ELEKTRONICKÉ ZABEZPEČOVACÍ SYSTÉMY

TEORIE

Ochranu objektu lze dělit na mechanickou a elektronickou.

Mechanická ochrana objektu

Mechanické zabezpečení tvoří všechna zařízení nebo předměty, které svojí přítomností ztěžují proniknutí do prostoru nebo objektu. Jsou to například dveře, zámky, brány, fólie na sklo, ploty, ostnaté dráty a spousta dalších technických prostředků. Záměrně bylo řečeno, že mechanické prostředky průnik do objektu pouze ztěžují, protože zcela zabránit jejich překonání nelze. Pro provoz mechanické ochrany nejsou zpravidla již potřebné žádné další finanční náklady.

Elektronická ochrana objektu

Elektronická ochrana je tvořena senzory nebo detektory reagujícími na narušení nebo na přítomnost osoby. Při detekci poplachu je spuštěna reakce systému, která upozorní na poplachový stav odbornou obsluhu, jež problém vyřeší. Součástí elektronického zabezpečovacího systému je vždy akustická siréna s vysokou hladinou hluku, která výrazně upozorní na stav narušení a zároveň má pachatele odradit od pokračování v trestné činnosti.

Nicméně je dnes ve velké míře využívána účinná komunikace systému s uživatelem a/nebo s již výše zmiňovanou odbornou obsluhou. Uživatel dostává zprávu o poplachu na mobilní telefon, ale velmi doporučován je zejména přenos kódované zprávy bezpečnostní agentuře, která provozuje tzv. pult centrální ochrany (PCO) a dokáže zajistit v krátké době i odborný zásah. Výhodou přenosu zpráv na odborné pracoviště je vedle aktivního postupu proti narušiteli i to, že stav elektronického zabezpečovacího systému je soustavně monitorován.

Kombinovaná ochrana objektu

Při ochraně objektu je vždy potřeba kombinovat mechanické a elektronické zabezpečení. Při návrhu zabezpečení je potřeba: **ZTÍŽIT PŘÍSTUP – DETEKOVAT NARUŠENÍ – ZAJISTIT VČASNÝ ZÁSAH.** Pouze dodržením těchto tří zásad lze efektivně chránit vás i váš majetek.

INSTALACE ELEKTRONICKÉ OCHRANY OBJEKTU

SVÉPOMOCÍ

Instalaci elektronické ochrany svépomocí nelze vůbec doporučit. Jedná se o velmi složitý soubor úkonů začínajících bezpečnostní analýzou daného objektu a pokračujících návrhem systému, výběrem odpovídající technologie, HW zapojením a zakončených SW programováním a oživením. Jedná se o zcela specifický elektronický systém řídící se vlastními pravidly instalace a technickými normami. Oživení a nastavení systému je složité a vyžaduje odborné znalosti zapojení a programování.

KVALITNÍ ELEKTRONICKÉ ZABEZPEČENÍ NEMŮŽE INSTALOVAT NEKVALIFIKOVANÁ OSOBA

UŽIVATEL – INSTALAČNÍ FIRMA

Určitě se obraťte se svými požadavky na zabezpečení na instalační firmu. Instalační firma má proškolené techniky s certifikátem pro instalaci daného bezpečnostního systému. Provede všechny kroky spojené s nasazením elektronického bezpečnostního systému od analýzy až po odborné zaškolení obsluhy.

PARAMETRY ZABEZPEČENÍ DEFINUJE INSTALAČNÍ FIRMA - UŽIVATEL

UŽIVATEL - INSTALAČNÍ FIRMA - PCO (pult centrální ochrany)

Pokud bude z objektu zajišťován přenos dat ze systému elektronické ochrany na PCO, je potřeba se nejdříve informovat, jestli PCO nemá nějaké další požadavky na vlastnosti systému. PCO přebírá odpovědnost za zásah po poplachu a ve smluvních podmínkách může být i specifikace vlastností systému. Toto musí při návrhu zohlednit instalační firma a uživatel.

PARAMETRY DEFINUJE INSTALAČNÍ FIRMA – UŽIVATEL A POŽADAVKY MŮŽE VZNÁŠET I PCO

UŽIVATEL – INSTALAČNÍ FIRMA – POJIŠŤOVNA

Při pojištění objektu je charakter zabezpečení již přímo dán pojišťovací smlouvou. Instalační firma a uživatel musejí při návrhu a jeho provedení zohlednit předpisy pojišťovny a její podmínky pro danou úroveň finančního plnění. Od jednání s pojišťovnou se tedy bude odvíjet charakter elektronického zabezpečení a volba jednotlivých prostředků.

PARAMETRY ZABEZPEČENÍ DEFINUJE POJIŠŤOVNA

PARADOX®
SECURITY SYSTEMS

ELEKTRONICKÉ ZABEZPEČOVACÍ SYSTÉMY

ANALÝZA

Správná bezpečnostní analýza je velice důležitým krokem pro ochranu majetku a osob, ale i pro zajištění spokojenosti uživatele při používání systému. Je nezbytné, abyste Vy jako uživatel přesně definoval své potřeby a také požadavky, které má zabezpečení poskytnout. V konzultaci s instalační firmou dojde ke sladění Vašich požadavků s možnostmi navrhovaného systému. Instalační firmy mají zkušenost s různými typy objektů a různými systémy zabezpečení. Jsou proto schopné Vám navrhnout vhodný režim užívání i systém, který pro danou aplikaci bude nejlépe vyhovovat.

REŽIM UŽÍVÁNÍ - OVLÁDÁNÍ

Každý systém, ať už mechanický nebo elektronický, vnáší do užívání objektu jistá pravidla, která je nutné dodržovat. U mechanické ochrany se jedná o uzamknutí dveří či používání branky v plotu a situace je uživatelsky poměrně jednoduchá. U elektronických systémů je režim užívání definován přísněji. Je potřeba systém kvalifikovaně zapínat / vypínat, používat příchodové a odchodové trasy a dodržovat další postupy, které zabezpečení vyžaduje. S tímto režimem je potřeba počítat a nechat si jej od instalační firmy navrhnout a podrobně vysvětlit. Pro rodinný dům je situace poměrně přehledná, ale v okamžiku, kdy je v objektu například několik samostatných firem, mají společné parkoviště a společnou chodbu, může být situace komplikovanější.

Vstupní trasa

Elektronický bezpečnostní systém má přesně definovanou přístupovou trasu a čas, do kterého je potřeba od první detekce vypnout systém. Již vlastním návrhem a instalací je potřeba omezit vznik falešných poplachů vinou obsluhy. Z těchto důvodů se jako první detektor volí vždy magnetický kontakt na dveřích. Otevření dveří aktivuje čas pro zadání kódu. Narušení jiného detektoru než magnetického kontaktu jako prvního ihned spustí poplach.

KAŽDÉ ZABEZPEČENÍ VYTVÁŘÍ PRAVIDLA PRO UŽÍVÁNÍ OBJEKTU

DETEKTORY

Všechny detektory pracují na vyhodnocování fyzikálních veličin. I když jsou detektory po technické stránce na vysoké úrovni, je potřeba počítat s jistými omezeními. Problémem může být například detekce v místnosti, ve které se pohybují domácí zvířata nebo jsou zde umístěny teplé předměty (kamna, horkovzdušné topení). Je potřeba si uvědomit, že způsob detekce neumožňuje rozlišit dva velké psy od pohybující se postavy. Problém rovněž způsobují závany teplého vzduchu. S těmito a dalšími podobnými omezeními je potřeba počítat již při návrhu a volit vhodné řešení detekce. Použití detektorů vždy uvádí výrobce a jejich vhodnou volbu Vám doporučí instalační firma.

KAŽDÝ DETEKTOR MÁ SVÉ FYZIKÁLNÍ LIMITY

OVLÁDÁNÍ JINÝCH TECHNOLOGIÍ

Elektronické zabezpečení se kromě vlastního hlídání velice často používá i pro ovládání dalších technologií (bezdrátové ovládání garážových vrat, vjezdové brány). V těchto případech je potřeba dodržovat zásadu, že tyto technologie výhradně ovládá elektronické zabezpečení. Z hlediska bezpečnosti je nepřípustné, aby zabezpečení bylo ovládáno těmito technologiemi (například vypínat systém z ostrahy přes dálkové ovládání ke garážovým dveřím).

Ovládání klíčenkou – velmi často se jedná o ovládání vně systému. Pokud není klíčenka obousměrná (přímo na těle klíčenky se zobrazuje stav systému), je vhodné o stavu systému zpětně uživatele informovat. Toto se provádí externí světelnou nebo zvukovou signalizací. Houknutí / bliknutí 1x zapnuto, houknutí / bliknutí 2x vypnuto. Pokud se klíčenkou ovládají například garážová vrata, je nutné zajistit, aby nešla otevřít při zapnutém systému. Pokud bude garáž v režimu hlídání, může ústředna blokovat otvírání garážových dveří a znemožní tím vstup do hlídaného prostoru. Tímto je vyloučena chyba obsluhy.

ELEKTRONICKÉ ZABEZPEČENÍ NADŘADIT OSTATNÍM TECHNOLOGIÍM

DRÁT / BEZDRÁT

Základní otázkou při výběru systému je, zda zvolit DRÁTOVÝ nebo BEZDRÁTOVÝ přenos signálu mezi detektorem a vyhodnocovací ústřednou. Tuto volbu doporučujeme probrat s instalační firmou, ale předem upozorňujeme, že nejjednodušší řešení nebývá tím nejlepším.

DRÁT

I přes značný technologický pokrok v bezdrátové komunikaci je drátové propojení mezi detektorem a ústřednou tím nejjistějším a nejspolehlivějším řešením. Drátové propojení ale vždy vyžaduje stavební zásah do objektu. Prvotní náklad na provedení instalace se mnohonásobně v budoucnu zúročí nízkými požadavky na údržbu detektorů a absolutní spolehlivostí přenosu signálu. Pokud to jen trochu jde, doporučujeme dát drátovému řešení přednost.

BEZDRÁT

Pokud je elektronické zabezpečení instalováno do již hotového objektu bez možnosti zasekání vodičů, je potřeba volit bezdrátový přenos. Systém PARADOX umožňuje volit přenos na dvou frekvencích - 433MHz a 868MHz. Přenos signálu je velmi spolehlivý a detektory předávají informace o poplachu i o stavu baterií. I přes technickou pokročilost detektorů je potřeba počítat s výměnou baterií v detektorech asi 1x za 2 roky a dávat pozor na to, aby v daném frekvenčním pásmu nebyly instalovány jiné technologie a nedocházelo tak k rušení.