W jaki sposób przydzielasz i kontrolujesz dostęp do infrastruktury IT w Twojej organizacji?

Zapewnienie bezpieczeństwa dla infrastruktury IT Twojej organizacji jest niezbędne, aby firma działała i stawiała czoła codziennym wyzwaniom. Złożoność i mnogość aplikacji, urządzeń, różnych systemów sprawia, że zarządzanie dostępem administracyjnym staje się dziś krytyczne. Dostęp administracyjny to połączenia użytkowników o szczególnych uprawnieniach. Niezależnie czy bierzemy pod uwagę pracowników firmy, czy zewnętrznych konsultantów kontrola dostępu staje się elementem wyjściowym budowy każdej polityki bezpieczeństwa systemów informatycznych. Polityka bezpieczeństwa to pierwszy ważny etap budowy bezpiecznego dostępu do systemów przetwarzania danych organizacji. W drugim kroku trzeba móc zaimplementować i wyegzekwować reguły i zasady zawarte w tejże polityce. Możesz szybko sprostać temu wyzwaniu, zaczynając od źródła i kontrolując dostęp do tych kont użytkowników, które mają najwyższe uprawnienia. Kontrola i monitoring działań dla tych kont jest najlepszą praktyką, kierunkiem w budowaniu bezpiecznego dostępu do infrastruktury.

Co jest jest Wallix Bastion?

WALLIX Bastion to jedno z głównych rozwiązań oferowanych przez firmę WALLIX w dziedzinie Zarządzania Dostępem Przywilejowanym (PAM - Privileged Access Management). WALLIX Bastion jest platformą służącą do zarządzania, nadzoru i rejestrowania dostępu do kont uprzywilejowanych. Bastion umożliwia ochronę krytycznych zasobów, w tym serwerów, baz danych, terminali oraz wszelkich innych urządzeń wewnątrz chronionej infrastruktury, dając twardy materiał dowodowy w postaci filmów oraz logów z każdego wykonanego polecenia podczas zdalnej sesji. Rozwiązanie oferuje nagrywanie uprzywilejowanych sesji administracyjnych w systemach IT, zarządzanie uprzywilejowanym dostępem do systemów, zarządzanie zmianami haseł administracyjnych

Cechy Wallix Bastion:

Elastyczność integracji:

Łatwe i szybkie wdrożenie Bastion (integracja z Microsoft Active Directory/LDAP/MFA)

Nie wymaga instalacji oprogramowania na systemach monitorowanych

Wykorzystuje protokoły uwierzytelnienia takie jak: LDAP, Microsoft Active Directory, Radius, TACACS+, Kerberos, X.509, OTP, Web SSO

Twórz użytkowników i systemy, aplikacje do których dostęp chcesz chronić i monitorować

Określ zasady rotacji haseł dla kont uprzywilejowanych(Windows, Unix, Cisco, Oracle, MySQL, Fortinet, PaloAlto i itp.)

Zarządzaj dostępem użytkowników do wybranych obszarów organizacji

Gromadź i zarządzaj hasłami oraz kluczami SSH z wykorzystaniem bezpiecznego sejfu haseł(AES 256)

Możliwość klastrowania HA(Ha z 3 lub większą ilością węzłów na klaster) w trybie active/active lub active/passive

Wsparcie dla wielu platform m.in. VMware, Microsoft Hyper-V, Microsoft Azure, Amazon Web Services lub instalacja na wydajnej platformie sprzętowej WALLIX

Ufaj i kontroluj:

Otrzymuj od Bastion powiadomienie o każdej rozpoczętej sesji administracyjnej

Monitoruj w czasie rzeczywistym pracę firmy zewnętrznej i kończ sesje zdalną w dowolnej chwili
Rejestruj sesje zarówno w postaci tekstu jak i wideo oraz zapisuj dzienniki zdarzeń na potrzebę audytu

Rozliczaj i kontroluj koszty zewnętrznych dostawców usług

Chroń poświadczenia dla kont uprzywilejowanych (np. root, local admin, dba, itp.)

Podność uprawnienia użytkowników i zarządzaj delegowaniem uprawnień(PEDM, BestSafe)

Ustaw reguły automatyczne:

Identyfikuj i reaguj na podejrzane zachowania użytkowników

Przerywaj sesje w których użyto zakazanych poleceń