ZARZĄDZANIE POPRAWKAMI DO OPROGRAMOWANIA I LUKAMI

WPROWADZENIE

Luki w zabezpieczeniach to luki, które mogą zostać wykorzystane przez złośliwą jednostkę w celu uzyskania większego dostępu lub przywilejów niż jest to dozwolone w systemie komputerowym. Poprawki to dodatkowe fragmenty kodu opracowane w celu rozwiązania problemów (powszechnie nazywanych „błędami") w oprogramowaniu. Łatki korygują problemy z bezpieczeństwem i funkcjonalnością oprogramowania i oprogramowania układowego. Zarządzanie poprawkami to proces identyfikacji, pozyskiwania, instalowania i weryfikowania poprawek dla produktów i systemów. Zarządzanie poprawkami to praktyka bezpieczeństwa mająca na celu proaktywne zapobieganie wykorzystywaniu luk w zabezpieczeniach IT istniejących w organizacji. Oczekiwanym rezultatem jest skrócenie czasu i pieniędzy przeznaczanych na radzenie sobie z lukami i wykorzystywaniem tych luk. Proaktywne zarządzanie podatnościami systemów zmniejszy lub wyeliminuje możliwość wykorzystania i będzie wymagało znacznie mniej czasu i wysiłku niż reagowanie po wystąpieniu eksploatacji. Ten rozdział ma na celu pomóc organizacjom we wdrażaniu programów naprawiających poprawki i luki w zabezpieczeniach. Najpierw wyjaśnia znaczenie zarządzania poprawkami, a następnie omawia wyzwania związane z zarządzaniem poprawkami. Następnie rozdział zawiera przegląd technologii zarządzania poprawkami w przedsiębiorstwie i zalecenia dotyczące ich użycia. Ma również na celu poinformowanie czytelnika o możliwych miarach i metrykach zarządzania poprawkami w przedsiębiorstwie.

ZNACZENIE ZARZĄDZANIA ŁATKAMI.

Z punktu widzenia bezpieczeństwa łatki są najczęściej interesujące, ponieważ łagodzą luki w oprogramowaniu; zastosowanie łat eliminujących te podatności znacznie ogranicza możliwości wykorzystania. Ponadto łatki są zwykle najskuteczniejszym sposobem ograniczania luk w oprogramowaniu i często są jedynym w pełni skutecznym rozwiązaniem. Czasami istnieją alternatywy dla poprawek, takie jak tymczasowe obejścia obejmujące oprogramowanie lub rekonfigurację kontroli bezpieczeństwa, ale te obejścia często negatywnie wpływają na funkcjonalność. Łatki służą innym celom niż tylko naprawianie wad oprogramowania; mogą również dodawać nowe funkcje do oprogramowania i oprogramowania układowego, w tym funkcje bezpieczeństwa. Nowe funkcje można również dodawać poprzez aktualizacje, które wprowadzają oprogramowanie lub oprogramowanie układowe do nowszej wersji w znacznie szerszym zakresie niż tylko nałożenie poprawki. Uaktualnienia mogą również rozwiązać problemy z zabezpieczeniami i funkcjonalnością w poprzednich wersjach oprogramowania i oprogramowania układowego. Ponadto dostawcy często przestają wspierać starsze wersje swoich produktów, co obejmuje zaprzestanie wydawania łatek usuwających nowe luki w zabezpieczeniach, przez co z czasem starsze wersje stają się mniej bezpieczne. Aktualizacje są niezbędne, aby takie produkty otrzymały obsługiwaną wersję, która jest załatana. Istnieje kilka wyzwań, które komplikują zarządzanie poprawkami. Jeśli organizacje nie sprostają tym wyzwaniom, nie będą w stanie skutecznie i wydajnie łatać systemów, co prowadzi do łatwych do uniknięcia kompromisów. Organizacje, które mogą zminimalizować czas poświęcony na instalowanie poprawek, mogą wykorzystać te zasoby do rozwiązywania innych problemów związanych z bezpieczeństwem. Już wiele organizacji w dużej mierze zoperacjonalizowało zarządzanie poprawkami, czyniąc je bardziej podstawową funkcją IT niż częścią bezpieczeństwa. Jednak nadal ważne jest, aby wszystkie organizacje starannie rozważyły zarządzanie poprawkami w kontekście bezpieczeństwa, ponieważ zarządzanie poprawkami jest tak ważne dla osiągnięcia i utrzymania solidnego bezpieczeństwa. Zarządzanie poprawkami jest wymagane przez różne struktury zgodności zabezpieczeń, mandaty i inne zasady. Na przykład specjalna publikacja NIST (SP) 800-532 wymaga kontroli bezpieczeństwa SI-2, FlawRemediation, która obejmuje instalowanie istotnych dla bezpieczeństwa poprawek

oprogramowania i oprogramowania sprzętowego, testowanie poprawek przed ich zainstalowaniem oraz włączanie poprawek do procesów zarządzania konfiguracją organizacji. Innym przykładem jest standard Payment Card Industry (PCI) Data Security Standard (DSS)3, który wymaga zainstalowania najnowszych poprawek i określa maksymalny czas instalacji najbardziej krytycznych poprawek.

WYZWANIA ZARZĄDZANIA ŁATKAMI

Czas, ustalanie priorytetów i testowanie.

Czas, ustalanie priorytetów i testowanie to powiązane ze sobą kwestie związane z zarządzaniem poprawkami w przedsiębiorstwie. Najlepiej byłoby, gdyby organizacja natychmiast wdrażała każdą nową poprawkę, aby zminimalizować czas, w którym systemy są podatne na ataki. Jednak w rzeczywistości jest to po prostu niemożliwe, ponieważ organizacje mają ograniczone zasoby, co powoduje konieczność ustalenia priorytetów, które łatki powinny być instalowane przed innymi łatami. Dalszą komplikacją jest znaczne ryzyko instalowania poprawek bez uprzedniego ich przetestowania, co może spowodować poważne zakłócenia operacyjne, potencjalnie nawet bardziej szkodliwe niż związany z tym wpływ na bezpieczeństwo wynikające z niewypychania poprawek. Niestety, poprawki testowe pochłaniają jeszcze więcej ograniczonych zasobów i sprawiają, że priorytetyzacja jest jeszcze ważniejsza. W przypadku zarządzania poprawkami czas, ustalanie priorytetów i testowanie często są ze sobą sprzeczne. Sprzedawcy produktów zareagowali na ten konflikt, dostarczając poprawki do swoich produktów. Zamiast wypuszczać dziesiątki poprawek pojedynczo przez okres trzech miesięcy, co wymaga testowania i wdrażania poprawek co kilka dni, dostawca może wypuszczać swoje poprawki w jednym pakiecie raz na kwartał. Dzięki temu organizacja może raz przetestować i raz wdrożyć poprawki, co jest o wiele bardziej wydajne niż testowanie i wdrażanie wszystkich poprawek osobno. Zmniejsza to również potrzebę nadawania priorytetów poprawkom — organizacja musi jedynie ustalić priorytety dla pakietu, zamiast osobno ustalać priorytety dla każdej zawartej w nim poprawki. Sprzedawcy, którzy dołączają łatki, wydają je zwykle co miesiąc lub co kwartał, z wyjątkiem przypadków, w których aktywnie wykorzystywana jest luka w zabezpieczeniach, która nie została załatana, w którym to przypadku zwykle wydają odpowiednią łatkę natychmiast, zamiast opóźniać ją w przypadku kolejnego pakietu. Łączenie łatek ma swoje wady; wydłuża czas od wykrycia luki do czasu, gdy łatka do niej stanie się publicznie dostępna. Jeśli atakujący odkryje tę samą lukę przed opublikowaniem poprawki, może mieć dłuższe okno na wykorzystanie luki z powodu celowego opóźnienia w wydaniu poprawki. Istnieją jednak dwa czynniki łagodzące. Jednym z nich jest to, że jeśli wiadomo, że dochodzi do nadużyć, sprzedawca prawdopodobnie natychmiast wyda poprawkę. Innym czynnikiem jest to, że łaty mogą być instalowane szybciej, jeśli są w pakiecie, niż jeśli wszystkie są wydawane osobno. Tak więc skutecznie pomaga to zmniejszyć okno możliwości wystąpienia luk związanych z dołączonymi łatami. Jest jeszcze więcej kwestii do rozważenia z czasem. Wydanie łaty może dostarczyć atakującym informacje, których potrzebują, aby wykorzystać daną lukę (np. dokonać inżynierii wstecznej luki w łacie), co oznacza, że nowo wydana poprawka może wymagać natychmiastowego zastosowania, aby uniknąć włamań. Jeśli jednak luka w zabezpieczeniach nie jest jeszcze wykorzystywana, organizacje powinny dokładnie rozważyć ryzyko związane z brakiem aktualizacji z ryzykiem operacyjnym związanym z aktualizacją bez uprzedniego przeprowadzenia dokładnych testów. W niektórych środowiskach operacyjnych, takich jak hosty wirtualne z włączonymi funkcjami migawek, zaleca się stosowanie poprawek bez testowania, o ile organizacja jest w pełni przygotowana do wycofania poprawek, jeśli występują przez nie problemy z użytecznością lub funkcjonalnością. Inną fundamentalną kwestią związaną z synchronizacją jest wymuszanie wprowadzania zmian, aby łatka zaczęła obowiązywać; może to wymagać ponownego uruchomienia poprawionej aplikacji lub usługi, ponownego uruchomienia systemu operacyjnego lub wprowadzenia innych zmian w stanie hosta. Ostatecznie liczy się nie to, kiedy poprawka została zainstalowana, ale

kiedy faktycznie zacznie ona obowiązywać. W niektórych przypadkach bardziej sensowne może być złagodzenie podatności za pomocą alternatywnej metody, przynajmniej do czasu, gdy poprawki będą w pełni funkcjonalne. Przykładem jest zmiana ustawień konfiguracyjnych dla podatnego oprogramowania w celu tymczasowego zablokowania funkcji aplikacji podatnych na ataki. Każda opcja łagodzenia ma inne konsekwencje dla bezpieczeństwa, funkcjonalności i operacji podatnego hosta, więc wybór jednej opcji nie jest sprawą trywialną.

Ponadto zmiana ustawień konfiguracyjnych wymaga zachowania starych wartości ustawień i przywrócenia ich w odpowiednim czasie. Innym problemem związanym ze zmianą ustawień konfiguracyjnych jest to, że często wymagają one zmiany stanu hosta, na przykład ponownego uruchomienia aplikacji. Wdrażanie zmian w konfiguracji może być tak samo zakłócające działanie hosta, jak instalowanie poprawki.

Wymuszenie wprowadzenia zmian, które wymaga ponownego uruchomienia systemu operacyjnego, może być problematyczne, gdy host wymaga uwierzytelnienia przed uruchomieniem, np. użycie oprogramowania do pełnego szyfrowania dysku (FDE). Organizacje korzystające z oprogramowania FDE lub innych technologii, które wymagają uwierzytelnienia przed uruchomieniem, powinny dokładnie rozważyć wpływ, jaki te technologie mogą mieć na instalację poprawki.

Ustalenie priorytetów, które poprawki należy zastosować i kiedy je zastosować, jest ściśle związane z czasem, ale są też inne kwestie. Może to zależeć od względnego znaczenia systemów podatnych na lukę (na przykład serwerów i klientów) oraz względnej ważności każdej z podatności (np. metryki ważności podatności, takie jak wspólny system punktacji luk w zabezpieczeniach [CVSS]). Inną kwestią są zależności, które mogą mieć między sobą poprawki; zainstalowanie jednej poprawki może wymagać uprzedniego zainstalowania innych poprawek, a w niektórych przypadkach wielokrotnego ponownego uruchamiania aplikacji lub ponownego uruchamiania hosta, aby poprawki zaczęły obowiązywać sekwencyjnie. Podsumowując, podczas planowania i wykonywania procesów zarządzania poprawkami w przedsiębiorstwie organizacje powinny dokładnie rozważyć odpowiednie kwestie związane z harmonogramem, ustalaniem priorytetów i testowaniem.

Konfiguracja zarządzania poprawkami

Innym poważnym wyzwaniem w zarządzaniu poprawkami w przedsiębiorstwie jest to, że zazwyczaj istnieje wiele mechanizmów stosowania poprawek. Na przykład:

* Oprogramowanie może się automatycznie aktualizować.

* Scentralizowane narzędzie do zarządzania systemem operacyjnym może być w stanie zainicjować poprawkę.

* Aplikacje do zarządzania poprawkami innych firm mogą być w stanie zainicjować instalowanie poprawek.

* Kontrola dostępu do sieci, technologie sprawdzania kondycji i podobne technologie mogą być w stanie zainicjować instalowanie poprawek.

* Użytkownik może być w stanie ręcznie skierować oprogramowanie do aktualizacji.

* Użytkownik może być w stanie ręcznie zainstalować poprawkę lub nową wersję oprogramowania.

Posiadanie wielu sposobów stosowania poprawek może powodować konflikty. Każda z metod może próbować załatać to samo oprogramowanie, co jest szczególnie problematyczne, gdy organizacja nie chce, aby niektóre poprawki były stosowane z powodu problemów z tymi poprawkami, opóźnień w

testowaniu itp. Wiele metod może również powodować opóźnienia lub pominięcie poprawek, ponieważ każde narzędzie lub administrator może założyć, że inny już zajmuje się konkretną łatką. Organizacje powinny określić wszystkie sposoby, w jakie poprawki mogą być zastosowane i podjąć działania w celu rozwiązania wszelkich konfliktów między metodami aplikacji poprawek. Powiązanym problemem z konfiguracją zarządzania poprawkami jest to, że użytkownicy mogą omijać lub omijać procesy zarządzania poprawkami. Jeśli użytkownicy są w stanie wprowadzać zmiany w oprogramowaniu swoich hostów, takie jak zmiana ustawień (np. włączanie bezpośrednich aktualizacji, wyłączanie oprogramowania do zarządzania poprawkami), instalowanie starych wersji oprogramowania i odinstalowywanie poprawek, mogą podważyć integralność zarządzania poprawkami. Aby rozwiązać te problemy, organizacje powinny upewnić się, że użytkownicy nie mogą wyłączać ani w inny sposób negatywnie wpływać na technologie zarządzania poprawkami w przedsiębiorstwie, a organizacje powinny stale monitorować technologie zarządzania poprawkami w przedsiębiorstwie w celu zidentyfikowania wszelkich występujących problemów

Alternatywne architektury hosta

Zarządzanie poprawkami w przedsiębiorstwie jest stosunkowo proste, gdy wszystkie hosty są w pełni zarządzane i uruchamiają typowe aplikacje i systemy operacyjne na zwykłej platformie. Gdy stosowane są alternatywne architektury hosta, zarządzanie poprawkami może być znacznie trudniejsze. Przykłady tych architektur obejmują:

Hosty niezarządzane. Jak omówiono w sekcji 40.3.2 tego rozdziału, kontrolowanie łatania może być znacznie trudniejsze, gdy hosty nie są zarządzane centralnie (tj. użytkownicy zarządzają własnymi hostami).

Hosty poza biurem (np. laptopy do telepracy). Hosty w innych sieciach nie są chronione przez mechanizmy zabezpieczeń sieci przedsiębiorstwa (zapory ogniowe, systemy wykrywania włamań do sieci, skanery luk w zabezpieczeniach itp.).

Niestandardowe komponenty IT (np. urządzenia). Na takich hostach często nie jest możliwe samodzielne łatanie poszczególnych aplikacji. Organizacja musi raczej poczekać, aż dostawca komponentu wyda zaktualizowane oprogramowanie.

Urządzenia mobilne. Smartfony, tablety i inne urządzenia mobilne (z wyjątkiem laptopów) zazwyczaj obsługują mobilne systemy operacyjne, a wprowadzanie poprawek na tych urządzeniach jest zasadniczo inne. Często konieczne jest podłączenie urządzenia mobilnego do komputera stacjonarnego lub laptopa oraz pobieranie i pobieranie aktualizacji za pośrednictwem tego komputera stacjonarnego lub laptopa. Niektóre urządzenia mobilne mogą bezpośrednio pobierać aktualizacje, ale może to być problematyczne ze względu na przepustowość (takie jak pobieranie dużych aktualizacji i uiszczenie opłat za transmisję danych). Inną opcją aktualizowania urządzeń mobilnych jest użycie oprogramowania do zarządzania urządzeniami mobilnymi w przedsiębiorstwie. Oprogramowanie do zarządzania urządzeniami mobilnymi w przedsiębiorstwie służy do zarządzania urządzeniami mobilnymi, nawet urządzeniami osobistymi, które nie są kontrolowane przez organizację. Może instalować, aktualizować i usuwać aplikacje, a także ograniczać dostęp przedsiębiorstwa, jeśli system operacyjny telefonu i oprogramowanie do zarządzania urządzeniami mobilnymi nie są aktualne. Aby uzyskać więcej informacji, zobacz sekcję 3 SP 800-124 wersja 1, Wytyczne dotyczące zarządzania i zabezpieczania urządzeń mobilnych w przedsiębiorstwie.

Wirtualizacja systemu operacyjnego (OS). Należy zachować poprawki dla każdego obrazu systemu operacyjnego i migawki używanej do pełnej wirtualizacji. Możliwości stosowania poprawek są często

wbudowane w środowiska zwirtualizowane, takie jak możliwość wprowadzania poprawek do obrazów offline i poddawania kwarantannie uśpionych instancji maszyn wirtualnych.

Oprogramowanie układowe. Aktualizacje oprogramowania układowego, takie jak aktualizacja systemu BIOS, zazwyczaj wymagają specjalnych uprawnień i obejmują inne procedury niż inne rodzaje aktualizacji. Zobacz NIST SP 800-147, Wytyczne dotyczące ochrony systemu BIOS, aby uzyskać dodatkowe informacje na temat aktualizacji systemu BIOS.

Organizacje powinny uważnie rozważyć wszystkie alternatywne architektury hosta używane w przedsiębiorstwie podczas projektowania zasad i rozwiązań zarządzania poprawkami w przedsiębiorstwie.

Inne wyzwania

W tej sekcji pokrótce omówiono inne wyzwania, które nie zostały omówione wcześniej w tej sekcji.

Zarządzanie spisem oprogramowania

Zarządzanie poprawkami w przedsiębiorstwie jest uzależnione od posiadania aktualnej i pełnej inwentaryzacji aktualizowanego oprogramowania (aplikacji i systemów operacyjnych) zainstalowanego na każdym hoście. Spis ten powinien obejmować nie tylko to, jakie oprogramowanie jest aktualnie zainstalowane na każdym hoście, ale także jaką wersję każdego oprogramowania zainstalowano. Bez tych informacji nie można zidentyfikować, uzyskać ani zainstalować właściwych poprawek. Te informacje o spisie są również niezbędne do identyfikacji starszych wersji zainstalowanego oprogramowania, aby można je było aktualizować. Główną zaletą aktualizacji starszych wersji jest zmniejszenie liczby wersji oprogramowania, które wymagają łatania i testowania ich.

Przeciążenie zasobów

Zarządzanie poprawkami w przedsiębiorstwie może spowodować przeciążenie zasobów. Na przykład wiele hostów może rozpocząć pobieranie tej samej dużej poprawki (lub pakietu poprawek) w tym samym czasie. Może to spowodować nadmierną przepustowość sieci lub, jeśli poprawki pochodzą z serwera poprawek organizacji, przeciążyć zasoby tego serwera. Organizacje powinny zapewnić, że zarządzanie poprawkami w przedsiębiorstwie może uniknąć sytuacji przeciążenia zasobów, na przykład poprzez dobranie rozmiaru rozwiązania do oczekiwanej liczby żądań i rozłożenie dostarczania poprawek w czasie, aby system zarządzania poprawkami w przedsiębiorstwie nie próbował przesyłać poprawek do zbyt wielu hostów w tym samym czasie.

Skutki uboczne instalacji

Zainstalowanie łaty może spowodować wystąpienie efektów ubocznych. Typowym przykładem jest instalacja, która przypadkowo zmienia istniejące ustawienia konfiguracji zabezpieczeń lub dodaje nowe. Może to stworzyć nowy problem bezpieczeństwa w procesie naprawiania pierwotnej luki w zabezpieczeniach poprzez łatanie. Organizacje powinny być w stanie wykryć skutki uboczne, takie jak zmiany ustawień konfiguracji zabezpieczeń, spowodowane instalacją poprawek.

Weryfikacja implementacji poprawek

Jak omówiono już, zainstalowana poprawka może nie zacząć działać, dopóki oprogramowanie, którego dotyczy problem, nie zostanie ponownie uruchomione lub nie zostaną wprowadzone inne zmiany stanu. Zbadanie gospodarza i ustalenie, czy dana łata zadziałała, może być zaskakująco trudne. Jest to jeszcze bardziej skomplikowane, gdy nie ma wskazania, że poprawka zacznie obowiązywać (ponowne

uruchomienie jest wymagane/nie jest wymagane itp.). Jedną z opcji jest próba wykorzystania luki w zabezpieczeniach, ale generalnie jest to wykonalne tylko wtedy, gdy exploit już istnieje i istnieje znaczne ryzyko związane z próbą wykorzystania, nawet w ściśle kontrolowanych warunkach. Organizacje powinny używać innych metod potwierdzania instalacji, takich jak skaner podatności niezależny od systemu zarządzania poprawkami.

Biała lista aplikacji

Technologie umieszczania aplikacji na białej liście mogą powodować konflikty z technologiami zarządzania poprawkami, ponieważ technologie dodawania aplikacji do białej listy działają na podstawie znanych charakterystyk plików wykonywalnych i innych składników aplikacji, które mogą zostać zmienione przez wprowadzenie poprawek. Jeśli sprzedawca dostarcza informacje o białej liście, będzie musiał zdobyć poprawkę, zarejestrować charakterystykę swoich plików i wysłać odpowiednie informacje do klientów. Jeśli organizacja tworzy własne informacje o białej liście, będzie musiała pozyskać każdą poprawkę, zarejestrować charakterystykę swoich plików i zaktualizować swoje białe listy o nowe informacje. Każda z tych metod może powodować problematyczne opóźnienia dla organizacji, które szybko stosują poprawki, zwłaszcza automatycznie; zaktualizowane oprogramowanie może być postrzegane jako nieznane oprogramowanie i nie może być uruchamiane.

Aby uniknąć tych problemów z aktualizacjami, większość technologii białej listy aplikacji oferuje opcje konserwacji. Na przykład wiele technologii umożliwia administratorowi wybranie pewnych usług (np. oprogramowania do zarządzania poprawkami) jako zaufanych aktualizatorów. Oznacza to, że wszystkie pliki, które dodają lub modyfikują na hoście, są automatycznie dodawane do białej listy. Podobne opcje są dostępne do wyznaczania zaufanych wydawców (tj. dostawców oprogramowania), użytkowników (takich jak administratorzy systemu), źródeł (takich jak zaufane ścieżki sieciowe) i innych zaufanych podmiotów, które mogą aktualizować białe listy. Organizacje korzystające z technologii białej listy aplikacji powinny upewnić się, że są skonfigurowane tak, aby uniknąć problemów z aktualizacjami.

TECHNOLOGIE ZARZĄDZANIA POPRAWKAMI W FIRMIE

Ta sekcja zawiera omówienie technologii zarządzania poprawkami dla przedsiębiorstw. Omawia ich skład, skupia się na zapewnianych przez nie funkcjach bezpieczeństwa i zarządzania oraz podaje zalecenia dotyczące ich użycia.

Komponenty i architektura.

Technologie zarządzania poprawkami dla przedsiębiorstw są architektonicznie podobne do innych rozwiązań bezpieczeństwa dla przedsiębiorstw: jeden lub więcej scentralizowanych serwerów zapewniających zarządzanie i raportowanie oraz co najmniej jedna konsola. Technologie zarządzania poprawkami dla przedsiębiorstw mogą być również oferowane jako usługa zarządzana. Pod względem architektonicznym technologie zarządzania poprawkami dla przedsiębiorstw różnią się od siebie technikami używanymi do identyfikowania brakujących poprawek. Trzy rozpowszechnione techniki to oparte na agentach, bezagentowe skanowanie i pasywne monitorowanie sieci. Wiele produktów obsługuje tylko jedną z tych technik, podczas gdy inne produkty obsługują więcej niż jedną. Wszystkie techniki są wyjaśnione bardziej szczegółowo w kolejnych podrozdziałach. Wybierając technologie zarządzania poprawkami dla przedsiębiorstw, organizacje powinny dokładnie rozważyć zalety i wady każdej techniki.

Oparte na agentach

Oparta na agentach technologia zarządzania poprawkami wymaga, aby agent działał na każdym hoście, na którym ma zostać zainstalowana poprawka, z co najmniej jednym serwerem, który zarządza

procesem instalowania poprawek i koordynuje pracę z agentami. (Zauważ, że technologia zarządzania poprawkami oparta na agentach jest wbudowana w niektóre systemy operacyjne). te poprawki i wykonywanie wszelkich zmian stanu potrzebnych do wprowadzenia poprawek (np. ponowne uruchomienie aplikacji, ponowne uruchomienie systemu operacyjnego). Każdy agent działa z uprawnieniami administratora, dzięki czemu może wykonywać te czynności. Serwer zarządzania poprawkami jest odpowiedzialny za dostarczanie agentom informacji o podatnym oprogramowaniu i dostępnych poprawkach, w tym o tym, gdzie można uzyskać łatki i jakie zmiany stanu są potrzebne. W porównaniu ze skanowaniem bezagentowym i pasywnym monitorowaniem sieci, technologie zarządzania poprawkami oparte na agentach są zdecydowanie preferowane w przypadku hostów, które nie są cały czas w sieci lokalnej, takich jak laptopy telepracowników i smartfony. Istnieje kilka ograniczeń związanych z technologiami zarządzania poprawkami opartymi na agentach. Hosty, które nie pozwalają administratorowi na bezpośredni dostęp do systemu operacyjnego, na przykład wiele urządzeń, zazwyczaj nie mogą uruchamiać agentów. Ponadto agenci mogą nie być dostępni dla wszystkich platform organizacji.

Skanowanie bez agenta

Bezagentowa technologia zarządzania poprawkami do skanowania obejmuje jeden lub więcej serwerów, które wykonują skanowanie sieciowe każdego hosta, który ma zostać załatany, i określają, jakich poprawek potrzebuje każdy host. Ogólnie rzecz biorąc, skanowanie bez agenta wymaga, aby serwery miały uprawnienia administracyjne na każdym hoście, aby mogły zwracać dokładniejsze wyniki skanowania i mieć możliwość instalowania poprawek i zaimplementuj zmiany stanu na hostach (ponowne uruchomienie aplikacji, ponowne uruchomienie systemu operacyjnego itp.). Główną zaletą skanowania bez agenta jest to, że nie wymaga instalacji i uruchamiania agenta na każdym hoście. Jednym z głównych ograniczeń skanowania bez agentów jest to, że pomija ono hosty spoza sieci lokalnej, takie jak laptopy telepracowników i urządzenia mobilne. Ponadto mechanizmy kontroli bezpieczeństwa sieci (np. zapory oparte na hoście) i technologie sieciowe (np. translacja adresów sieciowych) mogą nieumyślnie zablokować skanowanie lub w inny sposób negatywnie wpłynąć na wyniki skanowania. Skanowanie bez agenta może również negatywnie wpłynąć na operacje, zużywając nadmierną przepustowość. Wreszcie, skanowanie bez agenta może nie obsługiwać wszystkich platform organizacji.

Pasywne monitorowanie sieci

Technologie pasywnego monitorowania sieci lub zarządzanie poprawkami monitorują ruch w sieci lokalnej w celu identyfikowania aplikacji (aw niektórych przypadkach systemów operacyjnych), które wymagają zainstalowania poprawek. Technologie te mogą być skuteczne w identyfikowaniu hostów, które nie są obsługiwane przez inne rozwiązania do zarządzania poprawkami (skanowanie oparte na agentach, bezagentowe). Nie wymagają żadnych uprawnień na hostach do monitorowania, dzięki czemu mogą być używane do monitorowania stanu poprawek hostów, których organizacja nie kontroluje (systemy niezarządzane, systemy gości, systemy wykonawców itp.). Podstawową wadą pasywnego monitorowania sieci jest to, że działa tylko z oprogramowaniem, w którym można zidentyfikować wersję na podstawie ruchu sieciowego (zakłada się, że jest niezaszyfrowany). Oczywiście działa tylko z hostami w sieci lokalnej.

Możliwości bezpieczeństwa

W tej sekcji opisano typowe funkcje zabezpieczeń zapewniane przez technologie zarządzania poprawkami, podzielone na trzy kategorie: zarządzanie zapasami, zarządzanie poprawkami i inne.

Możliwości zarządzania zapasami.

Technologie zarządzania poprawkami zazwyczaj mają możliwość identyfikowania oprogramowania i wersji oprogramowania zainstalowanego na każdym hoście lub alternatywnie tylko identyfikowania wrażliwych wersji oprogramowania, które są zainstalowane. Ponadto niektóre produkty mają funkcje umożliwiające instalowanie nowych wersji oprogramowania, instalowanie lub odinstalowywanie funkcji oprogramowania oraz odinstalowywanie oprogramowania.

Możliwości zarządzania poprawkami

Technologie zarządzania poprawkami oczywiście zapewniają szereg możliwości zarządzania poprawkami. Typowe funkcje obejmują identyfikowanie potrzebnych łat, grupowanie i sekwencjonowanie łat do dystrybucji, pozwalanie administratorom na wybór, które łatki mogą lub nie mogą zostać wdrożone, a także instalowanie poprawek i weryfikację instalacji. Wiele technologii zarządzania poprawkami umożliwia również przechowywanie poprawek centralnie (w organizacji) lub pobieranie w razie potrzeby ze źródeł zewnętrznych.

Inne możliwości

Wiele produktów opartych na hoście, które mają funkcje zarządzania poprawkami, zapewnia również szereg innych funkcji bezpieczeństwa, takich jak oprogramowanie antywirusowe, zarządzanie konfiguracją i skanowanie podatności.

Możliwości zarządzania

Po wybraniu technologii zarządzania poprawkami administratorzy powinni zaprojektować architekturę rozwiązania, przeprowadzić testy, wdrożyć i zabezpieczyć rozwiązanie oraz zachować jego działanie i bezpieczeństwo. W tej części omówiono kwestie szczególnie interesujące z punktu widzenia zarządzania — wdrażaniem, eksploatacją i utrzymaniem — technologii zarządzania poprawkami oraz przedstawiono zalecenia dotyczące ich skutecznego i wydajnego wykonywania.

Bezpieczeństwo technologii

Wdrażanie korporacyjnych narzędzi do zarządzania poprawkami w przedsiębiorstwie może stworzyć dodatkowe zagrożenia bezpieczeństwa dla organizacji; jednak znacznie większe ryzyko stoją przed organizacjami, które nie łatają skutecznie swoich systemów. Takie narzędzia zwykle zwiększają bezpieczeństwo znacznie bardziej niż zmniejszają bezpieczeństwo, zwłaszcza gdy narzędzia zawierają wbudowane środki bezpieczeństwa w celu ochrony przed zagrożeniami i zagrożeniami bezpieczeństwa. Oto niektóre zagrożenia związane z używaniem tych narzędzi:

* Łatka mogła zostać zmieniona (nieumyślnie lub celowo).

* Poświadczenia mogą być niewłaściwie używane.

* Luki w komponentach rozwiązania (w tym agentach) mogą zostać wykorzystane.

* Jednostka może monitorować komunikację narzędzi w celu zidentyfikowania luk (szczególnie, gdy host znajduje się w sieci zewnętrznej).

Organizacje powinny ograniczać to ryzyko poprzez zastosowanie standardowych technik bezpieczeństwa, które powinny być stosowane podczas wdrażania dowolnej aplikacji w całym przedsiębiorstwie. Przykłady środków zaradczych obejmują:

* Utrzymywanie komponentów rozwiązania do poprawek (w tym ich łatanie)

* Szyfrowanie komunikacji sieciowej

* Weryfikacja integralności poprawek przed ich zainstalowaniem

* Testowanie poprawek przed wdrożeniem (w celu zidentyfikowania uszkodzenia)

Wdrażanie etapowe

Organizacje powinny wdrażać narzędzia do zarządzania poprawkami w przedsiębiorstwie, stosując podejście etapowe. Pozwala to na rozwiązanie problemów związanych z procesem i komunikacją z użytkownikiem w małej grupie przed uniwersalnym wdrożeniem aplikacji poprawki. Większość organizacji najpierw wdraża narzędzia do zarządzania poprawkami w ustandaryzowanych systemach stacjonarnych i jednoplatformowych farmach serwerów z podobnie skonfigurowanymi serwerami. Gdy to zostanie osiągnięte, organizacje powinny zająć się trudniejszą kwestią integracji środowisk wieloplatformowych, niestandardowych systemów stacjonarnych, starszych komputerów i komputerów o nietypowych konfiguracjach. W przypadku systemów operacyjnych i aplikacji nieobsługiwanych przez automatyczne narzędzia do łatania, a także niektórych komputerów o nietypowych konfiguracjach może być konieczne zastosowanie metod ręcznych; przykłady obejmują systemy wbudowane, przemysłowe systemy sterowania, urządzenia medyczne i systemy eksperymentalne. Dla takich komputerów powinna istnieć napisana i zaimplementowana procedura ręcznego procesu łatania.

Użyteczność i dostępność

Organizacje powinny równoważyć swoje potrzeby w zakresie bezpieczeństwa z potrzebami użyteczności i dostępności. Na przykład zainstalowanie łaty może „zepsuć" inne aplikacje; można to najlepiej rozwiązać, testując poprawki przed wdrożeniem. Innym przykładem jest to, że wymuszanie ponownego uruchomienia aplikacji, ponownego uruchomienia systemu operacyjnego i innych zmian stanu hosta jest uciążliwe i może spowodować utratę danych lub usług. Ponownie, organizacje muszą zrównoważyć potrzebę stosowania poprawek z potrzebą wsparcia operacji. Ostatnim przykładem, szczególnie ważnym w przypadku urządzeń mobilnych, jest pobieranie aktualizacji przez połączenia o niskiej przepustowości lub połączenia taryfowe; pobieranie dużych łat przez takie połączenia może być technicznie lub finansowo niewykonalne. Organizacje powinny zapewnić, że ich rozwiązanie do obsługi poprawek dla przedsiębiorstw działa na hostach mobilnych i innych hostach używanych w sieciach o niskiej przepustowości lub sieciach pomiarowych.

MIERNIKI I MIARY

Jak wyjaśniono w sekcji 3.3 NIST SP 800-55 wersja 1, Przewodnik pomiaru wydajności dla bezpieczeństwa informacji, tam są trzy rodzaje środków:

1. Środki wykonawcze są wykorzystywane do wykazania postępów we wdrażaniu programów bezpieczeństwa, określonych kontroli bezpieczeństwa oraz powiązanych polityk i procedur…

2. Mierniki skuteczności/wydajności są wykorzystywane do monitorowania, czy procesy na poziomie programu i środki kontroli bezpieczeństwa na poziomie systemu są prawidłowo wdrożone, działają zgodnie z przeznaczeniem i osiągają pożądany wynik…

3. Mierniki wpływu służą do określenia wpływu bezpieczeństwa informacji na misję organizacji…

Jeśli chodzi o tego typu środki, „mniej dojrzałe programy bezpieczeństwa informacji muszą opracować swoje cele i zadania, zanim będą mogły wdrożyć skuteczne pomiary. Bardziej dojrzałe programy wykorzystują środki wdrożeniowe do oceny wydajności, podczas gdy najbardziej dojrzałe programy wykorzystują wskaźniki skuteczności/wydajności i wpływu na biznes w celu określenia wpływu ich procesów i procedur bezpieczeństwa informacji." W związku z tym organizacje powinny wdrożyć i

stosować odpowiednie środki w zakresie technologii i procesów zarządzania poprawkami w przedsiębiorstwie. Przykłady możliwych środków wdrożeniowych obejmują:

* Jaki procent komputerów stacjonarnych i laptopów w organizacji jest objęty technologiami zarządzania poprawkami dla przedsiębiorstw?

* Jaki procent serwerów organizacji ma swoje aplikacje automatycznie ewidencjonowane przez technologie zarządzania poprawkami dla przedsiębiorstw?

Przykłady możliwych środków skuteczności/wydajności obejmują:

* Jak często hosty są sprawdzane pod kątem brakujących aktualizacji?

* Jak często aktualizowane są wykazy zasobów dla aplikacji hosta?

* Jaki jest minimalny/średni/maksymalny czas na nałożenie poprawek na X% hostów?

* Jaki procent komputerów stacjonarnych i laptopów w organizacji jest instalowany w ciągu X dni od wydania poprawki? Y dni? Z dni? (gdzie X, Y i Z to różne wartości, na przykład 10, 20 i 30).

* Jaki procent hostów jest średnio załatany w danym momencie? Odsetek hostów o dużym wpływie? Umiarkowany wpływ? Niewielki wpływ?

* Jaki procent poprawek jest nakładanych w pełni automatycznie, częściowo automatycznie, czy ręcznie?

Przykłady możliwych środków wpływu obejmują:

* Jakie oszczędności kosztów organizacja osiągnęła dzięki procesom zarządzania poprawkami?

* Jaki procent budżetu systemu informacyjnego agencji jest przeznaczony na zarządzanie poprawkami?