baramundi

CHECKLISTY BARAMUNDI zapewniają zwięzłe i szczegółowe wskazówki ekspertów odnoszące się do częstych pytań i problemów. Więcej z nich można znaleźć na stronie www.baramundi.com/checklisty

Bądź zawsze na bieżąco – 5 wskazówek do efektywnego zarządzania aktualizacjami

Oprócz ataków phishingowych, niezałatane luki w zabezpieczeniach systemów są najczęstszą metodą wykorzystywaną przez hakerów do naruszania bezpieczeństwa sieci i danych. Mimo że liczba luk w zabezpieczeniach rośnie z dnia na dzień, można je szybko i skutecznie wykrywać i usuwać, korzystając z odpowiednich narzędzi i 5 łatwych do wdrożenia wskazówek.

Określenie najważniejszego sprzętu i oprogramowania

Stale oceniaj bieżące ryzyko zaczynając od systemów i aplikacji o znaczeniu krytycznym, które są niezbędne do utrzymania produktywności w różnych działach. Odpowiednio priorytetyzuj wdrażanie poprawek i aktualizacji.

Testowanie przed wdrożeniem

Aktualizacje również mogą zawierać błędy. Dlatego należy je najpierw przetestować na kilku urządzeniach. Po upewnieniu się, że zmiany nie spowodują większych problemów niż te, które rozwiązują, aktualizacje mogą być wprowadzone na szerszą skalę.

Wprowadzenie topologii pierścienia

Utwórz pierścienie punktów końcowych lub logiczne grupy urządzeń, które otrzymają odpowiednie aktualizacje w tym samym czasie w stopniowej sekwencji coraz większych pierścieni. Pierścienie z najważniejszymi punktami końcowymi otrzymają łatki lub aktualizacje w pierwszej kolejności.

Zautomatyzowane bezpieczeństwo

Ręczne wprowadzanie aktualizacji jest nie tylko czasochłonne, lecz również podatne na błędy. Lepiej jest zautomatyzować ten proces, stosując narzędzia do zarządzania urządzeniami końcowymi. Wykrywanie luk w zabezpieczeniach również może zostać zautomatyzowane. Zaawansowane rozwiązania UEM zapewniają również obszerne biblioteki wstępnie przetestowanych pakietów poprawek gotowych do dystrybucji.

Zarządzanie ryzykiem

Nie wszystkie aktualizacje i poprawki powinny być wdrażane natychmiast. Niektóre z nich mogą być wadliwe lub niekompatybilne. Oprócz tego, niektórych systemów, zwłaszcza tych używanych w środowiskach produkcyjnych, nie da się łatwo zmienić. Konieczne może być ich odizolowanie, odłączenie lub zabezpieczenie za pomocą innych środków.

W pigułce: Regularne i wydajne zarządzanie aktualizacjami ma kluczowe znaczenie dla wyeliminowania niezałatanych luk w zabezpieczeniach. Identyfikacja krytycznych systemów, testowanie aktualizacji, koncepcja pierścienia, automatyzacja bezpieczeństwa i zrównoważone zarządzanie ryzykiem to podstawowe elementy strategii bezpieczeństwa, które można szybko i niezawodnie wdrożyć za pomocą pakietu baramundi Management Suite.