Acronis

Lista kontrolna wprowadzania ochrony cybernetycznej dla dostawców usług zarządzanych

Lista kontrolna ochrony cybernetycznej

Starsze technologie ochrony nie zapewniają integracji. Liczba zagrożeń cybernetycznych rośnie. Coraz częściej dochodzi do naruszeń bezpieczeństwa, które obejmują coraz większą liczbę urządzeń.

Jeśli chodzi o przestępstwa cybernetyczne, współczesne małe i średnie przedsiębiorstwa (MŚP) są łatwym celem. Ich budżet i personel są ograniczone, a znalezienie pracowników o odpowiednich umiejętnościach stanowi spore wyzwanie. Wiele firm decyduje się na wybór dostawcy usług zarządzanych w celu zarządzania ich procesami IT oraz zapewnienia bezpieczeństwa systemów i zasobów.

Jednak krajobraz zagrożeń cybernetycznych nieustannie się zmienia, co oznacza, że wiele MŚP ma problemy, aby nadążyć za nowymi zagrożeniami. W rzeczywistości cyberprzestępcy skutecznie zaatakowali już platformy, które stosują dostawcy usług do prowadzenia swojej działalności, aby zdobyć dostęp do danych MŚP oraz ich klientów.[1]

Kopie zapasowe i strategia odzyskiwania danych już nie wystarczą, aby zapewnić bezpieczeństwo danych.[2] Celem nowych odmian ransomware jest usuwanie plików kopii zapasowych, agentów i oprogramowania do ochrony. Kopie zapasowe bez zintegrowanych funkcji ochrony cybernetycznej nie są odpowiednim rozwiązaniem.

Nowe podejście

Potrzebne jest nowe podejście – takie, które skutecznie integruje ochronę cybernetyczną, ochronę danych i zarządzanie ochroną punktów końcowych. Integracja umożliwia ścisłą kontrolę oraz powiązaną automatyzację, których brakuje starszym rozwiązaniom, ale które są konieczne do pokonania współczesnych zagrożeń.

I chociaż istnieje wiele ram cyberbezpieczeństwa, takich jak NIST, COBIT i CIS, które zapewniają standardy branżowe i najlepsze praktyki dla organizacji w zakresie zarządzania ryzykiem bezpieczeństwa cybernetycznego, są one skomplikowane.

Integrując ochronę cybernetyczną i ochronę danych – **dyscyplinę IT obejmującą cyberbezpieczeństwo**[3] według IDC – organizacje mogą stać się bardziej odporne na zagrożenia.

Cyberbezbepieczeństwo integruje kopie zapasowe, odzyskiwanie danych po awarii, ochronę przed złośliwym oprogramowaniem opartą na sztucznej inteligencji, zdalną pomoc i ochronę cybernetyczną w jedno, szybkie, skuteczne i niezawodne narzędzie. Dzięki pięciu poniższym etapom możesz proaktywnie chronić dane przed współczesnymi zaawansowanymi zagrożeniami.

- **Zapobieganie** – proaktywnie chroń swoje dane, systemy i aplikacje przez zapobieganie atakom.
- **Wykrywanie** – wykrywaj problemy i zagrożenia, zanim zaczną stanowić zagrożenie dla jakiegokolwiek środowiska.
- **Reagowanie** – zezwól na szybkie działanie, aby zminimalizować ryzyko.
- **Odzyskiwanie** – szybko i bezpiecznie odzyskuj dane ze znanych, dokładnych kopii zapasowych, na wypadek, gdyby zostały naruszone.
- **Kryminalistyka** – ogranicz przyszłe ryzyko, gromadząc dane i wykonując dochodzenia kryminalistyczne.

Za pomocą tej listy kontrolnej możesz rozpocząć planowanie i porównywanie swojego poziomu ochrony cybernetycznej oraz z większym prawdopodobieństwem ograniczyć ryzyko.

> „Dodawanie zabezpieczeń do systemu informatycznego po jego utworzeniu prowadzi do problemów, których rozwiązywanie jest często bardziej kosztowne, niż gdyby zabezpieczenia te zostały włączone do procesu rozwoju od samego początku”. [4]
>
> **Tanner Johnson**
> **Starszy analityk ds. łączności i IoT,**
> **Omdia, Informa PLC**
>
> Pomagamy łączyć wszystkie części ekosystemu technologicznego w całość

ZAPOBIEGANIE

Proaktywna ochrona danych, systemów i aplikacji przez zapobieganie atakom.

	Element	Obecny status	Plan poprawy
1	**Oceny podatności na zagrożenia** W celu naprawy lub złagodzenia potencjalnego ryzyka, systematycznej oceny luk w zabezpieczeniach systemów informatycznych.		
2	**Zarządzanie poprawkami** Naprawa znanych luk ogranicza ryzyko narażenia organizacji na niebezpieczeństwo. Cofanie zmian wprowadzonych w ramach zarządzania poprawkami jest ograniczone i może być powolne. Tworzenie kopii zapasowej obrazu wybranych urządzeń przed zainstalowaniem systemu lub poprawki aplikacji.		
3	**Zapobieganie utracie danych (DLP)** Monitorowanie i blokowanie poufnych danych podczas używania i w spoczynku zapobiegnie potencjalnym naruszeniom danych i transmisji danych do szkodliwych podmiotów zewnętrznych.		
4	**Szkolenie w zakresie wiedzy o bezpieczeństwie** O bezpieczeństwie danych korporacyjnych często decyduje stopień przygotowania pracowników do cyberataków oraz przestrzegania przez nich wewnętrznych procesów z nastawieniem na bezpieczeństwo.		
5	**Ochrona narzędzi do pracy własnej i współpracy (Zoom, Webex, Teams)** Reguły samoobrony i wzmacniania dla określonych aplikacji pomagają rozszerzyć ochronę na wszystkie krytyczne aplikacje, zwłaszcza te zdalne.		

Czy Twoje rozwiązania do ochrony punktów końcowych proaktywnie skanują kopie zapasowe w poszukiwaniu wirusów, luk w zabezpieczeniach i poprawek w celu zapobiegania powtórnym infekcjom?

WYKRYWANIE

Wykrywaj problemy i zagrożenia, zanim zaczną stanowić zagrożenie dla jakiegokolwiek środowiska.

	Element	Obecny status	Plan poprawy
1	**Ochrona przed wirusami i złośliwym oprogramowaniem** Połączenie wykrywania opartego na sztucznej inteligencji i zachowaniu będzie chronić przed naruszeniami tradycyjnymi i nowej generacji, takimi jak ataki typu „zero day”.		
2	**Ochrona przed phishingiem** Gdy użytkownicy końcowi nie rozpoznają wiadomości phishingowej, środki bezpieczeństwa mogą uniemożliwić lub zablokować próby phishingu przed przedostaniem się do systemu poczty e-mail organizacji lub przed skuteczną kradzieżą informacji od użytkownika.		
3	**Filtrowanie adresów URL** Kontroluj dostęp do Internetu, zezwalając na dostęp lub zabraniając dostępu do określonych stron internetowych na podstawie informacji zawartych w liście kategorii URL.		
4	**Wykrywanie oparte na IoC** Sprawdzanie na znanej liście atrybutów naruszenia bezpieczeństwa, jeśli dowody na komputerze lub sieci wskazują, że bezpieczeństwo sieci zostało naruszone.		
5	**Wykrywanie i reakcja punktów końcowych (EDR)** EDR łączy stałe monitorowanie w czasie rzeczywistym i gromadzenie danych punktów końcowych (sprzęt komputerowy) z automatycznymi reakcjami i możliwościami analizy opartymi na regułach.		

Czy Twój stos bezpieczeństwa cybernetycznego obejmuje automatyczne generowanie list dozwolonych elementów z kopii zapasowych?

REAGOWANIE

Zezwól na szybkie działanie, aby zminimalizować ryzyko.

	Element	Obecny status	Plan poprawy
1	**Blokowanie uruchomienia złośliwego oprogramowania** Chroń użytkowników przed nieumyślnym uruchomieniem złośliwych plików i plików skryptów, w tym przed atakami bezplikowymi, które nie zapisują plików na dysku.		
2	**Izolacja urządzeń** Po wykryciu naruszenia zapobiegaj dostępowi przez urządzenia podłączone do sieci do innych zasobów podłączonych do tej samej lub innych sieci.		
3	**Reagowanie na incydenty** Szybkość i skuteczność, z jaką organizacja reaguje na naruszenia bezpieczeństwa danych będzie mieć wpływ na ewentualne szkody finansowe i utratę reputacji, z którymi będzie musiała się zmierzyć.		
4	**Powiadomienia i ostrzeżenia** Dostarczają aktualnych informacji o bieżących problemach z zabezpieczeniami, lukach i zagrożeniach.		
5	**Ochrona sieci** Scentralizowane zarządzanie infrastrukturą ochrony sieci umożliwi wgląd w ruch sieciowy i zagrożenia w celu zabezpieczenia dostępu, ochrony użytkowników i aplikacji oraz kontroli danych z dowolnego miejsca.		

Czy Twój obecny stos automatycznie dostosowuje poziomy zabezpieczeń i rozpoczyna tworzenie kopii zapasowych na podstawie powiadomień dotyczących ochrony?

ODZYSKIWANIE DANYCH

Szybko i bezpiecznie odzyskuj dane ze znanych, dokładnych kopii zapasowych, na wypadek, gdyby zostały naruszone.

	Element	Obecny status	Plan poprawy
1	**Usuwanie złośliwego oprogramowania z kopii zapasowych** Skanowanie kopii zapasowych całego dysku w scentralizowanej lokalizacji pomaga znaleźć potencjalne luki w zabezpieczeniach i infekcje złośliwym oprogramowaniem, zapewniając użytkownikom możliwość przywrócenia kopii zapasowej wolnej od złośliwego oprogramowania.		
2	**Natychmiastowe odzyskiwanie danych „w miejscu”** Natychmiastowe odzyskiwanie umożliwia tymczasowe uruchomienie obrazu kopii zapasowej jako maszyny wirtualnej (VM) w dodatkowej pamięci masowej po wystąpieniu awarii lub katastrofy.		
3	**Bezpieczne odzyskiwanie danych** Wprowadzanie poprawek do urządzenia i stosowanie najnowszych definicji oprogramowania chroniącego przed złośliwym oprogramowaniem umożliwia użytkownikom przywrócenie obrazu systemu operacyjnego z najnowszymi poprawkami, zmniejszając ryzyko ponownego wystąpienia infekcji.		
4	**Automatyzacja** Możliwość skonfigurowania wszystkich obszarów automatycznie – na poziomie procesu, aplikacji lub infrastruktury – ogranicza zależności od działań manualnych.		
5	**Archiwizacja i odzyskiwanie e-maili** Zachowywanie lub odzyskiwanie wiadomości e-mail o znaczeniu krytycznym dla firmy.		

Czy masz pewność, że możliwe będzie odzyskanie dane z czystych kopii zapasowych?

KRYMINALISTYKA

Ogranicz przyszłe ryzyko, gromadząc dane i wykonując dochodzenia kryminalistyczne.

	Element	Obecny status	Plan poprawy
1	**Pełne kopie zapasowe danych** Przechwytuj wszystkie dane z urządzeń źródłowych (komputerów, telefonów komórkowych, tabletów itp.) za pomocą metod kryminalistycznych, aby wszystkie oryginalne dane pozostały w niezmienionym stanie.		
2	**Dane kryminalistyczne w kopiach zapasowych** Przechwytuj obraz pamięci zawierający stan wszystkich uruchomionych procesów wraz z kopią zapasową.		
3	**EDR** Wykonaj analizę przyczyn źródłowych w celu zidentyfikowania źródła zagrożenia i ścieżki infekcji.		

Czy Twój system kryminalistyczny ma dostęp do kopii zapasowych w celu ułatwienia analizy reagowania na incydenty?

Źródła

[1] Cybersecurity for SMBs Is the Herculean Task of MSPs, Dark Reading, November 2020

[2] Ransomware protection means more than a simple backup, Omdia, March 2021

[3] Addressing Cyber Protection and Data Protection Holistically, IDC, April 2020

[4] Data Security Strategies Are at the Heart of Cybersecurity, Omdia, Tanner Johnson, October 2020