Wiceprezes Rady Ministrów
Minister Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Krzysztof Gawkowski

Warszawa, 24 lutego 2025 r.

KOMUNIKAT

w sprawie ataków na przemysłowe systemy sterowania (ICS/OT)

W ostatnim czasie zaobserwowano zwiększoną liczbę ataków na przemysłowe systemy sterowania (ICS/OT) dostępne bezpośrednio z internetu. Ataki te najczęściej są motywowane aktywistycznie lub politycznie i mają na celu medialne wykorzystanie udanego ataku. Odnotowano również zdarzenia, w których atak miał realny wpływ na działanie fizycznych systemów, a jego konsekwencje były odczuwalne dla użytkowników końcowych dostarczanej usługi.

W wielu przypadkach urządzenia przemysłowe podłączone są do internetu przez routery sieci komórkowych, a adresy IP im przypisane, wskazują na operatorów sieci mobilnych, których karty SIM zostały użyte. W takiej sytuacji nie ma możliwości dotarcia do właściciela systemu, można jedynie przekazać informacje do operatora telekomunikacyjnego.

W związku z powyższym zalecamy Jednostkom Samorządu Terytorialnego oraz innym podmiotom publicznym w zakresie wdrażania instalacji przemysłowych:

- Nie należy umożliwiać bezpośredniego zdalnego połączenia do instalacji przemysłowych systemów sterowania z wykorzystaniem protokołów, takich jak VNC czy RDP oraz oprogramowania zdalnego wsparcia technicznego.
- Nie należy umożliwiać bezpośredniego zdalnego dostępu do panelu WWW systemów sterowania i wizualizacji, nawet jeśli stosowane jest silne hasło.
- Nie należy udostępniać z otwartej sieci Internet portów komunikacyjnych, na których działają protokoły przemysłowe – w szczególności umożliwiające konfigurację urządzenia.
- Jeśli do odczytu lub sterowania procesem wymagany jest zdalny dostęp, należy skorzystać z VPN z wieloskładnikowym uwierzytelnianiem, co może się wiązać z dodatkową rozbudową konkretnej infrastruktury o niezbędne do tego celu urządzenia.
- W przypadku odnotowania incydentu cyberbezpieczeństwa związanego z instalacją przemysłową, należy bezzwłocznie dokonać zgłoszenia do właściwego CSIRT-u poziomu krajowego.

Dodatkowe środki bezpieczeństwa:

- Zmniejszenie do minimum ekspozycji sieci przemysłowej, zarówno sieci lokalnej, jak i punktów styku, poprzez identyfikację i ograniczenie do koniecznych połączeń „z" i „ do" tej sieci.

telefon: +48 22 245 59 22
adres email: sekretariat.dc@cyfra.gov.pl
adres strony internetowej: www.gov.pl/cyfryzacja

adres:
ul. Królewska 27
00-060 Warszawa

- Przeprowadzenie przeglądu zdalnego dostępu i ograniczenie go do niezbędnego minimum, w szczególności należy zwrócić uwagę na modemy komórkowe i metody zdalnego dostępu podwykonawców.
- W przypadku, gdy zdalny dostęp jest potrzebny, powinien być zawsze realizowany za pomocą VPN z wieloskładnikowym uwierzytelnianiem.
- Tam, gdzie to możliwe, ograniczenie dostępu do VPN dla określonych adresów IP lub ich zakresów. Przykładowo: gdy podmiot nie ma współpracowników ani podwykonawców zagranicznych, rekomenduje się ograniczenie możliwości nawiązania sesji VPN tylko dla polskich adresów IP.
- W przypadku, gdy niezbędne jest przesyłanie danych telemetrycznych do zewnętrznych systemów za pomocą sieci komórkowej, rekomenduje się wykorzystanie prywatnych sieci APN zakontraktowanych u operatora sieci komórkowej.
- Zmianę domyślnych danych uwierzytelniających z zastosowaniem dobrych praktyk związanych z silnymi hasłami (o ile urządzenie takie hasła wspiera) na wszystkich urządzeniach, w szczególności tych posiadających interfejs webowy (www), oraz wyłączenie niewykorzystywanych kont.
- W miarę możliwości, gdy nie ma przeciwwskazań, aktualizowanie wykorzystywanych systemów, w szczególności podczas planowanego wyłączenia instalacji.
- Stosowanie segmentacji sieci – wymaganie minimalne to separacja fizyczna lub logiczna sieci przemysłowej od innych sieci, a wymaganie preferowane, zależnie od rozmiaru i złożoności sieci, również wewnątrz sieci przemysłowej.
- Przeprowadzenie analizy widoczności urządzeń poprzez zewnętrzne skanowanie zakresu adresacji należącej do obiektu czy wykorzystanie narzędzi typu wyszukiwarka urządzeń sieciowych, czy wyszukiwarka podatności.
- Tam, gdzie to możliwe, zdalny dostęp powinien być realizowany na żądanie, co oznacza włączanie dostępu zdalnego na czas prac serwisowych. Każde prowadzenie zdalnych czynności w systemie powinno zostać odnotowane w sposób pozwalający jednoznacznie zidentyfikować czas, cel i źródło prowadzonych prac.
- Wykrywanie anomalii w ruchu sieciowym, czyli ruchu sieciowego odbiegającego od połączeń realizowanych podczas normalnego trybu pracy instalacji.
- Wzmacnianie konfiguracji wykorzystywanych urządzeń i oprogramowania przez wyłączenie niewykorzystywanych funkcji i konfigurację wbudowanych dodatkowych mechanizmów bezpieczeństwa. W domyślnie uruchamianych konfiguracjach często nie są one aktywne.
- Zgłoszenie osoby kontaktowej do właściwego CSIRT-u poziomu krajowego i systematyczna aktualizacja kontaktu w przypadku jego zmian. Celem tego jest usprawnienie ścieżki reakcji w przypadku wykrycia incydentu.

- Zarejestrowanie się w systemie n6 przez podanie swojej adresacji IP i domeny, co pozwoli na wysyłanie przez CERT Polska powiadomień w przypadku wykrycia nieprawidłowości.

Krzysztof Gawkowski
Wiceprezes Rady Ministrów
Minister Cyfryzacji
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

telefon: +48 22 245 59 22
adres email: sekretariat.dc@cyfra.gov.pl
adres strony internetowej: www.gov.pl/cyfryzacja

adres:
ul. Królewska 27
00-060 Warszawa