní manažeři jsou v kontaktu se zákazníky) a 35procentnímu oživení kontaktů přes salesforce.com apod.

www.cloudapps.com

PCS distributorem Microsemi

Společnost PCS se stala distributorem společnosti Microsemi. Jako první produkt ve svém portfoliu představila na bratislavském veletrhu IDEB 2014 PMMW skener GEN2. Ten využívá k pasivní detekci předmětů milimetrové vlny (PMMW – Pasive Millimetre Wave). Skenery dokáží na základě pasivní detekce milimetrových vln odhalit pod oblečením jak kovové předměty, tak plasty, tekutiny, gely, keramiku, práškové substance, výbušniny, peníze, léky nebo narkotika, elektroniku i datové nosiče.

www.pcs.cz

MEZINÁRODNÍ KONFERENCE BEZPEČNOSTNÍHO MANAGEMENTU 2014 – KBM 2014

Ve čtvrtek 24. dubna 2014 se uskutečnil již 10. ročník mezinárodní Konference bezpečnostního managementu 2014 s podtitulem „Lidský faktor v bezpečnostním systému“.

V našem ohlédnutí si vezmeme na pomoc oficiální zprávu z průběhu konference, přidáme několik postřehů a bernou mincí nám budiž hlas lidu – jakýsi sumář z komentářů zúčastněných, které, přiznáváme, nebyly v řadě případů určeny našim uším.

Připomeňme si, na co se konference zaměřila: „Cílem bylo nabídnout posluchačům program, který se bude věnovat detailům a umožní zaměřit se na bezpečnost v jakémkoliv odvětví, protože se jedná o obdobné problémy. Důraz byl kladen na bezpečnostní manažery a jejich osobní přístup, nasazení, excelenci, která spočívá v detailním řešení každodenních problémů,“ přiblížil záměry konference Zdeněk Kalvach, předseda společnosti ASIS International ČR, která byla pořadatelem akce.

V konferenčních prostorách Dorint Don Giovanni se sešlo přes 200 účastníků specializovaných na výrobní a obchodní závody, bankovnictví, dodavatelé služeb, zástupci leteckého průmyslu, bezpečnostních služeb a technologií apod.

Optimizmem, že nepůjde o promarněný čas, nás naplnilo již slavnostní zahájení. Bylo věnováno nenahraditelnosti lidského potenciálu; v jeho průběhu Libor Kutěj, ředitel odboru zahraničních pracovišť Ministerstva obrany ČR, krátce okomentoval situaci na Ukrajině a zmínil důležitá fakta o Ruské federaci, která si veřejnost neuvědomuje.

Na hlavní panel „Efektivní management bezpečnostního týmu“, který se zaměřil na propojení světa couchingu a bezpečnostních manažerů v oblasti řízení týmů, jsme již byli usazeni v sále mezi účastníky. Ti z části projevovali určitou nervozitu, která typicky panuje před každým panelem věnovaným řízení lidí, ať jste na jakékoliv konferenci. Pokud totiž máte štěstí, mezi panelisty se najde alespoň jeden, který ví, o čem mluví, skutečně chce něco sdělit a nepřišel si jen pozvednout ego. Který ví, že pokud zaujme, bude mít o práci postaráno. Bohužel většinou máte spíš chuť utéct, v nejhorších případech litujete, že u sebe nemáte granát, jehož výbuch by uvítalo i okolí, protože jde o milosrdnou cestu jak uniknout z dosahu žvanila. Z panelů o řízení lidí se totiž neodchází. Ono by se pak mohlo zdát, že se o problematiku správného řízení nezajímáte. Z tohoto pohledu byl panel uspokojující, mluvčí neměli potřebu si brát slovo na úkor druhých, pouze jeho rozjezd byl poněkud rozvláčný a potřebnou dynamiku do něj až v půlce vnesl psycholog Petr Brichcín, s jehož pohledem na efektivní management bezpečnostního týmu jako kombinaci dobrého řemesla a umění se dokázali posluchači ztotožnit. Lektorka a profesionální couch Tereza Marie Dočkalová rovněž předvedla fyzickou ukázku rychlého vyhodnocení situace či okamžitých potřeb manažera s pomocí flipchartu, takže závěrečné demonstraci vlivu nejednoznačných pokynů a různého výkladu pokynů s využitím překládání a trhání rohu papíru se věnoval celý sál. K ještě vyšší spokojenosti zúčastněných by přispělo větší množství příkladů z praxe.

Stačí si připomenout, jak dlouho trvalo, než lidé pracující v oblasti bezpečnosti začali brát vážně psychology. A oblast couchingu je na tom z tohoto pohledu výrazně hůře. Aby si vydobyl své místo, couching využil „mediální hype“, na který se nabalila řada „prodavačů hadího oleje“. A tak rozhodně nestačí říkat, my jsme ti dobří. Reklamštinou řečeno – chce to důkaz místo slibů.

Po přestávce pokračovala hlavní část panelem „Faktor stresu v bezpečnosti – psychologie útočníka a obránce“. Ten přinesl pohled na několik technik práce se stresem. Rozhodně neuškodilo připomenutí Radovana Spáčila (Tactical Gear and Solutions – TGAS), že strach zabíjí myšlení a jak se mu postavit. Suchou (i když mírně otřepanou) poznámku pronesl Tibor Brečka, psychoterapeut a generální sekretář KPA: „To, že jste paranoidní, ještě neznamená, že po vás nejdou.“ A je nutné se s tím naučit žít. I když podobně zaměřené panely často vypadají jako nošení dříví do lesa, jejich přínos, zejména z hlediska upozornění na opomíjenou problematiku, je nezanedbatelný. Což ukazují meziroční srovnání. Řada manažerů problematiku rozvoje osobních technik zaměřených na psychologickou odolnost podřízených totiž neřeší, respektive těžko hledá cestu a metody, jak bez externích zdrojů v této oblasti efektivně se svými lidmi pracovat. I na to částečně panel dokázal přinést odpověď.

V doprovodném panelu „Facility Management vs. Security“ se u moderátora Jaromíra Průši (Manager Facility Services Ahold Czech Republic) sešli za security manažery Marek Pour (Coca-Cola HBC Česká republika), Martin Bílek (ČEPS) a Petr Janovský (Divize průmyslu holdingu M2C) společně s Facility Managerem Romanem Baloghem (KD Pragma, člen představenstva

asociace IFMA CZ). Panel se tradičně věnoval v praxi z různých až pitoreskních důvodů často neřešené koexistenci těchto dvou oblastí managementu. Což podle zaplněnosti sálu i poznámek v sále naznačilo nejenom spokojenost s tímto tématem a příspěvky. I když se všichni jednoznačně shodli na nutnosti spolupráce těchto sektorů, půjde jistě i za rok o živé téma.

Zajímavě se vzhledem ke složení a tématu „Inteligentní funkce kamer, mobilní aplikace určené pro iPhone a Android“ jevil panel „Lidský faktor vs. Technologie“. Ivo Rosol představil za firmu OKsystem jejich software Babel, který slouží k šifrování textových zpráv v telefonu. Jde o zajímavou aplikaci, která nabízí solidní úroveň zabezpečení zpráv při jejich cestě vzduchem. Příště by to ale chtělo víc drzosti a odvahy ukrást trochu prostoru ostatním řečníkům. I když byl panel obecný, rozhodně bych od Romana Roxera, technického ředitele TSS Group, a Martina Grena, spoluzakladatele Axis Communication, čekal detailnější příklady, kromě toho, že se shodnou na tom, že kamery odlidšťují, existují kamery s rozlišením 1 Mpx–29 Mpx a je nutný specializovaný software pro efektivní práci. Přitom stačilo ukázat rozvinutí obrazu z 360° kamery do jedné roviny a bylo by o zábavu postaráno. Zvláště v případě Grena bychom čekali více, když panel zabrousil i do oblasti nahrazování analogových technologií IP kamerami a když existuje taková pěkná studie z Anglie, věnující se sektoru maloobchodních prodejců a jejich přístupu k CCTV. Stali jsme se tak ve výsledku diváky přátelského popovídání nad známými fakty. Pokud jste panel vynechali, o nic jste nepřišli.

Panel „Projekty ASIS“ představil „Fair Rate in Security“ a „MBAce in Security Management“ – kampaň směřující ke kultivaci bezpečnostního trhu a zlepšení podmínek zaměstnanců SBS. Kampaň „Fair Rate“ se týká citlivé oblasti, kterou jsou ceny za služby v oblasti SBS. Již na první pohled není reálné, aby za požadovanou cenu byla dodána služba v odpovídající kvalitě a standardu. To se týká i určité „minimální“ fakturované částky za hodinu práce, zlepšení platových podmínek, a tím i kvality služeb. Tedy nic, s čím by se nedalo souhlasit, ale v prostředí, kdy zadavatel tlačí na maximální úspory

a například v tendrech bývá často jediným rozhodujícím faktorem cena, se tato aktivita bude jen pomalu prosazovat.
V MBAce se Miloš Drdla ze Vzdělávacího institutu pro bezpečnostní studie věnoval problematice následného vzdělávání.

Náplň práce vyjednavačů a řešení krizových situací při cvičení na Rádiu Svobodná Evropa / Rádiu Svoboda simulujícím útok teroristů přiblížili očima přednášejících Paula H. Haertela, Supervisory Special Agent U. S. Embassy, FBI/DoJ, a Miroslav Vymyslický, národní koordinátor krizového vyjednávání Policie ČR.

Pro bezpečnostního manažera byl zajímavý i panel „Podvodné jednání a korupce v komerční sféře". Sice jde o oblast, se kterou primárně nepřichází do styku, ale panelisté upozornili na nedávno zavedený zákon o trestní odpovědnosti právnických osob, který už bezpečnostního manažera zajímat musí. Panelisté se shodli, že i přes nárůst odhalených případů podvodného a korupčního jednání zaměstnanců společností působících v rámci celé ČR není znatelný nárůst zdrojů určených pro prevenci a odhalování takového neetického, či přímo nezákonného jednání.

Kateřina Olahová (PwC Česká republika) nás provedla evolucí hospodářské kriminality a představila profil typického interního pachatele. Tomáš Kafka (Ernst & Young) ukázal několik nejběžnějších případů, ke kterým ve firmách dochází. Čímž se mu nepřímo podařilo kriminalizovat většinu zúčastněných, aniž by si to ovšem uvědomil. Jde o podvod označovaný jako cut-off, jehož provedení spočívá v tradičním „ulejvání budgetů" na konci roku/fiskálu. Manažer ví, že pokud peníze nevyfakturuje nyní, tak mu příští rok o tuto částku bude rozpočet pravděpodobně snížen. I když jde pouze u snahu ochránit si zdroje, tímto jednáním dochází ke zkreslení hospodaření (platbě za neexistující službu/zboží, následné plnění třetí stranou apod.). Je otázkou, zda hovořit o významné škodě pro firmu, když ve výsledku jsou prostředky vynaloženy tak jako tak. Nicméně je samozřejmě i s přihlédnutím k účetním standardům neoddiskutovatelnou pravdou, že ke zkreslení dochází a touto metodou lze napáchat i záměrné škody. V každém případě pan Kafka, jako ředitel oddělení investigativních služeb a řešení sporů, jistě zná někoho z auditorských služeb a řádně jim tedy vysvětlí, že by z pěkné řádky auditů mělo zmizet razítko EY. Zvláště u firem pracujících v prostředí IFRS i GAAP jde spíše o standardní nástroj, než něco, co považuje jejich in-house interní audit za podvod. Typickou částí firmy, která bez přelévání prostředků v podstatě nemůže fungovat, je marketing. Pěkně nám to však demonstrovalo stav, kdy bezpečnostní manažer nemá zájem se této oblasti přiblížit, protože má svých starostí dost.

Leopold Černý (Screening Solutions) nasypal trochu soli do ran některých přítomných, když svým příspěvkem zabrousil do oblasti business continuity, respektive do časté neexistence plánů pro krizové situace a zajištění nejrychlejší obnovy činnosti společností. Firma může být tvrdě postižena i policejní prohlídkou iniciovanou na základě lživých tvrzení v rámci konkurenčního boje. Obnova chodu společnosti, ve které provedla policie zajištění důkazů (často jde o servery, účetnictví apod.), může v případě neexistence plánu a potřebných záloh vést k jejímu konci. Zde jsme narazili i na otázku, co vlastně firma od svého CSO očekává, kam až má sahat loajalita společnosti, včetně součinnosti s policií (minimální součinnost nebo aktivní přístup), a na problematiku jurisdikce v případech cloudových služeb, mobility dat, BYOD politik apod.

Celkový dojem? I přes několik drobností si KBM drží svoji nepopiratelnou kvalitu a patří ke špičkovým oborovým konferencím jak složením přednášejících, tak odborné veřejnosti. Stačilo se při závěrečném vyhlášení cen podívat kolem sebe. Stále jsme byli ve slušně zaplněném sále a toho nelze dostáhnout bez nadstandardní a vyvážené úrovně jednotlivých panelů. Za rok tedy opět rádi spojíme svoje logo s KBM, jejímž mediálním partnerem jsme již tradičně byli. ■

SOUTĚŽE KBM 2014

V rámci odpolední After Party KBM 2014 byly vyhlášeny následující soutěže: Bezpečnostní projekt roku 2013, Bezpečnostní manažer roku 2013, Bezpečnostní bakalářská práce roku – a dvě novinky: Speciální ocenění za diplomovou práci a soutěž Security Magazínu – Dlouhodobý přínos na bezpečnostním trhu. Cílem ocenění osobností přispívajících k řízení bezpečnostního průmyslu, které se zasloužily o jeho kultivaci v ČR, byla stimulace rozvoje bezpečnostního managementu v českých podmínkách.

VÝHERCI SOUTĚŽÍ PRO TYTO ROČNÍKY JSOU:

VII. ROČNÍK BEZPEČNOSTNÍ MANAŽER ROKU 2013

Zdeněk Kalvach, předseda ASIS International ČR – za celorepublikový systém podpory, výcviku, školení a inovativních řešení v rámci světových bezpečnostních hrozeb – terorizmu, extremizmu, antisemitizmu, včetně přípravy a realizace jedinečného protiteroristického cvičení na rádiu Svobodná Evropa společně s IZS, útvarem rychlého nasazení Policie ČR (URNA) a zaměstnanců RFE.

V. ROČNÍK BEZPEČNOSTNÍ PROJEKT ROKU 2013

Portál Scaut společnosti Screening Solutions – Portál SCAUT je moderním nástrojem řízení rizik spojených s lidským kapitálem. SCAUT maximálně zjednodušuje administrativu spojenou s ověřením rizik plynoucích z finanční situace, podnikatelských aktivit a potenciálních skrytých konfliktů zájmů.
www.scaut.cz

II. ROČNÍK BEZPEČNOSTNÍ DIPLOMOVÁ PRÁCE

Magddaléna Šormová, Policejní akademie České republiky v Praze – za práci Kriminalita spojená s užíváním drog (rok vydání 2013).

SPECIÁLNÍ OCENĚNÍ ZA DIPLOMOVOU PRÁCI

Petra Žalmánková, Univerzita Tomáše Bati ve Zlíně – Fakulta aplikované informatiky – za práci Hodnocení intenzity útoku (rok 2012).

SOUTĚŽ SECURITY MAGAZÍNU – „DLOUHODOBÝ PŘÍNOS NA BEZPEČNOSTNÍM TRHU"

Tereza Daňková, vedoucí pracoviště autorizací na odboru bezpečnostního výzkumu a policejního vzdělávání MV ČR – za celorepublikový systém podpory, výcviku, školení a kontroly školitelů v rámci zkoušky odborné způsobilosti pro výkon pracovní činnosti strážný, který podporuje profesionální výkon služby jednotlivých strážných bezpečnostních agentur a rozvoj podnikání v komerční bezpečnosti. Dále za zastoupení „bezpečnosti" v tzv. Sektorové radě pro bezpečnost a ochranu osob a majetku a bezpečnost práce. Základním posláním sektoru bezpečnosti a ochrany osob a majetku je zejména ochrana zájmů a zajištění potřeb podnikatelů působících v této sféře v souladu s obecně závaznými právními normami České republiky a ve světě bezpečnostních služeb uznávanými standardy, zejména pak standardy Evropské unie. ■

Ilustrační foto redakce

MECHANICKÉ ZÁBRANNÉ SYSTÉMY

Petr Koktan

Pod pojem mechanické zábranné systémy (dále jen MZS) zahrnujeme výrobky, které mají chránit majetek, ceniny a další hodnoty před zcizením krádeží či vloupáním. Jejich úkolem není stoprocentní ochrana, ale vytvoření určitého časového prostoru pro další opatření, např. zásah bezpečnostní služby apod.

Z hlediska způsobu ochrany můžeme MZS rozdělit do tří skupin. První, které je třeba při napadení objektu překonat, jsou na perimetru – ploty, vjezdové závory, vstupní nebo vjezdová vrata atd. Druhou skupinu tvoří vstupy do vlastní budovy – otvorové výplně (okna, dveře, mříže atd.) a jejich komponenty. Třetí skupinou jsou úschovné objekty – trezory a ohnivzdorné skříně, které pak řeší přímou ochranu uložených hodnot, peněz a cenností.

Základní vlastnost, kterou od shora uvedených výrobků s ohledem na jejich aplikaci a účel použití v praxi požadujeme, je bezpečnost – SECURITY, kterou lze kvantitativně i kvalitativně vyjádřit jejich průlomovou odolností. Kvantitu lze spatřovat v délce časové prodlevy potřebné k jejich překonání, odstranění, otevření atd. Kvalitu pak ve způsobu překonání – agresivitě nářadí, kterého je nutno k tomuto cíli použít.

Tuto bezpečnost nelze zaměňovat s jiným typem bezpečnosti, tzv. SAFETY. Tato bezpečnost je dána legislativou, ať již českou (zákon č. 22/1997, Sb., o technických požadavcích na výrobky) či evropskou (CPR – nařízení pro uvádění stavebních výrobků na trh). Tato bezpečnost výrobku je definována základním požadavkem na jejich aplikaci, tedy tím,

Ilustrační foto redakce

že při užívání nemůže dojít k ohrožení zdraví, života, majetku či životního prostředí uživatele. Ohrožením majetku však není myšleno jeho zcizení, nýbrž např. jeho poškození v důsledku zřícení stavby či její části.

Na základě shora uvedeného lze MZS (platí to však obecně pro všechny výrobky uváděné v ČR na trh) rozdělit do dvou skupin. První početně menší skupinu výrobků tvoří tzv. stanovené výrobky, nazývané též „regulovaná sféra". Tyto MZS musí splňovat v České republice i v EU určité vlastnosti, než mohou být uvedeny na trh – do prodeje. Musí být tzv. SAFETY. Jedná se například o životnost (při určitém počtu otevření dveřního křídla nesmí dojít k destrukci jeho závěsů – ČSN EN 1935) či pevnost (čelní či boční tlak na střelku zadlabacího zámku ČSN EN – 12209) nebo životnost střelkového mechanizmu. Pokud tyto výrobky splňují uvedené požadavky, považují se za „bezpečné" a mohou být uvedeny na trh s označením CE podle CPR.

Za základní ukazatel, zda MZS patří do regulované sféry, či nikoliv, je existence harmonizované evropské normy hEN. V zásadě lze uvést, že dnes již pro 99 % MZS existují evropské normy, které jsou převzaty do českého normalizačního systému (ČSN EN xxxxx). Pokud tato norma obsahuje přílohu ZA, jedná se o hEN. V této příloze ZA jsou uvedeny parametry – vlastnosti, které musí předmětný výrobek MZS splňovat, než může být uveden na trh. Pro přehled hEN pro MZS, které lze řadit též do oblasti SECURITY, viz tabulku č. 1.

Druhou skupinu tvoří volně prodejné výrobky, u kterých není požadována de facto žádná SAFETY – tedy bezpečnost před jejich uvedením na trh. Tyto výrobky podléhají pouze zákonům o obecné bezpečnosti výrobku, o ochraně spotřebitele a o škodě způsobené vadným výrobkem. U žádných shora uvedených výrobků,

TABULKA 1

OZNAČENÍ VÝROBKOVÉ NORMY	VÝROBEK, KTERÉHO SE NORMA TÝKÁ	CHARAKTERISTIKA
ČSN EN 12209	Stavební zámek zadlabací	Životnost a požární odolnost střelkového mechanizmu
ČSN EN 14846	Elektromechanicky ovládané zámky	Životnost a požární odolnost střelkového mechanizmu
ČSN EN 1935	Jednoosé závěsy	Únosnost a životnost
ČSN EN 179	Nouzové dveřní uzávěry	Paniková funkce
ČSN EN 1125	Panikové dveřní uzávěry	Paniková funkce
pr EN 15685 – v přípravě	Vícebodové zámky	Životnost a požární odolnost střelkového mechanismu

TABULKA 2 – PŘEHLED VÝROBKOVÝCH NOREM

OZNAČENÍ VÝROBKOVÉ NORMY	VÝROBEK, KTERÉHO SE NORMA TÝKÁ	POŽADAVKY – TŘÍDY BEZPEČNOSTI OZNAČOVANÉ TB	CHARAKTERISTIKA
ČSN EN 1303	Profilové cylindrické vložky	Třída 1 až 6	Bezpečnost související s klíčem
ČSN EN 1303	Profilové cylindrické vložky	Třída 0 až 2	Odolnost proti napadení
ČSN EN 1906	Dveřní kování – dveřní štíty	Třída 1 až 4	Odolnost proti destrukci
ČSN EN 12209	Zadlabací zámky	Třída 1 až 7	Pevnost závory a odolnost proti odvrtání
ČSN EN 1935	Závěsy	Třída 1 až 3	Bezpečnost a odolnost proti vloupání
ČSN EN 12320	Visací zámky	Třída 1 až 7	Odolnost proti destrukci a překonání uzamykacího mechanizmu

ať již hodnocených v režimu SAFETY, nebo pouze uvedených na trh, není požadována odolnost proti destrukčnímu narušení – tedy SECURITY. Příkladem takovéto vlastnosti může být např. rozlomení, odvrtání, vytržení či bezklíčové otevření cylindrické vložky – tzv. její průlomová odolnost, která bezesporu podstatně ovlivňuje odolnost dveřního uzávěru proti vloupání.

Požadavky na bezpečnost výrobků SECURITY – jejich průlomovou odolnost, jsou pro MZS obsaženy jako základ v tzv. výrobkových normách – skupina Stavební kování (viz tabulku 1 a 2). Komplexně pak jsou požadavky na SECURITY výrobků – průlomovou odolnost, stanoveny jako systém norem ČSN EN 1627 až 1630, propojující požadavky na všechny komponenty dveří, oken, mříží, rolet a jejich vlastní konstrukci.

V normách ČSN EN 1627 až 1630 narozdíl od norem výrobkových (viz tabulku 1 a 2) jsou definovány zkoušky odolnosti otvorových výplní a jejich komponentů proti manuálním pokusům o jejich překonání – otevření, např. otevření cylindrické vložky pomocí planžety či SG – BK metody, nebo destrukce dveřního kování atd.

Za objektivní důkaz o základní bezpečnosti shora uvedených výrobků (tzn. plnění bezpečnostních požadavků podle uvedených výrobkových norem) se obecně považuje jejich certifikace a za listinný důkaz je považován CERTIFIKÁT SHODY vydaný v akreditovaném režimu. Shodně jako u výrobkových norem probíhá certifikační proces předmětných výrobků ve vztahu k normám ČSN EN 1627 až 1630 – Okna, dveře, uzávěry – Požadavky na bezpečnost – SECURITY. Tato certifikace probíhá komplexně ve vztahu k používaným způsobům krádeží vloupáním. Výrobky jsou certifikovány do bezpečnostních tříd RC 1 až RC 6 podle ČSN EN 1627, přitom běžně jsou používány bezpečnostní třídy RC 1 až RC 4. Bližší charakteristika jednotlivých tříd RC viz tab. 3.

Obecně platí, že čím je bezpečnostní třída RC vyšší, tím je průlomová odolnost výrobku (jeho odolnost proti narušení) větší, výrobek je kvalitnější a poskytuje vyšší ochranu zabezpečení, viz tab. 3 a 4.

U třetí skupiny výrobků – úschovných objektů (trezorů a ohnivzdorných skříní), je systém zkoušení a certifikace založen vždy pouze na jedné normě – výrobkové. Ta obsahuje jak požadavky, tak i metody a postupy zkoušení, včetně vyhodnocování výsledků zkoušek.

Základní norma ČSN EN 1143-1 klasifikuje úschovné objekty na mobilní skříňové

Ilustrační foto redakce

TABULKA 3

BEZPEČNOSTNÍ TŘÍDA RC	PŘEDPOKLÁDANÝ ZPŮSOB NAPADENÍ
RC 1	Příležitostný zloděj zkouší rozbít okno, dveře nebo uzávěr užitím fyzického násilí, např. kopáním, nárážením ramenem, zdviháním, vytrháváním
RC 2	Příležitostný zloděj dále zkouší rozbít okno, dveře nebo uzávěr užitím jednoduchých nástrojů, např. šroubovák, kleště, klín či použití nedestruktivních metod pro otevření zámků – cylindrických vložek – SG – BK, Hobbs – picking atd.
RC 3	Zloděj zkouší zajistit přístup použitím dalšího šroubováku, páčidla atd., včetně nedestruktivních metod
RC 4	Zkušený zloděj dále používá pilu, kladivo, sekeru, sekáč, jednoruční elektrickou vrtačku atd., včetně nedestruktivních metod
RC 5	Zkušený zloděj dále používá elektrické nářadí, např. vrtačku, přímočarou pilu, úhlovou brusku o průměru kotouče maximálně do průměru 125 mm
RC 6	Velmi zkušený zloděj dále používá výkonné elektrické nářadí, např. vrtačku, přímočarou pilu a úhlovou brusku o průměru kotouče maximálně do průměru 230 mm

trezory v bezpečnostní třídě 0 – X a komorové trezory 0 – XIII. Kritériem je jejich průlomová odolnost, počet a kvalita zámků a pevnost ukotvení. Pro informaci uvádíme klasifikační tabulku č. 5 pro skříňové trezory.

Na základě shora uvedených parametrů lze s určitou přesností stanovit pro jednotlivé MZS (ať již úschovné objekty, dveřní a okenní uzávěry, mříže nebo jejich komponenty) dobu potřebnou pro jejich překonání. Tuto znalost lze pak následně využít např. ke stanovení faktoru rizikovosti objektu, plánování zásahu v případě narušení objektu apod.

Prokázání shora uvedených parametrů pak slouží pro vydání certifikátu shody pro oblast SECURITY a případně i pro certifikaci technických prostředků pro utajované skutečnosti Národním bezpečnostním úřadem. ■

Autor je členem prezidia AGA. Pracuje ve společnosti Trezor Test, která poskytuje komplexní služby v oblasti zkoušení, certifikace a expertiz mechanických zábranných systémů.

TABULKA 4

BEZPEČNOSTNÍ TŘÍDA RC	DOBA PRŮLOMOVÉ ODOLNOSTI (MIN.) ČSN EN 1630	STATICKÉ ZATÍŽENÍ ČSN EN 1628 V kN	DYNAMICKÉ ZATÍŽENÍ ČSN EN 1629	TŘÍDA ZASKLENÍ ČSN EN 356
RC 1	neprovádí se	1,5/3	30 kg/800mm	bez požadavků
RC 2	3 minuty	1,5/3/6	30/800	PA4
RC 3	5 minut	3/6	30/1200	PA5
RC 4	10 minut	6/10	neprovádí se	P6B
RC 5	15 minut	10/15	neprovádí se	P7B
RC 6	20 minut	10/15	neprovádí se	P8B

TABULKA 5 – MINIMÁLNÍ POŽADAVKY PRO KLASIFIKACI SKŘÍŇOVÝCH TREZORŮ DO BEZPEČNOSTNÍ TŘÍDY

BEZPEČ-NOSTNÍ TŘÍDA	ZKOUŠKA NAPADENÍM S VYUŽITÍM NÁŘADÍ		PEVNOST KOTVENÍ	ZÁMKY		DOPLŇKOVÉ POŽADAVKY EX	DOPLŇKOVÉ POŽADAVKY CD
	HODNOTA PRŮLOMOVÉ ODOLNOSTIÍ		POŽADOVANÁ SÍLA	POČET	TŘÍDA PODLE EN 1300	HODNOTA PRŮLOMOVÉ ODOLNOSTI PO VÝBUCHU	HODNOTA PRŮLOMOVÉ ODOLNOSTI
	ČÁSTEČNÝ PRŮLOM	ÚPLNÝ PRŮLOM					
	RU	RU	kN			RU	
0	30	30	50	1	A	-	-
I	30	50	50	1	A	-	-
II	50	80	50	1	A	4	-
III	80	120	50	1	B	6	-
IV	120	180	100	2	B	9	1000
V	180	270	100	2	B	14	1000
VI	270	400	100	2	C	20	1000
VII	400	600	100	2	C	30	1000
VIII	550	825	100	2	C	41	1000
IX	700	1050	100	2	C	53	1000
X	900	1350	100	2	C	68	1000
PEVNOST UKOTVENÍ SE PROVÁDÍ PRO ÚSCHOVNÉ OBJEKTY, KTERÉ MAJÍ HMOTNOST MENŠÍ NEŽ 1000 KG.							

NA KOLIK VÁS PŘIJDE ZABEZPEČENÍ

Škody na majetku, které lupiči napáchají, bývají obecně výrazně vyšší než finance, které byste investovali do ochrany vašeho domova.
„Bezpečnostní dveře, které odpovídají třetí bezpečnostní třídě, pořídíte od 20 000 korun. Další účinné a přitom finančně velice dostupné řešení představují fólie na sklo. Vyjdou vás na několik stovek za metr čtvereční a vedle oken jimi můžete zabezpečit třeba světlíky, sklepní průhledy nebo prosklené dveře na terasu. Výhodou fólií je, že lidé nemusí vyměňovat stávající okna za bezpečnostní prosklení, což by bylo poměrně nákladné," říká Ivan Pavlíček z firmy Next, odborník na zabezpečení domů a bytů.
„Úroveň zabezpečení sice přímo neovlivní výši pojistného, má však vliv na rozsah pojistného krytí, což se odrazí ve výši pojistného plnění v případě pojistné události," říká Lucie Ponertová, produktová ředitelka Slavia pojišťovny.
„Nejnižší limity dostávají domácnosti s běžnými uzamykatelnými dveřmi, u certifikovaných dveří s bezpečnostním zámkem je to však až 300 tisíc korun.
U domů či bytů s vysokým stupněm zabezpečení a napojením na alarm či pult centrální ochrany může klient dosáhnout na pojistný limit až do výše 1,2 milionu korun." Obecně tedy platí pravidlo, že čím vyšší stupeň zabezpečení, tím vyšší limity pojistného plnění.
Nezapomínejte však také na odpovídající pojištění věcí. V rámci pojištění domácnosti lze pojistit věci v uzamykatelných prostorách, ať už jde o sklepní kóje nebo třeba garáže. „Jestliže zloděj překoná například dveře uzamčené obyčejným dózickým zámkem, může pojištěnému vzniknout nárok na plnění až do výše 50 tisíc korun. Jsou-li věci umístěny v uzavřeném prostoru, jehož dveře jsou uzamčeny například bezpečnostním zámkem nebo celoplošnou závorou, limit pojistného plnění může dosáhnout až na 300 tisíc korun," dodává Ponertová. ■

Foto: Václav Maletínský

BEZPEČNÉ STADIONY

Martin Synecký, bezpečnostní manažer Fotbalové asociace České republiky, si na nezájem médií nemůže poslední dobou rozhodně stěžovat. V oblasti bezpečnosti však je to málokdy vítaný jev, protože v drtivé většině případů je vyvolán negativními událostmi. V tomto případě násilím na stadionu, což bylo i tématem našeho rozhovoru.

Tomáš Jirásko

Martin Synecký, bývalý podplukovník Policie ČR, patří mezi uznávané bezpečnostní odborníky v oblasti diváckého násilí nejen u nás. Této problematice se věnuje od roku 2001, kdy tento elitní policista působil u Kriminální služby a v řadách Interpolu. Participoval na Euru 2000/2008/2012, fotbalovém MS 2006 v Německu, na zasedání Měnového fondu a Světové banky, Summitu NATO, MS v hokeji, MS v lyžování. Zúčastnil se více než 50 venkovních a 100 domácích utkání UEFA. Byl členem EU Think-Tank PCWG. Od roku 2011 působí jako bezpečnostní manažer Fotbalové asociace ČR.

Březnový incident během fotbalového utkání v Ostravě opět otevřel otázku bezpečnosti na stadionech, především těch fotbalových. Ministr vnitra Chovanec prohlásil, že vina je na straně fotbalové asociace. Jaký je váš pohled? Je technické zajištění stadionů odpovídající? Jaký je případný směr, kterým se budete v této oblasti ubírat?

Stadiony obecně a fotbal v České republice považujeme za bezpečné. Když se podíváte dva, tři roky dozadu, tak vážnější incidenty za celou dobu byly tak tři, čtyři. To je i na západní Evropu poměrně velmi nízký průměr. Mírná mediální hysterie, která nyní nastala po březnovém utkání Ostrava – Sparta, není až tak úplně na místě. Ve všech vyjádřeních jsme říkali, že jde o ojedinělý případ, který nicméně opět dokázal to, co pořád opakujeme. Že stát není schopen vytlačit pár lidí, kteří způsobují problémy, ze stadionů. Policie o nich ví, policie je stíhá, pořadatelé je znají, ale ti lidé stále nejsou odsouzeni za činy, které spáchali před dvěma, třemi lety. A pokud už tresty přijdou, přicházejí pozdě. Nezlobte se, ale trest osm hodin veřejně prospěšných prací za napadení pořadatele – to nám přijde úplně směšné. Asi největší problém, který tedy máme, je, že se nám nedaří vytěsnit poměrně malou skupinu lidí ze stadionů. Další obecný problém je skutečnost, že ne na všech stadionech jsou zcela odpovídající technické podmínky. V tom měl ministr vnitra pravdu. Bohužel stále žijeme v Čechách, čili ve světě výjimek a různých úlev. Nyní předseda Pelta garantoval, že s tím je konec, protože se na Baníku jasně ukázalo, že pokud se výjimky udělují, tak je to vždy na úkor bezpečnosti.

Ale stadionů, které mají tento problém, je v republice velmi málo. Většina klubů investovala do zlepšení bezpečnosti obrovské prostředky, zejména kluby s velkou fanouškovskou základnou. Nemůžeme chtít, aby kluby jako Příbram investovaly stejně jako Sparta. Stadiony jsou úplně rozdílné, základna jiná, rizikovost rovněž zcela jinde. Současným trendem na stadionech je propojení nových technologií, zejména s kamerovými a vstupními systémy. Tři nejmodernější arény – Eden, Sparta a Plzeň – již disponují velmi dobrými prostředky pasivní bezpečnosti na vstupech i kamerovými systémy. Jasně se ukazuje, že kvalitní kamerové systémy plus vstupní systémy jsou výbornou preventivní aktivitou. A je to i směr, kterým se chceme vydat.

Zmínil jste nízké tresty. Je to kvalifikací činu, kterou určuje státní zastupitelství nebo soud? Z našeho pohledu by se totiž v řadě případů mohlo pohlížet na fotbalové násilí jako na činnost prováděnou v organizované skupině. Nepamatuji si, že by tuto kvalifikaci někdo využil, v podstatě zůstáváme v oblasti výtržnictví.

Jako organizovanou skupinu odsoudil pachatele zatím jediný soud, a to byl soud v Opavě, přibližně před dvěma lety. Jinak nikdy ani státní zástupce ani soudce neklasifikovali tyto činy jako jednání organizované skupiny. Další problém je, že řada soudců přivírá oči, protože se jedná o fotbal. U stejného činu, kdyby byl spáchán jinde na veřejnosti, by padaly tresty daleko vyšší. Klasickým příkladem může být derby Slavia – Sparta z podzimu loňského roku, kde došlo k napadení policisty fanouškem, a státní zástupce to klasifikoval jako přestupek. Kdyby to udělal mimo fanouškovský průvod, tak je to zjevný útok na veřejného činitele. Nevidím jediný důvod, proč v této chvíli to nebylo posouzeno jako trestný čin, ale jenom přestupek. To pak dává vítr do plachet fanouškům, kteří si tuto informaci mezi sebou rychle předají a roste jim sebevědomí a pocit beztrestnosti.

Je tedy část problému i na straně ministerstva spravedlnosti? Nepomohlo by, aby ministerstvo například ve spolupráci s Nejvyšším soudem tyto činy jasně zařadilo a stanovilo, jak by je měli soudci posuzovat? Stejně jako učinilo v otázce hodnoty lidského života?

Ministerstvo spravedlnosti činnost a rozhodování soudů neovlivní. Jak jeho úředníci sami říkají – jsou spíš správci majetku soudů. To je ustálená fáma mezi lidmi, že ministerstvo spravedlnosti ovlivní soudy.

ROZHOVOR

Z našeho pohledu největší nedostatek legislativy tkví zejména ve výši trestů a rychlosti jejich udělování.

Doporučuje, ale autonomie soudu je nezpochybnitelná, každý soudce může na stejný skutek nahlížet jinak. Což je také jeden z velkých problémů, které máme v rámci fotbalu, protože za stejné skutky jsou fanoušci v různých krajích různě postihováni. A to není úplně optimální. My máme pořád snahu – a věřím, že komise, která pod vedením ministerstva vnitra, školství a FAČR vznikla, také ustálí výklad a vydefinuje skutky tak, aby vznikl speciální manuál pro soudce. Aby měli alespoň nějakého průvodce, jak na co nahlížet.

Naše právo nemá ukotven precedentní model, ale v jiných oblastech soudy přihlížejí k rozhodnutí ostatních soudů. V případě fotbalového násilí se v drtivé většině proti rozsudku státní zastupitelství neodvolává. Není problém i v tom, že stát rezignoval a spokojí se s málem, místo aby šel za „maximálním ziskem“?

Z našeho pohledu největší nedostatek legislativy tkví zejména ve výši trestů a rychlosti udělování trestů. Protože policie velmi často pachatele rychle dohledá, lidi identifikuje, sdělí obvinění. Státní zástupce je často poměrně rychle zažaluje. Nicméně poté následuje velká prodleva než proběhnou soudy. Tresty bývají roztříštěné a podle nás často úplně neodpovídají skutkům. Chybí větší právní povědomí o nebezpečnosti či spíše vnímání nebezpečnosti skutků na straně soudců. Bylo by možná přínosné realizovat specializovaný kurz/seminář ve spolupráci s ministerstvem spravedlnosti, který by se nějakým způsobem pokusil navrhnout rámec či metodiku, v nichž se budeme pohybovat při posuzování těchto činů. Uznávám, je to činnost velmi obtížná. A když před vás přijde v rámci soudního líčení devatenáctiletý mládenec, téměř ubrečený, v obleku, s rodiči a mladším sourozencem, tak dojem společenské nebezpečnosti z pohledu soudce bude logicky nízký – v potaz vezme, jako každý z nás, fakt, že tvrdý postih poznamená mladíka na celý život. Vidí slušně oblečeného člověka s podporou rodiny, a tak bere do úvahy i možnost jeho nápravy. Už nevidí to, že ten člověk se tři roky obléká do černé mikiny s kapucí, páchá něco na stadionech i mimo stadiony a je reálně nebezpečný společnosti. Při čtení rozsudků často slyšíte, že se jedná o fotbalové násilí, ale my přesto nemáme definici fotbalového násilí. Takže se domníváme, že kdyby soudní rozhodnutí byla rychlá (a neříkáme extrémně přísná) a odpovídající skutkům, tak aby to bylo citelné a nepadaly jenom pokuty a veřejně prospěšné práce, že by zde zapůsobil efekt odstrašení.

Stále existuje evropská dohoda o fotbalovém násilí. Lze říci, že Česká republika z hlediska legislativy a dohod toto doporučení Evropské komise plní?

Úmluva k diváckému násilí je poměrně hodně starý dokument, téměř 20 let. Byl několikrát novelizován, Česká republika jej podepsala prostřednictvím ministerstva vnitra. Podmínky, k jejichž splnění se Česká republika zavázala, jsou v ČR téměř všechny zavedeny a dodržovány. Řada věcí je navíc jenom doporučujících, nikoli nařizujících. Přesto jsme většinu zavedli s různými stupni úspěšnosti. Bohužel mezi ne zcela implementované patří evidence rizikových fanoušků. Ta u nás neexistuje v takové podobě, aby s ní pořadatelé mohli nakládat. Je to nyní předmětem velkého jednání, kterým budeme muset projít a získat stanovisko a povolení od Úřadu pro ochranu osobních údajů a databázi zavést.

Ministr Chovanec ale řekl, že již před lety vznikla „kuchařka“, jak kluby mají postupovat, aby databáze mohly udržovat. Kde je tedy problém? Protože my teď slýcháme ze strany státu, že všechno je na klubech, že kluby mají špatně nastavena svá pravidla, že se na stadionech mají chovat jako vlastníci.

Problém je právě v ochraně osobních údajů. Kluby mají možnost shromažďovat osobní údaje za účelem, který ÚOOÚ schválí. Většinou to jsou jmenné seznamy osob, které cestují na zahraniční utkání, vydávají se jim vstupenky, nebo v případě, že se jedná o rizikové utkání a jsou vydávané vstupenky na jméno. Problém, na který jsme narazili, je ale možnost efektivního vyměňování těchto informací mezi kluby, případně zavedení centrální databáze s možností využití zákazu vstupu v rámci institutu pána domu. Tady si úplně nejsme jistí a čekáme na vyjádření ÚOOÚ, kdy se chceme opřít o zákon o podpoře sportu, kde se v § 7a hovoří o tom, že pořadatel na sportovní nebo kulturní akci má učinit veškerá možná opatření k tomu, aby zaručil bezpečnost akce. Náš výklad je, že i tato databáze a výměny informací o rizikových fanoušcích jsou jedním z opatření, které tento zákon dokonce nařizuje. Myslím, že to bude jedno z největších témat právě vznikající komise.

Předseda Pelta navrhl několik modelů, včetně jeho oblíbeného holandského. Jaká je tedy představa ideálního stavu, počínaje ticketingem, identifikací fanoušků a podobně?

My jsme si navrhli třífázovou realizaci našich záměrů. Na prvním místě zavedení omezení vstupu osobám rizikovým, zejména těm, které mají již vyslovený zákaz vstupu. Ten princip je velmi jednoduchý, protože na to stačí čtečka čehokoliv, zatím nemůžeme říkat, jestli to bude nějaká karta nebo osobní doklad. Pokud například technologicky omezíme objem snímaných dat, není seznámen s konkrétními osobními údaji dané osoby ani pořadatel, protože ta jsou uložena na serveru v databázi a on obdrží pouze oznámení, že určitá osoba nemá oprávnění k vstupu, a nepotřebuje vědět proč.

Takže by šlo o princip bankovních registrů či autorizace jako u platební karty?

Víceméně. To je přibližně první krok. Druhým krokem by bylo propojení tohoto systému se systémem prodeje vstupenek a závěrečný krok by navázal speciální kamerové systémy zaměřené na vstupy tak, aby byly provázány osoby vstupující na stadion s obrazovým záznamem a kontrolou obrazu v databázích. Zde jsme si vědomi, že je to velmi drahá záležitost, proto jde až o poslední krok, který teoreticky můžeme nasadit. Když se podíváme po Evropě, tak mimo asi tří stadionů takový systém nikde není. Prakticky nejlépe vybavený stadion v Evropě je Amsterdam Arena, kde je těchto systémů obrovské množství. Ale i tam to bylo umožněno hlavně tím, že dodávající firma ho instalovala jako reklamu, referenční projekt. My si myslíme, že v prostředí českého fotbalu by možná již první krok mohl zabránit tomu, aby se na stadiony dostávali lidé, kteří již mají záznam v trestním rejstříku nebo je jim vysloven zákaz vstupu v souvislosti s fotbalem.

Vrátím se k pořadatelské službě. Často se jako problematický zmiňuje status pořadatele, který se neliší od postavení běžného občana. Médii je proto často dáván za příklad anglický model, kde má mít steward význačnější pravomoci. Jak tedy anglický model funguje?

Ani v Anglii nemá steward výjimečný status. Ale využívají velmi šikovně existující legislativu. Paradoxem je, že podobný princip umožňuje i zákon v ČR. I když si neumím představit jeho aplikaci. V Británii je pořadatel definován jako pořadatel a samozřejmě mají fotbalový zákon, který jasně vyjmenovává přestupky fanoušků a sankce, které jsou za tyto přestupky udělovány. Mimo jiné tam je odmítnutí výzvy pořadatele, což u nás sice je porušením návštěvního řádu, ale pro fanouška to neznamená prakticky vůbec nic. V Anglii jde o institut, a pokud nastane problém v hledišti, jde ho vyřešit steward (pořadatel). Pokud se situace vyvíjí tak, že ji pořadatel nemusí zvládnout, tak stačí přítomnost jediného zasahujícího policisty v uniformě, aby všichni ostatní pořadatelé, kteří tam v dané chvíli zasahují, požívali ochrany veřejného činitele. Tento institut je i v České republice. I u nás osoby, které pomáhají při zákroku policie, mají stejnou ochranu jako policista, který zasahuje. V praxi si to ovšem neumím představit. Byť je to jedna z možných cest, zcela legálních cesta, je to zatím nepoužívaná cesta. Je to i otázka vzniklé komise, zda by státní zástupci a soudy byli ochotni akceptovat tento model. Britský model je velmi účinný, protože fanoušci vědí, že pokud se objeví uniforma, každý pořadatel, který je v okolí, má stejný status jako policista. Z hlediska ekonomiky je to nejrozumnější i nejlacinější řešení pro daňového poplatníka.

Považujete z tohoto pohledu pořadatelskou službu za dostatečnou, dostatečně proškolenou, profesionální? Je řešením najmout za pořadatele skupinu boxerů, v lepším případě bezpečnostní agenturu?

Opět se vrátíme na začátek. Na hrubý pytel musí být hrubá záplata. Pokud by fanoušci nedělali problémy bezpečnostního charakteru, nebylo by potřeba tam mít bezpečnostní agenturu, ale stačili by pořadatelé. My velmi striktně rozdělujeme pořadatelskou službu a bezpečnostní agenturu. Samozřejmě vize je taková, aby na místě byla hlavně pořadatelská služba. Já tomu lidově

Foto: Václav Maletínský

říkám uvaděči. Tak jako v kině, v divadle, lidi, kteří uvádějí, vítají. Čím míň bude problémů v hledištích, tím míň tam bude lidí z bezpečnostních agentur. Na stadionech většinou bezpečnostní agentury slouží spíše jako záloha. Jsou tam na prvním místě standardní pořadatelé a teprve v případě problémů nastupují příslušníci bezpečnostních agentur. V ČR je praxe, že bezpečnostní agentura se a priori stará o sektor hostů místo pořadatelské služby. Je to zavedená praxe, která má svůj historický důvod. Je jasně zadokumentované, že 90 % problémů na stadionu vzniká v sektoru hostí, protože na výjezdy většinou jezdí spíše ti problémoví a pouze menší procento těch neproblémových fanoušků. Pořadatel proto umisťuje do sektoru hostů rovnou bezpečnostní agenturu.

Podívejme se na zákrok očima daňového poplatníka. Nezainteresovaný občan logicky usuzuje, že v okamžiku zásahu policie na stadionu vznikají náklady, které musejí být policii uhrazeny. Ale nevzpomínám si, že by soudce někdy do rozsudku zahrnul i to, že musela být nasazena policie a státu vznikla škoda. Alespoň klubu jako takovému. Pokud bychom pracovali s vyčíslením nákladů na zásah, tak se dostáváme minimálně do řádu desítek, či spíše stovek tisíc. Není chybou i to, že tyto zákroky považujeme za běžnou činnost policie na ochranu veřejnosti?

Vezměme to úplně od začátku. Případný zákrok policie na stadionu neznamená, že musí být policií vymáhaná náhrada škody po pořadateli. Protože zákon o podpoře sportu ve druhém odstavci jasně hovoří o tom, že pořadatel má povinnost udělat veškerá možná opatření, a dohoda policie a fotbalové asociace pracuje s pojmem místní ujednání, které hovoří o tom, že policie souhlasí s přípravou a zajištěním sportovní akce. Ve chvíli, kdy je podepsáno místní ujednání a policie souhlasí s opatřeními ze strany pořadatele, tak souhlasí s tím, jakým způsobem pořadatel akci zabezpečil, tudíž že přijal veškerá možná opatření. Policie jasně razí teorii, že pořadatelé nejsou od toho, aby se prali s výtržníky na stadionech. Nejsou vycvičení, vyškolení, nemají na to oprávnění. Tudíž pokud dojde k vážným střetům, zasahuje policie. Je to přesně i březnový případ na Baníku Ostrava, kdy policie sepsala místní ujednání a byli předem připravení, že v případě excesu pořadatelé nejen že nebudou zasahovat, ale vůbec v místě zásahu nebudou, aby se policii nepletli. Protože praxe z minulosti ukazuje, že pořadatelé, často v horlivé snaze pomoct, se policistům pletou. Nyní je praxe taková, že ve chvíli, kdy dojde k nějakému incidentu, který pořadatelská služba není schopna zvládnout, ale za předpokladu, že předtím učinila veškerá opatření k tomu, aby ta situace nenastala (a přesto nastala), tak hlavní pořadatel požádá o zákrok policie. Pokud s tím policie souhlasí, vydá hlavní pořadatel pokyn, aby se megafony nebo veřejným rozhlasem oznámilo, ve kterém sektoru proběhne zákrok policie. Rozhodčí má povinnost přerušit utkání a zavést hráče do bezpečného prostoru. A je to přesně ten okamžik, kdy vzniká dvou až pětiminutový prostor pro nezúčastněné diváky dotčený sektor opustit nebo se od problémového chování distancovat. Policie provede zákrok, situaci uklidní a poté předá odpovědnost zpátky pořadateli, pořadatel dá pokyn rozhodčímu a hra pokračuje. To je model nastavený na českých stadionech. Za poslední tři roky bylo utkání přerušeno kvůli zákroku policie asi jenom šestkrát. Třikrát se jednalo o vniknutí fanoušků na hrací plochu, z toho dvakrát v druhé lize a asi třikrát to bylo kvůli nebezpečné pyrotechnice. Čili zase: těch incidentů není tolik a policie za ty dva nebo tři roky ani jednou nepožadovala náhradu škody po pořadateli.

Zmínil jste pyrotechniku. Řada fanoušků tvdí, že pyrotechnika je bezpečná, že dochází ke zbytečné snaze o kriminalizaci.

> Rozhodčí má povinnost přerušit utkání a zavést hráče do bezpečného prostoru. A je to přesně ten okamžik, kdy vzniká dvou až pětiminutový prostor pro nezúčastněné diváky dotčený sektor opustit nebo se od problémového chování distancovat.

Jak se to vezme, třeba ve Francii se použití pyrotechniky na stadionu považuje za terorismus. U nich je to výbušný systém, ať je to velká, nebo malá pyrotechnika. U nás je pyrotechnika zakázaná obecně, neměla by být na stadionech vůbec. Pro ty fanoušky, kteří si říkají, že je bezpečná, bezpečná určitě není – jen za tuto sezónu už máme tři vážné úrazy. Jednoho fanouška odváželi s popáleninou břišní dutiny vrtulníkem do nemocnice. Propašování pyrotechniky na stadion je ale naprosto jednoduchá záležitost. Kdo ji chce propašovat, tak ji propašuje. Aby pořadatel zabránil pronesení tohoto druhu zábavní pyrotechniky, musel by provádět procedury jako při vstupu do letadla. My jsme to zkušebně počítali na stadionu Sparty Praha, kdy přes vstup číslo jedna projde zhruba šest tisíc lidí. Letištní procedurou by to trvalo šestnáct hodin. A pořadatel nemůže kontrolovat úplně veškeré tělesné dutiny, takže je prakticky nemožné zabránit tomu, aby se tam nějaká rachejtle dostala. Samozřejmě se odhalují nové a nové triky. Bohužel často spolupracují s někým přímo ze stadionu. Ať je to pořadatel, někdo z cateringu, vždy se někdo najde. A vraťme se i k infrastruktuře stadionů – pokud nemáte celistvě uzavřený plášť, tak můžete dělat, co chcete, a stejně vám ji někdo propašuje přes plot.

Připravuje se pro příští rok zpřísnění licenčních podmínek pro fotbalové kluby z hlediska bezpečnosti?

Já si myslím, že to dobře vystihl ministr vnitra s panem předsedou Peltou. My už teď máme velmi přísné vnitřní normy. Musíme ale trvat na tom, aby se bez výjimek dodržovaly. To je i nyní velmi nepopulární postup proti vulgarizmům na stadionech, výhružkám smrtí – protože to je v návštěvních řádech, je to v soutěžním řádu. Pouze se nic dlouho neřešilo, až se to dostalo do takovýchto hrozných rozměrů. My nebudeme zpřísňovat, nebudeme vymýšlet nic nového, pouze tvrdě požadovat uplatňování stávajících vnitřních norem.

Jaká je tedy odpovědnost klubů, tedy i za chování hostujících fanoušků? Slýcháváme, že klub za to nemůže, že zodpovědní jsou fanoušci hostí.

To je jednoduché. Pustili je na stadion. Tím vzniká odpovědnost. Ale tady se musíme zase vrátit k základním problémům – infrastruktuře, k ticketingovým systémům.

Na druhé straně pořadatel má povinnost učinit taková opatření v rámci zákona o sportu, aby zajistil bezpečný průběh. Prioritou je bezpečnost. Pokud se pořadatel akce rozhodne, že není schopen zajistit sektor hostí tak, aby mohl garantovat bezpečnost, má oprávnění ty lidi tam nepustit.

Je v rámci pořadatelské služby dostatečně pokryta krajní nouze, nutná obrana a podobné instituty?

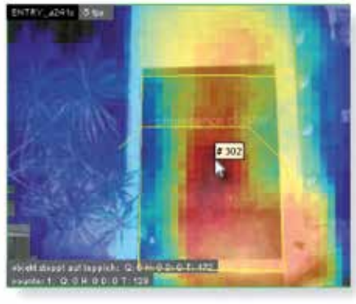
Určitě ano, my jsme v této oblasti pořadatele aktuálně školili, protože právní posouzení činu nepřísluší pořadateli. Pokud ale pořadatel v dané chvíli vyhodnotí, že by se mohlo jednat o trestný čin, má skutečně danou osobu zadržet a dokonce ji držet a omezovat na osobní svobodě na nezbytně nutnou dobu, než osobu předá Policii ČR. Dokonce máme i stanovisko státní zástupkyně pro Prahu 7, že je možné použít i různé zádržné systémy včetně pout a podobně, aby byl schopen osobu zajistit do příjezdu policie. Fanoušci Sparty argumentovali tím, že tam byl někdo spoutaný pořadatelskou službou. Bylo to vlastně jednoduché v tom, že šlo o mírnější prostředek, než kdyby ho drželi čtyři stokiloví chlapi. Čili oprávnění krajní nouzí, nutnou obranou a možnosti postupů jsou přesně to, co školíme. Ale rozhodně to není institut, který je pro nás ideální.

Takže ideální stav je … ?

Byli bychom rádi, aby měl pořadatel možnost jednoduše stanovit: na základě mých informací je toto utkání rizikové, tak zavedu adresný ticketing. Na normální fotbal – třeba když do Budějovic přijede Příbram – to není potřeba, ale na vybraná riziková utkání by tady ta možnost měla být. Jednoduchá možnost – bez obav, že tím porušuji něčí práva, nevhodně nakládám s údaji, nemusím složitě žádat, dokazovat k čemu to potřebuji. Do budoucna je třeba zavést adresný systém plošně. V Itálii – byli jsme na Juventusu – se to třeba takto dělá. Všichni automaticky chodí s občankou a lístkem v ruce a pípají si přes čtečky. Italové nám říkali, že ze začátku mírně opadl zájem fanoušků, protože z toho měli obavy, ale během dvou let návštěvnost začala rychle stoupat, protože od té doby nebyl žádný větší problém. Takže si myslím, že i u nás by to mohlo být správné řešení. ■

BEZPEČNOST NA STADIONECH Z HLEDISKA CCTV

SPECIFICKÉ POŽADAVKY PRO STADIONY



Požadavky na bezpečnost z hlediska kamerových systémů na sportovních stadionech se v některých ohledech blíží požadavkům např. na městské kamerové systémy, zabezpečení letišť, velkých nádraží apod. Pro stadiony je typické sledování na velké vzdálenosti, v nepříznivých světelných i klimatických podmínkách. To vyžaduje časté nasazení venkovních antivandal provedení kamer. Tomu ideálně vyhovují např. nové modely IP kamer Canon a ACTi. Například špičkový model speed dome kamery I96 od ACTi nabízí rozlišení 2 megapixely s 30násobným optickým zoomem, hodnotou WDR až 147 dB. V nabídce ostatních výrobců najdeme kamery srovnatelných parametrů jen u několika konkurentů.

VIDEOANALÝZA VYUŽITELNÁ PRO STADIONY

Videoanalýza zabudovaná v kameře

Možnosti analýzy obrazu přímo v kameře končí u převážné většiny výrobců funkcí detekce pohybu. Omezení na 3 detekční obdélníkové zóny nedává příliš možností na reálné použití. Výjimkou jsou zabudované videoanalytické funkce IP kamer Canon. Kamery poskytují až 15 nezávislých procesů, pro každý z nich je možné definovat samostatnou detekční zónu s polynomiálním ohraničením. Tím se nasazení takových kamer přibližuje systémům středního či rozsáhlého kamerového systému věnovat se plně řešení krizových situací.

Příklad instalace IP kamer na stadionu

Za příklad může posloužit referenční instalace IP kamer Canon na hokejovém stadionu HC Sparta Praha. Stadion je i domácí scénou HC Lev, bylo na něm tedy nutné dle podmínek KHL nainstalovat kamerový systém monitorující případné výtržnosti v hledišti. V prostorách sportovní haly jsou použity 2 pevné dome kamery a 4 PTZ kamery s rychlým kontinuálním autofokusem. Během zápasů kamerový systém obsluhuje bezpečnostní pracovník, který dle instrukcí pořadatelů snímá detailně místa incidentů. Pro výběr kamer byly důležité zejména jejich citlivost a velký rozsah dynamiky, která umožní rozlišit tváře v protisvětle (halogeny osvětlení svítí proti směru pohledu kamer, snímaná část hlediště je až za reflektory). Pro záznam je použitý SW Netavis. Celé zařízení se zapíná pouze na dobu zápasů. Funkce videoanalýzy nejsou v tomto případě využívané.

Pavel Koška
Autor pracuje jako
Projektový manažer CCTV
ve společnosti VARIANT plus

Možnosti pokročilé analýzy běžící na VMS serveru

Předností detekce běžící na VMS serveru je široká škála funkcí. Oproti funkcím integrovaným v kamerách (Canon) umožňuje VMS použití mnohem sofistikovanějších algoritmů. K dispozici je navíc např. počítání lidí/objektů, monitoring narušení zóny, zobrazení historie trajektorie objektu, grafické znázornění četnosti průchodů či doby setrvání. K dispozici jsou i funkce, které přesahují z oblasti bezpečnosti do marketingu. Např. modul Netavis iCAT nabízí možnost rozpoznávání obličejů pro určení demografické struktury návštěvníků (věková skupina + pohlaví). To otevírá nové možnosti využití kamerového systému. Takové řešení umožňuje operátorovi v dohledovém centru VMS s analýzou na serveru. Pro stadiony jsou vhodné zejména funkce detekce pohybu, sabotáže kamery, vyhodnocení úrovně zvuku, opuštěného předmětu a směrová detekce procházení.

FANOUŠEK VS. STUDENT V HOTELU

Fotbalový fanoušek není rozhodně žádné neviňátko a je zbytečné ho idealizovat. Jeho chování však do značné míry předurčuje legislativa, která platí v jeho zemi, a „kultura kmene". Představuje však skutečně tak velké riziko? A co třeba takový student?

Za asi nejnebezpečnější fanoušky jsou označováni angličtí tzv. „hooligans", s kterými u nás máme již řadu negativních zkušeností. V závěsu za nimi jsou pravděpodobně „Ultras" z Itálie. Ti ostatní jako „Torcidas Organizadas" z Brazílie či „Barra Brava" z Argentiny a další skupiny ze zemí Latinské Ameriky si s nimi asi nezadají, ale s těmi naštěstí moc zkušeností nemáme.

Za dlouhou dobu své praxe, kdy jsem z pozice člena nejvyššího vedení hotelových společností měl možnost řídit některé pražské hotely, jsem až na pár drobností v podobě rozbité vázy, strženého obrazu či „vystříkaného" hasičského přístroje nezažil vážnější útok na svěřený majetek, tedy hotelové budovy a jejich zařízení. Spíše se jednalo o úsměvné a někdy doslova humorné zážitky s fotbalovými fanoušky.

Jako příklad mohu uvést dvojici fanoušků z Británie, kteří si od prvního dne natolik oblíbili náš bar a jeho personál, že svůj zápas, kvůli němuž zaplatili letenky a ubytování v hotelu, nestihli. Stejně jak jsem je opustil odpoledne, našel jsem je i druhý den ráno stále popíjející na našem baru. Na moji otázku, jak to dopadlo, mi s typicky skotským humorem odpověděli: „Nevíme, ale máš dobré pivo!" Po snídani celá početná skupina skotských fans odjela spořádaně na letiště, bez jakéhokoli incidentu.

Za dlouhá léta v oboru jsem z dotazníkových šetření a cíleně vedených rozhovorů s kolegy hoteliéry opravdu nezaznamenal zdemolovaný hotel po fotbalových fanoušcích. Je zvláštní, že tato skupina hostů, která je označována za problémovou (dostane tento „cejch"), se chová v hotelech relativně slušně. Samozřejmě až na výstřelky při rušení nočního klidu, ale většinou na ně platila domluva a ráno se provinile šli na recepci omlouvat za svoje chování.

Samozřejmě se čas od času najdou tzv. „fanoušci", kteří v podnapilém stavu demolují vše, co jim přijde do cesty, ale tento jev se projevuje spíše v restauračních provozech, případně tam, kde do cesty „vstoupí" zahrádky se židlemi. Tak proběhl před několika lety incident v ulici Na Příkopech, kde vandalové doslova zničili „předzahrádku" u jedné z restaurací.

Musím se však přiklonit k názoru řady hoteliérů, kteří mi svorně potvrdili, že daleko nebezpečnější skupinou bývají zahraniční studenti, kteří naši republiku navštěvují obzvláště v průběhu zimních a jarních měsíců, tedy od ledna do začátku dubna. Po jejich „nájezdech" jsou některé hotelové pokoje neobyvatelné a musí projít alespoň základní renovací, od zakoupení nového nábytku až po vymalování hotelových pokojů a chodeb. V některých případech je toto jejich chování podporováno ze strany jejich dozoru, tedy pokud dozor není „zaměstnán" něčím jiným, případně se vůbec v hotelu nevyskytuje. Za nejhorší z těchto studentských skupin jsou označováni Italové, které ale v poslední době jasně překonali studenti dánští a švédští, čehož důkazem je nedávný případ, kdy doslova lehl popelem hotelový pokoj na náměstí Republiky v Praze.

Těmto excesům se lze snadno vyhnout, pokud na některé poptávky cestovních kanceláří nebudeme reflektovat, anebo přímo tyto studentské skupiny odmítneme. Bohužel, některé hotely z „ekonomických důvodů" jdou raději do rizika a tyto skupiny přijímají. Je pak jen a jen na schopnostech jejich vedení, zda dokáží z předem vybraných „kaucí" uhradit vzniklé škody. Někdy se to povede, ale nálepku „studentského" hotelu, která vám na základě stížností ostatních klientů může být přilepena, se po dlouhou dobu nemusí podařit odpárat. Pošramocená pověst vašeho hotelu se pak promítne do nižších tržeb, které budete potřebovat někde vykompenzovat.
A jedinou možností častokrát je jen to, že přijmete další studentskou skupinu – v obavách, jak to vše dopadne. A pak, že fotbaloví fanoušci jsou největší zlo!

Kromě fyzické bezpečnosti při podnikání nesmíte nikdy zapomenout ani na bezpečnost ekonomickou a opomíjet vážení rizik. U fotbalových ultras existují na mezinárodní úrovni mechanizmy, které těm nejhorším zabraňují v cestě. Možná bude nutné něco podobného zavést i u studentů. A mimochodem – víte vůbec, jaké skupiny hostů váš hotel navštěvují? ■

Marek Merhaut
Autor pracuje jako vedoucí katedry hotelnictví na Vysoké škole hotelové v Praze 8

BEZPEČNOST NA STADIONECH

V posledních týdnech se znovu otevřela diskuse o bezpečnosti na stadionech, zejména těch fotbalových. Není to nové téma, objevuje se v různých obměnách vždy po nějakém incidentu.

CO JE PODSTATOU PROBLÉMU?

Ve společnosti roste počet jedinců, kteří mají problémy se seberealizací a své komplexy si léčí prostřednictvím agresivních projevů pod rouškou anonymity davu. Takové prostředí umožňuje jednotlivci, aby svou frustraci ventiloval např. nějakým fyzickým útokem (ať už proti člověku nebo věci) nebo vědomým protiprávním chováním. Uvnitř komunity podobně zakomplexovaných tak dotyčný získá uznání a punc „hrdiny", ale přitom navenek zůstane anonymní. Toto chování není svojí podstatou přímo spojené s fotbalovými stadiony, tyto projevy můžeme v různých podobách vysledovat všude, kde se vytváří dav (např. při demonstracích) a kde se dá očekávat konflikt. Fotbalové stadiony jsou tedy pouze vhodným prostředím.

JAK PROBLÉMU ČELIT?

K výše zmíněným projevům dochází pouze ve skupinách – nikdy se tento jev nevyskytuje u osamocených jedinců. Čím jsou tyto skupiny větší, tím je větší i riziko takovýchto projevů. Často jsou k protiprávní činnosti používány prostředky nebo nástroje, které jsou i přes zákaz na stadion proneseny.

Organizační opatření

Jednou z cest, jak takovému chování zamezit, je rozdělení velkých rizikových skupin na menší části. To je také úlohou pořadatelské služby a případně zásahové jednotky policie.
Dalším opatřením může být např. prodej vstupenek na jméno, s nutnou identifikací držitele, a tím omezení anonymity prostředí.
Pokud někteří jedinci už byli dříve za podobné přestupky trestáni, je možné jim zakázat vstup na stadion. Bohužel, zatím u nás neexistuje centrální registr takových „hříšníků" a jeho sdílení všemi sportovními kluby, podobně jako je tomu např. ve Velké Británii.

Technické prostředky

Prostředí anonymity je možné také eliminovat instalací kvalitních (!) kamerových systémů. Takový kamerový systém musí disponovat nejen možností záznamu a dostatečně vysokým rozlišením, ale též vysoce světelnými objektivy a schopností zobrazit detail i za extrémních světelných podmínek (sluneční světlo, stín, umělé osvětlení…). Tyto systémy se však nedají pořídit levně. Nevýhodou kamerových systémů je, že dovedou protiprávní jednání pouze zaznamenat, ale nikoli mu předcházet.

Vedle kamerových systémů se dnes můžeme setkat i s preventivními opatřeními, konkrétně bezpečnostní kontrolou pomocí průchozích detektorů kovů a zavazadlových rentgenů, podobně jako je tomu na letištích. Taková kontrola může minimalizovat pronesení předmětů, které by mohly být použity k protiprávní činnosti. Tyto technologie jsou u nás instalovány např. v pražské O2 aréně, kam je dodávala společnost Rapiscan Systems.
Nejmodernějším prostředkem pro zamezení pronášení skrytých předmětů jsou detektory společnosti Microsemi, pracující na principu pasivních milimetrových vln (PMMW). Tato část elektromagnetického spektra, kterou vyzařuje samo lidské tělo, bez problému proniká oblečením, avšak ukryté předměty jsou pro něj překážkou. Přístroje dovedou odhalit i předměty, které jsou pomocí detektorů kovů neodhalitelné (dřevo, plast, zábavní pyrotechnika…). Navíc umožňují kontrolu osob za pohybu a neomezují tak propustnost vstupů.

Častým argumentem proti nasazení kontrolních technologií je argument omezení propustnosti vstupu. Ano, pokud bychom chtěli aplikovat kontroly na stejné úrovni jako na letišti, pak by zdržení, způsobené bezpečnostní kontrolou, bylo skutečně veliké. Ale ruku na srdce, opravdu potřebujeme při vstupu na stadion odhalovat předměty jako zapalovač, nůžky na nehty, lahev s vodou apod.? Pokud budeme racionálně zvažovat hrozbu, pak nám moderní technologie umožní kontrolovat bez problému 10–15 osob za minutu. A to není tak velké zdržení. Naopak, budou-li se muset diváci dostavit na stadion o něco dříve, budou mít více času, aby utratili své peníze např. za klubové předměty.

ZÁVĚR

Chceme-li minimalizovat agresivní projevy na stadionech, je nezbytně nutné provést kroky, spočívající v kombinaci organizačních i technických opatření. Stejně tak je nutná úzká spolupráce pořadatelů s policií a dodavateli bezpečnostních technologií. Pokud se to podaří, pak násilí na stadionech skutečně omezíme. Možná se však objeví někde jinde. Budeme-li chtít omezit agresivní chování ve společnosti obecně, je třeba se hlouběji zamyslet nad jeho skutečnými příčinami. ■

Milan Krása
Autor pracuje jako ředitel divize Rapiscan ve společnosti PCS

PROFESIONÁLNÍ PERIMETRICKÁ OCHRANA Z ITÁLIE

Firma Politec Srl je italská společnost s dlouholetou tradicí (od r.1990) sídlící v Miláně. Specializuje se na vývoj a výrobu profesionálních perimetrických systémů – infra bariér, mikrovlnných bariér a jejich příslušenství.

Převážnou část produkce vyráběné pro naši společnosť TSS Group tvoří IR a MW systémy pro outdoorové použití s dosahem od 15 až do 400 m.

Perimetrická ochrana výrobce slouží jako systém detektorů elektronické ochrany pozemku, přesněji jeho vnějšího obvodu – perimetru. V součinnosti s elektronickým zabezpečovacím systémem (EZS) chrání a varuje před vstupem narušitele nebo nepovolané osoby na chráněný pozemek. Výrobce využívá technologii IR závor i základní princip technologie objemové ochrany (mikrovlnné bariéry). Každá z nich má svá specifika a je určena pro různorodé prostředí nebo instalaci. Využitím jejich předností a vzájemnou kombinací lze významnou měrou a s dostatečným předstihem přispět k ochraně majetku ještě před vstupem do střeženého objektu. Primárně jsou určené pro budování rozsáhlých bezpečnostních projektů a mají včas upozornit uživatele na nechtěný vstup do průmyslových areálů, koridorů, vojenských objektů, letišť, fotovoltaických elektráren apod.

Samozřejmě je možné perimetrickou ochranu použít i v nenápadném nebo „maskovaném“ provedení, což ocení zejména klienti, kteří chtějí systém použít v domácím nebo komerčním prostředí. Takto použité systémy dokáží upozornit majitele na nežádoucí vstup na jejich pozemek, do zahrad, dvorů apod.

Hlavní výhodou použití perimetrických systémů Politec je technologie dvojité asférické optiky čoček a jejich snadné nastavení i bez předchozího složitého technického zaškolení obsluhy (SMA technology).

V IR bariérách je (podle typu modelu) osazených až 16 párů optických vysílačů/přijímačů. Každý pár je možno horizontálně otáčet až o 180 °, vertikálně o 20 °.

To je zárukou spolehlivosti bariéry, jejího libovolného nastavení podle potřeb,

rohového umístění, křížení (cross beam) pro zvýšení neprůchodnosti, možnosti vyloučení párů (PET imunity) atd.

V IR bariérách, pro usnadnění vizuální synchronizace, slouží několik vysoce svítivých LED diod na každém páru optiky s viditelností až několik set metrů. Použití bariér ve venkovním a ztíženém prostředí dovoluje stupeň krytí IP 54 a vnitřní vyhřívání s termostatem.

Detekce snížené viditelnosti (FOG detection) odpojuje automaticky poplachový výstup a pravidelně kontroluje opětovnou změnu podmínek pro obnovení střežicího režimu. Taková automatická minimalizace výskytu falešných poplachů enormně zvyšuje spolehlivost nasazeného systému.

Pro „domácí“ použití je na zařízeních integrovaná zajímavá funkce zabudovaného zahradního svítidla, což rozšiřuje jejich uživatelský komfort a zpřístupňuje instalaci pro masové komerční použití.

Při projektování systému a rozhodování o konkrétním řešení je třeba zohlednit řadu technických faktorů a vybrat vhodné

produkty. TSS Group a.s. jako autorizovaný distributor pro Českou a Slovenskou republiku disponuje týmem vyškolených pracovníků, kteří pomáhají instalačním společnostem právě při těchto návrzích řešení a jejich zavádění do projektů zabezpečení a ochrany majetku.

ALES
Jedná se o nejjednodušší dvoupaprskové IR závory malých rozměrů, s dosahem do 120 m v exteriéru a 480 m v interiéru. Jsou určeny pro univerzální použití.

SADRIN
Miniaturizované infra bariéry (konstrukční šířka jen 20 mm) s výškou 0,5 až 2 m jsou ideální pro pro ochranu oken, průčelí a fasád budov. Jejich dosah je od 5 do 15 m.

SANDOR, PARVIS
Sloupové infrabariéry jsou určeny pro uchycení na stěnu nebo „standalone“ volně v prostoru. Podle požadavků na úroveň bezpečnosti je dodáváno provedení s výškou až do 8 m. Osazeny jsou více páry IR vysílačů/přijímačů s asférickými čočkami a křížovou synchronizací, což dovoluje přesné optické zaměření mezi sloupy až do 400 m. Provedení se skrytou montáží ve sloupu zahradního svítidla umožňuje nenápadné použití skutečně kdekoli.

MANA
Technologicky nejvyspělejší varianta pro ultimativní ochranu perimetru – infra závory kombinované s mikrovlnnými bariérami. Využitím odlišných detekčních technologií zamezují jakémukoliv pokusu o překonání. Ideální pro použití v náročných bezpečnostních podmínkách. */PR/*

MARTIN GREN: NEJVĚTŠÍ ÚKOL IP KAMER JE DNES PORADIT SI V EXTRÉMNÍCH PODMÍNKÁCH

„Konkurence, která stále ještě prosazuje v bezpečnosti analogové video, to dělá proto, že jí plynou zisky z nákladné instalace. U IP kamer je dnes nejdůležitější, jak si zvládnou poradit s různými světelnými podmínkami. Klíčovou roli hraje také vysoké rozlišení, které dává iluzi 3D prostoru," říká Martin Gren, muž, který se umístil na prvním místě podle žebříčku IFSEC Global v hodnocení nejvlivnějších světových osobností v oblasti bezpečnosti a požární ochrany.

Firma Axis uvedla v roce 1996 na trh první síťovou kameru na světě. Jak vás něco takového v době tvrdé vlády analogu vůbec napadlo?
To je docela zajímavý příběh. Kdysi se naše společnost zabývala propojováním různých věcí pomocí datových sítí. V devadesátých letech jsem navštívil pracovně Japonsko a setkal se s místním zákazníkem, který měl velkou sbírku videokamer. S trochou lítosti se nás zeptal, proč se vlastně nevěnujeme také kamerám. Říkal jsem si, že je to docela dobrý nápad, ale po návratu domů jsem na to zapomněl. Kamarád mi pak jednou ukázal síťový videokonferenční systém, na kterém pracoval, a já jsem si vzpomněl na toho japonského zákazníka. Napadlo mě, že bychom mohli vytvořit síťové kamery.

Jaká byla v tomto ohledu vaše prvotní očekávání?
Když jsem hovořil s vedením a řekl jim, že chci vytvořit samostatné oddělení se síťovými kamerami, pokyvovali chvíli hlavami a pak řekli „fajn, ale musíte jich prodat alespoň 5 000". Naštěstí jsme jich nakonec prodali 12 000, což byl obrovský úspěch, a nové oddělení bylo na světě. IP kamery od té doby vyrábíme stále a jsme v této oblasti nejsilnějším hráčem na trhu.

Očekával jste, že se digitální síťové kamery stanou tím, čím jsou dnes?
Zpočátku ne. Ale když jsme začali navštěvovat bezpečnostní veletrhy, uvědomili jsme si, že veškerá naše konkurence je myšlením ještě v minulém století. Všichni využívali analogové technologie. Naši konkurenti si mysleli, že jsme firma s hračkami, která omylem vystavuje na špatném veletrhu. Řekli jsme si, že pokud budeme dělat to, v čem jsme dobří, staneme se rychle vedoucím hráčem na trhu. A také se to podařilo. Zajímavé je, že jsem se vždy považoval za technologa. Pak jsem byl zvolen za nejvlivnější osobnost v oblasti bezpečnosti a před dvěma nebo třemi roky jsem si uvědomil, že se nalézám v jiném oboru a jsem v něm navíc docela dobrý.

Proč přecházet z analogové technologie na digitální?
Je tu mnoho důvodů. Analogové kamery jsou technologií ze čtyřicátých let minulého století. Myslím, že je čas na upgrade. Dnes, když se díváte na video s rodinou, díváte se na HD formáty. Skutečným důvodem pro přechod je tedy možnost využívat HD video a ten je podpořen tím, že se ještě docela hodně ušetří za instalaci. Analogové video je totiž stále výdělečné právě díky tomu, že jeho instalace je nákladná. Když se zabýváte instalací kabelů, budete svým zákazníkům samozřejmě stále doporučovat analogové video, i když jde o již překonanou technologii.

Jaké podmínky musí vlastně dnes splňovat nahrávka, aby mohla být použita například proti někomu u soudu?
Na tuto otázku je velmi obtížné odpovědět. Když jdete k soudu s videem, zřídkakdy je na něm tvář té osoby. U soudu je většinou mnoho jiných důkazů a svědků, kteří dosvědčují, že tam byl dotyčný přítomen. V praxi hledáme většinou něco jiného než tvář, na videu lze snadno rozpoznat například to, že někdo přišel s prázdnou taškou a odešel s plnou.

Jak důležité tedy rozlišení skutečně je?
Záleží hlavně na kvalitě obrazu, na světle a stínu, a ne jen na rozlišení. Kamera musí být schopna si poradit s různými světelnými podmínkami. Když mě například vyfotografujete se sluncem za zády, nebude toho na té fotografii ze mě moc vidět. Stejně se to má s kamerami.

Jaké jsou dnes dominantní technické trendy v IP kamerách?
Důležité je hlavně to, jak si kamery poradí s různými světelnými podmínkami. Trendem je vyšší kapacita pamětí a výkon procesorů. Dále vysoké rozlišení v podobě 4K. Vysoká kvalita detailu dává pocit 3D obrazu. Je to úžasná záležitost, protože obraz má vysoké rozlišení z jakéhokoliv úhlu pohledu.

Máte nějaký názor na „bezpečnost jako službu" v byznysu s kamerami?
Je to trend, který se v České republice poměrně slibně rozvíjí. V mnoha zemích existuje zákon o verifikaci videa, než jej pošlete na policii. Nejlepší způsob, jak dělat video verifikaci, je nainstalovat online kamerový systém. Ve všech zemích, kde je dobré připojení na internet a rozvíjejí se cloudová řešení, tedy včetně ČR je tento segment na vzestupu.

Můžete nám říci něco o možnostech inteligentního rozpoznávání?
Naše kamery mají zabudované inteligentní funkce např. počítání osob a identifikaci pohybu. Společně s aplikacemi partnerů využívajících naší otevřené platformy ACAP jsou dostupná programová řešení pro identifikaci obličejů a pohlaví za určitých podmínek. Vzhledem k rostoucímu počtu aplikaci jde rozhodně o trend, který se stále vyvijí k dokonalejším řešením.

Co si myslíte o budoucnosti IP kamer?
Obrovský trend bude v nejbližší době 4K video. Bude ale trvat ještě dlouho, než se stane opravdovým standardem. Další trend, který vidím, je tzv. „edge storage" (vlastní paměťové úložiště v kameře). Úložná kapacita roste neuvěřitelným tempem, ale ještě rychleji rostou požadavky na ukládání dat z videozáznamů. Mohu s klidem říci, že 64 GB úložné kapacity přímo v kameře je standardem již dnes. Na konci letošního roku to bude až 128 GB. Na 128 GB dnes můžete uložit celý týden záznamu.

Je dnes trendem také využití dalších senzorů?
Ano, pokud máte komplexní integrovaný systém, není tam jen videodohled, ale různé další zabezpečovací elementy. Jde spíše o systémový trend než o směr přímo v oblasti kamer. Tím je integrace mezi kamerami a kontrolou přístupu.

A co například mikrofony?
Skoro všechny naše kamery mají podporu pro mikrofony a audio. Běžně se ovšem mikrofony na veřejných místech k záznamu mluveného slova nepoužívají (důvod je legislativní), lze je ovšem s úspěchem využít například při detekci incidentů – kamera zvukově vyhodnotí přijíždějící vlaku, nebo třeba výstřel. Například na nádraží je každému jedno, když ho nahrají na kameru, ale když nahrají to, co říká, to už je jiná věc. Audio zařízení by navíc šlo využít i na různá

oznámení, např. na nádraží upozornit jen osoby na pátém nástupišti, že se blíží vlak a že mají ustoupit. Dochází k neustálé integraci. Ve Spojených státech jsme uvedli vlastní řešení pro kontrolu vstupu, v Evropě jsme to ještě oficiálně neoznámili, ale není to žádným tajemstvím.

Jak dlouho trvá vývoj nové kamery?
Pokud jde pouze o novou generaci již existujícího produktu, trvá cyklus půl roku až rok. Ale pokud jde o vývoj zcela nového produktu, zcela nové technologie, jako je například naše kamera pro snímání ve tmě, je potřeba počítat na vývoj přibližně se třemi roky a třemi tisíci testů.

V oblasti IP kamer je dnes poměrně velká konkurence. Jaký je váš názor na agresivní asijské společnosti, jako je třeba Huawei?
Jsme jednoznačně největším hráčem. Všichni vyrábějí v Asii nebo Mexiku, výrobní náklady jsou tedy pro všechny přibližně stejné. My máme dokonce určitou výhodu, protože vyrábíme ve větším množství. Nabízíme však především nejlepší služby, technickou podporu a nejvyšší kvalitu. Když si má zákazník vybrat mezi dvěma produkty, samozřejmě zvolí raději ten od jedničky na trhu, což nám umožňuje nastavit ceny výš než konkurence. ■

Karel Wolf

NEWSLETTER

ASOCIACE TECHNICKÝCH BEZPEČNOSTNÍCH SLUŽEB GRÉMIUM ALARM

Vážení čtenáři,

tématem mého dnešního zamyšlení je sport a bezpečnost. Sport sám o sobě je činnost prospěšná pro lidské tělo. Aby však šlo sport provozovat na nejvyšší úrovni, musí k tomu být vytvořeny bezpečné podmínky. Bezesporu jste všichni zaznamenali obrovský boom v oblasti profesionálních (bezpečnostních) i webových kamer (domácí PC). Ještě před pár lety byl na světovém trhu CCTV poměr analogových kamer vs. IP kamer zhruba 8 : 2 ve prospěch analogových systémů. Nyní se skóre začíná vyrovnávat a momentální proporcionální rozdělení trhu je podle odhadu odborníků zhruba 6 : 4. Čili lze hovořit o totálním nástupu IP kamer. Tyto bezpečností kamerové technologie budou v obrovském množství nasazeny a využity, aby od příštího měsíce zajišťovaly bezpečnost návštěvníků a sportovců na stadionech, sportovních kolbištích, v hotelech či na ulicích ve všech velkých městech Brazílie, kde se bude konat fotbalové FIFA MS 2014. Vedle olympijských her je to největší oslava sportu a nejsledovanější sportovní událost roku. Potřeba zajištění globální bezpečnosti však již plně pronikla i do sportovního světa. Bezpečnostní otázky jsou v Brazílii ze známých důvodů na denním pořádku a je to velmi choulostivé téma. Organizátoři se spoléhají na to, že kamerová technika jim pomůže předejít mnoha kriminálním činům nebo je pomůže vyřešit. Již několik let zvažuje Mezinárodní fotbalová asociace FIFA nasazení tzv. „GLT" technologie (Goal Line Technology), což je speciální systém, který dokáže detailně rozpoznat, zda hráč vstřelil regulérní gól či ne (resp. dokáže rozpoznat, zda míč přešel přes brankovou čáru či nikoliv). Jde o podobnou technologii, kterou známe z tenisu pod názvem Hawk-Eye (jestřábí oko). Pochopitelně i tato technologie je založená na vysoce kvalitní profesionální kamerové technice a přední světoví výrobci CCTV se perou o to, kdo podepíše s FIFA lukrativní kontrakt. Ani zde se sport neobejde bez přítomnosti kamerové techniky.

S blížícím se létem vám přeji spoustu skvělých sportovních zážitků ať již doma, či v zahraničí a hlavně bezpečí a klid, který by si tolik přáli lidé na Ukrajině. Kamerové systémy (i když je vlastně nemáme příliš rádi) jsou tu především od toho, aby nám zajišťovaly jakousi minimální bezpečnost. Přeji vám bezpečné fotbalové léto a vězte, že nejbezpečněji bude doma, v pohodě u televizních obrazovek a v kruhu rodinném.

Václav Levíček, viceprezident AGA

Z činnosti AGA

více na www.gremiumalarm.cz

Vznik Sekce komerční bezpečnosti Hospodářské komory ČR

Představenstvo Hospodářské komory ČR na svém zasedání dne 16. 4. 2014 schválilo vznik Sekce komerční bezpečnosti Hospodářské komory České republiky. Sekce komerční bezpečnosti je poradním, iniciativním, koncepčním a koordinačním orgánem Představenstva HK ČR pro podnikatelskou činnost v oblastní komerční bezpečnosti.
Sekce se při výkonu své činnosti zaměří na záležitosti, jež vyplývají ze zájmů a potřeb členů HK ČR v oblasti soukromých bezpečnostních služeb. Bude to především právní úprava oboru, zvyšování profesionality poskytovaných služeb, vzdělávání v oboru i aktivní působení na zlepšení vztahu občanské veřejnosti k oboru soukromých bezpečnostních služeb.
Tuto činnost již po dobu tří let zčásti zajišťovala Rada soukromých bezpečnostních služeb HK ČR, kterou tehdy vytvořilo šest začleněných živnostenských společenstev HK ČR. Vzniklá Sekce komerční bezpečnosti HK ČR je povýšením této činnosti do oficiální podoby v souladu se Statutem HK ČR.
Předsedou Sekce komerční bezpečnosti HK ČR byl jmenován Ing. Václav Nepraš.

Fakulta aplikované informatiky UTB Zlín

Dne 19. 3. 2014 se uskutečnilo zasedání Vědecké rady Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně. Slavnostního zasedání Vědecké rady se zúčastnil i prezident asociace Ing. Václav Nepraš, člen vědecké rady, který při jednání s představiteli FAI dohodl, že spolupráce FAI UTB Zlín a AGA bude i nadále úspěšně pokračovat.
V souvislosti s ukončením druhého funkčního období děkana Fakulty aplikované informatiky UTB ve Zlíně skončil v této funkci prof. Ing. Vladimír Vašek, CSc. Rektor UTB, prof. Sáha, poděkoval odstupujícímu děkanu prof. Vladimírovi Vaškovi za jeho dvě funkční období, kdy dokázal rozvinout fakultu, kterou předtím jako ředitel Institutu řízení a procesů aplikované informatiky založil. Do funkce nového děkana FAI UTB Zlín byl senátem jednomyslně zvolen doc. Mgr. Milan Adámek, Ph.D.

České technické normy – informace

Na nových stránkách UNMZ je k dispozici seznam platných ČSN s jejich krátkou anotací. Normy na zabezpečovací techniku začínaly tradičně čísly 5013x-x, to bohužel již od letošního roku neplatí, do soustavy ČSN EN jsou totiž nově přejímány normy IEC pro přístupové a kamerové systémy. Vyhledávat podle slov v názvu v podstatě také nejde, rozptyl slov je příliš velký. Jediný způsob, jak v seznamu najít normu, kterou neumíme úplně přesně identifikovat, je pomocí zadání třídícího znaku 3345 – Elektrická řídící zařízení. Poté se nám zobrazí seznam 62 norem na zabezpečovací zařízení, kamerové systémy, přístupové systémy, dohledová centra atd.
Za poplatek 1 000 Kč na rok si na webu úřadu můžete koupit ČSN ON LINE s možností zobrazení textu všech norem. Při poplatku 3 500 Kč ročně si tyto normy můžete i tisknout (více na www.unmz.cz/urad/csn-on-line). Produkt nabízí i zrušené normy a můžete si tedy například vytisknout i ČSN 334590.

ASOCIACE TECHNICKÝCH BEZPEČNOSTNÍCH SLUŽEB GRÉMIUM ALARM, O.S.
profesionální sdružení firem a subjektů z oboru technických bezpečnostních služeb
- Autorizované živnostenské společenstvo Hospodářské komory ČR
- Člen evropkého sdružení EURALARM a evropského bezpečnostního klubu ESBOC
- Centrum technické normalizace pro bezpečnostní služby při AGA

Freyova 27/82, 190 00 Praha 9
Tel.: (+420) 266 721 831
GSM: (+420) 602 403 939
e-mail: info@gremiumalarm.cz
www.gremiumalarm.cz

ODBORNÁ KOMISE AGA MECHANICKÉ ZÁBRANY DOPORUČUJE

Naše Asociace technických bezpečnostních služeb Grémium Alarm, o. s., se jako profesní sdružení firem se zaměřením na technické služby k ochraně osob a majetku při své činnosti zabývá i mechanickými zábrannými systémy. Tuto oblast má v gesci komise pro mechanické zábrany. Z členské základny se přímo k činnosti v této oblasti hlásí cca 20 firem. Osobně se domnívám, že je to více než 75 % členů. Vždyť u každé společnosti, ostatně jako u každého z nás, dojde v běžném životě např. ke ztrátě klíče (a pak je nutno vyměnit profilovou cylindrickou vložku – tzv. FABku) či k poruše funkce zadlabacího zámku (a ten je nutno také vyměnit). Pravděpodobně si většina z nás tento jednoduchý úkon provede sama a nevolá hned zámečníka. Proto jako odborná komise přinášíme několik rad jak na to, respektive čeho se vyvarovat:

JAK TO NEMÁ BÝT:

Jedním z nejjednodušších způsobů překonání dveří je rozlomení profilové cylindrické vložky a otevření zámku šroubovákem. K rozlomení lze použít běžné nářadí, SIKA kleště, maticové klíče, hasák atd. K odemčení dveří pak stačí obyčejný šroubovák. Tomuto způsobu má zabránit bezpečnostní štít – kování, které znemožní nasazení nářadí na tělo cylindrické vložky. Pokud lze jednoduše dveřní štít demontovat/odšroubovat, je to špatně. ČSN EN 1906 požaduje, aby bezpečnostní dveřní kování mělo minimálně dva připevňovací prvky a kování nebylo možné z vnější strany dveří demontovat.

Obecně se má za to, že pokud cylindrická vložka nepřesahuje přes vnější štít bezpečnostního kování o víc než 3 mm, nelze ji ukroutit a rozlomit – pokud přesahuje více, je to opět špatně. V praxi se však ukazuje, že to platí pouze při rozlomení cylindrické vložky běžným nářadím (viz shora). Dnes však již specialisté používají takové nástroje (rozlamovač kombinovaný s vytrhovačem), které si poradí i s takovým zámkem. Proto lze jen doporučit, aby čelo cylindrické vložky lícovalo s vnější stranou bezpečnostního štítu.

CO LZE DOPORUČIT:

Běžné bytové dveře jsou vyráběny v protipožárním provedení. Na ně lze připevnit bezpečnostní kování spolu s profilovou cylindrickou vložkou v základním bezpečnostním provedení (min. pět stavítek, tvar otvoru pro klíč – zúžený, překrytý). Pro zvýšení odolnosti dveří je žádoucí nakovat na dveře ještě další, tzv. přídavný zámek.

Pokud chceme ochránit cylindrickou vložku proti vytržení či odvrtání, můžeme použít bezpečnostní kování s překrytím nebo použít cylindrickou vložku se zvýšenou odolností proti odvrtání a vytržení.

Při zvyšování odolnosti dveří nesmíme zapomenout též na pantovou/závěsovou stranu. Je třeba ji opatřit zábranami proti vysazení – například pevnými čepy nebo třmeny.

Takto nakované dveřní křídlo lze považovat za zajištěné proti překonání na minimální bezpečnostní úrovni.

Další informace lze nalézt v průlomových normách ČSN EN 1627 až ČSN EN 1630 a výrobkových normách ČSN EN 1303 – cylindrické vložky, ČSN EN 1906 – dveřní štíty, ČSN EN 12209 – zadlabací zámky.

za odbornou komisi
AGA Mechanické zábrany
Ing. Petr Koktan, člen prezidia AGA

FYZICKÉ ZABEZPEČENÍ DATOVÝCH CENTER

Objem dat v korporátních a kolokačních datacentrech meziročně geometricky roste. Společnost Cisco odhaduje, že příchozí a uložená data v datových sálech po celém světě zabírají již 3 ZB (zetabyte) a do roku 2017 to bude minimálně třikrát tolik. To je již dost veliké množství citlivých informací, které vyžadují adekvátní zabezpečení. Dostává se jim ho ale?

Karel Wolf

Datacentra dnes mají nejen na starosti více dat, ale také spravují řádově více infrastruktury, než tomu bylo ještě před čtyřmi nebo pěti lety. Nové technologie slučují servery, konstrukci a bezpečnost v celých infrastrukturách ať už místních, nebo cloudových. Rostoucí objem dat a konvergence výpočetní techniky mají ten důsledek, že datová centra doslova praskají ve švech. IT společnosti, které datová centra provozují, tráví mnoho času zabezpečováním těchto přeplněných center proti síťovým útokům. Ne nadarmo – existují celé hackerské komunity (v případě Asie dokonce i celé polostátní firmy), které útočí právě na síťovou bezpečnost datových center. Jak je na tom ale fyzická bezpečnost?

ACH, TA LIDSKÁ POVAHA

Je to zajímavý paradox, ale fyzické zabezpečení mnoha administrátorům datových center nepřipadá až tak důležité. Správci často uvažují například takto: „Když je korporátní datové centrum umístěné hluboko uvnitř kancelářské budovy, je velmi nepravděpodobné, že se zde objeví tým zločinců usilující o extrakci dat," nebo: „Koho by ty modře blikající černé bedny zajímaly?" Datová centra přesto fyzicky ohrožena jsou, a to jak ta velká – kolokační, tak i ta zdánlivě méně významná, firemní. Fyzický útok je snadno proveditelný, vydává-li se někdo za uklízečku nebo za počítačového technika. Chyby a zlé úmysly zaměstnanců jsou rovněž časté a škodu mohou způsobit také.

BEZPEČNOSTNÍ MINIMUM

Možná nepracujete s daty, která mohou ohrozit bezpečnost státu, ale informace z byznysu, obzvláště osobní data zákazníků či technologické know how, jsou často pro život vaší firmy stejně důležité, ne-li důležitější. Ujistit se, že je vaše datové centrum zabezpečeno proti živelným pohromám, energetickým výpadkům, přístupu kohokoli nepovolaného, odposlechům a dalším fyzickým hrozbám, by měl být základ, ne bonusová nadstavba či projev paranoie. Pokud máte alespoň část dat například v cloudu či jinak geograficky diverzifikovanou prostřednictvím velkých datacenter, platí to samé o stavu datacentra vašeho kolokačního partnera. Zde je ostražitost obzvláště na místě, neboť útoky na velká datacentra se budou stupňovat přímo úměrně tomu, jak poroste objem dat v cloudu.

Jednou z cest, jak si ověřit, zda datové centrum vašeho poskytovatele je v regulačním souladu s požadavky na síťovou a fyzickou bezpečnost, jsou příslušné certifikace. Pokud je poskytovatel nepoužívá, je to často samo o sobě určitým signálem, že existuje důvod zpozornět. Pokud váš poskytovatel operuje v Evropě, hledejte zejména certifikaci IRMS DataCenter Certification evropského standardu systémů datových center. Pokud je váš infrastrukturní provider ze Severní Ameriky, měly by vás zajímat certifikace z auditů SSAE-16/SAS 70, FISMA, nebo FEDRAMP (v případě datových center spojených s vládou USA).

JAKÉ SITUACE MOHOU DATACENTRUM FYZICKY OHROZIT?

Fyzická rizika ohrožující datová centra zahrnují velkou škálu možností, na které provozovatelé často ani nepomyslí. Ostatně pro příklady není třeba chodit daleko, stačí vzpomenout na překvapivé vytopení cloudového datacentra BIG Blue One české společnosti Casablanka letos na jaře. Kalamitu tehdy způsobilo prasklé potrubí v kancelářích nad datacentrem.

Většina hrozeb se dá naštěstí alespoň snadno kategorizovat, spadají zpravidla do jedné ze tří velkých skupin – živelné pohromy, fyzické vniknutí a potíže s energií.

Když uvažujeme o fyzických hrozbách ohrožujících datové centrum, naše mysl přirozeně tíhne k tomu představit si dramatickou živelnou pohromu: zemětřesení, tornáda, hurikány, extrémní teploty, přílivové vlny. Datová centra by měla být umístěna co nejdále od oblastí, kde podobné pohromy hrozí. To může vypadat jako samozřejmost, ale ne vždy to tak je, například cloudové datacentrum Microsoftu umístěné v Dublinu bylo v počátcích svého provozu několikrát vyřazeno z provozu bleskem. Projektant přitom mohl s tímto rizikem počítat, neboť divoké bouřky jsou v dané lokalitě poměrně běžné. Na druhé straně to ale neznamená, že musíte své datové centrum vybudovat na druhém konci kontinentu nebo uzavřít smlouvu s poskytovatelem datových služeb v jiné zemi, než žijí vaši IT zaměstnanci. Například americká společnost RagingFire chtěla

Technologie v rámci sálu je možné chránit také dalšími fyzickými bariérami v prostoru. Datové centrum Českých radiokomunikací na Žižkově.

vybudovat datové centrum v blízkosti svých kolokačních zákazníků v oblasti Bay Area. Ta je však pověstná svou seismickou aktivitou. V zájmu bezpečnosti nakonec stačilo datové centrum postavit v nedalekém Sacramentu, které není k zemětřesením tolik náchylné.

Energie

O energii většinou v souvislosti s fyzickými hrozbami ohrožujícími datová centra neuvažujeme. Ale energetické obtíže jsou mnohem častější než živelné pohromy a měli bychom se s nimi naučit počítat. „Část důvodů, proč jsou energetické záležitosti oddělovány od bezpečnosti, spočívá v tom, že korporátní oddělení IT a provozní oddělení nebývají často v souladu, pokud jde o financování energie a starosti s tím spojené. Oddělení IT mají sklon se domnívat, že využití energie není jejich záležitost. Jenže se mýlí: „Když vám selže chlazení, vaše úložiště dat se upečou," říká Ing. Vladimír Houška, Senior Consultant společnosti COMPLETE CZ, která se na výstavbu non-ICT infrastruktury datových center specializuje.

Chlazení

Možná nemáte takové štěstí jako společnost Iron Mountain, jejíž bezpečné zařízení v Pensylvánii je vestavěno do přírodních jeskyní a je chlazeno vodou z podzemního jezera. Moderní technologie mohou však takové prostředí simulovat pomocí chlazené vody, distribuované pod zvýšené podlahy datového centra. Vyšší stropy zase zajistí, že teplý vzduch bude stoupat vzhůru, místo aby se držel okolo vašich přístrojů. Efektivní řešení také skýtají různé modely nepřímého chlazení venkovním vzduchem.

Energetická síť

Pokud své datové centrum vybudujete v blízkosti městské oblasti, kde dochází energie, můžete se s plány na růst rozloučit. To, že jsou nová datová centra budována mimo velká města a jako své zaměstnance využívají příměstskou či venkovskou populaci, má svůj důvod. Příměstské a venkovské komunity využívají nízkých cen elektřiny a pozemků, aby budovatele datových center přilákaly.

Monitorování síťového operačního centra (NOC)

Zřídit monitorovací systém síťového operačního centra a najmout zaměstnance na jeho sledování je základ. Systém by měl zachytit případné požáry (to je zřejmé), monitorovat vlhkost (to už není tak zřejmé), dodávku elektřiny či venkovní a vnitřní teplotu.

Záložní energie 24/7

Když už hovoříme o dodávce elektřiny: ujistěte se, že váš záložní zdroj energie (UPS) správně funguje a bude fungovat dostatečně dlouho v případě oprav, uzavření systému nebo evakuace.

Fyzické vniknutí

Stává se to? Sice ne tak často jako ve špionážních filmech, ale přesto se to stává. Například v Londýně lupiči vnikli do datového centra společnosti Verizon, svázali zaměstnance a ukradli zařízení. Rok předtím došlo ke vloupání do kolokačního centra třetího stupně.

Lze ale opravdu data před zloději spolehlivě ochránit? Martin Petrovka, generální ředitel společnosti COMPLETE CZ, si myslí, že ano: „Za našimi hranicemi se již déle než desetiletí používají k ochraně

ŘEŠENÍ PRO PŘÍMOU FYZICKOU OCHRANU TECHNOLOGIÍ V DATOVÝCH CENTRECH

- Ocelové klece chránící kritické technologie před přímým kontaktem s nepovolaným personálem
- Ocelové opláštění datového sálu
- Kompaktní zabezpečená úložiště dat (datové sejfy, chráněné racky, bezpečné datové komory)

cenných dat unikátní řešení, která český trh doposud opomíjel. Řeč je o takzvaných datových sejfech a chytrých bunkrech španělské společnosti AST Modular," vysvětluje. „Ty existují v podobě od miniaturních datových sejfů s jedním serverem přes zabezpečené datové stojany až po celé datové komory (malé datové sály). Ve všech případech se jedná o opancéřovaná, hermeticky uzavíratelná prostředí, která garantují ochranu technologií před nezvanými návštěvníky, elektromagnetickými vlnami (ze silových kabelů, radaru či blesku), požárem i vytopením," doplňuje.

Kvalitní zámky

Je to prosté, ale v datových centrech na to často nemyslí. Většinu zámků lze snadno odemknout pomocí obyčejné plastové karty. Dobré zámky nejsou zase tak drahé. Investujte do nich, abyste zabezpečili citlivé oblasti vašeho datového centra. nezapomínejte investovat do alarmů.

LIDSKÝ FAKTOR

Jedním z nejsnadnějších způsobů, jak proniknout do datacentra, je tzv. tailgating (svezení se za někým). Jednomu konzultantovi, zabývajícímu se zabezpečením datových center, se podařilo proniknout do síťového operačního centra v přestrojení za prodejce, který nese tác s jídlem. Přestože centrum bylo biometricky chráněné, IT zaměstnanci mu otevřeli dveře. Jiným nezvaným návštěvníkům se do datových center podařilo proniknout prostě tak, že šli těsně za zaměstnanci. Aby působili nenápadně, telefonovali mobilním telefonem nebo šli o berlích a zaměstnanci jim zabezpečené dveře ochotně otevřeli.

Lze se efektivně bránit? Ano, stačí dodržet následující čtyři pravidla kontroly fyzického přístupu:

- **Zajistěte kontrolu zaměstnanců:** Nejsnadnější způsob, jak získat přístup do datového centra, je přes jeho zaměstnance. Už při jejich výběru byste měli dbát na bezpečnostní kontrolu a následně ji alespoň jednou za rok opakovat. Ještě lepší je provádět kontroly častěji, a to obzvláště v případě kolokačních datových center, která shromažďují velké množství dat o zákaznících.

- **Zpevněte stěny a okna:** Silné zdi ochrání volně stojící datové centrum před fyzickým útokem i před mnoha živelnými pohromami. Silné zdi společně s dvojitými vstupními bezpečnostními dveřmi a neprůstřelnými okny vaše DC ochrání ještě lépe.

- **Zabezpečte vstup pomocí elektronických systémů kontroly přístupu (ACS):** Biometricky chráněné vstupy se v citlivých datových centrech objevují čím dál častěji. Tyto systémy zahrnují čtečky dlaní a otisků prstů či senzory k rozpoznání duhovky, které známe ze špionážních filmů. Další stupeň tvoří dvoufaktorové identifikační karty a hesla. Škálu doplňují jednoduché vstupní karty.

- **Sledování a bezpečnostní týmy 24/7:** Vysoce bezpečná zařízení investují do vnitřních i vnějších digitálních bezpečnostních kamer. Nešetřete však a nekupujte obyčejné fixní kamery. Zloděje, kteří vědí, co dělají, fixní kamery nezachytí. Náklonné digitální kamery se zoomem jsou v tomto ohledu mnohem lepší volba.

Chraňte kritické technologie zabezpečenými skříněmi, nebo je alespoň oddělte klecemi. Přídavné zabezpečovací vrstvy zahrnují bariéry proti nárazu, ochranu okolí a udržování vegetace, pasti (jako přetlakové komory), klece na citlivá zařízení a vypracované strategie pro případ ohrožení.

CO ŘÍCI ZÁVĚREM?

Společnosti utrácejí miliony (eur, dolarů i korun) za síťovou bezpečnost. Ale když vaše datové centrum napadne útočník, je zničeno živelnou pohromou nebo výpadkem proudu, k čemu pak všechny ty investice byly? Nenechávejte dveře svého datového centra otevřené dokořán pro nezvané hosty. Ujistěte se, že tak nečiní ani váš poskytovatel datových služeb. ■

Zabezpečený ICT stojan společnosti AST Modular.

OCHRANA DATOVÝCH CENTER OD SPOLEČNOSTI SIEMENS

PLYNOVÉ STABILNÍ HASICÍ ZAŘÍZENÍ (GHZ) – AKTIVNÍ OCHRANA

Po celém světě neustále zpracovávají data desítky milionů serverů. Není divu, že datová centra jsou vystavena mimořádně velkému nebezpečí vzniku požáru v důsledku přítomnosti dvou rizikových faktorů – elektrické energie (možná inicializace požáru) a velkého množství hořlavého materiálu (plastové díly, složitá kabeláž, plošné spoje).

Důležitým parametrem zabezpečení datového centra je proto bezesporu vhodný a kvalitní hasební systém. Chráněná technologie, tj. servery, vyžaduje velice citlivý přístup. Použitím nevhodného hasebního systému na vodní bázi (vodní hašení), může dojít k sekundárním škodám, které mohou být ve výsledku horší než samotný požár. Oproti tomu plynový hasicí systém zajistí maximální možnou ochranu bez následků.

Společnost Siemens nabízí ucelené řešení zabezpečení datových center včetně hasební technologie. Pro menší datová centra (do 250 m^3) je z ekonomického hlediska vhodné použití systémů Sinorix 1230. Tento typ plynového GHZ využívá pro hašení tzv. chemický plyn Novec 1230, který je během 10 sekund vypuštěn do chráněného prostoru.

Větší datová centra (nad 250 m^3) je vhodné chránit pomocí hasební technologie Sinorix CDT N_2. Jedná se o speciální hasební systém využívající jako hasivo velmi levného dusíku, který do 60 sekund vytvoří požadovanou hasební atmosféru. Účinky samotného dusíku jsou pro lidský organismus zanedbatelné, avšak aplikací tohoto hasiva do chráněného prostoru dojde ke snížení koncentrace kyslíku s potenciálním vlivem na lidský organizmus. I přesto zůstává množství kyslíku v bezpečných tolerancích, které jsou dané normovou řadou ČSN EN 15 004. Využívání hašení pomocí čistého dusíku

PŘÍKLAD POUŽITÍ U MÍSTNOSTI V PODZEMNÍM PODLAŽÍ

1 Detekce požáru a ovládací ústředna hašení
2 Kouřový bodový hlásič
3 Kouřový nasávací hlásič
4 Kombinovaný zvukový a světelný alarm
5 Kombinovaný zvukový a světelný alarm
6 Tlakové lahve s hasebním plynem
7 Potrubní síť s tryskami
8 Odvod přetlaku a odvětrání

je známé a používané již dlouhá desetiletí. Hasební systém Sinorix CDT N_2 přináší naprosto nový prvek – technologii řízeného vypouštění (Constant Discharge Technology).

Klasická technologie plynového hašení je založena na okamžitém vypuštění hasebního plynu. To znamená, že všechny tlakové lahve s hasebním plynem jsou otevřeny najednou, a to do maximálního možného průtoku hasiva. Výsledkem je vznik tlakové špičky v potrubním systému a následně i v chráněném prostoru, odkud je nutné odvést vzniklý tlak pomocí přetlakové klapky. Potrubní systém musí být proto dimenzován tak, aby umožnil přenos prvotní „tlakové vlny". Již po několika sekundách se potrubí stává silně předimenzované s ohledem na klesající množství hasiva v tlakových lahvích.

Společnost Siemens analyzovala tyto skryté rezervy a vyvinula technologii řízeného vypouštění hasebního plynu. Pomocí speciálního ventilu na tlakové lahvi je hasební plyn konstantně dávkován do chráněného prostoru. Ventil automaticky a bezpečně zajistí vypuštění hasebního plynu tak, že je možné zredukovat velikost přetlakových klapek až o 70 % v porovnání s klasickou technologií plynového hašení. Díky průběžnému vypouštění plynu lze výrazně zredukovat průměry potrubí tak, aby bylo maximálně využité po celou dobu vypouštění. Pro zákazníka to znamená instalaci menší přetlakové klapky a nižší pořizovací cenu celého systému plynového hašení.

Společnost Siemens provedla celou řadu testů, které odhalily, že v průběhu vypouštění hasiva dochází ke generování velmi intenzivního hluku (až 125dB) ovlivňujícího správný chod serverů. Harddisky (HDD) vystavené této hlukové zátěži pak mají problémy se čtením nebo zápisem dat a může dojít i k jejich automatickému vypnutí (ochrana proti poškození).
Na základě velkého množství měření a zkoušek Siemens vyvinul speciální trysku s označením Sinorix Silent Nozzle, která v kombinaci s technologií Sinorix CDT N_2 dokáže upravit frekvenci a snížit intenzitu hluku pod 100 dB. Bylo zjištěno, že při této hodnotě je ovlivnění funkce HDD téměř nulové.

Při budování datového centra je nutné pamatovat i na umístění tlakových lahví. V případě menších systémů je výhodnější umístit tlakové lahve přímo v chráněném prostoru. U velkých datových center je většinou nutné vybudovat samostatné místnosti vyhrazené pouze pro tlakové lahve GHZ. Přesné podmínky pro umisťování tlakových lahví jsou řešeny v rámci ČSN 07 8304.

Technologie Sinorix CDT N_2 v kombinaci s tryskami Sinorix Silent Nozzle přináší nové možnosti pro komplexní a přitom ekonomicky výhodnou ochranu nejdůležitějších technologií. ■

Ing. Miloš Průha, Siemens, s.r.o.

ZABEZPEČENÍ VLASTNÍ FIREMNÍ INFRASTRUKTURY

„Dělat stejné věci stále stejně a očekávat jiný výsledek, to hraničí s duševní poruchou," uvedl jednou Albert Einstein. Útočník potřebuje najít nejslabší článek, aby mohl získat přístup a ukrást data. Proto je zapotřebí firemní infrastrukturu lépe chránit.

Eugene Kaspersky, zakladatel a majitel ruské antivirové společnosti Kaspersky Lab, na konferenci v Praze před zákazníky s úsměvem řekl: „Vše již bylo alespoň jednou ukradeno, pouze to čeká na svého kupce." On sám s tím má své zkušenosti, před pár lety mu dokonce unesli syna.

Ohledně IT prostředí platí, že ohrožen je dnes každý, včetně malých podniků, roboty hackerů si nevybírají. Dnešní (podnikový) uživatel je mobilní, je v cloudu, kvůli tomu je mnohem více ohrožený než „standalone" (osamocený) uživatel. Tento stav se týká každého jednotlivce i organizace, zvláště když vezmeme v úvahu horké téma poslední doby – BYOD (Bring Your Own Device).

TŘETÍ GENERACE IT

Kolem roku 2000 byl k internetu připojen zhruba milion počítačů. Podle analytické společnosti IDC už v roce 2012 došlo k vítězství mobilních zařízení; dnes už jich je připojeno několik miliard. V současné době hovoříme o tzv. třetí generaci IT, také o cloudu, o totální decentralizaci s centrální správou, což znamená opětovnou konsolidaci a zjednodušení (jak pro koho). Nástup cloudu umožnila virtualizace, která znamená provozování téměř libovolného operačního systému a vyšší bezpečnost běhu aplikací díky chráněnému prostředí, avšak zároveň neprůhlednost infrastruktury a vyšší nároky na správu IT.

LIDSKÝ FAKTOR

Podle jednoho průzkumu, který těsně před rokem 2000 uvedla tehdy ještě počítače vyrábějící společnost Siemens, mohli lidé za 95 % úniků informací.

Dnes mohou za zhruba 90 % úniků, což nekoreluje ani s počtem koncových zařízení ani s počtem zařízení připojených k internetu. Lidé jsou prostě určujícím faktorem a způsobují úniky buď z neznalosti, nebo úmyslně.

Podle všech expertů z toho vychází jednoduchý bezpečnostní vzorec: lidé, procesy, technologie. Takto by měl vypadat stupňovitý přístup k zajištění bezpečnosti firemních informací. Lepší či horší bezpečnostní „krabičku" totiž může organizaci, která se chce ochránit, prodat každý, avšak už málokdo je schopen zajistit její správné nasazení v infrastruktuře. V ní jsou lidé a jejich chování obtížně popsatelnou proměnnou, kterou lze řídit jedině nasazením procesů, a ty je nutné důsledně aplikovat a měřit. Až nakonec nastupují (bezpečnostní) technologie, jež tyto procesy podporují.

Zejména menší firmy (SMB – Small and Medium Business) si neuvědomují, že i ony jsou ohroženy. Například prostřednictvím firemní komunikace může dojít k napadení jejich velkého zákazníka – zfalšovaným pdf s objednávkou/nabídkou od úklidové firmy nebo výrobce gumiček do stěračů lze proniknout až do nechráněné komunikace přes firewall. Pokud není firemní ochrana vícevrstevná, jde to relativně snadno.

PROCESY

Pro zajištění podnikové bezpečnosti je třeba definovat strategii jako kontinuální proces, aby byla eliminována rizika popsaná výše.

Součástí strategie bezpečnostní politiky má být i prevence v podobě školení uživatelů, které musí být srozumitelné a jednoduché, logické, se zdůvodněním a uvedením příkladů ohrožení. Hesla by neměla být příliš jednoduchá. Obvykle se vyskytují hesla typu 1111, 1234, 0000, jméno syna, psa či jiného domácího miláčka … a takovéto slabé a odhadnutelné kódy se obvykle nevyplácejí. Pokud uživatel nafasuje firemní notebook, měl by vědět, že jej doma nemá půjčovat dětem na projíždění sociálních sítí. Školení o bezpečnosti by měla být navíc pravidelná. Ne všichni lidé jsou v IT odborníci a ten, kdo se umí hbitě pohybovat po internetu, nemusí ani vědět, jaký je rozdíl mezi MS Office a Windows. Podle průzkumu to neví osm z deseti běžných uživatelů.

Nejde však jen o ně. I tzv. odborníci, kteří ještě nedávno vedli svatou válku proti Microsoft Windows a oháněli se „neprůstřelným" za Linuxem a komerčními unixy, jsou dnes schopni bez uzardění provádět dálkovou správu z laciného čínského tabletu s tím nejnebezpečnějším operačním systémem – Androidem.

Při sestavování strategie a popisu bezpečnostních procesů je dobré dbát i na tzv. penetrační testy. Ty nemusejí být jen technologické, ale i fyzické. Ve velké firmě nevyvolá podezření například dobře vypadající (cizí) dáma, která projde kancelářemi; tu něco vezme (dokument, CD-ROM, flashdisk), tu něco přidá (totéž), nebo se na chvíli posadí k neodhlášené stanici.

BEZPEČNOSTNÍ TECHNOLOGIE

Komplexní bezpečnostní IT architektura podniku musí být vícevrstevná, technologie by měly mít centrální správu s jednoduchým přehledným ovládáním na centrální konzoli.

„Velký" podnikový bezpečnostní software má mít také jednotnou správu (ze serveru). Pro ochranu podnikových stanic by se neměly používat antimalwarové softwary „zadarmo", které nedosahují funkčnosti placených verzí (samozřejmě včetně absence dálkové správy, protože nejde o serverové řešení).

Pro bezpečnější přístup lze hesla posílit dvoufaktorovou autentizací, případně lze zablokovat USB porty.

Ochranné systémy pro nasazení v podniku – firewally, antispamové filtry, IDS/IPS (Intrusion Detection/Prevention System) apod., by měly běžet na originálním hardwaru, protože dodavatelé je mají se svým hardwarem dobře sladěny.

Ukázkou chybějící vícevrstevné ochrany může být spuštění viru Stuxnet, který před časem na pár let prakticky zlikvidoval íránský jaderný program. Uživatelé si bezstarostně zasunuli do USB portů Stuxnetem zavirované flashdisky, které jim kdosi hodil přes plot (neproškolený lidský faktor). Navíc nebyly chráněny koncové stanice (nepřítomnost technologie – antiviru, případně nepřítomnost bezpečnostní politiky – nezablokování USB portů na PC).

Kvůli nepřítomnosti filtrace příchozí pošty zase třeba nedojde k prověření podezřelého pdf ani k jeho odpojení do chráněné zóny – tzv. sandboxu, virtuálního prostoru v paměti, kde se dá bezpečně spustit a prověřit.

BEZPEČNOST NAKONEC

Ani odpojení koncových stanic a práce off-line nemusí znamenat 100% ochranu. Je znám případ technologické firmy podnikající mimo IT, která po několika cílených útocích svoje stanice odpojila, ale o data přesto nakonec přišla. Útočníci se do jejích prostor probourali násilím přes mříže a dveře a notebooky ukradli. I na to však existuje ochrana – šifrování dat už při zápisu na disk a vzdálená záloha mimo objekt. ■

Richard Voigts

HLEDÁNÍ PRAVDY JE NĚKDY ZDÁNLIVĚ NEKONEČNÉ

Jsme pouze lidé, se svými starostmi, problémy, neřestmi, tajemstvími, obavami.
Jsme také takoví, že chceme vědět víc, než je možné.
Jsme často zmítáni pochybnostmi a hledáme pravdu i řešení.
Nutí nás to snít o tom, jaké by to bylo, mít moc být neviditelný a vědět vše, vidět a slyšet, co potřebujeme.

Odposlech zaznamená vždy pravdu. Je pak jen na lidech, co s tím udělají.

JASNO PANÍ DOMINIKY

Dohady jsou hrozné, mučivé, noci probděné, myšlenky krouží kolem jednoho jediného – je to touha po zjištění skutečného stavu věci. Touha po zjištění PRAVDY. A je celkem jedno, zda pravdu hledáme v soukromém, nebo pracovním životě.

Tak nějak by mohl začít příběh paní Dominiky a jejího vnitřního trápení, které zdánlivě nebralo konce. Lže mi, anebo ne? Ve světě dospělých je to někdy jako v pohádkách, leč konce často pohádkové nebývají a dobro dostane pořádně na frak. Vysněný princ na bílém koni se leckdy změní v bídáka, ale to se na začátku nepozná. Naopak z krásné a milé princezny se často vyklube hnusná saň, která tvrdě sleduje své ekonomické cíle a jde přes mrtvoly. Tušení, intuice, mrazení v zádech a ty šílené dohady nás dohánějí téměř k zbláznění. Co s tím? Rozhodnutí paní Dominiky bylo jednoduché. Bohužel jí přineslo hodně slz, ale také tolik potřebné jasno.

Jednoho dne si po velkém a dlouhém čekání vyzvedla malou nenápadnou krabičku (můžeme již nyní prozradit, že se jednalo o citlivý odposlech s dlouhodobým záznamem do vlastní paměti), která jí „náhodou" vypadla před více jak týdnem z kabelky, a zapadla rovnou pod sedací soupravu v obýváku jejího milovaného prince. Někdo by snad mohl namítat, že ji tam určitě dala schválně, aby se, hnána touhou po zjištění skutečného stavu věci, dozvěděla vše potřebné. Co jí buď otevře oči, nebo potvrdí její oprávněnou zamilovanost. Ta krabička

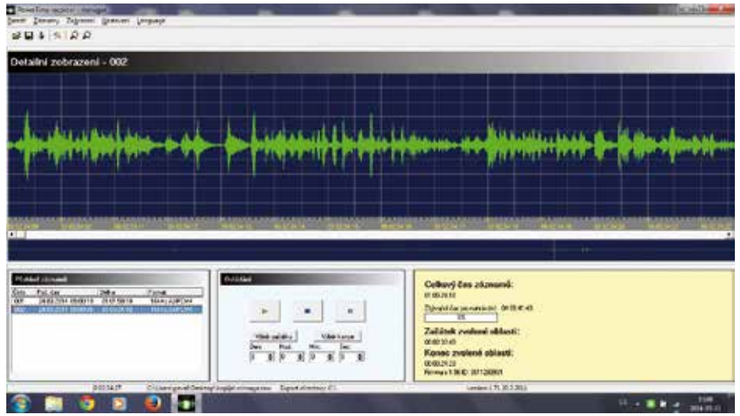
– vlastně nyní „černá skříňka života prince (bídáka) Kamila" se záznamem jeho osudových dní – spolehlivě nahrála stovky hodin odposlechu z celého bytu.

Tedy téměř dvanáct dní plných různých zvuků, událostí a zajímavých hovorů, které zůstaly uloženy ve velké paměti. Tento odposlech se mimochodem jmenuje Mikrodiktafon „AGENT 12D", protože umí nahrávat non-stop dvanáct dní.

Přichází rozhodující chvíle, plná napětí. Chvíle, kdy se otevře cesta k tolik

Použité zařízení „AGENT 12D"

Rozměry:	19x19x33mm
Baterie:	4x 1,5V ZA675 nebo PR44
Výdrž:	300 hodin
Max. čas záznamu:	26 000 min (přes 18 dní s 4GB katrou)
Záznamové médium:	Micro SDHC karta (Class 6 a lepší)
Odstup signál/šum:	65 dB
Záznam:	16bitový nekomprimovaný, 4 a 2bitový ADPCM (22/16/11,025/8/5.5 kHz)
Dosah mikrofonu:	8–10 m
Hlasová aktivace, AGC	



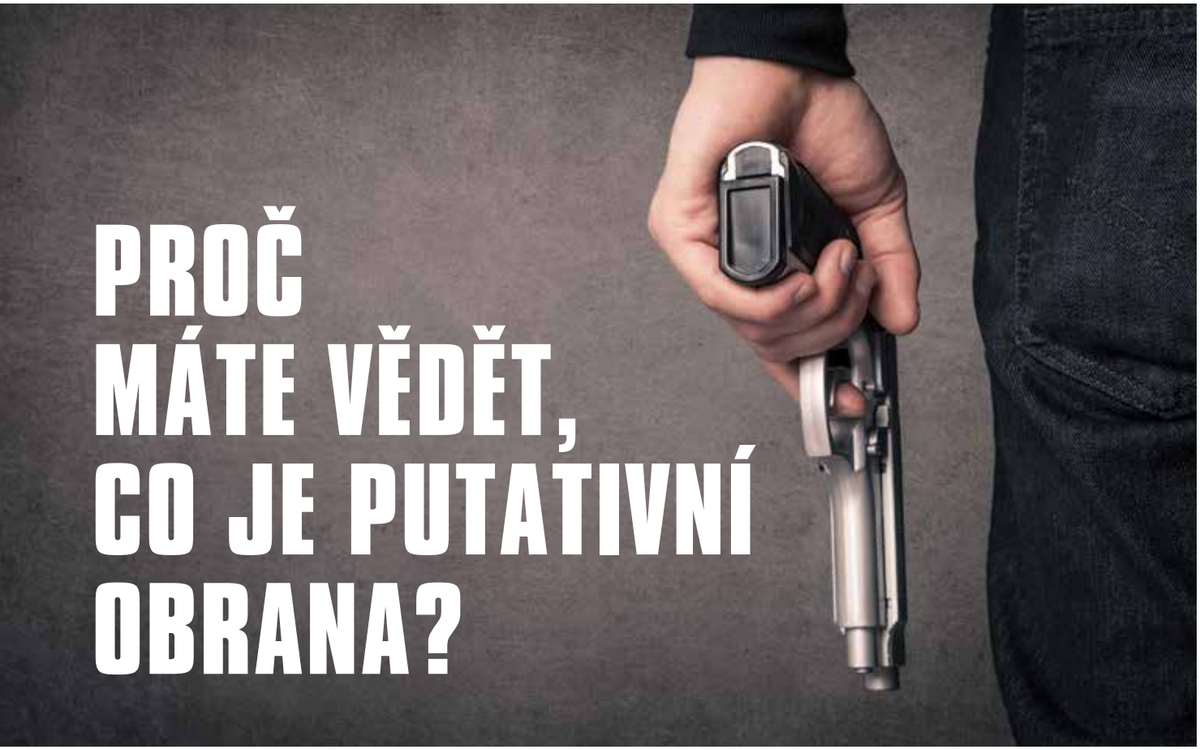
očekávanému poznání, které odpoví na ty násobící se otázky, jež mučivě bobtnaly v hlavě paní Dominiky. Ptaly se donekonečna, jak to tedy je, a zda se neděje něco, co by bylo dobré vědět (nebo spíš raději nevědět).

Dominika si přinesla odposlouchávací zařízení domů, vyjmula z něj maličkou paměťovou kartu chráněnou heslem, aby nedošlo k neoprávněnému přehrání záznamu, a zasunula ji do svého notebooku.

Na displeji počítače paní Dominiky speciální program pro vyhodnocení a poslech pořízeného záznamu v časové ose graficky ukazuje, že nahrávka je plná zvuků. Dominika je bledá a třese se jí ruka, když kliká na tlačítko PLAY. A pak už jen za pomoci sluchátek a pro jistotu i dvou panáků ginu s tonikem poslouchá. Na monitoru sleduje místa, kde je křivkami znázorněné ticho i zaznamenané zvuky.

Záznam je kontinuální, zachytil vše od počátku do konce. Kliká si na jednotlivé pasáže, kde je vidět, že je zde nahrán zvuk, a znovu a znovu si je přehrává. Je tam vše, bohužel úplně vše. Od zarachocení klíče v zámku, přes klidný hluboký mužský hlas, který tak dobře zná, ale který také vyslovuje jiné ženské jméno. Slyší zvonivý smích té cizí potvory, která se časem přestane smát a začne slastně vzdychat. Jsou slyšet i mlaskavé polibky, pravidelné šustění a vrzání, zřejmě pohyby v ložnici. Slyší slova svého milovaného prince, která jasně přikazují té nechutné couře, co má znovu a zase dělat. Nakonec tekoucí voda v koupelně. Pak jen ticho a tikání budíku, který netečně měří čas. Ten čas, který paní Dominika s tím zrádcem a darebákem už příště ztrácet nebude. Těch pár nahraných dní mění zásadně vše. Slzy se nedají zastavit. Bolí to, ale je to tak. Co dál? Co bude teď dál? Černé mraky se vyprší a blesky s hromy přejdou a odezní. Vysvitne sluníčko a na nebi se ukáže duha. Vlastně pak zase začne něco nového. Dalo by se říci, do slova a do písmene, že už je opět jasno. ■

Pavel Maletínský
Autor je jednatelem společnosti GoldSilver



PROČ MÁTE VĚDĚT, CO JE PUTATIVNÍ OBRANA?

Úspěšně jste se ubránili proti útoku. Jenže při vyšetřování se ukáže, že vůbec o žádný útok nešlo. Jak to asi bude posuzovat soud? Máte vůbec šanci se takové blamáži, která zavání i vězením, vyhnout? A můžete bezpečně rozlišit, kdy už se podle zákona bráníte útoku a kdy to ještě útok není?

Další díl našeho seriálu o právu a sebeobraně se zabývá domnělou obranou. Tedy nutnou obranou před útokem, který ve skutečnosti nehrozil. Nebo ještě nehrozil. Nebo nebyl tak závažný, jak se obránce domníval. Právní řečí se takové případy nazývají putativní obranou. Újma způsobená útočníkovi se v těchto případech posuzuje „pouze" jako nedbalostní trestný čin. Samozřejmě jen v případě, když skutečně o putativní obranu jde.

Podstatu domnělé obrany si můžeme přiblížit na několika příkladech. V minulém čísle jsme popisovali střet dvou mužů, z nichž jeden se snažil nedovoleně proniknout do hlídaného objektu.

Bezdomovec se nejprve do objektu snažil dobývat, po výzvě k odchodu odešel, jenže o pár minut později přišel znovu a žadonil o cigarety. Hlídač objektu bohužel situaci vyhodnotil mylně a bezdomovce při druhém setkání rovnou srazil k zemi. U soudu by se mohl hájit tvrzením, že šlo o takzvanou putativní obranu. Jenže nešlo.

„O ni by mohlo teoreticky jít v případě, že by fyzickým útokem reagoval na pokus se opět dostat do objektu. Ovšem jen v případě, pokud například domnělého vetřelce vyzval k odchodu a on by se přesto dál snažil vrata otevřít nebo přelézt," vysvětluje Pavel Rameš z pražské advokátní kanceláře Sikora, Truneček & Rameš.

STAČÍ ZVEDNOUT RUKU …

K domnělé obraně může snadno dojít kdekoli, třeba na diskotéce či v restauraci, zejména tam, kde vznikají nepřehledné situace, často navíc podpořené alkoholem.

Modelový příklad: Jste „vyhazovačem" v tanečním klubu. U baru stojí muž se skleničkou a píše „esemesku". Zezadu se k němu blíží urostlý mladík. Tušíte vznikající problém, takže vyrážíte také směrem k muži na baru. Ve chvíli, kdy se mladík pokusí muže uchopit zezadu za rameno, k němu přistupujete, chytáte napřaženou ruku a srážíte ho k zemi.

Posléze se ovšem ukáže, že urostlý mladík chtěl jen překvapit tátu, kterého v tomto podniku nečekal. Pokud jste měli štěstí a mladík si při pádu nic neudělal, nebo vaše případně nasazená páka neměla fatálnější následky, vše nakonec dopadlo dobře. Pokud ne, mohla by vás snadno čekat žaloba.

„V případě skutečné putativní obrany je pro soud hodně důležité i to, jak rychle poznáte svůj omyl, respektive jak brzy ukončíte svoji domněle obrannou akci," připomíná Pavel Rameš. „Významné samozřejmě bude i to, jak závažně mohl vypadat útok, i to, jak razantně na něj domnělý obránce reagoval. A především, zda reagoval opravdu bezprostředně, bez možnosti rozeznat svůj omyl," přibližuje advokát. „Když si třeba někdo počká, aby se zorientoval v situaci, a pak teprve zahájí svoji pseudoobrannou akci, je velmi pravděpodobné, že jej soud zcela správně označí za útočníka," dodává.

Souběh náhod však může být daleko horší než to, že udeříte syna, který chce zezadu překvapit tátu stojícího u výčepu. Domnělý útočník totiž může mít v ruce předmět, který zaměníte za zbraň, nebo udělá pohyb, jakoby pro zbraň sahal. Ve skutečnosti bude mít v ruce pouze pouzdro na brýle nebo si sáhne k opasku pro mobilní telefon. Ale vy k obranné akci přistoupíte tak, jakoby „útočník" měl zbraň.

„Takové případy jsou obzvlášť závažné. Obránce totiž použije proti ozbrojenému útočníkovi podstatně tvrdší akci, než proti neozbrojenému. Je to logické, protože jeho obava o zdraví je kvůli zbrani větší. Dochází tak k ještě většímu omylu," upozorňuje Pavel Rameš. Soudy v těchto případech musí brát v úvahu všechny okolnosti, včetně intenzity světla, hluku a všeho dalšího, co mohlo či nemohlo ovlivnit správné posouzení toho, zda má „útočník" skutečně zbraň.

„Jestli můžu poradit, doporučil bych všem čtenářům, aby pokud možno vnímali celkovou situaci. Lepší rada, jak se vyhnout putativní obraně, tedy nedbalostnímu trestnému činu, asi není," navrhuje advokát Rameš.

„Pokud nemáte čas a prostor na jinou než obrannou reakci, někdo vás třeba nečekaně zezadu obejme, udělejte jen obrannou část akce, vyprostěte se, ale s přechodem k navazující technice úderu nebo porazu zkuste vyčkat," doplňuje advokát.

VAŠE ROLE MUSÍ BÝT JASNÁ

Obětí putativní obrany se může stát i ten, kdo se snaží urovnat nějaký konflikt. Pokud se tedy dostanete do situace, že se rozhodnete přerušit nějakou strkanici, například dvou opilců před vchodem do vám svěřeného obchodního centra, pamatujte si, že vás někdo z jeho účastníků může považovat za útočníka. Musíte se proto chovat tak, aby vaše role byla zcela zřejmá. Doporučujeme hlasitě – tak aby si toho všimli i případní svědci – volat, o co se snažíte. Radši to křičte. Udržujte bezpečnou vzdálenost od všech aktérů sporu. Z vašeho chování musí být zřejmé, že nikomu nestraníte. Nikdo z účastníků sporu také nesmí získat dojem, že se pod rouškou uklidnění konfliktu snažíte zkrátit vzdálenost k němu, abyste ho mohli ohrozit. Dodržení všestranně bezpečné vzdálenosti a zřejmá nestrannost pro vás může v takových situacích být i životně důležitá.

Ukažme si to na příkladu: v roce 2010 se nejvyšší soud zabýval krvavým případem putativní obrany, ve kterém se střetl směnárník se dvěma Iráčany. Přímo v akci se tehdy objevily dokonce tři nože. Iráčané byli švagři a jeden z nich měl dlouhodobý spor se směnárníkem. Situace ve stísněném prostoru směnárny rychle zhoustla, Iráčan „A" posléze vytáhl na podporu svých požadavků nůž. Směnárník reagoval tím, že uchopil do rukou dva nože se zhruba třiceticentimetrovými čepelemi.

V tu chvíli se spor pokusil zmírnit Iráčan „B" a vstoupil mezi oba muže. Svůj záměr soudu popsal jako „zkusím ho pozastavit". Jenže kvůli stísněnému prostoru směnárny a krátké vzdálenosti mezi aktéry sporu se tak rovnou dostal na dosah směnárníka. Což znamenalo značnou taktickou změnu situace. Směnárník na změnu situace zareagoval použitím nože proti Iráčanovi „B". Výsledkem byla 12centimetrová rána na levém předloktí muže „B" s pravděpodobnými trvalými následky na pohyblivost ruky.

Právní definice toho, co je útok, případně momentu, kdy útok skutečně začal, v českém právním řádu není. Jednoduchý návod na to, s jakým předstihem před první ránou útočníka můžete zahájit svoji obrannou akci, vám tedy nikdo nedá. Avšak definicí (lépe řečeno podstatou) putativní nutné obrany je to, že pachatel mylně předpokládá útok na zájem chráněný trestním zákonem, vůči němuž zaměřil své obranné jednání. Takové počínání se hodnotí podle zásad o skutkovém omylu pozitivním (viz § 18 odst. 4 tr. zákoníku), který vylučuje úmyslné zavinění.

Soud situaci hodnotil velmi pečlivě, vzal například v úvahu i podmínky vyplývající ze stísněného prostoru směnárny. Putativní obrany se týkala především závěrečná část rozsudku nejvyššího soudu, ze které volně citujeme:

„Úloha poškozeného ‚B' se objektivně ukázala jako účast osoby, která se snažila konflikt urovnat, a to alespoň potud, aby nepřerostl do vzájemného fyzického napadení. Nicméně z hlediska obviněného to nemuselo být zřejmé. Poškozený se do směnárny dostavil společně s ‚A', jako jeho švagr byl členem rodiny, a to ho v souvislosti s povahou sporu, který v zásadě byl sporem rodin, stavělo v očích obviněného do pozice osoby podporující švagra. Není důvod pochybovat o tom, že pokud se konflikt odehrával pouze ve slovní rovině, vystupoval poškozený na straně svého švagra a jevil se jako jeho společník.

Jestliže se ‚B' za uvedených okolností fyzicky postavil před obviněného, není nic nepřijatelného na tom, že na obviněného to působilo jako součást útoku, který mu jinak hrozil od ‚A', a že obviněnému se situace jevila jako společný útok obou mužů. To, že ve skutečnosti nešlo o účast poškozeného na útoku proti obviněnému, lze hodnotit jako skutkový omyl obviněného ohledně okolnosti vylučující protiprávnost jeho jednání. Jde o tzv. putativní obranu. Proto je namístě posoudit jednání obviněného podle zásad o skutkovém omylu."

PUTATIVNÍ STŘELBA

Existuje i případ, kdy putativní obrana stála život domnělého útočníka. Obránce jej totiž zastřelil. „Na tomto případě je dobře vidět, co vše soud musí správně vzít v úvahu," předesílá advokát Pavel Rameš. Je totiž otázkou, jak by tento případ soudy posuzovaly, kdyby měl jiné aktéry.

Obráncem byl totiž senior, který s manželkou žil ve venkovském domě. Podroušený muž, který žil o několik domů dál, se při návratu z hostince spletl a jako domů se vydal právě k domku staršího páru. To, že se mu nepodařilo odemknout branku na pozemek, považoval za akci své manželky, která jeho pití neschvalovala. Popadl jej vztek. Přelezl branku a s mnoha nadávkami se vydal k domu. Pochopitelně ani domovní dveře nemohl svými klíči odemknout. To jej rozběsnilo a začal dveře vyrážet.

Senioři slyšeli spoustu nadávek, vyhrůžek a výzev „otevři ty dveře". Pak už se jejich dveře otřásaly při pokusech o jejich vyražení. Starý pán neváhal, vzal legálně drženou loveckou pušku, a aby předešel ohrožení sebe a své ženy, vystřelil přes zatím ještě odolávající dveře.

„Šlo o úplně klasický případ putativní obrany," hodnotí případ advokát Rameš. „Nejsem si ale úplně jistý, jak by dopadl soud, kdyby na místě starého pána byl třicetiletý adept bojových umění," připouští zároveň. „Na druhou stranu řetězec událostí nedával obránci celkem nikde prostor k tomu, aby zjistil, že jde o omyl. Protože těžko můžeme chtít – a nechce to ani zákon – aby si šel majitel domku s běsnícím vetřelcem nejprve popovídat před dveře," uzavírá advokát. ■

Přemysl Souček

STARÉ JAPONSKÉ ZKAZKY VYUŽIJETE I V SOUČASNOSTI

Podle představ nejednoho překvapeně zjistí, že stále výborně fungují různé zapomenuté postupy či „babské rady“. Ve sféře bezpečnosti to platí také.

V oblasti bezpečnosti je již většina obecných principů dávno objevená. Jenže o některých z nich dnes téměř nikdo neví. Nebo se na ně při různých školeních nabalila spousta moderních řečí a pouček, což z původně snadno pochopitelných zásad učinilo jen obtížně srozumitelné bláboly.

Zkusili jsme se proto podívat na to, zda některé moudrosti dávných samurajů mohou využít lidé pracující v bezpečnostním sektoru. A zdá se, že ano.

DÁVAT POZOR, NEBO BÝT POZORNÝ?

Mnoha vypjatým situacím a konfliktům se dá předejít tak, že možnost jejich vzniku předvídáte. Ovšem, jak si s předstihem uvědomit, že by mohl vzniknout nějaký problém? Nebo jak alespoň včas rozeznat, co už je k řešení pro „ochranku“ a co vlastně vůbec problém není? Inspiraci nabízí stará japonská zkazka.

„Starý samuraj chtěl vyzkoušet své tři syny. Vzal polštář a umístil jej nad závěs, který zakrýval vchod do pokoje. Pak nechal zavolat nejmladšího syna.

Mladík rychle vkročil do místnosti. Polštáře si všiml ve chvíli, kdy mu spadl zezadu na krk. Ale než dopadl na zem, přesekl jej mečem vedví.

Otec uložil nad dveře jiný polštář a poslal pro prostředního syna. Ten se dotkl závěsu, zachytil padající polštář a dal jej zpátky nad dveře.

Jako posledního povolal starý samuraj nejstaršího syna. Ten si netradičně umístěného polštáře všiml, když se blížil k závěsu. Sundal jej a položil ho v pokoji na jeho obvyklé místo.

Otec pak svolal syny. Nejmladšímu vyčinil, že dělá rodině ostudu, prostřednímu připomněl, že se musí ještě hodně učit, a nejstaršímu věnoval krásný meč.“

Starý samuraj chtěl po svých synech, aby byli pozorní a soustředění. Protože jen tak mohou vnímat dění kolem sebe v souvislostech, jako celek. A jen tak mohou dosáhnout takového výsledku, jakého dosáhl nejstarší syn. Zkrátka „pozornost znamená pozornost“, jak již kdysi vysvětloval zenový mistr Ikkjú. Nic jiného.

Pokud se chcete ve službě vyhnout zbytečným excesům, musíte být pozorní a soustředění po celou dobu. Jen tak dokážete včas identifikovat, kdo opravdu představuje problém a komu stačí jen ukázat, že o něm víte, protože hloupě žertuje. Tento přístup zvýší vaši šanci na to, abyste poznali, kdy jde do tuhého a problémový člověk se vás opravdu chystá napadnout.

Díky soustředěnosti a tomu, že vnímáte dění kolem sebe jako celek, neulpí vaše pozornost na nepodstatných věcech, jako je třeba délka sukní zákaznic. Pak si můžete včas všimnout, že se blíží člověk, který působí dojmem, že s ním budou potíže. A protože jste ho zpozorovalivčas, můžete se na něj připravit, můžete přivolat kolegu a můžete si také připravit možnosti, jak využít starou japonskou školu, která se jmenuje Škola bez ruky.

ŠKOLA BEZ RUKY

Je to v současnosti již jen zřídka vyučovaný způsob boje. O to však může lépe fungovat. Výhodou techniky je to, že nevyžaduje speciální dlouhodobý trénink. Jak se tedy chová bojovník Školy bez ruky?

Jeden z japonských šlechticů vyhlásil kdysi válku svému sousedovi. Jeho samurajové se sjížděli ze širokého okolí, aby vytáhli do války. Několik se jich po cestě setkalo u přívozu. Přijel převozník, oni se nalodili a loď vyplula k druhému břehu. Mladý samuraj se celou dobu holedbal, že je absolventem nejlepší šermířské školy v celém Japonsku. Všichni mu přikyvovali, jen starý samuraj ne. Dokonce to vypadalo, že se snad usmívá. Pro mladíka nepřekonatelná urážka. „Dědku, jakou máš ty školu šermu?“ obořil se na něj. „No, já mám Školu bez ruky,“ odpověděl kmet. To byla voda na mladíkův mlýn. „Převozníku, přiraz támhle k tomu ostrovu! Hned zjistíme, jak jsme na tom,“ zavelel. Jakmile se prám dotkl břehu, vyskočil z lodi, po pár krocích se otočil, zaujal předpisový bojový postoj a tasil svoji katanu.

Oči všech se otočily ke starému samurajovi, který seděl na bočním hrazení. Ten vytáhl svůj meč i s pouzdrem a opřel se jím celou vahou o mělčinu a prám odstrčil zpět do proudu. Pak se obrátil k mladíkovi, čekajícímu v bojovém postoji na rychle se vzdalujícím ostrově, a křikl na něj: „Tohle je, hochu, Škola bez ruky!“

Jistě, na recepci či někde u vjezdu do areálu nemáte ostrov, na který byste mohli vylákat problémovou osobu, kterou potřebujete zpacifikovat.

Jenže … co když se jen špatně díváte?

Tím ostrovem, ke kterému potřebujete přirazit, je pro každého něco jiného. Někomu stačí, když na chvíli odvede pozornost agresora, aby se mohl

bezpečně prosmýknout dveřmi, jež za sebou zamkne. A přivolá pomoc. Jiný zase potřebuje agresora přesvědčit k tomu, aby vstoupil do záběru kamery, aby si jej mohla všimnout služba u centrálního pultu. Nebo se jen potřebujete dostat k mobilu, k vysílačce …

VYHNOUT SE NEZNAMENÁ UTÉCT

Že je Škola bez ruky praktický přístup, potvrzuje i Vladimír Panýrek, trenér a loňský veteránský mistr světa v karate, který již 20 let trénuje pražskou městskou policii. Ještě než nastoupil k „měšťákům“, pracoval u dveří jako vyhazovač.

„U dveří je na vás hrozně vidět, tam si nemůžete moc dovolit. A strašně moc se toho dá vyřešit třeba tím, že odlehčíte situaci, že se zasmějete. Nebo musíte vymyslet nějakej fígl, jak toho člověka přesměrovat na něco jinýho než rvačku,“ nabízí vlastní recepty, jak se vyhnout přímému fyzickému střetu.

Vyhnout se boji totiž nemusí znamenat jen ustupovat a ustupovat, „nějak“ vyváznout a ztratit autoritu. Ve Škole bez ruky to znamená ustupovat proto, abyste dostali agresora tam, kam potřebujete. Aby se ocitl v pozici, která je pro vás nějakým způsobem výhodná. A samozřejmě celou dobu musíte vědět, co budete dělat, když tenhle plán selže. Stejně, jako to věděl ten starý bojovník. Kdyby takový plán neměl, nemohl by přece jet s ostatními samuraji do války …

NEZŮSTAŇTE U DETAILŮ

I když máte možnost uplatnit zásady Školy bez ruky a očekáváte, že se nastalý problém podaří vyřešit bez fyzického konfliktu, nesmíte pustit problémovou osobu ze zřetele. Opět, stejně jako v příběhu s polštářem nade dveřmi, je výhodné, když potenciálního agresora vnímáte jako celek. Včetně okolí.

Odpověď na to, proč je výhodné vnímat případného protivníka jako celek, poskytl již dávno mistr zenu Takuan:

„Jakmile se vaše mysl u něčeho zastaví – ať je to meč protivníkův, nebo váš vlastní, muž chystající se udeřit, nebo meč v jeho ruce, způsob nebo míra pohybu – přestáváte být svým pánem a stanete se zaručeně obětí nepřítelova meče.

Postavíte-li se protivníkovi, má zaujmout cele vaši mysl. Proto vůbec nemyslete na sebe. Soupeřův meč vás nepochybně může kdykoli zasáhnout, ale nepřipusťte si takovou myšlenku. Nechtějte odpovídat na každý jeho hrozivý pohyb protiútokem, nezabývejte se žádnými úvahami!

Vnímejte prostě protivníkův pohyb, nedopusťte však, aby na něm utkvěla vaše mysl. Postupujte proti protivníkovi stejně jako dřív a využijte jeho útoku tak, že jej obrátíte proti němu.“

Tyto zásady mají samozřejmě obecnější platnost, než je řešení samotného fyzického konfliktu. Soustředíte se například na to, aby kamery, jež máte instalovat, zabíraly

co nejlépe jedno konkrétní místo. Pokrytí onoho místa pak budete věnovat tolik péče, že vám unikne jiné důležité místo. A právě toho neomylně využije vetřelec.

Když vnímáte svůj úkol jako celek, ochranu slabých míst si připravíte také jako součást celku, a ne na jeho úkor. Nagahara Inosuke, proslulý japonský mistr meče, kdysi prohlásil: „Podstatou šermu je věnovat se cele úkolu, jak porazit protivníka.“ V kontextu článku to například znamená, že při umisťování kamer není možné věnovat větší pozornost zabezpečení vstupní brány než zbytku oplocení.

DEMONSTRACE BEZ AROGANCE

Dobrých výsledků můžete dosáhnout i včasnou demonstrací vlastní převahy. Nezáleží přitom, zda jde o převahu mentální, fyzickou či technologickou. Je však důležité při takové demonstraci nevyvolávat arogantní dojem, ale pouze svoji převahu. Nejde jen o nějakou samurajskou zásadu.

Zásadu „dominance bez arogance“ totiž vštěpuje svým žákům i zakladatel sebeobrany Pro Defence Stanislav Gazdik, který velkou část zkušeností nasbíral během 15 let strávených ve francouzské cizinecké legii.

V japonské hospůdce večeřel osamělý šermíř. Vypadal klidně, čtyři mouchy, které mu bzučely kolem hlavy, ho zřejmě vůbec nezajímaly. Do místnosti vstoupili tři róninové (samurajové bez pána, potulní rytíři, dalo by se říct). Všimli si nádherných mečů, které měl muž za šerpou, a podle starých ošumělých šatů poznali, že ani on nepatří k žádnému rodu

(nemá pána). Uvědomili si, že cena jeho mečů představuje malé jmění a že ten člověk rozhodně není společnost pro ně.

Usedli k vedlejšímu stolu a vyměňovali si nahlas poznámky o svém sousedovi. Doufali, že ho vyprovokují na souboj. Muž se však tvářil, jako by je neslyšel, ačkoli poznámky byly čím dál hrubší a drzejší. Jen zdvihl hůlky, jimiž jedl. Čtyřmi rychlými pohyby hravě chytil mouchy za křídla.

Zatímco pomalu kladl hůlky na stůl, róninové kvapem opouštěli hospodu. Dobře udělali, protože by se utkali s Mijamoto Musašim, jedním z nejslavnějších šermířů v dějinách Japonska.

Ať už ukážete svoji převahu – a stále se to týká nejen fyzické, ale i technologické převahy – jakýmkoli způsobem, nesmí to zároveň působit jako přímé vyzvání k měření sil, k boji, jako pověstná hozená rukavice. Zmíněný Mijamoto Musaši, přestože by pravděpodobně ze souboje s trojicí róninů vyšel vítězně, jim sice vyslal pro ně srozumitelný signál o své převaze, ale zároveň jim nechal možnost vyklidit pole. A zachovat si tvář.

Jestli neumíte, nebo nemůžete demonstrovat svoji převahu tak, abyste zároveň neprovokovali, pak nic nedemonstrujte. Lidé, proti kterým zaměstnanci bezpečnostního sektoru stojí, bývají na urážky svého ega obzvlášť citliví. Proto vaše demonstrace musí působit tak, aby oni sami zvážili situaci a usoudili, že pro ně není výhodná, a proto se o nic nepokusili. Nikoliv tak, aby získali dojem, že je jen zastrašujete.

Leckdy stačí vaše dostatečně viditelná pozorná přítomnost a vysílačka, kterou zjevně udržujete spojení. ■

Přemysl Souček

ZÓNA SOUMRAKU

NIKON D4S A FOTOGRAFOVÁNÍ PO SOUMRAKU

V dobrém denním světle lze pořídit kvalitní snímky s téměř jakýmkoli fotoaparátem. Co když ale potřebujete fotografovat v situaci, kdy světlo chybí?

Digitální fotoaparáty udělaly v posledních letech obrovský kvalitativní skok. Chytré telefony bezpečně zvládají většinu toho, na co jsme před pár lety potřebovali slušný kompakt. Kompakty běžně nabízejí dvacetinásobné i větší zoomy, relativně levné amatérské zrcadlovky se bez potíží vyrovnají pár let starým profesionálním modelům. Přesto existují oblasti a funkce, v nichž se stále vyplatí investovat do toho nejlepšího a nejdražšího, co je na trhu k dispozici. Týká se to především rychlého automatického ostření a schopnosti pořídit kvalitní a použitelný záběr i v hodně slabém světle, případně ve tmě. Právě na druhou ze jmenovaných oblastí jsme se dnes soustředili.

Teď není řeč o běžném nočním fotografování, třeba když při procházce městem chceme zvěčnit krásně nasvícené památky. To pro většinu přístrojů žádný problém není – stačí postavit fotoaparát na stativ (a pokud není k dispozici, třeba na zídku nebo jiné vhodné místo), zapnout samospoušť (abychom přístroj stiskem spouště nerozhýbali) a fotografovat. Automatika si sama nastaví dlouhý čas v řádu několika vteřin nebo klidně i minut. Fotografovaný objekt se nehýbe a tak dlouhá expozice ničemu nevadí. Jenže tenhle způsob fotografování na mysli nemáme.

Stejně tak neřešíme ani druhý obvyklý způsob fotografování ve slabém světle – v interiéru s bleskem. Zajímá nás fotografování z ruky, s běžným (tedy krátkým) expozičním časem, v situacích, kdy je nutné působit nenápadně (blesk tedy nepřichází v úvahu). V takovém případě pomůže jediné – fotoaparát vybavený mimořádně vysokou citlivostí, jaká ještě před pár lety patřila do říše fantazie. A musí také umět zaostřit téměř ve tmě, nebo aspoň zobrazit scénu tak dobře, že bude možné zaostřit ručně.

NIKON D4S – VE TMĚ JAKO DOMA

Jedním z fotoaparátů, o kterých se v souvislosti s fotografováním v šeru nebo dokonce v naprosté tmě hovoří nejčastěji, je nedávno představený Nikon D4S – profesionální model nejvyšší kategorie. Není divu, výrobci ho pro tento způsob práce obdařili skutečně výjimečnými vlastnostmi.

Tím nejdůležitějším je v tomto případě digitální snímač. Jako u správného profesionálního fotoaparátu je plnoformátový, tedy stejně velký jako políčko kinofilmu (většina zrcadlovek má snímače o něco menší). Na rozdíl od mnoha jiných modelů ovšem nenabízí žádné obří rozlišení – jen 16 megapixelů, což dnes najdeme i v lepších chytrých telefonech. Právě tato hodnota je přitom údajem, kterým se výrobci chlubívají hned na začátku. Neudělali tedy u Nikonu chybu, když svou vlajkovou loď vybavili relativně nízkým rozlišením?

Neudělali. Pozná se to právě při fotografování ve slabém světle. Menší počet pixelů totiž znamená, že jsou jednotlivé světločivé buňky mnohem větší než u modelů s vyšším rozlišením (fyzické rozměry snímače se nemění). V digitální fotografii platí jednoduché pravidlo: čím větší pixely, tím kvalitnější obraz. Na snímači totiž nevzniká tolik šumu, jako když jsou světločivé buňky natěsnané jedna na druhou. Čím vyšší hustota pixelů na snímači, tím silnější elektromagnetický náboj mezi nimi přeskakuje – a právě tím vzniká šum.

Další známé pravidlo říká, že intenzita šumu roste právě s citlivostí. Dnešní modely obecně odvádějí na tomto poli vynikající práci – ještě před deseti lety, v době prvních cenově dostupných zrcadlovek, byla za rozumnou hodnotu považována citlivost do ISO 400. ISO 800 a více už se nastavovalo jen v případech nouze, kdy na kvalitě fotografií nezáleželo, a málokterý model umožňoval překročit ISO 1600. Dnes u většiny zrcadlovek můžeme celkem bez obav používat i ISO 3200 a na stupnici citlivosti bývají běžně i pětimístné hodnoty. Při nich ale už se jednotlivé modely výrazně liší – některé fotografují ve slušné kvalitě v celém rozsahu citlivosti, u jiných bychom se do vyšších hodnot raději pouštět neměli. Jak si v tomto ohledu stojí nový Nikon?

V základním nastavení lze citlivost volit v rozmezí ISO 100–25600, s možností rozšíření až na 409 600. To je skutečně astronomické číslo, rozšiřující režim ovšem dává tušit, že tady přece jen o standardní kvalitu fotografií nepůjde. I v základním rozsahu je ale citlivost úctyhodná a nás samozřejmě zajímalo, jak budou fotografie vypadat v praxi.

FUNKCE A PARAMETRY

Ještě než se vrhneme na fotografování ve zdánlivě nemožných podmínkách, podívejme se na nový Nikon zblízka. Jako jedna z nejočekávanějších událostí sezóny si to koneckonců zaslouží.

D4S je nástupcem dosavadní vlajkové lodi D4 a navenek se mu hodně podobá. Nezměnil se ani zmíněný snímač, 16 megapixelů měl již předchozí model.

I novinka tak bude určena zejména reportérům, milovníkům divoké přírody a dalším fotografům, kteří před vyšším rozlišením dávají přednost právě bezkonkurenční práci ve slabém světle. (Kdo chce plnoformátový Nikon s vysokým rozlišením, má k dispozici modely D800 a D800E s 36 megapixely, což by mělo stačit opravdu každému.)

Místo staršího obrazového procesoru Expeed 3 je tu nejnovější verze s číslem 4, díky níž se dočkaly vylepšení mnohé funkce a parametry fotoaparátu. A opět většina z nich osloví hlavně milovníky akční a sportovní fotografie nebo reportáží. Týká se to například sekvenčního snímání – maximální rychlost nyní dosahuje 11 snímků za vteřinu a fotoaparát během celé sekvence dokáže přeostřovat na objekt v pohybu. Zkoušeli jsme to se psem běžícím přímo k fotoaparátu, což věru byl dosti náročný úkol. Výsledky nás opravdu přesvědčily – z nějakých padesáti snímků, které jsme tímto způsobem pořídili, byly neostré snad tři, čtyři, všechny ostatní se povedly na jedničku.

Díky novému obrazovému procesoru se vylepšily i další vlastnosti automatického ostření. Nově lze například vybrat místo jediného ostřícího bodu jejich skupinu, což přijde vhod ve chvíli, kdy se objekt pohybuje nepředvídatelně (např. pták v letu nebo hokejista na ledě) a fotografovi dělá potíže udržet ho pod jedním ostřícím bodem. Tahle funkce se mimochodem může skvěle osvědčit právě při fotografování v šeru či ve tmě, o čemž bude ještě řeč.

KONSTRUKCE A OVLÁDÁNÍ

Nikon D4S rozhodně není žádný kapesní model – větších fotoaparátů na současném trhu moc nenajdeme. Má trochu jiný tvar než velká většina zrcadlovek, jeho pevnou součástí je totiž grip pro fotografování na výšku (u běžných fotoaparátů si ho člověk musí dokoupit). Na druhou stranu padne výtečně do ruky a při práci se skvěle drží – rozhodně nehrozí, že by člověku vyklouzl.

Ovládání odpovídá standardům pro profesionální zrcadlovky – vše potřebné je po ruce, v podstatě všechny funkce se nastavují pomocí samostatných tlačítek, přepínačů a voličů. Do menu tak většina zkušenějších fotografů zavítá jen výjimečně – hlavně hned po zakoupení, kdy

je zapotřebí nastavit chování nejrůznějších předvoleb, režimů, obrazových stylů apod. Méně zběhlé uživatele může ta přemíra ovládacích prvků až polekat, stačí ovšem pár hodin nebo maximálně dnů a zvyknete si. A pokud jste už někdy libovolnou zrcadlovku od Nikonu měli, bude zvykání ještě rychlejší.

Velkou pochvalu zaslouží hledáček – je velký a hlavně dokonale jasný, scéna je v něm vidět stejně dobře jako pouhým okem. A to při fotografování ve slabém světle přijde pořádně vhod – ve starší zrcadlovce vyšší střední třídy D300, kterou jsme při testu používali pro srovnání, nebylo už v některých situacích vidět skoro nic, zatímco s D4S jsme pořád dokázali pomocí hledáčku i ručně zaostřit.

OPTIKA

Plnoformátové snímače samozřejmě vyžadují vysoce kvalitní objektivy – na rozdíl od běžných zrcadlovek (o kompaktech nemluvě) se v nich žádná obrazová vada neschová, vše je vidět. D4S je po této stránce přece jen o něco milosrdnější než třeba D800, při 16 megapixelech nejsou nároky na optiku úplně extrémní. I tak ale na kvalitě objektivů hodně záleží. Při běžném fotografování jsme používali výtečný širokoúhlý Nikon 14–24 mm f2,8 a oblíbené pevné sklo 50 mm f1,8, pro test ve slabém světle jsme se vybavili praktickým zoomovým teleobjektivem Nikon 70-200 mm f2,8 VR II.

Pro naše účely šlo o optimální variantu – objektiv je vybaven výkonným stabilizátorem, díky němuž lze v ruce pohodlně udržet až o 4 EV delší čas než bez stabilizace. Pokud tedy s běžným objektivem s ohniskem 200 mm potřebujeme čas minimálně 1/200 s (podle pravidla, že nejdelší udržitelný čas je roven inverzní hodnotě ohniskové vzdálenosti), lze ho díky stabilizaci prodloužit až na 1/15 s.

▲ *Fotografováno přibližně z patnáctimetrové vzdálenosti z úkrytu mezi keři, víceméně v naprosté tmě. Čas 1/20 při cloně f2,8 a citlivosti ISO 25 600 je na hranici udržitelnosti, ale podařilo se nakonec bez problémů. Kdyby na lavičce seděl člověk, je bezpečně k poznání.*

▲ *Fotografováno okolo deváté večer – na ulici nebylo zdaleka tolik světla, kolik by se z fotografie mohlo zdát. Clona f2,8, čas 1/40 s, ISO 25 600.*

V kombinaci se světelností f2,8 a vysokou citlivostí se na tento čas dostaneme i v téměř naprosté tmě. Kromě toho se zmíněný teleobjektiv vyznačuje velmi dobrou kresbou i při minimální hodnotě clony, což není zrovna standardní.

Výhrady by někdo mohl mít snad jen k nepříliš dlouhému ohnisku – pro náš záměr stačilo, ale třeba na fotografování zvěře v přírodě je 200 mm dost málo. V takovém případě lze použít telekonvertor, tedy přídavné optické zařízení, které ohnisko prodlouží. Jen pozor, při použití konvertoru klesá světelnost. S konvertorem s dvojnásobným přiblížením se nejdelší ohnisko prodlouží na 400 mm, ale světelnost bude činit pouhých f5,6.

TEST ANEB SLÍDĚNÍ V PARKU

Počkali jsme si až zapadne slunce a vyrazili do jednoho z pražských parků. Sem tam v něm svítí pouliční lampa, ale na většině míst je tma. Zpočátku bylo šero, to se ale hodně rychle změnilo ve tmu, v níž nebylo vidět ani na hodinky. V podstatě hned jsme museli nastavit maximální citlivost v běžném rozsahu, tedy ISO 25 600. Zpočátku nám při cloně f2,8 vycházel čas 1/40 s, poté se prodloužil na 1/20 s, což je při ohnisku 200 mm i se stabilizátorem na hranici udržitelnosti. Ani v naprosté tmě jsme ale nepotřebovali delší čas.

Výsledky byly skutečně impozantní – ostatně posuďte sami. Na některých fotografiích se zdá, že je světla díky pouličním a parkovým lampám dost, ale je to klam, za který může relativně dlouhá expozice (při ní má fotoaparát tendenci „posbírat" více světla, než kolik ho na scéně ve skutečnosti je). V reálu byla od začátku fotografování taková tma, že nebylo vidět na nastavení fotoaparátu. Proto je dobré mít rozložení uživatelských prvků takříkajíc „v prstech". Hodně pomáhá i třetí displej na zadní straně, na kterém se zobrazí základní nastavené parametry a který je (na rozdíl od stavového displeje na horní straně) při manipulaci decentně, ale zřetelně podsvícený.

Pokud na scénu dopadaly aspoň zbytky světla, fungovalo automatické ostření bez problémů, tedy spolehlivě a hlavně rychle (většinou se fotoaparát chytil napoprvé). To se zhoršilo až v úplné tmě, kdy jsme si vyhlédli lavičku v neosvětlené části parku. Pouhým okem byla vidět jen jako temná skvrna na trávníku a při ostření na jediný bod ji fotoaparát nezaregistroval. Když jsme ale přepnuli automatické ostření na skupinu bodů, kupodivu se mechanismus chytil. A když člověk chvíli sledoval scénu v hledáčku, dokázal na lavičku zaostřit i ručně. Na výsledných fotografiích je vidět naprosto zřetelně.

Na fotografování ve tmě je Nikon D4S v kombinaci s objektivem 70–200 mm f2,8 VR II zkrátka dělaný. Výhradu lze mít snad jen k hlasitějšímu cvaknutí zrcátka a závěrky, s tím ale u zrcadlovky nic dělat nelze. Jinak fotoaparát díky skvělému snímači s minimem šumu zachytí i jevy, kterých bychom si ani nevšimli. Díky světelnému stabilizovanému objektivu ani při nejvyšší citlivosti nehrozí, že bychom přístroj při fotografování z ruky neudrželi.

Nikon D4S
149 990 Kč
Nikon 70–200 f2,8 VR II
59 990 Kč

ALTERNATIVY

Canon EOS-1D X
159 990 Kč
Canon 70-200 mm f2, 8 IS II
59 990 Kč

Největší konkurent Nikonu nabízí v podstatě stejný objektiv a velmi podobně koncipovaný fotoaparát. Profesionální zrcadlovka s plnoformátovým snímačem má rozlišení 18 MPix, což rovněž není nijak mnoho, a stejně jako D4S je určená především reportérům, fotožurnalistům apod. Canon je vybaven snad ještě sofistikovanějším systémem automatického ostření, které lze optimalizovat například pro konkrétní sportovní disciplíny, na druhou stranu už je na trhu nějaký pátek a třeba obrazový procesor není tak výkonný jako u Nikonu.

Sony Alfa A99
59 990 Kč
Sony 70–200 mm f2,8 SSM II
77 690 Kč

Třetím výrobcem, který v současnosti vyrábí plnoformátové fotoaparáty, je Sony. Jeho Alfa A99 s rozlišením 24 MPix ovšem není v pravém smyslu zrcadlovka – je vybavena technologií polopropustného zrcátka SLT, která má své přednosti i nedostatky. Mezi výhody patří zejména tišší chod a rychlé automatické ostření, nevýhodou je absence kvalitního optického hledáčku, která zejména při fotografování ve tmě zamrzí. Další předností je nižší cena a také stabilizátor na snímači, takže není zapotřebí kupovat stabilizované objektivy. ■

Rani Tolimat

KLÍČOVÁ OTÁZKA

Časy jsou zlé a vždycky byly. Nic nemůže být pomýlenější než úvaha, že až dnešní zlý svět nás nutí chránit majetek i sebe pečlivým zamykáním a zavíráním. Historie psaná klíči a zámky je ve skutečnosti stejně dlouhá jako éra lidského rodu a provází nás stejně věrně jako domestikovaná zvířata.

Nepovolenému vstupu bránily zámky a klíče už dlouho předtím, než se začal psát náš křesťanský letopočet. První doložené zmínky o nich odkazují dokonce až na dobu před čtyřmi tisíci let ve starověkém Egyptě. Hojně se vyskytují také v různých mytologických příbězích a často jsou připomínány také ve Starém zákoně. Kromě jiného je například doloženo použití zámků při opravě městských bran Jeruzaléma někdy kolem roku 445 před naším letopočtem.

Zamykací mechanizmy oněch prvotních dob byly z pochopitelných důvodů vyráběny ze dřeva, a přestože byly relativně hrubě zpracované, využívaly konstrukčních principů příbuzných těm dodnes používaným. Typickým zámkem oné doby byly dřevěné čepy, které díky gravitaci zapadly do závory nebo zástrčky, a tím zámek zamkly. K otevírání sloužily dřevěné klíče s vsazenými kolíky nebo hroty, které čepy nadzvedly tak, aby zástrčku bylo možné volně odsunout. Ano, už tehdy se objevili předci dnešních stavítkových zámků. Nejstarším dochovaným dřevěným zámkem je archeologický nález z Persie, kde byl umístěn na bráně paláce Sargona II., postaveného mezi roky 722 a 705 př. n. l. Tím byl zároveň objeven velmi zajímavý způsob otevírání takového zámku. Nešlo rozhodně o dnes obvyklé otáčení klíčem kolem podélné osy. Celý zabezpečovací mechanizmus včetně závory byl umístěn na „neveřejné“ straně dveří. Kdo chtěl dovnitř, musel malým otvorem prostrčit ruku s poměrně rozměrným klíčem, zastrčit jeho kolíky správně do zámku a pak za pomoci síly a zručnosti nadzvednout všechny stavítka. Pak bylo možné odsunout stranou závoru a vstoupit.

DOBA KOVOVÁ

Změna materiálu pro výrobu zámků byla vynucena potřebou jejich vyšší odolnosti, musela si však počkat až na pokrok v technologiích zpracování kovů. Za dobu vzniku celokovových zámků se považuje období mezi léty 870 a 900 našeho letopočtu a zásluha na jejich vzniku se připisuje anglickým řemeslníkům. Odolnější zámky měly pouze jednoduché kovové západky, objevily se však poprvé tvarované vstupy pro klíč pro zabránění nechtěné manipulace se zámkem.

V následujících staletích byl technický rozvoj zámků jen pozvolný, nicméně zámečníci se stali uznávanými umělci a elitními řemeslníky. Jejich práce se totiž zpočátku stala privilegiem pro mocné a bohaté tehdejšího světa. Stále větší důraz se proto začal klást i na umělecké zpracování zámků a klíčů, přizpůsobených vládnoucímu dobovému stylu. Profilům klíčů byly dávány různé ornamentální a symbolické tvary, zejména pokud sloužily k uzamykání významných staveb, např. měšťanských domů, chrámů nebo hradních bran. Asi největší zdobností se zámky chlubily za gotiky, a zejména renesance. Rytí, umělecké kovářské práce, leštění nebo leptání kovů udělalo ze zámků skutečná výtvarná díla a z jejich výrobců se staly „celebrity“ mezi tehdejšími řemeslníky. Situace dospěla tak daleko, že když tovaryši zámečnického oboru skládali závěrečnou mistrovskou zkoušku, jejich ukázkovou prací byl zámek nikoliv pro praktické použití, ale s otevřenou konstrukcí, aby bylo dobře patrné, jaké finesy a principy při jeho konstrukci uchazeč použil.

Není proto divu, že v nové disciplíně se zhlédly i nejmocnější osobnosti, které by si jinak s obyčejnými řemeslníky příliš nezadaly. Málo se ví, že jedním z velkých nadšenců a odborníků na zámky byl francouzský král Ludvík XVI., manžel Marie Antoinetty. Zatímco povinnosti týkající se vládnutí ho příliš nebavily, více času raději trávil v dílně výrobou zámků a uplatňováním zkušeností, které získal od zámečníka jménem Gamin. Ludvík byl obzvláště pyšný na vlastnoručně vyrobenou a do zdi zabudovanou skříňku s důmyslným zámkem, kam ukrýval své nejtajnější dokumenty. Ani záliba v poctivém řemesle ale krále nepomohla ve vyjednávání s revolucionáři během Velké francouzské revoluce, kdy byl tajný sejf objeven a otevřen právě Gaminem. Tím byl zpečetěn osud urozeného páru.

Dalším šlechticem propadlým kouzlu zámků a klíčů byla ruská carevna Kateřina Veliká. Ne snad, že by zámky sama vyráběla, ale byla jejich náruživou sběratelkou a měla ve své době největší světovou kolekci zámků na světě. Za nejcennější kousky považovala ty s originálním nápadem a precizně zpracovanými detaily, takže často ona i její děti dostávaly podobné kousky jako originální dárky, vyrobené unikátně pro vladařskou rodinu. Traduje se dokonce historka, že jeden ze známých ruských zámečníků si unikátním dárkem u carevny vysloužil omilostnění z vyhnanství na Sibiři, kam se dostal za jakýsi přestupek.

NOVÉ ČASY

Moderní koncepce zámků se zrodila v Evropě během 18. století. Stále širší možnosti strojního zpracovávání kovů daly vývoji zcela nový směr a vše se od dekorativnosti a reprezentace začalo více posouvat směrem ke zvyšování bezpečnosti zámků a jejich odolnosti proti překonávání. Právě v té době se totiž překonávání zámků

stalo populární disciplínou mezi zločinci. Konstruktéři zámků se jim sice snažili zpočátku ztížit práci například dodatečnými překážkami pro nepovolený přístup do klíčové dírky či přidáváním falešných zámků – až po vytváření vyložených skládankových hlavolamů. Pro časté a rychlé odemykání však bylo třeba vymyslet něco rychlejšího a spolehlivějšího. Konstruování zámků nové koncepce se tak stalo masovou disciplínou.

Dobrým příkladem byl vývoj v koloniích v Severní Americe. Zpočátku se zde objevovalo zámků jen pomálu a šlo o modely, kopírující přesně evropské konstrukce. Po vzniku USA se ale činnost zámečníků rozjela naplno, takže mezi roky 1774 a 1920 si američtí výrobci patentovali neuvěřitelné tři tisíce různých konstrukcí zámků. Byl to dosti významný skok od doby počátků osidlování nového kontinentu, kdy otevírání dveří obstarával jednoduchý systém závory na jejich vnitřní straně, kterou nadzvedávalo lanko nebo provázek, prostrčený otvorem ven. Pokud tam byl, návštěva mohla zatáhnout a vejít, když chyběl, pohostinnost se nekonala a bylo lépe klid domu nerušit. Obdobný problém mimochodem na začátku 20. let minulého století řešil Walter Schlage u dveřního zámku s válcovou západkou, uzamykatelného jednoduchým stiskem tlačítka. Cílem bylo zamknout interiérové dveře rychle a bez klíče pomocí mechanizmu, který by díky malým rozměrům nehyzdil interiér.

VÝZNAMNÍ PRŮKOPNÍCI

K prvním průkopníkům moderního zámečnictví patřil Robert Barron, který si v roce 1778 nechal patentovat dvojčinný západkový zámek coby první zásadní příspěvek k jejich bezpečnosti.

Jen o pár let později se zapsal do dějin všestranný vynálezce Joseph Bramah. V roce 1784 založil nejstarší a dodnes existující londýnskou firmu věnující se zámkům a zabezpečování. K rozvoji oboru přispěl rovněž originálním po sobě pojmenovaným patentovaným zámkem. Svému nápadu věřil natolik, že vyhlásil roku 1790 veřejnou soutěž: kdo vyrobí nástroj schopný otevřít jeho zámek, získá odměnu 200 guinejí. Dnes se to zdá zvláštní, ale výzva byla v platnosti celých 61 let. Až v roce 1851 uspěl americký zámečník a podnikatel Alfred Charles

Hobbs. Nicméně i tak se s pokořením Bramahova zámku hmoždil celých 51 hodin čistého času. Přemýšlení a výroba nástrojů mu zabraly celkem 16 dní, ale stálo to za to. Celý experiment totiž podnikl v rámci Světové průmyslové výstavy konané v Londýně. A aby toho nebylo málo, jeho úsilí vzápětí neodolal ani do té doby rovněž zdánlivě nepřekonatelný Chubbův indikátorový zámek, patentovaný v roce 1818. Nic nepomohlo, že zámek se stal svého času vítězem vládní soutěže a ani zkušený zloděj s ním po tři měsíce nic nesvedl. Nicméně ještě předtím do rodinné firmy přibyl k Jeremiáši Chubbovi bratr Charles, který přišel s vylepšením konstrukce. Nejdříve odstranil nutnost použít speciální klíč pro resetování zámku, do kterého se pokoušel někdo dostat. V roce 1847 pak předvedl novou koncepci využívající šesti zdvihátek místo původních čtyř a přidávající kotouček, který dovoluje zasunutí klíče, ale zabraňuje přístupu ke stavítkům za pomoci šperháku. V té době už firma bratří Chubbů držela patent na výrobu prvního, zlodějům odolného sejfu, s jejichž výrobou začala v roce 1835.

ZPROPADENÉ VÁLEČKY

V běžném životě se všichni nejčastěji potkáváme se zámky stavítkovými. V anglosaských oblastech se také setkáte s označením yale zámek, to podle amerického konstruktéra a výrobce zámků Linuse Yalea seniora, který v roce 1844 přišel s revoluční koncepcí stavítkového zámku doplněného o soustavu odpružených blokovacích kolíků, které musí klíč pomocí rovněž pohyblivých stavítek pro odemčení nadzvednout do správné polohy. Vlastně nešlo o nic jiného než o princip stavítek, vynalezený už starými Egypťany, ve spojení s otočným válcem. Vznikla tak patentovaná cylindrická vložka – pro dříve narozené tuzemce prostě „fabka". Yaleův syn Linus junior pak ještě pokračoval v rodinné tradici a v roce 1861 původní koncepci svého otce ještě vylepšil zavedením menšího plochého klíče s drážkami a zubatým profilem pro různě dlouhé kolíky. Princip byl natolik geniální, že stejný systém používáme až do dnešních dnů, jen s různými evolučními vylepšeními.

Jedním z těchto pozdějších vylepšení konstrukce je vložení mezistavítka mezi stavítko a blokovací kolíky. Tím je umožněno použití univerzálního nebo také generálního klíče, kterým lze odemknout všechny zámky z dané skupiny, například u dveří kanceláří v jedné firmě nebo u hotelových pokojů.

VISÍ VISATEC

Zdánlivě nejobyčejnější ze všech druhů zámků jsou zámky visací. Jejich historie si ale v ničem nezadá s jejich sourozenci zabudovávanými do dveří. Díky většinou malým rozměrům i hmotnosti, a tudíž velké mobilitě, se s nimi lidstvo setkává už pěkně dlouho málem na každém kroku.

První visací zámky se objevují už zhruba 500 let před naším letopočtem u starých Římanů, ale také v dalších civilizacích. Vznik podobného zabezpečení si vynutil rozvoj obchodu se vzdálenými kraji, kdy karavany se zbožím putovaly celé dny a měsíce do neznámých a exotických zemí. V Číně jsou visací zámky dobře zdokumentovány díky jejich častému používání již za časů dynastie Han v prvním století po Kristu. Zámky se vyráběly nejdříve z mědi, později také z bronzu, stříbra a dalších kovů. Pokud jde o koncepci, používaly hlavně princip klíče a otočného kloubu nebo bezklíčový princip s kombinací písmen.

V pozdější době se základní konstrukce takzvaných „udírenských" zámků (skutečně původně používaných k zabezpečení domácích udíren a skladů masa) objevila v Anglii. Vyráběly se z plátu kované oceli, měly pouze jednoduchý mechanizmus, a tím nízkou odolnost proti překonání, výhodou ale byla jejich cena. Ve stejné době se zejména ve slovanské části Evropy staly populárními visací zámky se spirálovými klíči, které se musely do klíčové dírky „zašroubovat" a nakonec pootočením odjistit západku proti silnému odporu pružiny.

Okolo poloviny 19. století se objevily takzvané skandinávské zámky, nazývané také někdy Polhemovy podle jejich švédského vynálezce Christophera Polhema. Staly se bezpečnější alternativou k oběma starším koncepcím. Tělo zámku bylo z litiny a uvnitř se nacházelo několik disků s otvorem pro klíč a dvěma výřezy na obvodu. Skandinávský typ zámku byl tak

úspěšný, že jistá firma v americkém Newarku ho vyráběla až do padesátých let minulého století a mnozí menší výrobci pokračují v jejich výrobě stále.

Přibližně okolo roku 1870 si výrobci visacích zámků uvědomili, že by mohli spojit více stávajících technologií dohromady a umístit zamykací mechanismus do výrobně levnějšího ocelového nebo mosazného těla místo do masivní kovové schránky. V souvislosti s tím získala v roce 1877 společnost Yale & Towne patent na zámek, jehož třmen se po odemčení odklopil. S tím bylo spojeno, že zamykací mechanizmus byl sjednocen do podoby „vložky", která se při výrobě upevnila do těla zámku. Visací zámek tak bylo poprvé možné opravovat, měnit vložku v případě ztráty klíče a podobně.

Další posun ve způsobu výroby zámků přinesl na začátku 20. století rozvoj mechanického obrábění kovů. Tak se objevily první zámky s tělem z jednoho kusu kovu, do kterého se vkládal zamykací mechanizmus s kolíky a stavítky spolu s posuvným třmenem. Zámky se staly populárními pro snadnou výrobu a vysokou odolnost, takže se s nimi setkáváme dodnes. Zdánlivě jinou cestou se vydal ve dvacátých letech minulého století Harry Sofer, zakladatel firmy Master Lock, když přišel jako první na světě s konstrukcí visacího zámku skládaného z dílů. Kovové pláty se zamykacím mechanizmem uvnitř byly nakonec snýtovány a vznikl velmi levný, přitom proti násilnému otevření odolný zámek. Rovněž tato konstrukce je stále populární a používá se hlavně tam, kde je třeba chránit majetek nízké hodnoty. Když se ve třicátých letech 20. století objevil nový postup výroby kovových částí metodou tlakového lití tekutého kovu do kovové formy, s nadšením po něm sáhli i tvůrci visacích zámků. Novinka jim dovolila produkovat zámky takových tvarů a zdobení, jakých by se mechanickým opracováním dosahovalo jen za vysokých nákladů.

BEZPEČNÁ ČÍSLA

Zámek a klíč zdánlivě patří nerozlučně k sobě. Překvapením však může být, že ani zabezpečování bez klíče pomocí různých kombinačních zámků není až záležitostí novodobou. Nejstarší kombinační zámek byl objeven při vykopávkách v aténském Karameikosu a pochází z období starověkého Říma. První dochovaný písemný záznam pochází z počátku třináctého století, když se muslimský „inženýr" Al-Jazari zmiňuje o kombinačním zámku v knižním soupisu znalostí o mechanických výtvorech.

Další zmínky o kombinačních zámcích se vyskytují i později ve středověku, jejich novodobá historie ale přichází až s průmyslovou revolucí v 19. století. S principem moderního zámku schopného jednoduché a rychlé změny kombinace čísel přichází jako první James Sargent v roce 1857. Nový způsob uzamykání si okamžitě oblíbili výrobci sejfů i ministerstvo financí USA. Stejný tvůrce pak ještě o pár let později v roce 1873 přidal k dobru patent na časový zámek, bez jehož modernějších potomků se neobejde žádná současná bankovní pobočka. Dobový prototyp jenom na rozdíl od současných modelů odměřoval čas mezi zadáním správné kombinace a odjištěním dveří na čistě mechanickém principu a existoval způsob, jak činnost hodin obejít zadáním kódu, známého jen vybraným zaměstnancům firmy. Důvodem byla celkem logická obava, že v případě poruchy časovacího mechanizmu zámku bude nutné dveře trezoru nebo zabezpečené místnosti zdolávat velmi obtížně a nákladně hrubou silou. Zásadního zlepšení bezpečnosti ale bylo dosaženo, neboť zámek nemohl obejít nikdo z personálu banky, a tím se

snížil i počet vyloupení trezorů, neboť zločinci do té doby vydíráním nebo mučením získávali od pokladníků nebo ředitelů bank číselné kombinace k otevření sejfů.

Rozvoj kombinačních zámků byl vlastně vynucen překotným pokrokem v bankovnictví v 18. století. Prvními sejfy byly jen oplechované skříňky, opatřené často visacími zámky, které nebyly pro lupiče žádnou překážkou. Ani pozdější velké zabudované trezory před kasaři nic spolehlivě neuchránilo, neboť zločinci si zvykli strkat dynamit nebo jiné třaskaviny do klíčových dírek zámků, které následné explozi většinou neodolaly.

Ne všichni lidé schopní otvírat nedobytné pokladny ale přešli na špatnou stranu zákona. Příkladem může být Charles Courtney, už od dětství nadšenec pro mechanické stroje všeho druhu. Fascinovaly ho hlavně zámky, na něž se stal expertem. A když se ještě díky oblibě románu Julese Vernea Dvacet tisíc mil pod mořem stal potápěčem, zbývalo jen obě profese spojit. Byl tak prvním „lamačem zámků", který své řemeslo prováděl až 120 metrů pod hladinou. Na zakázku (a legálně) otevíral sejfy potopených a ztroskotaných lodí, aby bylo možné vyzvednout zde uložené cennosti. Pojišťovnám tak zachránil stovky milionů dolarů. Jako koníčka měl Courtney kupodivu opět zámky, tentokrát sbírání starých exemplářů – v obojím dosáhl světové proslulosti. ■

Tomáš Suchomel

Záštity

Primátor hl. m. Prahy RNDr. Tomáš Hudeček, Ph.D.
Ministerstvo kultury ČR
Kulturní atašé Amerického velvyslanectví v Praze
paní Sherry C. Keneson-Hall
Ministryně pro místní rozvoj České republiky
paní Věra Jourová

Pořadatelé

Art Movement o.s.

ghmp galerie hlavního města prahy city gallery prague

Jenny He & Tim Burton Productions

Hlavní partneři

PRA HA PRA GUE PRA GA PRA G

MINISTERSTVO KULTURY

Hlavní mediální partner

Česká televize

Mediální partner

Český rozhlas

Partneři

Allianz

Ligue Disney Prague

AMI COMMUNICATIONS

buddha-bar hotel PRAGUE

Clarion Hotel BY CHOICE HOTELS

US embassy

ZENIT

PRE

DNA!

SECURITY FOKUS
VĚDA
VÝZKUM
VÝVOJ
VZDĚLÁNÍ

MAPOVÁNÍ STAVU SEKTORU SOUKROMÝCH BEZPEČNOSTNÍCH SPOLEČNOSTÍ V ČR V POROVNÁNÍ S OSTATNÍMI EVROPSKÝMI ZEMĚMI A ČLENSKÝMI STÁTY SEVEROATLANTICKÉ ALIANCE

ANOTACE - V současné době probíhá v rámci Programu bezpečnostního výzkumu ČR na léta 2010–2015 BV II/2-VS Ministerstva vnitra České republiky aplikovaný výzkum „Metodiky řízení rizik a kvality služeb soukromého bezpečnostního sektoru ČR v rámci jeho domácího i mezinárodního působení a požadavků NATO" (dále Metodika).

***Klíčová slova:** robot, robotické pracoviště, riziko, laserový skener, optická clona*

Jedním z důležitých podkladů pro tvorbu Metodiky je výzkum v oblasti mapování současného stavu sektoru Soukromých bezpečnostních služeb (SBS) ve světě a v ČR. Takové zmapování představuje výchozí podklad pro další směřování výzkumu, a to zejména z pohledu zaměření Metodiky na aspekty chování zaměstnanců v sektoru soukromých bezpečnostních služeb i právnických osob podnikajících v tomto oboru.

Nedílnou součástí této části výzkumu je dále zmapování stavu legislativních úprav v jednotlivých zemích Evropské unie (EU) a členských států Severoatlantické aliance (NATO), míry takové regulace a sledování existence mezinárodních nebo národních standardů pro řízení kvality a řízení rizik v sektoru SBS.

V tomto kontextu byl také zkoumán přístup podnikatelů v rámci sektoru SBS k řízení rizik a kvality a jeho vliv na poskytované služby.

Hlavními prameny pro výzkum byla sonda provedená formou dotazníkového šetření v roce 2013, která oslovila 300 soukromých bezpečnostních a detektivních společností, a zpráva CoESS, *Private Security Service in Europe 2011* (kolektiv autorů); BUREŠ, Oldřich a kolektiv, *Privatizace bezpečnosti: České a zahraniční zkušenosti.* Praha, Grada Publishing, a.s., 2013, ISBN 978-80-247-4601-2 a dále vlastní zjištěná statistická data.

V současné době existuje pouze jeden národní standard (USA) zabývající se specificky sektorem SBS, který zároveň slouží jako srovnávací pro tvorbu samotné Metodiky (ANSI/ASIS PSC.1 – 2012 – *Management System for Quality of Private Security Company Operations – Requirements and Guidance,* ***ASIS International, 2012***, ISBN 978-1-934904-33-6). Tento standard byl v roce 2012 předložen ke schválení Evropské standardizační organizaci CEN v rámci Technické komise č. 391 – bezpečnost obyvatelstva, jako projekt k zavedení mezi evropské standardy, avšak byl hlasováním členských států CEN odmítnut jako příliš odpovídající legislativnímu, kulturnímu a politickému prostředí USA. V současné době je tento standard schválen jako projekt Mezinárodní standardizační organizace pro zavedení mezi tzv. ISO standardy.

NEEXISTENCE UCELENÝCH STATISTICKÝCH DAT KOMPLIKUJE MAPOVÁNÍ VÝCHOZÍ SITUACE V OBORU

V době spuštění projektu Metodiky neexistovala souhrnná statistika, ze které by bylo možné vycházet při tvorbě standardů a metodik řízení kvality nebo řízení rizik sektoru SBS. Vzhledem k tomu, že v ČR opakovaně dochází k obnovení přípravy neexistující zákonné regulace sektoru SBS (v současné době probíhá další kolo meziresortního připomínkování návrhu zákona o soukromé bezpečnostní činnosti a o změně souvisejících zákonů – finRZ26042014), je důležité znát současnou situaci v sektoru SBS. Znalost stavu sektoru SBS v ČR je pak nutné dát do mezinárodního kontextu především v EU, ale i v rámci členských států NATO.

Spojené státy americké se prostřednictvím ministerstva obrany vyjádřily, že budou vyžadovat při spolupráci se soukromými bezpečnostními společnostmi, aby řídily kvalitu poskytovaných služeb například na základě již zmiňovaného standardu. Takto specifikované požadavky pak mohou významně ovlivnit trh sektoru SBS v ČR.

Pro tvorbu Metodiky a úspěšné dokončení celého výzkumného projektu je důležité získat informace o přístupu soukromých bezpečnostních a detektivních společností k problematice řízení rizik a kvality jejich služeb.

KONCIPOVÁNÍ VÝZKUMNÝCH SOND

Výzkumná sonda

První výzkumná sonda byla uskutečněna v období od srpna 2013 do března 2014. Jejím cílem bylo získat základní informace o praxi soukromých bezpečnostních společností v oblasti řízení rizik a kvality poskytovaných služeb na trhu. Kvantitativní sběr dat proběhl prostřednictvím anonymního dotazníkového šetření. Výzkumný vzorek respondentů byl tvořen záměrným výběrem velkých, středních a malých společností působících na českém trhu. Přímým požadavkem i prostřednictvím aplikace jsme oslovili přes 300 soukromých bezpečnostních a detektivních společností (SBS).

Hypotézy (H1–H3) výzkumné sondy v oblasti SBS

H1. Většina SBS (nad 75 % odpovědí) bude vyhodnocovat rizika hrozící objektům a zájmům jejich klientů před přípravou nabídky služby.

H2. Většina SBS (nad 75 % odpovědí) bude mít zavedený reálný systém hodnocení kvality jednotlivých procesů pomocí kvantifikovatelných metod.

H3. Většina SBS (nad 75 % odpovědí) bude mít zavedeny prvky antikorupční politiky ve svých vnitřních dokumentech.

Struktura dotazníkového šetření v oblasti SBS

Dotazník se skládá ze 17 uzavřených (č. 1–3, 5–9, 11–16, 19–21), 2 polootevřených (č. 10, 22) a 3 otevřených otázek (č. 4, 17, 18). Otázky jsou také děleny dle kontextu odpovědí na povinně (č. 1, 2, 11, 12, 15, 17–22) a nepovinně (č. 3–10, 13, 14, 16) zodpovězené/zodpověditelné. Zaměřuje se na míru řízení kvality a rizik SBS v obecné i konkrétní rovině.

Ověřování hypotéz dotazníkového šetření v oblasti SBS

H1. Většina SBS (nad 75 % odpovědí) bude vyhodnocovat rizika hrozící objektům a zájmům jejich klientů před přípravou nabídky služby.
Většina soukromých bezpečnostních společností (konkrétně 100 % respondentských odpovědí) zodpověděla, že vyhodnocují rizika hrozící objektům a zájmům klientů před přípravou nabídky služby.
H1. se potvrdila.

H2. Většina SBS (nad 75 % odpovědí) bude mít zavedený reálný systém hodnocení kvality jednotlivých procesů pomocí kvantifikovatelných metod.
68,75 % respondentů má dle svého vyjádření zavedený reálný systém hodnocení kvality jednotlivých procesů pomocí kvantifikovatelných metod.
H2. se v tomto případě nepotvrdila.

H3. Většina SBS (nad 75 % odpovědí) bude mít zavedeny prvky antikorupční politiky ve svých vnitřních dokumentech.
Jen v 53,85 % případů respondenti odpověděli, že mají jejich SBS zavedeny prvky antikorupční politiky ve svých vnitřních dokumentech.
H3. se nepotvrdila.

Interpretace výsledků dotazníkového šetření v oblasti SBS

Celkem bylo dotazníkovým šetřením osloveno přes 300 soukromých bezpečnostních společností, což odpovídá stavu aktivních SBS na českém trhu z roku 2011 (viz týdeník Ekonom). Anonymita dotazníků snižovala riziko stylizace odpovědí ze strany respondentů, avšak dobrovolnost a nikoli nařízení zúčastnit se tohoto šetření se promítlo v počtu navrácených odpovědí. Dotazníkové šetření si zobrazilo 71 respondentů, z nichž 37 ihned skončilo, 17 respondentů dotazník začalo vyplňovat, ovšem neodeslali jej a zbylých 17 dotazník odeslalo ke zpracování. Úspěšnost v návratnosti dotazníku byla 23,94 %. Získané odpovědi lze z hlediska struktury trhu SBS, tedy široce zvolenému výzkumnému poli obsahující respondenty malých, středních i velkých společností působících v českém i zahraničním prostředí, považovat za reprezentativní vzorek současného stavu SBS v ČR.

Výzkumná sonda do neziskového sektoru

Od prosince 2013 do května 2014 probíhá sběr dat také prostřednictvím druhé výzkumné sondy, jejíž respondenti byli zvoleni záměrným výběrem. Jedná se o kombinaci kvalitativního šetření technikou dotazníků a zároveň kvalitativního šetření technikou řízených rozhovorů. Oslovili jsme zástupce těchto největších neziskových společností, které působí na českém trhu i v zahraničí: Člověk v tísni (NNO) a ADRA, o. p. s. Dále kontaktujeme menší společnosti podobného zaměření s predikcí možnosti využívání SBS.

Hypotézy výzkumné sondy do neziskového sektoru

H1. Největší neziskové společnosti, které působí na českém trhu, budou využívat (100 % odpovědí) při svých zahraničních aktivitách soukromé bezpečnostní služby.

H2. Většina respondentů (nad 75 % odpovědí) bude vyžadovat prokázání kvality služeb soukromé bezpečnostní agentury před dojednáním spolupráce.

H3. Většina respondentů (nad 75 % odpovědí) si vlastní analýzu rizik před dojednáním spolupráce s SBS dělá zřídka.

Struktura dotazníkového šetření do neziskového sektoru

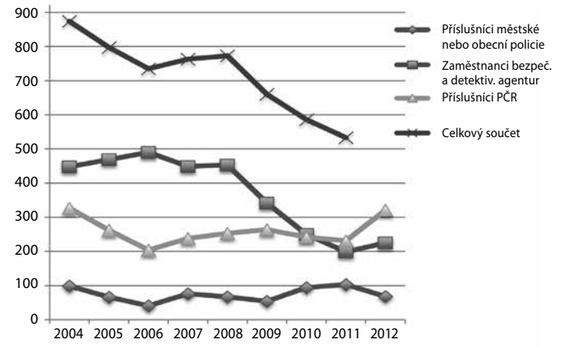
Dotazník se skládá ze 4 uzavřených (č. 2, 5, 6, 8), 1 polootevřené (č. 7) a 4 otevřených (č. 1, 3, 4, 9) otázek. Zaměřuje se na spokojenost a míru kvality využívaných služeb SBS.

Ověřování hypotéz dotazníkového šetření do neziskového sektoru

Po ukončení sběru dat výzkumnou sondou do neziskového sektoru, předp. konec května 2014.

Interpretace výsledků dotazníkového šetření do neziskového sektoru

Po ukončení sběru dat výzkumnou sondou do neziskového sektoru, předp. konec května 2014.
Na interpretaci výsledků sondy lze též pohlížet optikou nízké účasti respondentů. Takový přístup je způsoben jednak neexistencí povinnosti kvalitu a rizika řídit a dále výší nákladů, které takové řízení představuje.
Vzhledem k tomu, že sektor SBS v rámci EU a dalších zemí (převážně členských zemí NATO) představuje ročně obrat 35 miliard EUR, téměř 77 milionů pracovních hodin a v ČR zaměstnává více než 1 % všech pracovníků v soukromém sektoru obecně (O. Bureš), lze považovat znalost stavu v sektoru SBS za klíčovou.



Tabulka 1: Zdroj MVČR a GIBS – 2004–2013

TRESTNÁ ČINNOST ZAMĚSTNANCŮ SBS: ZÁVAŽNÝ PROBLÉM

V rámci zkoumání stavu sektoru SBS byly sestaveny statistiky trestných činů zaměstnanců SBS a porovnány s trestnou činností příslušníků Policie České republiky a Městských a obecních policií.

V posledních letech lze pozorovat nárůst dokonaných a objasněných trestných činů zaměstnanců SBS. Stav sektoru SBS dále ilustrují markantní rozdíly v objasněných trestných činech dle jednotlivých paragrafů Trestního zákona v letech 2004–2013. U silničních nehod z nedbalosti činil počet u SBS 213 a u příslušníků obecních policií 45, krádeže v objektech u SBS tvořily 146 objasněných případů, u obecních policií pouze 7, ohrožení pod vlivem návykové látky či opilosti činil počet objasněných trestních činů více než desetinásobek – u SBS 217 a u obecní policie 20.

Celkový poměr pak činí u zaměstnanců SBS 3 504 objasněných trestných činů a u obecních policií 719. Tato čísla dokládají nutnost řídit kvalitu a rizika v sektoru SBS.

Důležitým faktorem ovlivňujícím výše uvedené je i fakt, že v rámci Evropy představuje poměr počtu zaměstnanců SBS na deset tisíc obyvatel téměř stejné číslo jako počet policistů. Konkrétně: počet

STAV LEGISLATIVY DLE ÚROVNĚ REGULACE			
NÍZKÁ	**STŘEDNÍ**	**STRIKTNÍ**	**VELMI STRIKTNÍ**
ČESKÁ REPUBLIKA	LOTYŠSKO	FINSKO	ŠVÉDSKO
RAKOUSKO	VELKÁ BRITÁNIE	NORSKO	BELGIE
MALTA	IRSKO	ESTONSKO	LUCEMBURSKO
	FRANCIE	LITVA	MAĎARSKO
	NĚMECKO	DÁNSKO	SRBSKO
	BULHARSKO	NIZOZEMÍ	ŠPANĚLSKO
	KYPR	POLSKO	PORTUGALSKO
		SLOVENSKO	
		ŠVÝCARSKO	
		RUMUNSKO	
		ITÁLIE	
		SLOVINSKO	
		CHORVATSKO	
		BOSNA A HERCEGOVINA	
		MAKEDONIE	
		ŘECKO	
		TURECKO	

Tabulka 2: Zdroj CoESS – 2011

zaměstnanců soukromých bezpečnostních společností na deset tisíc obyvatel je průměrně 31 a naproti tomu počet policistů na deset tisíc obyvatel je průměrně 36.

ZÁKON O SBS: JSME JEDNI Z POSLEDNÍCH

V kontextu míry regulace patří Česká republika společně s Rakouskem a Maltou k nejméně legislativně specifickým zemím.

Zákonné regulace ve většině zemí Evropy představují především tzv. licencování prováděných činností, zahrnují například povinnosti splnění zdravotních, způsobilostních a fyzických testů, prokazování bezúhonnosti v pravidelných intervalech, vydávání osobních průkazů státní autoritou apod. V porovnání se zeměmi s nízkou nebo střední mírou regulace sektoru SBS pak mají zaměstnanci SBS pravomoci, které jsou nad rámec pravomocí běžného občana. Například v Belgii mají pracovníci SBS možnost zadržet osobu podezřelou ze spáchání trestného činu (do příjezdu policie), nebo dokonce provést prohlídku osoby.

SOUČASNÝ STAV SEKTORU SBS JE VÁŽNÝM OHROŽENÍM BEZPEČNOSTI A TRHU SBS V ČR

Na základě dosavadních výsledků lze konstatovat, že sektor SBS je v neutěšeném stavu a jeho regulace na legislativní úrovni je více než žádoucí. Na druhé straně je markantní nezájem o problematiku řízení rizik a kvality, kde tato situace je způsobena především výší nákladů. Navíc neexistuje jakákoliv metodika pro zavedení systému řízení v podmínkách ČR a EU.

Pro trh v rámci sektoru SBS je setrvání v současném stavu vážným ohrožením, protože pokud SBS nezareagují na požadavky NATO (kde nejvýznamnější roli hrají USA) v rámci řízení kvality, mohou se připravit nejen o příležitosti poskytovat služby pro NATO a organizace USA ve světě, ale i v ČR. Dokladem této skutečnosti je sčítání Ministerstva obrany USA, které uvádí, že v Iráku působilo 180 000 příslušníků SBS v porovnání s celkovým počtem 160 000 příslušníků regulérních jednotek armády USA ve stejnou dobu (O. Bureš, R. Makariusová, Z. Ludvík).

V rámci pokračujícího aplikovaného výzkumu Metodiky bude v nejbližší době provedeno vyhodnocení sondy v rámci klíčových uživatelů služeb SBS v oblastech s probíhajícím válečným konfliktem. Těmi jsou neziskové organizace zaměřující se na poskytování humanitární pomoci.

Mgr. Milena Bačkovská
(řešitelka projektu, Ministerstvo vnitra České republiky, odbor bezpečnostní politiky) – statistika trestné činnosti sektoru SBS a příslušníků Policie České republiky a Městských a obecních policií, stav legislativních úprav v EU.

JUDr. Ivo Chauer
(řešitel projektu, Ministerstvo vnitra České republiky, odbor bezpečnostní politiky) – statistika trestné činnosti sektoru SBS a příslušníků Policie České republiky a Městských a obecních policií, stav legislativních úprav EU.

Mgr. Radek Zapletal
(řešitel projektu a člen oborové neziskové organizace Security Club, člen Sektorové rady Hospodářské komory České republiky) – dotazníkové šetření u 300 soukromých bezpečnostních a detektivních společností.

Mgr. Veronika Matějková
(řešitelka projektu, Pinkerton ČR, s.r.o.) – dotazníkové šetření a vyhodnocení provedené sondy, mapování stavu sektoru SBS ve světě.

Lukáš Moravec
(řešitel projektu, Pinkerton ČR, s.r.o., člen CEN TC 391) – vyhodnocení výsledků sondy a kontext v oblasti mezinárodních standardů, vyhodnocení statistických dat.

Seznam použité literatury

CoESS: *Private Security Service in Europe 2011 – kolektiv autorů*, www.coess.eu

BUREŠ, Oldřich, a kolektiv: *Privatizace bezpečnosti: České a zahraniční zkušenosti*. Praha, Grada Publishing, a.s., 2013, ISBN 978-80-247-4601-2

ANSI/ASIS PSC.1 – 2012 – *Management System for Quality of Private Security Company Operations – Requirements and Guidance*, **ASIS International, 2012**, ISBN 978-1-934904-33.

MAKARIUSOVÁ, Radana, LUDVÍK, Zdeněk: *Case Study on the Role of Non-State Military Actors in the 2011 Libyan Conflict / Působení soukromých aktérů: Případová studie libyjského povstání 2011* (CEJISS 3-4/2012; společně s vedoucím disertace).

NEDVĚDICKÁ, Vendula: *Využívání služeb vojenských a bezpečnostních společností nevládními organizacemi,* DOI: 10.5817/CEPSR.2013.23.149, www.cespr.cz.

Návrh zákona o soukromé bezpečnostní činnosti a o změně souvisejících zákonů – (finRZ26042014), www.vlada.cz

AXIS COMMUNICATIONS

Doma mám HD televizi již řadu let.

A nyní máme v HD také naše parkoviště.

Díky síťovým kamerám Axis s HD rozlišením můžeme pracovat s velmi ostrým a detailním obrazem celého našeho objektu. Máme tak dokonalý přehled o veškerém dění jak venku, tak i uvnitř. Naše možnosti identifikace osob, vozidel i objektů jsou teď nesrovnatelně lepší - a to i na velkou vzdálenost. Pokud se, stejně jako já, staráte o bezpečnost celého parkoviště, věřte mi, že to opravdu oceníte.

Další informace o HDTV, použitelnosti obrazu a dohledovém řešení stvořeném přímo pro vás naleznete v interaktivním průvodci Axis na stránkách
www.axis.com/imageusability

Snižujeme ceny. Úspěšné projekty.

Odstartujte právě teď se společností Samsung Techwin.

Snižujeme už tak atraktivní ceny celé řady našich analogových výrobků. Žádné časové omezení, žádný jarní nebo letní výprodej, prostě už napořád. Digitální videorekordéry se 4, 8 a 16 kanály, kamery pro vnitřní i venkovní použití, dome kamery a širokou škálu příslušenství. Stručně řečeno: Vše co potřebujete k pořízení profesionálního videomonitorovacího systému. Tak na co čekáte? Další projekt se společností Samsung Techwin už na vás čeká!

Využijte příležitost ke kalkulaci úspěšného projektu. Odstartujte právě teď se společností Samsung Techwin.

Your Smart Security Solution

Chcete se o našich výrobcích dozvědět více nebo potřebujete pomoct s vaším projektem?
Pak nás kontaktujte, prosím! Rádi vám pomůžeme!

Webový server: www.samsungsecuritysolutions.cz
E-mail: mirek.ptacek@samsung.com / Telefon: 602 161 424
Trainings: www.samsungsecuritysolutions.cz/cs-cz/training.aspx

SAMSUNG TECHWIN

SAMSUNG