Zabezpieczenia wielowarstwowe stały się proste

Cyberataki są coraz częstsze. Ciągle o nich słyszymy, prawda? Nie bez przyczyny. W samych Stanach Zjednoczonych publicznie ujawniono ponad 500 przypadków naruszenia ochrony danych. W roku 2016 — prawie dwa razy więcej niż rok wcześniej.[i] W lutym 2017 r. firma badawcza Opinium stwierdziła, że 78 procent decydentów IT ankietowanych w Stanach Zjednoczonych i Europie doświadczyło co najmniej jednego ataku typu ransomware na swoją organizację w ciągu ostatniego roku. Shadow Brokers, grupa hakerska, która ujawniła bezbronność wobec niesławnego już WannaCry, obiecała regularnie ujawniać podobne problemy za pomocą modelu „Wine of the Month Club". Niedawno po raz pierwszy publicznie ujawniono wypłatę okupu o wartości miliona dolarów.[ii] A program Petya pokazał, jak będzie wyglądać złośliwe oprogramowanie w przyszłości.

Jak zatrzymać ten pędzący pociąg? Bez aktywnej strategii bezpieczeństwa różnorodność i rozproszenie urządzeń jest kosztowne, a urządzenia — trudne do kontroli. Zespoły IT poświęcają zbyt dużo czasu na zarządzanie tymi urządzeniami. Do tego należy dodać poważny niedobór siły roboczej w dziedzinie bezpieczeństwa cybernetycznego, który zmusza firmy do optymalizacji personelu ochrony, a także do opracowania strategii bezpieczeństwa intensywnie wykorzystującej nowoczesne technologie,

upraszczającej zarządzanie i koncentrującej się na podstawach bezpieczeństwa, które stanowią potężne bariery dla ataków w realnym świecie — strategii mającej silną przewagę nad innymi rozwiązaniami.

Jeśli 93% naruszeń ochrony danych zagraża organizacjom w ciągu kilku minut [iii], po prostu nie można sobie pozwolić na pomyłkę, jeśli chodzi o zabezpieczenie organizacji.

Na początek — obsługa poprawek

Rzecz w tym, że dla wielu istniejących słabych punktów są już dostępne poprawki. W marcu 2017 r. wprowadzono poprawkę usuwającą podatność na WannaCry dla obsługiwanych systemów operacyjnych Microsoft (od tego czasu Microsoft opublikował poprawkę nawet dla starszych systemów operacyjnych). Wiele istniejących zagrożeń, takich jak to, pozostaje aktualnych, bo poprawki dotyczące bezpieczeństwa nigdy nie zostały zaimplementowane. W 2015 roku zespół Verizon RISK stwierdził, że wiele zagrożeń można prześledzić do 2007 r.[iv] A 10 najbardziej znanych zagrożeń? Stanowią 85 procent pomyślnych ataków.[v]

Jak śledzić, usuwać i zgłaszać wszystkie słabe punkty — bez przerywania działalności banku i wywoływania bólu głowy u pracowników działu IT? Najlepszym rozwiązaniem byłoby znalezienie prostego sposobu na badanie, ocenę, testowanie i stosowanie poprawek w całej organizacji. A ponieważ większość zagrożeń dotyczy oprogramowania innego niż systemy operacyjne, obsługa poprawek i aktualizacji systemów operacyjnych to za mało.

Warto oszczędzać czas i pieniądze oraz skupiać się na działalności biznesowej. W ciągu kilku minut można uruchomić narzędzia Ivanti i wykorzystać je do wykrywania, oceny i naprawy systemów Windows, MacOS, Linux i UNIX w Twojej firmie — automatycznie, w oparciu o zdefiniowane wcześniej zasady. Nasze narzędzia upraszczają obsługę poprawek w systemach fizycznych i wirtualnych. Można przeszukać stacje robocze i serwery działające w trybie online i offline pod kątem brakujących poprawek i zastosować te poprawki. Następnie można obsługiwać poprawki do dowolnego oprogramowania, od systemów operacyjnych i aplikacji do maszyn wirtualnych (VM), szablonów wirtualnych, a nawet hiperwizora ESXi głęboko zintegrowanego z VMware.

Ivanti oferuje również wtyczkę do programu Microsoft System Center Configuration Manager, która automatyzuje i upraszcza proces wykrywania i wdrażania poprawek do aplikacji innych producentów za pośrednictwem konsoli SCCM.

Zaawansowany stos interfejsów API dla naszych rozwiązań do obsługi poprawek integruje się z rozwiązaniami bezpieczeństwa, skanerami luk w zabezpieczeniach, narzędziami do zarządzania konfiguracją, takimi jak Chef i Puppet, oraz narzędziami do raportowania. Podczas przeprowadzania operacji związanych z poprawkami charakterystycznych dla dużego ekosystemu produktów związanych z bezpieczeństwem ta integracja pomaga również wypełnić luki między bezpieczeństwem, IT i DevOps. Można na przykład automatycznie zaimportować najnowszą ocenę podatności na zagrożenia do następnej partii poprawek do przetestowania. Dzięki temu środowisko IT stanie się efektywnym elementem ochrony organizacji. Z kolei DevOps to ciągłe doskonalenie i automatyzacja, a po zintegrowaniu z zarządzaniem poprawkami infrastruktury i systemy mogą stać się bardziej odporne i spójne. Ponadto krytyczne dane można pobierać do narzędzi, takich jak Splunk, Reporting Services, Archer i Crystal Reports, w celu szybszej analizy, reagowania i zamykania w przypadku krytycznych zdarzeń zagrażających bezpieczeństwu.

Blokowanie zagrożeń, dla których nie ma poprawek

Oczywiście poprawki nie ochronią przed nieznanymi zagrożeniami. A jeśli nie można zastosować poprawek — na przykład dlatego, że są używane przestarzałe systemy lub istnieje obawa, że ich zastosowanie spowoduje destabilizację środowiska? Należy blokować aplikacje, do których nie są stosowane poprawki, za pomocą takich narzędzi, jak biała lista aplikacji czy zarządzanie

uprawnieniami. Jest bardzo ważne, aby użytkownicy mieli dostęp tylko do aplikacji, które są im niezbędne do pracy, oraz nie mogli korzystać z nieautoryzowanych aplikacji, które mogłyby zmniejszyć stabilność komputera, wpłynąć na bezpieczeństwo, naruszyć zgodność z licencjami, doprowadzić do przestojów użytkowników lub zwiększyć koszty zarządzania komputerem.

Jednak blokowanie komputerów wprawdzie zmniejsza ryzyko, ale również znacząco obniża jakość środowiska użytkowników końcowych. Użytkownicy, którzy źle się czują w pracy, pracują mniej wydajnie i częściej korzystają z pomocy technicznej. Ci użytkownicy mogą również reagować na blokady systemu, stosując obejścia i przechodząc do „szarej strefy IT", stwarzając w ten sposób nowe zagrożenia bezpieczeństwa.

Ivanti oferuje wiodące na rynku rozwiązania, które pomagają zapobiegać uruchamianiu nieautoryzowanego kodu bez ręcznego tworzenia dużych list i obniżania wydajności użytkowników. Oprogramowanie Trusted Ownership™ automatycznie zapobiega uruchomieniu kodu, nawet nieznanego, który próbuje uruchomić niezaufany właściciel (zwykle konto użytkownika). Można zarządzać uprawnieniami użytkowników i zasadami na wysokim poziomie szczegółowości, a w sytuacjach wyjątkowych samodzielnie podwyższać uprawnienia. Sprawiamy, że nadawanie użytkownikom dokładnie takich uprawnień, jakich potrzebują w pracy — nie za dużych i nie za małych — jest proste.

Rozszerzamy również naszą obsługę środowiska SCCM o kontrolę aplikacji. Teraz można na centralnej konsoli kontrolować aplikacje i działania użytkowników w punktach końcowych. Program System Center Operation Manager (SCOM) można wykorzystać do gromadzenia zdarzeń dotyczących programu Application Control i sprawdzać szczegóły.

Wyższy poziom zarządzania bezpieczeństwem

Platforma Ivanti do zabezpieczania punktów końcowych łączy zautomatyzowanie zarządzanie poprawkami i kontrolę aplikacji z rozbudowanym, zintegrowanym zarządzaniem punktami końcowymi, które obejmuje globalne zasady, diagnostykę zabezpieczeń, zdalną kontrolę punktów końcowych, tablice wskaźników dotyczących zabezpieczeń, raportowanie i wiele innych funkcji.

Na tym poziomie do oprogramowania Ivanti można dodawać zaawansowanie oprogramowanie antywirusowe i zabezpieczenia zachowania aplikacji, zezwalanie na uruchamianie skryptów tylko zaufanym aplikacjom, ochrona przed atakami w pamięci itd.). Dodatkowo można ograniczyć dostęp do autoryzowanych sieci lub adresów IP, a także dostosować konfiguracje zapór dla pojedynczych systemów lub grup systemów, w tym konfiguracje zapór najnowszych systemów Windows. Można wykrywać próby szyfrowania plików na komputerze lokalnym, zatrzymywać proces szyfrowania oraz powiadamiać wszystkie komputery w sieci o umieszczeniu na czarnej liście złośliwego oprogramowania, co oznacza odparcie ataku. przed złośliwym oprogramowaniem. Możemy również zapewnić kontrolę urządzeń (kontrolowanie użycia urządzeń wymiennych, wymuszanie szyfrowania na urządzeniach wymiennych i dyskach twardych) oraz zaawansowaną ochronę przed atakami bez plików (wyłączanie skryptów pobranych z Internetu, uczenie się

Wygodny pojedynczy interfejs upraszcza zarządzanie ustawieniami i zadaniami zintegrowanych elementów i usług związanych z bezpieczeństwem. A rozbudowane możliwości zdalnej kontroli oznaczają, że można izolować, śledzić i czyścić punkty końcowe w sieci. Można również przejąć kontrolę nad komputerami, które działają powoli lub w inny sposób stanowią zagrożenie dla bezpieczeństwa. Informacje w czasie rzeczywistym (reputacja aplikacji, czas wyszukiwania/uruchamiania i inne metadane) umożliwiają szybkie znalezienie przyczyny problemu i jej usunięcie — za pomocą tej samej konsoli. Integracja z narzędziami do zarządzania systemami poprawia efektywność środowiska IT i kontrolę nad nim.

Raportowanie wskaźników w czasie rzeczywistym

Na koniec, Ivanti może pomóc w poznaniu wyników.

Ponieważ nie ma prawdziwej obrony bez rzeczywistego wglądu w środowisko, Ivanti Xtraction zamienia raportowanie

w pole wyboru, z danymi na żądanie i możliwością łatwego tworzenia nowych tablic wskaźników i raportów, aby przekazać odpowiednie dane kierownictwu, dyrektorom oraz właścicielom linii biznesowych (LOB) i aplikacji.

Gotowe łączniki dla prawie każdego używanego narzędzia (stanowiska serwisowe, zestawy narzędzi monitorujących i ITAM, systemy telefoniczne itp.) oznaczają brak kodowania, guru inteligencji biznesowej, arkuszy kalkulacyjnych, a także brak silosów danych. Również oprogramowanie Xtraction można dostosować do łączenia wielu danych i przeglądać dane z całego przedsiębiorstwa w wybranym kontekście, co ułatwia podejmowanie mądrzejszych i szybszych decyzji.

[i] Privacy Rights Clearinghouse
[ii] https://arstechnica.com/security/2017/06/web-host-agrees-to-pay-1m-after-its-hit-by-linux-targeting-ransomware/
[iii] Verizon 2016 Data Breach Investigations Report (DBIR)
[iv] Verizon 2015 DBIR
[v] Verizon 2016 DBIR

ivanti.com.pl + 33 (0)1 49 03 77 80 sales@ivanti.pl