11 grudnia 2024

DOBRE PRAKTYKI WZMOCNIENIA BEZPIECZEŃSTWA DOSTĘPÓW ZDALNYCH

1. Przeanalizowanie istniejącej infrastruktury w celu udokumentowania aktualnego stanu - linii bazowej (tzw. baseline) dla codziennej aktywności sieciowej. Odchylenia od tej normy mogą być wskaźnikiem kompromitacji.
2. Uwzględnienie oraz stosowanie rozwiązań VPN przy zdalnym dostępie do zasobów.
3. Stosowanie tzw. białej listy dozwolonych narzędzi zdalnego dostępu. Ograniczy to wykorzystanie nieautoryzowanych narzędzi.
4. Stosowanie tzw. białej listy dozwolonych hostów i adresów IP, do których oraz z których można nawiązywać zdalne połączenia.
5. Stosowanie w organizacji zasady minimalnych uprawnień.
6. Stosowanie polityki silnych haseł.
7. Stosowanie uwierzytelniania wieloskładnikowego (ang. Multi Factor Authenticaton MFA)
8. Zarządzanie dostępami uprzywilejowanymi oraz ograniczenie takich uprawnień do niezbędnego minimum (np. administratorzy systemów, wsparcie zewnętrzne, helpdesk).
9. Korzystanie z praw administracyjnych powinno odbywać się tylko z dedykowanych kont, niewykorzystywanych do codziennej pracy.
10. Przeprowadzanie audytów dostępów dla kont w organizacji – maksymalne ograniczanie uprawnień nieaktywnych kont oraz przegląd ich uprawnień wraz z przypisanymi politykami.
11. Przeprowadzanie bieżących aktualizacji wszystkich aplikacji, w szczególności dostępnych z zewnątrz organizacji, ze szczególnym uwzględnieniem aktualizacji bezpieczeństwa.
12. Gromadzenie logów co najmniej z urządzeń sieciowych oraz z Active Directory i monitorowanie zdarzeń związanych z dostępem zdalnym.
13. Wdrożenie i stosowanie rozwiązań klasy Network Access Control (NAC).
14. Stosowanie ochrony antywirusowej na wszystkich stacjach roboczych oraz systemach w organizacji.
15. Stosowanie rozwiązań klasy Priviliged Access Managment (PAM), do celów administracyjnych oraz w przypadku przetwarzania danych wrażliwych.
16. Stosowanie rozwiązań klasy Mobile Device Managment (MDM), dla urządzeń mobilnych.
17. Stosowanie rozwiązań typu Identity Access Management (tzw. IAM).

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

18. Prowadzenie cyklicznych szkoleń Security Awareness dla pracowników oraz kadry menadżerskiej.
19. Prowadzanie cyklicznych audytów w celu weryfikacji prawidłowych i bezpiecznych konfiguracji urządzeń w organizacji.
20. Prowadzanie cyklicznych skanów bezpieczeństwa w poszukiwaniu podatności w systemach i aplikacjach.
21. Dążenie do architektury Zero Trust Network Access (ZTNA).
22. Stosowanie oraz utrzymanie segmentacji sieciowej, która pozwala na kontrolę i ograniczenie tzw. ruchu poziomego.
23. Blokowanie ruchu przychodzącego i wychodzącego na standardowych portach wewnątrz organizacji dla popularnych usług zdalnego dostępu.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706