



## Trendy, ktoré budú dominovať v roku 2012 (1)

Odborný časopis a&s International zisťoval medzi poprednými lídrami z priemyslu, aké trendy alebo fenomény môžu čitatelia očakávať v roku 2012 v oblasti automatizácie a bezpečnosti budov. Vzhľadom na nízku výkonnosť ekonomiky je preukazovanie rýchlej návratnosti investícií dôležitejšie ako kedykoľvek predtým.

### Schneider Electric: 12 trendov pre rok 2012

Riaditeľ vývoja bezpečnostných riešení pre budovy zo spoločnosti Schneider Electric Aaron Kuzmeskus vybral 12 dôležitých trendov. Pre čitateľov nie je žiadnou novinkou, že globálna ekonomika sa zviecha len veľmi pomaly. Riaditelia zodpovedajúci za bezpečnosť a prevádzku budov sa zároveň boria s riešením náročných výziev a obmedzenými finančnými možnosťami. Každý hovorí o návratnosti investícií (ROI) – no ako možno zlepšiť celkové výsledky hospodárenia? V nasledujúcej časti je opísaných 12 oblastí, ktoré stoja za povšimnutie.

**1. Dosiahnutie rýchlej návratnosti investícií** – ukážte vedeniu spoločnosti prínosy bezpečnostných riešení vzhľadom na celkové fungovanie spoločnosti. Využívajte bezpečnosť ako nástroj na realizovanie podnikania, nasadte bezpečnostné riešenia s cieľom zlepšovať iné procesy – od výrobných cez starostlivosť o pacientov až po vzdelávanie. Posuňte bezpečnosť z nákladového do výnosového strediska v účtovníctve.

**2. Prispôbitelnosť.** Budovy musia byť v súčasnosti prispôbitelné, inteligentné, energeticky úsporné a bezpečné a musia zabezpečovať komfort. Tieto požiadavky možno splniť výberom riadiaceho systému, ktorý svojou funkcionalitou prekračuje potreby dneška, a nasadením perspektívnych technológií umožňujúcich robiť úpravy, ktoré si vyžiada zajtrajšok.

**3. Integrácia.** Riadiace stredisko bezpečnosti je pri zabezpečení ochrany budovy odkázané na mnohé iné aplikácie. Každá z nich – od riadenia prístupu a video dohľadu až po detegovanie nepovolaných prienikov, hlasových služieb alebo biometrického prístupu – má často svoje vlastné používateľské rozhranie, spôsob

reportovania a kontrolných záznamov. Vyberte si preto systém, ktorý má všetky tieto aplikácie prepojené, čím ušetríte náklady na jednotlivé zariadenia, spotrebu energie a prevádzkové náklady.

**4. Schopnosť vzájomnej spolupráce.** Softvér na riadenie bezpečnosti a správu budovy dokáže automaticky zistiť a komunikovať s kompatibilnými zariadeniami na úrovni IP protokolu, a to bez potreby komunikačnej brány. Z hľadiska bezpečnosti a automatizačných systémov budov to znamená významnú úsporu nákladov, ktorá vyplýva z jednoduchšej architektúry systému, menšieho rozsahu hardvéru, jednoduchšej softvérovej konfigurácie a celkovej prevádzky a údržby systému.

**5. Jednoduchosť, zrozumiteľnosť.** Prispôbitelné používateľské rozhranie s menu zostavenom podľa jednotlivých úloh je jednoduché a intuitívne a odzrkadľuje typické bezpečnostné situácie z reálneho života. Ak sa v rozhraní podarí skombinovať aj riadenie pracovných postupov podľa jednotlivých pracovných pozícií, možno výrazne skrátiť čas zaškolenia a vykonávať prevádzku podstatne efektívnejšie, s vyššou produktivitou a maximálne obmedziť dodatočné zmeny systému.

**6. Zelená bezpečnosť.** Prepojte riešenie bezpečnosti s automatizáciou budovy a dosiahnete vyššiu energetickú účinnosť a bezpečnosť. Kľúčom je, že bezpečnostný systém vie, keď sa v budove/miestnosti niekto vyskytne a kto tá osoba je. Využite tieto informácie v rámci softvéru na správu budovy a vytvorte nové rutiny na využívanie energií. Postupne to povedie k úsporám energií.

**7. Spôľahlivosť.** Systémy, ktoré majú takú vlastnosť, že dokážu presunúť inteligenciu na zariadenia na najspodnejšej úrovni riadenia, prinášajú najvyšší stupeň svojej spoľahlivosti. Regulátory, na ktorých môžu bežať programy, logika, časovanie a plánovanie

úloh, generujú trendy alarmov a udalostí, udržiavajú požadovanú úroveň prevádzky – a to aj pri prerušení komunikácie so serverom.

**8. Systémy využívajúce IT technológie** sú základom spoločného využívania informácií v geograficky rozľahlých prevádzkach, čo umožňuje ich globálne fungovanie. Mnohé systémy dokážu fungovať v bežne dostupnej IT infraštruktúre a zrušiť tak náklady na prekáblovanie oddelených systémov.

**9. Bezdrôtové technológie.** Pokročilé kryptovanie a samonastavujúce sa siete možno už v súčasnosti nasadiť oveľa rýchlejšie a cenovo výhodnejšie ako káblové riešenie a to bez toho, aby sme znížili bezpečnosť alebo spoľahlivosť siete.

**10. Hostovanie (cloud).** Všetci hovoria o hostovaných riešeniach. Čo to je? Jednoducho povedané, ide o spoločne využívanú službu poskytujúcu úložisko údajov alebo určitú veľkosť spracovania vo virtuálnom prostredí. Pre tých, ktorí chcú takéto služby využívať, to znamená menej nákladov a v mnohých prípadoch aj dlhší čas bezporuchovej dostupnosti služieb.

**11. Analytika.** Analýza obrazu môže byť veľmi efektívny nástroj na maximalizáciu prevádzkového výkonu. Analýza môže napomôcť identifikovať obraz, ktorý by mal byť na základe istých aktivít monitorovaný. Analýza takisto ponúka výkonný forézny nástroj.

**12. Povedomie.** Správa bezpečnostných informácií je výkonný nástroj. Spojenie viacerých rôznorodých zdrojov do jednej množiny informácií prináša vysokú účinnosť a spoľahlivosť, a to v rámci celého podniku.

### **Johnson Controls: 12 trendov pre automatizáciu a bezpečnosť budov**

V roku 2012 si ešte viac podnikateľských subjektov vyskúša, ako prevádzkovať a chrániť budovy a ich nájomníkov. Oveľa väčší dôraz sa bude dávať na návrh zelených budov a obnovu tých starších tiež týmto smerom. Andre Greco, riaditeľ predaja Divízie bezpečnostných a požiarnych riešení v spoločnosti Johnson Controls, sa bez

pomoci sklenenej gule pozrel do budúcnosti na trendy, ktoré nás očakávajú v roku 2012.

**1. Lepšia integrácia systémov v budovách.** Platformy postavené na otvorených technológiách, zbierajúce a riadiace údaje z rôznych oddelených systémov a zdrojov zlepšia účinnosť prevádzky budov. Aplikácie využívajúce hostovanie služieb (cloud) sa stanú ďalšími nástrojmi na zvýšenie účinnosti. Získané údaje, ktoré budú dostupné na jednom zdrojovom mieste, uľahčia operátorom akejkoľvek nehnuteľnosti dosiahnuť jej lepší výkon.

**2. Integrácia automatizačných a bezpečnostných systémov v budove.** Možnosť monitorovať a riadiť teplotu, osvetlenie a spotrebu vody spolu s bezpečnostnými funkciami z jedného počítača môže pomôcť manažerom zvýšiť celkovú úžitkovosť nehnuteľnosti.

**3. Riadenie informácií o fyzickej bezpečnosti (PSIM – Physical Security Information Management).** Hovorí sa tomu aj bezpečnosť pod drobnohľadom. Riešenia PSIM využívajú sofistikovaný softvér na zachytenie a analýzu množstva údajov zo samostatných bezpečnostných systémov – video dohľad, riadenie prístupu, detekcia narušenia a iných snímačov. Údaje sú prezentované prostredníctvom intuitívneho grafického používateľského rozhrania, ktoré zvyšuje prehľadnosť o situáciách a v prípade bezpečnostných narušení pomáha používateľom lepšie sa rozhodovať.

**4. Zvýšený záujem o certifikáciu so štatútom „Zelená budova“.** Prevádzkovatelia budov sa pomocou zlepšení v oblasti znižovania spotreby energií, prevádzkových a investičných nákladov a vnútorného prostredia nových aj starších nehnuteľností snažia o získanie certifikátu LEED (Leadership in Energy and Environmental Design). Štúdiá vykonaná v Austrálii ukázala, že majitelia zelených budov môžu vo všeobecnosti stanovovať vyššie nájomné a menej neobsadených plôch.

**5. Reakcia na požiadavky (Demand Response-DR).** Technológie poskytujú manažerom a prevádzkovateľom budov informácie v reálnom čase, ktoré pomáhajú lepšie riadiť spotrebu elektrickej energie a generujú najväčšie úspory. Programy DR pomáhajú znížiť spotrebu



elektrickej energie v časovom úseku, keď dodávateľ elektrickej energie hlási, že rozvodná sieť sa dostala do blízkosti špičkového odberu, keď sú ceny energie pre odberateľov vyššie. Špičkové zaťaženie siete môže spôsobiť jej výpadok alebo znížiť jej výkon.

**6. Vzdelávanie.** Súkromné spoločnosti vzdelávajú novú generáciu technikov a inžinierov, ktorých doménou budú zelené budovy. Sponzorované programy prezentujú žiakom základných škôl hodnoty trvalo udržateľného rozvoja, stredoškôlaci zasa získavajú počas letných praxí vedomosti o spôsobe uskladňovania energie. Tento proces pokračuje na vysokej škole, kde študenti v rámci praktických cvičení získavajú skúsenosti z reálnych projektov využívania obnoviteľných zdrojov energií.

**7. Partnerstvo verejného a súkromného sektora.** Tieto partnerstvá vznikajú s cieľom nájsť a vytvárať energiu – a projekty úspory vody sú dobrým príkladom obojstranne víťazných riešení.

**8. Vzájomná komunikácia mobilných zariadení** – táto technológia umožňuje používať smart mobilné telefóny ako prístupové karty, pričom sa podstatne zvýši bezpečnosť. Uzamykací systém, ktorý sa dokáže spárovať so smart mobilným telefónom je lacnejší ako štandardná čítačka kariet, dokonca takýto systém dokáže vytvárať kontrolný záznam o tom, kto a kedy vstúpil do nejakého priestoru alebo použil nejaké zariadenie.

**9. Riadenie prístupu davu ľudí.** Nové systémy na báze počítačov dokážu pripojiť prevádzkovateľov štadiónov na webový portál, kde si fanúšikovia môžu zakúpiť lístky a zaregistrovať sa na najbližší zápas. Turnikety spolu s biometrickými, bezdotykovými a čiarovými čítačkami umiestnenými na vstupoch do štadióna rýchlo spracujú desiatky tisíc ľudí, dokážu ich porovnať s policajnými databázami a zakázať prístup problémovým osobám.

**10. Systém jednej karty pre fyzickú aj logickú bezpečnosť.** Vývoj pomaly, ale isto konverguje k systémom jednej karty umožňujúcej vstup do verejných alebo súkromných priestorov alebo do podnikovej siete. Zvyšuje sa tým aj bezpečnosť počítačov, tlačiarní a iných

externých zariadení. Inteligentné čipy na kartách umožňujú pridať aj biometrické identifikátory – odtlačok prstu či sken očnej dúhovky.

**11. Kamery s vysokým rozlíšením.** Koncoví používatelia aj súdy požadujú od video systémov čoraz viac informácií. Video s vysokým rozlíšením dokáže poskytnúť kontrastné a ostré obrázky, vďaka ktorým možno vykonať lepšiu identifikáciu a vyhodnotenie scény.

**12. Otvorené štandardy.** Po vzore komunity z oblasti informačných technológií aj riaditelia pre otázky bezpečnosti žiadajú otvorené štandardy pre zariadenia od kamier až po prístupové čítačky kariet. Otvorené štandardy dokážu chrániť vynaložené investície do pôvodných systémov a umožňujú pohodlne pridávať aj nové technológie.

V druhom pokračovaní článku sa pozrieme na to, aké trendy pre rok 2012 predpovedajú Magali Epin a Achim Schaepper zo spoločnosti Siemens pre oblasť budov.

## Literatúra

[1] Greco, A.: 12 Building Automation and Security Trends for 2012, Johnson Controls. Publikované online na <http://www.asmag.com/showpost/12557.aspx>, 27. 12. 2011.

[2] Kuzmeskus, A.: 12 for 2012, Schneider Electric. Publikované online na <http://www.asmag.com/showpost/12561.aspx>, 28. 12. 2011.

-tog-