

Wymagania bezpieczeństwa informatycznego dla systemów technologicznych

1. W systemie technologicznym mogą pracować wyłącznie aplikacje potrzebne do obsługi wspieranych procesów technologicznych. Wykonawca dostarczy listę aplikacji dozwolonych.
2. Wszystkie poprawne przepływy pomiędzy elementami systemu muszą być zidentyfikowane. Tylko te przepływy mogą być dozwolone.
3. Dostarczona zostanie dokumentacja systemu technologicznego określająca
 - a. Funkcjonalny opis instalacji
 - b. Zasoby informatyczne wchodzące w skład systemu wraz z określeniem ich krytyczności.
 - c. Dokładny opis konfiguracji każdego komponentu systemu.
 - d. Dokładny schemat połączeń fizycznych pomiędzy elementami systemu
 - e. Dokładny schemat połączeń logicznych pomiędzy elementami systemu
 - f. Poprawną dopuszczoną komunikację pomiędzy elementami systemu (źródło, protokół, cel)
 - g. Opis ról/profilu użytkowników systemu wraz z powiązanymi z nimi uprawnieniami na poszczególnych elementach systemu
 - h. Listę kont użytkowników systemów w powiązaniu z rolami/profilami.
 - i. Listę kont technicznych/serwisowych nie powiązanych z użytkownikami.

Dokumentacja musi być przechowywana w bezpiecznym miejscu z określonymi prawami dostępu. Zaleca się przechowywanie kopii dokumentacji poza obszarem eksploatacji. Przegląd dokumentacji powinien odbywać się co najmniej raz do roku.

4. Rozwiązanie będzie dostarczać następujące informacje:
 - a. Logi z urządzeń filtrujących ruch
 - b. Logi z systemu antywirusowego
 - c. Informacje o stanie implementacji aktualizacjach bezpieczeństwa systemów (dopuszcza się formę comiesięcznego raportu).
 - d. Logi dostępne z aplikacji oraz elementów systemu (nieudane autentykacje, itp.).Dane te muszą być dostarczane na bieżąco do systemu SIEM pracującego w sieci biznesowej. W celach śledczych logi te powinny być przechowywane co najmniej przez 6 miesięcy.
5. Zabroniony jest bezpośredni dostęp systemów technologicznych do sieci Internet lub systemów które, świadczą usługi dostępne bezpośrednio z sieci Internet.
6. Sieć komputerowa systemu bezpośrednio odpowiadającego za obsługę procesów technologicznych musi być jasno wydzielona i odseparowana od pozostałej sieci. Wszelka komunikacja na tym styku musi podlegać kontroli poprzez rozwiązania filtrujące ruch.
7. Sieć technologiczna musi być odseparowana od sieci biznesowej za pomocą pośredniej sieci DMZ.
8. Podczas wymiany danych pomiędzy siecią technologiczną i siecią biznesową, dane te powinny być wysyłane z sieci technologicznej zamiast pobierane z sieci biznesowej.
9. Rozwiązania filtrujące ruch muszą zostać wyposażone w systemy detekcji intruzów IDS. Wewnątrz rozwiązania nie powinny pracować systemy prewencji IPS.
10. Krytyczne elementy systemu muszą być zaprojektowane w sposób redundantny. Dotyczy to zarówno samych elementów, ich zasilania oraz połączeń między nimi. W regularnych odstępach czasu, nie rzadziej niż raz do roku powyższa redundancja powinna być testowana przez dostawcę.

11. Dostęp zdalny:
 - a. Dostęp zdalny do zasobów powinien być kontrolowany przez rozwiązanie centralne z zapewnieniem szyfrowania (VPN).
 - b. Dostęp zdalny możliwy jest na żądanie w ograniczonym, jak najkrótszym przedziale czasowym.
 - c. Dostęp do sieci technologicznej bezpośrednio odpowiedzialnej za sterowanie procesem produkcji może odbywać się tylko poprzez serwer przesiadkowy (bastion) umieszczony w technologicznym DMZ.
12. Komponenty systemu muszą zostać wyposażone w rozwiązanie zabezpieczające przed działaniem oprogramowania złośliwego.
 - a. Rozwiązanie to musi być sterowane centralnie.
 - b. Centralne zbieranie informacji o stanie/kondycji poszczególnych elementów systemu oraz wykrytych infekcjach.
 - c. Aktualizacje bazy sygnatur na końcowych elementach systemu muszą być przeprowadzane bez zbędnej zwłoki (nie rzadziej niż jeden tydzień).
13. Przez cały okres eksploatacji systemu dostawca zapewni wsparcie między innymi w zakresie:
 - a. Dostarczania i implementacji przetestowanych i zaakceptowanych aktualizacji systemów, aplikacji oraz sygnatur antywirusowych.
 - b. Zapewnienia serwisu elementów systemu w tym ich wymianę w przypadku uszkodzenia.
14. Aktualizacje oprogramowania (sygnatur systemu antywirusowego) elementów systemu przed instalacją w środowisku produkcyjnym muszą być uprzednio przetestowane i zaakceptowane przez dostawcę rozwiązania. Krytyczne aktualizacje bezpieczeństwa powinny być instalowane bez zbędnej zwłoki (nie rzadziej niż raz do roku).
15. Do budowy systemu powinny zostać wykorzystane najnowsze stabilne wersje oprogramowania, które zapewniać będą jak najdłuższy okres wsparcia producenta (aktualizacji bezpieczeństwa).
16. W odstępach miesięcznych należy wykonywać przegląd elementów pod kątem dostępnych aktualizacji bezpieczeństwa.
17. Przestarzałe lub niewspierane wersje sprzętu lub oprogramowania powinny być wymieniane nie później niż rok po zakończeniu wsparcia.
18. Raz do roku dostawca przeprowadzi przegląd systemu pod kątem bezpieczeństwa informatycznego wraz z analizą ryzyk oraz opracowaniem i implementacją planu naprawczego.
19. Muszą istnieć procedury aktualizacji:
 - a. oprogramowania
 - b. firmware
 - c. antywirus
 - d. systemów
20. Rozwiązanie musi być zaprojektowane w taki sposób aby możliwa była zmiana poświadczeń we wszystkich elementach systemu. Zmiana poświadczeń nie może wpływać na pracę całego systemu.
21. Hasła wykorzystywane w elementach systemu:
 - a. Muszą być odpowiednio silne (min.10 znaków, liczby, znaki specjalne, duże/małe litery)
 - b. Muszą zostać zmienione na inne niż domyślne

- c. Muszą być regularnie zmieniane (przynajmniej raz do roku).
 - d. Na elementach systemu lub na grupach elementów systemu muszą być używane różne hasła.
22. Wszystkie komponenty systemu powinny być chronione przed nieuprawnionym dostępem fizycznym. Każda próba dostępu do pomieszczeń lub szaf gdzie pracują elementy systemu powinna być odnotowana.
23. System będzie wyposażony w rozwiązanie pozwalające na wykonywanie kopii zapasowej oraz odtworzenie krytycznych elementów systemu. Poprawność kopii bezpieczeństwa będzie testowana w regularnych odstępach czasu, nie rzadziej niż raz do roku.
24. Wykonawca zapewni, że niewykorzystywane usługi oraz interfejsy elementów systemu będą wyłączone.
25. W systemie operacje użytkowników systemu powinny być logowane. Zebrane informacje powinny w jednoznaczny sposób identyfikować użytkownika który dokonał operacji.