

Beléptető rendszerek üzemeltetése a gyakorlatban

**A CIKK FILKORN JÓZSEF AZ MBVE KONFERENCIÁN,
2010. MÁJUS 25-ÉN ELHANGZOTT ELŐADÁSA ALAPJÁN KÉSZÜLT**

A Seawing Kft. műszaki igazgatójaként, mely a hazai piac legnagyobb beléptetőrendszer-gyártója, rálátásom van több száz általunk telepített, illetve partnereink által üzembe helyezett beléptető rendszerre, melyek üzemeltetéséhez műszaki segítséget adunk.

Az utóbbi időben megszorodtak azok a kérések is, hogy mások által gyártott beléptető rendszereket is segítsünk működtethető állapotba hozni.

Az így szerzett tapasztalatok késztettek arra, hogy a címben szereplő témát válasszam.

Miert kell az elektronikus vagyónvédelmi rendszerek üzemeltetésének tárgyalásánál külön kitérni a beléptető rendszerekre? Azért, mert a felhasználók a beléptető rendszer hibáira azonnal, és hevesen reagálnak.

Más vagyónvédelmi rendszereknél, ha kiesik egy elem, pl. nem működik egy kamera, hibás egy mozgásérzékelő, az kívülről nem látszik, az érzékelő kikapcsolásával (bypass) a hibát a javításig elfedheti az üzemeltető.

Ha egyetlen belépési pont nem működik, akkor azt vagy be kell zárni, és ki kell vonni a használatból, vagy folyamatosan nyitva kell tartani, és egyéb módon, például élőerős védelemmel kell gondoskodni az áthaladás ellenőrzéséről. Ez nem csak kényelmetlen, megbízhatatlan, de költséges is.

Az üzemeltetők előtt jól ismertek azok a nem rendszerhibának, csak hibás rendszerkezelésnek minősülő esetek, amikor csak bizonyos belépőkártyák belépési jogosultsága nem megfelelő.

Itt típuseset, amikor a cégvezetés egyik tagja akad fenn valamelyik átjárón, melyen egyébként eddig még soha nem közlekedett.

A fentiek egyenes következménye, hogy a beléptető rendszerek üzembiztonságával szemben magasabb követelményeket kell állítani, az esetleges hibákat gyorsan kell javítani.

Nehezíti a helyzetet, hogy a beléptető – elvileg – tisztán elektronikus kompo-

nenseket tartalmazó rendszerekkel – mindig tartalmaz elektromechanikus elemeket (mágneszár, forgóvilla, sorompó, stb.), melyek élettartama lényegesen kevesebb, karbantartásigénye nagyságrendekkel több.

Tovább nehezíti a helyzetet, hogy míg az egyéb vagyónvédelmi rendszerek felszerelése a napi folyamatokra nincs közvetlen hatással, addig a beléptető rendszer kiépítésekor mesterséges gátak kerülnek telepítésre, melyeken való áthaladás törvénytelenül akadályozza, nehezíti a mozgást.

A beléptető rendszerrel a védett területen tartózkodók közvetlenül találkoznak, és használata mindenkinek jelent kisebb-nagyobb kényelmetlenséget. A rosszul tervezett rendszerrel, esetlegesen aláméretezett kapacitással kapcsolatos véleményüket ritkán rejtik véka alá...

A megkövetelt biztonság, és a kényelmes használat ellentmondását már a tervezéskor figyelembe kell venni.

Az akadályozó szerkezet alaptípusának és számának kiválasztását a megkövetelt biztonság és a szükséges átbocsátó kapacitás determinálja. El kell dönten, kell-e szingularizáció (pl. ajtózár, vagy forgóvilla)? Milyen szintű a védelem az illegális behatolással szemben (pl. forgóvilla, vagy teljes magasságú forgókereszt)? A szükséges kapuszámot, a megkövetelt átbocsátó képesség alapján a csúcsterhelésre kell méretezni, és fő/perc vagy jármű/perc értékben kell megadni. És akkor jön még

a belsőépítész, akivel a kapuk formai megjelenítését kell egyeztetni, figyelembe véve rendelkezésre álló költségkeretet.

A tervezést csak olyan szakember végezheti, aki rendelkezik a megfelelő képzettséggel s tudással, szerepel a mérnökkamarai és vagyónvédelmi kamarai tervezői névjegyzékben.

Egyetlen feleslegesen felszerelt forgóvilla sokszorosan többbe kerül, mint a tervezési díj! Itt lehet elkövetni a legnagyobb baklövéseket is. Tudomásul kell venni, hogy olyan átjáróknál, ahol csúcsidőben percenként több száz ember halad át, felesleges és hibás olyan azonosítási technikát választani, mely bonyolult és lassú, mint például biometrikus azonosítás. Ráadásul ezek biztonságáról is sok a tévhit, de erről már többször ejtettünk szót.

Az azonosítás biztonságáról most nem beszélek, hiszen Pálffy Zoltán kollégám éppen ezt elemzi „**RFID és biztonság – 2010**” című cikkében (**lapunk következő számában publikáljuk. A szerk.**), de annyi ide kívánczok, hogy a proximity azonosítás önmagában már nem a biztonság záloga, és itt is van akkora különbség két rendszer között, mint kocsiiban a Trabant és a Mercedes között. És itt is igaz az „olcsó húsnak híg a leve” közmondás. A ma tömegesen kínált olcsó proximity megoldások zöméről a legendás „soproni zár” jut eszembe, ahol egy kulcskarikával egy egész lakótelepet lehetett nyitni.

Minimális elvárás a telepítendő rendszertől, hogy feleljen meg a vonatkozó szabványnak (MSZ-EN 50133), és legyen MABISZ minősítése. Tudjuk, hogy ezek néha csak formalitások, de ha egy rendszer szállítója még ezeket sem tartja be, akkor mi az a szint, melyet teljesíteni kíván? Naponta jutnak el hozzám is azok a hirdetések, melyekről már a reklámszöveg alapján is a szabvány alábbi félmondata jut eszembe: „akkor a gyártó írásos dokumentációjának világosan ki kell nyilvánítania, hogy a termék nem alkalmas egy beléptető felület alacsonyabb biztonsági szintű oldalán való használatra”.

Minél nagyobb a biztonsági rendszerek által védett érték – és itt már nem csak anyagi, hanem szellemi értékekre is gondoljunk – annál nagyobb a kísértés is azok kijátszására. Ha ez átlép egy szintet, akkor biztosan megjelenik az is, aki meg

tudja fizetni a biztonsági rendszer feltöréséhez szükséges tudást, vagy aki kihívásnak, szakmai bravúrnak tekinti azt.

Visszatérve a tervezéshez: Nagyobb létszámú csoportokat ellenőrző rendszer nem lehet meg szingularizált átjáró nélkül, ahol egy azonosításra csak egy áthaladás engedélyezett (pl. forgóvilla). Ez célszerűen az első ellenőrzési szint, ahol mindenkinek át kell haladnia, aki a védett területre érkezik. E nélkül a videomegfigyelő rendszerből a személy nem beazonosítható, főleg akkor, ha az elkövető jól ismeri a kamerák helyzetét.

A beléptetőrendszer technikailag leggyengébb pontjai a menekülési útvonalak. Ezek a menekülési irányból mindig nyithatóak mindenféle segédeszköz és azonosítás nélkül, és így „lyukak a sajton”. Hogyan lehet elkerülni ezek jogosulatlan használatát? Csak egy módon: az illegális használatot szankcionálni kell!

Nem elegendő csak a tervezésre figyelni. Rossz kivitelezéssel a legjobb rendszer is elrontható! Elrettentő példaként a saját eszközeinkből mutatok be két rémképet (1. és 2. kép).



1. kép



2. kép

Ezeket a kivitelezőket már töröltük a partnereink listájából, de ebből a rendszerből megbízható varázsolni nyilván csak teljes átépítéssel lehet.

Hogyan lehet a kivitelezőket előzetesen minősíteni? A vonatkozó törvények szerint vagyonvédelmi tevékenység végzéséhez szakképesítés, rendőrségi regisztráció és vagyonvédelmi kamarai tagság szükséges. A vagyonvédelmi cégnek vagyonvédelmi kamarai regisztráció szükséges. Ha a kivitelezésre vállalkozó ezeket nem tudja igazolni, szóba sem szabad állni vele. További lehetősége a megrendelőnek, ha elkéri a technológiai utasításokat, melyeket a kivitelezésnél be kívánnak tartani. Így elkerülhető, hogy olyan rendszert kapjunk, mint ami a 3. képen látható.

Ez egy városi fürdő exkluzívnak szánt bejárata.

De ez a rendszer belülről sem különb. Néhány illusztráció (4. és 5. kép).

Külön figyelmet érdemel a karikával jelzett



3. kép



4. kép



5. kép



6. kép



7. kép

„bedugós” tápegység 230 voltos csatlakoztatása (5. kép).

És ez még nem a legrosszabb. Láttam már olyat, hogy a kertkapuhoz egy ásonyom mélyen, UTP kábelben vitték a 230 V betápot együtt az adatvonallal.

Megrendelés előtt referenciákat kell kérni, és ezekből érdemes néhányat meglátogatni. Mutatok két kontrasztot (6. és 7. kép).

A két rendszernek természetesen különbözik az ára is. De ha számításba vesszük, ahogy az első két év után ki kellett dobni, mert párás környezetben a forgóvillák tönkrementek, és a fogaskerekekből kihulló rozsdazott az elektronikát is javíthatatlanul ➔

Beléptető rendszerek üzemeltetése a gyakorlatban

☞ tönkretette, akkor fajlagos költség tekintetében már a második megoldás nyer! A megrendelőt is minősíti, ha átvesz és kifizet ilyen kivitelezést (8. kép).

Venni kell a fáradságot, és az átadásakor bel kell nézni néhány dobozba (9. kép). Ha ilyet látunk, kezdjünk gyanakodni! Legalább ilyen fontos, hogy van-e szabotázsvédelem, a rendszer riaszt-e bármelyik elem megbontásakor?

Ellenőrizni kell a mellékelt dokumentációt. Itt két véglet a divatos: az egyikhez nincs semmi, a másikhoz több száz oldal semmitmondó prospektus másolat. A jó dokumentáció az egyetlen garancia, hogy a telepítőn kívül más is átláthassa a rendszert. Minimális elvárások: Műbizonylat, Garancialevél (ha nem szerződésben vállalt), Nyomvonalrajz szintenkénti lapra, Informatikai hálózat rajza (topológia), Belépési pont vázlatrajz, eszközök elhelyezése, kábelek nyomvonala, Szoftver adatlap (portkiosztás, paraméterezés), Bekötés áramköri rajzok (típusminták), Érintésvédelmi jegyzőkönyv.

Fontos a változások folyamatos követése a dokumentációban is, és meg kell oldani azok tárolását, hogy amikor szükséges, akkor hozzá lehessen férni, de ugyanakkor védett is legyen az illetéktelen betekintés ellen, hiszen a jó doku elárulja az Achilles sarkokat is.

A rendszer paraméterbeállításait elsőre nem könnyű eltalálni, azokat fokozatosan finomítani kell. Már a szerződésben ajánlott kikötni, hogy a próbaüzem után ez még a kivitelezés része legyen. Leggyakoribb hiba, amikor túl érzékenyre állítják a rendszert, és abból folyton dőlnek a riasztások, amikkel egy idő után egyáltalán nem foglalkoznak, vagy automatikusan törlik őket. Így a sok semmitmondó esemény között észrevétlenül maradnak az igen fontosak is. Alapszabály: a **riasztás emberi beavatkozási kérelem!** Az első időben feltétlenül erőt kell fordítani arra, hogy a nem kívánt eseményre elkövetőt közvetlenül érintő intézkedés történjen (betörjenek a felhasználók). Azok a kisebb vétségek, melyek tolerálhatóak nem kell riasztásnak, csak naplózandó



8. kép



9. kép

üzenetnek paraméterezni, így elkerülhető a kezelők túlterhelése, de szükség esetén visszakereshetőek. Ilyen például a jogosulatlan belépési kísérlet, hiszen érvénytelen kártyával úgy sem lehet belépni a védett térbe, de gyanú esetén kiszűrhető, hogy ki az, aki számára tiltott helyeken kísérletezik a bejutással. Típushiba még, hogy túl hosszú állítják a „szabályos belépés után nyitva maradt” jelzést. Ha ez 20 másodperc, akkor már régen messze van, aki nyitva hagyta az ajtót, és esélye sincs észrevenni és javítani, hogy begyűrődött a lábtörő.

Az üzembiztonság, a két meghibásodás közötti várható idő az eszközökre megadott paraméterek alapján számítható. Beléptető rendszerekben az elektromechanikus komponensek és az akkumulátorok a gyenge pontok, mert ezek nagyságrendekkel kisebb megbízhatóságúak, mint az elektronikus elemek. Itt a védekezés csak a rendszeres karbantartás, és az elhasználódás előtti csere. Az elektronikának a külső zavarok a gyenge pontjai. Ez lehet hálózati eredetű, a villámcsapások másodlagos hatásából, illetve a statikus

lyezettettségi szintnek megfelelő tervezés, a gondos kivitelezés.

A beléptető rendszernek vannak hasznos kiegészítői. Itt az off-line záratka említethetem, mint amilyen a Seawing OffLock termékcsaládja. Ezek illeszkednek az on-line rendszerhez, de ahhoz képest olcsó eszközök, korlátozott funkciókkal, de jelentősen képesek az irodai lopások kockázatát csökkenteni. Alkalmazásuk elsősorban az idegenek által is elérhető helyeken indokolt.

Végezetül a szoftvermentésről és archiválásról kell beszélni.

A mentés biztosítja a rendszerleállás, vagy számítógéhibá utáni gyors visszaállást. Célszerű automatikusra állítani, és a mentési hely feltétlenül másik gép adathordozójára történjen.

Az archiválás az aktív adatbázis méretének csökkentése, amikor egy időpontra régebbi elemeket egy archiv állományba mentenek. Elegendő fél évente, a rendszeres karbantartás idején elvégezteni. Ez biztosítja, hogy az adatbázis ne duzzadjon fel, és a rendszer ne lassuljon be, ugyanakkor, ha szükséges, akkor a régebbi adatok az archiv állományban továbbra is elérhetőek.

A számítógépek megbízhatósága elmarad a többi komponensétől, ezért kiemelt üzembiztonsági igény esetén lehetőség van párhuzamosan, akár nagyobb távolságban üzemelő szerverek használatára, hiba esetén automatikus átkapcsolással.

Beléptető rendszereknél is már van olyan struktúra, hogy nem csak a számítógépek lehetnek párhuzamosak, de a vezérlő egységből is kettő csatlakozik egy vonalra. A második vezérlő figyeli az adatforgalmat, és hiba esetén (másik vezérlő leállása, adatvonal-szakadás, stb.) átveszi a vezérlést. Ilyen a Seawing SC-1000 rendszere. Összefoglalva: Beléptető rendszer kivitelezésére adott ajánlatoknál az árat a műszaki tartalommal kell összevetni. A kivitelezőt még a megbízás előtt érdemes minősíteni. Az elkészült rendszert kritikusán kell átvizsgálni, melynek feltétele a használható dokumentáció is. A rendszerek üzemeltetésére érdemes szerződést kötni. Könnyen és hatékonyan kizárólag jól tervezett és jól kivitelezett rendszer alkalmas.

Filkorn József