



Ratels

Data Security Project Management Consulting

Bezpieczeństwo Informacji

Zarządzanie projektami

Doradztwo

Szkolenia

Oferta

RATELS – autoryzowany partner:

websense
ESSENTIAL INFORMATION PROTECTION™

AUREA[®]
BUSINESS PROCESS MANAGEMENT

WebSpy[®]

Propentus
www.propentus.com

Wersja dokumentu: 4.0

RATELS s.c.

NIP: 522-291-48-55
REGON: 141773253

www.ratels.pl
biuro@ratels.pl

tel: +48 601 143 892
tel: +48 516 958 519

Strona 1 z 14

Spis treści oferty:

O RATELS	3
OPIS OFERTY	4
AUDYTY ZGODNOŚCI.....	4
AUDYTY BEZPIECZEŃSTWA	4
<i>Testy penetracyjne i analiza konfiguracji systemów IT</i>	4
<i>Testy bezpieczeństwa systemów IT/aplikacji</i>	4
<i>Audyty dopuszczające</i>	4
<i>Analizy zabezpieczeń stacji roboczych</i>	5
<i>Weryfikacje zabezpieczeń fizycznych pomieszczeń, w których są przetwarzane dane chronione</i>	5
<i>Weryfikacje zabezpieczeń serwerowni</i>	5
<i>Analizy procesu zarządzania użytkownikami i ich uprawnieniami w systemach</i>	5
<i>Weryfikacje uprawnień w systemach</i>	5
<i>Analizy wykorzystania Internetu przez pracowników</i>	5
<i>Weryfikacje zagrożeń potencjalnych źródeł wycieku danych</i>	5
<i>Audyty funkcjonowania systemów bezpieczeństwa</i>	6
<i>Audyty stanu zasobów IT</i>	6
BUDOWA SYSTEMÓW I MECHANIZMÓW BEZPIECZEŃSTWA INFORMACJI.....	7
<i>Dokumentacja bezpieczeństwa zgodna z normami ISO 27000</i>	7
<i>Systemy Zarządzania Bezpieczeństwem Informacji</i>	7
<i>Systemy monitorowania wykorzystania Internetu</i>	7
<i>Systemy zapobiegające wyciekowi informacji z firmy</i>	7
<i>Systemy bezpiecznego przesyłania informacji</i>	8
<i>Plany ciągłości działania</i>	8
<i>Wskaźniki efektywności systemów bezpieczeństwa</i>	8
<i>Systemy zarządzania ryzykiem</i>	8
<i>Odzyskiwanie danych / bezpieczne usuwanie danych</i>	8
ANALIZA RYZYKA	9
OCHRONA DANYCH OSOBOWYCH I TAJEMNICY PRZEDSIĘBIORSTWA	9
<i>Administrator bezpieczeństwa informacji (ABI)</i>	9
<i>Zgłaszanie/aktualizacja zbiorów danych do GIODO</i>	9
<i>Zgodność z ustawą o ochronie danych osobowych</i>	9
<i>Tajemnica przedsiębiorstwa</i>	10
ZARZĄDZANIE PROJEKTAMI.....	10
USŁUGI DORADCZE.....	10
SZKOLENIA.....	11
<i>Bezpieczeństwo informacji</i>	11
<i>Zarządzanie projektami</i>	11
PRODUKTY	12
<i>WebSpy – monitorowanie aktywności w Internecie i analiza logów</i>	12
<i>Websense – ochrona przed wyciekiem informacji</i>	12
<i>PPM – zarządzanie prawami dostępu</i>	13
<i>proCertum Form – bezpieczne przesyłanie dokumentów</i>	13
<i>Aurea - automatyzacja procesów biznesowych</i>	13
<i>Risicare – analiza ryzyka bezpieczeństwa informacji</i>	13
KONTAKT	14

RATELS s.c.

O Ratels

Jesteśmy zespołem doświadczonych specjalistów dysponujących wieloletnim doświadczeniem nabytym podczas pracy dla największych firm sektora finansowego i ubezpieczeniowego. Posiadamy wyższe wykształcenie techniczne poparte wieloletnią praktyką wynikającą z pracy na stanowiskach technicznych oraz menedżerskich w działach IT dużych firm. Legitymujemy się także prestiżowymi certyfikatami zawodowymi.

Szerokie doświadczenie naszych specjalistów bezpieczeństwa informacji potwierdzone jest między innymi certyfikatami CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), CISA (Certified Information Systems Auditor) oraz Audytora wiodącego systemu ISO 27001.

Nasi kierownicy projektów prowadzili zarówno małe projekty, jak i duże, obejmujące swoim zasięgiem cały kraj oraz wiele zespołów wykonawczych i podwykonawców. Uczestniczyli także w projektach międzynarodowych. Doświadczenie nabyli między innymi w projektach realizowanych dla największych firm finansowych w Europie środkowej oraz dla firm sektora ubezpieczeniowego z państw WNP i Wielkiej Brytanii a także Unii Europejskiej. Posiadają certyfikaty PRINCE2TM Foundation oraz PRINCE2TM Practitioner.

Nasi konsultanci posiadają także certyfikaty producentów rozwiązań m.in.: Cisco oraz Microsoft.

Dzięki kompetencjom specjalistów oraz wysokiej jakości świadczonych usług, naszymi klientami są firmy różnych sektorów i różnej wielkości, m.in.: Netia, Polska Agencja Rozwoju Przedsiębiorczości, Raiffeisen Bank Polska, Inteligo Financial Services, Unizeto Technologies, Kancelaria prawna Wardyński i Wspólnicy, Urząd Dozoru Technicznego. Z naszych usług, jako podwykonawców, korzystały między innymi Ministerstwo Transportu i Telekomunikacji Republiki Albanii (podwykonawca EGIS Route) oraz Ministerstwo Spraw Zagranicznych RP (podwykonawca Koncept). Aktualna lista referencyjna naszych klientów dostępna jest na naszej stronie: <http://www.ratels.pl/index.php/referencje.html>

Jesteśmy także autoryzowanym partnerem Websense, WebSpy, Propentus oraz Tecna (producent Aurea BPM). Dzięki autoryzacji możemy oferować naszym klientom skuteczne rozwiązania podnoszące bezpieczeństwo informacji oraz wydajność pracy.

Oferta RATELS obejmuje usługi związane z szeroko rozumianym bezpieczeństwem informacji. Zajmujemy się zarówno bezpieczeństwem informatycznym, jak i zagadnieniami formalno-prawnymi i organizacyjnymi ochrony informacji. Jako jedna z niewielu firm oferujemy więc szerokie i kompleksowe spojrzenie na sprawy bezpieczeństwa.

Drugim obszarem naszej działalności są usługi w zakresie zarządzania projektami. Profesjonalne zarządzanie każdym etapem projektu jest bowiem gwarancją pomyślnego zakończenia każdego projektu.

Korzystając z naszego bogatego doświadczenia wspieramy także naszych Klientów świadcząc usługi doradcze w zakresie systemów informatycznych oraz organizacji działów bezpieczeństwa oraz działów IT.

Nasze usługi to gwarancja wysokiej jakości w rozsądnej cenie!

RATELS s.c.

Poniżej przedstawiamy szczegółowy opis naszych usług. Jeżeli Państwa potrzeby wykraczają poza poniższą ofertę prosimy o kontakt.

Opis oferty

Audyty zgodności

Sprawdzamy, w jakim stopniu pracownicy przestrzegają istniejących w firmie regulacji dotyczących bezpieczeństwa informacji. Testy są realizowane z wykorzystaniem metod socjotechnicznych.

Weryfikujemy dokumentację bezpieczeństwa (polityka bezpieczeństwa wraz z dokumentami szczegółowymi i procedurami) pod kątem aktualności, kompletności oraz poprawności merytorycznej, a także zgodności z obowiązującym prawem i standardami.

Wykonujemy audyt zgodności Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) z wymogami prawa oraz wewnętrzną dokumentacją bezpieczeństwa.

Audyty bezpieczeństwa

Wykonujemy:

Testy penetracyjne i analiza konfiguracji systemów IT

Dzięki testom możliwe jest wykrycie faktycznych oraz potencjalnych luk i błędów w oprogramowaniu, konfiguracji urządzeń informatycznych, portalach i aplikacjach webowych, które mogą być wykorzystane do naruszenia bezpieczeństwa przetwarzanych informacji, a także bezpieczeństwa firmy lub jej klientów.

Testy bezpieczeństwa systemów IT/aplikacji

Weryfikacja bezpieczeństwa jest istotnym elementem procesu twórczego i zdawczo-odbiorczego. Nasze testy, wykonywane również podczas procesu twórczego, pozwolą na zbudowanie/wdrożenie systemu gwarantującego wymagany poziom bezpieczeństwa.

Audyty dopuszczające

Dokonyjemy sprawdzenia firmy-podwykonawcy pod kątem spełniania wymagań stawianych przez firmę-zleceniodawcę odnośnie bezpieczeństwa przetwarzania danych zleceniodawcy w siedzibie i systemach podwykonawcy.

Weryfikujemy stan zabezpieczeń przed powierzeniem przetwarzania danych chronionych. Dzięki naszemu audytowi firma przekazująca do przetwarzania informacje chronione do podwykonawcy ma możliwość upewnienia się, czy dane te będą należycie zabezpieczone. Audyt obejmuje elementy analizy ryzyka oraz weryfikację, czy podwykonawca spełnia wszystkie zalecenia i standardy wymagane przez firmę-właściciela informacji. Pozytywna rekomendacja z audytu powinna być warunkiem koniecznym do rozpoczęcia współpracy z podwykonawcą. W przypadku stwierdzenia przez naszych audytorów niedociągnięć, współpraca powinna nastąpić po ich usunięciu.

RATELS s.c.

Analizy zabezpieczeń stacji roboczych

Sprawdzamy skuteczność zabezpieczeń, chroniących przed wyciekami danych chronionych lub instalacją niedozwolonego lub złośliwego oprogramowania na stacji roboczej.

Weryfikacje zabezpieczeń fizycznych pomieszczeń, w których są przetwarzane dane chronione

Sprawdzamy skuteczność i zgodność zabezpieczeń z wymogami prawa i dobrych praktyk.

Weryfikacje zabezpieczeń serwerowni

Analizujemy istniejące zabezpieczenia pod kątem skuteczności ich działania i zapewnienia niezawodnej pracy serwerowni. Analizujemy rozwiązania bezpieczeństwa fizycznego, środowiskowego oraz ciągłości pracy. Analizujemy także procedury bezpieczeństwa i awaryjne.

Analizy procesu zarządzania użytkownikami i ich uprawnieniami w systemach

Analizujemy istniejący stan procesu zarządzania użytkownikami pod kątem jego optymalizacji, zdefiniowania potencjalnych ról z przypisanymi zakresami uprawnień. Wyniki naszej analizy mogą być wykorzystane w celu przejścia z tradycyjnego sposobu zarządzania uprawnieniami w systemach na zarządzanie uprawnieniami przez role.

Weryfikacje uprawnień w systemach

Weryfikujemy rzeczywiste uprawnienia użytkowników w systemach informatycznych z istniejącym rejestrem/bazą wniosków o nadanie/zmianę uprawnień.

Analizy wykorzystania Internetu przez pracowników

Analizujemy wielopłaszczyznowo i prezentujemy zrozumiałym językiem biznesowym informacje o sposobie wykorzystania Internetu, zarówno zbiorczo na poziomie całej firmy, jak i przez poszczególne działy lub pojedynczych pracowników.

Weryfikacje zagrożeń potencjalnych źródeł wycieku danych

Analizujemy i dokonujemy oceny poziomu zagrożenia związanego z wyciekami danych z systemów informatycznych (zarządzanie prawami dostępu, stacje robocze, nośniki przenośne, Internet, poczta elektroniczna).

Audyty funkcjonowania systemów bezpieczeństwa

Wykonujemy kompleksową analizę skuteczności działania, analizę procedur utrzymaniowych i monitorowania systemów bezpieczeństwa. Weryfikujemy także poprawność ich konfiguracji. Weryfikujemy lub opracowujemy wskaźniki efektywności. Za systemy bezpieczeństwa uważamy np.:

- System antywirusowy
- System antyspamowy
- System DLP (Data Leak Prevention/Data Loss Prevention)
- System Proxy
- System Firewall
- System backupowy
- System zasilania awaryjnego

Audyty stanu zasobów IT

Przygotowujemy opis istniejącego stanu zasobów IT oraz procedur i mechanizmów funkcjonowania działu IT. Taki opis, jako audyt otwarcia, jest szczególnie przydatny menedżerom, którzy obejmują w zarządzanie dział IT. Dzięki audytowi stanu zasobów, menedżerowie są w stanie szybko rozpoznać istniejący stan w zarządzanym dziale i bez zbędnej zwłoki podejmować odpowiednie działania zarządcze. Audyt stanu zasobów obejmuje na przykład takie działania jak:

- Opracowanie zestawienia zasobów kadrowych z przyporządkowaniem do systemów
- Opracowanie zestawienia dokumentacji regulującej pracę IT i bezpieczeństwo
- Opracowanie zestawienia posiadanych licencji na oprogramowanie
- Opracowanie zestawienia posiadanego sprzętu komputerowego (stacje robocze, drukarki, serwery, urządzenia sieciowe)
- Opracowanie zestawienia obowiązujących umów IT
- Opracowanie zestawienia sprzętu - inwentaryzacja
- Opracowanie zestawienia oprogramowania systemowego/narzędziowego
- Opracowanie zestawienia oprogramowania zainstalowanego na stacjach roboczych
- Opracowanie zestawienia aplikacji
- Weryfikacja zarządzania incydentami, problemami
- Weryfikacja zarządzania zmianą (w zakresie sprzętu i/lub aplikacji)
- Weryfikacja zarządzania pojemnością
- Weryfikacja zarządzania siecią LAN, WAN, stykiem z Internetem
- Weryfikacja kompletności i skuteczności procedur operacyjnych IT

Budowa systemów i mechanizmów bezpieczeństwa informacji

Dokumentacja bezpieczeństwa zgodna z normami ISO 27000

Aktualizujemy istniejącą, lub budujemy od podstaw, dokumentację bezpieczeństwa zgodną z normami ISO 27000. Przedmiotem prac są dokumenty główne polityki bezpieczeństwa, a także procedury szczegółowe.

Systemy Zarządzania Bezpieczeństwem Informacji

Budujemy oraz wdrażamy System Zarządzania Bezpieczeństwem Informacji (SZBI) zgodny z normą PN-ISO/IEC 27001. Dla istniejących systemów wykonujemy aktualizacje, także cykliczne SZBI lub jego dopasowanie do wymagań normy PN-ISO/IEC 27001 oraz innych aktualnych przepisów. Przeprowadzamy także audyt istniejącego SZBI pod względem zgodności z obowiązującymi przepisami oraz normą PN-ISO/IEC 27001.

Systemy monitorowania wykorzystania Internetu

Projektujemy i wdrażamy systemy monitorowania wykorzystania Internetu w firmie. Dzięki naszym systemom, każdy menedżer uzyska przystępną informację biznesową o tym, co tak naprawdę dzieje się w podległych mu zespołach, na ile efektywni są jego pracownicy, czy nie ma próby wykorzystywania Internetu do celów niesłużbowych lub wręcz zagrażających firmie.

Systemy zapobiegające wyciekowi informacji z firmy

Ochrona firm przed zamierzonym lub przypadkowym wyciekami poufnych informacji jest kluczowym wyzwaniem biznesowym i technicznym, przed którym stają obecnie organizacje. Z powodu tego złożonego problemu osoby odpowiedzialne za bezpieczeństwo informacji w firmie zmuszone są chronić swoje dane przy narastającej presji ze strony regulacji i korporacyjnych zarządzeń, klientów i konkurencji oraz upublicznianiu i rosnących kosztach wycieków danych.

Projektujemy i wdrażamy w oparciu o sprawdzone rozwiązania systemy zapobiegające wyciekowi informacji z firmy. Dzięki naszym systemom, każdy menedżer uzyska pewność, że informacje stanowiące tajemnicę firmy lub informacje, które muszą pozostać pod kontrolą nie opuszczą firmy i nie przedostaną się do konkurencji lub innych niepożądanych odbiorców. Jednocześnie dostępna jest pełna informacja o próbach podejmowania działań prowadzących do ujawnienia informacji.

Systemy bezpiecznego przesyłania informacji

Projektujemy i wdrażamy systemy do bezpiecznego przesyłania informacji między oddziałami firmy lub między firmą a jej kontrahentami lub agencjami. Dzięki naszym systemom, wykorzystującym mechanizmy kryptograficzne oraz infrastrukturę klucza publicznego (PKI), informacje są przesyłane w sposób zapewniający poufność, integralność oraz pełną rozliczalność. Dzięki mechanizmom poświadczenia nadania i odbioru, zarówno nadawca, jak i odbiorca mają pewność, że informacja została wysłana i dotarła do adresata.

Plany ciągłości działania

Opracowujemy lub weryfikujemy plany ciągłości działania firmy na wypadek zaistnienia sytuacji kryzysowych. Oferujemy również oprogramowanie, które pozwala zamodelować plan ciągłości działania i procedury awaryjne. Dzięki takiemu systemowi możliwe jest przeprowadzenie testów planów awaryjnych/ciągłości działania w sytuacjach zbliżonych do rzeczywistych (pozwala to na utrzymywanie aktualności planów, identyfikację i eliminację słabych punktów). W przypadku rzeczywistego zagrożenia, dzięki naszemu systemowi, plany wykonywane są w sposób uporządkowany i zgodnie z założoną sekwencją, a kierownictwo w każdej chwili ma informację, na jakim etapie jest realizacja planu awaryjnego.

Wskaźniki efektywności systemów bezpieczeństwa

Projektujemy i wdrażamy wskaźniki efektywności systemów bezpieczeństwa. Dzięki wskaźnikom możliwe jest dokonywanie obiektywnej i miarodajnej oceny, zarówno skuteczności działania systemów bezpieczeństwa, jak i oceny pracy pracowników działu bezpieczeństwa w firmie.

Systemy zarządzania ryzykiem

Projektujemy i wdrażamy systemy pozwalające na zarządzanie ryzykiem w bezpieczeństwie informacji. Dzięki naszym rozwiązaniom możliwe jest sprawne wykonanie m.in. analizy ryzyka w sposób efektywny i kompleksowy. System zarządzania ryzykiem jest szczególnie przydatny w firmach, które są zobligowane przez obowiązujące przepisy do regularnego wykonywania analizy ryzyka.

Odzyskiwanie danych / bezpieczne usuwanie danych

Odzyskujemy utracone dane z nośników danych. Wykonujemy również bezpieczne usuwanie danych, które polega na nieodwracalnym usunięciu (zamazaniu) danych, w sposób uniemożliwiający ich ponowne odtworzenie (również przy zastosowaniu profesjonalnych metod odzyskiwania danych).

Analiza ryzyka

Wykonujemy analizę ryzyka bezpieczeństwa informacji. Analiza ryzyka umożliwia wyznaczenie najważniejszych kierunków działań dla podniesienia poziomu bezpieczeństwa firmy oraz racjonalizację wydatków na bezpieczeństwo. Oferujemy szeroki zakres usług związanych z przeprowadzeniem analizy ryzyka:

- o Opracowanie i/lub wdrożenie metodyki oceny ryzyka zgodnego z normami PN-ISO/IEC 27001:2007 oraz PN-ISO/IEC 27005:2010
- o Wykonywanie analizy ryzyka (okresowej lub przed certyfikacją zgodności) zgodnie z normami PN-ISO/IEC 27001:2007 oraz PN-ISO/IEC 27005:2010
- o Ocena potrzeby wdrożenia systemu bezpieczeństwa
- o Analiza ryzyka szczytkowego po wdrożeniu systemu bezpieczeństwa
- o Analiza ryzyka w ramach projektu i wdrożenia systemu informatycznego
- o Analiza ryzyka bezpieczeństwa informacji w firmie-podwykonawcy przed rozpoczęciem lub w trakcie współpracy pomiędzy nią, a firmą-zleceniodawcą

Ochrona danych osobowych i tajemnicy przedsiębiorstwa

Administrator bezpieczeństwa informacji (ABI)

Każda firma, która przechowuje/przetwarza dane osobowe wyznacza Administratora Bezpieczeństwa Informacji (ABI) - osobę, która odpowiada za bezpieczeństwo informacji. Jeżeli taka osoba nie zostanie wskazana, pełną odpowiedzialność ponosi Kierownictwo firmy. Oferujemy usługę polegającą na wskazaniu/wydelegowaniu do Klienta konkretnej osoby, która będzie pełnić rolę Administratora Bezpieczeństwa Informacji (ABI). Dzięki temu kierownictwo Klienta przenosi odpowiedzialność za ochronę danych, wynikającą z przepisów ustawy o ochronie danych osobowych.

Zgłaszanie/aktualizacja zbiorów danych do GIODO

Zbiory danych, które nie podlegają ustawowemu zwolnieniu, muszą być zgłoszone do GIODO. Każda zmiana ich charakteru lub zakresu gromadzonej informacji musi również zostać zgłoszona w formie aktualizacji. Oferujemy pomoc w zakresie przygotowywania wniosków zgłoszeniowych lub aktualizacyjnych i dokonanie zgłoszenia lub aktualizacji w imieniu Klienta.

Zgodność z ustawą o ochronie danych osobowych

Weryfikujemy istniejące rozwiązania (techniczne, formalne i organizacyjne) pod kątem zgodności z Ustawą o ochronie danych osobowych oraz odpowiednimi rozporządzeniami. Przygotowujemy odpowiednią dokumentację (lub uzupełniamy braki w istniejącej), definiujemy odpowiednie struktury organizacyjne oraz wskazujemy rozwiązania organizacyjne, techniczne i formalne, których spełnienie jest wymagane przez Ustawę oraz odpowiednie rozporządzenia.

Tajemnica przedsiębiorstwa

Wspieramy w poprawnym zdefiniowaniu tajemnicy przedsiębiorstwa. Weryfikujemy istniejące lub pomagamy zbudować i wdrożyć rozwiązania organizacyjne, formalne i techniczne, których celem jest ochrona tajemnicy przedsiębiorstwa.

Zarządzanie projektami

Oferujemy wysokiej jakości usługi zarządzania projektami informatycznymi zgodnie z metodyką PRINCE2. Współpraca z nami to ograniczenie stałych kosztów posiadania pracownika na etat oraz wykorzystanie dużego doświadczenia i głębokiej wiedzy naszych specjalistów.

- Zarządzamy całymi projektami lub pomagamy w wybranych obszarach, zgodnie z potrzebami Klienta
- Pomagamy rozwiązać problemy w istniejących projektach
- Ratujemy projekty zagrożone
- Pomagamy w definiowaniu i organizowaniu nowych projektów

Usługi doradcze

Świadczymy usługi doradcze w obszarze IT. Dzięki doświadczeniu menedżerskiemu i technicznemu pomagamy wybrać optymalne rozwiązania oraz ograniczyć koszty. Wspieramy naszego Klienta w całym obszarze IT:

- Analizujemy potrzeby biznesowe firmy
- Usprawniamy pracę działów IT
- Pomagamy zdefiniować założenia i wymagania funkcjonalne
- Pomagamy przygotować uzasadnienie biznesowe, koncepcje i założenia techniczne
- Wspieramy w rozmowach z dostawcami systemów informatycznych
- Pomagamy wybrać optymalną ofertę
- Pomagamy zarządzać dostawcami rozwiązań IT

Szkolenia

Uzupełnieniem naszej oferty są szkolenia specjalistyczne. Poniżej zamieszczone są propozycje szkoleń standardowych. Na życzenie opracowujemy również nowe tematy szkoleń lub modyfikujemy programy szkoleń już istniejących w celu jak najlepszego dopasowania się do potrzeb Klienta.

Bezpieczeństwo informacji

Kod	Nazwa szkolenia	Czas trwania
BI01	„Tajemnice firmy” - Szkolenie dla pracowników	1 dzień
BI02	„Tajemnice firmy” - Szkolenia dla kadry zarządzającej	1 dzień
BI03	Testy bezpieczeństwa z wykorzystaniem metod socjotechnicznych – praktyczne podejście do zagadnienia	1 dzień
BI04	Czym powinien zajmować się zespół ds. bezpieczeństwa? – praktyczne podejście do zagadnienia	1 dzień
BI05	Pozyskiwanie informacji o firmach i ich pracownikach z ogólnie dostępnych w Internecie źródeł - praktyczne podejście do zagadnienia	1 dzień
BI06	Odzyskiwanie i bezpieczne usuwanie danych – normy, praktyka, narzędzia	1 dzień
BI07	Bezpieczeństwo sieci bezprzewodowych	1 dzień
BI08	Techniki przełamania zabezpieczeń systemów i aplikacji	3 dni
BI09	Podstawy podpisu elektronicznego	1 dzień
BI10	Podstawy Infrastruktury Klucza Publicznego (PKI)	1 dzień
BI11	Podstawy kryptografii	1 dzień
BI12	Zarządzanie ryzykiem w bezpieczeństwie informacji, zgodne z normami PN-ISO/IEC 27001:2007 oraz PN-ISO/IEC 27005:2010	2 dni

Zarządzanie projektami

Kod	Nazwa szkolenia	Czas trwania
PM01	Skuteczny Kierownik Projektu w oparciu o metodykę PRINCE2™	2 dni

RATELS s.c.

Produkty

Oferujemy sprzedaż oraz wdrożenie specjalizowanych rozwiązań. Dzięki posiadanym autoryzacjaom możemy świadczyć usługi z zachowaniem najwyższej jakości.

WebSpy – monitorowanie aktywności w Internecie i analiza logów

Oprogramowanie WebSpy umożliwia monitorowanie, analizowanie i raportowanie wykorzystania Internetu, poczty elektronicznej e-mail oraz sieci w firmie. Na podstawie logów z urządzeń sieciowych i serwerów, oprogramowanie przygotowuje zaawansowane raporty, zarówno przekrojowe, jak i szczegółowe zawierające te informacje, które są oczekiwane przez użytkownika. Dzięki przejrzystości i jasnemu sposobowi prezentacji informacji, raporty są wsłaniałym narzędnem nie tylko dla działów technicznych, ale przede wszystkim dla osób zarządzających działem lub całą firmą. Rozwiązania WebSpy są nieinwazyjne i skalowalne. Poprzez wybór odpowiedniego produktu możliwe jest dopasowanie rozwiązania do wielkości firmy oraz jej budżetu.

Więcej o oprogramowaniu na:

<http://www.webspy.com>

Websense – ochrona przed wyciekami informacji

Websense Data Security Suite to wiodące rozwiązanie chroniące przed przypadkowym jak i zamierzonym wyciekami danych zarówno na zewnątrz jak i wewnątrz organizacji. Websense Data Security Suite odnajduje miejsce przechowywania danych w sieci, monitoruje kto i w jaki sposób używa tych danych i pomaga chronić dane zabezpieczając procesy biznesowe. Wspomaga także zarządzanie ryzykiem i zapewnia spełnienie wysokich standardów zarządzania dostępem do informacji.

Websense Data Security Suite to jedyne rozwiązanie do ochrony przed utratą danych (DLP), które definiuje zawartość, kontekst, przeznaczenie wiadomości pozwalając administratorom zarządzać tym kto, jak i gdzie może przesyłać określone informacje.

Websense Data Security Suite znacznie wychodzi poza proste rozwiązanie porównujące słowa kluczowe i wzorce. Websense dostarcza technologii Deep Content Control™ aby wykrywać, monitorować i chronić poufne informacje w tym dane personalne, regulacje i własność intelektualną, bez względu na typ lub format plików.

Więcej o oprogramowaniu na:

<http://www.websense.com>

PPM – zarządzanie prawami dostępu

PPM (Propentus Permission Manager) jest rozwiązaniem klasy Access Rights Management dla średnich i dużych firm oraz korporacji. PPM umożliwia firmom w sposób efektywny i optymalny kosztowo zarządzać prawami dostępu do systemów informatycznych (przydzielanie praw, weryfikacja posiadanych praw dostępu, odbieranie praw) oraz dostępu do innych zasobów (np. służbowe telefony, samochody, sprzęt), czy obszarów (np. przepustki, karty dostępu). PPM jest w pełni funkcjonalnym i kompletnym systemem, który potrafi sprostać wszystkim wyzwaniom, które związane są z procesem zarządzania prawami dostępu (access rights management). PPM może być łatwo dostosowany do potrzeb firmy/organizacji.

Więcej o oprogramowaniu na:

http://www.propentus.com/en/products/identity_management.html

proCertum Form – bezpieczne przesyłanie dokumentów

proCertum Form umożliwia bezpieczne przesyłanie dokumentów elektronicznych w postaci podpisanych elektronicznie i zaszyfrowanych plików. Możliwa jest również obsługa plików, które nie są podpisane elektronicznie i szyfrowane. Może być wykorzystywany do bezpiecznej wymiany dowolnych dokumentów, przesyłanych z wielu lokalizacji (oddziałów, placówek terenowych, komórek organizacyjnych) do centralnego serwera (centrali).

Więcej o oprogramowaniu na:

http://www.unizeto.pl/unizeto/uni.oferta_proCertum_Form.xml

Aurea - automatyzacja procesów biznesowych

Aurea BPM to system zarządzania procesami biznesowymi w firmie. Aurea wspiera modelowanie, automatyzowanie, zarządzanie i optymalizowanie procesów biznesowych. System umożliwia zarządzanie wszystkimi procesami w firmie (np. produkcyjnymi, zaopatrzeniowymi, marketingowo-sprzedażowymi, finansowymi, administracyjnymi), w tym także procesami składającymi się na efektywnie działający system ochrony informacji.

Więcej o oprogramowaniu na:

<http://www.aurea-bpm.com>

Risicare – analiza ryzyka bezpieczeństwa informacji

Risicare to oprogramowanie do wykonywania analizy ryzyka bezpieczeństwa informacji zgodnie z normą ISO 27005 w oparciu o metodę MEHARI. Oprogramowanie RISICARE może zostać dostosowane do specyficznych wymagań Klienta. RISICARE jest narzędziem zalecanym przez Clusif i ma akceptację większości instytucji światowych związanych z bezpieczeństwem, w tym ANSI-Quebec, ANSI-Tunezja i ANSI-Luxemburg. RISICARE aktualnie jest stosowana przez ponad 300 podmiotów na świecie. Oferujemy oprogramowanie w wersji polskojęzycznej.

Więcej o oprogramowaniu na:

<http://www.risicare.fr>

Kontakt

Celem omówienia szczegółów naszej oferty lub przedyskutowania Państwa potrzeb zapraszamy do kontaktu:

Sławomir Michałowski

tel: +48 516 958 519

e-mail: s.michalowski@ratels.pl

Krzysztof Olszewski

tel: +48 601 143 892

e-mail: k.olszewski@ratels.pl