DELL Technologies

Podręcznik przetrwania w cyberprzestrzeni:

Jak reagować na współczesne zagrożenia cybernetyczne

Świat cyfrowy stał się niebezpiecznym miejscem, gdzie każde kliknięcie, pobranie lub zalogowanie może spowodować cybernetyczną pułapkę.

Dzisiejszy krajobraz cybernetyczny jest bardziej niebezpieczny niż kiedykolwiek, a zagrożenia takie jak ransomware, ataki DDoS, oszustwa phishingowe i infiltracja kopii zapasowych stają się coraz bardziej zaawansowane. Hakerzy wykorzystują teraz sztuczną inteligencję do przechytrzenia tradycyjnych zabezpieczeń, przekształcając to, co kiedyś było oportunistycznymi atakami, w obliczone i trwałe zagrożenia, które mogą powodować rozległe szkody.

Klienci firmy Dell zgłaszali alarmujące ataki oparte na sztucznej inteligencji, w których hakerzy wykorzystują media społecznościowe, aby tworzyć przekonujące wiadomości, które mogą oszukać nawet najbardziej świadomych cybernetycznie pracowników.

Takie historie są wyraźnym przypomnieniem o tym, w jaki sposób atakujący wykorzystują zaawansowane technologie do manipulowania, oszukiwania i infiltrowania organizacji z niespotykaną dokładnością.

Aby poruszać się po tym nieprzyjaznym środowisku, organizacje potrzebują kompleksowej strategii cyberbezpieczeństwa — zestawu do przetrwania, który łączy najnowocześniejsze narzędzia, proaktywne strategie i kulturę czujności. Ten przewodnik przedstawia elementy takiej strategii pomagającej organizacjom budować odporność na współczesne zagrożenia cybernetyczne.

Mapa ochrony organizacji: Model „zero trust”

W dzisiejszym świecie zagrożeń opartych na sztucznej inteligencji wdrożenie modelu „zero trust” nie jest już opcjonalne. Atakujący wykorzystują sztuczną inteligencję do automatyzacji rozpoznania, kradzieży danych uwierzytelniających i szybkiego dostosowywania swoich technik, przez co tradycyjne zabezpieczenia są mniej skuteczne. Model „zero trust” działa w oparciu o „założenie naruszenia”, stale weryfikując każdą prośbę o dostęp i wdrażając ścisłe procesy uwierzytelniania w celu zminimalizowania ryzyka.

Dzięki proaktywnemu monitorowaniu użytkowników, urządzeń i aplikacji model „zero trust” zmniejsza ryzyko nieautoryzowanego dostępu i wycieku danych. To nowoczesne, ujednolicone podejście do zarządzania tożsamością.

Zadbaj o wspólne bezpieczeństwo: zmniejsz powierzchnię ataku

Ograniczenie powierzchni ataku jest kluczowe w obronie przed zagrożeniami wspieranymi przez sztuczną inteligencję, ponieważ punkty końcowe, interfejsy API oraz luki w łańcuchu dostaw są często wykorzystywane przez cyberprzestępców. Punkty końcowe i interfejsy API służą jako punkty wejścia do sieci i są często wykorzystywane do instalacji złośliwego oprogramowania lub kradzieży wrażliwych danych.

Zabezpieczenie tych obszarów wymaga warstwowej strategii obrony, w tym silnego uwierzytelniania, szyfrowanych danych w ruchu, regularnych testów luk w zabezpieczeniach, narzędzi do wykrywania punktów końcowych i reagowania (EDR), zarządzania poprawkami i wzmacniania urządzeń. Rozwiązania do monitorowania punktów końcowych oraz ciągłe wykrywanie zagrożeń pomagają identyfikować i blokować złośliwą aktywność w czasie rzeczywistym.

Organizacje muszą przyjąć proaktywne strategie w celu zabezpieczenia swoich łańcuchów dostaw oprogramowania i cyklu życia rozwoju. Egzekwowanie zasady najmniejszego uprawnienia daje pewność, że tylko autoryzowani użytkownicy i aplikacje mogą wchodzić w interakcje z krytycznymi systemami, a automatyczne wykrywanie i reagowanie na zagrożenia może szybko eliminować luki w zabezpieczeniach w miarę ich pojawiania się.

Zapoznaj się z doświadczonym narzędziem Wilderness Tracker: Proaktywne wykrywanie i reagowanie na zagrożenia

Ataki oparte na sztucznej inteligencji wykorzystują luki w zabezpieczeniach, naśladują prawidłowe zachowania i dynamicznie się dostosowują w celu omijania środków bezpieczeństwa, co utrudnia ich wykrycie. Aby przeciwdziałać tym zaawansowanym zagrożeniom, organizacje potrzebują więcej niż środków reaktywnych — wymagają zaawansowanych systemów wykrywania zagrożeń w połączeniu z funkcjami szybkiego reagowania. Wykorzystując sztuczną inteligencję i uczenie maszynowe, zespoły ds. bezpieczeństwa mogą analizować wzorce zachowań, wykrywać anomalie i reagować na zagrożenia w czasie rzeczywistym, rozwiązując problemy przed wystąpieniem poważnych strat.

Skuteczne systemy wykrywania i reagowania muszą pobierać ogromne ilości danych operacyjnych, aby wykrywać zagrożenia i wyzwalać automatyczne odpowiedzi. Ta analiza zagrożeń sama się również uczy, dzięki czemu system staje się coraz bardziej inteligentny i jest w stanie proaktywnie identyfikować i przeciwdziałać pojawiającym się taktykom przeciwników.

DELL Technologies

Praktyka budowy schronienia przed burzą: reagowanie na incydenty i odzyskiwanie danych

Chociaż zapobieganie atakom jest pierwszym krokiem, organizacje muszą działać tak, jakby atak był nieunikniony. Celem jest przetrwanie ataku przy minimalnych stratach, a skuteczna strategia obejmuje dwa elementy:

- Silny plan reagowania na incydenty i odzyskiwania (IRR).
- Pomiary technologiczne skupione wokół tworzenia kopii zapasowych krytycznych danych i aplikacji.

Plan odzyskiwania danych po incydentach powinien być kompleksowy. Ponieważ potężny atak prawdopodobnie zniszczy większość, jeśli nie wszystkie operacje firmy, plan powinien obejmować to, co każdy dział w firmie zrobiłby w przypadku incydentu cybernetycznego. Plan powinien również określać, w jaki sposób organizacja będzie komunikować się zarówno wewnątrz, jak i na zewnątrz, i zawierać gotowe do użycia szablony komunikacji. Plan musi być również regularnie aktualizowany i utrzymywany. Wreszcie plan jest tak dobry, jak często jest ćwiczony. Gdy atak nastąpi, każdy musi być instynktownie gotowy do działania.

Z punktu widzenia technologii organizacje powinny zacząć od określenia, jak wyglądają operacje **Minimum Viable Company (MVC)**: które systemy MUSZĄ pozostać operacyjne, nawet jeśli oznacza to konieczność pracy przy użyciu papieru i ołówka? Czy ważne jest, aby sprzedaż nadal działała? A co z obsługą klienta?

Po dokonaniu tych ustaleń należy wokół nich zbudować mechanizmy tworzenia kopii zapasowych i odzyskiwania danych. Możliwość powrotu do znanych dobrych danych nie tylko pozwala organizacji szybko wznowić operacje, ale także eliminuje złośliwe podmioty próbujące wykorzystać dane jako zakładnika. Ponadto nowoczesne strategie IR muszą wykraczać poza tradycyjne podejścia, traktując systemy sztucznej inteligencji/LM, takie jak chatboty i agenty wirtualne, jako zasoby poziomu 1 z takim samym priorytetem odzyskiwania jak systemy płatności czy dane klienta.

Aby zwalczać zaawansowane zagrożenia, plany IR powinny zrównoważyć automatyzację z kontrolami ręcznymi. Ważne jest, aby wiedzieć, jak organizacja będzie działać w przypadku całkowitej awarii systemu. Co się stanie, jeśli trzeba będzie wrócić do pióra i papieru?

Każdy musi się zaangażować: świadomość pracowników

Pracownicy są pierwszą linią obrony przed zagrożeniami cybernetycznymi, podobnie jak zespół ratunkowy, który porusza się po niebezpiecznych terenach. Każdy członek personelu odgrywa kluczową rolę w identyfikacji zagrożeń i ochronie zasobów. Aby wzmocnić tę ochronę, organizacje potrzebują solidnych programów świadomości, takich jak symulacje ataków, które obejmują zagrożenia właściwe dla sztucznej inteligencji, takie jak zaawansowany phishing i oszustwa typu deepfake.

Najlepsze programy łączą nieustanną edukację, otwartą komunikację, symulacje w świecie rzeczywistym i kulturę wspólnej odpowiedzialności. Kiedy wszyscy, od personelu pierwszej linii po kierownictwo, rozumieją zagrożenia zarówno tradycyjne, jak i oparte na sztucznej inteligencji, organizacja staje się czujnym, dobrze poinformowanym podmiotem. Poprzez promowanie pracy zespołowej i przygotowania organizacja może wyprzedzić zmieniające się zagrożenia cybernetyczne i zbudować odporny system obronny przed potencjalnymi atakami.

Najlepsze praktyki dotyczące utrzymywania odporności na ataki oparte na sztucznej inteligencji

Aby zachować odporność na ataki oparte na sztucznej inteligencji, organizacje muszą przyjąć proaktywne i strategiczne podejście. Oto 10 najlepszych praktyk:

Architektura „zero trust”

Wymagaj ciągłej weryfikacji, ścisłych kontroli dostępu i segmentacji sieci, aby zapewnić uwierzytelnienie każdego użytkownika i urządzenia przed udzieleniem dostępu — pomagając blokować i ograniczać szybko poruszające się, napędzane sztuczną inteligencją ataki.

Wzmacniaj zarządzanie tożsamością i dostępem:

Wdrażaj solidne uwierzytelnianie (MFA, RBAC) i egzekwuj silne zasady dotyczące poświadczeń, aby ograniczyć skuteczność phishingu i używania skradzionych poświadczeń.

Automatyczne wykrywanie i inwentaryzacja zasobów:

Stale wykrywaj i monitoruj wszystkie zasoby, w tym chmurę, IoT i zjawisko Shadow IT, aby uniknąć ukrytych ekspozycji.

Mikrosegmentacja i kontrola dostępu do sieci:

Segmentowanie oraz izolowanie sieci i obciążeń roboczych w celu zapobiegania ruchom osób atakujących i powstrzymywania zagrożeń.

Wzmocnienie punktów końcowych i interfejsu API:

Korzystaj z zaawansowanej ochrony punktów końcowych (EDR/XDR) i bezpiecznych bram API; silnego uwierzytelniania, ograniczania prędkości, weryfikacji danych wejściowych i szyfrowania.

Rygorystyczne zarządzanie lukami w zabezpieczeniach i poprawkami:

Zautomatyzuj skanowanie i szybkie poprawki systemu operacyjnego, oprogramowania wewnętrznego, aplikacji, interfejsów API i oprogramowania innych firm.

Wykrywanie zagrożeń oparte na sztucznej inteligencji i monitorowanie:

Wykorzystaj wykrywanie zachowań i anomalii oparte na sztucznej inteligencji/uczenia maszynowego, aby wykrywać subtelne lub zautomatyzowane zagrożenia w czasie rzeczywistym.

Zautomatyzowane reagowanie na incydenty:

Korzystaj ze zautomatyzowanych podręczników do szybkiego izolowania, ograniczania i usuwania zagrożeń, minimalizując czas obecności atakującego w systemie.

Regularne realistyczne symulacje i ciągłe doskonalenie:

Przeprowadzaj ćwiczenia scenariuszowe, testy typu red teaming oraz symulacje phishingowe; aktualizuj plany IR i modele wykrywania w oparciu o wyniki.

Niezmienne, odizolowane kopie zapasowe i odzyskiwanie:

Zachowaj odporne na manipulacje kopie zapasowe — najlepiej odizolowane i regularnie testowane — w celu zapewnienia czystego i szybkiego odzyskiwania danych.

DELL Technologies

Dell Technologies: Twój przewodnik po niezbadanych terytoriach

Ochrona organizacji przed zaawansowanymi zagrożeniami cybernetycznymi wymaga odpowiednich narzędzi i wiedzy eksperckiej, aby wyprzedzać zmieniające się zagrożenia. W dzisiejszym złożonym środowisku cyberbezpieczeństwa solidna strategia jest niezbędna do ochrony danych, systemów i reputacji. W tym miejscu wkracza firma Dell Technologies, oferując kompleksowy pakiet rozwiązań dostosowanych do potrzeb organizacji każdej wielkości.

Od bezpiecznego łańcucha dostaw, zaawansowanego wykrywania zagrożeń i ochrony punktów końcowych po bezpieczne zarządzanie danymi — firma Dell wyposaża Twoją firmę w technologię niezbędną do obrony przed nowoczesnymi cyberatakami. Zespół firmy Dell, wspierany przez czołową w branży wiedzę ekspercką, ściśle współpracuje z Tobą w celu opracowania niestandardowej strategii bezpieczeństwa. Dzięki funkcjom takim jak monitorowanie w czasie rzeczywistym, zautomatyzowane reagowanie na zagrożenia i architektura „zero trust", firma Dell pomaga organizować proaktywną i odporną organizację.

Niezależnie od tego, czy chodzi o ataki ransomware, ataki phishingowe, czy zgodność z przepisami, firma Dell Technologies pomoże Ci bezpiecznie poruszać się po dzisiejszym świecie zagrożeń. Współpracuj z firmą Dell, aby chronić swoją firmę i rozwijać się w erze cyfrowej, uzyskując bezpieczeństwo, wydajność i gotowość na przyszłość.

> Twój plan reagowania na incydenty musi być wydrukowany na papierze, ponieważ systemy mogą być podczas ataku niedostępne".
>
> ***Rachel Tyler***
> *Konsultant ds. cyberbezpieczeństwa, Dell Services*

Produkty i rozwiązania firmy Dell, które mogą pomóc

Polecane rozwiązanie firmy Dell	Opis
Dell Trusted Infrastructure	Połączenie serwerów Dell, rozwiązań sieciowych, pamięci masowej oraz systemów cyberodporności tworzy nowoczesną, bezpieczną i odporną podstawę dla innowacji.
Cyberodporność	Kompleksowa oferta rozwiązań zaprojektowanych z myślą o ochronie danych i zapewnieniu bezpiecznego odzyskiwania. Obejmuje urządzenia, oprogramowanie i oferty w formie usług.
Usługi w zakresie cyberbezpieczeństwa	Pakiet usług, które mogą pomóc w opracowaniu i wdrożeniu kompleksowej strategii bezpieczeństwa w zakresie obciążeń roboczych. Oferta obejmuje usługi doradcze, VCISO, zarządzane wykrywanie i reagowanie, testy penetracyjne i badanie luk w zabezpieczeniach oraz reagowanie na incydenty i odzyskiwanie danych.
Dell Trusted Workspace (zabezpieczenia punktów końcowych)	Połączenie wbudowanych i opcjonalnych funkcji dodatkowych zaprojektowanych z myślą o zabezpieczeniu komputerów komercyjnych. Wykorzystanie bezpiecznych praktyk łańcucha dostaw i wbudowanych funkcji takich jak SafeBIOS i SafeID z modułem TPM. Opcjonalne dodatki obejmują Secured Component Verification, SafeID with ControlVault oraz oprogramowanie partnerskie CrowdStrike i Absolute, które maksymalizują bezpieczeństwo przestrzeni roboczej.

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