DELL Technologies

Większe cyberbezpieczeństwo i większa zgodność z modelem „zero trust”

Nie pozwól, by zagrożenia bezpieczeństwa stłumiły innowacje

Poznaj stan swojego cyberbezpieczeństwa

Poznaj stan, jaki musi osiągnąć

W dzisiejszym złożonym i szybko zmieniającym się krajobrazie zagrożeń organizacje często napotykają ograniczenia zasobów i wiedzy, jeśli chodzi o utrzymanie solidnych praktyk w zakresie cyberbezpieczeństwa. Aby walczyć ze zmieniającymi się zagrożeniami cybernetycznymi w celu zapewnienia bezpieczeństwa środowiska, a jednocześnie nie hamować innowacji, należy poprawić cyberbezpieczeństwo i przygotować się do przyjęcia modelu „zero trust”.

Skorzystaj z tych list kontrolnych, aby ocenić bieżący stan dojrzałości cyberbezpieczeństwa. Znajomość mocnych i słabych stron organizacji umożliwia podjęcie właściwych kolejnych kroków w celu zwiększenia dojrzałości cyberbezpieczeństwa.

Spis treści

Więcej informacji

Dowiedz się więcej na temat poprawy cyberbezpieczeństwa i przygotowania do modelu „zero trust”

Lista:

Zmniejszenie obszaru narażonego na ataki

Obszar narażony na ataki obejmuje wszystkie możliwe punkty lub obszary w środowisku, które mogą zostać zaatakowane lub wykorzystane przez cyberprzestępcę. Punkty te mogą obejmować luki w oprogramowaniu, błędne konfiguracje, słabe mechanizmy uwierzytelniania, systemy bez poprawek, nadmierne uprawnienia użytkowników, otwarte porty sieciowe, niedostateczne zabezpieczenia fizyczne i inne. Poniższe pytania mogą pomóc w określeniu, w jaki sposób można zminimalizować luki w zabezpieczeniach i punkty wejścia, które złośliwy podmiot może naruszyć.

Tak	Nie	
☐	☐	Czy Twoja organizacja przeprowadza regularne oceny, testy penetracyjne lub symulacje ataków naruszających w celu zidentyfikowania luk i słabych punktów systemów i sieci, co pozwala na terminowe działania zaradcze i ulepszenia?
☐	☐	Czy Twoja organizacja przeprowadza regularne szkolenia w zakresie bezpieczeństwa dla swoich pracowników?
☐	☐	Czy Twoja organizacja korzysta z uwierzytelniania wieloskładnikowego (MFA) i kontroli dostępu opartej na rolach (RBAC)?
☐	☐	Czy Twoja organizacja wdrożyła segmentację sieci w celu odizolowania krytycznych zasobów i ograniczenia dostępu między różnymi częściami sieci?
☐	☐	Czy Twoja organizacja wdraża bezpieczne praktyki kodowania, przeprowadza regularne testy zabezpieczeń i przeglądy kodu oraz używa zapór aplikacji internetowych (WAF) w celu ochrony przed typowymi atakami na poziomie aplikacji i zmniejszenia obszaru narażonego na ataki aplikacji internetowych?
☐	☐	Czy Twoja organizacja wybiera dostawców IT, którzy mogą potwierdzić procesy i procedury mające na celu zabezpieczenie łańcucha dostaw?
☐	☐	Czy Twoja organizacja wdraża zasady „zero trust' w celu zastąpienia tradycyjnych zabezpieczeń obwodowych?
☐	☐	Czy Twoja organizacja korzysta z zasady najniższych uprawnień, aby ograniczyć konta użytkowników i konta systemowe do posiadania tylko minimalnych praw dostępu wymaganych do wykonywania zadań?
☐	☐	Czy Twoja organizacja regularnie instaluje poprawki systemów i oprogramowania?
☐	☐	Czy narzędzia bezpieczeństwa Twojej organizacji wykorzystują możliwości sztucznej inteligencji / uczenia maszynowego, aby pomóc w proaktywnym identyfikowaniu luk w zabezpieczeniach?

Lista:

Wykrywanie zagrożeń i reagowanie na nie

Wykrywanie zagrożeń cybernetycznych i reagowanie na nie jest niezbędnym elementem każdej strategii bezpieczeństwa. Obejmuje monitorowanie i analizowanie ruchu sieciowego, dzienników systemowych i innych obszarów, a także danych dotyczących bezpieczeństwa w celu identyfikowania oznak nieautoryzowanego dostępu, włamań, zainfekowania złośliwym oprogramowaniem, naruszenia bezpieczeństwa danych lub innych zagrożeń cybernetycznych. Te pytania mogą pomóc w określeniu, w jaki sposób organizacja proaktywnie identyfikuje i aktywnie reaguje na potencjalne incydenty zabezpieczeń oraz złośliwe działania w sieci komputerowej, systemie lub organizacji.

Tak	Nie	
☐	☐	Czy Twoja organizacja stale monitoruje działania sieciowe i systemowe przy użyciu narzędzi oraz technologii bezpieczeństwa, takich jak rozszerzone wykrywanie zagrożeń i reagowanie na nie (XDR), systemy wykrywania włamań (IDS), systemy zapobiegania włamaniom (IPS), SIEM i analiza dzienników?
☐	☐	Czy Twoja organizacja analizuje zebrane dane w celu zidentyfikowania wzorców, anomalii oraz wskaźników naruszenia bezpieczeństwa (IoC) i/lub wskaźników ataku (IOA), które mogą wskazywać na potencjalne zagrożenie cybernetyczne?
☐	☐	Czy Twoja organizacja wdrożyła najnowsze narzędzia do zwiększenia widoczności oraz monitorowania, aby szybko wykrywać potencjalne incydenty i otrzymywać o nich alerty?
☐	☐	Czy Twoja organizacja monitoruje ruch sieciowy pod kątem nietypowych wzorców lub podejrzanych działań, które mogą wskazywać na trwający cyberatak?
☐	☐	Czy Twoja organizacja wdrożyła jakiekolwiek narzędzia wykorzystujące sztuczną inteligencję / uczenie maszynowe, które pomagają wykrywać zagrożenia cybernetyczne poprzez analizę w czasie rzeczywistym nietypowych wzorców danych lub zachowań?
☐	☐	Czy Twoja organizacja rozważa wdrożenie rozwiązania SIEM nowej generacji w celu lepszego zarządzania powiadomieniami bezpieczeństwa i rozpoczęcia korelacji danych zdarzeń bezpieczeństwa z całego ekosystemu IT?
☐	☐	Czy Twoja organizacja stosuje testowanie luk w zabezpieczeniach i zarządzanie nimi, aby określać priorytety i usuwać istniejące luki w zabezpieczeniach, a także skutecznie reagować na nowe luki?
☐	☐	Czy Twoja organizacja ma plan reagowania na zdarzenia w celu badania potwierdzonych incydentów bezpieczeństwa i minimalizowania ich skutków?
☐	☐	Czy Twoja organizacja korzysta z narzędzi SOAR (Security Orchestration, Automation and Response) w celu przyspieszenia działań związanych z reagowaniem na incydenty, które mogą pomóc w ograniczeniu rozprzestrzeniania się cyberataku?
☐	☐	Czy plan reagowania na incydenty w organizacji uwzględnia zasady ograniczania rozprzestrzeniania się zagrożenia, plany komunikacji, wymagania dotyczące zgodności z przepisami, analizę kryminalistyczną i proces odzyskiwania?

Lista:

Powrót do normalności po cyberataku

Powrót do normalności po cyberataku to proces przywracania systemów, sieci i danych po naruszeniu zabezpieczeń do stanu bezpieczeństwa i działania. Obejmuje to podjęcie działań mających na celu złagodzenie szkód spowodowanych atakiem, odbudowę naruszonych lub zakłóconych usług i urządzeń, analizę incydentu w celu zapobieżenia przyszłym atakom i przywrócenie normalnego działania organizacji. Te pytania mogą pomóc w określeniu, czy Twoja organizacja skutecznie powraca do normalności po cyberatakach.

Tak	Nie	
☐	☐	Czy Twoja organizacja wdrożyła jakiekolwiek środki powstrzymywania incydentów w celu odizolowania i ograniczania rozprzestrzeniania się cyberataku?
☐	☐	Czy Twoja organizacja wdrożyła procesy przywracania systemu lub urządzeń po opanowaniu incydentu?
☐	☐	Czy Twoja organizacja wykorzystuje izolację, niezmienność lub cybermagazyn danych do ochrony swoich danych?
☐	☐	Czy Twoja organizacja wdrożyła procedury czystego odzyskiwania danych w przypadku ich naruszenia, zaszyfrowania lub usunięcia?
☐	☐	Czy Twoja organizacja wykorzystuje technologie sztucznej inteligencji / uczenia maszynowego do automatyzacji lub przyspieszenia powrotu do normalności po cyberataku?
☐	☐	Czy Twoja organizacja stale ocenia incydenty i identyfikuje obszary wymagające poprawy po ataku i powrocie do normalności?
☐	☐	Czy Twoja organizacja przeprowadziła analizę kryminalistyczną w celu zrozumienia metodologii ataku, określenia zasięgu naruszenia, zidentyfikowania systemów i danych, których dotyczy naruszenie, a także zebrania dowodów w celu zwiększenia bezpieczeństwa i podjęcia działań prawnych lub dyscyplinarnych?
☐	☐	Czy Twoja organizacja wie, że należy powiadamiać o cyberataku oraz potencjalnym wpływie na dane lub operacje odpowiednie strony, takie jak klienci, partnerzy i dostawcy?
☐	☐	Czy Twoja organizacja ćwiczy wiele razy w roku strategie powrotu do normalności, aby zyskać pewność przywrócenia działalności i spełnienia wymogów umów SLA?
☐	☐	Czy Twoja organizacja współpracuje z usługodawcami pomagającymi w powrocie do normalności?

Zaawansowane cyberbezpieczeństwo i model „zero trust”

Gdy chodzi o cyberbezpieczeństwo, organizacje IT muszą przygotować się na najgorszy możliwy scenariusz i korzystać z wielu warstw obrony. W nieustannie zmieniającym się krajobrazie zagrożeń cyberbezpieczeństwa kluczowe znaczenie ma ciągłe doskonalenie praktyk bezpieczeństwa i stosowanie zasad modelu „zero trust”. Obejmuje to:

Zmniejszenie obszaru narażonego na ataki

Zminimalizuj luki w zabezpieczeniach i podatne obszary, które mogą zostać wykorzystane do naruszenia bezpieczeństwa systemu.

Wykrywanie zagrożeń cybernetycznych i reagowanie na nie

Aktywnie identyfikuj i reaguj na potencjalne incydenty bezpieczeństwa i złośliwe działania.

Powrót do normalności po cyberatakach

Przywróć wcześniejszy stan operacyjny organizacji po incydencie bezpieczeństwa.

Wykorzystując wiedzę specjalistyczną w zakresie profesjonalnych usług i współpracując z zaufanymi partnerami handlowymi, firma Dell może pomóc organizacjom w ustanowieniu kompleksowego stanu bezpieczeństwa, który chroni przed zmieniającymi się zagrożeniami cybernetycznymi. Technologia stale się rozwija, więc nasze podejście do cyberbezpieczeństwa musi również ewoluować, abyśmy mogli chronić naszą infrastrukturę cyfrową i utrzymać zaufanie do świata cyfrowego.

DELL Technologies

Informacje o firmie Dell Technologies

Firma Dell Technologies pomaga klientom w rozwijaniu nowoczesnego środowiska cyfrowego oraz przekształcaniu sposobu pracy, stylu życia i korzystania z rozrywki. Firma zapewnia klientom najszersze i najbardziej innowacyjne w branży portfolio technologii i usług w erze danych.

Więcej informacji na ten temat można znaleźć na stronie www.dell.com/securitysolutions