

# BEZPIECZEŃSTWO



## Zarządzanie bezpieczeństwem informacji



Według nas aspekt bezpieczeństwa pozostaje niekwestionowanym priorytetem w codziennym życiu Twojej firmy. Efektywne zarządzanie bezpieczeństwem wymaga zaangażowania potencjału wiedzy nie podlegającego dewaluacji. Orientacja ta sugeruje ustanowienie trwałych relacji z kompetentnym partnerem, jakim jest Wola Info. Pozyskanie zaufanego doradcy i reaktywnego kooperanta rozkładającego przewencyjny parasol nad infrastrukturą informatyczną, będzie gwarantem bezpieczeństwa danych.

## ■ ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI W PRZEDSIĘBIORSTWIE

### Znaczenie informacji we współczesnym przedsiębiorstwie

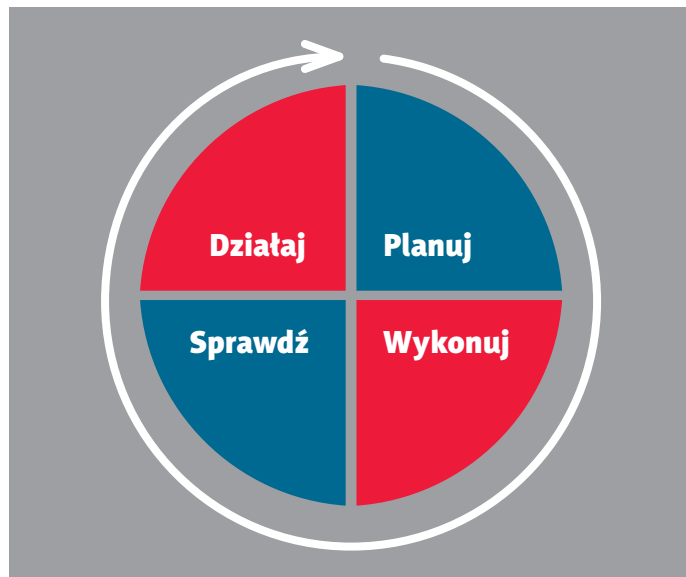
Informacja i jej ciągła dostępność stanowią fundament prawidłowego funkcjonowania coraz większej liczby organizacji. Dane, które są składowane i przetwarzane głównie w systemach teleinformatycznych przedsiębiorstwa, służą nie tylko pracownikom ale podlegają wymianie z partnerami biznesowymi w zakresie realizacji statutowych zadań firmy. Ponadto informacja udostępniana jest także inwestorom w przypadku prezentacji wyników działania organizacji oraz klientom jako potwierdzenie zrealizowanych zobowiązań. Utrata integralności, dostępności lub poufności informacji na każdym z etapów jej życia może prowadzić do strat finansowych, konsekwencji prawnych, czy zakłócenia ciągłości działania przedsiębiorstwa. Rezultatem braku optymalnego bezpieczeństwa informacji może być utrata wizerunku przedsiębiorstwa, a nawet koniec dalszego istnienia na rynku. W profesjonalnie zarządzanych organizacjach świadomość wartości informacji w biznesie jest nieodłącznym atrybutem strategii rozwoju elementów bezpieczeństwa informacji.

Zapewnienie bezpieczeństwa informacji jest zadaniem złożonym, wymagającym usystematyzowanego podejścia – wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (ang. Information Security Management System) obejmującego następujące obszary:

- bezpieczeństwa teleinformatycznego
- bezpieczeństwa osobowego
- bezpieczeństwa prawnego
- bezpieczeństwa fizycznego

Warunkiem osiągnięcia maksymalnego poziomu bezpieczeństwa informacji jest kompleksowe objęcie systemem wymienionych powyżej obszarów.

System Zarządzania Bezpieczeństwem Informacji oparty na ogólnie przyjętych standardach (polska norma PN-ISO/IEC 27001:2007) pozwala ocenić zdolności instytucji do spełniania wymagań postawionych wewnątrz organizacji oraz z punktu widzenia oczekiwań klientów lub organów nadzoru.



Odpowiednie zaprojektowanie i wdrożenie SZBI uzależnione jest od precyzyjnie zdefiniowanych celów biznesowych, potrzeb przedsiębiorstwa, realizowanych procesów i zachodzących między nimi interakcji oraz wielkości i struktury instytucji.

Podejście procesowe (Planuj, Wykonuj, Sprawdź, Działaj) koncentruje uwagę użytkowników na następujących zagadnieniach:

- zrozumieniu biznesowych wymagań bezpieczeństwa informacji oraz potrzebie ustanowienia zasad i celów jej bezpieczeństwa
- wdrażaniu i eksploataowaniu zabezpieczeń, w kontekście kompleksowego zarządzania ryzykiem w instytucji
- monitorowaniu i dokonywaniu przeglądu wydajności oraz skuteczności SZBI
- ciągłym doskonaleniu w oparciu o obiektywny pomiar

### Zalety usystematyzowanego zarządzania bezpieczeństwem informacji

- Określenie podstawowych zasad związanych z bezpiecznym przetwarzaniem informacji
- Wzrost poziomu bezpieczeństwa informacji w organizacji
- Usprawnienie zarządzania informacjami
- Określenie zasad postępowania w sytuacjach awaryjnych
- Budowanie profesjonalnego wizerunku organizacji godnej zaufania, poparte dodatkowo certyfikatem
- Zwiększenie świadomości pracowników na temat właściwego podejścia do informacji
- Określenie odpowiedzialności i uprawnień pracowników w obszarze bezpieczeństwa informacji
- Wdrożenie mechanizmów regularnej weryfikacji skuteczności stosowanych zabezpieczeń

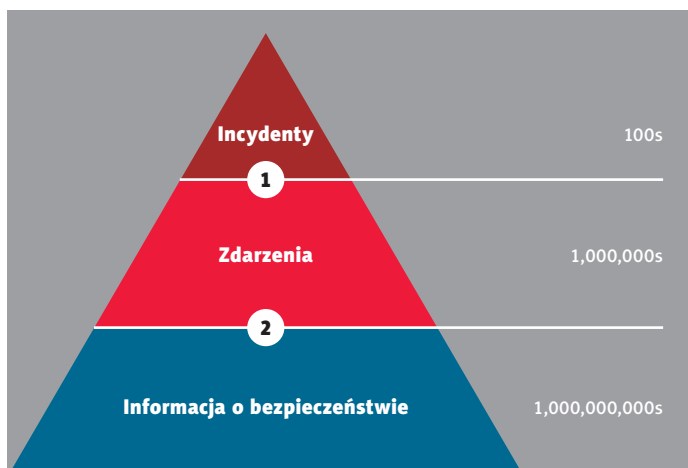
## ■ ZARZĄDZANIE INFORMACJĄ O BEZPIECZEŃSTWIE I ZDARZENIAMI

### Ciągłe monitorowanie poziomu bezpieczeństwa informacji

Mnogość występujących zagrożeń bezpieczeństwa informacji i infrastruktury technicznej przetwarzającej dane, stanowi duże wyzwanie dla współczesnego przedsiębiorstwa. Sprowadzenie zagrożeń do akceptowalnego dla organizacji poziomu ryzyka wymaga zastosowania wielu technicznych i nietechnicznych środków bezpieczeństwa, których działanie i skuteczność musi podlegać ciągłemu monitorowaniu. W związku z powyższym dokonuje się systematycznych przeglądów dzienników zdarzeń urządzeń w poszukiwaniu incydentów wskazujących na wystąpienie nadużycia. Ponadto prowadzi się okresowe badania systemów bezpieczeństwa pod względem skuteczności działania, których wyniki są uwzględniane w procesie monitorowania logów. Powyższe działania mają na celu nie naruszenie integralności, dostępności i poufności informacji, a w konsekwencji ochronę przed zakłóceniami funkcjonowania procesów biznesowych w organizacji.

**System Zarządzania Informacją o Bezpieczeństwie i Zdarzeniami (ang. SIEM – Security Information and Event Management)** jest odpowiedzią na potrzeby związane z zarządzaniem informacją o bezpieczeństwie. Ponadto stanowi skuteczne narzędzie przeznaczone do automatyzacji procesu monitorowania skuteczności działania mechanizmów ochrony bezpieczeństwa informacji. Mechanizm działania SIEM polega na monitorowaniu dzienników zdarzeń aplikacyjnych systemów i urządzeń, przetwarzając je za pomocą wbudowanych narzędzi analitycznych.

1. Wykrywanie zdarzeń: przetwarzanie informacji o bezpieczeństwie z technicznych środków bezpieczeństwa (FW, IDS/IPS, AV, audyt po datności)
2. Analiza: korelacja zdarzeń, ocena ich skuteczności i wpływu na biznes, ocena ryzyka i spełnienie zgodności z regulacjami wymogami formalnymi



Przy podejmowaniu decyzji o wyborze rozwiązań idealnie dopasowanych do potrzeb organizacji oraz rozwiązań oferowanych przez SIEM, kluczowym kryterium jest minimalizacja zagrożeń dla bezpieczeństwa informacji, zidentyfikowanych na etapie analizy zasobów i oceny ryzyka.

### Zadania stawiane przed SIEM

- Gromadzenie danych o działaniu zaimplementowanych mechanizmów ochrony bezpieczeństwa informacji
- Kontrola skuteczności działania mechanizmów ochrony zasobów informacyjnych
- Automatyczne wykrywanie incydentów bezpieczeństwa i wsparcie dla procesu ich rozwiązywania
- Przekrojowa analiza zgromadzonych danych o zdarzeniach, ukierunkowana na osiągnięcie i spełnianie regulacji formalnych i prawnych (np. SOX, Basel I/II, ISO/IEC 17799:2005, ISO/IEC 27000, polityka bezpieczeństwa organizacji).
- Wsparcie dla ciągłego procesu oceny ryzyka i zarządzania ryzykiem w środowisku systemów informatycznych

### Korzyści z wdrożenia narzędzi wspierających monitorowanie poziomu bezpieczeństwa informacji

Wdrożenie skutecznego Systemu Zarządzania Informacją o Bezpieczeństwie i Zdarzeniami w organizacji, spełniającego wymagania przedsiębiorstwa w zakresie bezpieczeństwa informacji, przyczynia się do generowania następujących korzyści:

- Obniżenie wskaźników ryzyka operacyjnego
- Poprawa bezpieczeństwa informacji i weryfikacja stosowania przyjętej polityki bezpieczeństwa
- Wsparcie dla identyfikacji i rozwiązywania incydentów bezpieczeństwa
- Zmniejszenie kosztów monitorowania i poprawa efektywności pracy personelu zarządzającego
- Osiągnięcie i zachowanie ciągłej zgodności z regulacjami i wymogami formalnymi
- Rozszerzenie Systemu Zarządzania Jakością w przedsiębiorstwie o obszar bezpieczeństwa informacji

## ■ OFERTA WOLA INFO W ZAKRESIE ROZWIĄZAŃ SIEM

Wola Info dostarcza swoim Klientom kompleksowe rozwiązania teleinformatyczne, adresujące ich potrzeby w zakresie bezpieczeństwa informacji i systemów teleinformatycznych przetwarzających dane. Konsultanci Wola Info uwzględniając istniejące normy i regulacje prawne, a także dobre praktyki i doświadczenie firmy w tym obszarze, pomagają Klientom efektywnie i skutecznie zarządzać bezpieczeństwem informacji w przedsiębiorstwie.

Metodyka naszego działania składa się z kilku etapów:

- analizy potrzeb Klienta oraz procesów biznesowych funkcjonujących w jego organizacji
- weryfikacji skuteczności działania i optymalizacji stosowanych rozwiązań
- doboru i wdrożenia niezbędnych środków bezpieczeństwa

Naszym celem jest zabezpieczenie ciągłości działania Państwa organizacji oraz wzrost efektywności funkcjonowania przedsiębiorstwa.

Konsultanci Wola Info pomogą Państwu w doborze rozwiązania dla Systemu Zarządzania Informacją o Bezpieczeństwie i Zdarzeniami (ang. SIEM – Security Information and Event Management) najlepiej adresującego Państwa potrzeby związane z ochroną informacji. Kolejnym krokiem będzie wdrożenie w Państwa organizacji efektywnego Systemu Zarządzania Informacją o Bezpieczeństwie i Zdarzeniami.

W realizacji SIEM korzystamy z produktów wiodących dostawców, takich jak:

- Cisco
- netForensics
- Novell
- RSA

W naszej ofercie znajdują się takie rozwiązania jak Cisco MARS, netForensics SIM One, Novell Sentinel i RSA enVision, produkty o zaawansowanej funkcjonalności, wysoko skalowalne, z możliwością dostosowania do wymagań organizacji dowolnej wielkości.

Oferowane przez nas rozwiązania doskonale „współpracują” z różnymi technicznymi środkami bezpieczeństwa. Unikatowość dostarczanych przez narzędzi sprawia, że dzięki swej funkcjonalności idealnie wpierają wymogi uwarunkowań formalnych i prawnych.

Szczegóły na temat naszej oferty oraz pełna prezentacja rozwiązań Wola Info, z uwzględnieniem Państwa indywidualnych potrzeb, zostaną przedstawione podczas warsztatów zorganizowanych na Państwa życzenie.

Jeśli chcieliby Państwo dowiedzieć się więcej na temat oferowanych przez nas rozwiązań lub są Państwo zainteresowani zorganizowaniem warsztatów, prosimy o kontakt z przedstawicielem handlowym Wola Info, dzwoniąc pod numer +48 22 431 84 00.



**Wola Info SA**  
**Ul. Cybernetyki 7, 02-678 Warszawa**  
**Tel: +48 22 431 84 00, [www.wolainfo.com.pl](http://www.wolainfo.com.pl)**