

# Spostrzeżenia na temat cyberodporności

Analiza luk w cyberodporności, ewoluujących zagrożeń, obrony opartej na AI i strategii odzyskiwania w regionie EMEA

Wyzwania związane z cyberodpornością nasilają się, ponieważ cyberataki i luki w ochronie danych zwiększają ryzyko zakłóceń. Organizacje o dojrzałych strategiach odporności\* mają prawie trzykrotnie większe szanse na pomyślne odzyskanie sprawności. Dzięki modernizacji strategii odporności, poprawie zdolności wykrywania i priorytetowi ciągłej optymalizacji liderzy IT mogą zminimalizować ryzyko i nabrać zaufania do swoich zdolności dostosowywania się do zmieniających się zagrożeń.

## Nadmierna pewność siebie kadry zarządzającej

59% specjalistów IT uważa, że ich kierownictwo przecenia gotowość firmy na cyberataki. Gdy górę bierze nadmierna pewność siebie, powstają niebezpieczne martwe punkty, które opóźniają kluczowe inwestycje i pozostawiają luki w zabezpieczeniach.



## Rozdźwięk między zaufaniem a zdolnościami

**99,8%** organizacji ma wdrożone strategie cyberodporności

Ale **59%** nie zdołało skutecznie przywrócić sprawności po ostatnim teście lub incydencie

## Zapobieganie a odzyskiwanie: nierównowaga w podejściu

**74%**

uważa, że ich organizacja koncentruje się bardziej na zapobieganiu atakom, niż na przygotowaniu się do odzyskania sprawności po ataku

Ale tylko

**26%**

ma kompleksową platformę do wykrywania zagrożeń obejmującą podstawową pamięć masową, pamięć masową do tworzenia kopii zapasowych i infrastrukturę sieciową

A tylko

**36%**

skutecznie powstrzymało atak lub odzyskało sprawność po incydencie cybernetycznym / ćwiczeniach przy minimalnym wpływie na działalność firmy

W konsekwencji, gdy nieuchronnie dochodzi do naruszeń, wiele organizacji jest nieprzygotowanych na fazę odzyskiwania, która decyduje o przetrwaniu firmy.

## Droga naprzód:

Dojrzałe organizacje osiągają wymierne wyniki

Organizacje o dojrzałych strategiach cyberodporności mają prawie 2,7 razy większe szanse na pomyślne odzyskanie danych

Strategiczna dojrzałość w obszarze trzech kluczowych filarów współdziała, tworząc niezachwianą odporność.



### BEZPIECZEŃSTWO:

#### Budowanie fundamentu zaufania

Organizacje o dojrzałych strategiach cyberodporności cechuje:

**1,3 razy** częściej chronią urządzenia za pomocą mechanizmów kontroli bezpieczeństwa na poziomie oprogramowania wewnętrznego / systemu BIOS

**Większe prawdopodobieństwo** wykorzystania magazynów cybernetycznych do ochrony krytycznych danych przed ewoluującymi zagrożeniami

Ale bezpieczeństwo to dopiero początek. Prawdziwą zaletą jest inteligentne wykrywanie, które wykrywa zagrożenia, zanim naruszą najcenniejsze zasoby.



### WYKRYWANIE:

#### Inteligencja, która nigdy nie śpi

#### Wyzwanie związane z widocznością:

Tylko 26% organizacji dysponuje solidnymi mechanizmami wykrywania zagrożeń w pamięci kopii zapasowych, podstawowej pamięci masowej i infrastrukturze sieciowej

#### Rozwiązanie oparte na sztucznej inteligencji:

**61%** traktuje priorytetowo inwestycje w wykrywanie zagrożeń za pomocą sztucznej inteligencji i uczenia maszynowego

**40%** kompleksowo skanuje dane kopii zapasowych przy użyciu sztucznej inteligencji i uczenia maszynowego w poszukiwaniu wskaźników naruszenia bezpieczeństwa

Organizacje o dojrzałych strategiach są **3,6 razy bardziej skłonne** do wykorzystywania narzędzi sztucznej inteligencji i uczenia maszynowego z proaktywnymi procedurami ograniczania ryzyka i reagowania



### ODZYSKIWANIE:

#### Odpowiednie przygotowanie zapewni wydajność

#### Zalety testowania:

**51%** organizacji przeprowadzających comiesięczne lub częstsze symulacje cyberataków pomyślnie odzyskało sprawność po incydentach

**64%** organizacji, które przeprowadza symulowane ataki cybernetyczne rzadziej niż raz na miesiąc, nie było w stanie przywrócić danych po incydentach

#### Wynik:

Organizacje, które testują często, mają znacznie większe szanse na spełnienie zarówno celów dotyczących czasu odzyskiwania (Recovery Time Objective), jak i punktu odzyskiwania (Recovery Point Objective) niż te, które testują sporadycznie.

## Twoja droga do doskonałości w zakresie cyberodporności

Organizacje o dojrzałych strategiach cyberodporności mają 1,9 razy większe szanse na stałe spełnianie warunków umów SLA

#### Budowa solidnego fundamentu

Priorytetem powinno być zarówno zapobieganie, jak i szybkie odzyskiwanie sprawności.

**Bezpieczeństwo:** zmniejsz ryzyko dzięki zabezpieczeniu na poziomie systemu BIOS, szyfrowaniu danych i magazynom cybernetycznym dla danych krytycznych.

**Wykrywanie:** wykorzystaj sztuczną inteligencję i uczenie maszynowe w czasie rzeczywistym do wykrywania zagrożeń i reagowania na nie w całej pamięci masowej, w tym w pamięci podstawowej i chronionej.

**Odzyskiwanie:** regularnie testuj proces odzyskiwania – organizacje, które robią to co miesiąc, znacznie częściej osiągają cele odzyskiwania.

## Chcesz wzmocnić cyberodporność?

Chcesz wzmocnić cyberodporność? Zapoznaj się z kluczowymi wnioskami z raportu [Dell 2026 Cyber Resilience Insights Research](#).

**DELL**Technologies

Zródło: Badanie Vanson Bourne | Dell Technologies dotyczące cyberodporności (Cyber Resilience) 2025. Copyright © Dell Inc. lub jednostki zależne Dell Inc. Wszelkie prawa zastrzeżone. Dell i inne znaki towarowe są znakami towarowymi firmy Dell Inc. lub jej podmiotów zależnych. Inne znaki towarowe mogą stanowić własność odpowiednich właścicieli.

\* Organizacje o dojrzałych strategiach cyberodporności definiuje się jako te, które mają w pełni ugruntowaną i ciągle optymalizowaną strategię, wykorzystującą analizę predykcijną, automatyzację i wgląd w dane w czasie rzeczywistym (np. kanały informacji o zagrożeniach, korekty oparte na uczeniu maszynowym, wskaźniki KPI kierujące usprawnieniami)