

RISINĀJUMU | ĒRA

JAUNUMI
№ 20, JŪLIJS 2012



Tiem, kuri seko līdzīgu inženiertehnisku risinājumu tendencēm

Saturs

- **Ziņu lente** 2-3 lpp.
- **Vadības uzruna** „Fima” aizvadīts veiksmīgākais gads uzņēmuma vēsturē 2-3 lpp.
- **Jauns projekts** „Fima” speciālisti izbūvē Varšavas kardioloģijas institūta modulāro datu centru 4-5 lpp.
- **Sadarbības partneru jaunumi** Bagāžas pārbaude lidostās kļuvusi ātrāka un drošāka 5 lpp.
- **Intervijas** SEB bankas eksperti: efektīvas informācijas drošības pamatā ir kompleksi lēmumi un sabiedrības izglītošana 6-7 lpp.
- **Drošības labirinti** Uzņēmumi Eiropā arvien vairāk līdzekļu atvēl informācijas drošībai 8-9 lpp.
- **Tirgus tendences** Tehnoloģiju integrācija: jaunas iespējas transporta sektorā 10-11 lpp.

Ziņu lente

- ▶ Latvijā uzņēmums „Fima” ir parakstījis līgumu par **Starptautiskās lidostas „Rīga”** ārējā perimetra apsardzes sistēmām paredzētu iekārtu piegādi. Modernie risinājumi drošības jomā nodrošinās nepārtrauktu lidostas teritorijas videonovērošanu un nepiederošu personu vai objektu operatīvu identificēšanu.
- ▶ Lietuvā turpinās vērienīgā **platjoslas datu pārraides tīkla attīstības projekta RAIN-2** īstenošana, kurā piedalās arī kompānija „Fima”. Uzņēmuma speciālisti jau uzstādījuši iekārtas piekļuvei platjoslas sakaru līnijām vairāk nekā 1000 objektos visā Lietuvā; projekta ietvaros tiek izmantotas ASV ražotāja „Extreme Networks” augstas drošības pakāpes tīkla iekārtas.
- ▶ Latvijā **„Fima” turpina dzelzceļa posma Skrīveri – Krustpils** otro sliežu ceļu inženiertehnisko sistēmu uzstādīšanas veiksmīgu īstenošanu. Šobrīd notiek zemes kabeļu guldišanas darbi 20 km garajā ceļa posmā. Šogad kopumā „Fima” projektā plāno ieguldīt 200 km dažādu kabeļu.
- ▶ „Fima” ir parakstījusi līgumu ar AS „Kauno tiltai” par darbu veikšanu **Viļņas apbraucamā dzelzceļa** būvniecības projekta

Turpinājums seko 3 lpp.

VADĪBAS UZRUNA

”Fima” aizvadīts veiksmīgākais gads uzņēmuma vēsturē

Godātie kolēģi, klienti un partneri!

2011. gadu intelligento inženierisrinājumu uzņēmums ”Fima” noslēdzis ar labākajiem rezultātiem tā darbības 20 gadu ilgajā vēsturē. ”Fima” apgrozījums Latvijā 2011.gadā bijis 2,5 miljoni latu; ”Fima” grupas uzņēmumu konsolidētais apgrozījums pērn bijis 34 miljoni latu - 59 % pieaugums salīdzinājumā ar 2010.gadu.



Andis Lagzdīņš, SIA Fima valdes priekšsēdētājs

”“

Lai mums visiem kopā izdodas gāzt kalnus!

▶ Turpinājums seko 3 lpp.

Ziņu lente

ietvaros. Ceļa 25 km garajā posmā uzņēmuma speciālisti rekonstruēs funkcionējošo pirmā ceļa vadības sistēmu un no jauna uzstādīs otrā ceļa vadības sistēmu, kā arī ieviesīs citus inženierisinājumus un atjaunos staciju signalizācijas iekārtas, kas nodrošinās vēl lielāku dzelzceļa caurlaides spēju un kravas vilcienu ātruma palielināšanos līdz 80 km/h.

- ▶ Latvijā „Fima” uzsāk sadarbību ar Rīgas Tehniskās universitātes paspārnē esošo **starptautisko studentu organizāciju „BEST-RIGA”**, kas tehnisko zinātņu studentiem organizē pasākumus ar mērķi paplašināt viņu profesionālās un sociālās kompetences. Šogad uzņēmums „Fima” sponsorē studentu vasaras nometni „Kā kļūt par labāko no labākajiem” (Step by Step: How to Be the Best of the Best).
- ▶ Augstas izšķirtspējas videosistēmu ražotājs **„Mobotix”**, viens no vadošajiem nozares spēlētājiem, novērtējis „Fima” **Baltkrievijas** filiāles realizēto projektu, piešķirot tam balvu savā nomināciju kategorijā **„Gada projekts”**. Zvaigžņu projekts - „British Petroleum” grupas uzņēmuma „TNK-BP” Baltkrievijas degvielas uzpildes staciju un naftas bāzu IP videonovērošanas sistēmu modernizācija.

▶ Turpinājums no 2 lpp.

Izsakot pateicību mūsu klientiem, partneriem un darbiniekiem par ieguldījumu un sadarbību šādu lielisku rezultātu sasniegšanā, turpinās neatlaidīgs darbs, lai 2012.gada rezultāti būtu vēl viens iemesls sarunām par sasniegtiem finanšu rādītāju rekordiem!

Šogad Latvijā turpinām veiksmīgi uzsākto datu centru infrastruktūras būvniecības jomā – zināms, ka tuvāko piecu gadu laikā prognozētais uzņēmumu datu apjoms pieaugums būs 800 %, tādēļ šī ir ārkārtīgi perspektīva nozare. Tāpat turpinām nopietni strādāt arī komplekso drošības risinājumu jomā, kā arī VAS “Latvijas Dzelzceļš” infrastruktūras modernizācijas jomā.

Šobrīd Latvijā “Fima” darbinieku skaits sasniedzis jau apaļo skaitli 50 - neapšaubāmi var teikt, ka “Fima” savā darbībā Latvijā sasniegusi to punktu, kad radīti visi priekšnosacījumi stabilai izaugsmei – mums ir lieliska komanda, mums ir lieliski klienti, mums ir ambiciozi mērķi par jaunu klientu piesaistīšanu, un galvenais – mēs gribam realizēt efektīvus un inovatīvus projektus, kas maksimāli atbilst katram mūsu klientam individuāli. Tam visam pāri - moderna un sakārtota inženiertehnisko sistēmu infrastruktūra Latvijā.



Ar vislabākajiem vēlējumiem, Andis Lagzdīņš

„Fima” speciālisti izbūvē Varšavas kardioloģijas institūta **modulāro datu centru**

Inteliģento inženiertehnisko risinājumu uzņēmums „Fima”, kas nesen Polijā nodibināja savu meitasuzņēmumu „Fima Polska”, uzsāk jauna projekta īstenošanu: tiek izbūvēts **Varšavas Kardioloģijas institūta datu centrs**. Saskaņā ar „Fima Polska” direktoru **Robertu Zdunek** – projektu plānots pabeigt jau šā gada rudenī, kad institūta darbinieki varēs izmantot datu centru, ko raksturo modernas iekārtas un efektīvi inženiertehniskie risinājumi.

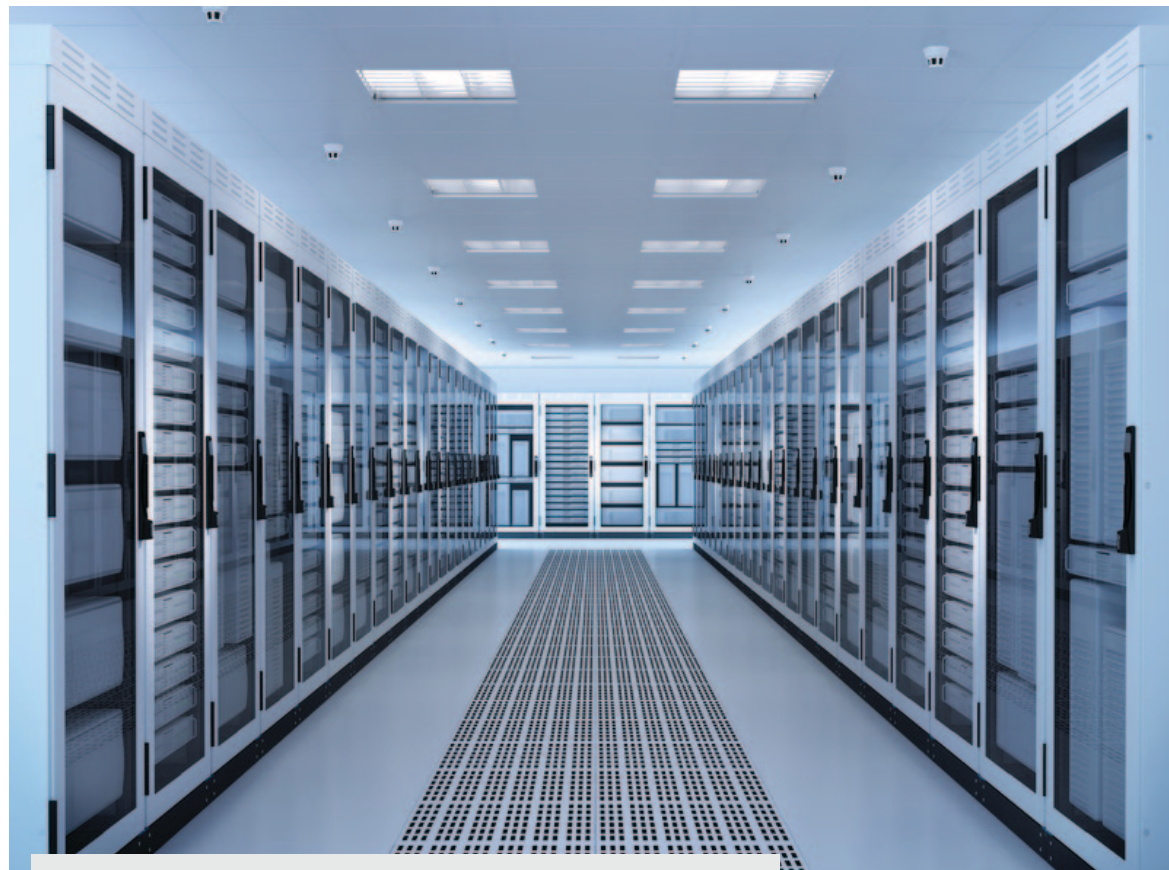


„Fima Polska” direktors R. Zdunek norāda, ka, pateicoties datu apstrādes centra modulārajai konstrukcijai, Kardioloģijas institūts nākotnē varēs viegli un ātri to paplašināt.

Drošība – pirmajā vietā

Varšavas Kardioloģijas institūts visu diennakti sniedz medicīnisko palīdzību pilsētas un tuvējo rajonu iedzīvotājiem. Slimnīcā tiek veikts liels daudzums nopietnu medicīnisko manipulāciju: no sirds aritmijas ārstēšanas ar intervences metodi līdz sirds transplantācijas operācijām.

«Šobrīd datu apstrādes centru nozare strauji aug. Modernie risinājumi nodrošina nepārtrauktu sistēmu darbību, ekspluatācijas vienkāršību, sistēmu vadības un datu centru paplašināšanas iespējas, augstus energoefektivitātes rādītājus. Tieši šādu risinājumu mēs piedāvājam Varšavas Kardioloģijas institūtam – tā kā viņiem, ņemot



„“

Polijas uzņēmumi orientējas uz diezgan šaurām inženierjomām, kamēr pasūtītājiem ir ērtāk strādāt ar vienu darbuzņēmēju, kurš var piedāvāt visus nepieciešamos risinājumus un pakalpojumus vienuviet

vērā darba specifiku, datu centra drošības jautājums ir ļoti būtisks», – norāda R. Zdunek.

Modulārais risinājums - vienkāršs paplašināšanas process

Uzņēmuma „Fima Polska” speciālisti izbūvēs institūta datu

centru pēc modulārās konstrukcijas principa. R. Zdunek uzsver, ka šāda tipa konstrukcija ļauj uzņēmumiem investēt līdzekļus un paplašināt savus datu centrus pakāpeniski, ņemot vērā arvien pieaugošās IT vajadzības. Turklāt šāds risinājums ļauj būtiski ietaupīt ekspluatācijas izdevumus, ļaujot

izmantot tieši tik iekārtu, cik nepieciešams konkrētajā brīdī.

Tāpat projekta izpildes gaitā tiks izbūvēta infrastruktūra, kas nepieciešama datu centra vadībai, tehniskajai apkalpošanai un apsardzei – no serveru dzesēšanas iekārtām līdz ugunsdzēsības un videonovērošanas sistēmām. Datu centra infrastruktūras vadība tiks īstenota ar kompānijas APC by Schneider Electric ražotās sistēmas StructureWare palīdzību. Šī sistēma ir paredzēta centra infra-

► Turpinājums seko 5 lpp.

struktūras stāvokļa reālā laika monitoringam, apkalpojošo sistēmu automātiskai vadībai, palīdzībai izmaiņu plānošanā un vadībā, kā arī enerģijas patēriņa kontrolei un optimizācijai.

Polijā trūkst uzņēmumu ar kompleksu pieeju

Lai gan Polijā darbojas ne viens vien inženiertehnisko risinājumu uzņēmums, tomēr kompānijas „Fima Polska” priekšrocība slēpjas plašajā piedāvāto inženierisinājumu klāstā un sniegto pakalpojumu daudzveidībā. «Polijas uzņēmumi orientējas uz diezgan šaurām inženierjomām. Mēs varam piedāvāt visus nepieciešamos risinājumus inženiertehniskās infrastruktūras jomā, īstenot sistēmu projektēšanas, montāžas un tehniskās apkalpošanas darbus. Pasūtītājam ir izdevīgāk, ja visu no sākuma līdz beigām īsteno vienā kontrolē viens darbuzņēmējs», - sacīja R. Zdunek.

Pēc viņa teiktā, Polijas datu apstrādes centru tirgum piemīt liels potenciāls – tā ikgadējais pieaugums ir apmēram 10%. «Tikai Varšavā vien uz šodienu ir vairāk nekā 20 tūkstoši kvadrātmetru komercīpašumu, bet datu centru nozare atrodas tikai sākuma attīstības stadijā - šobrīd ļoti aktīvi piedalāties datu centru projektēšanas un izbūves konkursos», - norāda R. Zdunek.

SADARBĪBAS PARTNERU JAUNUMI

Bagāžas pārbaude lidostās kļuvusi ātrāka un drošāka

Uzņēmums „Fima” piedāvā jaunās paaudzes iekārtas automātiskai bagāžas pārbaudei lidostās. Šo iekārtu ražotājs ir kompānija „Morpho” – pasaules līderis drošības nodrošināšanas līdzekļu tirgū. Jaunie risinājumi ļauj ne tikai ātri un efektīvi veikt liela bagāžas daudzuma pārbaudi, bet arī nodrošina augstu lidostu un pasažieru drošību.

”“

EDS sistēmas caurlaides spēja ir 1080 čemodāni stundā.

Kompānijas „Morpho” izstrādātā sprāgstvielu atklāšanas sistēma EDS (angļu val. Explosive Detection System) jau tiek izmantota dažādās modernās lidostās. Šīs iekārtas tiek iebūvētas kopējā bagāžas pārvaldības sistēmā un pārbaudes laikā ļauj ar lielu precizitāti atklāt sprāgstvielas, narkotiskās vielas, ieročus un citus aizliegtus priekšmetus.

EDS sistēma ļauj īstenot bagāžas pārbaudi ne tikai precīzāk, bet arī ātrāk. Tās caurlaides spēja ir 1080 čemodāni stundā, kas vairākas reizes pārsniedz analogisku iepriekšējās paaudzes skeneru caurlaides spēju. Aizliegta priekšmeta atklāšanas gadījumā sistēma nosūta automātisku paziņojumu, pateicoties kam nav nepieciešama dežurējošā operatora pastāvīga klātbūtne.

Drošības līmeņa paaugstināšanai uzņēmums „Fima” piedāvā iekārtas sprāgstvielu atklāšanai XRD (angļu val. X-Ray Diffraction), kuras darbojas pēc rentgena difraktometrijas principa. Šīs iekārtas ir paredzētas tās bagāžas papildu pārbaudei, kuru EDS sistēma ir identificējusi kā aizdomīgu. XRD sistēma veic šķidrumu analīzi un to molekulārās struktūras identifikāciju, kas ļauj tai atšķirt sprāgstvielas un narkotiskās vielas no nekaitīgām vielām. Šīs iekārtas tiek integrētas kopējā bagāžas pārvaldības sistēmā un darbojas autonomi, bez operatora klātbūtnes.



SEB bankas eksperti: efektīvas informācijas drošības pamatā ir kompleksi lēmumi un sabiedrības izglītošana

Ik dienu gan katrs individuāli, gan uzņēmumi kopumā baudām Interneta, datoru un citu mūsu modernās dzīves priekšrocību sniegtās ērtības, tomēr tas saistās ar zināmiem naudas zādžības riskiem. Un, kaut gan precīzas statistikas nav, tiek uzskatīts, ka zaudējumi, ko cietuši vienkāršie lietotāji un uzņēmēji saistībā ar tiesību pārkāpumiem un noziegumiem elektroniskajā interneta telpā, 2011. gadā sastādīja 400 miljardus ASV dolāru. **SEB bankas (Lietuva) Prevencijas departamenta direktors Audrijušs Šapola** uzskata, ka informācijas drošība rada pastāvīgas bažas kā katrai organizācijai, tā arī katram no mums atsevišķi. «Dažkārt šīs bažas rada sarežģīti kiberuzbrukumi, bet visbiežāk tās rodas neuzmanības un piesardzības pasākumu trūkuma rezultātā», - tā bankas eksperts. Mēs paaieresējāties, kā ar šo jautājumu tiek galā bankas sektors un kādus profilaktiskos pasākumus, pēc eksperta domām, ir jāveic.

„“

Vienotas uzņēmuma drošības politikas ietvaros ir jāapvieno fiziskās apsardzes metodes ar programmu drošības sistēmām



SEB bankas Prevencijas departamenta direktors Lietuvā Andrius Šapola: „Kaut gan Lietuva ir neliela valsts, datu zādžību gadījumi ir samērā reti. Tomēr privātajiem uzņēmumiem un valsts institūcijām nevajadzētu vadīties pēc šī faktora, nosakot savu informācijas aizsardzības investīciju apjomu.“

► **Banka pārvalda liela apjoma īpaši konfidencialu informāciju par iedzīvotājiem un uzņēmumiem. Kāda ir informācijas aizsardzības specifika bankas sektorā?**

Vienu no īpatnībām mēs jau minējām. Bankās cirkulē ārkārtīgi lieli finanšu datu apjomi, kas ir īpaši jūtīgs personisko datu veids. Cits šī sektora aspekts - gan uzņēmumi, gan privātpersonas kā klienti nes lielu atbildību par savu personisko datu aizsardzību. Piemēram, sākotnēji tirgū sniegtie bankas pakalpojumi globālajā tīmeklī bija kā

jaunums, taču tos nevarēja piedāvāt patērētājiem, neparedzot šādu pakalpojumu izdevīgumu, kā arī ar to saistītos iespējamos riskus. Tāpēc tos ieviesa tirgū tikai pēc tam, kad tehnoloģijas varēja nodrošināt drošību un uzticamību naudas operāciju veikšanas procesā. Bankas pastāvīgi pilnveido šo sistēmu drošību, jo hakeri ir modri. Tāpēc šodien datu zādžības tiek realizētas nevis bankas sistēmu uzlaušanas ceļā, bet gan izmantojot bankas klientus, t.i., krāpnieki vienkārši izmāna no viņiem paroles un citus personisko datus, lai pieslēgtos internetbankai.

► **Kā mainījušās bankas metodes ar nolūku garantēt informācijas drošību, ņemot vērā pēdējās tendences?**

Bankas neskata datu drošību tā, kā pirms 20 gadiem – šobrīd dominē kompleksa pieeja. Tas nozīmē, ka fiziskās aizsardzības līdzekļi jāapvieno ar programmu nodrošinājuma sistēmām vienotās uzņēmuma drošības politikas ietvaros. Bankas turpina vēltīt daudz uzmanības elektroniskajām drošības sistēmām – ievieš modernākās ēku videonovērošanas,

► Turpinājums seko 7 lpp.

signalizācijas, vadības kontroles sistēmas. Šobrīd šīs sistēmas tā pilnveidotas, ka, piemēram, signalizācija jau reaģē uz mazāko spiediena vai temperatūras izmaiņu, mazāko plaisu stiklā. Protams, liela investīciju daļa tagad tiek piešķirta IT risinājumiem, jo arī iespējamie riski mainījušies. Šodien mēs reti dzirdam par fizisku bankas aplaupīšanas gadījumiem, un tas ir dabiski, jo darbība pamatā notiek elektroniskajā telpā. Tas savukārt veicināja speciālu IT risinājumu izveidi tieši banku sektora drošības jomā.

► **Interesanti, kā strādā speciālais programmu nodrošinājums, kas piemērots datu aizsardzības vajadzībām banku sektorā.**

Piemēram, bankām ir speciālas monitoringa sistēmas, kas izseko karšu maksājumus, naudas pārskaitījumus globālajā tīmeklī un var konstatēt iespējamās noziedzīgas darbības, pateicoties speciālam programmas scenārijam. Pieņemsim, banku sistēma fiksē, ka cilvēks pulksten 9 no rīta nopirka tasīti kafijas vienā no Viļņas kafejnīcām un norēķinājās ar karti, bet pēc dažām minūtēm vai stundām par kaut ko samaksā ar to pašu karti Atlantijas okeāna otrā pusē. Sistēma nosaka, ka cilvēks nevar vienlaikus atrasties vairākās vietās vai tik ātri pārvietoties telpā. Tā nodod informāciju atbildīgajiem bankas darbiniekiem, kuri operatīvi reaģē, kontaktējas ar klientu,

bloķē karti un veic citus pasākumus nozieguma novēršanai. Bet, ja runājam par datu drošību, tad ir vēl viens ļoti svarīgs faktors – sabiedrības informēšana par iespējamajiem riskiem, jaunām noziegumu metodēm un elementāriem personiskās drošības pasākumiem, t.i., nedot savus datus nepiederošām personām, pārbaudīt elektroniskā veikala drošību līdz pirkuma veikšanai utt.

► **Kā Jūs domājat, vai pietiekama uzmanība tiek veltīta Lietuvas privātā un publiskā sektora informatīvajai drošībai?**

Lietuva, protams, ir neliela valsts, elektronisko noziegumu mērogs un apjoms šeit ir ievērojami mazāks kā Lielbritānijā vai ASV. Neskatoties uz to, neprivātie uzņēmumi, ne valsts institūcijas nevar vadīties no šiem faktoriem, nosakot investīciju apjomu informācijas aizsardzībā. Cita problēma, kas raksturīga ne tikai Lietuvai, ir tā, ka visbiežāk par informācijas drošību sāk domāt jau post factum, kas sāpīgi atsaucas uz organizācijas reputāciju un uzticību tai, kuru pēc tam ir ļoti grūti atjaunot. Protams, šī iemesla dēļ ne Lietuvā, ne visā pasaulē neeksistē reāla statistika par elektronisko noziegumu radīto zaudējumu apmēru, jo organizācijas cenšas noklusēt datu zudumus un atrisināt šīs problēmas bez īpašas publicitātes. Tostarp hakeri samērā aktīvi komunicējas savā starpā, apmainās ar informāciju, apvienojas pagrīdes tīklos. Tas

sniedz tiem zināmas priekšrocības un ļauj pilnveidoties.

► **Kā, pēc Jūsu domām, var mainīties informācijas drošības izpratne Lietuvā tuvākajos piecos gados?**

Bez šaubām, kā sabiedrība, tā biznesa un sabiedriskais sektors arvien vairāk uzmanības veltīs datu aizsardzībai. Jau tagad tiek veikti mēģinājumi uzlauzt valsts institūciju vietnes un tās bloķēt, tā piesavinoties datus. Visā pasaulē elektroniskajā telpā pieaug rūpnieciskās izlūkošanas un intelektuālā īpašuma zādžību gadījumu skaits. Tāpēc mums jādomā par to un jāseko citu valstu piemēram, lai laikus mācītos no to kļūdām un panākumiem. Lietuvai nāksies palielināt investīciju apjomu informatīvajai drošībai un vēl aktīvāk izglītot sabiedrību par šo tēmu. Kā jau minēju, šodien aplaupīt banku fizikā veidā ir samērā sarežģīti vai pat neiespējami, ēkās uzstādītas vismodernākās video novērošanas, signalizācijas, informatīvo tīklu sistēmas, tāpēc hakeri atrod visvājāko posmu – bankas klientus. Pozitīvu rezultātu dotu arī sadarbības veicināšana starp uzņēmumiem un valsts institūcijām. Citu pieredze ļauj efektīvāk organizēt datu apsardzi, sadalīt izmaksas un, protams, novērst elektroniskos tiesību pārkāpumus vēl pirms to veikšanas. Tāpēc palīdzēt var arī vispārpieņemto noteikumu ieviešana savu datu aizsardzībai.

Paldies par sarunu!

A. Šapolas padomi uzņēmumu informatīvās drošības speciālistiem :

- **Mājas darbi** Identificēt iespējamās riskus, iespējamās datu zādžības modeļus, atrast citu valstu pieredzi par līdzīgiem gadījumiem;
- **Kompleksa pieeja** Ņemot vērā sava uzņēmuma darba specifiku, izvēlēties integrētu drošības risinājumu – sākot ar fiziskiem apsardzes līdzekļiem un beidzot ar IT risinājumiem, kā arī izstrādāt vienotu drošības politiku;
- **Aktīvi jaunu variantu meklējumi** Izņemot jau pierastos programmu risinājumus – tādus, kā antivīrusi programmas – šodien eksistē neskaitāms daudzums citu, ļoti efektīvu drošības līdzekļu – sistēmas var ierobežot pieeju konkrētai informācijai pašā uzņēmumā, bloķēt konkrētu datu pārsūtīšanu caur iekšējām adresēm, pārtraukt pieeju datu bāzēm pēc darba dienas beigām utt.;
- **Atjaunošana** Nepieciešams pastāvīgi novērtēt jaunu risku rašanos, pārskatīt un atjaunot uzņēmuma drošības politiku, plānot investīcijas jaunu informatīvās drošības risinājumu ieviešanai un veco risinājumu atjaunošanai.



Bankas aprīkotas ar vismodernākajām pieejas kontroles sistēmām, apsardzes signalizāciju, videonovērošanu. To datu bāzes aizsargātas ar speciāliem IT risinājumiem, tāpēc hakeri pievēršusi savu uzmanību banku klientiem.

Uzņēmumi Eiropā arvien vairāk **līdzekļu atvēl informācijas drošībai**

IT speciālisti ceļ trauksmi – pēdējo divu gadu laikā hakeru uzbrukumu skaits informācijas sistēmām pieaudzis gandrīz divas reizes. Saskaņā ar „PricewaterhouseCoopers” pētījuma datiem «2012 Information Security Breaches Survey», 2011. gadā valsts lielie uzņēmumi saskārās vidēji ar 54 hakeru uzbrukumiem – kas ir 1,5 reizes vairāk kā pērn. Ar šo ziņojumu tika atklāta viena no Eiropā lielākajām un populārākajām informatīvās drošības izstādēm „Infosecurity”. Uzņēmuma „Fima” speciālisti, kuri piedalījās šajā pasākumā, norāda, ka Eiropā pieaug to uzņēmumu skaits, kuri savu datu maksimālas drošības un izmaksu efektīvas sadales nolūkos iegādājas kompleksus IT pakalpojumus no trešajām personām.

„Kompleksie IT risinājumi drošības jomā aizsargā ne tikai kompānijas konfidenciālo informāciju, bet arī tās reputāciju

Sargā ne tikai datus, bet arī reputāciju

Mūsdienu hakeri ļoti ātri pilnveidojas. Taču no viņiem neatpaliek arī IT sfēra, kura pastāvīgi atjauno jau esošos un piedāvā jaunus drošības risinājumus. „Iz-

stādē mēs redzējam, ka Eiropas uzņēmumu interese par šo tēmu ir ievērojami pieaugusi. To, neapšaubāmi, nosaka arī elektronisko zādzību skaita pastāvīgais pieaugums. Tomēr nepieciešams

► Turpinājums seko 9 lpp.



domāt par kompānijas reputāciju, par uzticēšanos tai”, - norāda komunikāciju risinājumu nodaļas vadītājs V.Čerņauskis. Viņš arī norāda, ka Baltijas valstīs vēl aizvien valda diezgan šaura un vienusīga pieeja datu drošības jautājumam.

«Ar vienu pašu antivīrusa programmu nepietiek. Sarunas un diskusijas ar izstādes dalībniekiem pārliecināja mūs par to, ka ārvalstu kompānijas izmanto kompleksus IT drošības risinājumus un arvien biežāk uztic šo darbu profesionāļiem. Tas nodrošina IT tīklu vienotu vadību,

speciālistus savu tīklu drošības testēšanai, bet pastāvīgi. Tas ir kļuvis iespējams, pateicoties tīkla resursu audita programmnodrošinājuma uzstādīšanai, kas regulāri pārbauda datortīklu un operatīvi nosaka tā vājās vietas.

Arvien vairāk Eiropas uzņēmumu un organizāciju lieto lokālā bezvadu tīkla WLAN (angļu val. Wireless Local Area Network) tehnoloģijas, kas ļauj samazināt datortīklu uzstādīšanas izmaksas. Taču bezvadu tīklā informācijas pārraidīšana tiek īstenota ar radioviļņu palīdzību, kas uzlauzējiem dod iespēju pārtvert un izmantot datus. Pēc

V. Čerņauska teiktā, izstādē bija ļoti daudz ražotāju, kuri piedāvāja tāda tīkla drošības risinājumus,

„*“ Eiropā pieaug to uzņēmumu skaits, kuri savu datu maksimālas drošības un izmaksu efektīvas sadales nolūkos egādājas kompleksus informāciju tehnoloģiju pakalpojumus no trešajām personām.*”

pastāvīgu risinājumu atjaunošanu un to efektīvu integrāciju, lai nodrošinātu paaugstinātu informācijas drošību», - paskaidroja V. Čerņauskis.

Modernākie risinājumi datortīklu infrastruktūras jomā

Izstāde „Infosecurity” veltīja īpašu uzmanību risinājumiem datortīklu infrastruktūras jomā. Viena no jaunākajām tendencēm ir tīkla resursu audita programmu pieaugošā popularitāte. Pēc V. Čerņauska teiktā, tīkla resursu auditu šodien var veikt nevis reizi gadā, kad kompānija pieaicina IT

un interese par tiem no apmeklētāju puses bija samērā augsta.

Lielākā daļa ražotāju prezentēja izstādē gan uzlabotu programmnodrošinājumu aizsardzībai pret informācijas noplūdi (angļu val. data leakage prevention), gan daudzfunkcionālus jaunās paaudzes starptīklu ekrānus (angļu val. next generation firewalls). Šie līdzekļi īsteno informācijas plūsmas analīzi, uz kuras pamata var atpazīt programmas, to atsevišķas funkcijas, sasaistīt programmas ar to lietotājiem, kā arī atklāt vīrusus un identificēt noteiktas slepenas



Kompānijas „Fima” projektu vadītājs komunikāciju risinājumu jomā Vaidotas Čerņauskas: «Vienota informācijas tīklu vadība, pastāvīga to atjaunošana un dažādu risinājumu efektīva apvienošana ir galvenie priekšnoteikumi, lai nodrošinātu paaugstinātu informācijas drošību».

ziņas, piemēram, finanšu. Tādā veidā starptīklu ekrāns nodrošina pastāvīgu datu kontroli un analīzi, kā arī rakstura atpazīšanu, tā novēršot informācijas zādzību.

«Izstādē mums bija iespēja tikties ar daudziem speciālistiem, komunicēt ar ražotājiem un viņu klientiem. Ir acīmredzams, ka šodien ieguvējas ir tās organizācijas, kurām ir kompleksa pieeja informatīvās drošības jautājumam un kuras, atskaitot fiziskus vai elementārus aizsardzības līdzekļus, tādus kā antivīrusu programmas, izmanto daudz sarežģītākus IT risinājumus», - tā kompānijas „Fima” eksperts izstādes noslēgumā.

SVARĪGI ZINĀT

Tendences datortīklu drošības jomā

- Tīklu audita programmu popularitātes pieaugums - tās pastāvīgi seko līdzi tīklu stāvoklim un palīdz operatīvi atrast to vājās vietas;
- Darbinieku pieaugošā mobilitāte stimulē piedāvājuma pieaugumu bezvadu tīklu drošības jomā;
- Aktīva risinājumu pilnveidošana informācijas noplūdes novēršanas jomā;
- Daudzfunkcionālu jaunās paaudzes starptīklu ekrānu ieviešana - detalizēti analizē datu raksturu un sasaista tos ar konkrētiem lietotājiem;
- Integrēta visu risinājumu vadība informatīvās drošības jomā.

Tehnoloģiju integrācija: jaunas iespējas transporta sektorā

Pavasara Starptautiskajā ceļu satiksmes un transporta infrastruktūras drošības izstādē „**Intertraffic 2012**” piedalījās vairāk nekā 800 šīs nozares ražotāju un apkalpojošo uzņēmumu no 100 pasaules valstīm. Uzņēmuma „Fima” speciālisti izpētīja jaunās tendences transporta sektorā un jaunākos piedāvājumus ceļu satiksmes organizācijas problēmu risināšanai Eiropā un visā pasaulē.



Autotransporta rūpniecības tendences – sistēmu integrācija un mobilitāte

Mūsdienu autotransporta rūpniecība arvien vairāk saistās ar elektroniku, informācijas un komunikāciju tehnoloģijām. Uzņēmuma „Fima” risinājumu departamenta direktors R. Šlekis norāda - šīs tendences skaidri atspoguļojušās šī gada izstādē, kur daudz uzmanības tika veltīts gan pašai tehnoloģiju integrācijai, gan arī iespējām, ko šie procesi sniedz.

Tehnoloģiju integrācijas un mobilitātes tendence pēdējā laikā izpaužas arvien spēcīgāk, pateicoties viedtālrunu un citu tamlīdzīgu ierīču popularitātes

reģistru apvienošanai, šī sistēma piedāvā autovadītājiem un speciālajiem dienestiem informāciju par ceļu apstākļiem reālā laikā. Sistēmas attīstīšanas turpmākās iespējas ir visai plašas: piemēram, pēc meteostaciju apvienošanas ar mainīgām ceļa zīmēm varēs automātiski regulēt ātruma ierobežojumus laika vai ceļu apstākļu izmaiņu gadījumā”, norāda R. Šlekis.

Transporta plūsmu vadība nezaudē savu aktualitāti

Izstādē «Intertraffic 2012» tika prezentēti arī dažādi risinājumi transporta plūsmu analīzes jomā. Šis jautājums vienmēr ir bijis aktuāls, jo, pilsētām kļūstot

„“

Moderna autotransporta joma arvien ciešāk savstarpēji saistīta ar elektroniku, informāciju un komunikāciju tehnoloģijām

pieaugumam. Tas stimulējis jaunas paaudzes pakalpojumu parādīšanos arī transporta sektorā – piemēram, iespēja saņemt informāciju par ceļa apstākļiem vai iespēja plānot un izvēlēties konkrētā brīža īsāko maršrutu. „Viens no pirmajiem tehnoloģiju integrācijas piemēriem Lietuvas transporta sektorā ir Ceļu satiksmes dalībnieku informatīvā nodrošinājuma sistēma, kura apvieno vairāk nekā 90 meteostacijas un transporta plūsmas detektorus. Pateicoties specializēta programmnodrošinājuma izmantošanai un dažādu

arvien lielākām, paplašinoties to infrastruktūrai un palielinoties transportlīdzekļu skaitam, ceļu satiksmes drošības jautājums saasinājies arvien vairāk.

«Ražotāji prezentēja dažādus risinājumus transporta plūsmu analīzes jomā: detektorus, radarus, videokameras, indukcijas cilpas utt. Var atzīmēt, ka iespējas šajā nozarē turpina augt – ražotāji pilnveido savu tehniku, panākot arvien lielāku precizitāti, ilgmūžību, lietošanas ekonomiskumu», - stāsta R. Šlekis.

Izstādes apmeklētāji tika ie-

➤ Turpinājums seko 11 lpp.



Rokas Šlekis, uzņēmuma „Fima” risinājumu departamenta direktors: „Lietuvā autotransporta modernizācijas infrastruktūra vēl tikai uzņem apgriezienus, taču mūsu kompleksie un mūsdienīgie risinājumi ved mūs pareizā virzienā”.

► Turpinājums no 10 lpp.

pazīstināti ar bezvadu iekārtu transportlīdzekļu atpazīšanai un analīzei, kas parādījusies tirgū salīdzinoši nesen. Šādu sistēmu galvenās priekšrocības slēpjas to izturīgumā, montāžas ērtībā ceļa klātnē un tehniskās apkalpošanas izmaksu samazināšanā. Uzņēmuma „Fima” speciālisti jau ir uzstādījuši šādu sistēmu Lietuvā, vienā no Kauņas krustojumiem. Mo-

„” Viens no pirmajiem tehnoloģiju integrācijas piemēriem Lietuvas transporta jomā ir Ceļu kustības dalībnieku informatīvās nodrošināšanas sistēma

dernie sensori īsteno transporta plūsmas analīzi un veic atbilstošas korekcijas ceļu satiksmes regulēšanas algoritmā.

Risinājumi gudrai pilsētai

Izstādes «Intertraffic 2012» laikā tika prezentētas arī jaunāko tehnoloģisko risinājumu

izmantošanas iespējas pilsētas infrastruktūras uzlabošanai.

Piemēram, ielu apgaismošanas izmaksas var samazināt, ne tikai pateicoties ekonomisku gaismas diodžu izmantošanai, bet arī apvienojot šīs tehnoloģijas ar meteoroloģisko novērojumu sistēmu – tādā gadījumā apgaismojums ieslēgsies automātiski atkarībā no diennakts laika, ga-

„Fima” piedāvā inteligentās transporta sistēmas:

- Transporta plūsmas regulēšana pilsētā
- Transporta līdzekļu ātruma un plūsmas kontrole
- Ceļu satiksmes noteikumu pārkāpumu fiksēšana: braukšana pie luksofora sarkanās gaismas, iebraukšana maršruta transporta līdzekļu kustības joslā, automašīnu novietošana aizliegtā vietā un tml
- Ceļu transporta negadījumu automātiskā fiksācija
- Informācijas sniegšana autovadītājiem un specdienestiem par laika un ceļa apstākļiem uz auto ceļiem
- Maksas organizācija atsevišķās braukšanas zonās
- Automobiļu plūsmas vadība pie auto stāvvietām utml

dalaika un laikapstākļiem.

Tāpat izstādē tika prezentēti daudzi risinājumi arī automašīnu stāvvietu pārvaldības jomā. Parādījusies jauna tendence, ko diktējušas pieaugošās patērētāju vajadzības: ražotāji arvien biežāk piedāvā ne tikai aprīkojumu, bet arī veselu pakalpojumu paketi, kas ietver sevī datu apstrādi un analīzi, atskaišu sagatavošanu. Tas palīdz operatoriem pieņemt efektīvākus lēmumus, plānojot pilsētas autostāvvietu tīkla attīstību. Par otru jauninājumu šajā sfērā kļuva automašīnu novietošanas stāvvietā procesa infor-

matīvās uzturēšanas risinājumi atklātām platībām, kad detektori tiek uzstādīti nevis virs automašīnām, bet tieši ceļa klātnē, ļaujot modernizēt autostāvvietas, kas atrodas klajām debesīm.

«Izstādes laikā mums bija brīnišķīga iespēja apmainīties idejām ar citu valstu inženiertehnisko risinājumu uzņēmumiem un iegūt jaunus partnerus šajā nozarē. Baltijas valstīs transporta infrastruktūras modernizācijai vel ir milzīgs potenciāls, taču tie risinājumi, ko piedāvā „Fima”, ved mūs pareizā virzienā», - noslēgumā norāda R. Šlekis.



Kontakti

LIETUVA **UAB „FIMA“**

Žirmūnų g. 139
LT-09120 Vilnius, Lietuva
Tel: +370 5 236 3535
E-pasts: info@fima.lt
www.fima.lt

BALTKRIEVIJA **OOO „FIMA BR“**

ul. Biriuzova 10a, No7H
Minsk 220073, Baltkrievija
Tel. +375 17 200 59 99
E-pasts: info@fima.by
www.fima.by

LATVIJA **SIA „FIMA“**

Dzelzavas iela 120g
Rīga, LV-1021, Latvija
Tel. +371 677 222 77
E-pasts: info@fima.lv
www.fima.lv

POLIJA **Fima Polska Sp. Z o.o.**

ul. Poleczki 12, 02-822
Warszawa, Polija
Tel. +48 22 894 60 13
E-pasts: biuro@fimapolska.pl
www.fimapolska.pl

Par „Fima” uzņēmumiem

Uzņēmums „Fima” ir inteligento inženiertehnisku risinājumu līderis Baltijas valstīs, kas piedāvā telekomunikāciju, drošības, automātikas, datu centru, kā arī transportam un enerģētikai paredzētus risinājumus.

Uzņēmums inteligentus inženiertehniskus risinājumus ievieš biznesa uzņēmumos un valsts organizācijās Baltijas valstīs un Baltkrievijā, pastāvīgi piedalās projektos, kuros tiek izmantotas tehnoloģiskas inovācijas. Gandrīz divdesmit darbības gados „Fima” jau ir īstenojusi vairākus tūkstošus dažāda apjoma un sarežģītības projektu.

Uzņēmuma „Fima” galvenā mītne atrodas Lietuvā, Viļņā, meitasuzņēmumi nodibināti Latvijā, Polijā, Baltkrievijā.

Vairāk informācijas **www.fima.lv**

Jums ir idejas, piedāvājumi vai komentāri? Rakstiet mums **solutions.era@fima.lv**

Atsauce uz informācijas avotu FIMA jaunumu izdevums „Risinājumu ēra” pārpublicācijas vai citāta gadījumā obligāta.