Acronis

RAPORT

12-etapowy plan reagowania na atak ransomware dla firm

Jak bronić się przed największym cyberzagrożeniem na świecie i jak przywrócić zwykłą działalność po ataku

W ciągu zaledwie kilku lat ransomware stał się ulubionym narzędziem cyberprzestępców wykorzystywanym do zarabiania na straszeniu firm groźbą utraty danych i przestojami. Gwałtowny wzrost popularności ransomware podniósł średni koszt naruszenia danych, który w 2023 roku ma wynieść 5 milionów USD na incydent. Częstotliwość ataków rośnie w zastraszającym tempie, ponieważ cyberprzestępcy zwiększają skalę rozwoju i dystrybucji złośliwego oprogramowania. Każdego miesiąca pojawia się dziewięć milionów nowych instancji złośliwego oprogramowania.

Jednocześnie cyberprzestępcy nieustannie opracowują nowe taktyki i wykorzystują nowe technologie, takie jak sztuczna inteligencja (AI), w celu zwiększenia skuteczności ataków. Przykładowo szyfrowanie krytycznych danych ofiary w ataku ransomware nie jest już jedyną metodą wymuszania okupu. Większość ataków ransomware poprzedzona jest teraz etapem szyfrowania. Przestępcy najpierw kradną poufne dane, aby mogli zagrozić ich wyciekiem online, jeśli ofiara nie zapłaci okupu. Atakujący mogą również kontaktować się z klientami i partnerami ofiary, grożąc wyciekiem ich prywatnych danych, co zwiększa presję, aby spełnić żądania przestępców. Jeszcze inną taktyką jest grożenie, że w przypadku braku zapłaty dojdzie do ataku DDoS na publiczne serwery ofiary.

Atakujący wykorzystują teraz również nowe narzędzia sztucznej inteligencji, takie jak ChatGPT, aby poprawić pozorną autentyczność i wiarygodność wiadomości wyłudzających informacje, automatycznie skanować aplikacje pod kątem luk w zabezpieczeniach oraz poprawić zarządzanie wieloetapowymi atakami. Ulepszenia ataków oparte na sztucznej inteligencji, nowe taktyki wymuszeń i rosnąca częstotliwość ataków spowodowały, że firmy oferujące ubezpieczenie cybernetyczne zrezygnowały z ochrony firm, które nie mogą udowodnić, że stosują solidną ochronę.

Pomimo tej ponurej perspektywy, firmy mogą podjąć szereg konkretnych działań, aby znacznie zmniejszyć prawdopodobieństwo skutecznego ataku ransomware i zminimalizować szkody spowodowane przestojami i utratą danych, do których może dojść po ataku. Acronis zaleca przyjęcie następującego 12-etapowego planu przeciwdziałania zagrożeniu ransomware. Obejmuje on taktyki z trzech kategorii: aktywne środki obrony, nowe umiejętności i procesy dla IT i pracowników oraz usprawnione programy łagodzenia skutków ataków i odzyskiwania danych.

Usprawnij aktywne środki obrony

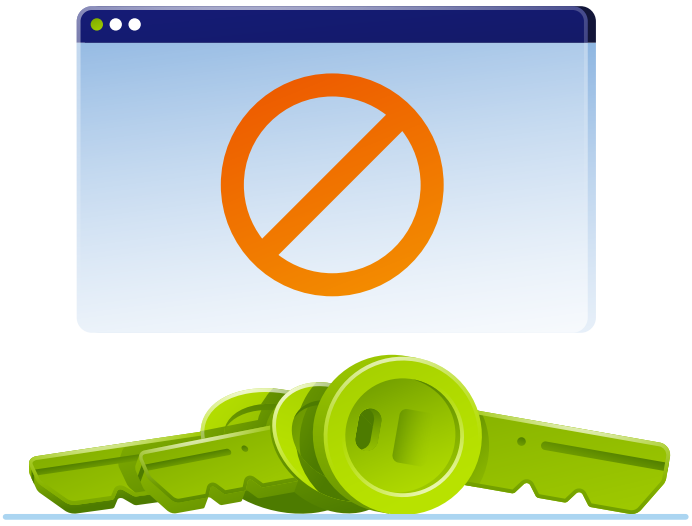
Etap pierwszy **Wprowadź środki obrony przed złośliwym oprogramowaniem, które są w stanie identyfikować ransomware na podstawie jego zachowania, aby uzupełnić starsze oprogramowanie antywirusowe oparte na sygnaturach**. Uczenie maszynowe i sztuczna inteligencja odgrywają w tym zakresie kluczową rolę, ponieważ umożliwiają wykrywanie wzorców złośliwego zachowania, a nie tylko dopasowywanie sygnatury instancji złośliwego oprogramowania do bazy danych znanych zagrożeń. Bez takiego podejścia behawioralnego żaden środek ochrony przed złośliwym oprogramowaniem nie jest w stanie z powodzeniem zidentyfikować tysięcy przypadków złośliwego oprogramowania typu zero-day, które są generowane każdego dnia przez cyberprzestępców.

Etap drugi **Zaktualizuj środki zaradcze, takie jak zabezpieczenia poczty e-mail i filtrowanie adresów URL.** W 2022 roku aż 30,6% wszystkich otrzymanych wiadomości e-mail było spamem, a 1,6% wiadomości zawierało złośliwe oprogramowanie lub linki wyłudzające informacje. Wyłudzanie informacji było stosowane w 76% wszystkich udanych ataków w 2022 roku, a w tym samym okresie około 8% punktów końcowych próbowało uzyskać dostęp do złośliwych adresów URL. Cyberprzestępcy znacznie lepiej radzą sobie z ukrywaniem złośliwych linków i załączników w wiadomościach e-mail. Dlatego jedną z najskuteczniejszych metod, jakie mogą wprowadzić firmy, jest inwestowanie w aktualne zabezpieczenia poczty e-mail, które będą wykrywać i odfiltrowywać wiadomości wyłudzające informacje, zanim dotrą one do skrzynki odbiorczej pracownika.

Etap trzeci **Wdrażaj narzędzia, które zwiększają widoczność zasobów IT i przepływów danych.** Po ataku ransomware bardzo często kadra zarządzająca zwraca się do działu IT z pytaniem: „W jaki sposób przestępcy przejęli cały terabajt naszych poufnych danych bez naszej wiedzy?” Aby uniknąć tego typu nieprzyjemnych sytuacji, monitoruj i rejestruj aktywność w swojej infrastrukturze, w tym dostęp do usług w chmurze, oraz prowadź bieżącą analizę dzienników. Narzędzia IT do inwentaryzacji i zapobiegania utracie danych (DLP) mogą również zapewnić lepszy wgląd w to, gdzie dane są przechowywane i jak są przenoszone, aby wykrywać kradzież danych i blokować potencjalne zagrożenia. Rozważ wdrożenie technologii wykrywania i reagowania w punkcie końcowym (EDR), która wykorzystuje monitorowanie w czasie rzeczywistym, analizę behawioralną i uczenie maszynowe w celu identyfikowania złośliwego oprogramowania, włamań i nieautoryzowanego dostępu.

Etap czwarty **Wyeliminuj zewnętrzne i wewnętrzne zagrożenia sieciowe.** Wyłącz protokół Microsoft Remote Desktop Protocol (RDP), z wyjątkiem przypadków, gdy jest on konieczny, i zabezpiecz punkty końcowe, dezaktywując nieużywane usługi. Używaj zapór sieciowych i systemów zapobiegania włamaniom, aby ograniczyć dostęp ruchu przychodzącego do Internetu. Zastanów się nad ograniczeniem dostępu VPN do określonych lokalizacji geograficznych. Możesz także ustanowić zasady pracy zdalnej, które ograniczają dostęp do zasobów firmy z urządzeń osobistych lub go zabraniają. Aby zminimalizować potencjalne zagrożenia ze strony złośliwych podmiotów lub nieostrożnych pracowników, podziel swoje sieci wewnętrzne na segmenty. W ten sposób powstrzymasz rozprzestrzenianie się ransomware z zaatakowanych systemów na inne punkty końcowe i serwery.

Etap piąty **Ostrożnie zarządzaj hasłami i prawami dostępu.** W 2022 roku wyciek lub kradzież danych uwierzytelniających stanowiła niemal połowę zgłoszonych naruszeń. Przestępcy stosujący ransomware często wykorzystują hasła, które udostępniono w sieci, hasła używane kilkakrotnie na wielu kontach, słabe hasła oraz uwierzytelnianie jednoskładnikowe. Atakujący często przejmują narzędzia operacyjne IT, takie jak Mimikatz, w celu kradzieży haseł przechowywanych w pamięci serwerów. Aby zwalczyć te taktyki, wprowadź uwierzytelnianie wieloskładnikowe, zwłaszcza w systemach z wrażliwymi danymi. Zawsze zmieniaj domyślnie ustawione poświadczenia logowania administratora. Po skutecznym ataku zmień wszystkie hasła, ponieważ cyberprzestępcy często przeprowadzają kolejny atak na swoją wcześniejszą ofiarę przy użyciu tych samych wykradzionych danych uwierzytelniających, które umożliwiły pierwszy atak. Przyjmij zasadę najmniejszego uprzywilejowania w zakresie praw dostępu. Ściśle kontroluj dostęp do systemów za pomocą zaawansowanych narzędzi administracyjnych lub poufnych danych, z wyłączeniem jedynie niezbędnych pracowników, oraz ogranicz uprawnienia czasowe lub jednorazowe tam, gdzie to możliwe.



Optymalizuj umiejętności i procesy

Etap szósty **Utwórz program szkoleniowy w zakresie bezpieczeństwa.** Wyłudzanie informacji jest nadal jedną z najskuteczniejszych technik wprowadzania złośliwego oprogramowania do zewnętrznych zabezpieczeń firmy. Dlatego ograniczenie kliknięć w złośliwe załączniki i linki w wiadomościach e-mail (a także w SMS-ach, wiadomościach z komunikatów internetowych i aplikacjach społecznościowych) może znacznie ograniczyć ryzyko. Wyszkol użytkowników, aby byli wyczuleni na podejrzane wiadomości, rutynowo wysyłając im fałszywe e-maile wyłudzające informacje. Oferuj kursy przypominające dla tych, którzy dali się nabrać na podstęp. Upewnij się, że wszyscy pracownicy biorą udział w szkoleniach, zwłaszcza kadra kierownicza, ponieważ to właśnie ona jest najczęstszym celem ataków ze względu na jej podwyższone uprawnienia i możliwość autoryzacji przelewów pieniężnych.

Etap siódmy **Wprowadź zautomatyzowane, programowe skanowanie luk w zabezpieczeniach oraz zarządzanie poprawkami.** Małe i średnie firmy mają zwykle trudności z terminowym instalowaniem poprawek oprogramowania otrzymywanych od dostawców technologii, przez co luki w zabezpieczeniach pozostają niezałatane średnio przez ponad 90 dni. Cyberprzestępcy są świadomi tej sytuacji i stale ją wykorzystują. Aby szybko i skutecznie zlikwidować luki w zabezpieczeniach, stosuj zautomatyzowane narzędzia do tego żmudnego, ale krytycznego zadania operacyjnego IT.

Etap ósmy **Zmniejsz liczbę agentów na punktach końcowych i konsolach w centrum operacyjnym.** Przeciętna firma wraz z upływem czasu wdraża fragmentarycznie różne rozwiązania w zakresie bezpieczeństwa cybernetycznego i ochrony danych, co powoduje mnożenie się zdalnych agentów na punktach końcowych i konsolach zarządzania w dziale IT. Wielu agentów punktów końcowych marnuje zasoby i często powoduje konflikty. Stosowanie wielu różnych konsoli zmniejsza wydajność operacyjną IT i zwiększa koszty szkoleń. Konsoliduj agentów tam, gdzie to możliwe, aby wyeliminować luki w zabezpieczeniach, pozbyć się konfliktów oraz poprawić wydajność punktów końcowych. Gdy to możliwe, łącz funkcje konsoli zarządzania, aby zmaksymalizować efektywność i szybkość wdrażania personelu IT.

Etap dziewiąty **Korzystaj z platform bezpieczeństwa, takich jak NIST, aby regularnie oceniać i aktualizować strategie obrony i ograniczania zagrożeń przed oprogramowaniem ransomware i innymi cyberzagrożeniami.** Oferują one sprawdzone najlepsze praktyki i wskazówki dotyczące ustalania priorytetów dla środków zaradczych związanych z bezpieczeństwem oraz ciągłego doskonalenia technologii, procesów i umiejętności pracowników.

Usprawnij łagodzenie ataków i odzyskiwanie danych

Etap dziesiąty **Wprowadź solidny schemat ochrony danych.** Atakujący działają pierwsi, więc zawsze mają przewagę. Często nawet najlepsza obrona przed atakami może nie poradzić sobie z nowymi taktykami i technologiami. Załóż, że atak w pewnym momencie będzie skuteczny i staraj się ulepszyć swój schemat ochrony danych, który jest ostatnią linią obrony. Przywrócenie danych z ostatniej kopii zapasowej może umożliwić szybkie wznowienie działalności biznesowej – nawet bez płacenia okupu. Należy jednak pamiętać, że cyberprzestępcy często próbują zlokalizować i zaszyfrować lub usunąć archiwa kopii zapasowych oraz wyłączyć środki tworzenia kopii zapasowych i zabezpieczeń. Stosują także operacje i narzędzia ofiary do tworzenia kopii zapasowych w celu kradzieży danych i rozprzestrzenienia ataku w sieci. Dlatego konieczne jest przechowywanie wielu kopii zapasowych, najlepiej zaszyfrowanych, na różnych nośnikach i w różnych lokalizacjach: poza siedzibą firmy, offline i w chmurze. Przeprowadzaj regularne testy planu tworzenia kopii zapasowych, aby zweryfikować integralność archiwów i procesów oraz upewnić się, że możesz szybko przywrócić dane, aby osiągnąć cele firmy w zakresie czasu odzyskiwania. Pamiętaj także, aby przeskanować kopie zapasowe w poszukiwaniu złośliwego oprogramowania i niezałatanych luk w zabezpieczeniach oraz naprawić te problemy przed przywróceniem systemów i ponownym wprowadzaniem ich do działania.

Etap jedenasty **Weź pod uwagę wdrożenie programu do odzyskiwania po awarii.** Proces oczyszczania i odzyskiwania po ataku ransomware, w tym przywracanie dużych ilości danych z kopii zapasowej, może opóźnić wznowienie normalnej działalności biznesowej o wiele dni lub tygodni. Możliwość natychmiastowego wznowienia działania przez przełączenie na zreplikowane aplikacje i dane (zarówno poza siedzibą firmy, jak i w chmurze) jest cennym zabezpieczeniem przed takimi przedłużającymi się przestojami. Wraz z udostępnieniem odzyskiwania po awarii jako usługi, takie sytuacje awaryjne stały się znacznie tańsze i łatwiejsze do zarządzania, nawet dla mniejszych firm.

Etap dwunasty **Utwórz plan reagowania na incydenty i regularnie go testuj oraz aktualizuj.** Sporządź listę nazwisk i numerów kluczowych kontaktów wewnętrznych i zewnętrznych w formie papierowej, ponieważ atak ransomware może uniemożliwić dostęp do danych online. Zidentyfikuj i przetestuj awaryjny kanał komunikacji wewnętrznej (np. komunikator na smartfonie lub przez aplikację społecznościową) na wypadek, gdyby zwykłe systemy przestały działać. Przygotuj strategię komunikacji, która określi, którzy odbiorcy powinni zostać poinformowani i przez kogo, w oparciu o wagę i etap ataku: operacje i zarządzanie IT i bezpieczeństwem; kadra wykonawcza; zespoły prawne i ds. zgodności; partnerzy i klienci; prasa i opinia publiczna; organy regulacyjne; bankierzy i inwestorzy itp. Regularnie testuj plan podczas ćwiczeń z zespołem online i na żywo. Zbieraj dane kryminalistyczne po ataku, używaj ich do identyfikowania i usuwania luk w zabezpieczeniach, które umożliwiły naruszenie, oraz odpowiednio aktualizuj plan reagowania.

Podsumowanie

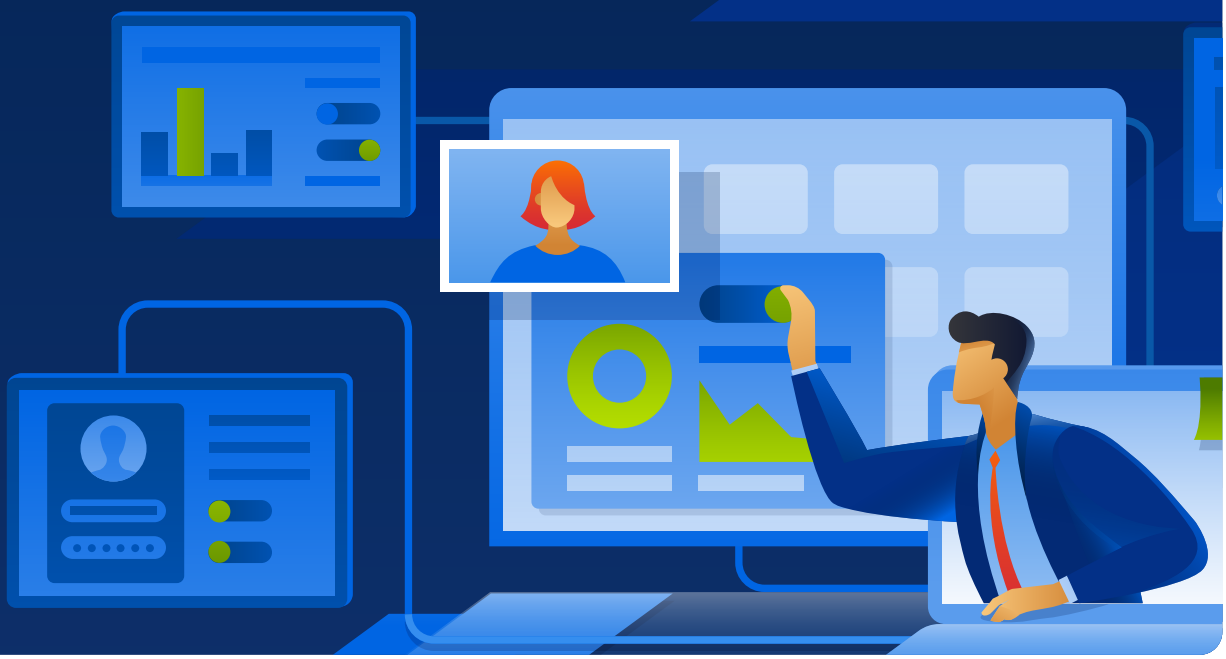
Każda firma, która chce zmniejszyć ryzyko związane z rosnącym zagrożeniem atakiem ransomware musi agresywnie podejść do obrony, ale także przygotować plan działań na wypadek udanego ataku. Aby przeciwdziałać zagrożeniom ransomware, które stają się coraz częstsze i coraz bardziej wyrafinowane, firmy muszą tworzyć plany obrony i łagodzenia skutków w oparciu o procesy i technologie, które zmniejszają ogólną złożoność i wzmacniają personel IT za pomocą sztucznej inteligencji, automatyzacji i integracji.

Zasoby

Raport Acronis na temat cyberzagrożeń: druga połowa 2022 r.
https://www.acronis.com/pl-pl/resource-center/resource/726/

Globalny krajobraz cyberochrony w 2022 r.: główne trendy i luki
https://www.acronis.com/pl-pl/resource-center/resource/721/

Acronis Cyber Protect
https://www.acronis.com/pl-pl/products/cyber-protect/



Acronis

Dowiedz się więcej na
www.acronis.com