ENCON

THE FUTURE OF AUTOMATION

DYREKTYWA NIS2 I STANDARD IEC 62443

czyli co trzeba będzie zrobić w zakładach przemysłowych w zakresie IACS Cybersecurity

BROSZURA INFORMACYJNA

CZYM JEST DYREKTYWA NIS2?

Dyrektywa NIS2 (Network and Information System Directive) to regulacja prawna, która ma na celu zapewnienie wysokiego, jednolitego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej. Wprowadza rygorystyczne
przepisy dotyczące zarządzania ryzykiem i raportowania incydentów, rozszerza swój zakres o kolejne branże i nakłada surowe kary za nieprzestrzeganie przepisów.

Dyrektywa NIS2 weszła w życie 16 stycznia 2023 roku, natomiast termin implementacji nowych wymagań upływa 17 października 2024 roku. Po upływie tego terminu, nowe przepisy będą obowiązywać we wszystkich krajach Unii Europejskiej.

NIS2 WAŻNE TERMINY!

- Ogłoszenie ustawy (< 17.10.2024)
  wejście w życie 1 miesiąc od ogłoszenia
- Uruchomienie wykazu podmiotów
  1 miesiąc od wejścia w życie
- Realizacja obowiązków
  6 miesięcy od wejścia w życie
- Powołanie CSIRT sektorowych (Computer Security Incident Response Team) – 18 miesięcy od wejścia w życie

Dyrektywa NIS2

- Wdrożenie systemu zarządzania bezpieczeństwem informacji i systematyczne szacowanie ryzyka
- Obsługa i zgłaszanie incydentów poważnych
- Audyty bezpieczeństwa:
- Na własny koszt co najmniej raz na 2 lata, po razpierwszy w terminie 12 miesięcy od dnia spełnieniaprzesłanek do uznania za podmiot kluczowy lub ważny
- Wykonuje akredytowana jednostka oceniająca zgodność lub co najmniej 2 audytorów o określonych ustawą kompetencjach
- Obowiązkowe szkolenia z cyberbezpieczeństwa dlakadry kierowniczej oraz zalecane dla pracowników
- Wdrożenie procedur zarządzania ciągłością dostępności usług oraz łańcuchem dostaw
- Wdrożenie mechanizmów podwójnej autoryzacji, szyfrowania danych
- Zapewnienie bezpieczeństwa zasobów ludzkich, polityki kontroli dostępu i zarządzania aktywami
- Obowiązkowe szkolenia z cyberbezpieczeństwa dla kadry kierowniczej oraz zalecane dla pracowników
- Wdrożenie procedur zarządzania ciągłością dostępności usług oraz łańcuchem dostaw
- Wdrożenie mechanizmów podwójnej autoryzacji, szyfrowania danych
- Zapewnienie bezpieczeństwa zasobów ludzkich, polityki kontroli dostępu i zarządzania aktywami

NIS2 – sektory kluczowe

- Energetyka
- Transport
- Opieka zdrowotna
- Administracja publiczna
- Bankowość i infrastruktura rynku finansowego
- Infrastruktura cyfrowa, rejestry DNS
- Woda pitna i ścieki
- Przestrzeń kosmiczna

NIS2 – sektory kluczowe

- Dostawcy cyfrowi
- Przemysł spożywczy
- Przemysł chemiczny
- Produkcja
- Badania naukowe
- Gospodarka odpadami
- Usługi pocztowe i kurierskie

NIS2 KOGO DOTYCZY?

- Przedsiębiorstwa, które przynależą do określonego
- sektora (kluczowego lub ważnego)
- Wielkość – średnie lub większe
- Średnie – zatrudniające co najmniej 50 osób (<250)
- oraz obroty roczne lub roczna suma bilansowa wynoszą od 10 do 50 mln Euro

OBOWIĄZKOWA **„CHECK LISTA”**

- Czy posiadasz oprogramowanie do szyfrowania i kryptografii?
- Czy stosujesz uwierzytelnianie wieloskładnikowe lub ciągłe?
- Czy posiadasz aktualną politykę kontroli dostępui zarządzania aktywami?
- Czy wdrożyłeś procedury postępowania w przypadku ujawnienia podatności?

NIS2 **KARY**

- W przypadku podmiotów sektora kluczowego – może to być kara w wysokości do 10 mln EUR lub 2% łącznego rocznego światowego obrotu w poprzednim roku obrotowym
- W przypadku podmiotów sektora ważnego – może to być kara w wysokości do 7 mln EUR lub 1,4 % łącznego rocznego światowego obrotu w poprzednim roku obrotowym

www.encon.pl/security

Zapisz się już dzisiaj
na szkolenie lub zgłoś swoją
firmę na audyt bezpieczeństwa.

PODSTAWY CYBERBEZPIECZEŃSTWA DLA **PRACOWNIKÓW**

Celem szkolenia jest przekazanie uczestnikom podstawowej i aktualnej wiedzy na temat podstaw bezpieczeństwa cyfrowego oraz jej wykorzystania w pracy jak i prywatnie.

Uczestnik w trakcie szkolenia nauczy się w jaki sposób rozpoznawać podstawowe ataki, próby wyłudzenia, jak poprawić swoje bezpieczeństwo oraz jakie narzędzia wspomagające ten cel można stosować.

Program szkolenia opracowany został przez ekspertów Encon ponad 20 lat zajmujących się automatyką przemysłową i rozwiązaniami IT, którzy swoje doświadczenie potwierdzają uznanymi międzynarodowymi certyfikatami (ISA/IEC 62443, COMPTIA CASP+, CISA).

Każdy uczestnik otrzymuje certyfikat uczestnictwa w szkoleniu z zakresu cyberbezpieczeństwa zgodny z wymaganiami dyrektywy NIS2.

Program szkolenia

- Dlaczego bezpieczeństwo informacji i systemów jest istotne?
- Konsekwencje cyberataków
- Jakie są typy ataków i jak na nie reagować?
- Jakie są metody rozpoznawania i obrony przed atakami?
- Jak chronić swoje hasła i dane poufne?
- Gdzie szukać informacji o lukach bezpieczeństwa?

Umiejętności jakie dzięki szkoleniu uczestnik będzie potrafił

- Identyfikował zagrożenia cyberbezpieczeństwa
- Rozpoznawał ataki, których będzie celem, np. phishing
- Prawidłowo reagował w przypadku ataków, wycieków danych
- Zwiększał poziom bezpieczeństwa swoich urządzeń bądź systemów, z których korzysta na co dzień w pracy i prywatnie
- Wiedział, gdzie i jak szukać informacji na temat bezpieczeństwa
- W bezpieczny sposób przechowywał swoje poufne dane oraz hasła
- Znał zalety i metody korzystania z uwierzytelniania wieloskładnikowego (MFA) i kluczy fizycznych.

Czas trwania szkolenia
6 godzin.

CYBERBEZPIECZEŃSTWO W SYSTEMACH AUTOMATYKI PRZEMYSŁOWEJ

Celem szkolenia jest przekazanie uczestnikom wiedzy na temat planowania skutecznych, kompleksowych zabezpieczeń przed zagrożeniami w obszarze cyberbezpieczeństwa. Szkolenie przeznaczone jest dla osób technicznych odpowiedzialnych za zarządzanie i utrzymanie środowiska OT.

Zajęcia prowadzą certyfikowani trenerzy z wieloletnim praktycznym doświadczeniem. Obok teorii przedstawione są rzeczywiste przykłady ataków i wyłudzeń, które wydarzyły się w ostatnich miesiącach.

Uczestnicy zajęć otrzymują certyfikat ukończenia szkolenia, który jest potwierdzeniem wymagań zdefiniowanych w dyrektywie NIS2 w zakresie rozwoju kompetencji związanych z cyberbezpieczeństwem.

Program szkolenia

- czym różni się podejście do cyberbezpieczeństwa IT a IACS i jakie powinno mieć skutki praktyczne?
- definicja podstawowych zagrożeń dla systemów przemysłowych
- koncepcja „defense in depth"
- norma IEC 62443 podstawowe wymagania i oczekiwania, definicja poziomów bezpieczeństwa
- hardening stacji roboczych w sieciach przemysłowych
- rozwiązania VPN, ZTNA, SIEM, SOAR, IDS, FIREWALL i ich rola w sieciach przemysłowych
- kopie zapasowe w systemach IASC
- jak się przygotować do audytu cyberbezpieczeństwa – wstęp do analizy GAP w obszarze „IT/OT security"

Umiejętności jakie dzięki szkoleniu uczestnik będzie potrafił

- Określić niezbędną infrastrukturę sprzętową do realizacji założonych polityk cyberbezpieczeństwa
- Zdefiniować wymagania bezpieczeństwa dla obszaru IASC
- Uwzględniać wymagania cybersecurity dla przyszłych modernizacji obszaru IASC
- Uczestniczyć w analizach GAP security w obszarach OT

Czas trwania szkolenia
8 godzin.

AUDYT SPEŁNIENIA WYMAGAŃ DYREKTYWY NIS2 (GAP ANALYSIS)

Analiza luk w cyberbezpieczeństwie to proces mający na celu identyfikację i ocenę różnic między obecnym stanem cyberbezpieczeństwa organizacji a pożądanym poziomem ochrony. Proces dochodzenia do spełnienia poziomu bezpieczeństwa wymaganego przez przepisy może być mniej lub bardziej złożony i generować znaczne koszty.

Każda organizacja powinna rozpocząć ten proces od usługi audytu zerowego (GAP analysis) spełnienia wymagań dyrektywy NIS2 i ustawy o cyberbezpieczeństwie.

Audyt zerowy polega na przeprowadzeniu wywiadów i analiz istniejących procedur i wdrożonych rozwiązań w zakresie bezpieczeństwa i ciągłości funkcjonowania istotnych obszarów działalności audytowanej organizacji.

Nasze doświadczenie w systemach sterowania produkcją, znajomość specyfiki wymagań dla systemów IACS potwierdzone powszechnie uznanymi certyfikatami gwarantuje, że wykonywane przez nas usługi inżynierskie i audytorskie są na najwyższym poziomie. Audyt GAP oparty jest o wymagania ustawy oraz światowe normy i standardy w zakresie bezpieczeństwa, w tym między innymi:

- ISO/IEC 27001
- ISO 22301
- NIST SP 800-82
- NIST SP 800-53
- Wymagania i wytyczne Rządowego Centrum Bezpieczeństwa

Na podstawie wykonanej analizy **GAP security** powstanie raport stanu faktycznego wraz z zestawieniem prac koniecznych do wykonania (o ile będą zasadne) w celu uzyskania założonego poziomu cyberbezpieczeństwa w organizacji.

POZNAJ LIDERÓW BRANŻY

Bartłomiej Ryś

Ekspert z 23 letnim doświadczeniem w systemach automatyki przemysłowej

Certyfikaty
- DCS
- SCADA
- PLC
- ISA/IEC 62443 Cybersecurity Fundamentals Specialist
- ISA/IEC 62443 Cybersecurity Design Specialist
- ISA/IEC 62443 Cybersecurity Risk Assessment Specialist
- Siemens Functional Safety Professional - IEC 61511

Michał Kołodziejczyk

25 lat doświadczenia w IT

Certyfikaty
- MCT
- COMPTIA CASP +
- CISA – Certified Information System Auditor

ENCON
THE FUTURE OF AUTOMATION

ENCON Sp. z o.o.
ul. Kwiatkowskiego 8
52-407 Wrocław PL
NIP: PL8992535167
www.encon.pl