Odporność zaczyna się od fundamentów. Jak budować bezpieczeństwo infrastruktury krytycznej?

Energia, komunikacja, dane - dopóki działają bez zakłóceń, ich znaczenie bywa niedostrzegane. Problem pojawia się dopiero w momencie awarii, wtedy ujawnia się ich kluczowa rola. Właśnie dlatego kwestia odporności infrastruktury krytycznej staje się dziś jednym z najważniejszych wyzwań strategicznych państwa. Odporność infrastruktury krytycznej staje się dziś jednym z najważniejszych wyzwań, to ona stanowi fundament działania nowoczesnego państwa i gospodarki.

Jak budować odporność państwa, gospodarki i organizacji w warunkach rosnących zagrożeń cybernetycznych, postępującej cyfryzacji oraz rozwoju sztucznej inteligencji?

Infrastruktura krytyczna tworzy system wzajemnie powiązanych sektorów, w którym zakłócenie jednego obszaru może szybko wpłynąć na działanie pozostałych. Dlatego kluczowe jest podejście systemowe oparte na współpracy i koordynacji, ponieważ odporność państwa wynika ze spójnych, wspólnych działań.

Cyberbezpieczeństwo, jako warunek ciągłości działania

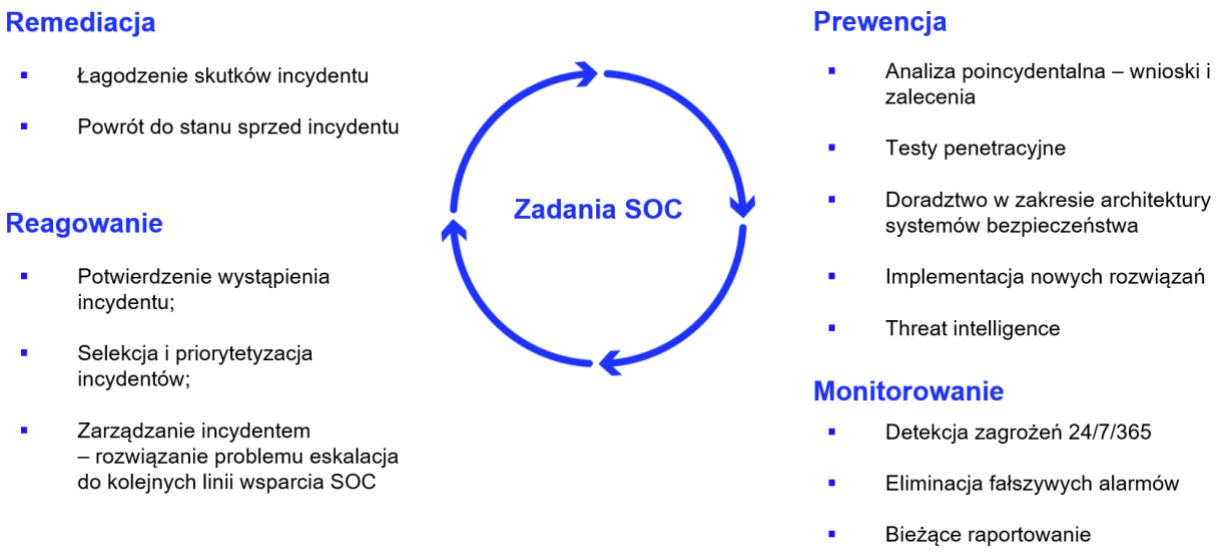
Naturalną konsekwencją takiego podejścia jest rosnąca rola cyberbezpieczeństwa, które dziś stanowi fundament ciągłości działania całych sektorów gospodarki. Jeszcze niedawno było ono traktowane głównie jako obszar IT, obecnie jednak bezpośrednio wpływa na stabilność funkcjonowania państwa i organizacji od dostaw energii, przez komunikację, aż po dostęp do kluczowych usług.

Z perspektywy EXATEL cyberbezpieczeństwo nie jest już dodatkiem, a podstawą i fundamentem budowania odporności. W tym kontekście szczególnego znaczenia nabierają regulacje, takie jak Krajowy System Cyberbezpieczeństwa (KSC), które definiują wymagania wobec podmiotów kluczowych i ważnych i wyznaczają kierunek dla bezpiecznego, odpornego państwa i gospodarki.

Cyberbezpieczeństwo to proces ciągły

Nowoczesne podejście do bezpieczeństwa zakłada, że nie jest ono jednorazowym projektem, lecz procesem, który musi być stale rozwijany i dostosowywany do zmieniających się zagrożeń. W praktyce oznacza to cykl działań (w EXATEL realizowanych przez Security Operations Center (SOC)), obejmujący:

- **całodobowe monitorowanie środowiska IT i OT,**
- **wykrywanie i analizę incydentów,**
- **szybkie reagowanie,**
- **remediację i przywracanie ciągłości działania,**
- **działania prewencyjne, takie jak testy penetracyjne i analiza podatności.**



Takie podejście, oparte na ciągłości, automatyzacji i wiedzy operacyjnej - pozwala budować i zapewnia odporność w organizacji i bezpieczeństwo.

Cyberbezpieczeństwo – kompleksowa oferta EXATEL, a etapy budowania odporności

Skuteczne cyberbezpieczeństwo nie zaczyna się od technologii, lecz od świadomości. Dlatego podejście EXATEL opiera się na etapowym budowaniu odporności organizacji od edukacji pracowników

(poprzez kampanie phishingowe EXATEL) przez analizę infrastruktury (testy penetracyjne i audyty), aż po wdrażanie zaawansowanych usług bezpieczeństwa.

Kluczową rolę odgrywają tu rozwiązania takie jak ochrona anty-DDoS, firewalle nowej generacji czy systemy SIEM i EDR/XDR, które pozwalają identyfikować i ograniczać zagrożenia w czasie rzeczywistym. Całość uzupełnia stały monitoring i reakcja realizowane przez centra SOC działające 24/7.

Bezpieczeństwo to ludzie, procesy, technologie: w EXATEL wierzymy, że skuteczne cyberbezpieczeństwo wymaga jednoczesnego działania w tych trzech obszarach: od uporządkowanych procedur i polityk bezpieczeństwa, przez rozwój kompetencji i świadomości pracowników, aż po wdrożenie i integrację zaawansowanych rozwiązań technologicznych działających 24/7, które wspólnie budują realną odporność organizacji.

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa

W kontekście ustawy o krajowym systemie cyberbezpieczeństwa organizacje powinny planować wydatki na cyberbezpieczeństwo w sposób całościowy, obejmujący trzy wzajemnie uzupełniające się obszary: **organizację i procesy, kompetencje oraz technologię.**

Oznacza to inwestycje zarówno w uporządkowanie procedur i wdrożenie mechanizmów zarządzania bezpieczeństwem, jak i w rozwój świadomości pracowników, którzy stanowią pierwszą linię obrony. Równolegle konieczna jest modernizacja i rozbudowa narzędzi technologicznych wspierających wykrywanie i reagowanie na zagrożenia. Takie zintegrowane podejście pozwala nie tylko spełnić wymagania regulacyjne, ale przede wszystkim budować realną i długoterminową odporność organizacji.

Usługi EXATEL wspierające obszar organizacji i procesów koncentrują się na budowaniu uporządkowanego i świadomego podejścia do bezpieczeństwa, zgodnego z wymaganiami KSC oraz międzynarodowych norm. Obejmują one m.in. **rekonesans bezpieczeństwa**, który pozwala zidentyfikować kluczowe luki i ryzyka, a także **audyty bezpieczeństwa** **i** **testy penetracyjne**, umożliwiające ocenę realnego poziomu ochrony organizacji.

Na tej podstawie EXATEL dostarcza **konkretne rekomendacje dotyczące polityk i procedur bezpieczeństwa**, wspiera ich wdrażanie oraz pomaga w budowaniu struktur odpowiedzialnych za zarządzanie incydentami i ciągłością działania. Takie podejście pozwala nie tylko osiągnąć zgodność z regulacjami (m.in. KSC, NIS2, ISO 27001), ale przede wszystkim wdrożyć efektywne, procesowe zarządzanie bezpieczeństwem, które zwiększa odporność organizacji i buduje zaufanie klientów oraz partnerów.

Usługi EXATEL wspierające obszar kompetencji koncentrują się na budowaniu świadomości i wzmacnianiu czynnika ludzkiego jako jednego z kluczowych elementów cyberbezpieczeństwa. Obejmują one kompleksowe działania edukacyjne od szkoleń online i warsztatów prowadzonych przez ekspertów, po programy dopasowane do specyfiki danej organizacji. Istotnym elementem są również **kampanie phishingowe**, które w bezpiecznych warunkach symulują realne ataki i pozwalają

identyfikować obszary wymagające poprawy. Dzięki temu pracownicy uczą się właściwych reakcji na zagrożenia, zmieniają codzienne nawyki i zwiększają swoją świadomość na temat cyberzagrożeń. Takie podejście nie tylko podnosi poziom wiedzy w organizacji, ale realnie przekłada się na ograniczenie ryzyka incydentów i budowę świadomości i bezpieczeństwa.

W obszarze technologii inwestycje w cyberbezpieczeństwo koncentrują się na **zakupie, modernizacji oraz integracji rozwiązań technicznych**, które umożliwiają skuteczną ochronę infrastruktury i danych. Obejmują one zarówno wdrożenie zaawansowanych usług bezpieczeństwa: takich jak anty-DDoS, SOC, MDR czy rozwiązania chmurowe, a także rozwój środowiska sprzętowego (np. zapory sieciowe, systemy VPN, macierze danych czy urządzenia sieciowe). Kluczową rolę odgrywa również oprogramowanie klasy SIEM, EDR/XDR, IDS/IPS czy systemy zarządzania tożsamością i dostępem. Istotne jest jednak nie tylko samo wdrożenie technologii, ale także jej utrzymanie, aktualizacja oraz integracja w spójny system bezpieczeństwa, który działa w sposób ciągły i wspiera organizację w wykrywaniu oraz neutralizowaniu zagrożeń w czasie rzeczywistym.

UoKSC - Mapowanie obszarów bezpieczeństwa na usługi EXATEL

Wymaganie	Obszar Cyberbezpieczeństwa	Produkt/usługa EXATEL
Polityki, procesy, procedury i plany: szacowania ryzyka, ciągłości działania, odtworzenia systemów informacyjnych po zdarzeniach, oceny skuteczności środków technicznych i organizacyjnych, stosowania kryptografii, zarządzania aktywami, kontroli dostępu, zarządzania incydentami, zarządzania konfiguracją, zmianami w systemie, testowanie systemu	**Polityki i procedury**	Wdrożenie / audyt SZBI/KRI/ISO 27001
Zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi	**Testy penetracyjne**	Testy penetracyjne
Zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi	**Analiza bezpieczeństwa infrastruktury**	Usługa rekonesansu bezpieczeństwa (RED/BLUE team)
	Raportowanie i zgłaszanie incydentów	Usługa SOC/system SIEM
Bezpieczeństwo zasobów ludzkich (poprzez dbałość o zrozumienie wymogów bezpieczeństwa wśród personelu. Edukacja z zakresu cyberbezpieczeństwa dla personelu podmiotu	**Szkolenia i budowanie świadomości cyberzagrożeń**	Usługi szkoleniowe oraz kampanie phishingowe
Stosowanie bezpiecznych środków komunikacji elektronicznej	**Zabezpieczenie poczty e-mail**	Usługa Secure Mail Gateway
Wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych	**Zabezpieczenie styku z Internetem**	Usługa anty-DDoS TAMA (L3 i L7) + Zarządzany firewall (IDS/IPS/WebProxy)
Ochrona przed nieuprawnioną modyfikacją w systemie informacyjnym	**Ochrona stacji roboczych i serwerów**	Wdrożenie EDR/XDR lub usługa MDR
Objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym	**Monitorowanie i reagowanie na incydenty**	Wdrożenie SIEM i usługa SOC
Zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi	**Zarządzanie podatnościami**	Wdrożenie oprogramowania do zarządzania podatnościami lub usługa zarządzania podatnościami
Wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych (ad. ciągłość działania)	**Backup i ciągłość działania (BCP/DR)**	Wdrożenie backup + Zasilanie awaryjne (UPS/agregat)
Wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych	**Kontrola dostępu i tożsamości**	Wdrożenie usług katalogowych (IAM) + MFA
Wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych	**Kontrola użytkowników uprzywilejowanych**	Wdrożenie oprogramowania PAM lub usługa zarządzana

Program DIG.IT stanowi ważny element podejścia EXATEL do cyberbezpieczeństwa

Zachęcamy do zapoznania się z założeniami DIG IT, programu Agencji Rozwoju Przemysłu, w ramach którego firmy MŚP mogą skorzystać z grantu na transformacje cyfrową.

EXATEL koncentruje się na praktycznym wsparciu organizacji w podnoszeniu odporności cyfrowej. W ramach inicjatywy DIG.IT firmy mogą nie tylko skorzystać z dofinansowania nowoczesnych rozwiązań technologicznych, ale także rozwijać kompetencje zespołów i porządkować procesy bezpieczeństwa zgodnie z aktualnymi wymaganiami.

DIG.IT pomaga przełożyć regulacje i dobre praktyki na konkretne działania, wspierając organizacje w budowie spójnego podejścia do cyberbezpieczeństwa od świadomości i analizy, aż po monitorowanie i reagowanie.

Podsumowując, budowanie odporności infrastruktury krytycznej wymaga dziś podejścia systemowego, w którym cyberbezpieczeństwo stanowi fundament ciągłości działania państwa i gospodarki.

W EXATEL wierzymy, że skuteczna ochrona nie opiera się na pojedynczych rozwiązaniach, lecz na spójnym modelu łączącym **ludzi, procesy i technologię** od budowania świadomości i kompetencji, przez uporządkowanie procedur i zgodność z regulacjami KSC, aż po wdrażanie kompleksowych rozwiązań technologicznych. Kluczowe znaczenie ma również postrzeganie **cyberbezpieczeństwa jako ciągłego procesu, realizowanego w modelu 24/7,** który obejmuje monitorowanie, reagowanie i prewencję. W tym kontekście inicjatywy takie jak DIG.IT oraz kompleksowe usługi EXATEL umożliwiają organizacjom przełożenie wymagań regulacyjnych na konkretne działania, realnie zwiększające odporność w dynamicznie rozwijającej się gospodarce, ta także zmieniającym się środowisku zagrożeń.