Synology®

Chroń swoją organizację przed oprogramowaniem ransomware

Przewiduje się, że przez ataki ransomware organizacje poniosą koszty w wysokości łącznie 8 bilionów USD w samym 2023 roku[1]. Plany ochrony danych z opcjami szybkiego przywracania mają kluczowe znaczenie dla złagodzenia wpływu oprogramowania ransomware i innych form cyberprzestępczości.

Date 13 paź 2023

Kopie zapasowe: ostatnia linia obrony w przypadku katastrofy

W przypadku utraty danych po złośliwym usunięciu lub modyfikacji kopie zapasowe umożliwiają przywrócenie danych o znaczeniu krytycznym i uniknięcie kosztownych przestojów. Skorzystaj z rozwiązań firmy Synology w zakresie ochrony danych, aby zaprojektować strategię tworzenia kopii zapasowych dla całej infrastruktury IT.

Pełna ochrona

Zabezpiecz punkty końcowe, a także podstawowe kopie zapasowe, aby utworzyć wiele sieci bezpieczeństwa dla danych.

Szybkie przywracanie

Ogranicz przestoje w przypadku awarii do minimum dzięki opcjom natychmiastowego odzyskiwania.

Przechowywanie w stanie Niezmienne

Zapobiegaj nieautoryzowanym zmianom danych i migawek.

Kopie zapasowe bez licencji

Twórz kopie zapasowe tylu danych, na ile pozwala miejsce w pamięci masowej, bez ograniczeń i ukrytych opłat.

Scentralizowana ochrona przed oprogramowaniem ransomware

Konsoliduj kopie zapasowe z flot stacji roboczych, serwerów, maszyn wirtualnych i aplikacji w chmurze. Zoptymalizuj zużycie pamięci masowej i unikaj ograniczeń przepustowości dzięki technologii deduplikacji danych i przyrostowych kopii zapasowych. https://www.synology.com/dsm/solution/infrastructure

Obciążenia fizyczne

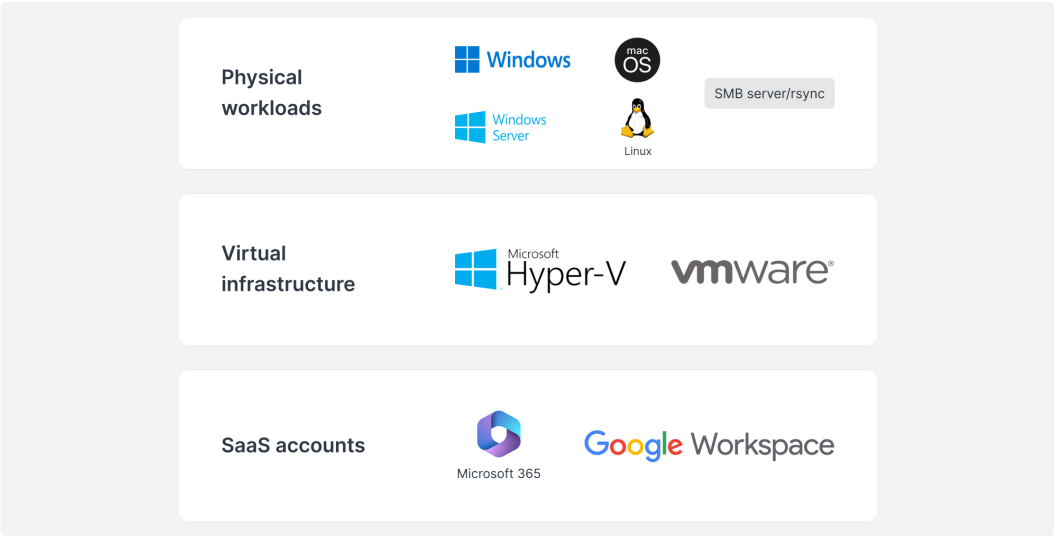
Chroń punkty końcowe w przypadku złośliwych ataków dzięki tworzeniu kompleksowych kopii zapasowych typu bare-metal i elastycznemu odzyskiwaniu danych na poziomie plików.

Infrastruktura wirtualna

Twórz kopie zapasowe maszyn wirtualnych VMware® vSphere™, Microsoft® Hyper-V® i jednostek LUN za pomocą zaawansowanych technologii redukcji danych.

Konta SaaS

Zastosuj ciągłą ochronę danych przechowywanych w chmurze dzięki automatycznemu wykrywaniu nowo dodanych kont.



Skuteczne odzyskiwanie

Zminimalizuj czas przestojów krytycznych systemów produkcyjnych, szybko przywracając kopie zapasowe z lokalnego lub zdalnego systemu Synology.

Cel RTO bliski zeru

Montuj obrazy kopii zapasowej w programie VMware®, Hyper-V® lub Synology Virtual Machine Manager, aby jak najszybciej wznowić pracę. Przywracaj maszyny wirtualne do innego monitora maszyny wirtualnej w celu uniknięcia zakłóceń w działaniu usług.

Minimalny cel RPO

Skonfiguruj częstotliwość tworzenia kopii zapasowych zgodnie z potrzebami, ograniczając do minimum ilość danych potencjalnie dotkniętych atakiem. Szybko chroń systemy dzięki technologii tworzenia przyrostowych kopii zapasowych i deduplikacji.

Intuicyjne działanie

Pozwól pracownikom przeszukiwać i przeglądać wiadomości e-mail, kontakty i pliki z wygodnego portalu zanim zostaną przywrócone, zapewniając bardziej przyjazne dla użytkownika doświadczenie i zmniejszając obciążenie IT zespołów.

Dodatkowa warstwa ochrony

Stosuj strategię tworzenia kopii zapasowych 3-2-1, przechowując trzeci zestaw danych w lokalizacji zdalnej lub w chmurze, chroniąc dane przed pożarem, klęską żywiołową lub kradzieżą.

W serwerach w lokalizacji zdalnej

Przechowuj kopie zapasowe na serwerze Synology w lokalizacji dodatkowej, aby chronić się przed klęskami żywiołowymi i replikować migawki bez możliwości wprowadzania zmian, aby zapewnić dodatkową ochronę przed oprogramowaniem ransomware.

W chmurze

Twórz kopie zapasowe danych u dowolnego popularnego dostawcy pamięci masowej w chmurze chroniąc dane przed nieautoryzowanym dostępem dzięki szyfrowaniu AES-256 po stronie klienta. https://c2.synology.com/storage/nas

Zaufanie różnych branży

„Rozwiązania Synology [...] pozwoliły nam zmniejszyć wydatki na sprzęt serwerowy [...], jednocześnie upraszczając tworzenie kopii zapasowych infrastruktury i stacji roboczych, rejestrowanie systemu i zarządzanie plikami”.
https://www.synology.com/company/case_study/Investortools

„Dzięki funkcji Active Backup for Business wszystkie nasze kopie zapasowe są teraz scentralizowane i dostępne przez całą dobę 7 dni w tygodniu, co pomaga zminimalizować czas przestoju i zachować zgodność z przepisami FERPA”.
https://www.synology.com/company/case_study/University_of_Washington

Pakiet Active Backup for Business zapewnia niesamowitą szybkość tworzenia kopii zapasowych i działa cuda w kwestii usuwania duplikatów danych — zajmuje tylko 28 TB z 58 TB pamięci serwera [...]”.
https://www.synology.com/company/case_study/SHISEIDO_Taiwan_ABB

„[...]Active Backup for Business umożliwia centralizację wszystkich zadań tworzenia kopii zapasowych i zarządzanie nimi za pomocą jednej konsoli. Szybkie i niezawodne odzyskiwanie zapewnia również ciągłość pracy”.
https://www.synology.com/company/case_study/UNESCO

Często zadawane pytania

Co to jest oprogramowanie typu ransomware?

Ransomware to rodzaj złośliwego oprogramowania, który szyfruje pliki ofiar. Następnie atakujący żąda okupu za przywrócenie dostępu do danych, często grożąc trwałym zniszczeniem danych, jeśli okup nie zostanie opłacony. Ataki typu ransomware mogą prowadzić do znacznych zakłóceń pracy i powodować ogromne straty finansowe dla osób fizycznych i organizacji. Ważne jest, aby chronić siebie i swoje urządzenia przed atakami ransomware, na przykład poprzez regularne aktualizowanie oprogramowania i tworzenie kopii zapasowych plików.

Jakie są rodzaje oprogramowań ransomware?

Istnieje wiele różnych typów oprogramowań ransomware, a ich nowe odmiany są stale tworzone. Niektóre z najczęstszych typów oprogramowania ransomware to:

- **Szyfrujące oprogramowania ransomware** — najpopularniejszy typ oprogramowania ransomware szyfruje pliki ofiary tak, aby nie można było uzyskać do nich dostępu bez klucza deszyfrowania. Następnie atakujący żąda zapłaty okupu w zamian za klucz
- **Blokujące oprogramowanie ransomware** — typ oprogramowania ransomware blokujący dostęp ofiary do komputera poprzez zmianę poświadczeń logowania lub wyświetlanie komunikatu, który uniemożliwia ofiarom uzyskanie dostępu do systemu. Następnie atakujący żąda zapłaty okupu za odblokowanie komputera
- **Ransomware jako usługa (RaaS)** — model biznesowy, w którym atakujący oferuje oprogramowanie ransomware innym osobom lub grupom, które chcą przeprowadzić ataki. Pierwszy typ zazwyczaj dostarcza oprogramowanie ransomware i obsługuje płatności, podczas gdy drugi otrzymuje procent od zapłaconego okupu
- **Scareware** — oprogramowanie ransomware mające na celu zastraszenie ofiary w celu zapłacenia przez nią okupu. Zwykle polega na wyświetlaniu fałszywych ostrzeżeń dotyczących bezpieczeństwa lub wiadomości, informujących, że komputer ofiary jest zainfekowany wirusem. Następnie atakujący żąda zapłaty okupu w celu usunięcia rzekomej infekcji

Jak rozprzestrzeniane jest oprogramowanie ransomware?

Oprogramowanie ransomware jest zwykle rozprzestrzeniane za pośrednictwem wiadomości e-mail wyłudzających informacje lub wykorzystujących luki w zabezpieczeniach systemu komputerowego. Podczas ataku phishingowego atakujący wysyła wiadomość e-mail, która wydaje się pochodzić z wiarygodnego źródła, takiego jak bank lub znana firma. Taka wiadomość e-mail często zawiera łącze lub załącznik, który po kliknięciu instaluje oprogramowanie ransomware na komputerze ofiary. Wykorzystanie luk w zabezpieczeniach systemu działa podobnie, z tą różnicą, że atakujący wykorzystuje błąd zabezpieczeń systemu do zainstalowania oprogramowania ransomware bez wiedzy ofiary. W obu przypadkach po zainstalowaniu oprogramowania ransomware może szybko rozprzestrzenić się na inne komputery w tej samej sieci.

Jak wygląda typowy przebieg ataku ransomware?

Atak ransomware przebiega zazwyczaj w trzech fazach:

1. Atakujący uzyskuje dostęp do komputera ofiary, wysyłając wiadomość e-mail wyłudzającą informacje lub wykorzystując lukę w zabezpieczeniach systemu
2. Po uzyskaniu dostępu do komputera ofiary instaluje na komputerze oprogramowanie ransomware
3. Oprogramowanie ransomware szyfruje pliki ofiary, przez co stają się one niedostępne dla użytkownika
4. Następnie atakujący żąda od ofiary okupu, zazwyczaj w formie waluty cyfrowej, takiej jak Bitcoin, w zamian za klucz odszyfrowujący, który odblokuje zaszyfrowane pliki
5. Jeśli ofiara zapłaci okup, osoba atakująca dostarczy klucz odszyfrowujący, a ofiara będzie mogła ponownie uzyskać dostęp do swoich plików. Nie ma jednak gwarancji, że osoba atakująca faktycznie dostarczy klucz, a nawet jeśli to zrobi, pliki ofiary mogą zostać uszkodzone lub ulec degradacji w wyniku procesu szyfrowania

Ważne jest, aby pamiętać, że istnieje wiele odmian tego procesu i nie wszystkie ataki ransomware będą przebiegały dokładnie według tego schematu. Niektóre ataki mogą na przykład w ogóle nie obejmować szyfrowania plików, podczas gdy inne mogą stosować inne formy wymuszania lub szantażu.

W jaki sposób można paść ofiarą oprogramowania ransomware?

Ofiarą oprogramowania ransomware można paść na kilka sposobów. Jednym z najczęstszych sposobów jest kliknięcie złośliwego łącza lub załącznika w wiadomości e-mail wyłudzającej informacje. Ten typ wiadomości e-mail ma wyglądać wiarygodnie, często wydaje się pochodzić od znanych firm lub organizacji. Kliknięcie łącza lub załącznika powoduje zainstalowanie oprogramowania ransomware na komputerze. Innym sposobem jest odwiedzenie zaatakowanej witryny. Witryny takie są hakowane przez atakujących, którzy wprowadzając kod automatycznie instalujący oprogramowanie ransomware na komputerze po odwiedzeniu witryny. Ofiarą oprogramowania ransomware można również paść pobierając zainfekowane pliki z Internetu. Może się tak zdarzyć w przypadku pobrania pliku z podejrzanej witryny lub pobrania pliku udostępnionego przez nieznaną osobę. Krótko mówiąc, podczas przeglądania Internetu należy zachowywać ostrożność i unikać klikania łączy lub pobierania plików z nieznanych źródeł. Może to pomóc w ochronie przed złośliwym oprogramowaniem typu ransomware i innymi rodzajami złośliwego oprogramowania.

W kogo są wymierzone ataki ransomware?

Ataki typu ransomware mogą obrać za cel każdego użytkownika, który korzysta z komputera lub innego urządzenia podłączonego do Internetu. Jednak niektóre grupy są na nie bardziej narażone niż inne. Na przykład ataki typu ransomware często są wymierzone w firmy, ponieważ zazwyczaj mają one więcej cennych danych i mogą być bardziej skłonne do zapłaty okupu, aby je odzyskać. Częstymi celami ataków są również szpitale, szkoły i inne organizacje świadczące usługi o znaczeniu krytycznym, ponieważ atak typu ransomware może zakłócić ich działalność i narażać życie ludzi. Celem ataków ransomware mogą być również osoby fizyczne. W takich przypadkach osoby atakujące mogą próbować wyłudzić pieniądze od ofiary, grożąc usunięciem jej plików osobistych lub opublikowaniem poufnych informacji, chyba że zostanie zapłacony okup. Cele ataków ransomware są często wybierane w oparciu o wartość ich danych i gotowość do zapłaty okupu w celu ich przywrócenia.

Jakie ryzyko niesie za sobą zapłacenie okupu oprogramowaniu ransomware?

Płacenie okupu osobie przeprowadzającej atak ransomware może wydawać się najprostszym sposobem na odzyskanie plików, ale może to być bardzo ryzykowna decyzja. Istnieje kilka niebezpieczeństw związanych z opłaceniem okupu, w tym:

- Nie ma gwarancji, że atakujący faktycznie dostarczy klucz deszyfrowania. W wielu przypadkach ofiary, które zapłacą okup, nigdy nie otrzymują klucza i nie odzyskują dostępu do swoich plików
- Zapłacenie okupu może zachęcić atakujących do kontynuowania działalności. Jeśli atakujący wiedzą, że ofiary są skłonne zapłacić okup, mogą być bardziej skłonni do przeprowadzenia kolejnych ataków w przyszłości
- Płacąc okup możesz stać się celem przyszłych ataków. Jeśli osoba atakująca wie, że jesteś w stanie zapłacić okup, jest bardziej prawdopodobne, że w przyszłości staniesz się celem kolejnego ataku
- Zapłacenie okupu może być nielegalne. W niektórych przypadkach płacenie okupu organizacji przestępczej może być uznane za formę finansowania terroryzmu lub innej nielegalnej działalności

Chociaż zapłacenie okupu może wydawać się najprostszym sposobem na odzyskanie plików, może to być naprawdę bardzo ryzykowna decyzja. Ważne jest, aby przed podjęciem decyzji dokładnie rozważyć ryzyko.

Jaka jest wysokość okupu ransomware?

Koszt ataku ransomware może się znacznie różnić w zależności od wielu czynników, takich jak typ użytego oprogramowania ransomware, liczba zaszyfrowanych plików i skuteczność ataku. W niektórych przypadkach koszt ataku ransomware może być stosunkowo niski, a atakujący mogą żądać okupu z wysokości kilkuset dolarów. W innych przypadkach koszt może być znacznie wyższy, a atakujący mogą żądać tysięcy dolarów lub nawet więcej za przywrócenie ofierze dostępu do plików. Oprócz bezpośrednich kosztów związanych z płaceniem okupu, ataki ransomware mogą również spowodować znaczące koszty pośrednie. Atak ransomware może na przykład prowadzić do przestojów i utraty produktywności, co może spowodować utratę dochodów i przychodów. Może również nadszarpnąć reputację firmy i zaufanie klientów, co może mieć długoterminowy negatywny wpływ na prowadzoną działalność. Te pośrednie koszty są często znacznie wyższe od samego okupu.

Jakie są objawy ataku ransomware?

Objawy ataku ransomware mogą się różnić w zależności od konkretnego typu użytego oprogramowania. Jednak niektóre typowe objawy są następujące:

- Twoje pliki są zaszyfrowane i nie możesz uzyskać do nich dostępu
- Otrzymujesz wiadomość od osoby atakującej, która domaga się zapłaty okupu w zamian za klucz odszyfrowujący
- Widzisz nieznane programy lub procesy uruchomione na komputerze
- Komputer działa wolno lub nie odpowiada
- Komputer wyświetla nietypowe komunikaty o błędach lub wyskakujące okna

Jeśli podejrzewasz, że komputer został zainfekowany oprogramowaniem ransomware, ważna jest szybka reakcja. Odłącz komputer od Internetu, aby zapobiec rozprzestrzenianiu się oprogramowania ransomware.

Jak zapobiegać atakom typu ransomware?

Istnieje kilka działań, które można podjąć, aby zapobiec atakom ransomware, na przykład:

- Korzystaj ze znanego oprogramowania antywirusowego lub zabezpieczającego i dbaj, by było zawsze aktualne. Może to pomóc w ochronie komputera przed oprogramowaniem ransomware i innymi rodzajami złośliwego oprogramowania
- Zachowaj ostrożność podczas otwierania załączników do wiadomości e-mail lub łączy. Oprogramowanie ransomware jest często dostarczane za pośrednictwem wiadomości e-mail wyłudzających informacje, dlatego warto podchodzić ostrożnie do klikanych elementów
- Dbaj o aktualność systemu operacyjnego i innych oprogramowań. Aktualizacje oprogramowania często zawierają poprawki zabezpieczeń, które mogą pomóc chronić komputer przed oprogramowaniem ransomware i innymi zagrożeniami
- Regularnie twórz kopie zapasowe plików. Może to pomóc w ochronie danych, jeśli komputer zostanie zainfekowany oprogramowaniem ransomware. Przestrzegaj jednej z zalecanych strategii tworzenia kopii zapasowych, takich jak strategia tworzenia kopii zapasowych 3-2-1
- Pamiętaj o ryzyku związanym z oprogramowaniem typu ransomware i edukuj o nich innych pracowników w organizacji. Może to pomóc w zapobieganiu atakom ransomware oraz ułatwić ich wykrywanie i reagowanie na ich wystąpienie

Najlepszym sposobem zapobiegania atakom ransomware jest zachowanie czujności i podjęcie kroków w celu ochrony komputera i danych. Może to pomóc zmniejszyć ryzyko ataku ransomware i ułatwić złagodzenie jego skutków, jeśli już nastąpi.

W jaki sposób rozwiązania Synology mogą chronić mnie przed atakami ransomware?

Działania zapobiegawcze mają zasadnicze znaczenie w unikaniu ataków typu ransomware. Oprócz wybranego oprogramowania antywirusowego korzystaj z następujących rozwiązań Synology:

- **Ogranicz dostęp** — zmniejsz rozprzestrzenianie się oprogramowania typu ransomware, ustawiając uprawnienia plików, aplikacji i dostępu oraz konfigurując bezpieczne poświadczenia logowania za pomocą usług Secure SignIn i C2 Password
- **Chroń urządzenia** — nieaktualne systemy są bardziej narażone na ataki. Aktualizuj wszystkie swoje serwery NAS jednocześnie za pomocą systemu Synology Central Management System (CMS) i zabezpiecz inne urządzenia za pomocą zasad grupy w Synology Directory Server i C2 Identity
- **Unikaj podejrzanych plików** — spam i phishingowe wiadomości e-mail zawierające podejrzane pliki to typowe metody rozpowszechniania oprogramowania ransomware. Synology MailPlus zapewnia skuteczną ochronę przed złośliwym oprogramowaniem i zapobiega spamowi
- **Sprawdzaj zabezpieczenia pod kątem luk** — skorzystaj z narzędzia Doradca ds. zabezpieczeń Synology, aby rutynowo skanować system w poszukiwaniu złośliwego oprogramowania, luk w zabezpieczeniach i nietypowych aktywności logowania. Wdróż zalecane zmiany w celu poprawy bezpieczeństwa serwera NAS.
  https://www.synology.com/dsm/overview/security

Więcej sposobów ochrony danych

Zarządzanie flotą

Korzystaj z rozbudowanych funkcji do centralnego zarządzania uprawnieniami dostępu do danych, stanem oprogramowania, stanem systemu i innymi funkcjami.
https://www.synology.com/dsm/overview/administration

Monitorowanie wszystkich urządzeń

Rozpoznawaj podejrzane aktywności logowania, zarządzaj aktualizacjami i monitoruj stan urządzeń bez względu na to, gdzie znajdują się urządzenia.
https://www.synology.com/dsm/feature/active-insight

Ochrona danych

Postępuj zgodnie ze strategią tworzenia kopii zapasowych 3-2-1, aby chronić dane przed przypadkową i złośliwą zmianą lub usunięciem.
https://www.synology.com/dsm/solution/data_backup

Chroń z każdej strony

Pobierz naszą listę kontrolną cyberbezpieczeństwa i zidentyfikuj swoje słabe punkty w przypadku ataku hakerskiego.
https://global.download.synology.com/download/Document/Software/Brochure/Firmware/DSM/7.0/plk/Se

Informacje ogólne

Kontakt z nami

Skontaktuj się z regionalnym działem sprzedaży, aby uzyskać więcej informacji
https://www.synology.com/form/inquiry/sales

Gdzie kupić

Znajdź partnera firmy Synology w swoim regionie
https://www.synology.com/wheretobuy

Uwagi:

1. eSentire, Oficjalny raport o cyberprzestępczości z 2022 r.
   https://www.esentire.com/resources/library/2022-official-cybercrime-report

Chroń swoją organizację przed oprogramowaniem ransomware

https://www.synology.com/pl-pl/dsm/solution/ransomware

Strona internetowa Synology

https://www.synology.com/

Kontakt z nami

https://www.synology.com/company/contact_us