baramundi

White Paper

Zarządzanie słabymi punktami w systemie

Automatyczne wykrywanie i szybkie usuwanie luk w zabezpieczeniach

Empower your IT

SPIS TREŚCI

Składane w niniejszym dokumencie oświadczenia dotyczące urządzeń i funkcjonalności technicznych nie są wiążące i służą wyłącznie celom informacyjnym.
Informacje podane w broszurze mogą ulec zmianie. DocID WP-VM-200916

1 Jak uniemożliwić hakerom obchodzenie zabezpieczeń infrastruktury informatycznej?

Spektakularne ataki cybernetyczne, w wyniku których kradzione lub niszczone są tysiące zapisów danych, wielokrotnie pojawiają się na pierwszych stronach gazet. Co ciekawe, tak naprawdę tego rodzaju ataki na dużą skalę nie mogą być przypisywane geniuszowi utalentowanych hakerów. W rzeczywistości są one coraz częściej wywoływane przez przestępców, którym udaje się obejść zabezpieczenia bez użycia drogiego sprzętu i profesjonalnej wiedzy z zakresu programowania. Korzystają oni z darmowych programów mających na celu wykorzystywanie istniejących błędów w oprogramowaniu, czyli tzw. exploitów. Exploity są dostępne online i dają możliwość „sforsowania" wielu tysięcy rodzajów luk w zabezpieczeniach, które pojawiają się u każdego użytkownika Windows i na serwerach firmowych. Każda z tych luk umożliwia cyberprzestępcom przeprowadzenie skutecznego ataku. Zapory sieciowe i skanery antywirusowe nie zapewnią skutecznej ochrony przed tego typu atakami. W grupie ryzyka znajdują urządzenia, które nie zostały bezpiecznie skonfigurowane – przykładowo, wykorzystując wielokrotnie to samo hasło na kontach w wielu usługach, niepotrzebnie ułatwiasz hakerom atak na swoje urządzenie i działalność w internecie.

Luki w zabezpieczeniach potrafią spędzać sen z powiek administratorów IT, którzy ponoszą odpowiedzialność za bezpieczeństwo danych oraz bezawaryjne funkcjonowanie infrastruktury. Dane o klientach, dane na temat kwot transakcji biznesowych, dokumenty rozwojowe – wszystko to może zostać skradzione. Konsekwencje udanego ataku cybernetycznego mogą sparaliżować działalność przedsiębiorstwa i ujawnić jej poufne informacje. Poza stratami finansowymi i pogorszeniem wizerunku firmy, w najgorszym przypadku istnieje nawet ryzyko wszczęcia dochodzenia z nakazu państwa, na przykład w przypadku podejrzenia naruszenia przepisów o ochronie danych lub gdy skonfiskowane komputery firmowe zostały podłączone do sieci botnet i były zdalnie sterowane w celu przeprowadzania ataków cybernetycznych. Trop w postaci adresów IP zawsze doprowadzi z powrotem do firmy.

Duża i stale rosnąca liczba luk w zabezpieczeniach oznacza, że administrator IT nie jest w stanie kontrolować wszystkich urządzeń i zapewnić najwyższego stopnia bezpieczeństwa na wszystkich urządzeniach końcowych bez korzystania z zautomatyzowanych zasobów. To samo dotyczy konfiguracji wielu urządzeń w firmie. Niniejszy biuletyn informacyjny opisuje najważniejsze zagrożenia oraz przedstawia sposób wdrożenia automatycznego zarządzania słabymi punktami za pośrednictwem oprogramowania do zarządzania punktami końcowymi, które umożliwi zespołowi IT wykrywanie i szybkie usuwanie groźnych luk w zabezpieczeniach.

2 Od słabych punktów do cyberataku

2.1 Definicja: Przepis na cyberatak: słabe punkty, exploity i (złe) chęci

Słabe punkty w zabezpieczeniach Twojej infrastruktury informatycznej są jak okno, które zapomniałeś zamknąć wychodząc z domu: stanowią istotny z punktu widzenia bezpieczeństwa błąd – w tym przypadku, w systemie informatycznym. Ignorując słabe punkty, stwarzasz przestępcy możliwość włamania się do Twojego systemu – tak, jak w przypadku pozostawienia otwartego okna. Oczywiście nie jest to równoznaczne z przeprowadzeniem ataku, jednak pozostawienie otwartego okna na dłużej niż to konieczne jest działaniem dość nieostrożnym, prawda?

Sytuacja robi się niebezpieczna, jeżeli w przestrzeni internetu znaleźć można odpowiednie narzędzie do wykorzystania takiej luki – na przykład oprogramowania typu exploit. W ten sposób przestępca znajduje swego rodzaju drabinę, z pomocą której będzie mógł przedostać się do Twojego otwartego okna. Warto jednak zauważyć, że gdy człowiek w ciemnym ubraniu, w masce złodzieja i z aluminiową drabiną pod pachą pojawi się w Twojej okolicy, trudno będzie go nie zauważyć – a program exploit może zostać bardzo łatwo i anonimowo pobrany z internetu. W ostatnich latach powstał cały przemysł podziemny, który utrzymuje się z zarabiania poprzez wykorzystywanie exploitów do kradzieży ważnych danych. Przykładowo, przyjrzyjmy się popularnemu serwisowi, za pośrednictwem którego dokonywane są płatności, czyli PayPal. W internecie znaleźć można darmowe exploity, dzięki którym możliwa będzie kradzież danych z serwera usługi PayPal.

Exploity wykorzystywane są do przemycania tzw. payloads (czyli części szkodliwego oprogramowania, które wykonuje szkodliwe działanie) do systemów będących przedmiotem cyberataków. Payload to popularne złośliwe oprogramowanie umożliwiające śledzenie danych, usuwanie plików lub włączania danego punktu końcowego do sieci botnet. Innymi słowy, payload to worek, którego włamywacz używa do ukrywania i przenoszenia swojego łupu.

Narzędzia takie jak Metasploit, który został opracowany w celu wykrywania luk w zabezpieczeniach, umożliwiają posiadającym odrobinę doświadczenia użytkownikom korzystanie z exploitów i przeprowadzanie ataków. Metasploit jest instalowany w systemie Windows lub Linux, posiada interfejs kontrolowany za pośrednictwem menu lub graficzny i jest dostępny również w formie maszyny wirtualnej. A dla tych, którzy nie umieją posługiwać się tego rodzaju narzędziem – wszystkie niezbędne wskazówki można znaleźć na forach internetowych lub w krótkich instruktażach na YouTube. Wracając do naszej analogii – potencjalni hakerzy mają dostęp do narzędzia, które jest równie łatwe w użyciu, co drabina, przy czym znacznie mniej rzuca się w oczy.

2.2 Cykl życia słabych punktów zabezpieczeń

Oprogramowanie jest wyjątkowo złożonym produktem: jak podają przedstawiciele firmy Microsoft, Windows 7 został stworzony z wykorzystaniem około 40 milionów linii kodu programu. Dobre oprogramowanie zawiera z reguły mniej niż jeden błąd na 1000 linii kodu. Tak więc nawet po przeprowadzeniu najbardziej surowych kontroli jakości, kod programu zawiera wystarczająco dużo luk, które mogą stać się zagrożeniem dla bezpieczeństwa IT w firmie.

Ryzyko jest niewielkie, jednak tylko do momentu, dopóki ktoś nie zauważy słabych punktów w systemie. Prędzej czy później Twoje otwarte okno przykuje czyjąś uwagę – być może będzie to specjalista ds. oprogramowania, ekspert ds. bezpieczeństwa lub programista-amator. Osoby te komunikują się ze sobą za pośrednictwem forów internetowych, dokumentują słabe punkty, które udało im się zidentyfikować w konkretnych bazach danych i zgłaszają je twórcy oprogramowania. Duże przedsiębiorstwa, takie jak Microsoft czy Google, wypłacają swoim pracownikom premie za wykrycie nowych luk w zabezpieczeniach, tak, aby móc je jak najszybciej zidentyfikować i zamknąć.

Zazwyczaj nie potrzeba dużo czasu, aby dostępna była odpowiednia łatka, która zamknie lukę. Co wcale nie oznacza, że zagrożenie zostało wyeliminowane – wręcz przeciwnie! Twórcy programów typu exploit również przeszukują bazy danych w celu wykrycia słabych punktów. Analizują oni łatki wdrożone przez twórców właściwego oprogramowania, wykorzystując uzyskaną w ten sposób wiedzę do wyciągnięcia wniosków, w jaki sposób wykorzystać zaistniałe luki w zabezpieczeniach. Tak długo, jak odpowiednia łatka nie zostanie zainstalowana na wszystkich urządzeniach z wadliwym oprogramowaniem, istniejąca luka może zostać wykorzystana do przeprowadzenia skutecznych ataków z jej wykorzystaniem.

Słabe punkty są źródłem zagrożenia dopóki łatka nie zostanie zainstalowana na wszystkich urządzeniach.

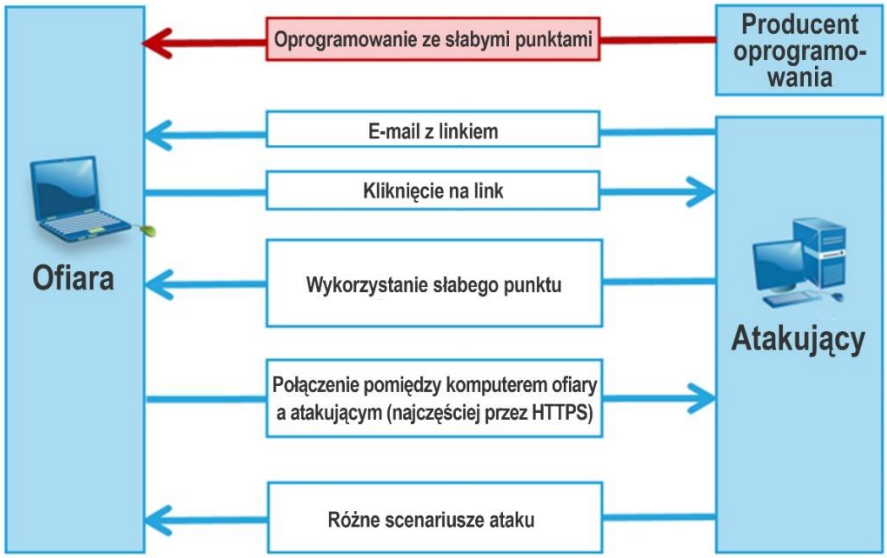
2.3 Schemat ataku na środowisko IT: Jak radzić sobie z cyberatakami na Twoją zaporę sieciową

W przeszłości, cyberprzestępcy na ogół starali się usunąć zaporę sieciową, co było równoznaczne z uzyskaniem dostępu do kryjącej się za nią sieci. Jednak stosowane dziś zabezpieczenia są na tyle zaawansowane i skuteczne, iż metoda stała się zawodna.

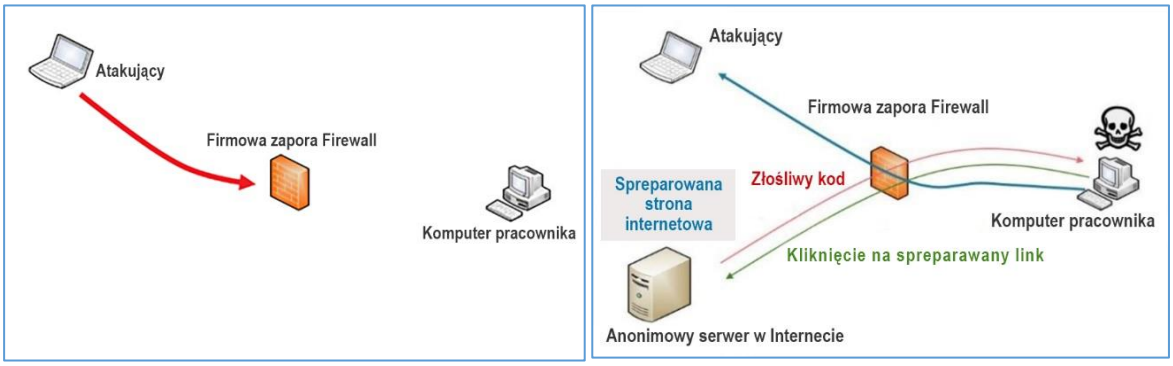
Współcześni cyberprzestępcy preferują stosowanie bardziej subtelnych rozwiązań. Obecnie cyberatak może przyjąć formę wyświetlania stron internetowych, które w rzeczywistości są nieszkodliwe. Często też hakerzy zwabiają swoje ofiary na wcześniej przygotowane strony

internetowe, które wykorzystują złośliwe oprogramowanie. Używają także plików poddanych modyfikacjom, które wykorzystują luki w programach do wyświetlania dokumentów (w formacie doc., PDF itd.) zainstalowanych przez użytkownika. Poszukując celu swoich ataków, hakerzy wykorzystują informacje pozyskane za pośrednictwem serwisów społecznościowych i podobnych źródeł.

Klasyczny przykład: Wiadomość e-mail wysłana do pracowników dużej firmy, której temat oferuje rewelacyjne rabaty na popularny produkt. Nie ulega wątpliwości, iż część odbiorców kliknie na link znajdujący się w treści maila. Strona, na którą zostanie przeniesiony użytkownik to fałszywy sklep internetowy, przy użyciu którego hakerzy wyszukują luki w przeglądarce lub w flash playerze. Użytkownik zaczyna się irytować, ponieważ strona, na której chciał zrobić zakupy, nie chce się poprawnie załadować; po chwili zamyka okno przeglądarki. Jedno jest pewne: pracownik nie poinformuje o zaistniałym zdarzeniu administratora IT, ponieważ surfowanie po internecie w godzinach pracy jest zabronione.



Możliwe scenariusze przeprowadzenia cyberataku z wykorzystaniem słabych punktów w oprogramowaniu



Nawiązywanie połączenia z osobą przeprowadzającą cyberatak

Jeżeli luka w zabezpieczeniach znajduje się w oprogramowaniu zainstalowanym na komputerze, którego użytkownik kliknął w przesłany link, jest już za późno... atak został zakończony sukcesem. Złośliwe oprogramowanie zostało zainstalowane na komputerze i umożliwia hakerowi dostęp do urządzenia. Ponieważ połączenie zostało nawiązane z wykorzystaniem sieci firmowej, zapora sieciowa nie wykryje ataku.

Dobra zapora sieciowa, skuteczne oprogramowanie antywirusowe i zarządzanie uprawnieniami użytkowników nadal są koniecznością. Należy je jednak wdrożyć dodatkowe środki bezpieczeństwa: zwiększanie świadomości wszystkich użytkowników, a w szczególności konsekwentne i możliwie jak najszybsze zamknięcie wszystkich luk bezpieczeństwa w oprogramowaniu zainstalowanym na indywidualnych urządzeniach.

3 Identyfikacja i zamykanie luk w zabezpieczeniach

3.1 Rozwiązanie niepraktyczne: Manualne zarządzanie słabymi punktami

W praktyce niemal niemożliwe jest, aby administratorzy IT manualnie monitorowali oprogramowanie i luki w zabezpieczeniach na wszystkich komputerach PC, laptopach i serwerach w środowisku informatycznym. Tylko w ciągu ostatnich trzech lat, w amerykańskiej bazie słabych punktów National Vulnerability Database[1] zarejestrowano ponad 80 000 nowych luk w zabezpieczeniach[2] – to około 550 nowych luk tygodniowo. Należy do tego dodać znane od dawna luki w oprogramowaniu, które nadal jest użytkowane, różne wersje językowe oprogramowania, jak również systemy operacyjne i architekturę procesów.

Administrator IT musi na bieżąco przeszukiwać bazy danych i blogi w poszukiwaniu raportów o lukach, oceniać słabe punkty, sprawdzać komputery i pakiety, testować i wdrażać aktualizacje, a także rejestrować, czy wdrożenie zakończyło się sukcesem. W przypadku większych sieci i przedsiębiorstw obejmujących kilka zakładów lub zatrudniających przedstawicieli terenowych, brak automatyzacji skazuje informatyków na porażkę. Jednocześnie kierownik działu IT musi również zagwarantować zgodność w środowisku informatycznym, w razie potrzeby być w stanie zgłosić status implementacji łatek, a w skrajnych przypadkach ponosić odpowiedzialność za zaistniałe problemy.

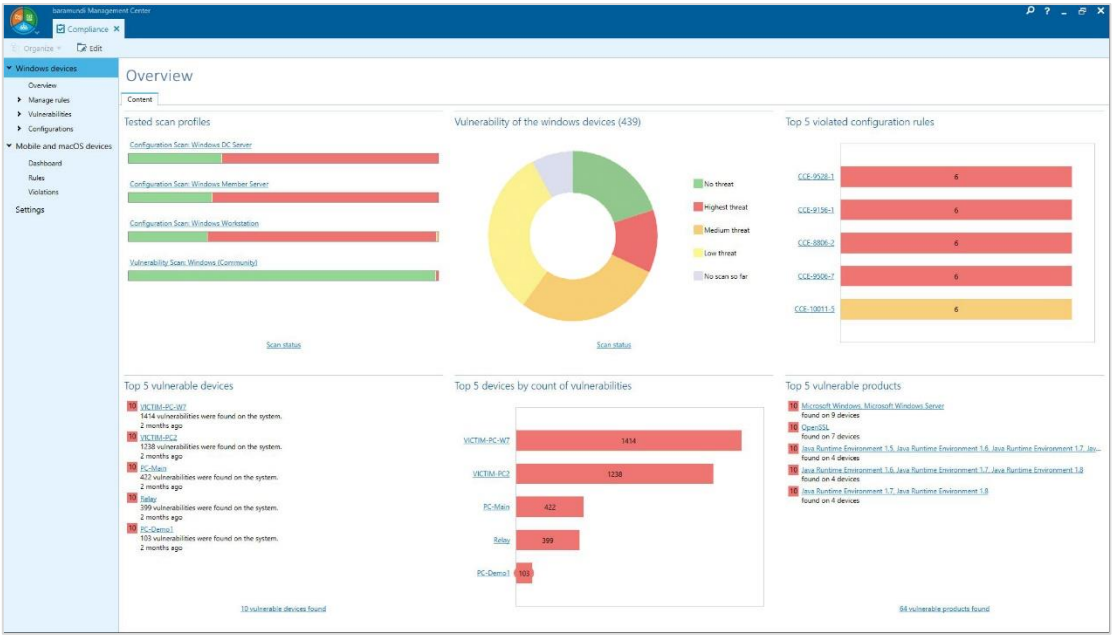
3.2 Automatyczne śledzenie luk w zabezpieczeniach oprogramowania zainstalowanego na wszystkich urządzeniach przenośnych

Na rynku dostępne są narzędzia z zakresu automatyzacji procesów informatycznych, takie jak oprogramowanie do zarządzania punktami końcowymi baramundi Management Suite. Oprogramowanie bMS nieprzerwanie skanuje punkty końcowe i serwery w danym środowisku informatycznym w poszukiwaniu słabych punktów. Dzięki temu możliwe jest szybkie i scentralizowane zamykanie luk w zabezpieczeniach. Program sprawdza zarówno urządzenia podłączone w siedzibie przedsiębiorstwa, jak również punkty końcowe w obiektach zewnętrznych lub urządzenia przenośne należące do przedstawicieli firmy pracujących w terenie.

W tym celu system uzyskuje dostęp do stale aktualizowanych baz danych opracowanych przez renomowane organizacje, w których gromadzone są dane o lukach. Narzędzie do

[1] Od stycznia 2017 r. do grudnia 2019 r.
[2] https://nvd.nist.gov

wyszukiwania słabych punktów – baramundi Vulnerability Scanner – wchodzące w skład pakietu baramundi Management Suite wykorzystuje katalog zidentyfikowanych słabych punktów w celu wykrywania luk w zabezpieczeniach w środowisku IT. Pulpit nawigacyjny zapewnia przejrzysty widok wszystkich informacji, pokazując administratorom aktualny stan ich środowiska informatycznego. Listy pozwalają administratorom na przeglądanie danych według komputera, słabych punktów lub poziomu zagrożenia: umożliwiają zlokalizowanie urządzeń z największą liczbą luk w zabezpieczeniach, największą ilością słabych punktów w środowisku informatycznym lub najbardziej niebezpiecznymi lukami, w celu jak najszybszego wyeliminowania zagrożenia.



baramundi Management Suite: Przegląd zagrożeń dla środowiska informatycznego – pulpit zgodności

Wyszukiwanie luk odbywa się „w tle”, przy użyciu minimalnych zasobów i nie ma wpływu na pracę użytkowników zalogowanych na punkcie końcowym. Dzięki narzędziu baramundi administratorzy IT znajdują się o krok przed hakerami: otrzymują wszystkie niezbędne informacje, dzięki czemu mogą szybko zamknąć istniejące luki, zanim zostaną one wykorzystane do przeprowadzenia cyberataków.

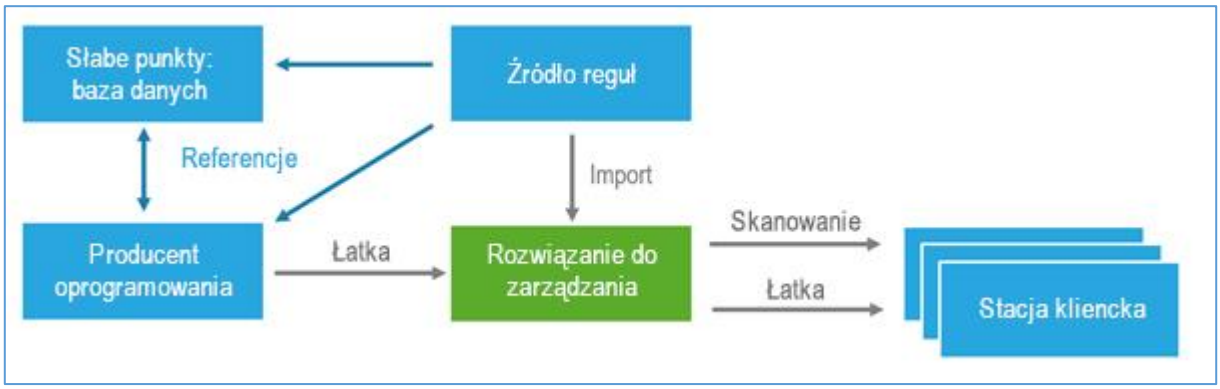
Szybka instalacja łatek skraca czas ryzyka przeprowadzenia ataku (oznaczony kolorem czerwonym)

3.3 Scentralizowane i automatyczne zamykanie luk bezpieczeństwa

Oprogramowanie do zarządzania punktami końcowymi baramundi oferuje użytkownikom również zautomatyzowane rozwiązania w zakresie wdrażania niezbędnych aktualizacji i łatek. Aktualizacje produktów firmy Microsoft są dostarczane za pośrednictwem modułu do zarządzania łatkami, który dostarcza komputerom wszystkie niezbędne aktualizacje, w oparciu o szereg reguł. Instalacja aktualizacji odbywa się w tle; jeżeli kilka z nich wymaga restartu urządzenia, zostanie ono uruchomione ponownie tylko raz w celu ograniczenia czasu potrzebnego na instalację. Ponieważ łatki mogą być instalowane z wielu serwerów plików, sieć nie jest tak bardzo obciążona. Administratorzy mogą wybrać między automatyczną lub ręczną dystrybucją łatek, a także możliwość definiowania różnych reguł dla poszczególnych grup użytkowników. Po wprowadzeniu łatek zbiorczych przez Microsoft, możliwe jest przeprowadzenie aktualizacji związanych z funkcjami i bezpieczeństwem punktów końcowych i serwerów w ramach jednej operacji.

Aktualizacje programów dla produktów innych niż marki Microsoft są również dostarczane przez innych producentów oprogramowania (np. Adobe, Mozilla) w formie gotowych do wdrożenia pakietów oprogramowania, które mogą być również wykorzystywane do początkowej instalacji lub odinstalowania. Oprogramowanie do zarządzania punktami końcowymi zwalnia administratorów IT również z obowiązku przeprowadzania aktualizacji i wgrywania łatek – nawet w przypadku urządzeń zlokalizowanych w zewnętrznych obiektach należących do firmy, podłączonych do sieci za pośrednictwem internetu, lub laptopów pracowników terenowych.

Ponieważ wszystkie procesy przeprowadzane w ramach pakietu zarządzania punktami końcowymi są ze sobą połączone, administratorzy IT otrzymują wszelkie istotne informacje zwrotne na temat procesów: instalacje zakończone sukcesem, instalacje w toku, zaistniałe błędy – dzięki temu łatki bezpieczeństwa nie tylko są wysyłane, ale także trafiają do odpowiedniego urządzenia i zamykają lukę w zabezpieczeniach.



Importowanie reguł i łatek, skanowanie punktów końcowych w poszukiwaniu luk w zabezpieczeniach oraz scentralizowane wdrażanie łatek

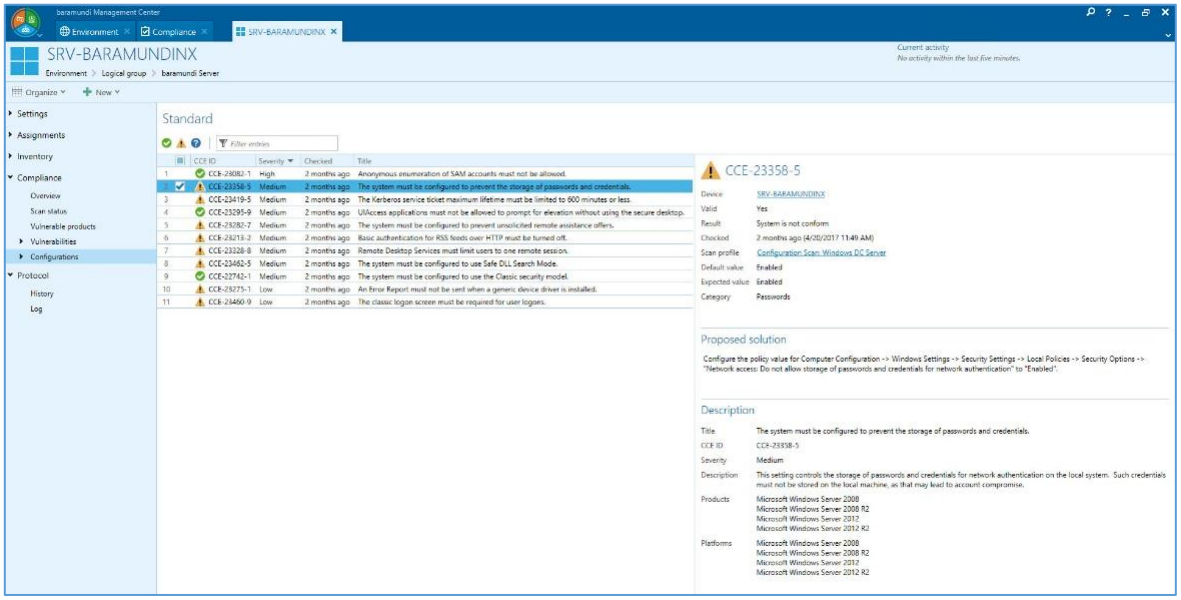
4 Zarządzanie konfiguracją

4.1 Egzekwowanie wprowadzenia bezpiecznych ustawień

Długość hasła i żądanie hasła po okresie bezczynności – tego typu ustawienia są niezbędne dla zapewnienia bezpieczeństwa punktu końcowego. Ważne jest również, aby sprawdzić, czy funkcja AutoPlay jest wyłączona dla wszystkich dysków, jakie rodzaje zdalnego dostępu na komputerach przenośnych są dostępne oraz czy możliwe jest szyfrowanie odwracalne hasła.

Te typy ustawień są zazwyczaj wdrażane zgodnie z wytycznymi dla grupy urządzeń. Jednak, aby wyegzekwować wysoki poziom bezpieczeństwa, należy również sprawdzić, czy odpowiednie zabezpieczenia zostały wdrożone na wszystkich punktach końcowych. Zdarzają się przypadki zmiany konfiguracji ustawień w ramach wsparcia lub użytkownika końcowego nieposiadającego odpowiednich uprawnień.

Podobnie jak w przypadku wyszukiwania luk w aplikacjach i systemach operacyjnych, administrator IT nie jest w stanie śledzić konfiguracji ustawień na każdym komputerze będącym częścią dużego środowiska informatycznego bez korzystania z rozwiązań z zakresu automatyzacji. Narzędzie do zarządzania konfiguracją ustawień na urządzeniach stanowić będzie dla niego nieocenioną pomoc. Tego rodzaju kontrole powinny być standardem dla punktów końcowych; ich celem jest zapewnienie, aby odpowiadały konfiguracja urządzeń odpowiadała wewnętrznym wymaganiom firmy w zakresie konfiguracji. Narzędzia do zarządzania konfiguracją – często sprzedawane w pakiecie z rozwiązaniami do zarządzania słabymi punktami w oprogramowaniu – oferowane są w postaci zintegrowanej z systemem zarządzania punktami końcowymi.



Wynik skanowania konfiguracji dla klienta Windows

Wynik skanowania ukazuje administratorowi IT, w przypadku których urządzeń wykryto naruszenia. Wyniki mogą być wyświetlane dla poszczególnych punktów końcowych lub dla grup i/lub jednostek organizacyjnych. Program zaproponuje również rozwiązania mające na celu naprawienie wszelkich naruszeń w sposób zorganizowany i ukierunkowany.

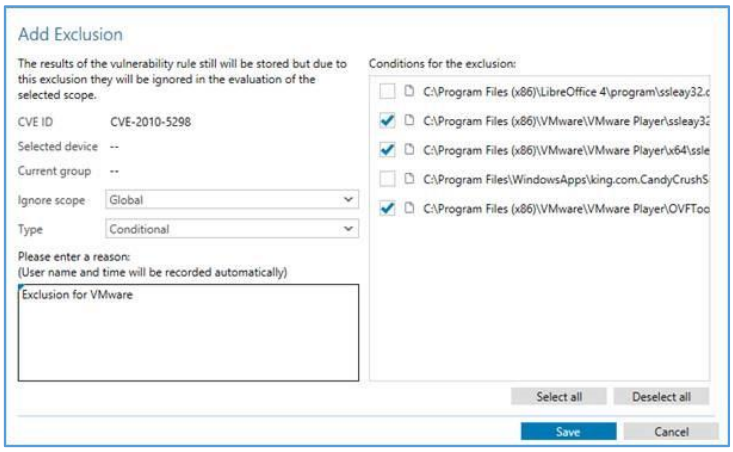
4.2 Wyjątek potwierdza regułę

W przypadku złożonych środowisk informatycznych, oprogramowanie zainstalowane na poszczególnych urządzeniach może się od siebie znacznie różnić. Na urządzeniach końcowych w przedsiębiorstwie znaleźć można różne wersje standardowego oprogramowania, oprogramowanie dostosowane do potrzeb użytkownika i/lub różne komponenty systemu operacyjnego. Zainstalowane oprogramowanie zawierać może izolowane komponenty (np. biblioteki SSL), które z kolei mogą zawierać luki.

Użytkownik nie ma zazwyczaj możliwości wymiany takich bibliotek bez przeprowadzenia aktualizacji uzyskanej od dystrybutora oprogramowania. Jeżeli programy, których dotyczy ten problem są firmie zbędne, wówczas odinstalowanie ich może okazać się dobrą opcją. Jednak jeśli po przeprowadzeniu oceny ryzyka i potencjalnych korzyści firma podejmie decyzję o dalszym użytkowaniu oprogramowania, biblioteki OpenSLL mogą zostać sklasyfikowane jako wyjątki.

Dobre narzędzie do zarządzania słabymi punktami dostarczane w ramach rozwiązania do zarządzania punktami końcowymi, powinno po pierwsze zapewnić przejrzystość potencjalnych luk w zabezpieczeniach; po drugie: zaoferować możliwość zdefiniowania wyjątków, które celowo stanowią słaby punkt oraz są tolerowane.

Poniższy przykład przedstawia, jak pakiet baramundi Management Suite „toleruje” wyjątek w postaci biblioteki (będącej słabym punktem) w kontekście VMware Player; ten sam plik nie będzie akceptowany w przypadku LibreOffice lub innych programów.



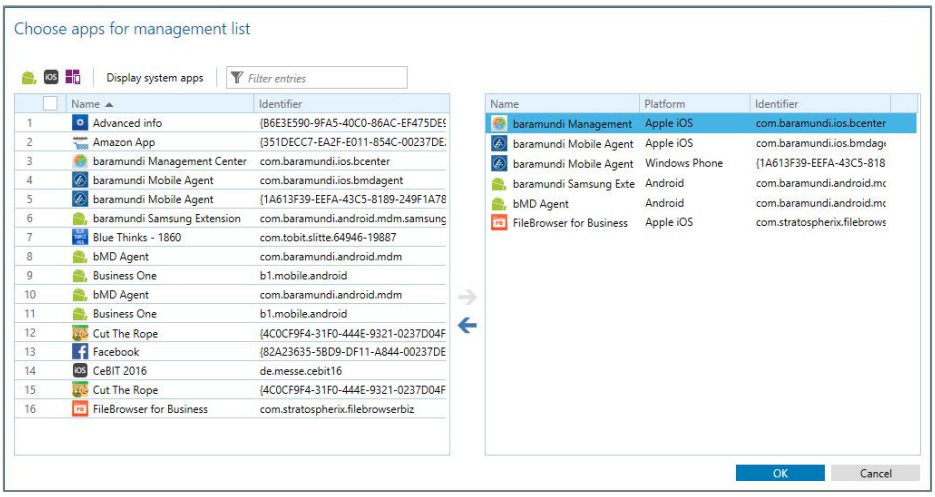
Określanie wyjątków w zakresie słabych punktów zabezpieczeń

5 Od zarządzania słabymi punktami w systemie do bezpiecznych punktów końcowych

Zautomatyzowane zarządzanie słabymi punktami oraz konfiguracją ustawień na urządzeniach jest ważną częścią udanej strategii zapewniania bezpieczeństwa infrastruktury informatycznej. Chcąc zapewnić wysoki poziom bezpieczeństwa punktów końcowych oraz odpowiednią ochronę danych, należy uwzględnić również inne kwestie.

Luki w zabezpieczeniach smartfonów i tabletów, które obecnie są częścią niemal każdej dużej infrastruktury informatycznej, muszą zostać zidentyfikowane w celu szybkiego wprowadzenia środków zaradczych. Skanowanie oprogramowania zainstalowanego na urządzeniach przenośnych w celu znalezienia jego słabych punktów jest co najmniej tak samo istotne jak w przypadku komputerów PC, ponieważ ustawienia urządzeń przenośnych skonfigurowane z myślą o użytkowniku końcowym zazwyczaj nie uwzględniają roli administratora IT, która umożliwiłaby użytkownikowi końcowemu zatrzymać instalację niepożądanego oprogramowania. Również w tym przypadku dostępne są zautomatyzowane narzędzia, takie jak baramundi Mobile Devices, zintegrowane z pakietem baramundi Management Suite. Narzędzie sprawdza dowolnie definiowane reguły na zarządzanych urządzeniach mobilnych i wykrywa takie rzeczy, jak oprogramowanie Jailbreak, ataki na rooty czy niepożądane aplikacje.

Kolejne rozwiązania z zakresu oprogramowania do zarządzania punktami końcowymi pozwalają na centralne i automatyczne tworzenie kopii zapasowych danych i ustawień użytkownika, szyfrowanie mobilnych nośników danych (np. pamięci USB), zapobieganie tworzeniu nielegalnych kopii na przenośnych nośnikach danych, czy blokowanie – za pomocą list aplikacji i list zezwoleń dostępu do urządzenia – uruchamiania nieznanych, nieautoryzowanych aplikacji w sieci firmowej, skutecznie wspierając administratorów IT w zapewnianiu jak najwyższego poziomu bezpieczeństwa.



Tworzenie listy aplikacji blokowanych oraz aplikacji, które mają dostęp do urządzenia

baramundi software GmbH

Firma baramundi software rozwija zintegrowane zarządzanie punktami końcowymi do centralnego zarządzania komputerami, urządzeniami mobilnymi i serwerami. Automatyzuje dystrybucję oprogramowania, upraszcza zarządzanie poprawkami i zapewnia przejrzystość w sieci. baramundi wnosi w ten sposób znaczący wkład w bezpieczeństwo IT i redukuje zasoby.

www.baramundi.com

Chcesz dowiedzieć się więcej o rozwiązaniu baramundi Management Suite? Zapisz się na nasz webinar!

Odkryj wieloplatformowe zarządzanie punktami końcowymi dla komputerów PC, serwerów, urządzeń mobilnych, komputerów Mac oraz środowisk wirtualnych dzięki pakietowi baramundi Management Suite – zapisz się na nasz darmowy webinar.

www.baramundi.com/pl-pl/it-training/warsztaty-niestandardowe/

baramundi

Czekamy na was!

Skontaktuj się z nami.

baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany

+49 821 5 67 08 - 380
request@baramundi.com
www.baramundi.com

+44 2071 93 28 77
request@baramundi.com
www.baramundi.com

+48 735 91 44 54
request@baramundi.com
www.baramundi.com

+49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 401
Framingham, MA 01701, USA

+1 508 808 3542
requestUSA@baramundi.com
www.baramundi.com

baramundi software Austria GmbH
Landstraßer Hauptstraße 71/2
1030 Wien, Austria

+43 1 7 17 28 - 545
request@baramundi.com
www.baramundi.com