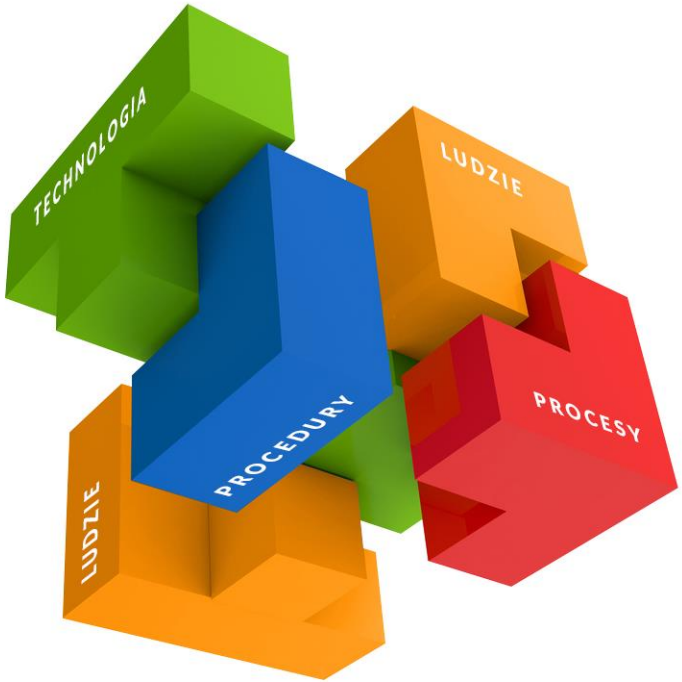


EXATEL

Usługi wspierające proces skutecznej ochrony danych osobowych

Jakub Syta
Dyrektor Departamentu Cyberbezpieczeństwa EXATEL

Myśli przewodnie

Wraz ze wzrostem świadomości potrzeb w zakresie cyberbezpieczeństwa organizacje (słusznie) szukają pomocy na zewnątrz.

Popyt na tego typu usługi bezpośrednio przełożył się na ich podaż. Wydaje się, że liczba doradców rośnie wykładniczo. Coraz poważniejszym zagadnieniem jest więc wybór najlepszych z usług.

Niestety, z punktu widzenia zamawiających, raporty z obserwacjami i rekomendacjami coraz częściej kończą się pytaniem „Co dalej?”

Krok #1

PREWENCJA

Cel: Bezpieczna organizacja procesów biznesowych

Co trzeba zrobić:

- przegląd bezpieczeństwa (audyt/analiza luk),
- przygotowanie analizy ryzyka,
- przygotowanie szablonów dokumentów.

Zanim zamówisz usługę:

- sprawdź czy organizacja **sama stosuje zasady**, które wdraża u innych (sprawdź wdrożone normy, przejrzyj politykę bezpieczeństwa i certyfikaty pracowników),
- poproś o profile osób, które będą **wykonywać** prace,
- przeczytaj i przeanalizuj jakość artykułów publikowanych przez doradców.

Wskaźnik sukcesu: uporządkowane procesy biznesowe

Cel: Stworzenie architektury IT odpornej na próby ataku

Co trzeba zrobić:

- utwardzanie architektury teleinformatycznej,
- wdrożenie metod bezpiecznej wymiany danych,
- skanowanie podatności w systemach teleinformatycznych,
- testy penetracyjne.

Zanim zamówisz usługę:

- poproś o referencje z wcześniejszych wdrożeń i prac integratorskich/testów penetracyjnych,
- dowiedz się jakimi narzędziami będą wspierane prace,
- poproś o profile osób, które będą **wykonywać** prace.

Wskaźnik sukcesu: zinwentaryzowana infrastruktura IT

Cel: Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji

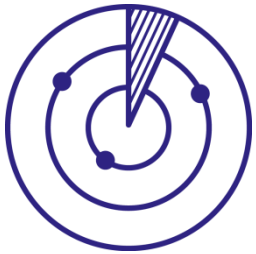
Co trzeba zrobić:

- wdrażanie systemu zarządzania bezpieczeństwem informacji („wdrażanie polityki bezpieczeństwa”).

Zanim zamówisz usługę:

- sprawdź czy organizacja **sama stosuje zasady**, które wdraża u innych (sprawdź wdrożone normy, przejrzyj politykę bezpieczeństwa i certyfikaty pracowników).

Wskaźnik sukcesu: plan prac doskonalących SZBI



Krok #2

DETEKCJA

Cel: Identyfikacja prób ataku na brzeg sieci

Co trzeba zrobić:

- wdrożyć i utrzymywać rozwiązania chroniące brzeg sieci takie jak firewall, IDS/IPS, WAF, DAM, antymalware, AntyDDoS (w zależności od zidentyfikowanego ryzyka),
- monitorować zdarzenia realizowane przez Security Operations Center (SOC).

Zanim zamówisz usługę:

- sprawdź kompetencje w ramach wdrażanych technologii,
- potwierdź możliwość podłączania źródeł do systemów SIEM,
- potwierdź godziny pracy SOC,
- sprawdź wykonawców pod kątem normy, certyfikatów, poświadczeń bezpieczeństwa itp.

Wskaźnik sukcesu: wiesz, kto Cię atakuje

Cel: Identyfikacja przypadków wycieku informacji

Co trzeba zrobić:

- wdrożyć i utrzymywać rozwiązania DLP (Data Leak Protection),
- monitorować zdarzenia realizowany przez SOC.

Zanim zamówisz usługę:

- sprawdź kompetencje w ramach wdrażanych technologii,
- potwierdź możliwość podłączania źródeł do systemów SIEM,
- potwierdź godziny pracy SOC,
- sprawdź wykonawców pod kątem normy, certyfikatów, poświadczeń bezpieczeństwa itp.

Wskaźnik sukcesu: wiesz, co chcesz chronić

Krok #3

REAKCJA

Cel: Analiza incydentów

Co trzeba zrobić:

- analiza malware,
- zabezpieczanie dowodów,
- identyfikacja przebiegu incydentu.

Zanim zamówisz usługę:

- sprawdź wykonawców pod kątem wdrożonych u niego normy, certyfikatów oraz poświadczeń bezpieczeństwa,
- dowiedz się, w jakim czasie rozpocznie pracę (nie tylko „przyjmie zgłoszenie”).

Wskaźnik sukcesu: wiesz, co się stało

Cel: Aktywne przeciwdziałanie próbom ataku

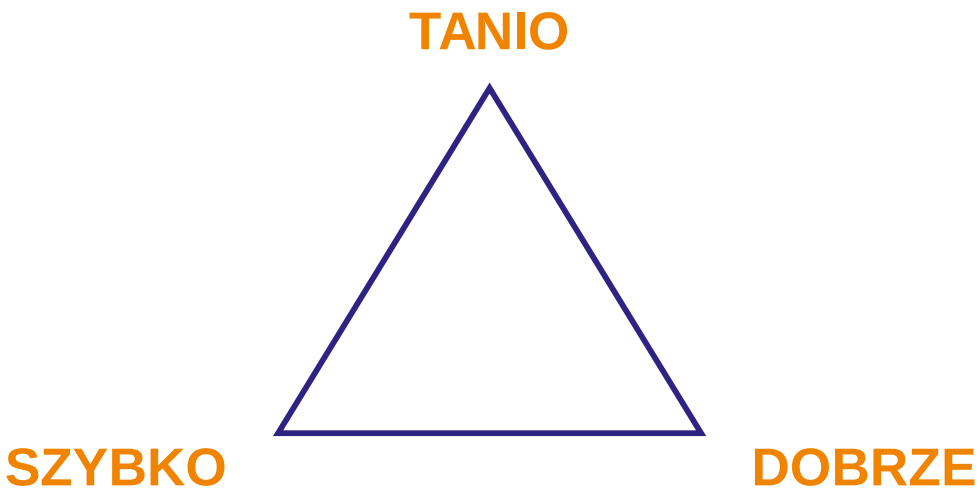
Co trzeba zrobić:

- powstrzymywać zagrożenia / incydenty.

O czym należy pamiętać:

- sprawdź wykonawców pod kątem wdrożonych u niego normy, certyfikatów oraz poświadczeń bezpieczeństwa,
- poproś o profile osób z zespołu DFIR (Digital Forensics and Incident Response),
- dowiedz się, w jakim czasie rozpocznie pracę (nie tylko „przyjmie zgłoszenie”),
- upewnij się, że pracuje w trybie 24/7.

Wskaźnik sukcesu: wiesz, do kogo zadzwonić w razie problemu



Czego oczekujesz od usługodawcy?

Przeprowadź analizę ryzyka swojego biznesu i wybierz dwie opcje.

Cyberbezpieczeństwo w EXATEL

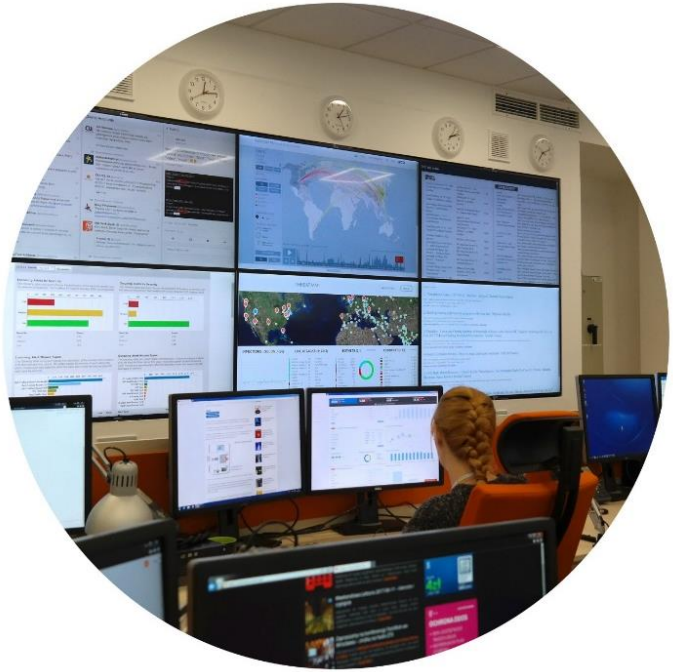
SOC, NOC i BOK **działające w trybie ciągłym, 24x7**

SOC to wyłącznie osoby z **doświadczeniem zawodowym w informatyce, zatrudnione na etat, regularnie szkolone i posiadające certyfikaty** w zakresie bezpieczeństwa informacji

Kadra kierownicza to **osoby z kilkunastoletnim doświadczeniem, uznani i aktywni eksperci** w środowisku cyberbezpieczeństwa

Usługi realizowane są w oparciu o **najlepsze światowe technologie**

EXATEL **posiada wydzielony dział R&D,** w którym opracowywane są **własne narzędzia** z zakresu cyberbezpieczeństwa



Dziękuję za uwagę

www.exatel.pl