WDROŻENIE SZBI[1] W POLSKIEJ TELEFONII KOMÓRKOWEJ CENTERTEL SP. Z O.O., OPERATORA SIECI ORANGE

Andrzej Kalinowski

Streszczenie. Informacja jest jednym z ważniejszych narzędzi uzyskiwania przewagi konkurencyjnej, a jej bezpieczeństwo stanowi kluczowy element wiarygodności przedsiębiorcy i niezbędny warunek spełnienia wymagań prawa. Dla zapewnienia skutecznej ochrony informacji w organizacji nie wystarczy tradycyjny zamek w drzwiach, firewalle i zabezpieczony hasłem komputer, niezbędne jest kompleksowe podejście do złożonych zagadnień bezpieczeństwa. Artykuł relacjonuje przebieg prac projektowo-wdrożeniowych w zakresie budowy w Polskiej Telefonii Komórkowej „Centertel" – operatora sieci telefonii mobilnej Orange – systemu zarządzania bezpieczeństwem informacji (SZBI) zgodnego z wymaganiami normy ISO/IEC 27001:2005. Pełne wdrożenie systemu i jego certyfikację poprzedziła pilotażowa implementacja w wytypowanym obszarze funkcjonalnym przedsiębiorstwa. W zakończeniu artykułu przedstawiono uzyskane korzyści wynikające z wdrożenia systemu oraz sformułowano wnioski praktyczne.

Wprowadzenie

Informacja jest jednym z ważniejszych narzędzi uzyskiwania przewagi konkurencyjnej, dlatego też zarządzanie jej aktywami stało się jednym z kluczowych procesów zarządczych we współczesnych przedsiębiorstwach. W dobie globalizacji i nieustającej walki konkurencyjnej pozycję lidera rynkowego, szczególnie w branży telekomunikacyjnej, zdobyć może ta firma, która potrafi szybko pozyskiwać, odpowiednio przetwarzać i racjonalnie wykorzystywać informacje oraz jest w stanie zagwarantować ich bezpieczeństwo. Skuteczna ochrona informacji to gwarancja, że klienci otrzymują usługi telekomunikacyjne na najwyższym poziomie, zgodnym z obowiązującymi międzynarodowymi standardami bezpieczeństwa, a firma zyskuje wysoki poziom zaufania partnerów, współpracowników i klientów.

Powyższe uwarunkowania oraz wymagania ochrony informacji wynikające z przepisów prawa (krajowego i międzynarodowego), a także korporacyjne zalecenia bezpieczeństwa legły u podstaw wypracowania w 2004 r. założeń polityki bezpieczeństwa informacji w PTK Centertel.

Obowiązywały wówczas dwa charakterystyczne podejścia do zagadnień bezpieczeństwa informacji w organizacji:

1) *make security* – utrzymywanie bezpieczeństwa,
2) *manage security* – zarządzanie bezpieczeństwem.

---

[1] SZBI – system zarzadzania bezpieczeństwem informacji wg ISO/IEC 27001:2005 (ang. ISMS – *Information Security Management System*).

Pierwsze podejście było dominujące i wyrażało przekonanie wielu menedżerów, że wystarczy tradycyjny zamek w drzwiach i zabezpieczony hasłem komputer oraz firewalle, aby skutecznie rozwiązać problem bezpieczeństwa informacji.

Drugie podejście implikowały wiedza i doświadczenie specjalistów w tej dziedzinie, którzy uważali, że zapewnienie skutecznego bezpieczeństwa informacji nie jest wcale takie oczywiste i proste, wymaga wysiłku i zaangażowania wszystkich pracowników, a optymalnym rozwiązaniem jest zarządzanie nim, stosując podejście systemowe oraz uznane wzorcowe sposoby postępowania (*best practices*).

Założenia

W przyjętych założeniach polityki bezpieczeństwa informacji uwzględniono charakterystyczne aspekty organizacyjno-funkcjonalne **PTK Centertel oraz następującą specyfikę:**

- firma telekomunikacyjna, przetwarzająca bardzo duże ilości informacji podlegających prawnej ochronie:
  - Ustawy o zwalczaniu nieuczciwej konkurencji,
  - Ustawy prawo telekomunikacyjne,
  - Ustawy o ochronie danych osobowych,
  - Ustawy o ochronie informacji niejawnych,
  - Sarbanes-Oxley Act 2002,
- standardy korporacyjne,
- ogromna konkurencja na rynku (duża waga poufności niektórych informacji),
- organizacja rozproszona,
- funkcjonujący system zarządzania jakością (ISO 9001),
- występowanie wyraźnego podziału na bezpieczeństwo IT oraz bezpieczeństwo organizacyjno-prawne,
- reaktywne działania w zakresie bezpieczeństwa, nienakierowane na zapobieganie,
- słabe powiązania bezpieczeństwa z biznesem,
- narastająca liczba incydentów bezpieczeństwa.

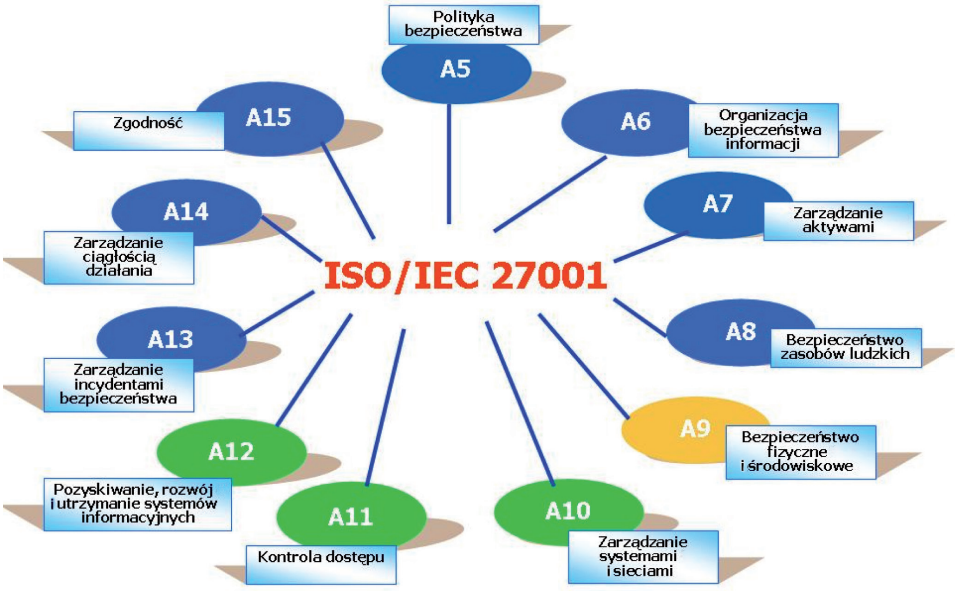
Wyniki przeprowadzonych analiz oraz przychylne stanowisko ówczesnego kierownictwa PTK Centertel do podejścia *manage security* jednoznacznie ukierunkowały dalsze prace na zaprojektowanie i wdrożenie systemu zarządzania bezpieczeństwem informacji, gwaranta bezpieczeństwa biznesowego i skuteczności działania.

W przyjętej koncepcji zastosowano systemowe podejście oraz skorzystano z zaleceń najlepszych światowych standardów i praktyk, w tym zwłaszcza zaleceń ówczesnej normy BS 7799 (późn. ISO/IEC 17799, ISO/IEC 27001). Modelowe rozwiązania przyjętej normy, zbliżone do systemu zarządzania jakością wg ISO 9001,

wdrożonego przez dziesiątki tysięcy firm, gwarantowały realność i efektywność wdrożenia tej koncepcji. Przede wszystkim wskazywały na konieczność:

1) opracowania mechanizmu cyklicznie przeprowadzanej analizy ryzyka utraty bezpieczeństwa informacji i podejmowania działań minimalizujących (opracowania i wdrożenia planu postępowania z ryzykiem),
2) wdrożenia adekwatnych zabezpieczeń organizacyjno-technicznych – spełnieniających wymagania dziesięciu obszarów normy (późn. 11 rozdziałów normy ISO/IEC 27001 zawierających 133 zabezpieczenia):

Obszary zabezpieczeń wg normy ISO/IEC 27001



Źródło: opracowanie własne

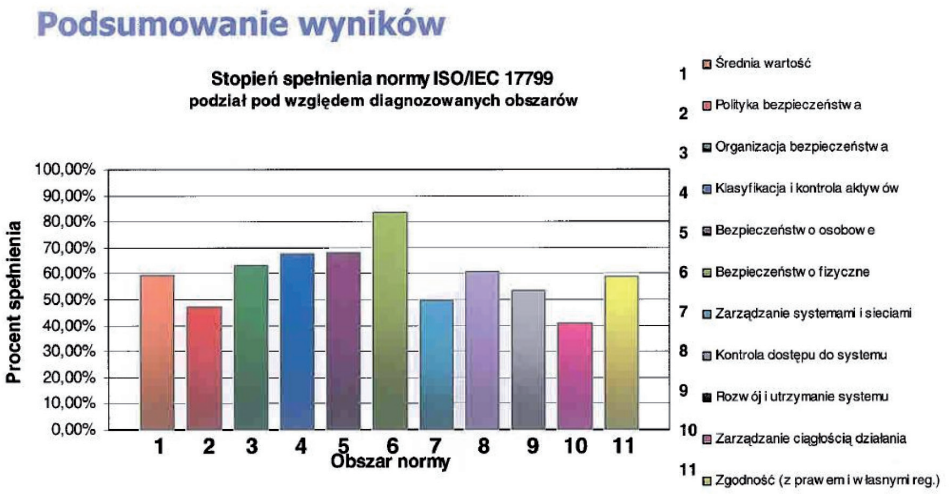
3) opracowania i wdrożenia zintegrowanej struktury zarządzania bezpieczeństwem informacji w organizacji,
4) opracowania i wdrożenia dokumentacji SZBI (polityki, regulaminy, procedury, itp.).

Dzięki aktywnemu zaangażowaniu w projekt kierownictwa i pracowników spółki, głównie Departamentu Bezpieczeństwa, oraz środkom finansowym przyznanym przez zarząd, przystąpiono do etapowej realizacji prac projektowych – budowy SZBI, który do końca 2006 roku miał objąć swoim zasięgiem wszystkie obszary operacyjne organizacji. Ponadto przyjęto założenie o pełnej integracji systemu z innymi obszarami zarządzania (SOX, zarządzanie jakością).

Etapy prac projektowych – budowy SZBI

I. Diagnoza (październik 2004–czerwiec 2005)

- Przeprowadzono audyt aktualnego stanu organizacji pod kątem bezpieczeństwa przetwarzanych informacji oraz przeanalizowano:
  - strukturę organizacji,
  - bezpieczeństwo prawne,
  - bezpieczeństwo teleinformatyczne – poziom podstawowy,
  - bezpieczeństwo fizyczne,
  - komponenty ciągłości działania.
- Po podsumowaniu wyników uzyskano wiedzę na temat spełnienia wymagań standardu ISO/IEC 17799 oraz opracowano katalog proponowanych działań doskonalących.



Źródło: opracowanie własne

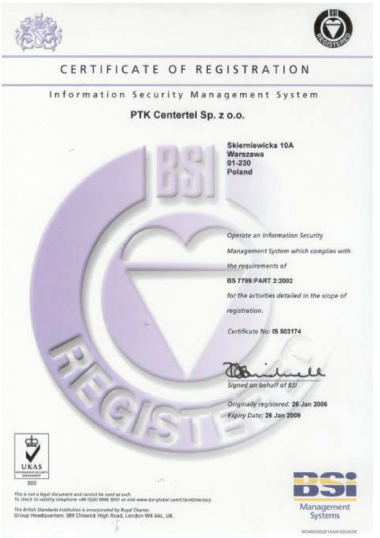
II. Opracowanie dokumentu Polityki Bezpieczeństwa Informacji (czerwiec–wrzesień 2005)

- Określono strukturę zarządzania bezpieczeństwem w spółce (poziom zarządczy, poziom koordynacji i nadzoru, poziom wykonawczy);
- Zdefiniowano rolę i odpowiedzialności za bezpieczeństwo informacji w organizacji:
  - Zarządu Spółki,
  - Koordynatora SZBI – Departamentu Bezpieczeństwa,
  - WI – Właścicieli Informacji,
  - WS – Właścicieli Systemów,

  - Pracowników i współpracowników spółki;
- Dokonano wyboru i opisano metodę analizy ryzyka utraty bezpieczeństwa informacji, w szczególności:
  - sposób zarządzania ryzykiem,
  - częstotliwość i sposób przeprowadzania analizy ryzyka utraty bezpieczeństwa informacji;
- Określono sposób tworzenia i akceptowania planu postępowania z ryzykiem utraty bezpieczeństwa informacji (PPR);
- Utworzono hierarchiczny układ dokumentacji (regulaminy, procedury, instrukcje);
- Zatwierdzono PBI przez Zarząd Spółki;
- Przeprowadzono cykl szkoleń dla kadry.

III. Pilotażowe wdrożenie SZBI (sierpień–grudzień 2005)
- Wytypowano proces zarządzania finansami do pilotażowego wdrożenia systemu (Pion Finansów i Administracji);
- Przeprowadzono klasyfikację informacji;
- Zinwentaryzowano sprzęt, oprogramowanie oraz miejsca przetwarzania informacji;
- Przeanalizowano podatności oraz zagrożenia;
- Przeprowadzono analizę ryzyka;
- Opracowano Plan Postępowania z Ryzykiem i wdrożono działania doskonalące. Opracowano dokumentację bezpieczeństwa (regulaminy, procedury, instrukcje);
- Budowano świadomość pracowników podczas szkoleń z zakresu wdrażanych zasad ochrony informacji, obowiązków i odpowiedzialności za bezpieczeństwo informacji;
- Przeprowadzono wewnętrzne audyty bezpieczeństwa;
- Przeprowadzono przegląd zarządzania bezpieczeństwem na forum Zarządu Spółki.

IV. Certyfikacja Procesu Zarządzania Finansami (grudzień 2005)
- W grudniu 2005 przeprowadzono audyt certyfikujący PTK Centertel przez British Standard Institution – BSI;
- Audyt zakończył się przyznaniem rekomendacji do otrzymania certyfikatu BS 7799-2 **w zakresie zarządzania finansami**.



CERTIFICATE OF REGISTRATION

Information Security Management System

PTK Centertel Sp. z o.o.

Skierniewicka 10A
Warszawa
01-230
Poland

Operate an Information Security Management System which complies with the requirements of

BS 7799:PART 2:2002

for the activities detailed in the scope of registration.

Certificate No: IS 503174

Signed on behalf of BSI

Originally registered: 26 Jan 2006

Expiry Date: 26 Jan 2009

UKAS

BSI Management Systems

Źródło: BSI

V. Wdrożenie SZBI w całej organizacji (styczeń–grudzień 2006)

- Wykonano wszystkie przedsięwzięcia etapu III w pozostałych pionach organizacji.

W grudniu 2006 roku ukończono budowę SZBI (schemat) i przystąpiono do wdrażania i utrzymywania realnych i skutecznych narzędzi do efektywnego zarządzania bezpieczeństwem informacji w spółce.

Struktura zarządzania bezpieczeństwem informacji po wdrożeniu SZBI

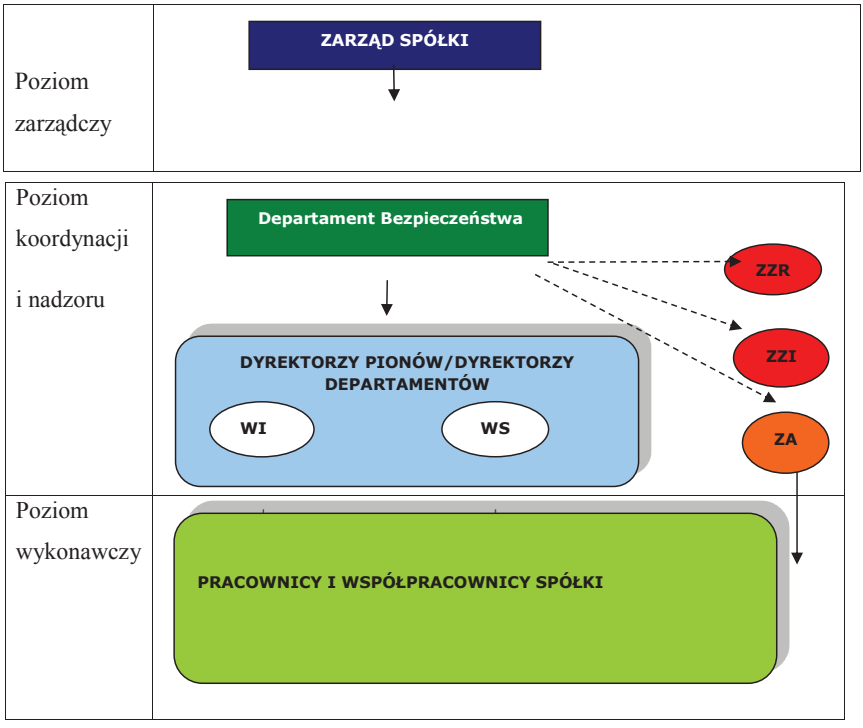
WYMAGANIA BEZPIECZEŃSTWA

- **Prawo polskie (ustawy…)**
- **Prawo międzynarodowe (Ustawa SOX)**
- **Zalecenia Bezpieczeństwa FT**
- **Wspólne zasady ochrony Informacji w GK TP**
- **Norma ISO/IEC 27001**

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Kluczowe elementy strategii spółki w zakresie bezpieczeństwa określające podstawowe procesy regulujące funkcjonowanie systemu

SZBI



CYKLICZNA ANALIZA RYZYKA UTRATY BEZPIECZEŃSTWA INFORMACJI

PLAN POSTĘPOWANIA Z RYZYKIEM

Obejmujący przedsięwzięcia: inwestycyjne, organizacyjne, szkoleniowe itp.

Źródło: opracowanie własne

LEGENDA:

- **Zarząd spółki** – wyznacza cele w zakresie bezpieczeństwa dla całej spółki i nadzoruje SZBI – akceptuje wyniki oceny ryzyka i planu minimalizacji ryzyka utraty bezpieczeństwa informacji.
- **Departament Bezpieczeństwa** – zarządza systemem bezpieczeństwa informacji.
- **ZZR** – Zespół Zarządzania Ryzykiem realizuje proces analizy ryzyka.
- **ZZI** – Zespół Zarządzania Incydentami – analizuje zgłaszane incydenty bezpieczeństwa i inicjuje działania naprawcze.
- **ZA** – pracownicy Departamentu Bezpieczeństwa, którzy przeprowadzają okresowe audyty wewnętrzne bezpieczeństwa pod kątem zebrania informacji niezbędnych do oceny ryzyka.
- **WI** – Właściciel Informacji, osoba zajmująca kierownicze stanowisko, określa poziom bezpieczeństwa dla informacji w podległym obszarze operacyjnym.
- **WS** – Właściciel Systemu informatycznego, realizuje poziom bezpieczeństwa systemu informatycznego adekwatnego do wagi przetwarzanych informacji.

Certyfikacja i wdrożenie SZBI

Po pomyślnym audycie certyfikacyjnym, 12 grudnia 2006 r., PTK Centertel otrzymała z rąk jednostki certyfikacyjnej British Standards Institution Management

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2005

This is to certify that:

PTK Centertel Sp. z o.o.
ul. Skierniewicka 10A
01-230 Warszawa
Poland

Holds Certificate No: IS 503174

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2005 for the following scope:

All operations related to provision of mobile telecommunication services to the clients, as well as all supporting processes. This is in accordance with the Statement of Applicability, Version 4, date 31 October 2008 .

For and on behalf of BSI:

Regional Director, BSI Management Systems (CEMEA)

Originally registered: 09/01/2006 Latest issue: 30/12/2008 Expiry Date: 28/02/2012

Page: 1 of 1

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract. An electronic certificate can be authenticated online. Printed copies can be validated at www.bsi-global.com/ClientDirectory or telephone +44 (0)20 8996 7033.

The British Standards Institution is incorporated by Royal Charter. Management Systems (CEMEA) Headquarters: 389 Chiswick High Road, London, W4 4AL, United Kingdom

BSI Management Systems

Źródło: BSI

Systems certyfikat Nr IS 503174 zgodności zbudowanego SZBI z międzynarodowym standardem ISO 27001 w zakresie wszystkich działań związanych ze świadczeniem usług telefonii ruchomej oraz związanych z działalnością procesów wspomagających.

O powyższym fakcie informowały media krajowe w następujących komunikatach prasowych: „**Certyfikat bezpieczeństwa dla Orange** – BSI Management Systems nadał certyfikat systemu zarządzania bezpieczeństwem informacji firmie PTK Centertel (operator sieci Orange i POP)", „**PTK Centertel/ Orange otrzymała z rąk Dyrektora Firmy BSI Certyfikat Rejestracji zgodności z ISO 27001**. PTK Centertel jest jednym z nielicznych przedsiębiorstw w Polsce, które otrzymało potwierdzenie wdrożenia i uzyskania certyfikatu systemu zarządzania bezpieczeństwem informacji".

Na monitorach komputerów pracowników PTK Centertel 13 lutego 2007 roku pojawił się komunikat: ***Informacje pod specjalną ochroną – PTK Centertel otrzymała certyfikat ISO 27001*** o następującej treści:

„Z dużą satysfakcją informujemy, iż nasza firma uzyskała certyfikat zgodności systemu zarządzania bezpieczeństwem informacji z międzynarodowym standardem ISO 27001. Dołączyliśmy tym samym do grona nielicznych firm sektora telekomunikacyjnego w Europie, które mogą poszczycić się zgodnością z uznanym międzynarodowym standardem w zarządzaniu bezpieczeństwem informacji.

Jesteśmy pierwszym operatorem telekomunikacyjnym na krajowym rynku, który sprostał temu wyzwaniu, wdrażając z sukcesem międzynarodowe standardy bezpieczeństwa.

Efektywny system zarządzania informacją w obliczu zmian otoczenia rynkowego i ostrej konkurencji to jeden z kluczowych procesów we współczesnych organizacjach. Ma istotny wpływ na utrzymanie konkurencyjności, płynności finansowej, zysku, zgodności z przepisami prawa oraz poziomu zaufania partnerów, współpracowników i klientów.

Gratulujemy osiągniętego sukcesu wszystkim pracownikom zaangażowanym we wdrożenie tego systemu w naszej Spółce, a w szczególności pracownikom Departamentu Bezpieczeństwa.

Certyfikat międzynarodowej normy ISO 27001 stawia przed nami nowe wyzwania w zakresie ochrony informacji, tak istotnej w naszej firmie. Pamiętajmy, że w warunkach dynamicznego rozwoju rynku i silnej konkurencji zaufanie klienta i jego przywiązanie do marki Orange stanowią dla nas szczególną wartość. Wymagania, jakie spoczywają na każdym z nas w związku z wdrożonym systemem, powinny być w realizowane w codziennej pracy ze szczególną troską".

Dyrektor Generalny PTK Centertel otrzymał z rąk Dyrektora Pionu Bezpieczeństwa GK TP list gratulacyjny następującej treści:

„Szanowny Panie Dyrektorze,

uprzejmie proszę o przyjęcie serdecznych gratulacji w związku z uzyskaniem przez Polską Telefonię Komórkową Centertel Sp. z o.o. Certyfikatu Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z wymaganiami normy ISO/IEC 27001:2005.

Kierowana przez Pana Spółka otrzymała jako pierwsza w Grupie Kapitałowej TP S.A. i jako pierwsza wśród operatorów komórkowych w Polsce wspomniany Certyfikat.

Nadany przez BSI (British Standard Institute) Management Systems Certyfikat jest potwierdzeniem wdrożenia w PTK Centertel Sp. z o.o. efektywnego systemu zarządzania bezpieczeństwem informacji, którego struktura została zbudowana w oparciu o najlepsze światowe standardy i praktyki wynikające z wymagań wspomnianej normy.

Certyfikat potwierdza także, iż Spółka jest liderem na polskim rynku telekomunikacyjnym również w aspekcie bezpieczeństwa przetwarzanych informacji w ramach świadczonych usług. Wdrożony efektywny system bezpieczeństwa informacji to gwarancja, że abonenci i użytkownicy sieci Orange będą nadal otrzymywać usługi telefonii komórkowej na najwyższym, europejskim poziomie. **Pragnę przy tym dodać, że wdrożenie tego systemu jest zgodne z polityką bezpieczeństwa realizowaną zarówno w Grupie TP, jak i w Grupie FT, oraz zostało bardzo wysoko ocenione przez naszych kolegów z Dyrektoriatu Bezpieczeństwa Grupy FT.**

Korzystając z okazji, pragnę raz jeszcze serdecznie pogratulować osiągniętego sukcesu i wyrazić moje najwyższe uznanie dla profesjonalizmu i zaangażowania kierownictwa oraz oraz pracowników Departamentu Bezpieczeństwa PTK Centertel w realizację tego projektu.

Mam też nadzieję, iż doświadczeniami zdobytymi w trakcie wdrażania w Spółce standardów normy ISO/IEC 27001, pracownicy Departamentu Bezpieczeństwa podzielą się na forum Centrum Zarządzania Bezpieczeństwem Grupy Kapitałowej TP S.A."

Rzeczywiście wdrożenie i certyfikacja SZBI w PTK Centertel nie uszło uwadze naszych kolegów z FT:

From: DULUC Philippe SG [mailto:philippe.duluc@francetelecom.com]
Sent: Wednesday, June 07, 2006 8:03 PM
To: Janusz.Wojciechowski@telekomunikacja.pl
Cc: DUPRAT Julien SOFRECOM
Subject: newsletter

Dear Janusz,

I forgot in my last email (of thanks after my visit in Warsaw) to write about what you have done in Centertel beginning of the year by getting 7799 certification. This is an important new for the group in the field of security: you know that Orange UK got this certification 2 years ago.

I would be very grateful if you agree to provide a small article for our security newsletter (I suppose you are receiving this newsletter) explaining this action and its advantages. I put Julien DUPRAT in copy of this mail: he is in charge of making this newsletter. If necessary, Julien will answer your questions (format, size, etc.)

Sincerely yours, Philippe

Ukazały się liczne artykuły okolicznościowe na ten temat np. DSEC – Info Issue 46 June 2008 – Implementation of ISO 27001 at PTK Centertel sp. z o.o. oraz odnotowano w materiałach sprawozdawczych Grupy FT fakt, iż to właśnie PTK Centertel, jako drugi operator Grupy FT po brytyjskim Orange, został posiadaczem certyfikatu ISO 27001.

Korzyści wynikające z wdrożenia certyfikowanego SZBI

Certyfikat uzyskany od niezależnej organizacji był potwierdzeniem, że PTK Centertel wdrożyła i utrzymuje efektywny system zarządzania bezpieczeństwem informacji, a zarządzanie ochroną informacji odbywa się w sposób sformalizowany i przewidywalny. W konsekwencji pojawiły się nowe szanse rozwojowe, które wzmocniły pozycję rynkową spółki i dostarczyły bezpośrednich korzyści, takich jak:

- zwiększenie zaufania i wiarygodności PTK Centertel jako przedsiębiorcy świadczącego usługi telekomunikacji mobilnej oraz zapewnienie, że powierzone i przetwarzane informacje są w odpowiedni sposób chronione. Pracownicy, partnerzy wiedzą, kto za co odpowiada i jak mają postępować w zakresie ochrony informacji, z którą mają do czynienia. Jasno określone są odpowiedzialność, procedury oraz podejmowane działania. Sam proces zarządzania bezpieczeństwem zawiera mechanizmy kontroli, oceny i doskonalenia funkcjonowania. W szczególności uzyskane korzyści przekładają się bezpośrednio na:

- znaczące obniżenie ryzyka utraty informacji (np. w wyniku jej przypadkowego lub celowego zniszczenia, zgubienia, kradzieży czy przecieku poufnych informacji do prasy lub konkurencji),
- jednolity, jasno i precyzyjnie zdefiniowany standard ochrony informacji,
- zwiększenie kontroli nad wewnętrznym i zewnętrznym przepływem informacji,
- pozyskanie nowych rynków i klientów. Podobnie jak certyfikat ISO 9001, ISO 27001 otwiera drogę do klientów o nieprzeciętnych wymaganiach, dla których spełnienie określonych norm jest podstawowym warunkiem do rozpoczęcia współpracy,
- zapewnienie, że spełnione są wymagania prawa oraz wymagania i zalecenia korporacyjne, do których przestrzegania zobowiązana jest spółka w zakresie:
  - ustawodawstwa polskiego:
    - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
    - ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji,
    - ustawa z dnia 16 lipca 2004 r. prawo telekomunikacyjne,
    - rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
  - zaleceń bezpieczeństwa France Telecom,
  - wymagań ustawy SOX w obszarach 302 „Security of information" oraz 404 „Manage Security",
  - wspólnych zasad ochrony Informacji w GK TP, w tym polityki bezpieczeństwa informacji Grupy TP.

Zmniejszeniu ulega ryzyko naruszenia prawa (np. ujawnienie danych osobowych klientów, tajemnicy telekomunikacyjnej, danych finansowych lub przetwarzanie danych osobowych bez uzyskania stosownej zgody) i w efekcie możliwe jest uniknięcie kar za naruszenie bezpieczeństwa informacji.

- Zabezpieczenie informacji na wypadek katastrof lub awarii – zarządzanie ciągłością działania.
- Dostosowanie systemu bezpieczeństwa informacji do unijnych i światowych standardów oraz dołączenie do elitarnego grona organizacji posiadających certyfikat na zgodność systemu zarządzania z wymaganiami standardu ISO 27001.
- Budowanie wizerunku firmy profesjonalnej.
- Wzrost świadomości pracowników w zakresie kultury bezpieczeństwa i ochrony informacji.

Wnioski końcowe

- dokonana ocena stanu bezpieczeństwa w oparciu o jedenaście rozdziałów normy ISO/IEC 27001 pozwoliła kompleksowo zidentyfikować problemy bezpieczeństwa w spółce;
- zaangażowanie najwyższego kierownictwa było podstawowym motorem sukcesu wdrożenia rozwiązań bezpieczeństwa;
- piony biznesowe wykazują duże zainteresowanie współpracą i aktywnie uczestniczą w procesach zarządzania bezpieczeństwem informacji po zapewnieniu im wsparcia;
- zauważalnym dziś sukcesem jest zaszczepienie dbałości o bezpieczeństwo informacji u pracowników na każdym szczeblu. Jednocześnie jest to najtrudniejsze zadanie przy wdrażaniu SZBI;
- poważnym problemem we wdrażaniu SZBI było pokonanie niechęci do zaangażowania się pionu IT w implementację wymaganych normą ISO 27001 rozwiązań systemowych. Niechęć ta wynikała z tradycyjnej optyki patrzenia IT na bezpieczeństwo informacji, tzn. sprowadzania zagadnień bezpieczeństwa informacji do bezpieczeństwa teleinformatycznego. Ponadto obawy IT przed zmianami były powodem nieporozumień w pracach projektowych.

The implementation of "SZBI" by Polish Mobile Phone Company Centertel, the operator of Orange

Abstract: Information is one of the most important tools for obtaining competitive advantage, and its safety is a key element of the entrepreneur and essential credibility to meet the requirements of the law. The effectiveness of informational protection in organizations is not possible by the old means: by door lock, firewalls and password-protected computer. It is essential to take a comprehensive approach to complex security issues. Article recounts the course of design and implementation of the construction of the Polish Mobile Phone "Centertel" – the mobile phone network operator Orange – Information Security Management System (ISMS), consistent with the requirements of ISO / IEC 27001:2005. Full implementation of the system and its certification was preceded by a pilot implementation in a selected functional area businesses. In conclusion, the paper presents the benefits of implementing the system and formulates practical conclusions.