AUDYT HARDERING SYSTEMÓW I USŁUG

W CELU ZMINIMALIZOWANIA RYZYKA UTRATY DANYCH PRZEZ SŁABE PUNKTY, MOGĄ POWODOWAĆ PODATNOŚCI SPRZĘTOWE I SYSTEMOWE, POLECAMY CYKLICZNE WYKONYWANIE AUDYTÓW HARDERING SYSTEMÓW I USŁUG

Głównym celem zapewnienia ciągłości działania organizacji i stabilnej pracy systemów informatycznych powinno być **zapewnienie kompleksowego bezpieczeństwa** tych systemów przez **zoptymalizowanie zabezpieczeń systemów operacyjnych**, głównych systemów softwarowych i **maksymalne zoptymalizowanie pełnego środowiska informatycznego**.

Jednym z narzędzi służących do wykrycia tych podatności jest wykonanie: **AUDYTU HARDERING SYSTEMÓW I USŁUG**.

Podczas takiego audytu niezależny zespół specjalistów oceni poziom bezpieczeństwa – odporności systemu na wszelkiego typu podatności.

AUDYT HARDERING SYSTEMÓW I USŁUG można podzielić na trzy powiązane etapy:

I ETAP

OPTYMALIZACJA I ZABEZPIECZENIE WARSTWY SPRZĘTOWEJ BIORĄCEJ UDZIAŁ W PROCESIE

Przykład:
Optymalizacja i zabezpieczenie serwera (HARDERING SERWERA) Specjalista wykonuje czynności mające na celu zwiększenie bezpieczeństwa serwera. Najpierw określane są **wszystkie podatności urządzenia,** a następnie wykonywane są czynności mające na celu **podniesienie jego odporności** na różnego typu działania czynników wewnętrznych i zewnętrznych – następuje HARDERING czyli **utwardzenie – zwiększenie odporności i stabilizacji pracy systemu**.

Servus Comp Sp. z o.o. Sp. K.
30-019 Kraków ul. Mazowiecka 25/502
tel. 12 631-91-22 biuro@servus-comp.pl
https://firmapremium.zadbajobezpieczenstwo.pl

Wykonując na serwerze ważne dla organizacji działania musimy pamiętać, aby chronić naszą infrastrukturę przed utratą reputacji i stabilności tak, aby Klient był pewien, że nasza organizacja dba o stabilną pracę systemów. Wizerunkowo jest to dla nas bezcenne, gdyż codziennie podejmowane są próby profanacji urządzeń, a Klienci, wybierając dostawcę usług, oceniają stan bezpieczeństwa infrastruktury informatycznej, przetwarzającej dane o wysokim znaczeniu dla firmy.

Lista wykrywanych luk w bezpieczeństwie serwerów i innych urządzeń składających się na całą infrastrukturę informatyczną stale się wydłuża. Aby skutecznie móc się przeciwstawić temu procesowi, konieczne są cykliczne działania.

Po przeprowadzeniu audytu hardering systemów i usług, w raporcie przedstawiamy Klientowi metody **wzmocnienia bezpieczeństwa warstwy sprzętowej,** w tym wypadku serwerów. Metodologia ujednolicenia systemów:

- wskazanie niepożądanych plików binarnych i innych zbędnych funkcji do wyłączenia
- wyłączenie plików SUID i SGID
- optymalizacja SSH
- optymalizacja zapory
- analiza i propozycja fizycznego bezpieczeństwa środowiska serwerowego
- usunięcie niebezpiecznych protokołów, które mogą doprowadzić do ujawnienia nazwy użytkownika i jego hasła dostępu
- możliwość usunięcia niepotrzebnych systemów z powierzchni dysków twardych serwera w porozumieniu z administratorem
- przedstawienie propozycji metod szyfrowania danych w celu podniesienia bezpieczeństwa przepływu danych
- wykrycie, zmapowanie i zablokowanie:
  brut force - blokowanie ataków na usługi systemowe takie jak: ssh, mail, ftp, apache. Blokowanie IP intruza, robota po zidentyfikowaniu zadanej liczby błędnych logowań podanej w konfiguracji systemu.
  SQL Injection – blokowanie dodatkowych zapytań, które mogą niszczyć dane.

servus comp
Servus Comp Sp. z o.o. Sp. K.
30-019 Kraków ul. Mazowiecka 25/502
tel. 12 631-91-22 biuro@servus-comp.pl
https://firmapremium.zadbajobezpieczenstwo.pl

Należy pamiętać, że audyt hardering systemów i usług nie dotyczy tylko podanego powyżej przykładu audytu podatności serwera. Audytu **powinien również obejmować inne urządzenia odpowiedzialne za utrzymanie infrastruktury** na najwyższym poziomie bezpieczeństwa np.: routery brzegowe, które szczególnie są narażone na podatności, switche itd.

II ETAP

OPTYMALIZACJA I ZABEZPIECZENIE WARSTWY SOFTWAROWEJ, SYSTEMOWEJ BIORĄCEJ UDZIAŁ W PROCESIE

- analiza warstwy podatności systemów produkcyjnych
- analiza warstwy podatności systemów Microsoft Windows
- analiza warstwy podatności systemów LINUX
- analiza warstwy podatności innych systemów

III ETAP

RAPORT POAUDYTOWY

W raporcie poaudytowym Klient otrzymuje opis wszystkich wykrytych podatności wraz z wykazem metod, jakimi te podatności mogą zostać usunięte.

Audyt hardering systemów i usług **powinien być wykonywany cykliczne**. Daje nam to pewność, że bezpieczeństwo infrastruktury informatycznej jest utrzymane na wysokim poziomie, a wszelkie podatności są eliminowane na bieżąco.

servus comp
Servus Comp Sp. z o.o. Sp. K.
30-019 Kraków ul. Mazowiecka 25/502
tel. 12 631-91-22 biuro@servus-comp.pl
https://firmapremium.zadbajobezpieczenstwo.pl

W celu uzyskania pełnej informacji w omawianych zakresach zapraszamy do kontaktu:

602 220 749 andrzej.popiolek@servus-comp.pl

781 555 025 anna.strek@servus-comp.pl

12 631 91 22 biuro@servus-comp.pl

Servus Comp Sp. z o.o. Sp.k.
ul. Mazowiecka 25/502, 30-019 Kraków
Sąd Rejonowy dla Krakowa – Śródmieście,
XI Wydział Gospodarczy Krajowego Rejestru Sądowego
NIP: 6772394344 | Regon: 362815411 | KRS: 0000582481

https://zadbajobezpieczenstwo.pl
https://firmapremium.zadbajobezpieczenstwo.pl
https://premiumbank.zadbajobezpieczenstwo.pl