Cyberbezpieczeństwo w przemyśle, dyrektywa NIS2

TOMASZ KAWKA

Kierownik projektu w Introl Automatyka Sp. z o.o.
Pełnomocnik do spraw cyberbezpieczeństwa świadczonych usług kluczowych zgodnych z normami PN-EN ISO/IEC 27001:2017-06, PN-EN ISO22301: 2020-04 oraz RODO.

tel. 601 553 336

Cyberbezpieczeństwo jest kluczowym elementem współczesnego zarządzania technologią i informacją, którego głównym celem jest ochrona systemów komputerowych, sieci oraz danych przed nieautoryzowanym dostępem, atakami i uszkodzeniami.

Wśród tworzących się zagrożeń wykorzystujących podatności systemów lub błędy ludzkie należy wymienić ataki na systemy sterowania, ransomware oraz ataki na łańcuch dostaw. Ze względu na wprowadzenie Przemysłu 4.0, wzrosły głównie podatności branży produkcyjnej. Okazało się, że najważniejszymi funkcjami cyberbezpieczeństwa w obecnym momencie stają się ochrona danych i infrastruktury, zapobieganie przestojom, zachowanie reputacji oraz określone podejście do bezpieczeństwa wskazywane przez regulacje prawne.

Unia Europejska, aby zwiększyć odporność sektorów gospodarki, opracowała dyrektywę NIS2 dla całej UE na początku 2023 roku (Dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium UE), której wdrożenie **zaplanowano na 17 października 2024 roku**. Obecnie znamy jedynie projekt implementującej dyrektywę nowelizacji polskiej ustawy o krajowym systemie cyberbezpieczeństwa.

ZMIANY NARZUCANE PRZEZ AKT PRAWA – DYREKTYWĘ NIS2

Do najważniejszych zmian wprowadzonych dyrektywą NIS2 należą:

- Znacznie rozszerzony zakres podmiotowy.
- Wyrównanie obowiązków dla dwóch głównych grup: podmiotów kluczowych i ważnych, wśród których znajdują się podmioty z sektora automatyki przemysłowej.
- Osobista odpowiedzialność zarządu za nadzór i wdrożenie przepisów.
- Wysokie kary finansowe nakładane na organizację za nieprawidłowości w stosowaniu się do wymogów nowego prawa. W przypadku powstania nieprawidłowości dla podmiotu kluczowego jest to co najmniej 10 000 000 EUR lub 2% całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego, przy czym zastosowanie będzie mieć kwota wyższa. Dla podmiotów ważnych kary to: co najmniej 7 000 000 EUR lub 1,4% całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego, przy czym zastosowanie będzie mieć kwota wyższa.

NIS2: Podmioty ważne i kluczowe
(uwaga: oprócz sektora/branży, ważna jest też wielkość przedsiębiorstwa)
(kolorem pomarańczowym zaznaczono branże ważne dla sektora automatyki przemysłowej)

SEKTORY KLUCZOWE	SEKTORY KLUCZOWE/WAŻNE
ENERGETYKA • **Energia elektryczna**: przedsiębiorstwa energetyczne zajmujące się wytwarzaniem, dystrybucją i obsługą punktów ładowania. • **System ciepłowniczy**: operatorzy systemów ciepłowniczych i chłodniczych. • **Ropa naftowa**: operatorzy ropociągów oraz instalacji związanych z produkcją, przetwarzaniem, magazynowaniem i przesyłem ropy naftowej. • **Gaz**: przedsiębiorstwa dostarczające gaz, operatorzy systemów dystrybucyjnych, przesyłowych, magazynowania, LNG oraz instalacji rafinacji i przetwarzania gazu ziemnego. • **Wodór**: produkcja, magazynowanie i przesył wodoru. **OPIEKA ZDROWOTNA** • **Świadczeniodawcy** • **Podmioty produkujące leki**: produkcja leków, substancji i krytycznych wyrobów medycznych, działalność B&R w zakresie produktów leczniczych, laboratoria referencyjne EU. **INFRASTRUKTURA CYFROWA** • Dostawcy punktu wymiany ruchu internetowego • Dostawcy usług chmurowych • Dostawcy usług zaufania • Dostawcy publicznych sieci łączności elektronicznej **ZARZĄDZANIE USŁUGAMI ICT** • Dostawcy usług zarządzanych • Dostawcy usług zarządzanych w zakresie bezpieczeństwa. **WODA PITNA** • **Dostawcy i dystrybutorzy wody pitnej** odpowiedzialni za dostarczanie wody przeznaczonej do spożycia przez ludzi. **ŚCIEKI** • **Przedsiębiorstwa zbierające, odprowadzające lub oczyszczające ścieki**: komunalne, bytowe lub przemysłowe oczyszczalnie ścieków.	• **Wyroby medyczne i diagnostyka in vitro**: narzędzia, aparaty, oprogramowanie, implanty i odczynniki stosowane w medycynie i badaniach laboratoryjnych. • **Komputery, wyroby elektroniczne i optyczne** • **Urządzenia elektryczne**: generatory prądu, baterie, ładowarki, odkurzacze i otwieracze do puszek. • **Inne maszyny i urządzenia**: • **Pojazdy samochodowe, przyczepy i naczepy** • **Pozostały sprzęt transportowy** • **Produkcja i dystrybucja chemikaliów (w tym budowlanych)**: przedsiębiorstwa zajmujące się produkcją substancji chemicznych oraz ich dystrybucją, w tym klejów, cementu i innych materiałów budowlanych. • **Produkcja i dystrybucja żywności**: przedsiębiorstwa spożywcze zajmujące się przemysłową produkcją i przetwarzaniem żywności oraz dystrybucją hurtową. • **Gospodarowanie odpadami**: firmy zajmujące się zarządzaniem odpadami, z wyłączeniem tych, dla których gospodarowanie odpadami nie jest główną działalnością gospodarczą. • **Badania naukowe**

Tabela 1
Podmioty ważne i kluczowe według NIS2

NOWE OBOWIĄZKI

W ramach nowych obowiązków należy wymienić:

- Raportowanie – każde zagrożenie, które nosi znamiona incydentu (najprawdopodobniej zdefiniowanego zgodnie z normą ISO/IEC 27001), będzie musiało zostać zgłoszone w ciągu 24 godzin do CSIRT (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego), wraz z opisem jego przyczyny.

Do najważniejszych zmian wprowadzonych dyrektywą NIS2 należą osobista odpowiedzialność zarządu za nadzór i wdrożenie przepisów oraz wysokie kary finansowe za nieprawidłowości w stosowaniu się do wymogów nowego prawa.

- Obowiązek natychmiastowej reakcji na incydent wraz z jego raportowaniem, obejmującym również opis incydentu z propozycją rozwiązania problemu (tzw. CAPA).
- Nowe wymagania w zakresie dynamicznych analiz ryzyka, regularnych testów i audytów, tworzenia i aktualizowania planów ciągłości działania, szkoleń (zwłaszcza kadry zarządzającej), opracowywania planów naprawczych.

Dyrektywa NIS2 zwraca również uwagę na powstałe zagrożenia dla łańcucha dostaw i powiązanych partnerów (usługodawców) przedsiębiorstwa. Negatywne zdarzenie (incydent) może spowodować powstanie incydentu (kompromitacji) w organizacjach współpracujących, dlatego powstaje obowiązek wykazywania szczególnej staranności w doborze usługodawców/kontrahentów.

Producenci od dawna wykorzystują systemy sterowania przemysłowego dla zwiększenia szybkości i wydajności produkcji. Dotąd jednak systemy sterowania produkcją były w znacznej mierze odseparowane od systemów administracyjnych i innych procesów realizowanych w przedsiębiorstwach.

ZAGROŻONA INFRASTRUKTURA TO GŁÓWNIE OT

Sieci technologii operacyjnej (OT) współpracują z sieciami technologii informacyjnej (IT) i wykorzystują szeroką gamę inteligentnych, połączonych urządzeń IoT na dużą skalę. Pojedynczy zakład produkcyjny może mieć dziesiątki tysięcy urządzeń i czujników IoT, które wysyłają stały strumień danych do zewnętrznych sieci lub systemów w chmurze. Producenci używają wielu urządzeń IoT, takich jak: kamery monitoringu, cyfrowe oznakowania, systemy automatyzacji budynków oraz kontroli środowiskowych.

Czujniki i urządzenia IoT nie zawsze posiadają wbudowane mechanizmy bezpieczeństwa, a stosunkowo niedawna popularyzacja IoT wpływa na brak historii podatności związanej z bezpieczeństwem IT tych urządzeń wykorzystywanych w przemyśle. Połączenie urządzeń IoT oraz wykorzystanie nie zawsze bezpiecznej chmury, wraz ze rozszerzoną łącznością, stwarzają duże możliwości przeprowadzania frontalnych, niespotykanych wcześniej ataków. Operacje bezpieczeństwa w procesach produkcji wymagają analizy zautomatyzowanej w czasie rzeczywistym całych sieci. To pozwala przedsiębiorstwom proaktywnie wykrywać i reagować na zagrożenia w trakcie ich trwania, zanim wyrządzą szkody.

ZACHOWANIA CYBERPRZESTĘPCÓW W PRZEMYŚLE PRODUKCYJNYM

W wielu przypadkach wielkość analityki związanej z podejrzanym ruchem sieciowym jest dwukrotnie większa niż w pozostałych sektorach gospodarki. Niektórzy producenci mają niewystarczającą kontrolę nad możliwością dostępu do linii produkcyjnych z powodów biznesowych. Nowoczesne systemy bezpieczeństwa współpracują z archaicznymi urządzeniami, co może zakłócać i izolować systemy produkcyjne. Wiele fabryk łączy urządzenia IoT z płaskimi, niepodzielonymi sieciami, które polegają na komunikacji wszystkiego ze wszystkim: od komputerów z aplikacjami przedsiębiorstwa po maszyny. Coraz częściej

tego typu struktury są bezpośrednio podłączane do Internetu, aby generować dane telemetryczne i zapewnić zdalne zarządzanie.

Według Jürga Affoltera, CIO w Brugg Cables, *Wzrost liczby urządzeń przemysłowego IoT wykładniczo zwiększa powierzchnię ataku na producentów, a wdrożenie ciągłego monitorowania sieci wewnętrznej pod kątem zachowań atakujących oraz dodatkowych kontroli dostępu jest ważne, ponieważ rozwiązanie oparte na agentach nie jest możliwe dla urządzeń przemysłowego IoT.*[1]

Najczęściej występującymi zagrożeniami dla przemysłu 4.0 są: zagrożenia związane z tzw. zewnętrzną jednostką zarządzania i kontroli, zagrożenia związane z rozpoznaniem wewnętrznych słabości organizacji. Gdy atakujący ustanowi przyczółek w urządzeniach IoT, systemy bezpieczeństwa sieci często mają trudności z identyfikacją takiego zaplanowanego dostępu, tzw. „Backdoor". Typowe zachowania związane z wewnętrznym rozpoznaniem w przemyśle produkcyjnym obejmują wewnętrzne skanowanie sieci przedsiębiorstwa (INTRANET) i skanowanie protokołu Server Message Block (SMB), czyli protokołu sieciowego udostępniania plików i struktury danych. Przestępcy dokonują w ten sposób inwentaryzacji urządzeń w sieci przedsiębiorstwa przez wykrycie adresów IP urządzeń.

Dodatkowo, sieci produkcyjne składają się z wielu bram (routerów) komunikujących się z inteligentnymi urządzeniami i maszynami. Analityka połączeń tych urządzeń pozwala odkryć (zmapować) urządzenia w sieci produkcyjnej w poszukiwaniu krytycznych zasobów do kradzieży lub uszkodzenia. Zagrożenia obejmują zachowania związane z Lateral Movement (stopniowe poruszanie się po sieci w poszukiwaniu kluczowych danych i zasobów) oraz eksfiltracją (ekstrakcja) danych.

Ochrona w sektorze przemysłowym, niezależnie od wyzwań ery Przemysłu 4.0, wymaga kompleksowego podejścia, które obejmuje zarówno techniczne, jak i organizacyjne środki bezpieczeństwa:

- segmentacja sieci,
- monitorowanie i analiza ruchu sieciowego,
- zarządzanie dostępem,
- regularne aktualizacje i łatki (patch),
- szkolenia i świadomość pracowników,
- kopia zapasowa i plan odzyskiwania danych,
- współpraca z ekspertami,
- zgodność z regulacjami,
- bezpieczeństwo fizyczne,
- testy penetracyjne.

CO POWINNAM/POWINIENEM ZROBIĆ?

- Wykonać tzw. audyt podatności i braków w organizacji – tzw. **GAP ANALYSIS**. Pozwoli to określić stan faktyczny organizacji w ujęciu wymagań prawnych. Taki audyt powinien być przeprowadzony przez jednostkę zewnętrzną.
- Przygotować się do sporządzenia **samodeklaracji** jednostki, wykorzystując w/w audyt.
- Przeprowadzić konsultacje z audytorem zewnętrznym w oparciu o **specjalne matryce odpowiedzialności**.
- Już teraz przeprowadzać **testy oprogramowania automatycznej detekcji i wykrywania zagrożeń** z tworzeniem automatycznego raportowania incydentów.
- Rozważyć możliwość **outsourcingu analityki** do odpowiedniej jednostki SOC, czyli Security Operations Center.
- Odpowiednio przygotować prace związane z wdrożeniem w przedsiębiorstwie wymogów ustawy.
- W przypadku zidentyfikowania zagrożenia konieczny jest **natychmiastowy kontakt** z dostawcą rozwiązania.

> ***Czujniki i urządzenia IoT nie zawsze posiadają wbudowane mechanizmy bezpieczeństwa, a stosunkowo niedawna popularyzacja IoT wpływa na brak historii podatności związanej z bezpieczeństwem IT.***

Problematyka cyberbezpieczeństwa to temat tak obszerny, że nie sposób szczegółowo omówić jej na łamach kilku stron. A jest to temat krytyczny dla większości organizacji. Brak działań w zakresie zabezpieczenia cyfrowej komunikacji w zakładzie może skutkować bowiem nie tylko ogromnymi karami finansowymi, ale również całkowitą utratą zdolności prowadzenia działalności.

Podobnie złożony problem dotyczy samej Dyrektywy NIS2, której wdrożenie wymaga specjalistycznej wiedzy. Dlatego wszystkie opisane prace przygotowawcze, audytowe oraz usługi wdrożeniowe dotyczące oprogramowania czy zabezpieczenia już zaszyfrowanego systemu, warto przekazać profesjonalnej firmie posiadającej niezbędne kompetencje i doświadczenie w tego typu wdrożeniach.

[1] – www.vectra.ai