

1. Zabezpieczenie portów i urządzeń sieciowych

- Wszystkie nieużywane porty w urządzeniach sieciowych OT muszą być zabezpieczone zaślepkami z numerem identyfikacyjnym oraz datą założenia.
- Zaśleпки mogą być zdejmowane wyłącznie przez upoważnionych pracowników działu process controll, po uprzednim zgłoszeniu i weryfikacji potrzeby podłączenia nowego urządzenia.
- Stan zabezpieczeń portów powinien być dokumentowany i podlegać rocznym audytom.
- W przypadku naruszenia zabezpieczenia portu należy zgłosić incydent do zespołu bezpieczeństwa IT/OT.
- Porty aktywne powinny być monitorowane pod kątem nieautoryzowanych prób podłączenia (np. alerty SNMP, monitoring NAC).
- Zaleca się wdrożenie mechanizmów Port Security oraz MAC filtering.

2. Procedura podłączania nowych urządzeń

- Zgłoszenie podłączenia urządzenia musi zawierać: typ urządzenia, lokalizację, cel, dane kontaktowe oraz planowany czas.
- Blokada portu sieciowego zdejmowana jest tylko i wyłącznie przez pracowników proces controll.
- Po zdjęciu blokady portu należy wykonać test komunikacji i zgodności z polityką bezpieczeństwa.
- Zmiany w konfiguracji sieci muszą być rejestrowane.
- Po podłączeniu urządzenia należy przeprowadzić testy funkcjonalne oraz monitoring ruchu sieciowego przez minimum 24h.
- Dokumentacja architektury sieci powinna być aktualizowana po każdej zmianie.

3. Zasady dostępu dla firm zewnętrznych

- Dostęp możliwy tylko po podpisaniu umowy określającej zakres, czas i wymagania bezpieczeństwa.
 - Umowa powinna zawierać: zakres uprawnień, harmonogram dostępu, wymagania dotyczące uwierzytelniania, zasady monitorowania oraz procedurę zgłaszania incydentów.
 - Każda sesja zdalna musi być rejestrowana i przechowywana przez minimum 12 miesięcy.
 - Dostęp zdalny realizowany wyłącznie przez VPN z dwuskładnikowym uwierzytelnianiem i systemem PAM.
 - W uzasadnionych przypadkach dział process controll może nie wyrazić zgodny na przeprowadzenie prac w proponowanym terminie lub przez wyznaczonego przez firmę zewnętrzną programistę.
 - Zakres dostępu powinien być ograniczony wyłącznie do niezbędnych zasobów, a usługi podlegają monitorowaniu i przeglądowi w przypadku wystąpienia incydentu.
 - Dostęp do systemów krytycznych wymaga zatwierdzenia przez właściciela zasobu.
-

4. Wymagania techniczne i organizacyjne

- Sieć OT musi być fizycznie i logicznie oddzielona od sieci IT oraz od sieci publicznej (Internet).
- Segmentacja sieci powinna być realizowana przez VLAN, mikro segmentację oraz dedykowane strefy bezpieczeństwa (np. DMZ).
- Wymagana jest cykliczna inwentaryzacja wszystkich urządzeń sieciowych, gniazd, portów oraz szaf przemysłowych.
- Systemy operacyjne, firmware oraz aplikacje na urządzeniach sieciowych muszą być regularnie aktualizowane zgodnie z informacjami producentów.
- Krytyczne poprawki bezpieczeństwa powinny być wdrażane w jak najkrótszym czasie od daty publikacji.
- Backupy konfiguracji urządzeń pracujących w sieci OT oraz systemów krytycznych muszą być wykonywane codziennie i przechowywane w lokalizacji off-site oraz szyfrowane.
- Testy odtwarzania danych z backupu powinny być realizowane raz w roku.
- Dostęp do sieci OT z urządzeń mobilnych jest zabroniony.
- **Dopisać mirroring portów**

5. Polityka bezpieczeństwa i szkolenia

- Szkolenia z zakresu cyberbezpieczeństwa powinny być realizowane co najmniej raz w roku dla wszystkich pracowników i dostawców. **One page PC dla jumphost itp.**
- Testy socjotechniczne (np. phishing) powinny być przeprowadzane cyklicznie nie rzadziej niż z 1 letnim odstępem czasu.
- Polityka bezpieczeństwa musi być dostępna dla wszystkich pracowników i aktualizowana zgodnie z potrzebami.
- Wymagane jest prowadzenie dokumentacji architektury sieci, mapy ruchu sieciowego oraz wdrożenie polityk zarządzających ruchem sieciowym.
- Zaleca się organizowanie kampanii edukacyjnych oraz testów świadomości bezpieczeństwa.

6. Procedury reagowania na incydenty

- Każdy incydent musi być zgłoszony do zespołu bezpieczeństwa IT/OT w ciągu 1 godziny od wykrycia.
- Incydenty powinny być klasyfikowane według poziomu krytyczności i dokumentowane w systemie ticketowym.
- Po incydencie należy przeprowadzić analizę przyczynową (root cause analysis) i wdrożyć działania naprawcze.
- Raporty z incydentów powinny być przekazywane do kierownictwa oraz poddawane cyklicznej analizie trendów.

7. Polityka zarządzania zmianą

- Każda zmiana w infrastrukturze musi być zatwierdzona przez Change Advisory Board (CAB).
- Zmiany powinny być planowane, testowane i dokumentowane przed wdrożeniem.
- Wdrożenie zmiany musi być poprzedzone analizą ryzyka i planem przywracania.
- Po wdrożeniu zmiany należy przeprowadzić testy funkcjonalne oraz monitoring skutków.

8. Audyt

- Audyt bezpieczeństwa powinien być przeprowadzany co najmniej raz w roku przez niezależny zespół.
- Wyniki audytu muszą być raportowane do kierownictwa i skutkować planem działań korygujących.

9. Zarządzanie uprawnieniami

- Uprawnienia użytkowników powinny być nadawane zgodnie z zasadą najmniejszych uprawnień (least privilege).
- Przegląd uprawnień musi być realizowany minimum raz w roku.
- Dostęp do systemów krytycznych wymaga zatwierdzenia przez właściciela zasobu.
- Każda zmiana uprawnień powinna być dokumentowana i zatwierdzana.

10. Polityka backupu

- Backupy muszą być wykonywane codziennie dla systemów krytycznych.
- Kopie zapasowe powinny być przechowywane w lokalizacji off-site i szyfrowane. **Miesięczne**
- Testy odtwarzania danych z backupu powinny być realizowane raz w roku.
- Backupy powinny być monitorowane pod kątem poprawności i integralności.

12. Zarządzanie urządzeniami mobilnymi OT

- Urządzenia mobilne muszą być zarządzane przez system MDM (Mobile Device Management) w usłudze SNOW.
- Dostęp do sieci OT z urządzeń mobilnych jest zabroniony.
- Urządzenia muszą mieć aktywne szyfrowanie danych i możliwość zdalnego wymazania.
- Wymagane jest cykliczne aktualizowanie polityk bezpieczeństwa dla urządzeń mobilnych.

13. Polityka aktualizacji oprogramowania

- Aktualizacje systemów operacyjnych i aplikacji muszą być realizowane zgodnie z wymaganiami producentów systemów sterowania.
- Krytyczne poprawki bezpieczeństwa muszą być wdrażane w ciągu 72 godzin od publikacji.
- Systemy muszą być testowane po aktualizacji w środowisku testowym.

14. Zgodność z normami

- Infrastruktura IT/OT musi być zgodna z normami ISO/IEC 27001, IEC 62443 oraz NIST CSF. Sprawdzić te normy
- Wdrożenie standardów musi być udokumentowane i podlegać cyklicznym przeglądom.
- Wyniki audytów powinny być raportowane do zarządu i skutkować wdrożeniem działań naprawczych.