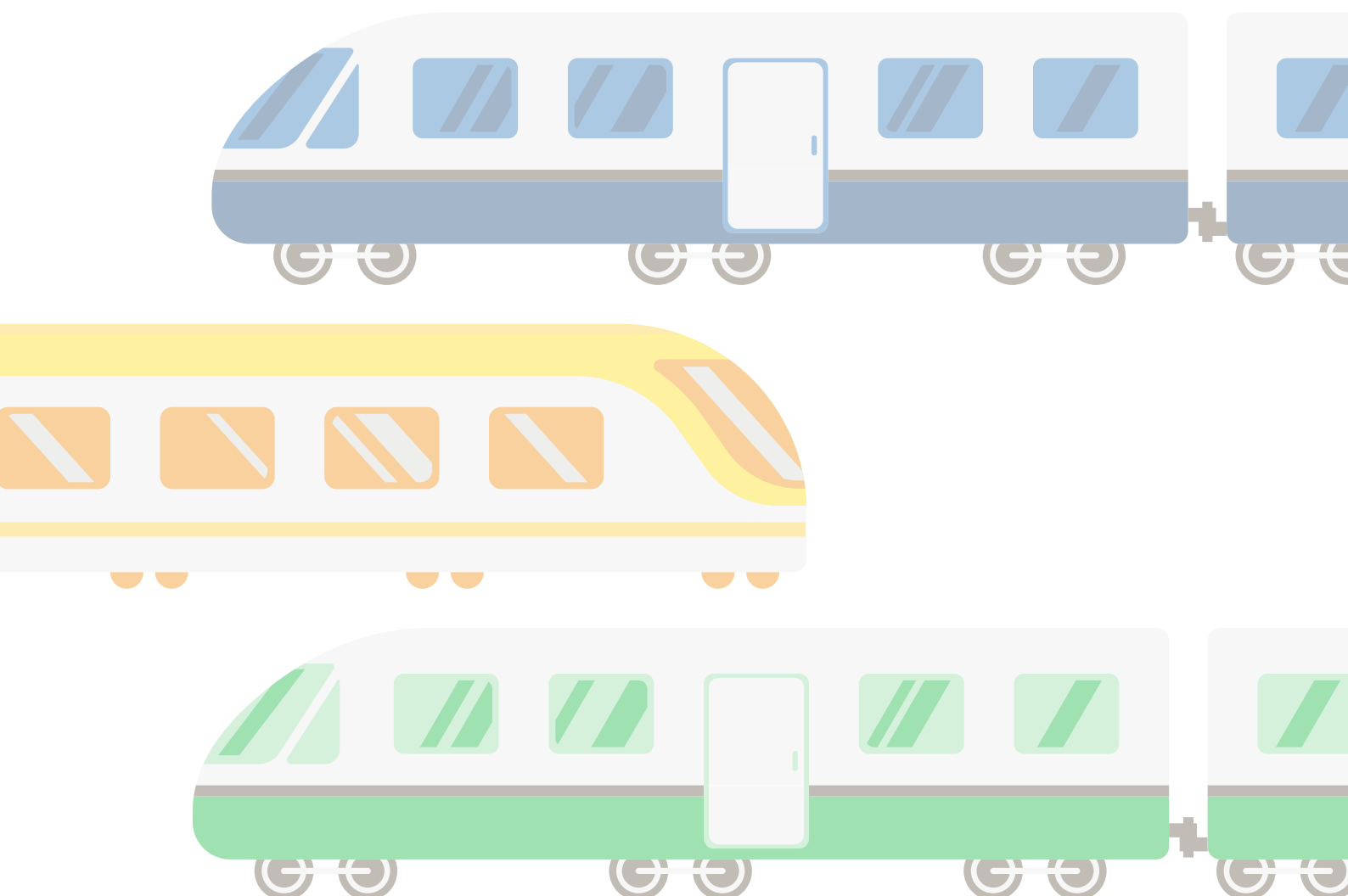


INTRATEL



ZAGROŻENIA CYFROWE W BRANŻY TRANSPORTOWEJ

JAK FREIGHTLINER CHRONI SWOJE DANE



WPROWADZENIE

W dzisiejszym cyfrowym świecie bezpieczeństwo danych jest krytyczne dla każdej firmy. Nowoczesne przedsiębiorstwa operują ogromnymi ilościami informacji, które są kluczowe dla ich codziennego funkcjonowania i długoterminowego sukcesu. Dane te obejmują zarówno wrażliwe informacje klientów, jak i wewnętrzne raporty finansowe, plany strategiczne czy dane operacyjne. Utrata dostępu do tych danych lub ich naruszenie może mieć druzgocące skutki, dlatego ochrona przed cyberzagrożeniami, w tym atakami ransomware, stała się priorytetem.

ATAKI RANSOMWARE: NA CZYM POLEGAJĄ I JAKIE MAJĄ SKUTKI? ✓

Ataki ransomware to forma cyberprzestępczości, w której złośliwe oprogramowanie szyfruje dane ofiary, a cyberprzestępcy żądają okupu za ich odblokowanie. Zazwyczaj atak rozpoczyna się od zainfekowania systemu komputerowego lub sieci poprzez phishing (fałszywe e-maile) lub złośliwe oprogramowanie pobierane z internetu. Gdy ransomware uzyska dostęp do danych, zaczyna je szyfrować, co uniemożliwia użytkownikom dostęp do swoich plików. Następnie cyberprzestępcy wyświetlają wiadomość z żądaniem okupu, grożąc trwałym usunięciem lub opublikowaniem danych, jeśli okup nie zostanie zapłacony.

SKUTKI ATAKÓW RANSOMWARE ✓

„W naszej branży, gdzie każde opóźnienie i każda utrata danych mogą oznaczać poważne straty, bezpieczeństwo danych jest absolutnym priorytetem. Właśnie dlatego zdecydowaliśmy się na rozwiązania Veeam i Intratel. Widzimy, że to najlepsza ochrona dla naszych kopii zapasowych, która zapewnia nam nie tylko bezpieczeństwo przed atakami ransomware, ale również gwarantuje ciągłość działalności.”

Rafał Śladowski, kierownik ds. IT, Freightliner

1

Utrata danych

Bez możliwości odszyfrowania plików firmy mogą stracić dostęp do kluczowych danych, co prowadzi do przerw w działalności i utraty zaufania klientów

2

Przestoje w działalności

Firmy mogą zostać zmuszone do czasowego zamknięcia lub znacznego ograniczenia operacji, co prowadzi do poważnych strat finansowych

3

Koszty finansowe

Oprócz potencjalnego okupu, firmy ponoszą koszty związane z przywracaniem systemów, śledztwem w sprawie incydentu i wprowadzaniem nowych zabezpieczeń

4

Reputacja

Utrata danych klientów lub niemożność świadczenia usług może negatywnie wpłynąć na reputację firmy, co ma długoterminowe konsekwencje biznesowe

5

Ryzyko prawne

Firmy mogą być narażone na działania prawne związane z naruszeniem ochrony danych osobowych, zwłaszcza w kontekście regulacji takich jak RODO

PRZYPADEK FREIGHTLINER: DĄŻENIE DO BEZPIECZEŃSTWA

Freightliner, spółka zajmująca się przewozem towarów kolejną w Polsce i krajach sąsiednich, doskonale zdaje sobie sprawę z powagi tych zagrożeń. Przedsiębiorstwo to, operujące w kluczowym sektorze transportu, przechowuje i przetwarza ogromne ilości danych dotyczących logistyki, harmonogramów transportowych, kontraktów i klientów. Zrozumienie, jak istotna jest ochrona tych danych przed ransomware i innymi zagrożeniami, skłoniło Freightliner do poszukiwania solidnych rozwiązań w zakresie ochrony kopii zapasowych.

Bezpieczeństwo kopii zapasowych to jeden z fundamentalnych elementów strategii obrony przed ransomware. Dzięki odpowiednio zabezpieczonym i odizolowanym kopiom zapasowym, przedsiębiorstwa mogą szybko odzyskać dostęp do swoich danych. Rozwiązania takie jak regularne tworzenie kopii zapasowych, testowanie ich integralności oraz przechowywanie w bezpiecznych, zaszyfrowanych lokalizacjach, stają się nieodzowną częścią strategii IT w firmach świadomych ryzyka, jakim są ataki ransomware.

Freightliner, inwestując w nowoczesne technologie ochrony danych, zyskuje nie tylko zabezpieczenie przed ransomware, ale także zwiększa swoją odporność na różnorodne inne zagrożenia cybernetyczne. Wprowadzenie skutecznych mechanizmów obronnych zapewnia ciągłość działalności operacyjnej i chroni reputację firmy na rynku.

WYZWANIE



Dotychczasowe rozwiązania w zakresie tworzenia kopii zapasowych w firmie Freightliner wymagały modernizacji, aby skutecznie przeciwdziałać nowym zagrożeniom, takim jak ataki ransomware. System nie zapewniał odpowiedniej ochrony przed możliwością szyfrowania lub usunięcia danych przez cyberprzestępców. W przypadku skutecznego ataku, utrata danych mogłaby sparaliżować operacje Freightliner na długi czas, co miałyby katastrofalne skutki zarówno dla ich logistyki, jak i dla ich klientów.

W obliczu tych zagrożeń, klient poszukiwał zaawansowanego rozwiązania, które nie tylko zabezpieczyłoby kopie zapasowe, ale także gwarantowałoby ich integralność i nienaruszalność. Wymagał systemu, który chroniłby kopie zapasowe przed modyfikacjami przez osoby nieuprawnione, zapewniając jednocześnie, że dane te będą stale dostępne i gotowe do przywrócenia w przypadku jakiegokolwiek awarii. Nowe rozwiązanie miało również oferować funkcje takie jak niezmienność zapisów, monitoring w czasie rzeczywistym oraz mechanizmy detekcji i odpowiedzi na podejrzane aktywności, co umożliwiłoby natychmiastowe reagowanie na potencjalne zagrożenia.

Takie podejście miało na celu nie tylko zwiększenie ochrony danych, ale także podniesienie standardów bezpieczeństwa informatycznego w całej organizacji, dając Freightliner pewność, że ich dane są bezpieczne i dostępne w każdej chwili, niezależnie od skali ataku, na jaki mogliby być narażeni.

ROZWIĄZANIE

VEEAM HARDENED REPOSITORY: NIEZAWODNA OCHRONA KOPII ZAPASOWYCH FREIGHTLINER

W odpowiedzi na narastające zagrożenia związane z atakami ransomware, Freightliner zdecydował się na wdrożenie rozwiązania Veeam Backup & Replication z funkcjonalnością Hardened Repository, rekomendowanego przez Intratel, eksperta w dziedzinie bezpieczeństwa i dostępności danych. To innowacyjne narzędzie oferuje zaawansowane funkcje ochrony kopii zapasowych, zapewniając ich niezmienność i odporność na nieautoryzowane modyfikacje.

NIEZMIENNOŚĆ DANYCH



1

Definiowanie Okresu Niezmienności

Ustal czas, przez jaki kopie zapasowe mają pozostać niezmiennie, uniemożliwiając ich edycję lub usunięcie

2

Wykorzystanie Systemu Linux

Funkcje niezmienności w systemie operacyjnym Linux zabezpieczają pliki kopii zapasowych

3

Atrybut Niezmienności

Każdy plik kopii zapasowej jest chroniony atrybutem niezmienności, co zapobiega jego modyfikacji

4

Ochrona Metadanych

Metadane powiązane z kopiami zapasowymi są zabezpieczone przed zapisem i usunięciem do czasu wygaśnięcia okresu niezmienności

„Veeam Hardened Repository to jedno z naszych ulubionych rozwiązań przy wdrożeniach u klientów, którzy poszukują najwyższego poziomu ochrony dla swoich kopii zapasowych. Jego zaawansowane funkcje bezpieczeństwa, takie jak niezmienność danych i jednorazowe poświadczenia, nie tylko skutecznie chronią przed atakami ransomware, ale również gwarantują integralność i dostępność danych w każdej sytuacji. To narzędzie zapewnia nam pewność, że dane klientów są bezpieczne, niezawodne i zgodne z wymogami regulacyjnymi.”

Paweł Mikulicz, Ekspert ds. Rozwiązań IT w Intratel

JEDNORAZOWE POŚWIADCZENIA



1

Maksymalizacja Bezpieczeństwa

Podczas dodawania serwera Linux do infrastruktury kopii zapasowych wykorzystywane są jednorazowe poświadczenia

2

Bezpieczne Przechowywanie

Poświadczenia nie są przechowywane na serwerze Veeam Backup & Replication, co minimalizuje ryzyko wycieku w przypadku włamania

3

Ochrona w Razie Naruszenia

Nawet jeśli serwer Veeam zostanie zaatakowany, atakujący nie uzyskają dostępu do zabezpieczonych kopii zapasowych

DODATKOWE KORZYŚCI VEEAM HARDENED REPOSITORY ✓

1

Ochrona przed Ransomware

Skutecznie zabezpiecza kopie zapasowe przed szyfrowaniem przez ransomware i innymi złośliwymi oprogramowaniami

2

Odporność na Awarie

Gwarantuje integralność kopii zapasowych, chroniąc je przed przypadkowym usunięciem lub modyfikacją

3

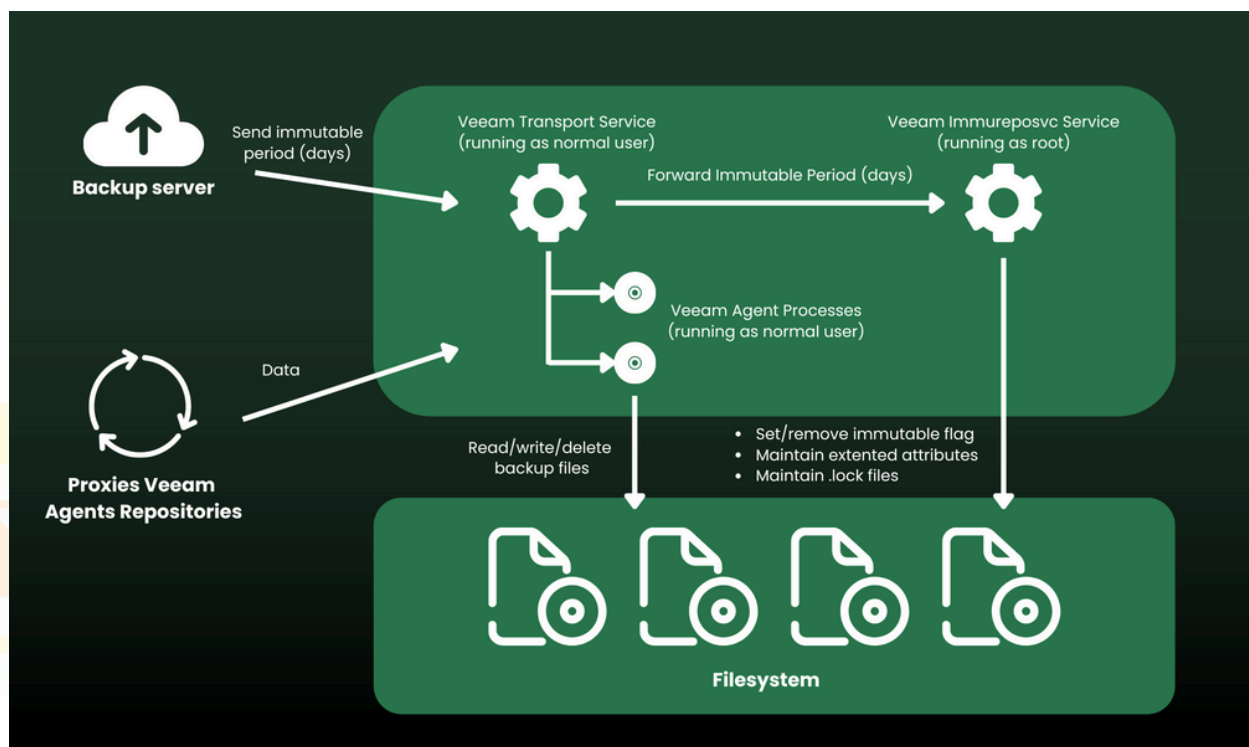
Usprawnione Odzyskiwanie Danych

Umożliwia szybkie i sprawne odzyskiwanie danych w przypadku awarii lub cyberataku

4

Zgodność z Wymogami Regulacyjnymi

Pomaga w spełnieniu rygorystycznych wymagań dotyczących ochrony danych



WNIOSKI

Wdrożenie Veeam Hardened Repository okazało się ogromnym sukcesem dla Freightliner, przynosząc wiele korzyści wykraczających poza początkowe oczekiwania. Rozwiązanie to nie tylko skutecznie podniosło poziom ochrony kopii zapasowych przed atakami ransomware i innymi zagrożeniami, ale również znacząco zwiększyło ogólną wydajność oraz usprawniło monitorowanie procesów związanych z kopiami zapasowymi.

Wzrost Bezpieczeństwa i Ochrony Danych

Dzięki Veeam Hardened Repository, Freightliner zyskał pewność, że ich kopie zapasowe są chronione przed szyfrowaniem, usunięciem czy modyfikacją przez złośliwe oprogramowanie. Funkcje takie jak niezmienność danych zapewniają, że pliki kopii zapasowych pozostają nienaruszalne przez określony czas, co uniemożliwia ich nieautoryzowaną modyfikację. To oznacza, że nawet w przypadku skutecznego ataku ransomware, dane zapasowe są odporne na manipulację, co umożliwia szybkie odzyskiwanie danych bez ryzyka utraty informacji.

Poprawa Wydajności i Monitorowania

Implementacja Veeam Hardened Repository poprawiła również wydajność operacyjną w zakresie zarządzania kopiami zapasowymi. System został zoptymalizowany pod kątem szybszego tworzenia i odtwarzania kopii zapasowych, co zminimalizowało czas przestoju w razie awarii. Udoskonalone narzędzia monitorowania umożliwiły bardziej precyzyjne śledzenie statusu kopii zapasowych i natychmiastowe wykrywanie potencjalnych problemów, co z kolei pozwala na szybsze reagowanie i rozwiązywanie ewentualnych zagrożeń.



Wyższy poziom bezpieczeństwa danych



Lepszą wydajność



Niezmienność i integralność kopii zapasowych



Usprawnione monitorowanie



Spełnienie wymagań regulacyjnych

WSPARCIE INTRATEL – KLUCZ DO SUKCESU



Za sukcesem tego wdrożenia stoi nie tylko samo rozwiązanie technologiczne, ale również wsparcie Intratel, zaufanego doradcy w dziedzinie bezpieczeństwa IT. Eksperti z Intratel dokładnie przeanalizowali potrzeby Freightliner, uwzględniając specyfikę działalności firmy i jej wymagania w zakresie ochrony danych. Dzięki temu, Intratel pomógł w wyborze i skutecznym wdrożeniu Veeam Hardened Repository, które idealnie wpisuje się w strukturę operacyjną Freightliner, gwarantując zgodność z wymaganiami regulacyjnymi oraz standardami bezpieczeństwa.