KOMPAS IT

DELL Technologies

Cyfrowy Bunkier – nowy standard cyfrowej odporności organizacji

W erze cyfrowej transformacji, ochrona danych stała się fundamentem stabilności biznesowej i technologicznej każdej organizacji. Kluczowe mogą okazać się rozwiązania do backupu i archiwizacji danych, gwarantujące możliwość ich odzyskania w przypadku jakiegokolwiek ataku hakerskiego lub ransomware.

Dzisiejsze realia wskazują, że pytanie nie brzmi już „czy", ale „kiedy" organizacja padnie ofiarą cyberataku. W obliczu dynamicznie zmieniającego się krajobrazu cyberzagrożeń, niedoboru specjalistów i rosnącej liczby prób wyłudzeń informacji, wdrożenie zaawansowanych, zautomatyzowanych i skutecznych zabezpieczeń stało się priorytetem dla działów IT.

Cyfrowy Bunkier to znaczący krok naprzód w poprawie bezpieczeństwa firmy i budowaniu odporności na ataki cyfrowe. Stanowi uzupełnienie strategii Disaster Recovery, eliminując wady tradycyjnych podejść do zapewnienia wysokiej dostępności w obliczu cyberataków. Dojrzałość i odpowiedzialność strategii IT polega na przygotowaniu organizacji na potencjalne włamania, które mogą przedostać się przez istniejące sieci zabezpieczeń i zapewnienie organizacji ciągłości działania.

Cyfrowy Bunkier to:

- **Izolowana, bezpieczna enklawa bezpieczeństwa**, która monitoruje zasoby i poszukuje objawów nadchodzących lub już istniejących ataków cyfrowych, uzupełniona o **indywidualny zestaw przygotowanych procedur i planów odtworzeniowych.**
- **Odporność na różnorodne ataki** – system zakłada możliwość wystąpienia skutecznego ataku i przygotowuje organizację na szybkie odtworzenie zarówno w przypadku zagrożeń zewnętrznych, jak i wewnętrznych.
- **Elastyczność i automatyzacja** – system działa automatycznie, umożliwiając w pełni zautomatyzowaną codzienną ochronę krytycznych systemów oraz ciągłe monitorowanie pod kątem potencjalnych lub już istniejących ataków cyfrowych.
- **Zgodność z regulacjami** – zapewnia wsparcie w wypełnianiu międzynarodowych i krajowych przepisów dotyczących bezpieczeństwa i ochrony danych, co jest kluczowe dla utrzymania zaufania klientów i unikania kar regulacyjnych.
- **Wsparcie ekspertów Dell Technologies** – rozwiązanie gwarantuje dostęp do globalnej sieci ekspertów Dell, którzy zapewniają wsparcie techniczne, implementację systemu oraz doradztwo strategiczne i technologiczne w zakresie bezpieczeństwa cyfrowego.

ROLA I ZNACZENIE

W dzisiejszych realiach cyfrowych, bezpieczeństwo danych jest kluczowym priorytetem każdej organizacji. Brak gwarancji niezawodności rozwiązań w zakresie bezpieczeństwa cyfrowego, trudności w pozyskaniu i szybkiej edukacji specjalistów oraz ludzkiej podatności na wyłudzenia informacji sprawiają, że głównym zadaniem działów IT jest stworzenie niezawodnej tarczy ochronnej (muru) wokół systemów IT. Jednak im bardziej skomplikowana infrastruktura IT, tym więcej możliwych płaszczyzn ataku. Wystarczy jeden błąd popełniony przez pracownika lub jedna niezałatana luka, w którymś z dziesiątek programów, działających na jednym z wielu komputerów w organizacji, aby umożliwić cyberatak. Można – i należy – podejmować działania mające na celu minimalizację ryzyka ataku, ale bez wdrożenia zaawansowanych rozwiązań, jak Cyfrowy Bunkier, poziom zabezpieczeń można uznać za niekompletny.

Kluczowe elementy ochrony to:

- Obrona systemów IT i informacji
- Monitorowanie użytkowników i kontrola dostępu
- Raportowanie i predykcja zagrożeń

Firmy traktują backup, jako narzędzie zapewniające integralność danych, nawet w przypadku najbardziej zaawansowanych ataków, które przełamią istniejące zabezpieczenia.

Tradycyjny backup, koncentrujący się na szybkim tworzeniu kopii zapasowych i ich skutecznym odtwarzaniu w razie awarii, jest niewystarczający. Współczesny, efektywny system backupu musi być dostępny dla wielu aplikacji i administratorów jednocześnie, zapewniając optymalne parametry i szybki czas reakcji.

Aby zapewnić odtworzenie danych niezależnie od rodzaju cyfrowego ataku, strategie backupu należy uzupełnić o zaawansowane rozwiązania Cyber Recovery, takie jak **Cyfrowy Bunkier, który gwarantuje:**

- Przywrócenie danych po dowolnym ataku hakerskim lub ransomware z najnowszej „zdrowej” kopii
- Wykrywanie „na bieżąco” cyfrowych ataków
- Automatyzacja procesu odtworzenia danych po ataku cyfrowym

MOŻLIWOŚCI I ZASTOSOWANIE

Cyfrowy Bunkier Dell Technologies ma zastosowanie w każdym sektorze gospodarki, który wymaga szczególnej ochrony danych ze względu na ich wrażliwość lub strategiczne znaczenie.

Instytucje Finansowe:

- Wzmocniona ochrona danych finansowych klientów oraz operacji bankowych przed intensywnymi atakami cyberprzestępców.
- Wsparcie w wypełnieniu wymogów regulacyjnych dotyczących ochrony danych, takich jak DORA, Rekomendacja D, GDPR, oraz SOX.

Sektory Rządowe i Obronne:

- Ochrona informacji klasyfikowanych, kluczowych dla bezpieczeństwa narodowego.
- Wzmocnienie odporności na cyberataki oraz próby fizycznego włamania.
- Wsparcie w spełnieniu regulacji NIS2.

Opieka Zdrowotna:

- Zapewnienie zgodności z regulacjami HIPAA i NIS2.
- Ochrona danych medycznych pacjentów, wymagających wysokiego poziomu poufności i zabezpieczenia przed ransomware.

Edukacja i Badania:

- Ochrona badań i danych naukowych, zwłaszcza w projektach o strategicznym znaczeniu dla innowacyjności i bezpieczeństwa.

Przemysł i Produkcja:

- Zabezpieczenie przed szpiegostwem przemysłowym.
- Ochrona procesów produkcyjnych kontrolowanych cyfrowo, zapewniająca ciągłość i bezpieczeństwo operacji.

ARCHITEKTURA

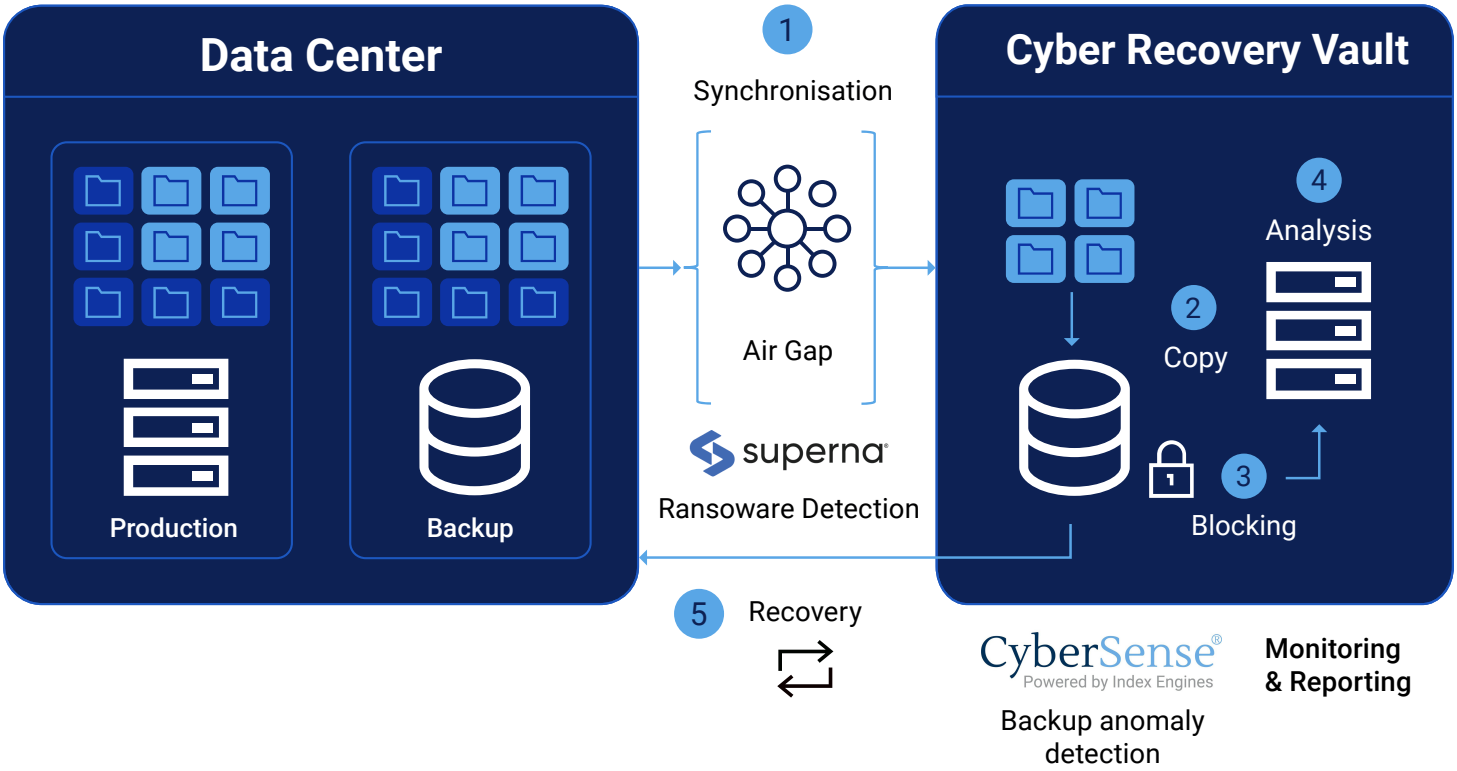
Architektura Dell Cyber Recovery została zaprojektowana w celu zapewnienia kompleksowej, wielopoziomowej ochrony przed zagrożeniami wewnętrznymi i zewnętrznymi:

- **Fizyczna warstwa ochrony** obejmuje zabezpieczenia biometryczne, systemy rozpoznawania twarzy oraz zaawansowane technologie monitorowania fizycznego i elektronicznego, które są niezbędne do ochrony przed fizycznym dostępem do urządzeń.
- **Sieciowe zabezpieczenia** zapewniają możliwość włączenia segmentacji sieci i zastosowanie tzw. „air gap" – izolacji krytycznych zasobów poprzez sztuczną przerwę w sieci, która skutecznie zapobiega rozprzestrzenianiu się ataków w korporacyjnej infrastrukturze sieciowej.
- **Funcjonalność WORM (Write Once Read Many)** gwarantuje, że dane zapisane w Bunkrze nie mogą być modyfikowane ani usuwane, co jest potwierdzone certyfikatem bezpieczeństwa.
- **Weryfikacja danych (Analityka).** System zawiera zaawansowany komponent analityczny, który na bieżąco monitoruje przesyłane dane na podstawie wielu wskaźników, przy użyciu sieci neuronowych. Dzięki temu możliwe jest wykrywanie wszelkich odchyleń od normy, nieprawidłowości oraz natychmiastowe alertowanie w przypadku ataku. Analityka umożliwia również szybkie zidentyfikowanie ostatnich zdrowych kopii danych, co znacznie skraca czas odtworzenia.

- **Procedury Odtworzeniowe.** Zespół Dell Technologies współpracuje z klientem w zakresie opracowania i testowania optymalnych procedur odtworzeniowych Z Bunkra dla krytycznych systemów, aby zapewnić ich szybkie i efektywne przywrócenie po cyfrowym ataku.
- **Ochrona Danych** poprzez szyfrowanie danych przy użyciu najnowszych standardów kryptograficznych oraz wdrożenie ścisłych polityk kontroli dostępu i autentyfikacji, co gwarantuje najwyższy poziom bezpieczeństwa.
- **Redundancja i Odporność.** Systemy są zaprojektowane do pracy w trybie ciągłym, wyposażone w automatyczne mechanizmy failover oraz funkcje szybkiego przywracania działania po awarii, co zapewnia ciągłość operacyjną i minimalizuje przestoje.

CYFROWY BUNKIER

Bezpieczeństwo krytycznych danych i izolacja od sieci produkcyjnej



KLUCZOWE FUNKCJE I KORZYŚCI

Cyfrowy Bunkier to:

Gwarancja przywrócenia danych po ataku:
system zapewnia szybkie i skuteczne odzyskanie danych po każdym ataku hakerskim lub ransomware.

Ciągłe monitorowanie i wykrywanie zagrożeń:
Nieustanna analiza i monitorowanie systemów w celu wykrywania i natychmiastowego reagowania na wszelkie cyfrowe zagrożenia.

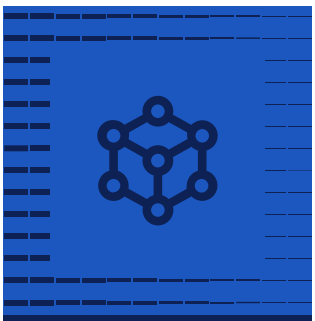
Automatyzacja Procesu Odtworzenia:
Automatyczne procedury odtworzenia danych minimalizują przestoje i przywracają normalne funkcjonowanie firmy w krótkim czasie.

Wielopoziomowa Architektura Ochrony:
Zaawansowane fizyczne i sieciowe zabezpieczenia, segmentacja sieci, funkcjonalność WORM (dane niemodyfikowalne), szyfrowanie danych, oraz redundantne mechanizmy zabezpieczające zapewniają kompleksową ochronę.

Zgodność z Regulacjami:
Pomaga spełniać międzynarodowe i krajowe przepisy dotyczące bezpieczeństwa i ochrony danych (np. GDPR, HIPAA, NIS2), co zwiększa zaufanie klientów i unika kar regulacyjnych.

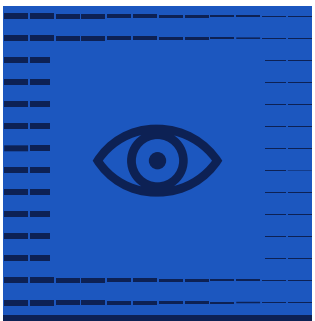
Wsparcie Globalnej Sieci Ekspertów Dell Technologies:
Dostęp do profesjonalnej pomocy technicznej, strategicznego doradztwa i wsparcia w implementacji oraz utrzymaniu systemów bezpieczeństwa.

Elastyczność i Skalowalność:
Rozwiązanie dostosowuje się do specyficznych potrzeb różnych sektorów, takich jak finanse, rząd, zdrowie, edukacja i przemysł, zapewniając ochronę najbardziej wrażliwych danych.

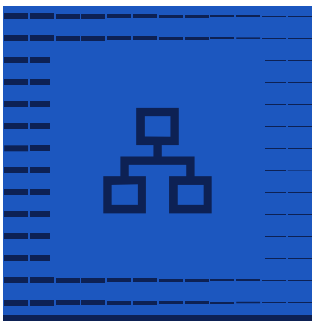


IZOLACJA
Fizyczna i logiczna separacja danych

NIEZMIENNOŚĆ
Blokada przed edycją lub skasowaniem danych.
Gwarancja niezmienności danych



WERYFIKACJA
Analityka i wykrywanie ataków



PROCEDURY
Przetestowanie metody odtwarzania danych

PODSUMOWUJĄC

Cyfrowy Bunkier Dell Technologies to nie tylko produkty, ale kompleksowe rozwiązanie dla organizacji, które chcą zapewnić sobie najwyższy możliwy poziom ochrony danych w obliczu rosnących zagrożeń cybernetycznych.

CERTYFIKACJE

Rozwiązanie PowerProtect Cyber Recovery Dell Technologies, to pierwsze rozwiązanie zgodne z wymaganiami **Sheltered Harbor**, umożliwiające instytucjom finansowym spełnienie standardów dotyczących przechowywania danych i zapewnienie operacyjnej odporności i odzyskiwania danych.

Dell jest aktywnym członkiem inicjatywy Sheltered Harbor i stale pracuje nad rozwiązaniami spełniającymi coraz wyższe wymagania regulacyjne i środowiska biznesowego.

ZOBACZ TAKŻE

Zgodność z NIS2 – cyberbezpieczeństwo w zgodzie z dyrektywą europejską

Zgodność z DORA – efektywne strategie bezpieczeństwa cyfrowego

Kompas IT – innowacyjne rozwiązania dla efektywności i cyfrowej odporności IT

Poznaj rozwiązania Dell Technologies

Porozmawiajmy o nowych standardach cyfrowej odporności organizacji

Paweł Chruściak
Senior Data Protection Account Executive
Dell Technologies
pawel.chrusciak@dell.com