MADE IN GERMANY

G DATA TechPaper

Patch Management

Spis treści

1. Wstęp

Złożoność sieci korporacyjnych i stałe zagrożenie złośliwym oprogramowaniem stanowi wyzwanie dla każdego administratora sieci i systemów. Nie tylko liczba oprogramowania, która powinna zostać zaktualizowane znacznie wzrosła ale szybkość, przy której luki są eksploatowane również silnie wzrosła. Aby poradzić sobie z zadaniem instalacji poprawki, specjalistyczne systemy zarządzania poprawkami wykonują zautomatyzowane zadania i zapewniają terminowe wdrażanie poprawek związanych z bezpieczeństwem. Aby rozwinąć pełny obieg wokół zarządzania poprawkami, w tym pełną kontrolę zasobów sieciowych i oprogramowania, przedsiębiorstwa muszą myśleć o czymś więcej niż tylko o oprogramowaniu do zarządzania wdrażaniem. Aby pomóc w skutecznym prowadzeniu procedury zarządzania poprawkami, dokument ten przedstawia standardy zarządzania poprawkami, a także porady najlepszych praktyk w małych firmach (do 50 klientów sieciowych), jak i przedsiębiorstw (powyżej 50 klientów w sieci).

1.1. Definicja

Choć wielu producentów dąży do perfekcji w czasie premiery oprogramowania, większość produktów zostanie zaktualizowana i poprawiona w okresie ich życia. Zazwyczaj aktualizacje zapewniają nowe funkcje lub lepszą wydajność, natomiast poprawki mają naprawić błędy oprogramowania. Pierwsza kategoria zwykle nie ma decydującego znaczenie przy wdrożeniu w przedsiębiorstwie, ale ta druga wymaga szybkiego działania: szczególnie w przypadku kwestii bezpieczeństwa, poprawki powinny być szybko wdrożone w całej sieci korporacyjnej, aby zapobiec możliwej eksploatacji.

Patch Management ma na celu usprawnienie wdrażania poprawek. Aktualizacje są często zawarte w procesie, dzięki czemu używana infrastruktura techniczna i organizacyjna, która jest utworzona w celu stworzenia ujednoliconego systemu aktualizacji (Unified Update) / Patch Management (UPMS). Kompletny UPMS obejmuje więcej niż tylko możliwości techniczne potrzebne do wdrożenia poprawki przez sieć. Czas spędzony na rzeczywistym rozmieszczeniu powinien być ograniczony do minimum, aby skoncentrować dostępne zasoby na rozpoznaniu, klasyfikowaniu i rozwiązaniu kwestii bezpieczeństwa. W zależności od wielkości organizacji, może to wymagać wyspecjalizowanego personelu lub co najmniej procedury przepływu pracy w celu zapewnienia szybkiego podejmowania decyzji w sytuacjach awaryjnych.

Procedury zarządzania poprawkami powinny być stosowane w każdej firmie, gdzie integralność i bezpieczeństwo sieci komputerowej musi być sprawnie zarządzane. Odnosi się to do małych sieci biznesowych podobnie jak w przypadku dużych sieci korporacyjnych. Scentralizowane zarządzanie poprawkami pomaga ustanowić podstawę bezpieczeństwa dla całej sieci oraz umożliwia prostą i szybką instalację poprawki.

1.2. Znaczenie

Poprawki często naprawiają luki w zabezpieczeniach, przez którą atakujący może uzyskać dostęp do systemów uruchamiając zarażone oprogramowania. W odpowiedzi na zagrożenia bezpieczeństwa, szybkie rozmieszczenie poprawek jest ważne. Czynnikiem komplikującym wydanie poprawki właściwie pobudza hakerów do rozwoju i wykorzystywania błędów bezpieczeństwa, ze względu na publiczne ujawnienie informacji na temat poprawki. Dzięki inżynierii wstecznej plików, atakujący może uzyskać informacje konieczne do etapu skutecznego ataku. Stawia to dodatkową presję na administratorów do terminowego zaktualizowania swoich systemów. Patch Management pomaga przyspieszyć wdrożenie poprawki i poprawia efektywność kompletnego procesu poprzez koordynację i standaryzację procedur wdrażania poprawki.

Nie stosowanie poprawek stwarza dla systemów zagrożenie. Atakujący, którzy korzystają z błędów oprogramowania mogą, w zależności od powagi problemu, uzyskać dostęp do plików zapisanych na komputerze, uruchamiać programy, podejmują działania w stosunku do innych komputerów w sieci firmowej. Natomiast infekcja złośliwym oprogramowaniem poprzez drive-by download lub ataki hakerów są irytujące dla

użytkowników domowych, a sieci korporacyjne są szczególnie wrażliwe. Stawka jest dużo wyższa: sama obecność hakera w sieci firmowej zagraża integralności danych i może prowadzić do utraty danych, jeśli jeden lub więcej systemów jest nieodwracalnie uszkodzony. Inne zagrożenia to przestoje w systemach krytycznych, kradzież własności intelektualnej, utratę renomy lub nadmiernych kosztów obrony prawnej, jeżeli dane klienta zostaną utracone.

Wystandaryzowane procedury aktualizowania oprogramowania zapobiegają pomyślnemu wykorzystaniu błędów oprogramowania przez hakerów. Jednak Patch Management nie jest jedynym środkiem, który należy podjąć. Nawet jeśli oprogramowanie jest w pełni poprawione, hakerzy mogą mieć świadomość błędów, które nie zostały jeszcze odkryte przez dostawców oprogramowania. Sieci biznesowe oraz stacje robocze powinny być zawsze chronione przez produkty bezpieczeństwa na poziomie klienta, zapewniające środki, takie jak sygnatury oparte na znanym złośliwym oprogramowaniu, skanowaniu heurystycznym i reputacji plików, jak również ochronę na poziomie sieci.

1.3. Zgodność

Procedury dotyczące zarządzania poprawkami jako niezależnego procesu rzadko istnieją. Dla wielu firm, Patch Management jest częścią szerszego wachlarza środków podjętych w kontekście bezpieczeństwa informacji. To pole jest dobrze udokumentowane, a wiele firm już spełnia obowiązujące normy, przede wszystkim ISO/IEC 27002:2013[1]. Norma ta, która została zaadaptowana przez wiele krajowych organów normalizacyjnych, ustanawia wytyczne dotyczące wszystkich aspektów organizacyjnych zarządzania informacją, oraz przedstawia standardy dla pełnej ochrony zarządzania systemem bezpieczeństwa informacji[2]. Podobnie, Information Security Forum's jest standardem dobrych praktyk jako najlepsze praktyki na podstawie instrukcji do bezpieczeństwa informacji. Dodatkowo, norma ISO 15408-1: 2009, znana także jako Common Criteria dla Information Technology Security Evaluation (CC), stanowi ramy do określania, wdrażania i testowania wymagań bezpieczeństwa[3].

Na poziomie bardziej praktycznym, agencje rządowe w kilku krajach opublikowały na własną rękę standardy i zalecane praktyki dotyczące zarządzania poprawkami. Różne wskazówki odnoszą się do różnych sektorów gospodarki. Prywatne przedsiębiorstwa w Stanach Zjednoczonych, na przykład, mogą zasięgnąć wiedzy w przewodniku Narodowego Instytutu Standardów i Technologii dla technologii zarządzania poprawkami w przedsiębiorstwie (SP 800-40 Rev. 3 Projekt)[4].

Krytyczni dostawcy infrastruktury, w tym organizacji związkowych, przemysłu ciężkiego i wojskowego, są obsługiwani przez National Cyber Security Division w departamencie bezpieczeństwa wewnętrznego. W roku 2008 ta instytucja opublikowała dokument zalecanych praktyk dla systemów sterowania Patch Management, koncentrując się na krytycznej infrastrukturze[5].

Rządy państw europejskich podjęły podobne starania. Wielka Brytania dla Centrum Ochrony Infrastruktury Narodowej zapewnia podręcznik dobrych praktyk Patch Management skierowany do krytycznych krajowych organizacji infrastrukturalnych[6].

W Niemczech Federalny Urząd Bezpieczeństwa Informacji (BSI) zapewnia doradztwo dla małych firm jak i dużych przedsiębiorstw jako część szerszego doradztwa zarządzania zmianami[7].

---

[1] zobacz: www.iso.org/iso/catalogue_detail?csnumber=50297

[2] zobacz: www.securityforum.org/downloadresearch/publicdownload2012sogp

[3] zobacz: www.commoncriteriaportal.org/cc

[4] zobacz: csrc.nist.gov/publications/PubsSPs.html

[5] zobacz: ics-cert.us-cert.gov/practices/documents/PatchManagementRecommendedPractice_Final.pdf

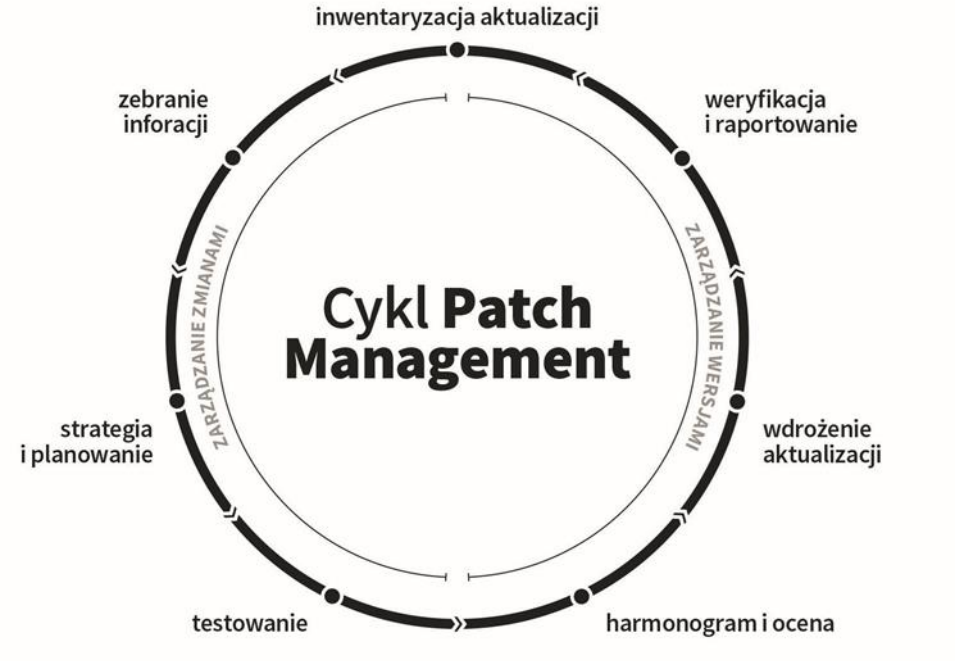
[6] zobacz: www.cpni.gov.uk/Documents/Publications/2006/2006029-GPG_Patch_management.pdf

[7] punkty startowe: www.bsi.bund.de/ContentBSI/grundschutz/kataloge/baust/b01/b01014.html dla administratorów w globalnym przedsiębiorstwie lub www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m02/m02221.html dla małych przedsiębiorstw.

2. Patch Management

Zarządzanie poprawkami jest ważne dla każdego komputera, czy to dla urządzenia w domu lub stacji roboczej w korporacji. W każdym przypadku dostępność nowych poprawek zabezpieczeń powinna być aktywnie monitorowana a poprawki powinny być wdrożone jak najszybciej. Jednak sposób, w jaki poprawki są zarządzane i wdrażane jest głównie pytaniem o skalę wdrożenia poprawek. Dla użytkowników domowych, wbudowany w systemy Microsoft Windows - Windows Update może zapewnić bezpieczeństwo zarządzania poprawkami dla systemu Windows w sposób całkowicie zautomatyzowany, a więcej producentów zmierza w kierunku w pełni przejrzystego, automatycznego procesu aktualizacji (Firma Adobe z oprogramowaniem Adobe Reader i Adobe Flash Player, a także przeglądarki takie jak Mozilla Firefox i Google Chrome). Użytkownicy są regularnie informowani przy użyciu wbudowanych narzędzi o aktualizacji programu. Doświadczeni użytkownicy mogą wybrać komercyjne narzędzia powiadomienia o aktualizacji oprogramowania, aby upewnić się, że żadne poprawki nie zostały pominięte. Niemniej jednak komputery domowe należą do jednych z najbardziej niezabezpieczonych urządzeń w odniesieniu do zarządzania poprawkami, głównie z powodu obojętności lub braku pilnego poczucia aktualizacji oprogramowania od strony użytkownika końcowego. Kompleksowe utrzymanie, przegląd zainstalowanego oprogramowania, jego słabych punktów oraz poprawek jest przytłaczająca dla pojedynczego użytkownika komputera - nie mówiąc już o administratorach sieci biznesowych z dowolnej liczby od pięciu do kilku tysięcy klientów. W miejscu gdzie są wdrożone znormalizowane, powtarzające się procedury zarządzania poprawkami, skracają czas wymagany do podjęcia inwentaryzacji oprogramowania, luk oraz automatyzacji rozmieszczania. Skuteczna procedura zarządzania poprawkami precyzuje jakie zadania będą wykonane, aby zapewnić metodę wycofywania, obszernego testowania wszystkich proponowanych zmian i ogłoszenia zmian dla wszystkich zaangażowanych stron.

Najlepsza ochrona przed szkodnikami wymuszającymi opłaty za dostęp do danych to oczywiście zablokowanie możliwości uruchomienia ransomware w systemach operacyjnych. Zaleca się stosowanie rozwiązań dedykowanych do wykrywania i blokowania aktywności ransomware. Oprogramowanie zabezpieczające, poza standardowym wykrywaniem zagrożeń w oparciu o sygnatury, powinno być wyposażone w szereg mechanizmów do wykrywania i blokowania aktywności typowej dla najnowszych jeszcze nieznanych zagrożeń.



Rysunek 1: Cykl zarządzania poprawkami

Cykl zarządzania poprawkami może być podzielony na różne etapy (które zostaną omówione szczegółowo w rozdziale 3). Należy pamiętać, że jest to cykl, a nie notacja EPC(event - driven process). Poprawki powinny być proaktywnie rozmieszczone, więc zarządzanie poprawkami powinno być proaktywnie przeprowadzone. Każdy krok cyklicznej procedury powinien być jednoznacznie określony i przypisany do kogoś. W zależności od woli i wymagań, firmy mogą połączyć etapy, poprzez łączenie i przypisywanie ich do tej samej osoby, lub zdefiniować kolejne punkty działania w razie potrzeby. Istniejące standardy zarządzania zmianami oraz zarządzania wydaniami mogą być (częściowo) zintegrowane. Niektóre etapy procedur mogą być zautomatyzowane, zwłaszcza rozmieszczenie, ale kilka kluczowych działań będzie musiało być wykonywane ręcznie dla każdego cyklu. Planowanie ma kluczowe znaczenie, aby zoptymalizować ten proces.

Tempo nawrotów cyklu Patch Management zależy od zasobów, które zostały udostępnione, aby go wykonać, a także od szybkości z jaką są publikowane poprawki dla oprogramowania, które jest w używane w sieci. Głównym źródłem poprawek jest Microsoft, którego system operacyjny Windows jest poddawany comiesięcznym najnowszym aktualizacją zabezpieczeń i poprawek. Niektórzy producenci wybrali w tym celu dostosowanie ich cyklu aktualizacji. Przede wszystkim Adobe (którego Adobe Reader i Flash Player są najczęściej wdrażanymi aplikacjami).

Te przewidywalne cykle poprawek planowane są w określonym terminie, w przypadku Microsoftu i Adobe co drugi wtorek miesiąca. Pozwala to administratorom systemu zaplanować cykliczną, niezawodną procedurę rozciągnięcia najnowszych aktualizacji w skali miesiąca. Inni dostawcy wydają aktualizacje rzadziej, jak Oracle, który wybrał dystrybucję poprawek bezpieczeństwa dla powszechnie stosowanej platformy Java co trzy do cztery miesiące.

Niektórzy producenci zdecydują się wydać poprawki dopiero gdy krytyczna kwestia stanie się widoczna. Planowanie zarządzania poprawkami, w tym szybki czas reakcji ma swoją cenę: może upłynąć trochę czasu, zanim nieprzewidywalnie wydana poprawka zostanie dokładnie przetestowana i wdrożona. Z drugiej strony, pakiet poprawek może powodować pewne luki bezpieczeństwa dla nie poprawionych błędów oprogramowania aż do następnej daty wydania poprawki.

2.1. Polityka zarządzania poprawkami

Przed planowaniem miesięcznych kroków cyklu zarządzania poprawkami i przypisania odpowiedzialności, muszą być zdefiniowane pewne standardy. Polityka zarządzania poprawkami pomaga podczas podejmowania decyzji. Polityka powinna obejmować pytania o strategię instalowania poprawek. Wszystkie dostępne poprawki powinny być zainstalowane jako domyślne lub czy będą klasyfikowane w zależności od powagi kwestii bezpieczeństwa do czasu naprawy? Czy łatki powinny być instalowane proaktywnie (zatamować ewentualne luki bezpieczeństwa) lub reaktywnie (tylko w przypadku pojawienia się problemów) lub kombinacja obu? Aby nie tracić czasu dla pojedynczych aktualizacji, zaleca się zdefiniowanie tak wiele podstawowych zasad jak to tylko możliwe. Nie jest rozwiązaniem instalowanie wszystkich dostępnych poprawek w tym samym czasie: należy dokonać świadomego wyboru, aby zapobiec sieciowych i systemowych obciążeń i problemów ze zgodnością.

Pozostałe parametry cyklu zarządzania poprawkami zależą od standardu instalacji, sieci i konfiguracji zabezpieczeń aplikacji. Chociaż każdy cykl obejmuje dokonywanie inwentaryzacji obecnego stanu sieci, nakład pracy ulega znacznemu zmniejszeniu, gdy środowisko sieciowe zostało skonfigurowane zgodnie ze standardami. Należy określić, które oprogramowanie będzie dopuszczone, które maszyny będą zaopatrzone w jakie oprogramowanie. Korzystanie z białych lub czarnych list inwentaryzacji sieciowej oprogramowania znacznie pomaga przy wdrożeniu poprawek. To samo odnosi się do konfiguracji zabezpieczeń, kont użytkowników i haseł.

Dzięki standaryzacji zasad w całej sieci zmniejszy się liczba wyjątków, którą należy obsłużyć podczas wdrażania poprawek. Musi być to efektywnie zdefiniowanie, które działania podjąć w przypadku wyjątków jeżeli się zdarzają. Administratorzy nie powinni być zaskoczeni przez maszyny, które okazują się nieosiągalne w czasie wdrażania poprawek, które powodują problemy z kompatybilnością podczas testowania, wdrażania lub kwestii

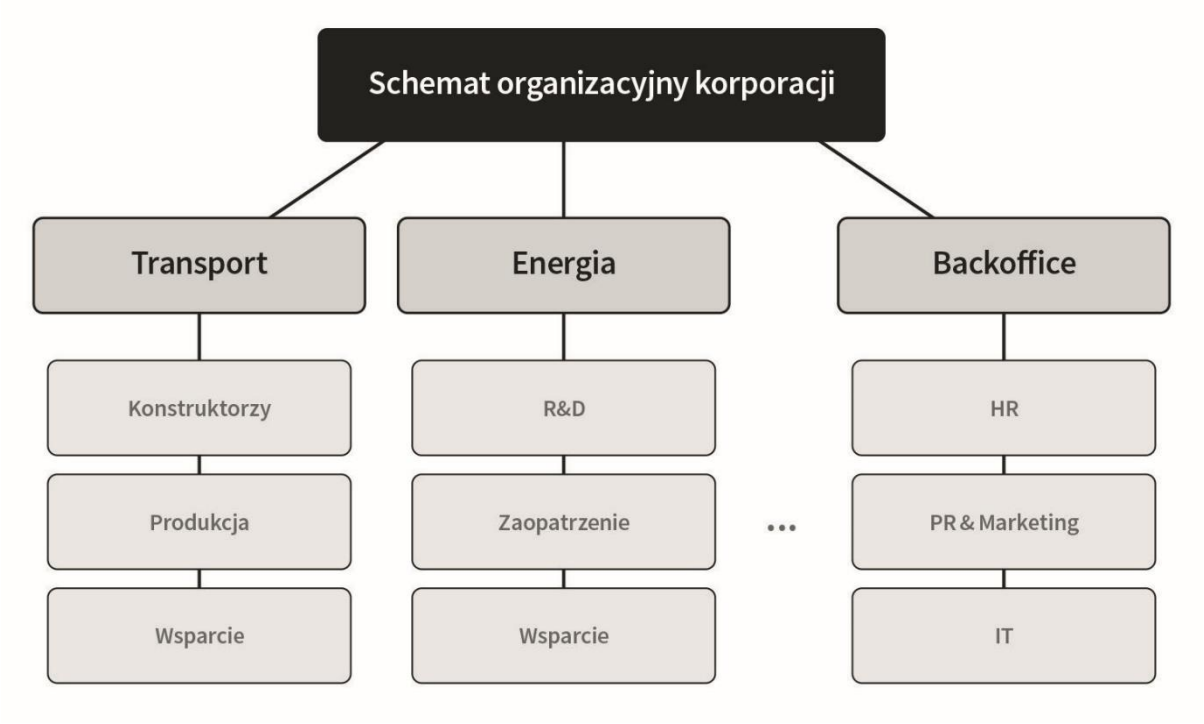
bezpieczeństwa. Szybkie przesunięcia, rekonfiguracja oprogramowania i eskalacja incydentu powinny być zdefiniowane jako część polityki zarządzania poprawkami.

Ważnym aspektem, o którym należy pamiętać, jest wdrożenie nowych urządzeń w sieci firmowej. Choć wykracza to poza ścisły zakres zarządzania poprawkami, ważnym krokiem jest upewnienie się, że obrazy systemów, z którymi nowi klienci są rozmieszczani zawierają najnowszy zestaw poprawek. Przestarzałe systemy powodują lukę bezpieczeństwa, która musi zostać zamknięta w nowo rozmieszczonych maszynach i powinna się stać częścią cyklu zarządzania poprawkami.

2.2. Korporacje kontra małe przedsiębiorstwa

Klienci biznesowi wymagają większej kontroli nad tym, jak i kiedy, które poprawki będą instalowane niż użytkownicy w domu. Korzystanie ze standardowych mechanizmów aktualizacji dla każdego zainstalowanego produktu prowadzi do chaotycznego stanu sieci, w której niektórzy klienci uruchamiają inne wersje oprogramowania niż pozostali. Centralnie rozmieszczone aktualizacje dają dużo korzyści każdej sieci biznesowej, poprzez zmniejszenie wpływu na użyteczność i zapewnienie szybkiego łagodzenia problemów bezpieczeństwa. Jednak nie wszystkie sieci biznesowe są tworzone jednakowo. Zarządzanie poprawkami dla sieci korporacyjnych różni się od sieci w małym przedsiębiorstwie.

W zarządzaniu poprawkami w przedsiębiorstwie, ważne jest, aby dokonać właściwej oceny organizacji sieci, stref oraz różnych ról klientów sieciowych. Zależnie od wielkości sieci, musi być kilka grup klientów, z których każdy ma swoją własną odrębną konfigurację. Niektóre grupy mogą być poddawane niemal każdej dostępnej poprawce, podczas gdy inne muszą być testowane bardziej uważnie. Rozważmy następujący przykład:

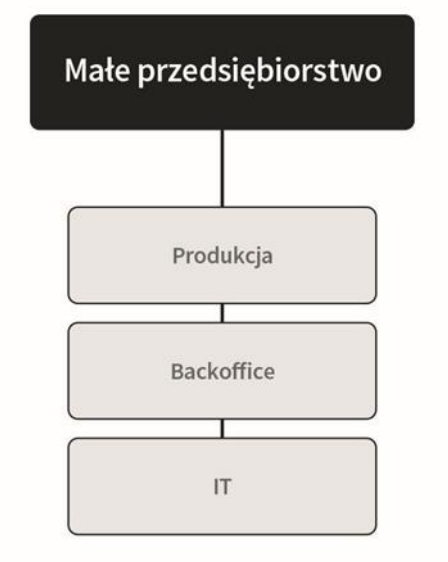


Rysunek 2: Organizacja sieci w korporacji

Korporacja z wieloma grupami biznesowymi z kilkoma dyscyplinami zwykle nie może zastosować tej samej polityki poprawek do wszystkich grup. Poszczególne pakiety oprogramowania, które są stosowane w różnych grupach to jedna sprawa, ale w szczególności wpływ jaki mogą mieć poprawki w środowisku pracy jest problematyczne. Chociaż ogólne konfiguracje klienta (Microsoft Office, przeglądarka), które są często stosowane w roli klienta backoffice, mogą być łatwo zaktualizowane, niektóre grupy biznesowe potrzebują środowisko pracy,

które nie zmienia się. Klienci, którzy wykorzystują kontrolę jakości lub podobnej funkcji, zależną od niezmiennego środowiska, muszą być ostrożni z integracją środowiska z UPMS lub ręcznie je obsługiwać.

Brak zasobów ludzkich i budżetu są to główne wyzwania zapobiegawcze małego przedsiębiorstwa po uruchomieniu w pełnym wymiarze czasu procedury monitorowania zarządzania poprawkami najnowszych problemów z bezpieczeństwem w czasie zbliżonym do rzeczywistego. W tym samym czasie, są głównym celem dla cyberprzestępców, którzy zdają sobie sprawę z braku dbałości o bezpieczeństwo i braku budżetu na zaawansowane narzędzia bezpieczeństwa. Dlatego zarządzanie poprawkami dla małych przedsiębiorstw, choć oparte na tym samym cyklu, jak procedura dla korporacji, ma kilka kluczowych różnic. Należy upewnić się, że procedura może być również przeprowadzona w sieciach, w których nie ma budżetu i zasobów ludzkich dla trwałej ochrony, wiele środków może być skalowane w dół (pod warunkiem, że w sieci nie ma zbyt wielu klientów - około pięćdziesięciu, dla typowej sieci małego przedsiębiorstwa).



Rysunek 3: Organizacja sieci małego przedsiębiorstwa

Strategia dystrybucji poprawek i testowania jest niezwykle uproszczona, gdy liczba scenariuszy do przetestowania jest ograniczona. Mniejsze firmy mają znacznie mniej grup biznesowych, a tym samym mniejszą rolę klienta w sieci. Mimo to, podobnie jak w przypadku zarządzania poprawkami w korporacji, konieczne jest, aby spędzić trochę czasu na przeglądzie sieci oraz przyjrzeniu się specyfice klientów działających w niej. Schemat pokazuje firmę tylko dla jednej grupy biznesowej. Małe przedsiębiorstwo z tylko jedną specjalizacją produkcyjną może podzielić swoich klientów sieciowych w zaledwie na dwie lub trzy role. Różnorodność zainstalowanych poprawek jest dużo mniejsza i choć żadne etapy cyklu zarządzania poprawek nie zostały pominięte, pobierają znacznie mniej czasu. Dalsze zwiększenie wydajności można osiągnąć w znacznym stopniu standaryzacją wdrożenia oprogramowania w całej sieci. Specjalnie dla mniejszych firm, które nie mogą mieć dedykowanego systemu lub administratora sieci, usprawnienie procedury jest bardzo ważne. Małe i średnie firmy mogą używać rozwiązania do automatyzacji zarządzania poprawkami prawie przez cały cykl. Prowadzenie na bieżąco inwentaryzacji oprogramowania z najnowszymi informacji o exploitach oraz wersjami oprogramowania może wymagać dużo czasu. Rozwiązanie Patch Management może pomóc tym firmom, które nie mają zasobów ludzkich, aby stale monitorować sieci i stan bezpieczeństwa. Alternatywą jest całkowity outsourcing bezpieczeństwa IT, w tym zarządzania poprawkami, który zajmie się infrastrukturą IT jako usługa zarządzana.

Jako pomocne narzędzie, małe firmy mogą stworzyć listę kontrolną lub listę zadań, która ma służyć jako wytyczne zarządzania poprawkami. Na podstawie cyklu zarządzania poprawkami, lista kontrolna zapewnia sposób w jaki należy wykonać najważniejsze działania w stosunkowo krótkim czasie. Dla małych i średnich firm, może nawet

zastąpić politykę zarządzanie poprawkami, ale musi dodatkowo zostać zdefiniowane wiele punktów. Należy zwrócić uwagę na:

- Aktualizację ewidencji oprogramowania
    - Lista zainstalowanych produktów w całej sieci oraz ich dostawców
    - Sprawdzanie cyklu poprawek dla każdego dostawcy
    - Priorytet produktów według wagi
- Zbieranie informacji
    - Sprawdzenie dostępności nowych poprawek raz na cykl dla każdego dostawcy
- Testowanie
    - Przetestowanie poprawki dla wszystkich stosowanych systemów
- Rozlokowanie
    - Wdrażanie poprawek i weryfikowanie wdrożenia

3. Procedura zarządzania poprawkami

3.1. Etap 1: Aktualizacja ewidencji oprogramowania.

Pierwszym etapem cyklu zarządzania poprawkami jest aktualizacja ewidencji oprogramowania. W każdym cyklu, to podsumowanie musi zostać zaktualizowane i uzupełnione o statystyki, takie jak informacje o wersji oprogramowania dla wszystkich maszyn. Kilka metod może być pomocne w upewnieniu się, że wszystkie urządzenia są zawarte w wykazie oprogramowania. Wiele sieci w przedsiębiorstwach posiada Windows Server i może skorzystać z usługi Active Directory. Kontroler domeny może stworzyć listę wszystkich dostępnych klientów w domenie. Jednak, może być wiele potencjalnych maszyn, które nie przystąpiły do domeny Windows. Listę niższego poziomu klientów sieci można otrzymać poprzez dostęp do plików dziennika sieci serwera DHCP (adres IP lub skan podsieci) lub sprawdzając lokalne rejestracje w serwerze DNS. Połączenie tych metod przyniesie najlepsze rezultaty, ponieważ nie wszystkie urządzenia zostaną wymienione przez każdą z metod. Może być konieczny, skan w wielu punktach w tym samym czasie aby uzyskać pełną listę maszyn. W przypadku mniejszych sieci, uzyskanie przeglądu klientów nie powinno być problematyczne. Jeśli udostępnianie plików i drukarek Windows zostało włączone, maszyny powinny pojawić się w oknie miejsc sieciowych. Szczególnie skomplikowana jest obecność maszyn wirtualnych w sieci. Zwirtualizowani klienci sieci mogą być niedostępni podczas ewidencji lub rozmieszczania. Mimo to, istotne jest aktualizowanie ich. Powinni być wymienieni w wykazie jako integralna część sieci, ponieważ każda maszyna wirtualna stanowi potencjalny punkt wejścia do sieci.

Strategia zarządzania poprawkami klientów sieciowych oraz konfiguracji powinna być wdrażana według pewnych standardów, dzięki czemu uzupełnienie pełnej listy oprogramowania będzie stosunkowo łatwe. Jeżeli jest wdrażanie tylko oprogramowanie, które jest absolutnie konieczne zmniejsza to prawdopodobieństwo luk bezpieczeństwa w obecnym systemie i sprawia, że jest to mniej czasochłonne podczas zarządzania poprawkami. Monitorowanie instalacji oprogramowania lub całkowicie zablokowania niezatwierdzonych aplikacji, zmniejsza ilość czasu spędzonego na identyfikacji, pozyskiwaniu i dystrybucji poprawek. Korzystanie z czarnej lub białej listy oprogramowania jest skutecznym sposobem na ograniczenie nowych instalacji oprogramowania. Ponadto, użytkownicy końcowi nie powinni być w stanie zmodyfikować poprawki i ustawień aktualizacji dla lokalnych instalacji oprogramowania, aby zapobiec rozbieżności pomiędzy wdrożeniem a polityką lokalną serwera. Obejmuje to wyłączenie automatyczne aktualizacje oprogramowania, takiego jak Adobe Flash Player i Adobe Reader, a także samodzielnego pobieranie aktualizacji z usługi Windows Update. Należy dokładnie sprawdzić całe wdrożone oprogramowanie oraz ich polityki aktualizacji i upewnienie się, że funkcje są pod centralną opieką.

Zbiór informacji, który uzyska się w ramach inwentaryzacji powinien zawierać informacje o wersji systemu operacyjnego jaki jest używany oraz pełną listę oprogramowania. Te dane to minimum, które należy gromadzić dla każdego klienta w sieci, aby umożliwić łatwe zapytanie o dostępność poprawki. Zbieranie informacji o sprzęcie, który jest w użyciu może pomóc w zapobieganiu lub obejściu problemów, takich jak brak miejsca

na dysku lub mocy procesora potrzebnego do przetworzenia poprawki. Znacznie upraszcza to proces identyfikacji i sprawia, że cała procedura staje się bardziej przewidywalna.

Aby być pewnym, że rzeczywiste wdrożenie można przeprowadzić bez problemów, należy wziąć pod uwagę wszystkie usługi uruchomione na klientach sieciowych. Środowisko, powinno być skonfigurowane do uzyskania maksymalnej wydajności i minimalnej podatności: im mniej usług uruchomionych na komputerze klienckim, tym mniejsze prawdopodobieństwo, że jeden z nich może być użyty jako źródło ataku. Podczas fazy inwentaryzacji, zbędne usługi można zidentyfikować i wyłączyć, wówczas, żadna z nich nie powinna zakłócić procesu instalowania poprawek. Podobnie, należy upewnić się, że każdy klient będzie dostępny z odpowiednimi uprawnieniami wymaganymi do zainstalowania oprogramowania. Bez dostępu praw administratora, proces instalowania poprawek może się nie powieść. Wreszcie, należy upewnić się, że wszystkie maszyny mają prawidłowy, nieprzerwany dostęp do sieci w przyzwoitą prędkością. Problemy z łącznością sieciową, albo przeciążenie sieci lub lokalne problemy, mogą powodować znaczne ilości błędów, które później muszą zostać rozwiązane ręcznie lub znacznie spowolnią rozmieszczanie poprawek.

Można wykorzystać różne techniki do aktualizacji ewidencji oprogramowania, w zależności od tego jakie dane są zbierane. Stosunkowo nieinwazyjnym sposobem jest wykonywanie zbierania informacji bez agentów. Ta scentralizowana metoda pozwala zebrać informacje do serwera z klientów sieci bez konieczności instalowania agenta w każdej maszynie. W celu zbadania komputerów, serwer musi mieć poprawne uprawnienia. Scentralizowany układ pozwala na stosunkowo łatwe procedury konfiguracji: tylko serwer musi być skonfigurowany. Maszyny, które zostały niedawno dodane do sieci mogą być skanowane, nawet bez lokalnego agenta. Minusem jest brak wsparcia dla maszyn, które nie zawsze są podłączone do sieci firmowej, czy też nie zawsze włączone. Dodatkowo, oprogramowanie dla bezpieczeństwa sieci może blokować bez agentowe techniki skanowania. Skanowanie oparte na agencie omija te problemy. Agent nawiązuje połączenie z serwerem niezwłocznie po włączeniu klienta. Ogromna przewaga nad skanowaniem bez udziału metod skanowania agentami jest integracja zarządzania poprawkami z istniejących rozwiązaniami - opartymi o rozwiązania bezpieczeństwa. Informacje, które są generowane podczas regularnej ochrony mogą być łatwo dostosowane w cyklu zarządzaniu poprawkami. Dzięki oddzielnej technice, monitorowanie sieci może być wykorzystywane do identyfikacji oprogramowania poprzez ruch sieciowy. Dla platform, na których agenci nie są wspierani, może być to użytecznym dodatkowym narzędziem, ale pasywne monitorowanie sieci jest zbyt zawodne, aby używać go jako głównego składnika. Sama technika jednak może być całkiem przydatna: wiele luk w zabezpieczeniach oprogramowania może być wykryte przez skaner sieciowy. Uruchomienie skanowania luk zabezpieczeń jako część fazy inwentaryzacji pomaga szybko lokalizować kwestie bezpieczeństwa, które muszą zostać poprawione (ale nie zawsze dostarczają wystarczającej ilości informacji na temat dostępności poprawki lub obejścia).

Nie wszystkie stacje robocze będą włączone do cyklu zarządzania poprawkami. Choć powinno się zapewnić wszystkim maszynom najnowsze aktualizacje. Istnieją ważne powody do wykluczenia niektórych klientów. Niektóre grupy biznesowe mogą wymagać niezmiennych środowisk (do testów, oceny i celów porównawczych), wymagające dodatkowych testów przed wdrożeniem poprawki. Podobnie starsze maszyny potrzebują dodatkowej uwagi. Niektóre programy są przestarzałe i mogą wymagać starszych systemów operacyjnych lub oprogramowania, wykraczających poza wyjściowe oprogramowanie lub nie są już aktualizowane. Aktualizowanie takich systemów może zatrzymać krytyczne aplikacje systemowe, więc dodatkowe testy są zalecane. Część oprogramowania może wymagać osobnego dostawcy poprawki, aby dodać zgodną wersję poprawki z innym oprogramowaniem. Ważne jest odkrycie tego rodzaju wymogów tak wcześnie, jak to możliwe. Jeżeli w fazie inwentaryzacji wskazano, że występuje przestarzałe oprogramowanie, jest większe prawdopodobieństwo wystąpienia problemów z kompatybilnością.

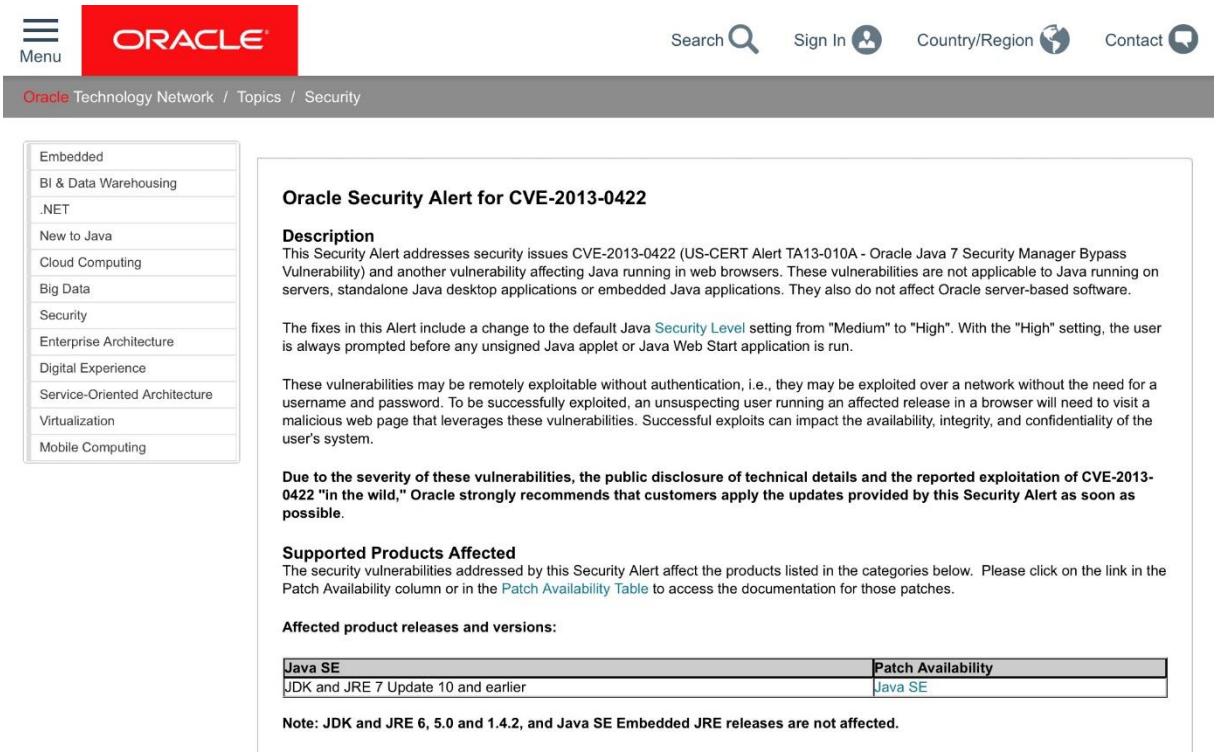
Stacje robocze, które nie zawsze są podłączone do sieci, takie jak laptopy dla personelu mobilnego, lub klienci VPN, nadal mogą być aktualizowani podczas regularnego cyklu, lecz nie mogą połączyć się z siecią zaraz po zaplanowaniu inwentaryzacji lub w czasie wdrażania poprawek. Upewnij się, że sieć i urządzenia nie są obciążone przy pierwszym logowaniu; jest wskazane rozmieszczenie zadań inwentaryzacji oprogramowania i wdrażania poprawek w czasie dla tego typu klientów. Maszyny wirtualne, które są uruchomione bezpośrednio

w sieci firmowej powinny być również zarządzane, jeśli nie są one oddzielone od zwykłego środowiska produkcyjnego przez ochronę urządzeń lub konfigurację VLAN.

Ogólnie rzecz biorąc, urządzenia, które w zależności od tego powodu, nie są (jeszcze) zawarte w cyklu zarządzania poprawkami, lub mają przestarzałe instalacje oprogramowania, należy dodatkowo starannie przetestować pod względem dziur i infekcji złośliwym oprogramowaniem. Planowanie dodatkowego skanowania przeciw wirusom lub ustanowienie odrębnej sieci lub stref w zaporze pomaga zapobiegać problemom. Korzystanie z polityki bezpieczeństwa, dostępu do zasobów sieciowych pomaga w ograniczeniu uprawnień. Blokowanie nośników wymiennych może zapobiec ewentualnym infekcjom i rozprzestrzenieniu się w sieci.

3.2. Etap II: Zbieranie informacji

Jeśli tylko kompletny inwentarz oprogramowania został utworzony lub zaktualizowany, ważne jest, aby mieć oko na nowe wersje aktualizacji oprogramowania i poprawek, a także exploity i inne możliwe kwestie bezpieczeństwa. Dla każdego wdrożonego produktu na klientach sieciowych, administrator powinien zawsze wiedzieć, w której są wersji, czy są jakieś znane błędy lub luki w zabezpieczeniach, a także czy poprawki lub aktualizacje są dostępne. Jest to ważne zarówno dla sieci korporacyjnych oraz małych i średnich firm: nawet jeśli małe przedsiębiorstwa nie mają budżetu przeznaczonego dla administratora systemu w pełnym wymiarze godzin, zbieranie informacji stanowi podstawę odpowiedzialnej procedury zarządzania poprawkami. Powołując się na strony internetowe oprogramowania firm trzecich, takie jak strony informacyjne lub rozwiązania do zarządzania poprawkami, które oferują powiadomienia o nowych poprawkach. Mogą zaoszczędzić czas.



*Rysunek 4: Poradnik zabezpieczeń dostawcy oprogramowania**

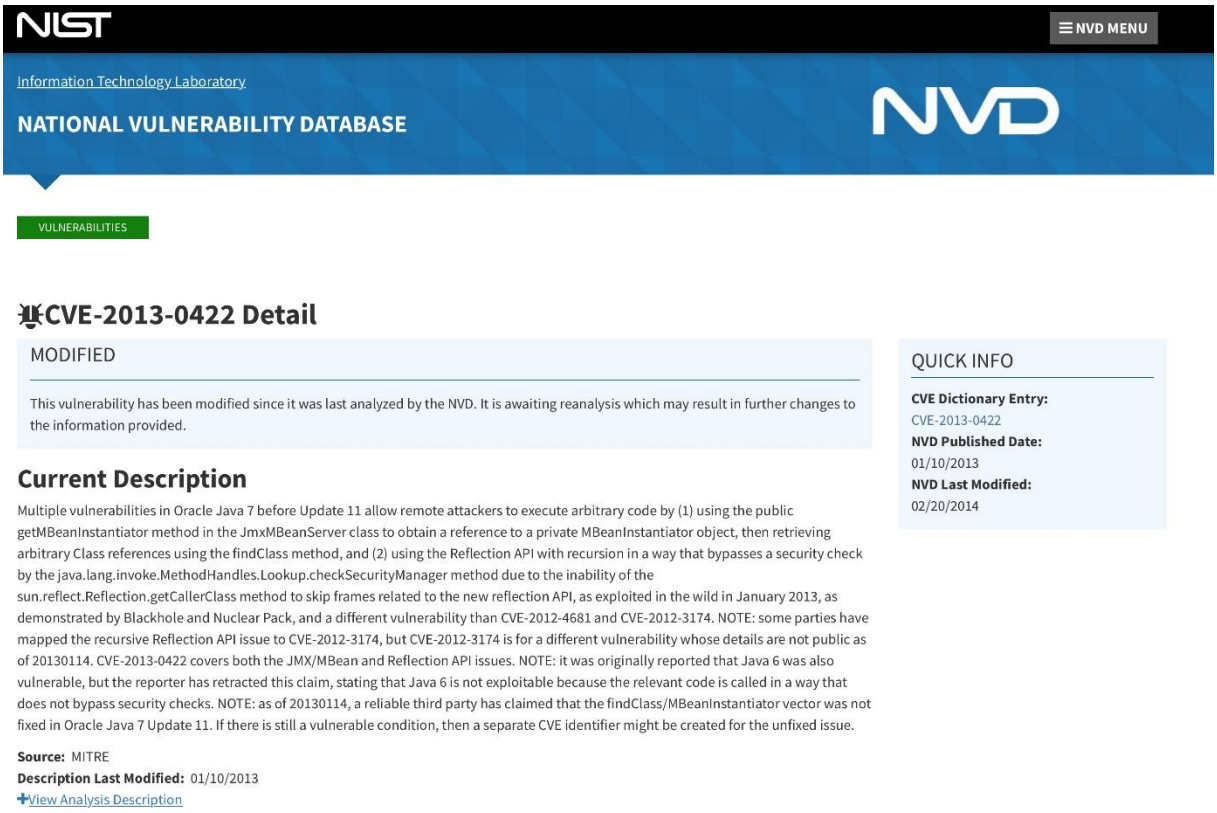
Prostym sposobem sprawdzania aktualizacji jest kontaktowanie się z odpowiednimi dostawcami. Producenci dla większości oprogramowania publikują aktualizacje oprogramowania na swojej stronie internetowej, w tym często

*zobacz: http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html

z wyszczególnieniem najnowszym poprawek i uzupełnień. Niektóre strony internetowe mają dostępne usługi RSS lub adres e-mail dla powiadomień. Jest to tani i bardzo skuteczny sposób, aby być na bieżąco. Uzyskiwanie

informacji bezpośrednio ze źródła jest bardzo niezawodnym sposobem zapewnienia autentyczności poprawki. Konieczność sprawdzania dostępności aktualizacji dla każdego produktu obejmuje oddzielnie dużo niepotrzebnej pracy. Wiele rozwiązań programowych do zarządzania poprawkami posiada własną bazę informację o wersji oprogramowania, co pozwala administratorom na szybkie porównanie ich inwentarza z najnowszymi dostępnymi informacjami o poprawce. Choć istnieje ryzyko, w zależności od firmy trzeciej w informowaniu o aktualizacjach, bo jeżeli administrator nie uzyska informacji bezpośrednio od producenta, skorzystanie z bazy danych firm trzecich znacznie uprości proces zbierania informacji. Bazy danych firm trzecich udzielają informacji o wyższej jakości, często są wzbogacone o dodatkowe klasyfikacje poprawek i weryfikacji dokumentacji na temat zgodności z dobrze znanymi produktami oprogramowania biznesowego.

Chociaż informacje na temat samych poprawek są niezbędne do zarządzania środowiskiem oprogramowania, nie obejmują one całego spektrum. Przed wydaniem poprawki, istnieje kilka etapów rozwoju podczas których już wiadomo, że poprawka jest w przygotowaniu. Gdy dostawca oprogramowania jest świadomy kwestii bezpieczeństwa, często publikuje poradniki bezpieczeństwa, jak na zdjęciu powyżej. Poradniki zazwyczaj zawierają szczegółowe informacje na temat powagi problemu, a także oś czasu rozwoju poprawki. Mogą być dostępne obejścia tymczasowe w celu umożliwienia administratorom złagodzić ten problem, zanim zostanie wydana poprawka przez dostawcę oprogramowania.



Rysunek 5: Baza danych znanych luk i zagrożeń bezpieczeństwa[1]

Dostawcy mogą zdecydować się powiadomić Common Vulnerabilities and Exposures Numbering Authority, który zarządza bazą danych znanych luk i zagrożeń (CVE). Wiele luk ma przypisany numer CVE, umożliwiając łatwą

[1]zobacz: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0422

komunikację na temat kwestii bezpieczeństwa jeszcze przed wydaniem poprawki. Centralna baza danych CVE może pomóc administratorom śledzenie luk w oprogramowaniu, które będą musiały być poprawione w pewnym momencie. W tej chwili, centralna baza danych jest utrzymywana przez Narodowy Instytut Standardów Stanów

Zjednoczonych i Technologii (NIST)[2], którego witryna jest na zdjęciu powyżej. Chociaż w bazie CVE jest szeroko stosowanym centralne repozytorium, nie wszystkie luki bezpieczeństwa są tam przekazywane. Dla większości administratorów, śledzenie wszystkich nowych numerów CVE okaże się zbyt pracochłonne. Niezależne strony, a także sponsorowane przez rząd zespoły reagowania kryzysowego (CERT) są użytecznymi źródłami informacji. Amerykański Departament Bezpieczeństwa Wewnętrznego, na przykład, aktualizuje posty podatności oraz ogólne informacje na swojej witrynie[3]. Europa dysponuje wieloma organami krajowymi, jak również centralnie skoordynowane CERT-UE[4] oraz Agencje Europejskiej Sieci Informacji i Bezpieczeństwa[5]. Większość z tych stron udziela porad bezpieczeństwa codziennie aktualizując wiadomości.

Zarówno dostawcy informacji i baz danych CVE dostarczają informacji względnie technicznych, w oparciu o incydenty. Informacje z CERT są zazwyczaj bardziej dostępne, a także mogą pouczać oraz informować o ogólnych trendach w złośliwym oprogramowaniu. Wiele mediów oferuje artykuły online na temat aspektów bezpieczeństwa komputerowego. Dostawcy oprogramowania antywirusowego często sami wydają biuletyny informacyjne lub prowadzą blogi dotyczące najnowszych zagrożeń.

3.3. Etap III: Strategia i planowanie

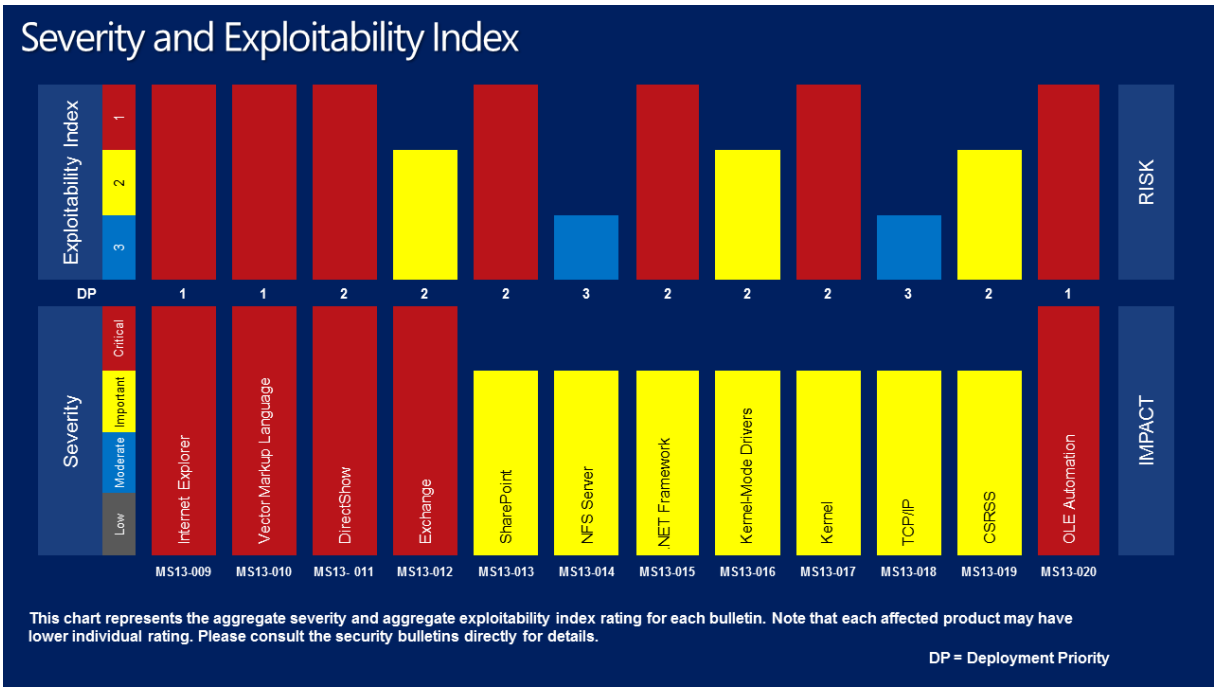
Jak tylko zostały uzyskane informacje o wydaniu poprawki i aktualizacji, zaczyna się faza strategii i planowania. Wiele pytań, na które należy odpowiedzieć podczas tego etapu powinna być już uwzględniona w polityce zarządzania poprawkami. Na przykład, ważne jest, aby wybrać, które poprawki zainstalować jako pierwsze, a które wcale. Na podstawie dotkliwości luki bezpieczeństwa, może być konieczne, aby zainicjować szybsze wprowadzenie poprawek niż zwykle lub rozmieszczanie szybkiego obejścia.

Po pierwsze ważne jest uświadomienie sobie, że nie wszystkie dostępne poprawki i aktualizacje muszą zostać zainstalowane. Polityka zarządzania poprawkami powinna określać, jakie zostaną zainstalowane w sieci rodzaje poprawek i aktualizacji, aby uniknąć skomplikowanych pytań pochodzących od spowolnionego procesu decyzyjnego. Na przykład, gdy dostawca może uznać pewną aktualizację za konieczną, firma nie musi dodawać specyficznej funkcji, której aktualizacja dotyczy. Dostawcy mogą nawet zdecydować się na usunięcie funkcji, od której zależy bezpieczeństwo przedsiębiorstwa. Nie zwracając uwagi na aktualizację we wczesnym stadium pozwala to zaoszczędzić czas poprzez unikanie dalszych rozważań, wdrażania i zarządzania, dzięki czemu administratorzy mogą przydzielić zasoby dla odpowiednich aktualizacji i poprawek. W pewnych okolicznościach, nawet poprawki zabezpieczeń mogą być ignorowane, jeśli naprawiają luki w zabezpieczeniach, które nie mogą być nadużywane w kontekście wdrożenia korporacyjnego oprogramowania. Jednak w tym przypadku zaleca się "lepiej dmuchać na zimne". Polityka zarządzania poprawkami jest zalecana.

Niezależnie od źródła, informacje na temat kwestii związanych z bezpieczeństwem lub poprawki prawie zawsze zapewniają ocenę szkodliwości, która pozwala zdecydować, czy wdrożyć poprawkę, czy nie, a jeśli tak, to jak szybko. Sami albo poprzez stosowną agencję dostarczającą ocenę dotkliwości luki bezpieczeństwa. Powyższe zdjęcie przedstawia typową szkodliwość i możliwości wykorzystania wskaźnika publikowanego przez Microsoft. Zawiera szczegóły ryzyka wszystkich luk w zabezpieczeniach, które będą poprawione w określonym miesiącu, jak również wpływ, na który komponent może być przeprowadzony atak. Ocena wrażliwości pomaga zdecydować, które z nich mają załatać jako pierwsze, jeśli mają one zastosowanie dla produktu, który jest używany w sieci firmowej.

---

[1] zobacz: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0422
[2] zobacz: nvd.nist.gov
[3] zobacz: www.us-cert.gov
[4] zobacz: cert.europa.eu
[5] zobacz: www.enisa.europa.eu



*Rysunek 6: Wskaźnik firmy Microsoft na temat dotkliwości i możliwości wykorzystania luki**

Im bardziej dotkliwa luka bezpieczeństwa, tym szybciej powinna być załatana poprzez wprowadzenie poprawki. Ocena szkodliwości jest zależna od kilku parametrów. Jeśli atakujący może wykorzystać lukę tylko lokalnie, wymaga fizycznego dostęp do komputera, na którym zainstalowano oprogramowanie, szkodliwość byłaby oceniana niżej niż ataku, który można przeprowadzić na odległość (tj. przez Internet). Przez niektóre ataki, hakerzy mogą tylko dokonać awarii dotkniętego oprogramowania. Inne kwestie pozwalają im na odczyt lub zapis danych do systemu plików lub uruchomienie dowolnego programu - pozwala na dostęp do danych i kradzież oraz mogą być zagrożone podłączone urządzenia. Te poważne luki bezpieczeństwa powinny być poprawione tak szybko, jak to możliwe. Innym czynnikiem jest dostępność wiedzy o luce. Jeśli został wykryty przez producenta, jest tylko niewielka szansa, że jest aktywnie wykorzystywana przez hakerów, którzy musieliby oddzielnie odkryć tę samą wadę. Jednakże, jeśli luka w zabezpieczeniach została ujawniona publicznie przez badaczy bezpieczeństwa, lub jeżeli dostawca uzyskał informację o problemie z przedsiębiorstwa handlowego, o wiele więcej stron może mieć dostęp do informacji na temat wady i przeprowadzić z powodzeniem atak. Producenci będą musieli przystąpić do wydania poprawki jak najszybciej i dodatkowo wdrożenia powinny zostać odpowiednio zaplanowane. Problem związany jest faktem, że wydanie poprawki często sygnalizuje początek okresu intensywnych ataków: hakerzy wykorzystują inżynierię wsteczną dla poprawki, aby dowiedzieć się, w jaki sposób luka działa i starają się jak najszybciej wykorzystać systemy bez poprawek.

W każdym razie, role klienta sieci, które zostały określone w polityce zarządzania poprawkami powinny być brane pod uwagę. Klienci we wrażliwych rolach (na przykład komputery, które są wykorzystywane do komunikacji zewnętrznej, albo stanowią wrażliwą część infrastruktury) wymagają szybszego aktualizowania oprogramowania niż łatanie maszyn, które są wykorzystywane do wykonywania zadań, które nie obejmują informacji poufnych. Dla każdej dostępnej poprawki, należy dokładnie sprawdzić, czy powinna być wdrożona w całej sieci, czy tylko do klientów w określonych rolach, albo wcale. Sieci w małym przedsiębiorstwie nieco łatwiej utrzymać w tym zakresie, ponieważ ilość ról jest bardziej ograniczona. Mimo to, należy dokonać rozróżnienia między różnymi rodzajami ról klienckich w sieci. Wdrożenie tej samej konfiguracji poprawek do wszystkich maszyn zazwyczaj nie jest zalecane.

*zobacz: http://blogs.technet.com/b/msrc/archive/2013/02/12/baseball-bulletins-and-the-february-2013-release.aspx.

Na tym etapie ważne jest również, aby dowiedzieć się, czy wybrane poprawki nie mają żadnych zależności. Niektórzy producenci oprogramowania implementują proste aktualizatory, które pomagają zaktualizować dowolną wersję oprogramowania do najnowszej wersji. Inni używają przyrostowych aktualizacji, która koniecznie będzie cofać wersję, aby znaleźć wszystkie odpowiednie poprawki, które mają być stosowane w określonym porządku. Poprawka oprogramowanie może także wymagać pewnej wersji sterownika, frameworka lub innego produktu, który musi być zainstalowany. Informacje o takich zależnościach są zazwyczaj dostępne w opisie poprawki, dostępne razem z poprawką lub bezpośrednio od producenta oprogramowania. Zależności mogą stać się coraz bardziej skomplikowane, gdy planuje się wstępny etap wdrażania dla systemów, na których nie zostały jeszcze zainstalowane poprawki. Aktualizacje systemu Windows i service packi często zależą od siebie i mogą wymagać dużo uwagi, aby je poprawnie wdrożyć. Zarówno na etapie strategicznym i w trakcie fazy testowej, szczególną uwagę należy zwrócić na ewentualne poprawki, które wymagają dodatkowych instalacji.

Wdrożenie jest stosunkowo proste, jednak na niektóre pytania należy sobie odpowiedzieć w fazie planowania. Przede wszystkim, zdecydować o momencie, w którym powinny zostać zainstalowane poprawki. Dla poprawek bezpieczeństwa, administratorzy mogą instynktownie wybrać podejście "im szybciej tym lepiej". Chociaż szybkie wdrożenie rzeczywiście szybko naprawia luki w zabezpieczeniach, ale istnieje jeszcze kilka czynników wchodzących w grę. Aby uniknąć problemów z kompatybilnością, poprawki muszą być testowane, co może potrwać kilka dni. Same rzeczywiste wdrażanie również potrzebuje czasu. W niewielu przypadkach, klienci są zmuszeni do restartu po instalacji poprawki. Jeżeli restart nie jest wymuszony, może minąć trochę czasu, zanim poprawka rzeczywiście wejdzie w życie. W zależności od wielkości sieci, zaplanowana dystrybucja poprawek może wymagać dalszego rozszerzenia harmonogramu wdrażania. Dla pracowników mobilnych i sieci VPN, rozmieszczenie może potrwać dłużej, bo nie zawsze mogą być podłączeni do sieci firmowej, a nie wszystkie aktualizacje mogą być wdrażane natychmiast.(Dla klientów o ograniczonej przepustowości, branie pod uwagę rozmiaru pliku przy ustalaniu priorytetów poprawek może to być nawet przydatne).

Należy upewnić się, że poprawki krytyczne są wdrażane od 48 godzin do jednego tygodnia od ich wydania. Mniej krytyczne poprawki zabezpieczeń i aktualizacje funkcjonalne mogą zostać opóźnione. Jednak, jak wspomniano, planowanie silnie zależy od układu sieci, strategii aktualizacji poprawek i dotkliwości. Nawet w zarządzaniu poprawkami, bezpieczeństwo musi być zrównoważone z użytecznością i dostępnością. Dla niektórych systemów przestój może mieć efekt przeciwny do zamierzonego i wdrożenie poprawek musi zostać opóźnione. Dla innych, jest akceptowalne zmuszenie użytkownika o ponowne uruchomienie systemu. Należy także pamiętać, że to nie ma znaczenia, kiedy poprawka zostanie wdrożona, ale kiedy zaczyna ona obowiązywać. Restarty, strategia dystrybucji lub inne opóźnienia mogą popchnąć skuteczną realizację poprawki, czasami wymagają (tymczasowego) obejścia. Jednak obejście powinno być zawsze środkiem tymczasowym: luki w zabezpieczeniach są ostatecznie tylko wiarygodnie naprawione przez konkretną poprawkę.

Usprawnienie procesu podejmowania decyzji, jest pomocne w określeniu harmonogramu z góry, biorąc pod uwagę wszystkie właściwości sieci i uwzględnienie dotkliwości exploita jako jedyną zmienną. Definiowanie poziomu zgodności rozmieszczenia poprawek określa ilościowo wielkość wysiłku. Powinna być określona jako stały procent po kilku pierwszych dniach i stopniowo wspinać się. Osiągnięcie 100 procent zgodności poprawki jest prawie niemożliwe, ponieważ niektóre urządzenia mogą być używane bardzo rzadko, albo są w trakcie prac konserwacyjnych.

3.4. Etap IV: Testowanie

Procedura testowa jest najważniejszym krokiem w zapobieganiu powikłaniom w trakcie i po wdrożeniu poprawki. Produktywność może zostać ograniczona, jeśli wdrożenie poprawki czyni klientów (tymczasowo) bezużytecznymi. Niestety, szybkość, przy której krytyczne poprawki bezpieczeństwa powinny zostać wdrożone może czasami ograniczyć rozległość testów. Podobnie jak w przypadku planowania, które poprawki wdrożyć, bezpieczeństwo i użyteczność nie zawsze są kompatybilne. Należy zauważyć, że czasami trzeba wszystkie poprawki przejść tą samą procedurą. Małe, proste poprawki nie powodują problemów z obciążeniem sieci, rozmieszczeniem lub kompatybilnością jak w przypadku większych poprawek, więc lżejszy system testowania jest zalecany. W tym

samym czasie, drobne poprawki o zmniejszonym stopniu dotkliwości mogą być badane przez dłuższy okres czasu, ponieważ nie muszą być bardzo szybko rozmieszczone. W każdym przypadku, każda poprawkę należy badać stosując bazową, która zapewnia rozmieszczenie bezproblemowe. Podobnie jak w innych etapach zarządzania poprawkami administratorzy małych przedsiębiorstw mają nieco ułatwione zadanie. Mniejsze scenariusze do testowania, cała procedura może być przeprowadzone znacznie szybciej, co umożliwia szybką instalację poprawki.

W celu przeprowadzenia testów, musi zostać zdefiniowane środowisko testowe. Idealnie środowisko oferuje wszystkie możliwe konfiguracje klienta, które istnieją w sieci. Błędy i wyjątki mogą być tylko zlokalizowane poprzez jak najdokładniejszą emulację wdrożenia, jaka będzie przeprowadzona w rzeczywistej sieci. Oznacza to stworzenie wielu fizycznych komputerów klienckich, każdy z przedstawicielem konfiguracji z jednym z zadań klienta w sieci. Komplikacje pojawiają się, gdy planuje się testy dla maszyny, które odgrywają zasadniczą rolę w sieci, takie jak serwery. Bardzo trudno jest ustawić właściwe środowisko testowe, które bierze pod uwagę wszystkie aspekty konfiguracji sieci. Jedną z opcji jest rozmieszczenie w wirtualnym środowisku testowym serwera wirtualnego i klientów. Podczas gdy nie pozwala na konfigurację oprogramowania i zlokalizowanie problemów jak przy fizycznym aspekcie wdrożenia poprawki (np. przepustowość, szybkość odczytu dysku, CPU). Nie mogą być testowane prawidłowo na maszynie wirtualnej. Alternatywnie, nieistotną część rzeczywistej sieci można wyznaczyć jako obszar do testów. Pozwala to administratorowi przetestować poprawki w bardzo realistycznym środowisku. Rzeczywiste testy sieci może być również bardzo pomocne. Jednakże, oprócz oczywistego zwiększenia ryzyka powikłań, takie podejście łączy etap testowania z etapem wdrożenia. Śledzenie urządzeń stosowanych do testów i oddzielając je od pozostałych klientów może stać się bardzo szybko skomplikowane.

Kiedy odpowiedni zestaw maszyn został wybrany jako środowisko testowe, testowane poprawki mogą zostać wdrożone. Należy sprawdzić opis dostawcy poprawki, aby zobaczyć, czy są jakieś znane problemy lub inne problemy, które wyraźnie muszą być przetestowane w sieci. Pierwszą przeszkodą jest rodzaj instalatora jakiego dostawca zdecydował się użyć. Popularnym standardem jest instalator Microsoft Windows (MSI). Ponieważ większość, jeśli nie wszystkie maszyny Windows mają zainstalowane odpowiednie frameworki, także wielu dostawców rozwija swoje instalatory przy użyciu tej technologii. Instalator Windows pozwala na łatwe zarządzanie wersjami i bez nadzoru instaluje, wymagane technologie, aby umożliwić instalację poprawki. Jednak nie jest to w pełni samoobsługowe rozwiązanie. Aby umożliwić procedurę konfiguracji bez interakcji z użytkownikiem, testy powinny być prowadzone w celu sprawdzenia, czy proces MSI nie rzuca nieoczekiwanymi błędami. Brakujące materiały instalacyjne lub pliki cache są jednymi z najczęstszych przyczyn przerwania instalacji MSI lub procedury instalowania poprawek i może poważnie zakłócić dystrybucję poprawek na wielu klientach sieciowych. Dostawcy mogą także zdecydować na dostarczanie oprogramowania na własnym instalatorze. Podczas gdy wiele firm korzysta standardowego rozwiązania, co z kolei może być ponownie oparte na podstawie instalatora MSI może powodować zamieszanie. Słabo udokumentowane lub nieudokumentowane zachowanie instalatorów i standardów instalowania poprawek może skomplikować rozmieszczenie poprawek. Uruchomienie tego typu instalatora w środowisku testowym jest okazją do spojrzenia na jego zachowanie i dostosowanie jego parametrów do masowego wdrożenia.

Z punktu widzenia użyteczności, ważne jest sprawdzenie, czy instalowana poprawka wymaga ponownego uruchomienia komputera. Gdy pliki, które zostaną poprawione są używane podczas wdrażania poprawki, mogą być zastąpione jedynie gdy klient zostanie ponownie uruchomiony. Może okazać się konieczne sprawdzenie, jakie usługi w tle wykorzystują pliki, które zostaną poprawione i zamknąć je tymczasowo przed rozpoczęciem procedury instalowania poprawek. Dla bardziej złożonych poprawek, takich jak poprawki zabezpieczeń systemu Windows lub service packów, restart jest prawie zawsze wymagany, niezależnie od środków zapobiegawczych. Jeśli okaże się, że ponowne uruchomienie jest wymagane, rozmieszczenie powinno być starannie zaplanowane w następnym kroku procedury instalowania poprawek (harmonogram i ocena) lub należy zintegrować procedurę z harmonogramami użytkowników końcowych lub przerwami w konserwacji.

Po zakończeniu procedury instalowania poprawek, w tym jednego lub większej liczby restartów, jeśli to było konieczne, system generalnie powinien być nadal funkcjonalny. Z wyjątkiem zmian wprowadzonych przez

poprawkę, oprogramowanie powinno nadal funkcjonować, jak to miało miejsce wcześniej. System powinien nadal być w stanie się uruchomić, w rozsądnym czasie, a użytkownik końcowy nie powinien być zaskoczony oknami dialogowymi, komunikatami, czy procesami porządkowymi lub innymi resztkami pozostawionymi przez instalator poprawki.

Nie tylko procedura instalacji powinna zostać przetestowana. Przyszłe problemy ze zgodnością mogą wymagać odinstalowania poprawki gdy użytkownicy napotykają problemy z wcześniej niesprawdzonym scenariuszem. Upewnij się, że oprogramowanie może również być przywrócone do stanu sprzed instalacji poprawek. Może to być bardzo prosta procedura przy standardowym instalatorze (MSI). W przypadku oprogramowania, których pliki programu nie mają zarządzania wersjami lub produktów, które używają niestandardowych instalatorów, może być konieczne utworzenie kopii zapasowej plików przed wdrożeniem poprawki co umożliwi dalsze wycofanie poprawki. Niektóre poprawki są tak wszechobecne, że nie będzie możliwości odinstalowania ich bez ponownego wdrożenia zasadniczej część systemu (takie jak Windows Service Pack). Upewnij się, aby przeczytać całą dokumentację, która towarzyszy poprawce, aby móc przewidzieć problemy z kompatybilnością, powikłaniami po instalacji lub innymi problemami. Jeśli istnieją jakiekolwiek wątpliwości, które nie zostały wyjaśnione w trakcie procedury testowej, należy zdecydować się przenieść poprawkę do następnego cyklu, w oczekiwaniu na dalsze testy lub rozmieścić je w kilku etapach, a następnie dokładnie monitorować wpływ na pierwszych grupach wdrożeniowych.

Procedura testowa instalacji poprawek nie jest przeznaczona jedynie dla zweryfikowania poprawności wdrożenia, ale także ma na celu oszacować skutki wdrożenia dla użytkowników końcowych. Po pomyślnym zainstalowaniu poprawki, oprogramowanie może funkcjonować inaczej niż wcześniej, ze względu na nowe funkcje, które aktualizacja oprogramowania może dodać. W testowym środowisku powinno znaleźć się środowisko pracy użytkownika końcowego, w celu umożliwienia szybkiego porównania sprzed i po zastosowaniu poprawki. W zależności od ilości czasu spędzonego na testowaniu różnych użytkowników końcowych przepływ pracy również powinien być sprawdzony. Wdrożenie poprawek nie musi być całkowicie przejrzyste, ale zmiany powinny być udokumentowane z wyprzedzeniem i przekazane do użytkownika końcowego przed rzeczywistym wdrożeniem.

Gdy proces wdrażania poprawek i aktualizowania oprogramowania funkcjonuje bez problemów, testowanie powinno skupić się na czynnikach zewnętrznych. Jeśli zaktualizowane oprogramowanie nie jest rozpoznawane w przedsiębiorstwie białą i czarną listą oprogramowania, zwłaszcza odkąd pliki wykonywalne zostały zmienione. Upewnij się, aby edytować listę kontrolną aplikacji lub użyć innego poziomu szczegółowości: filtrowanie oprogramowania według nazwy produktu, wersji lub dostawcy. Podobnie polityki Windows mogą kolidować z niektórymi funkcjami poprawionego oprogramowania. Jeżeli procedura testowa odkrywa ewentualne konflikty, spróbuj rekonfiguracji oprogramowania lub dostosuj problematyczne polityki.

3.5. Etap V: Harmonogram i ocena

Rzeczywiste wdrożenie może być przeprowadzone kiedy został ustalony cel wdrożenia poprawki, jej funkcjonowanie i zależności. Krok ten konsoliduje informacje z prawie wszystkich poprzednich zadań w ramach procedury zarządzania poprawkami. Inwentaryzacja sieci, zależności i zachowanie poprawek prowadzą do jednego planu wdrażania. Ten etap polityki zarządzania poprawkami zapewnia pewne możliwości ponownego wykorzystania lub konsoliduje z wcześniejszą praktyką dla przedsiębiorstw, które przyjęły standard taki jak ISO 27002 i mogą już posiadać zarządzanie zmianami i politykę oceny ryzyka. Przynajmniej, muszą zostać opracowane procedury obsługi wyjątków wdrażania, a także formalna ocena ryzyka dla każdej poprawki.

Teraz, jeżeli już znane są poprawki, które będą wdrożone i zostały im przypisane priorytety dotkliwości. Przy czym dotkliwość nie jest jedynym czynnikiem w podejmowaniu decyzji, kiedy wdraża się poprawkę. Większość poprawek może mieć szczególne wymagania systemowe lub problemy ze zgodnością, które należy zminimalizować przed rozpoczęciem wdrożenia. Ponadto, nie wszystkie stacje robocze mogą być aktualizowane w tym samym czasie. Niektóre z nich są używane, inne są bardzo ograniczone harmonogramem systemu Windows.

W każdym przypadku, jest zalecana stopniowa dystrybucja poprawek, w przeciwieństwie do grupy klientów z aktualizacją w tym innym czasie. Niespodziewane konflikty mogą być dostrzeżone wcześniej w całej sieci; w skrajnych przypadkach dystrybucja poprawek może być nawet wstrzymana. Jeśli w testowanej procedurze wskazano możliwe trudności z pewną poprawką, wdrożenie harmonogramu dla danej poprawki zaleca się tylko na kilku pierwszych klientach, następnie należy rozszerzyć zasięg harmonogramu tylko wtedy, gdy dystrybucja poprawek dla pierwszych maszyn skończyła się powodzeniem.

W oparciu o inwentaryzację oprogramowania i role sieciowego klienta, stacje robocze mogą być podzielone na kilka grup zorganizowane według momentu, kiedy poszczególne stacje zostaną zaktualizowane. Chociaż, zgodnie z ogólną zasadą, maszyny najbardziej podatne na luki bezpieczeństwa powinny być najpierw zaktualizowane. W praktyce wygląda to inaczej. Ważne jest, aby uniknąć niepotrzebnych opóźnień we wdrażaniu poprawek. Aktualny proces dystrybucji należy rozpocząć zaraz po zakończeniu fazy testowania i oceny.

Ograniczenia fizyczne również odgrywają rolę w planowaniu dystrybucji poprawek. Instalacja poprawki może znaczne obciążyć infrastrukturę sieciową. Wdrażana poprawka może być zaplanowana poza godzinami pracy jeśli przepustowość sieci jest ograniczona. Dla klientów, które mają ograniczoną ilość wolnego miejsca, przed wdrożeniem poprawek należy zaplanować zadania oczyszczania twardych dysków.

Jeśli harmonogram został opracowany, w tym momencie klienci mogą być powiadamiani o planowanym wdrożeniu. Szczególnie jeżeli faza wdrażania doprowadzi do wymuszonego restartu lub innych rodzajów awarii klienta końcowego. Pozwala użytkownikom dowiedzieć się wcześniej i przyczynia się do rozwoju wiedzy. W obecnej fazie wdrażania, administrator może nawet wybrać umożliwienie użytkownikom opóźnienia instalacji poprawki lub restartu, jeśli komputer kliencki jest potrzebny w tym czasie.

Aktualizowanie serwerów produkcyjnych powinno być wykonane bardzo starannie, aby być pewnym, że serwer uruchomi się ponownie i nieoczekiwany przestój nie spowoduje zbyt wiele niedogodności. Należy zarezerwować z wyprzedzeniem szczelinie czasową a następnie ogłosić planowaną aktualizację wszystkim zainteresowanym użytkownikom. Jeśli wystąpią jakieś komplikacje podczas procesu aktualizacji oprogramowania powinien być dostępny serwer awaryjny.

3.6. Etap VI: Wdrożenie poprawki

W momencie wdrożenia łączą się wszystkie poprzednie etapy. Zaczyna się zadanie fizycznej dystrybucji poprawek dla wszystkich klientów sieciowych. Jednak wdrożenie jest czymś więcej niż po prostu instalowaniem poprawek do klientów. W starszych systemach, na przykład, może być przydatne do pierwszego wymuszonego pełnego skanowania, szczególnie wtedy, gdy system nie został zaktualizowany w ostatnim czasie. Uporczywy malware zostanie oczyszczony przez skaner antywirusowy, w celu umożliwienia instalacji poprawek.

Po wdrożeniu, weryfikacja i raportowanie pomoże ocenić wpływ wdrożenia poprawek oraz odkryć problemy. Zanim cokolwiek zostanie wdrożone do klientów, należy zatem określić, które działania będą rejestrowane i zgłaszane. Teoretycznie każde działanie, które wpływa na układ klienta powinno być rejestrowane, aby umożliwić późniejszą analizę. Harmonia wszystkich działań systemu plików i mutacja rejestru jest jedną z możliwości, ale należy uważać, aby nie gromadzić zbyt dużo danych. Niekończące się dzienniki aktywności utrudniają szybką analizę.

Niektórzy producenci wydają różne poprawki, publikują tylko zmiany, między jedną wersją a następną. Chociaż w ten sposób zaoszczędzą znaczną ilość miejsca na dysku i przepustowość ale muszą wypuścić osobną poprawkę dla każdej wersji docelowej. Aby zaoszczędzić czas przy budowaniu poprawek, większość produktów jest wydawana ze wszystkimi plikami poprawek, które zawierają pełne wersje plików, które mają być poprawione. Upraszcza to przypadki, w których przestarzałe stacje robocze będą musiały być poprawione przy użyciu wielu plików, ale średni rozmiar pliku poprawki jest znacznie zwiększony. Faza wdrażania poprawek może zatem poważnie wpłynąć na przepustowość sieci. Wszystkie poprawki są pobierane przez centralny serwer zarządzający poprawkami, który następnie dystrybuuje je do wszystkich obowiązujących klientów sieciowych. Przeszkadzające

inne zadania sieciowe mogą uniemożliwić uruchomienie procesu aktualizacji oprogramowania. Należy spróbować ograniczyć jednoczesne obciążenie sieci. Wdrożenie powinno być planowane w takim czasie, gdy sieć nie jest silnie używana. Dodatkowo, rozmieszczenie powinno być etapowe. Nie wszyscy klienci muszą być aktualizowani w tym samym czasie, ze względu na kompatybilność i wydajność. Grupy klientów, które są fizycznie blisko można skupić według wykorzystania sieci lub dodać kilka klientów z każdej strefy sieci do grupy, aby rozłożyć obciążenie równomiernie. Nawet jeśli faza testowa została zakończona bez większych wyjątków lub incydentów, nadal zaleca się grupować klientów w oparciu o ryzyko: przed przejściem do bardziej skomplikowanych maszyn w sieci należy wdrożyć poprawki dla pierwszych standardowych klientów stacjonarnych lub pojedynczej grupy serwerów.

Poprawki nie muszą koniecznie instalować się bezpośrednio po tym, jak zostały wypuszczone do klienta. Indywidualne okoliczności mogą opóźnić instalację poprawki. Jeżeli poprawki są dystrybuowane podczas godzin pracy, gdy stacje robocze są w użyciu. Lepiej jest opóźnić instalację poprawki do momentu wyłączenia, restartu lub zamknięcia działań stacji roboczej. Alternatywnie, skonfigurować oprogramowanie do zarządzania poprawkami do wypuszczanie plików poprawek tylko raz podczas rzeczywistego procesu instalowania poprawek, łącząc zarówno działania oraz umożliwienie całemu procesowi podjęcie działań podczas zaplanowanej konserwacji. Podobnie, jeśli restarty są wymagane, powinny być planowane w celu zminimalizowania niedogodności. Instalacja poprawek i restarty mogą być wymagane, jeżeli argument zagrożenia bezpieczeństwa przeważa użyteczności i nie powinno być to zaniedbanie. Alternatywnie, użytkownik może mieć możliwość, opóźnienia instalacji poprawki lub uruchomienia w określonym czasie, aby zakończyć swoją obecną pracę. Umożliwienie właściwej synchronizacji wdrożenia oprogramowania z pozostałymi klientami sieciowymi, powinno być ograniczone na przykład maksymalnie do jednego dnia na instalację poprawki lub jedną godzinę dla restartów.

Przed uruchomieniem i instalacją plików poprawki należy zweryfikować autentyczność pliku. W kilku etapach pliki mogą ulec uszkodzeniu, umyślnie lub nie. Serwery dostawców nie są godne zaufania, ponieważ pliki poprawek mogą nadal ulec uszkodzeniu podczas początkowego pobierania. Aby sprawdzić autentyczność pobieranego pliku poprawki, dostawcy często udostępniają sumę kontrolną pliku lub hashe, którymi można sprawdzić pobrane pliki. Po kolejnym wdrożeniu poprawki w sieci, jest ponownie zalecane sprawdzenie plików poprawki w oparciu o ich hashe aby zapobiec nieoczekiwanym zdarzeniom z powodu uszkodzenia plików. Dla dodatkowego bezpieczeństwa, dystrybucję poprawki przez sieć można szyfrować, ale strata wydajności może nie być warta zwiększeniu niezawodności.

Zaleca się, aby aktywnie monitorować wdrażanie poprawek. Jeśli poprawka nie trafia do instalatora, to może mieć konsekwencje dla innych instalowanych poprawek, które zależą od nich. Brak wolnego miejsca na dysku jest bardzo częstym powodem porażki podczas instalacji poprawek, a powodów może być wiele innych. Instalatory poprawek często zwracają kody błędów, gdy coś pójdzie nie tak podczas pracy w trybie bez nadzoru. Jest często konieczna interwencja ręczna podczas wdrażania poprawek gdy coś idzie źle. Z tego powodu w polityce zarządzania poprawkami należy określić sposób obsługi wyjątków i ramy czasowe.

3.7. Etap VII: Weryfikacja i raportowanie

Chociaż weryfikacja powinna odbyć się już podczas procesu wdrożenia poprawki. Z chwilą, gdy zostaną wdrożone do wszystkich klientów sieciowych wyznaczają początek formalnej weryfikacji oraz procesu raportowania. Przegląd po wdrożeniu składa się z analizy logów wdrażania i wyjątków, jak również formalną kontrolę, aby sprawdzić, czy wszystkie planowane wdrożenia zostały przeprowadzone prawidłowo. Jeżeli wszelkie wyjątki wystąpią podczas procesu aktualizacji poprawek, dalsze wdrażanie poprawek może zostać usprawnione poprzez analizowanie co dokładnie się stało i określenie przyczyn problemu. Niektóre błędy mogą wystąpić z powodu problemów ze sprzętem poszczególnych klientów; inne mogą być śledzone ogólnymi politykami domeny lub kwestiami obciążenia sieciowego.

Oprócz zbadania dzienników, które zostały utworzone podczas wdrożenia, podsumowanie instalacji może być sprawdzone na kilka sposobów. W ramach polityki wdrażania poprawek, pełna inwentaryzacja oprogramowania na każdym kliencie sieci powinna być dostępna. Odświeżanie inwentarza i porównanie go w stosunku do wersji poprzedniej zapewnia dokładny sposób, aby sprawdzić, czy program rzeczywiście został zaktualizowany do wybranej wersji. Jednak nie wszystkie poprawki zwiększają numer wersji oprogramowania. Mniejsze poprawki, poprawki bez dobrego instalatora, a nawet niedopatrzenie dostawcy może prowadzić do niekonsekwentnego numerowania wersji albo nie numerowania programu w ogóle przez producenta. Czytanie sumy kontrolnej pliku może pomóc, ale przy większej ilości danych może być przytłaczające. Jeśli jest dostępna dokumentacja, dane techniczne o luce mogą ujawnić w prosty sposób sprawdzenie, czy poprawka została prawidłowo zainstalowana: próba przeprowadzenia ataku exploitem, zweryfikuje czy problem został naprawiony. Wyspecjalizowane skanowanie luk wykona automatyczne skanowanie sieci w celu sprawdzenia, czy jakieś luki nadal istnieją.

Jeśli poprawka nie została prawidłowo zainstalowana, istnieje kilka środków zaradczych. Jeśli obciążenie sieci lub przestrzeń wolnego miejsca na dysku była problemem, zmniejszając obciążenie lub uwalniając przestrzeń pozwoli na wdrożenie poprawki. Po drugiej próbie instalacja poprawki zostanie przeprowadzona pomyślnie. Jednakże, jeśli istnieją problemy z kompatybilnością z istniejącym oprogramowaniem lub innymi wyjątkami, może być konieczne przeczytanie podręcznika instalacji poprawki. Mając zdalny dostęp do klienta można spróbować uruchomić instalator poprawki ręcznie.

Nie automatycznym ale cennym sposobem na weryfikację wdrożenia właściwej poprawki jest udział użytkownika końcowego. Mimo, że rzeczywiste pliki poprawek zostały prawidłowo zainstalowane, problemy ze zgodnością mogą wystąpić w przypadku innego oprogramowania zależy od dokładnej wersji naprawionego produktu. Ponadto łatwiej rozpoznać problemy z wydajnością w codziennej pracy użytkownika końcowego, niż w sztucznym środowisku testowym. Szczególnie w przypadku wdrożenia na nietypowych klientach. Ryzyko problemów jest większe. Dając użytkownikom możliwość dostarczania informacji zwrotnej o poprawkach, administratorzy mają świadomość o problemach, których nie mogli dowiedzieć się sami. W wiadomości zwrotnej użytkownika końcowego często brakuje koniecznej informacji do zidentyfikowania problemu, ale może być doskonałym wskaźnikiem wydajności poprawki.

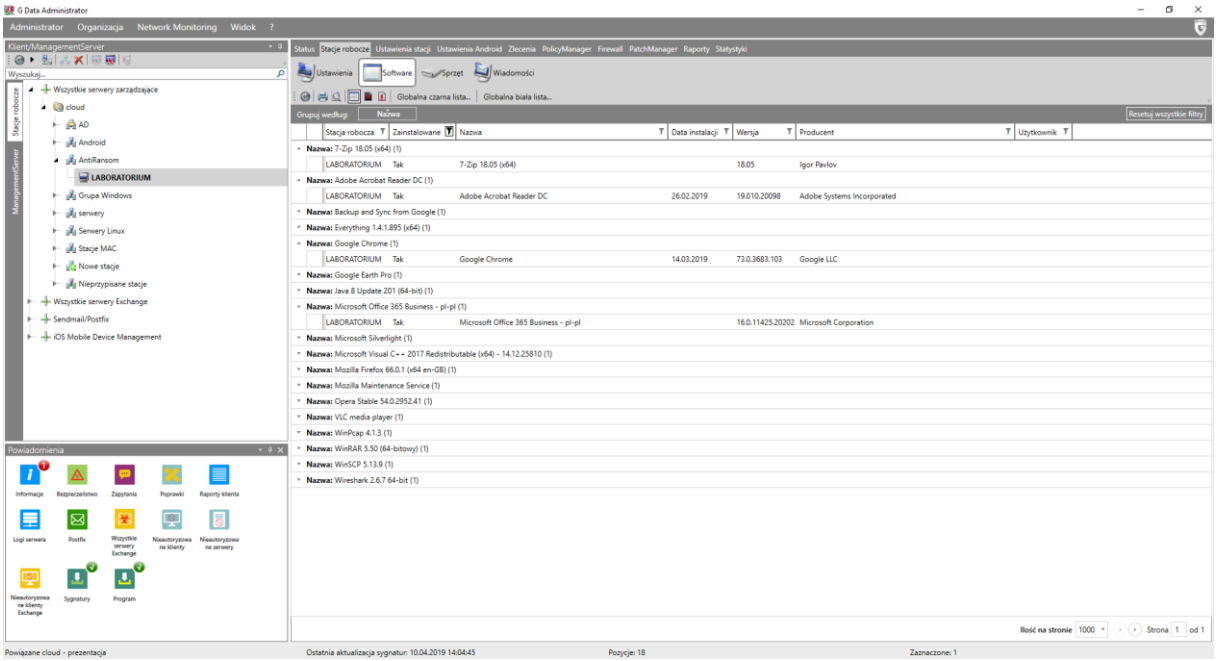
Z lub bez wiadomości zwrotnej od użytkownika, zawsze powinno być technicznie możliwe wycofanie poprawki. Faza testowa powinna zagwarantować, że poprawki, które zostały wdrożone nie powodują problemów, ale w indywidualnych przypadkach, utrata wydajności lub funkcjonalności zawsze może wystąpić. Administrator powinien być w stanie zainicjować procedurę centralnego wycofywania poprawek.

4. Zautomatyzowanie zarządzania poprawkami

G DATA oferuje zarządzanie poprawkami w ramach swoich rozwiązań biznesowych. Funkcjonalność jest dostępna jako opcjonalny moduł dla wszystkich użytkowników produktów biznesowych w połączeniu z istniejącymi modułami G Data AntiVirus, Client Security i Endpoint Protection.

4.1. Etap I: Inwentaryzacja oprogramowania

Po pierwsze, ważne jest utrzymywanie aktualnego wykazu maszyn w sieci, ich oprogramowania oraz sprzętu komputerowego. Aby wspierać procedurę zarządzania aktualizacjami, należy wiedzieć, jakie wersje oprogramowania są w użyciu w sieci firmowej w danym momencie. G Data zapewnia sprawną inwentaryzację. Moduł Klienci umożliwia administratorom dostęp do pełnej listy zainstalowanego oprogramowania dla każdego klienta sieci. Inwentaryzacja może być zorganizowana tak, aby zapewnić różne rodzaje ewidencji. Domyślny widok pokazuje płaską listę całego oprogramowania zainstalowanego dla wybranych klientów. Lista zawiera datę instalacji, producenta oprogramowania oraz aktualnie zainstalowaną wersję. Poprzez grupowanie elementów według nazwy dla każdego produktu szybki przegląd umożliwia sprawdzenie, czy najnowsza wersja oprogramowania została zainstalowana na wszystkich komputerach.



Rysunek 7: G DATA Administrator, widok inwentaryzacji oprogramowania

Na tym etapie zaleca się sprawdzenie czy klienci sieci mają uruchomione oprogramowanie, które nie jest częścią standardowej aktualizacji oprogramowania. Administratorzy mogą nie być świadomi potencjalnych zagrożeń bezpieczeństwa dla wszystkich programów istniejących w sieci. Korzystanie z inwentaryzacji oprogramowania pomaga w tym miejscu wyświetlenie niedozwolonego oprogramowania.

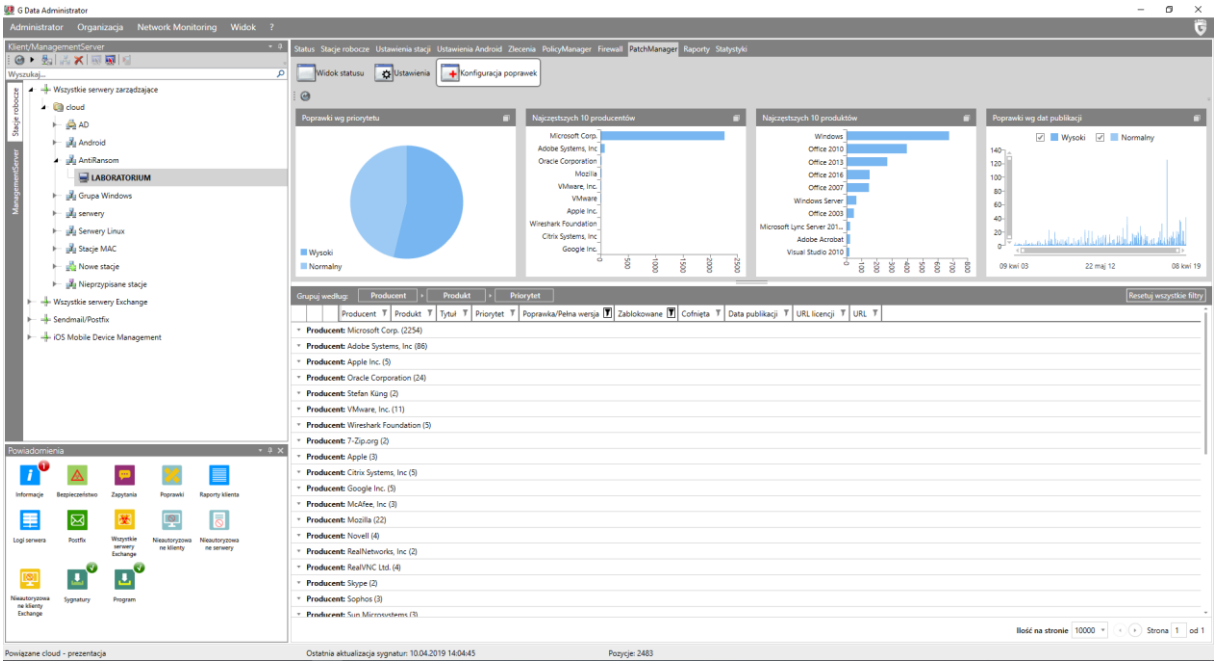
Administratorzy mogą zdecydować, czy dodać oprogramowanie do oficjalnej listy aktualizacji oprogramowania(biała lista) lub je usunąć i zablokować przed instalowaniem lub uruchamianiem(czarna lista). Użytkownicy G Data Endpoint Protection mogą użyć modułu PolicyManager do stosowania w całej sieci polityk do kontroli instalowanego oprogramowania na podstawie białej lub czarnej listy.

Nie tylko jest ważne śledzenie oprogramowania. Udane wdrożenie aktualizacji zależy również od fizycznych warunków, takich jak obciążenie sieciowe oraz od sprzętowej specyfikacji. Te ostatnie warunki mogą być wyświetlone przy użyciu modułu Sprzęt. Szeroki zakres specyfikacji taki jak prędkość CPU, ilość pamięci RAM, może pomóc przewidzieć szybkość wdrażania poprawki.

Ważne jest sprawdzenie ilości wolnego miejsca na dyskach, aby zapobiec rozmieszczeniu aktualizacji oprogramowania i nie generowanie błędów. Dodatkowo może być śledzona wersja BIOS oraz oprogramowania płyty głównej. Umożliwia to porównanie z wersją opublikowanego przez producenta firmware'u.

4.2. Etap II: Zbieranie informacji

Jeżeli inwentaryzacja została ukończona, administratorzy powinni nadążać z informacjami o najnowszych łatkach i porównywać je z istniejącymi zasobami. Moduł PatchManager zapewnia listę najnowszych dostępnych łatek dla szerokiej gamy produktów na karcie Konfiguracja poprawek. Baza jest aktualizowana automatycznie, gdy tylko producenci publikują nową łatkę. Listę można sortować według daty ukazania się, aby zobaczyć, które łatki zostały niedawno opublikowane. Więcej informacji, a często pełne informacje o wydaniu, mogą być widoczne poprzez kliknięcie prawym przyciskiem myszy na łatkę i sprawdzenie jego właściwości.



Rysunek 8: G DATA Administrator, PatchManager konfiguracja poprawek

4.3. Strategia i planowanie

Administratorzy mogą bezpośrednio sprawdzić jedną lub więcej poprawek przed ich dystrybucją na systemach klienckich. Aby sprawdzić pojedynczą łatkę należy kliknąć prawym przyciskiem myszy na łatce i wybrać Sprawdź stosowalność poprawek. Zostanie uruchomione zlecenie rozpoznawania dla określonego klienta(ów). Ewentualnie może zostać przeprowadzone automatyczne skanowanie dla każdej nowej łatki, która jest dodawana do bazy danych. Korzystanie z modułu zleceń pozwala zaplanować rozpoznawanie oprogramowania. Zadanie to jest wykonywane natychmiast dla nowej łatki gdy jest dostępna. PatchManager sprawdza nowe łatki czy mają zastosowanie dla określonych klientów.

PatchManager nie instaluje automatycznie poprawek, aby umożliwić administratorom wybranie poprawek oraz planowanie testów. Po sprawdzeniu stosowalności poprawek, należy wybrać odpowiedni serwer lub klienta(ów) w obszarze zarządzania Klienta i otworzyć zakładkę PatchManager -> Widok statusu.

Należy pogrupować poprawki przeciągając kolumnę Stan na pasek grupuj według powyżej listy. To pomaga szybko zlokalizować łatki, które mają zastosowanie, nie mają zastosowania lub zostały już zainstalowane. Poprawki, które mają zastosowanie dla systemu(ów) klienta są to te, które muszą zostać poddane weryfikacji, testom i zostać ostatecznie wdrożone.

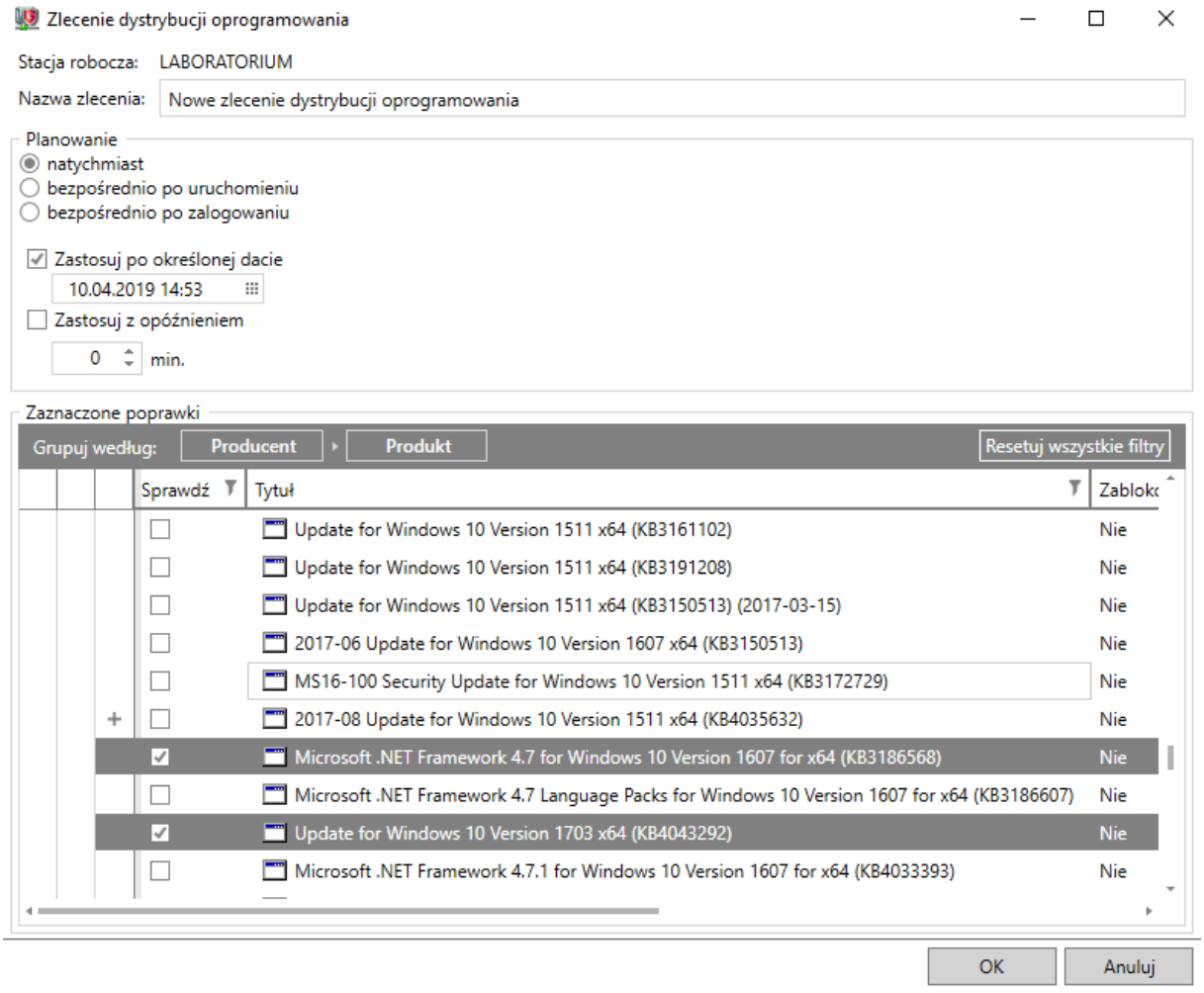
Aby pomóc zdecydować, czy należy wdrożyć pewne poprawki, czy też nie, PatchManager zawiera zestaw informacji dla każdej poprawki. Na zakładce Konfiguracja poprawek moduł PatchManager wyświetla, że poprawka dotyczy danego produktu jak również zawiera datę premiery, oficjalny tytuł, priorytet, pełny opis i zazwyczaj adres URL do oficjalnych informacjach o wydaniu. Te informacje pomagają Administratorom zdecydować, jaka jest waga problemu zabezpieczeń i jak szybko poprawka musi zostać wdrożona. Poprawki z większą dotkliwością powinny być instalowane z wyższym priorytetem niż te niekrytyczne. W tym samym czasie, nie wszystkie programy, które są używane przez sieć są ważne: aplikacje krytyczne powinny być zawsze zaktualizowane przed aplikacjami mniej krytycznymi. Polityka zarządzania poprawkami jest istotna, pomaga szybko zdecydować, które poprawki przeznaczone są do wdrożenia i w jakiej kolejności.

Ważną rzeczą do zapamiętania jest to, że nie wszystkie poprawki powinny być instalowane domyślnie. Punktem zwrotnym automatyzacji zarządzania poprawkami jest zapewnienie wystarczającej ilości szczegółów do podejmowania świadomych decyzji, a także usprawnienie procesu wdrażania. PatchManager dostarcza tak

dużo informacji jak to możliwe, ale decyzję, aby przetestować i ostatecznie wdrożyć poprawkę należy zawsze do administratora.

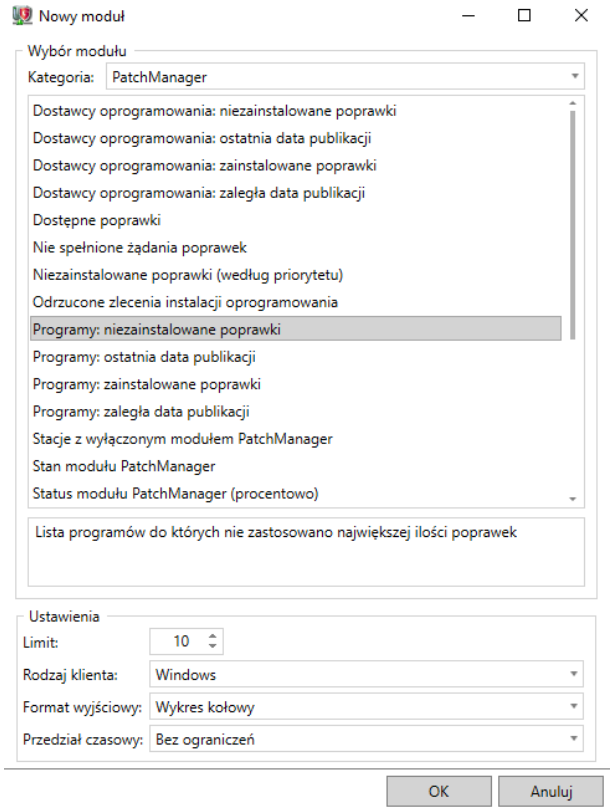
4.4. Testowanie

Gdy podjęto decyzję, że konkretna łatka zostanie wdrożona można uruchomić procedurę testowania. Zaleca się korzystanie z zestawu maszyn reprezentatywnych aby przetestować poprawki. Te maszyny powinny być podobne do klientów, które są obecnie używane w celu zbadania możliwych problemów bez zakłócania rzeczywistych maszyn. Jednak nie każdy administrator będzie miał dostęp do wystarczającej ilości maszyn aby zbudować małej wielkości replikę swojej sieci. Zalecana jest metoda wirtualizacji jeśli nie ma innego rozwiązania. W każdym przypadku, G Data pomaga w zarządzaniu siecią dla testów. W G Data Administrator, środowisko testowe może być zorganizowane w jedną lub więcej grup. Poprawki mogą być stosowane dla jednego lub kilku klientów z jedną lub kilkoma grupami, w celu obserwowania instalacji i jej skutków.



Rysunek 9: G DATA Administrator, zlecenie dystrybucji oprogramowania(testy)

Aby wdrożyć jedną lub więcej poprawek do grupy testowej, zaznacz grupę w obszarze zarządzania klientem. Otwórz moduł zleceń i utwórz nowe zlecenie dystrybucji oprogramowania. Wybierz poprawkę(ki), które mają być dystrybuowane i określ, w jakim czasie powinno to nastąpić. Wybór poprawki może być ułatwiony poprzez grupowanie listy łatek na podstawie producenta lub produktu. Powtórz ten proces dla wszystkich odpowiednich łatek i dla wszystkich odpowiednich grup testowych. Zaleca się, aby przetestować tylko jedną poprawkę na system w tym samym czasie, aby być w stanie zidentyfikować potencjalne problemy po instalacji określonej poprawki.



Rysunek 10: G DATA Administrator, wybór modułu ReportManager

W okresie testowania, jak również w fazie weryfikacji po wdrożeniu moduł ReportManager może pomóc w ustaleniu, jaki jest status wdrażania poprawek, a które komputery generują błędy. ReportManager umożliwia administratorowi wybranie kilku modułów, które mogą być połączone w jednym raporcie. Kategoria PatchManager oferuje kilka przydatnych opcji. Takie jak programy, do których nie zastosowano największej ilości poprawek(co może wskazywać na problemy podczas instalacji).

Ponadto obok modułu ReportManager status testowanej poprawki może również znajdować się w zleceniach modułu PatchManager. Należy otworzyć odpowiednie zlecenie i sprawdzić szczegóły, aby zobaczyć status każdej poprawki. Jeśli wydaje, że łatka nie została wdrożona z sukcesem, należy sprawdzić raport z uaktualnienia oprogramowania dla tego klienta. Jeśli poprawka nie może zostać wdrożona, sprawdź system lokalnie i spróbuj ręcznie łatkę zainstalować. Jeśli poprawka jest przyczyną problemów w fazie testów, to nigdy nie powinna zostać wdrożona automatycznie na dużą skalę.

4.5. Etap V: Harmonogram i ocena

Po zakończeniu etapu testów, mogą być planowane rzeczywiste wdrożenia. Dla wszystkich, których poprawki obowiązują można skonfigurować harmonogram. Stosując politykę zarządzania poprawkami należy podjąć decyzję, dla których maszyn poprawki powinny być wdrażane i do których(grup) maszyn w pierwszej kolejności. Użyj funkcji Wiadomości w module Klienci aby powiadomić użytkowników o harmonogramie poprawki i ostrzec ich o potencjalnym restarcie stacji roboczej.

4.6. Wdrożenie poprawki

Dla poprawek, które zostały odpowiednio przetestowane, można zaplanować zadanie dystrybucji oprogramowania. Użyj modułu zleceń aby zaplanować dystrybucję oprogramowania za pośrednictwem właściwej poprawki dla odpowiednich klientów. Aby uniknąć ingerencji w pracę użytkowników końcowych, poprawki mogą być zaplanowane. Mogą zostać uruchomione w określonym czasie lub bezpośrednio po następnym rozruchu lub

logowaniu. Opcjonalne opóźnienie zapobiega wdrożenie poprawek podczas gdy inne procesy systemowe intensywnie są wykorzystywane.

4.7. Weryfikacja i raportowanie

W celu sprawdzenia i oceny wdrażanej poprawki, narzędzie inwentaryzacji oprogramowania może być wielką pomocą. Do tego, moduł G DATA PatchManager oferuje możliwość bezpośredniej odpowiedzi zwrotnej od użytkowników. Jeśli administrator włączy odpowiednią opcję, użytkownicy końcowi mogą żądać wycofania poprawek z powodu wydajności lub problemów z kompatybilnością. System żądania dystrybucji i wycofywania integruje się bezpośrednio z modułem PatchManager i pozwala administratorowi zaplanować pracę dystrybucji lub wycofywania bezpośrednio z modułu Raportów. Rozważmy następujący przykład: użytkownik końcowy nie może korzystać z aplikacji 1 i czeka na poprawkę, która będzie wdrożona. Podczas fazy testowania, administrator odkrywa problemy ze zgodnością z aplikacją 2 i decyduje, że poprawka nie zostanie wdrożona do sieci. Użytkownik końcowy nie korzysta z dotkniętymi problemami aplikacji 2 i postanawia, że poprawka dla aplikacji 1 powinna zostać wdrożona. Dzięki dwukierunkowej dystrybucji poprawek G DATA, użytkownik może zażądać poprawki do zainstalowania. Po zatwierdzeniu żądania, odbędzie się dystrybucja poprawki dla aplikacji 1.