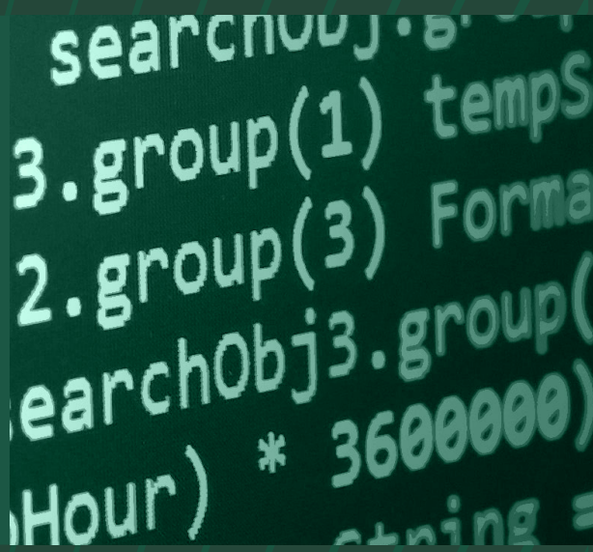
DELL Technologies

5 Zalecenia dotyczące przetrwania ataku ransomware



1	2	3	4	5
Opracuj kompleksowy plan reagowania na incydenty	**Przygotuj jasną strategię komunikacji**	**Zadbaj o solidną ochronę danych**	**Nie zakładaj natychmiastowego powrotu do normalności**	**Kładź nacisk na szkolenia i edukację**
Skup się na minimalizacji skutków ataku	Twórz z wyprzedzeniem szablony komunikacyjne	Chroń najważniejsze dane w niezmiennym i odizolowanym magazynie danych	Zapłacenie okupu powinno być ostatecznością	Przeprowadzaj symulacje ataków
Często ćwicz, testuj i aktualizuj	Zadbaj o terminową i przejrzystą komunikację wewnątrz organizacji	Ustalaj priorytety przywracania według usługi/infrastruktury	Zapewnij zgodność z wymaganiami prawnymi i regulacyjnymi przed dokonaniem płatności	Monitoruj i testuj praktyki pracowników w zakresie bezpieczeństwa i higieny pracy
Przygotuj zespół ds. reagowania z wyprzedzeniem na incydenty	Przygotuj się na komunikację zewnętrzną, jeśli Cię dotyczy	Przećwicz możliwość przywrócenia	Nie ma gwarancji, że haker zwróci Twoje dane, nawet po zapłaceniu okupu	Korzystaj z narzędzi takich jak testy phishingowe i szkolenia z zakresu bezpieczeństwa poczty e-mail
Rozważ ubezpieczenie cybernetyczne jako część swojej ogólnej strategii odporności	Przestrzegaj obowiązujących regulacji dotyczących powiadomień	Łącz możliwości, takie jak pomieszczenie czyste, z docelowym czasem odzyskiwania		
Uwzględnij plany współpracy z organami ścigania		Zapewnij integralność danych możliwych do przywrócenia		

To już nie jest kwestia „czy”, ale „kiedy”.

Przedsiębiorstwa muszą planować tak, jakby atak był nieunikniony, pomimo najlepszych środków obrony. Aby omówić działania na wypadek katastrofy, eksperci merytoryczni firmy Dell: Jim Shook, dyrektor globalny ds. cyberbezpieczeństwa i zgodności z przepisami, oraz Steven Granat, główny konsultant ds. rozwiązań w zakresie cyberbezpieczeństwa i partnerstw strategicznych, spotkali się z Brianem Whitem, starszym konsultantem ds. marketingu produktów w firmie Dell Data Protection.

> Trzeba zaangażować odpowiednich ludzi, przeprowadzić ćwiczenia i symulować działania, aby w przypadku ataku wszyscy od razu wiedzieli, co mają robić.
>
> ***Steven Granat**, główny konsultant, rozwiązania w zakresie cyberbezpieczeństwa i partnerstwa strategiczne, Dell Technologies*

Opracuj kompleksowy plan reagowania na incydenty

Kiedy dochodzi do ataku, wszyscy kluczowi interesariusze — prawie wszyscy w organizacji, a także podmioty zewnętrzne, takie jak dostawcy — muszą wiedzieć, co robić. Shook radzi, aby pisemny plan reagowania na incydenty nakreślał jasną sekwencję działań. Kompleksowy plan ma obejmować etapy technologiczne, procesowe i komunikacyjne, od natychmiastowego działania aż po przywrócenie sprawności. Pamiętaj, aby przechowywać również pisemny dokument papierowy, ponieważ cyfrowe sposoby komunikacji mogą nie działać. „Potrzebny jest plan, który można dosłownie ściągnąć z półki” — mówi Granat.

Miej jasną strategię komunikacji

Większość organizacji będzie musiała komunikować się z kluczowymi interesariuszami, a w wielu przypadkach będzie musiała stosować się do wymagań prawnych. Twórz różne szablony zarówno dla komunikacji wewnętrznej, jak i zewnętrznej z systematycznymi instrukcjami kogo powiadamiać, w jakiej kolejności i kiedy. Planuj na wypadek awarii telefonów i poczty e-mail.

Wdroż solidną strategię ochrony danych

Kluczowym celem przetrwania ataku ransomware jest przywrócenie danych i odzyskanie ich możliwie najbardziej bezboleśnie, przy jednoczesnym uniknięciu płacenia okupu. Solidna strategia ochrony danych jest kluczowym elementem osiągnięcia tych celów, ale musi obejmować zarówno technologie, jak i procesy. „Korzystaj z niezmiennych danych i cybermagazynów, aby przechowywać wystarczającą ilość danych, którym możesz zaufać, lub przynajmniej jako punkty walidacji, które umożliwią przywrócenie sprawności systemów” — radzi Shook. Zapewnienie ochrony danych to pierwszy krok; musisz również mieć ludzi i procesy, aby je odzyskać. Eksperci zewnętrzni mogą pomóc, ale powinni być zaangażowani na etapie planowania.

Nie zakładaj natychmiastowego powrotu do normalności — nawet jeśli zapłacisz okup

Zapłata okupu, którą należy rozważać tylko w ostateczności, nie gwarantuje, że przełącznik zostanie natychmiast ponownie włączony. Pamiętaj, że negocjujesz z przestępcą, a nawet jeśli zdobędziesz klucze do dekodera, potrzebujesz strategii dla nowo odzyskanych danych. Na początek musisz przetestować odszyfrowane dane i metodycznie odbudować wszystkie systemy. Przypominanie o zwróceniu uwagi na zdarzenia typu „co by było, gdyby”, zanim jeszcze dojdzie do ataku, znacznie przyczyni się do osiągnięcia odporności. „Zrozumienie różnych zastosowań i zależności w infrastrukturze technologicznej ma kluczowe znaczenie dla skutecznego powrotu do stanu ustalonego. „Czy mam realne źródło przywracania sprawności i cel możliwy do przywrócenia?” „Czy dysponuję danymi, które są wolne od zagrożeń?” Są to ważne kwestie, które należy wziąć pod uwagę” — mówi Granat.

W fazie przywracania musisz również dopilnować, aby przestępca faktycznie opuścił Twoje systemy. „Musisz wiedzieć, że w twoim domu wybuchł pożar, a także zorientować się, co go spowodowało, ponieważ bez tych dwóch istotnych informacji narażasz się na ataki w przyszłości” — mówi Shook.

Szkolenie i praktyka mają kluczowe znaczenie

Ważnym elementem cyberodporności jest kompleksowe przeszkolenie, które obejmuje zarówno dopilnowanie, aby pracownicy przestrzegali zasad higieny cyberbezpieczeństwa, jak i rutynowe stosowanie planu przywracania. „Trzeba zaangażować odpowiednich ludzi, przeprowadzić ćwiczenia i symulować działania, aby w przypadku ataku wszyscy od razu wiedzieli, co mają robić” — mówi Shook.

Ataki ransomware mogą być nieuniknione w dzisiejszym krajobrazie zagrożeń, ale poprzez planowanie i realizację można minimalizować ich konsekwencje operacyjne, finansowe i reputacyjne. Celem jest jak najszybszy i bezbolesny powrót do normalności.

Więcej informacji o tym, jak radzić sobie z największymi wyzwaniami związanymi z cyberbezpieczeństwem, znajdziesz na stronie **dell.com/cybersecuritymonth**

DELL Technologies