Kaspersky®
Vulnerability & Patch
Management

Uprość i wzmocnij ochronę dzięki scentralizowanym narzędziom do zarządzania IT

Luki w popularnych aplikacjach znacząco zagrażają bezpieczeństwu IT w firmach. Problem stanowią nie tylko luki dnia zerowego, ale także coraz większa złożoność infrastruktury IT, która komplikuje zadanie sprawnego eliminowania luk w oprogramowaniu: jeśli nie wiesz, czym dysponujesz, jak masz to ochronić?

Zarządzanie aktualizacjami oprogramowania przy jednoczesnym monitorowaniu potencjalnych luk to jedno z najważniejszych, a równocześnie najbardziej nużących i czasochłonnych zadań, z jakimi muszą mierzyć się działy IT. Centralizując i automatyzując podstawowy poziom ochrony oraz zadania konfiguracji i zarządzania — takie jak zarządzanie lukami, dystrybucja łat i aktualizacji, zarządzanie inwentarzem czy instalacja aplikacji — rozwiązanie Kaspersky Vulnerability and Patch Management pozwala oszczędzać czas i optymalizuje bezpieczeństwo.

Miej oko na wszystko

Pełna widoczność sieci z poziomu jednej konsoli eliminuje niepewność administratora i zapewnia mu kompletną wiedzę odnośnie każdego urządzenia i aplikacji — w tym urządzeń gości— które mają dostęp do sieci. Takie scentralizowane podejście umożliwia pełną kontrolę nad dostępem do firmowych danych i aplikacji, uzyskiwanym przez użytkowników i urządzenia, a także zapewnia zgodność z politykami IT i wymogami prawnymi.

Zwiększ ochronę

Zwiększ ochronę IT i zmniejsz czasochłonne rutynowe zadania dzięki zautomatyzowanym zadaniom związanym z łatami i aktualizacją. Rozwiązanie Kaspersky Vulnerability and Patch Management daje pełny obraz sytuacji, dzięki czemu wiesz dokładnie, co trzeba zrobić, aby zapewnić firmie bezpieczeństwo. Automatyzacja całego cyklu zarządzania lukami i łatami — w tym wykrywania luk i priorytetyzacji ich eliminowania, pobierania łat i aktualizacji, testowania i dystrybucji, monitorowanie i raportowanie efektów — pomaga zwiększyć wydajność i znacząco zmniejsza obciążenie zasobów.

Upraszczanie zadań IT

Kaspersky Vulnerability and Patch Management zawiera zestaw narzędzi do zarządzania klientami w celu automatyzacji wielu funkcji związanych z administracją IT. Automatyczne przydzielanie aplikacji, dostęp zdalny i rozwiązywanie problemów pomagają minimalizować czas i zasoby potrzebne do przygotowania nowych stacji roboczych i instalacji nowych aplikacji.

Zarządzanie centralne

Kaspersky Vulnerability and Patch Management to komponent zarządzany wchodzący w skład rozwiązania Kaspersky Security Center. Konsola ta umożliwia zarządzanie i dostęp do każdej funkcji, przy użyciu zwięzłych, intuicyjnych poleceń i interfejsów, które pozwalają zautomatyzować rutynowe działania związane z infrastrukturą IT.

Łatanie luk i zarządzanie łatami

Monitorowanie efektów i generowanie raportów

Rozwiązanie Kaspersky Vulnerability and Patch Management informuje administratorów IT o stanie instalacji łat i umożliwia im generowanie raportów na temat skanowania, wyszukiwanie potencjalnych słabych punktów, śledzenie zmian i uzyskiwanie szerszego wglądu w bezpieczeństwo IT na każdym urządzeniu i w każdym systemie należącym do sieci firmowej.

Wykrywanie i priorytetyzacja luk

Zautomatyzowane skanowanie w poszukiwaniu luk umożliwia szybkie ich wykrywanie, priorytetyzację i eliminowanie. Skanowanie w poszukiwaniu luk może być przeprowadzane automatycznie lub zgodnie z harmonogramem, według potrzeb administratorów. Elastyczne zarządzanie profilami ułatwia dystrybucję aktualizacji, kompatybilność oprogramowania, jak również tworzenie wyjątków w celu obsługi niestandardowych rozwiązań.

Oszczędność czasu dzięki dystrybucji oprogramowania

Wdrażaj lub aktualizuj zdalnie, z jednej konsoli. Automatycznie można instalować ponad 150 popularnych aplikacji, które znajdują się w bazie rozwiązania Kaspersky Security Network. Co ważne, może się to odbywać nawet poza godzinami pracy. Zastosowanie technologii Multicast do lokalnej dystrybucji oprogramowania pozwala oszczędzać ruch sieciowy podczas przesyłania pakietów instalacyjnych do biur zdalnych.

Pobieraj, testuj i dystrybuuj łaty oraz aktualizacje

Aktualizacje i łaty można pobierać automatycznie za pośrednictwem serwerów Kaspersky Lab. Przed dystrybucją mogą one zostać sprawdzone w celu upewnienia się, że nie zmniejszą wydajności systemu czy pracowników. Łaty i aktualizacje mogą być dystrybuowane natychmiast, a instalacja łat może zostać odroczona na bardziej odpowiedni moment (na przykład poza godzinami pracy firmy).

Skanuj swoją sieć w celu sporządzenia inwentarzy sprzętu i oprogramowania

Automatyczne identyfikowanie i monitorowanie sprzętu oraz oprogramowania daje administratorom szczegółowy wgląd w każdy zasób znajdujący się w sieci firmowej. Automatyczne skanowanie oprogramowania umożliwia szybkie wykrywanie przestarzałych programów, które mogą stwarzać zagrożenie dla bezpieczeństwa.

Narzędzia służące do zarządzania klientami

Zdalne rozwiązywanie problemów

W celu zmniejszenia czasu reakcji, zwiększenia wydajności i ułatwienia wsparcia dla lokalizacji zdalnych rozwiązanie Kaspersky Security Center wykorzystuje protokół Remote Desktop Protocol (RDP) i technologię Windows Desktop Sharing (używaną również w usłudze Windows Remote Assistance). Zdalne połączenie z komputerami klienckimi za pośrednictwem agenta sieciowego umożliwia pełny dostęp na poziomie administratora do danych i aplikacji zainstalowanych na urządzeniu klienckim, nawet jeśli jego porty TCP i UDP są zamknięte. Mechanizm autoryzacji zapobiega uzyskiwaniu nieautoryzowanego dostępu zdalnego. W celu umożliwienia śledzenia i przeprowadzenia audytu rejestrowane są wszystkie aktywności wykonywane w ramach sesji zdalnego dostępu.

Instalacja systemu operacyjnego

Rozwiązanie Kaspersky Vulnerability and Patch Management automatyzuje i centralizuje tworzenie, przechowywanie i klonowanie bezpiecznych obrazów systemu, a także wspiera instalację i reinstalację systemu operacyjnego na nowych maszynach. Wszystkie obrazy są przechowywane w specjalnym inwentarzu i można do nich uzyskiwać dostęp podczas instalacji. Obraz może zostać zainstalowany na klienckiej stacji roboczej zarówno przy użyciu serwerów PXE (Preboot eXecution Environment – także na nowych maszynach bez systemu operacyjnego), jak i przy użyciu zadań zleconych Kaspersky Vulnerability and Patch Management (w celu instalacji obrazów systemu na zarządzanych maszynach klienckich). Wysyłając do komputerów sygnały Wake-on-LAN, możesz automatycznie dystrybuować obrazy poza godzinami pracy firmy. Dodatkowo rozwiązanie obsługuje interfejs UEFI.

Dostępność

Rozwiązanie Kaspersky Vulnerability and Patch Management jest dostępne:

- W ramach rozwiązania Kaspersky Total Security for Business
- W ramach rozwiązania Kaspersky Endpoint Security for Business Advanced

Produkt można również nabyć w postaci dodatku do Kaspersky Endpoint Security for Business Select lub jako oddzielne rozwiązanie Kaspersky Vulnerability and Patch Management

Kaspersky Lab

Ochrona dla firm: **kaspersky.pl/biznes**
Unikatowa technologia: **kaspersky.pl/true-cybersecurity**
Wszystko o cyberzagrożeniach: **securelist.pl**
Oficjalny blog: **kaspersky.pl/blog**
#truecybersecurity
#HuMachine

www.kaspersky.pl