Na straży bezpieczeństwa

Nikt bardziej, niż Straż Graniczna nie wykorzystuje w sposób tak masowy wszelkiego rodzaju czytników dokumentów. Przy tak ogromnej skali dokonywanych kontroli granicznych wszelkie usprawnienia pracy mają bezpośredni wpływ na skrócenie całości procesu sprawdzenia, identyfikacji odprawianej osoby. Rozmowa z mjr SG Grzegorzem Wojtkunem, zastępcą dyr. Biura Łączności i Informatyki KGSG.

MJR GRZEGORZ WOJTKUN

Zastępca dyrektora Biura Łączności i Informatyki Komendy Głównej Straży Granicznej. Z wykształcenia – mgr inż. Elektroniki i Telekomunikacji. W Straży Granicznej jest od początku jej powstania. Służył na różnych szczeblach funkcjonowania i zarządzania strukturami łączności i informatyki SG. Karierę zawodową zaczynał pracując bezpośrednio na granicy. Zdobytą tam wiedzę wykorzystał służąc w Pomorskim Oddziale SG w Szczecinie a następnie w Komendzie Głównej SG. Autor koncepcji budowy nowoczesnego systemu telekomunikacyjnego Straży Granicznej, spełniającego wszelkie normy niezawodnościowe oraz bezpieczeństwa informacji. W 2002 roku uruchomił największy w Europie system telefonii IP (ponad 6 tyś. użytkowników), przełamując stereotyp organizacji łączności telefonicznej z wykorzystaniem technologii Voice over IP. Autor koncepcji budowy najnowocześniejszego w chwili obecnej obiektu technologicznego w administracji państwowej kraju. W maju 2007 roku Straż Graniczna uruchomiła Centralny Węzeł Teleinformatyczny – tzw. Data Center z prawdziwego zdarzenia. Obiekt spełnia wszelkie reżimy bezpieczeństwa fizycznego i niezawodnościowego, jest pierwszym tej klasy obiektem w służbie administracji państwowej. Za swoje osiągnięcia wielokrotnie nagradzany: odznaczony brązowym krzyżem zasługi, srebrnym medalem za zasługi dla Straży Granicznej, brązowym medalem za zasługi dla obronności kraju.

Jak ocenia Pan poziom bezpieczeństwa danych w Polskiej Straży Granicznej na tle naszych europejskich sąsiadów?

Poziom bezpieczeństwa danych można rozpatrywać na kilku płaszczyznach. Począwszy od fizycznej ochrony zgromadzonych zasobów, poprzez zabezpieczenie informacji przed ich utratą, a kończąc na niepowołanemu przechwyceniu ich podczas transmisji, włamaniu do serwerów czy uszkodzeniu przez złośliwe oprogramowanie. Straż Graniczna, budując od kilku lat kompleksową infrastrukturę teleinformatyczną, wzięła pod uwagę każde z tych zagrożeń. Fizyczne zabezpieczenie danych Polskiej Straży Granicznej realizowane jest w supernowoczesnym ośrodku obliczeniowym, zbudowanym od podstaw w 2007 roku. Centralny Węzeł Teleinformatyczny SG (CWT) jest wyspecjalizowanym obiektem budowlanym, zabezpieczającym zgromadzone dane. Budynek wyposażony jest w kabiny odporne na atak elektromagnetyczny, pożar, przechwycenie danych wyciekających w formie ulotu. Kabiny serwerowe umieszczone są w sarkofagu żelbetonowym. Całość rozwiązania chroniona jest strefą buforową, posiada wszelkie obecnie dostępne systemy kontroli dostępu, monitoring wizyjny oraz dedykowany zespół funkcjonariuszy odpowiedzialnych za ochronę fizyczną obiektu. CWT posiada niezależne dwie 1MW linie zasilające, własne generatory energii elektrycznej z zapasem paliwa na wielogodzinną pracę. Budowa obiektu została sfinansowana ze środków Unii Europejskiej, mając na celu zapewnienie niezawodności pracy systemów wspomagających przepływ ludzi na polskim odcinku zewnętrznej granicy UE. Kolejno należy rozważyć bezpieczeństwo przetwarzanych danych podczas ich przesyłu z centralnego serwera do przejść granicznych. Straż Graniczna wykorzystuje infrastrukturę Telekomunikacji Polskiej w formie outsourcingu transmisji danych. Wszystkie lokalizacje graniczne połączone są dedykowaną, wydzieloną wirtualnie siecią z zasobów operatora. Ze względu na rozlokowanie placówek SG, zakup usług wydaje się uzasadniony ekonomicznie, w porównaniu z budową własnej infrastruktury teletransmisyjnej. Całość sieci te-

letransmisyjnej zabezpieczona jest urządzeniami szyfrującymi, wykorzystującymi silne algorytmy kryptograficzne AES 256. Ponadto każdy węzeł systemu posiada własne urządzenia firewall oraz IPS, zabezpieczające przed włamaniem czy atakiem hackerskim. W sumie w systemie pracuje kilkaset urządzeń IPS, firewall i sond analizujących anomalie. Całość rozwiązania zarządzana jest oraz monitorowana z całodobowego centrum monitoringu (umiejscowionego w obiekcie CWT). Przetwarzana informacja zabezpieczona jest również jednorodnym systemem antywirusowym. W skład systemu wchodzi oprogramowanie antywirusowe uruchomione na każdym z komputerów, sprzętowe urządzenia filtrujące całość ruchu przychodzącego z sieci Internet, skanery poczty elektronicznej, narzędzia badające on-line reputację serwisów internetowych oraz przychodzących e-maili. Na szczycie całości rozwiązania zabezpieczającego zasoby danych jest system autoryzacji użytkowników oraz stanowisk końcowych sieci, wykorzystujący w swoim działaniu infrastrukturę klucza publicznego – PKI. Dostęp do centralnego serwera z danymi możliwy jest wyłącznie z autoryzowanego stanowiska komputerowego oraz przez uprawnioną osobę posiadającą aktualny certyfikat PKI. W konsekwencji każdy komputer wpięty do sytemu Straży Granicznej w momencie uruchamiania jest autoryzowany, a w przypadku braku autoryzacji – zostaje zablokowany fizyczny interfejs sieci oraz generowany jest alarm o włamaniu do systemu. Reasumując, zbudowana infrastruktura, w której funkcjonuje kilkadziesiąt tysięcy urządzeń, daje rękojmię bezpieczeństwa dla przetwarzanych informacji. Przy czym trudno mi porównać stosowane rozwiązania naszych sąsiadów. Straż Graniczna, budując system w chwili obecnej (zakończenie planowane jest na marzec 2009 roku), wykorzystuje najlepsze i najnowsze obecnie dostępne rozwiązania technologiczne, co może dawać przewagę nad rozwiązaniami już zbudowanymi kilka lat temu.

Czy Polacy mogą być zadowoleni z rozwiązań informatycznych wspomagających ochronę granic państwa?

Stosowane przez Straż Graniczną rozwiązania techniczne są na najwyższym poziomie, przez co dają możliwość jak najlepszego zabezpieczenia granicy. Należy przy tym zaznaczyć, że ze względu na specyfikę działania SG, tj. nieustanną obsługę milionów podróżnych (średnio granicę przekracza rocznie grubo ponad 100 mln ludzi) stosowane rozwiązania techniczne oraz technologia muszą spełniać najwyższe normy niezawodności oraz wydajności, co w konsekwencji wpływa na koszty rozwiązania. Reżim czasowy pojedynczej odprawy, przyjęty na średnim poziomie 5 sekund na odprawę graniczną, powoduje, że system posiada powiększoną przepustowość a kluczowe urządzenia są zdublowane, umożliwiając nieprzerwalną pracę systemów obsługujących naszych podróżnych. Nie mniej jednak inwestycja w niezawodne (lecz droższe) systemy ma w konsekwencji uzasadnienie ekonomiczne. Nawet krótkotrwałe wstrzymanie obsługi granicznej powoduje zachwianie przepływu podróżnych oraz towarów (nie wspominając przestojów na lotniskach) a koszty z tym związane są ogromne i trudne do oszacowania. Dlatego też myślę, że Polacy mogą być zadowoleni z zaimplementowanej w Straży Granicznej infrastruktury teleinformatycznej, która będzie niezawodnie służyć przez wiele lat. Szczególnie, że większość jej kosztów udało się sfinansować z funduszy pomocowych Unii Europejskiej (SG w ramach funduszu Schengen pozyskała środki i zbudowała część systemu teleinformatycznego za ponad 300 mln zł).

Odpowiadamy za bezpieczeństwo zewnętrznej granicy Unii Europejskiej. Głośno mówiło się o budowie systemu stacjonarnej i mobilnej obserwacji, czujnikach laserowych, sejsmicznych, czy elektromagnetycznych i mikrofalowych. Na jakim etapie jest proces uszczelniania granicy wschodniej Polski?

W tej kwestii nie mogę pochwalić się znaczącymi osiągnięciami. W ramach funduszu Schengen Straż Graniczna otrzymała ogromne środki (ponad 250 mln zł) na budowę Systemu Elektronicznego Wspomagania Nadzoru Granicy Zewnętrznej (SEWN). System miał zabezpieczyć lądowy odcinek granicy zewnętrznej Polski. Wzdłuż granicy rozlokowane miały zostać wysokie wieże obserwacyjne z bardzo czułymi kamerami termowizyjnymi, umożliwiającymi obserwację odcinka granicy. Dodatkowo wzdłuż granicy miały zostać położone kable perymetryczne wyczuwające zbliżanie się do granicy lub jej przekroczenie. System miał zrewolucjonizować ochronę dość trudnego odcinka granicy Unii Europejskiej. Niestety, ze względu na zawiłe procedury przetargowe, nieporozumienia w interpretacji przepisów Polskiego Prawa Zamówień Publicznych wśród zagranicznych oferentów, nie udało się skutecznie rozstrzygnąć przetargu, co w konsekwencji spowodowało odstąpienie od realizacji projektu. Dość nowatorski charakter zamówienia, ale głównie wartość kontraktu, spowodowały, że do przetargu zgłosiło się kilkanaście zagranicznych konsorcjów. Ze względu na obowiązujące przepisy zdecydowana większość ofert została odrzucona za niespełnienie wymogów formalnych. To spowodowało lawinę odwołań, arbitraży oraz spraw sądowych. Co prawda, wszystkie sprawy sądowe wygraliśmy, lecz tzw. pyrrusowe zwycięstwo zmusiło nas do zaniechania realizacji projektu ze względu na brak czasu pozostałego do sztywno określonego okresu zakończenia programu finansowego. W chwili obecnej, ze środków budżetowych realizujemy namiastkę systemu. Uruchamiane jest 10 wież obserwacyjnych usytuowanych w miejscach wcześniej przewidywanych w projekcie SEWN. Ponadto, w tym roku powiększymy flotę o 14 specjalnych samochodów patrolowych – tzw. Przewoźnych Jednostek Nadzoru (PJN) wyposażonych w system obserwacji dziennej oraz nocnej. PJN umożliwia skanowanie terenu wzdłuż granicy w promieniu kilkunastu kilometrów oraz obserwowanie i rejestrowanie incydentów nielegalnego przekraczania granicy. Dodatkowe pojazdy mają zrekompensować brak SEWN. Nie mniej jednak system ochrony technicznej byłby zdecydowanie lepszym rozwiązaniem wspomagającym ochronę granicy zewnętrznej, lecz ze względu na ogromne koszty implementacji SG nie ma możliwości powtórzenia projektu. Obecnie dostępne dla Straży Granicznej środki z funduszy Europejskich, funduszy pomocowych Norwegii i Szwajcarii są proporcjonalnie niewielkie na rozpoczęcie tak dużej inwestycji. Ponadto chciałbym podkreślić, że koncepcja technicznego zabezpieczenia granicy nie została zarzucona i cały czas trwają testy nowych sensorów, kamer i jeżeli podjęta zostanie decyzja o budowie sytemu – Biuro Łączności i Informatyki KGSG jest przygotowane na realizację tego skomplikowanego przedsięwzięcia.

W jaki sposób szyfrowane są informacje przekazywane z centralnych baz danych do jednostek Straży Granicznej?

Wszelkie dane przetwarzane wewnątrz systemu teleinformatycznego SG są zabezpieczone tunelami GRE IPSec szyfrowanymi kluczem AES 256. Ponadto dostęp do najbardziej kluczowych aplikacji produkcyjnych dodatkowo odbywa się za pośrednictwem przeglądarki oraz protokołem *https*.

Czy posiadacie dodatkowe zabezpieczenia, które zostały wrożone na specjalne potrzeby SG?

Nie. Staramy się stosować standardowe rozwiązania wykorzystywane przez innych użytkowników. Dedykowane rozwiązania mają fundamentalną wadę – są wykorzystywane przez jeden podmiot, co w konsekwencji może prowadzić do braku supportu. Na rynku jest mnóstwo sprawdzonych, przetestowanych rozwiązań i te implementujemy.

Czy wszystkie przejścia graniczne mają łączność on-line z centralnymi bazami danych SG?

Tak, wszystkie placówki mają stały dostęp do sieci. Wykorzystujemy IPVPN w technologii MPLS w ramach umowy z TP SA. Placówki graniczne, w zależności od zapotrzebowania, posiadają łącza o przepustowości od 512kbit/s do 4Mbit/s. W ramach systemu teleinformatycznego SG placówki mają dostęp do sieci wewnętrznej, stałe łącze do Internetu oraz transmisję głosu i wideo.

W jaki sposób współpracujecie z innymi organami, np. z Policją?

Ze względu na zcentralizowane zasoby bazodanowe, wymiana danych z innymi organami odbywa się bezpośrednio w Warszawie. W ramach prowadzonych inwestycji teleinformatycznych w ubiegłych latach SG wybudowała kilkadziesiąt kilometrów linii światłowodowych na terenie Warszawy. Za ich pośrednictwem w sposób bezpieczny i niezawodny połączeni jesteśmy z serwerowniami innych organów państwowych. Z nich pozyskiwane są zasoby bazodanowe niezbędne do skutecznej kontroli granicznej. Ponadto Straż Graniczna w ramach współpracy udostępnia swoje obiekty technologiczne na potrzeby innych instytucji. Między innymi SG zapewnia infrastrukturę dla Urzędu ds. Cudzoziemców, w serwerowniach SG zamontowane są elementy systemów bazodanowych Policji. W tym roku planowane jest implementacja zasobów mocy obliczeniowej dla Państwowej Straży Pożarnej oraz utrzymywany jest resortowy system ePUAP.

Jaki sprzęt pomaga w sprawdzeniu autentyczności dokumentów osób przekraczających granice?

Nikt bardziej, niż Straż Graniczna nie wykorzystuje w sposób tak masowy wszelkiego rodzaju czytników dokumentów. Przy tak ogromnej skali dokonywanych kontroli granicznych wszelkie usprawnienie pracy ma bezpośredni wpływ na skrócenie całości procesu sprawdzenia, identyfikacji odprawianej osoby. Do chwili obecnej SG wykorzystuje czytniki kodu OCRB, stosowanego w paszportach. Tego rodzaju czytniki jedynie umożliwiają przyspieszenie procesu wprowadzania danych do sytemu. Nie sprawdzają autentyczności przedstawianych do kontroli dokumentów. Pojawiające się nowe dokumenty podróży wyposażone są w zatopione chipy mikroprocesorowe – niosą ze sobą dodatkowe informacje, na podstawie których oprócz typowych danych identyfikacyjnych można dokonać kontroli autentyczności dokumentu. Ponadto planowane wydanie europejskich wiz oznakowanych biometrycznie powoduje, że Straż Graniczna planuje masowy zakup nowych czytników. Pomimo, że posiadamy wystarczające środki na zakup tych urządzeń nadal nie możemy rozpocząć wyposażania stanowisk kontrolerskich ze względu na brak ostatecznej wersji rozwiązań biometrycznych. Niewielka ilość nowych dokumentów powoduje, że decyzję o zakupie nowych czytników możemy odsunąć na okres późniejszy, do momentu zakończenia prac nad specyfikacją rozwiązań biometrycznych zastosowanych w dokumentach podróży.

SG posiada największą w Polsce sieć Voice over IP. W jaki sposób jest wykorzystywana?

Straż Graniczna była prekursorem, i to na skalę europejską, budowy rozwiązań systemów telefonii IP. W 2003 roku został zaimplementowany system Voice over IP, który swoim zasięgiem objął wszystkie lokalizacje organizacyjne SG. Uruchomiono ponad 6 tys. aparatów telefonicznych IP. W chwili obecnej system został rozbudowany do 10 tys. terminali IP oraz zastosowano nowszą wersję oprogramowania, co w stu procentach wyeliminowało tradycyjne systemy telefoniczne. Generalnie system telefonii IP nie różni się funkcjonalnie od standardowych cyfrowych rozwiązań telefonicznych. Główną zaletą zastosowanego rozwiązania jest wykorzystywanie przez system telefoniczny eksploatowanej sieci komputerowej. Ciągły wzrost zapotrzebowania na pasmo transmisyjne dla transferu danych powoduje, że sama transmisja telefoniczna, choć nadal kluczowa, zajmuje marginalne zasoby transmisyjne. Ponadto zarządzanie mocno rozproszonym systemem jest łatwiejsze. Wdro-

żenie telefonii IP zredukowało potrzeby związane choćby z okablowanie budynków – na jednym kablu Ethernet funkcjonuje jednocześnie telefon i komputer. Ze względu na to, że aparat telefoniczny jest przeglądarką XML, dystrybuujemy za ich pośrednictwem dodatkowe serwisy, np. centralny spis abonentów automatycznie generowany z bazy danych kadrowych LDAP, aplikacje monitorujące stan pracy innych aparatów telefonicznych lub aplikację do dystrybucji newsów do grupy zainteresowanych osób. Podsumowując – rozstając się z tradycyjnymi rozwiązaniami telefonicznymi przenieśliśmy i tak skąpe zasoby inżynierskie do administracji systemami komputerowymi, co umożliwiło nam podniesienie poziomu obsługi utrzymania sytemu.

Czy do modernizacji swoich służb wykorzystujecie ofertę krajowych czy firm obcego kapitału?

Straż Graniczna, ze względu na przytaczane powyżej uwarunkowania niezawodnościowe oraz wagę zadań, w swoich rozwiązaniach wykorzystuje najwyższej klasy sprzęt oraz oprogramowanie teleinformatyczne. Rozwiązania sieciowe oraz bezpieczeństwa sieciowego oparte są wyłącznie na bazie produktów Cisco Systems. W systemie SG zaimplementowanych jest ponad 20 tys. urządzeń produkcji Cisco Systems, dając gwarancję niezawodności oraz kompatybilności całości rozwiązania. Centralne zasoby serwerowe wraz z systemami dyskowymi oraz backupu zbudowane są wyłącznie z wykorzystaniem produktów IBM. Straż Graniczna wykorzystuje obecnie najnowocześniejsze produkty klasy enterprises infrastruktury mocy obliczeniowej. Cztery serwery RISC klasy IBM p590, połączone klastrem niezawodnościowym dają pełną gwarancję ciągłej pracy nawet przy dużym obciążeniu transakcyjnym. Pojemne Storage IBM DS8100 oraz biblioteki taśmowe IBM TS3500 umożliwiają przechowywanie ogromnej ilości informacji, skanów dokumentów, nagrań telefonicznych realizowanych z aparatów telefonicznych sieci wewnętrznej itp. Oprócz kluczowych aplikacji produkcyjnych na centralnych serwerach zaimplementowane są aplikacje wspomagające funkcjonowanie informacji, funkcjonują m.in.: centralny serwer poczty elektronicznej (10 tys. skrzynek pocztowych na bazie IBM Lotus Domino), centralny portal komunikacyjny SG (IBM WebSphere Portal), centralny system e-learning (IBM Workplace Collaborative Learning), centralne archiwum skanów dokumentów (IBM Lotus Domino), centralny system ewidencji materiałowej oraz pierwsza linia wsparcia – helpdesk (IBM MAXIMO), system elektronicznego obiegu dokumentów (IBM Lotus Workflow), centralny monitoring systemu teleinformatycznego SG (IBM Tivoli).

Jakie przynosi to rezultaty?

Zastosowanie produktów niekwestionowanych liderów technologicznych daje gwarancję stabilnej (z punktu widzenia funkcjonowania państwa) pracy kluczowych systemów odpowiedzialnych za całodobowy przepływ podróżnych oraz towarów przez granicę naszego kraju. Wyszliśmy z założenia, że przyjęte rozwiązania techniczne, choć są kosztowne, stanowią odsetek potencjalnych strat, jakie mogą powstać w sytuacji awarii i w konsekwencji wstrzymania odprawy na granicy. Pomimo zastosowania zagranicznych technologii system budowy był wieloetapowo a jego wykonawcami były w większości polskie firmy integratorskie.

Chciałbym zapewnić podróżnych, że systemy teleinformatyczne stosowane przez Straż Graniczną są budowane z myślą o ich bezcennym czasie, komforcie oraz z chęcią zminimalizowania nieuniknionych utrudnień związanych z procedurami przekroczenia granicy. ■

Dziękuję bardzo
Katarzyna Czajkowska