INTROL Automatyka Sp. z o.o.
ul. Kościuszki 112
40-519 Katowice

Monika Wolańczyk
+48 785 901 227
mwolanczyk@introlautomatyka.pl

Jak zniwelować lukę GAP pomiędzy celami biznesowymi a celami technicznymi przy wdrażaniu nowych technologii informatycznych AI/ML uwzględniając konieczność wdrożenia zmian wynikających z cyberbezpieczeństwa.

Monika Wolańczyk
Starszy Specjalista ds. Walidacji
Pełnomocnik SZJ

Jesteśmy obecnie świadkami wdrażania u wielu wytwórców farmaceutycznych i wyrobów medycznych w Europie zarządzania cyber-ryzykiem w związku z Dyrektywą NIS 2. Zmiany dotyczą również branży life-science i Health Care. Oznacza to, że tysiące podmiotów po raz pierwszy podlega rygorystycznym wymogom bezpieczeństwa sieci i informacji. W przemyśle farmaceutycznym i wyrobów medycznych wymagana jest integracja dotychczasowych systemów jakości (GMP/GDP, MDR/IVDR) z reżimem cyber w całym łańcuchu wartości – od R&D i wytwarzania po dystrybucję i serwis.

Cyfrowy paradoks: tempo zmian kontra stabilność GxP

Napisanie artykułu eksperckiego w dzisiejszych realiach to paradoks. Mimo powszechnego dostępu do zaawansowanych narzędzi, największym wyzwaniem staje się aktualność wiedzy. To, co dziś jest trafnym wynikiem analizy, za miesiąc lub trzy wymaga rewizji na podstawie nowych raportów. Tempo rozwoju platform danych w chmurze, Sztucznej Inteligencji (AI), Uczenia Maszynowego (ML) oraz technologii cyberbezpieczeństwa jest zawrotne. Sytuacja ma charakter dynamiczny i rozwojowy.

Dyrektywa NIS 2 dodaje nową warstwę: obowiązkowe środki zarządzania ryzykiem (m.in. polityki, zarządzanie podatnościami, bezpieczeństwo łańcucha dostaw, ciągły monitoring) oraz krótkie terminy notyfikacji incydentów do właściwych organów. Wymogi te są bardziej szczegółowe w cyber sferze niż klasyczne standardy jakości, co

INTROL Automatyka Sp. z o.o.
ul. Kościuszki 112
40-519 Katowice

Monika Wolańczyk
+48 785 901 227
mwolanczyk@introlautomatyka.pl

wywołuje ryzyko kolizji proceduralnych. Wdrożenie kontroli cyber w systemach IT/OT/ICS może wymagać zmian w infrastrukturze, które następnie muszą być zgodnie z cGMP/EU GMP i zwalidowane, udokumentowane oraz utrzymane w stanie kontrolowanym, aby nie naruszyć integralności danych i ciągłości procesu wytwórczego, umów kontraktowych. Patrząc na to z punktu zgodności w wymaganiami branżowymi obowiązującymi w przemyśle farmaceutycznym, zarówno obecnymi jak i wchodzącymi zaktualizowanymi zapisami EU GMP, (w tym Aneksu 11 oraz nowego Aneksu 22) potrzebne jest opracowanie strategii i planów działania. Planowanie rozwoju cyfrowego w firmie pozwala kontrolować i dostosowywać postępowanie do przyjętej strategii działania, aby nie pogrążyć się łatwo w chaosie i dużych kosztach biznesowych.

EU GMP/GDP historycznie koncentrują się na bezpieczeństwie pacjenta, jakości produktu i integralności danych (ALCOA+), a nie na szczegółowej topologii zabezpieczeń sieci, detekcji zagrożeń czy zarządzaniu podatnościami. NIS 2 przesuwa punkt ciężkości na proaktywną cyberodporność: segmentację, aktualizacje i łatanie, EDR-System do wykrywania i reagowania na zagrożenia na urządzeniach końcowych/SIEM-System zbierający i analizujący zdarzenia z całej infrastruktury IT/SOC-zespół (lub centrum) ludzi, którzy monitorują i reagują na incydenty cyber, testy penetracyjne, zarządzanie incydentami oraz nadzór nad dostawcami (także oprogramowania i komponentów OT).

W rezultacie typowe dla farmacji cykle „kwalifikacji i walidacji" (DQ/IQ/OQ/PQ) muszą zostać zsynchronizowane z cyklem życia zabezpieczeń, tak aby aktualizacje wymagane przez bezpieczeństwo nie stały w sprzeczności z kontrolą zmian GMP i nie wymuszały zamrożenia wersji z ryzykiem technicznego długu bezpieczeństwa. Jest to szczególnie newralgiczne w zakładach wykorzystujących systemy sterowania (DCS/PLC/SCADA), dotąd często pomijane w formalnych reżimach cyber, a dziś wyraźnie znalazły się w zakresie NIS 2 dla podmiotów krytycznych czy ważnych.

Dodatkowo NIS 2 wprowadza szybką notyfikację incydentów (z reguły w 24h) – implementacja tego wymogu obliguje do ujednolicenia globalnych procedur reagowania w korporacjach, ustalenia jednoznacznych kryteriów „istotności" incydentu oraz utrzymania gotowości do gromadzenia materiału dowodowego w sposób spójny z GMP (audytowalność, nieusuwalność logów, kontrola dostępu). W praktyce oznacza to formalne połączenie planów reagowania na incydenty (IRP) z systemem jakości i rewalidacji systemów skomputeryzowanych (CSV), by raportowanie organom NIS 2 nie naruszało obowiązku zapewnienia integralności danych w procesach krytycznych.

INTROL Automatyka Sp. z o.o.
ul. Kościuszki 112
40-519 Katowice

Monika Wolańczyk
+48 785 901 227
mwolanczyk@introlautomatyka.pl

Chciałabym wspomnieć też o wytwórcach i dystrybutorach wyrobów medycznych, dla których bezpieczeństwo cyfrowe kojarzone jest jako cecha jakości wyrobu medycznego.

NIS 2 obejmuje również producentów określonych kategorii wyrobów medycznych i podmioty z ich łańcucha wartości. W epoce urządzeń połączonych (zdolność urządzenia do nawiązywania i utrzymywania zdalnie połączenia, zdalne aktualizacje oprogramowania wysyłane przez Internet, bez potrzeby fizycznego dostępu do urządzenia, interoperacyjność z systemami szpitalnymi) Internet staje się elementem bezpieczeństwa wyrobu i ciągłości świadczeń zdrowotnych. Dyrektywa podkreśla znaczenie bezpieczeństwa dostawców i raportowania incydentów, co wymaga integracji praktyk inżynierskich (secure-by-design, SBOM, zarządzanie podatnościami) z procesami MDR/IVDR i nadzoru po wprowadzeniu wyrobu na rynek. W rezultacie zarządzanie ryzykiem cyber nie może być doklejką po certyfikacji wyrobu medycznego – staje się częścią planu monitorowania bezpieczeństwa i efektywności wyrobu medycznego na rynku.

Na poziomie operacyjnym pomocne są wytyczne techniczne i mapowania wymagań publikowane przez ENISA, które wspierają organizacje w dowodzeniu spełnienia wymogów NIS 2 (np. przykładowe dowody kontroli, powiązania z aktami wykonawczymi KE, praktyki dla łańcucha dostaw i zarządzania podatnościami). Materiały te ułatwiają audytowalność i mogą ograniczać fragmentację wdrożeń między krajami członkowskimi.

Jeśli wytwórcy produktów leczniczych i wyrobów medycznych nie mają określonej w tym obszarze strategii i planów działania na najbliższe 2, 3 lata będzie im coraz trudniej działać efektywnie w obecnej rzeczywistości.

Trudno sobie wyobrazić brak ustalonej strategii postępowania i wynikających z niej Planów operacyjnych dla poszczególnych obszarów działania.

Planowanie bez strategii to lista życzeń a realizacja takiego planu prowadzi do dobrze zaplanowanej i zrealizowanej porażki.

Strategia bez planu wyznacza cel, jednak brak dobrego planu i realizacji kończy się staniem w miejscu.

Aby dobrze przygotować strategię i plany rozwojowe warto zacząć od przeglądu okresowego systemów skomputeryzowanych i uzgodnić go ze spisem aktywów w firmie.

INTROL Automatyka Sp. z o.o.
ul. Kościuszki 112
40-519 Katowice

Monika Wolańczyk
+48 785 901 227
mwolanczyk@introlautomatyka.pl

O zaletach takiego podejścia pisałam np. w artykule „Przełom 2023/2024 obowiązkowy przegląd okresowy systemów skomputeryzowanych, ważniejszy niż zazwyczaj wobec wyzwań najnowszych technologii AI/ML" Świat Przemysłu Farmaceutycznego (nr 04/2023).

Bardzo prawdopodobna luka i pomysły co zrobić

Zacznę od moich „ulubionych" kolizji prawnych i operacyjnych, które zignorowane lub źle zarządzane prowadzą, jak nigdzie indziej, do bardzo poważnych konsekwencji wraz z cofnięciem zezwolenia na wytwarzanie lub dopuszczenie do obrotu, a w najgorszym wypadku wycofanie produktu lub wyrobu medycznego w rynku.

a) Model „top-down" zarządzania i odpowiedzialność zarządu.

Należy ustanowić formalne role i KPI-cyber na poziomie zarządu i zintegrować z komitetem jakości/GxP. To nie tylko dobra praktyka – NIS 2 przewiduje mechanizmy odpowiedzialności kierownictwa, a niektóre kraje wprowadzają dodatkowe wymogi w tym obszarze

b) Zsynchronizowana kontrola zmian (GMP) i cykl życia zabezpieczeń (NIS 2).

Warto wdrożyć „dwutorową" kontrolę zmian: ścieżka „szybkich" aktualizacji bezpieczeństwa (łatki krytyczne, segmentacja, reguły detekcji) z uprzednio zdefiniowaną metodyką oceny wpływu na walidację, oraz ścieżkę „pełną" dla zmian funkcjonalnych wymagających pełnej rewalidacji. Pozwoli to pogodzić wymóg cyberodporności z zasadą „state of control" w GMP.

c) Jednolity program zarządzania dostawcami.

Kwalifikacja dostawców (GxP) wymaga rozszerzenia o kryteria cyber:

- praktyki SDLC to uporządkowany sposób tworzenia oprogramowania, a Secure SDLC zapewnia, że bezpieczeństwo jest częścią procesu, a nie dodatkiem.
- zarządzanie podatnościami,
- ciągłość działania,
- przejrzystość SBOM to pełna wiedza o tym, z czego zbudowane jest oprogramowanie, umożliwiająca szybkie wykrywanie i ograniczanie ryzyka cyberzagrożeń.

INTROL Automatyka Sp. z o.o.
ul. Kościuszki 112
40-519 Katowice

Monika Wolańczyk
+48 785 901 227
mwolanczyk@introlautomatyka.pl

Warto zastosować proporcjonalne podejście do krytyczności komponentów i lokalnych progów krajowych w UE, które mogą się różnić między państwami członkowskimi.

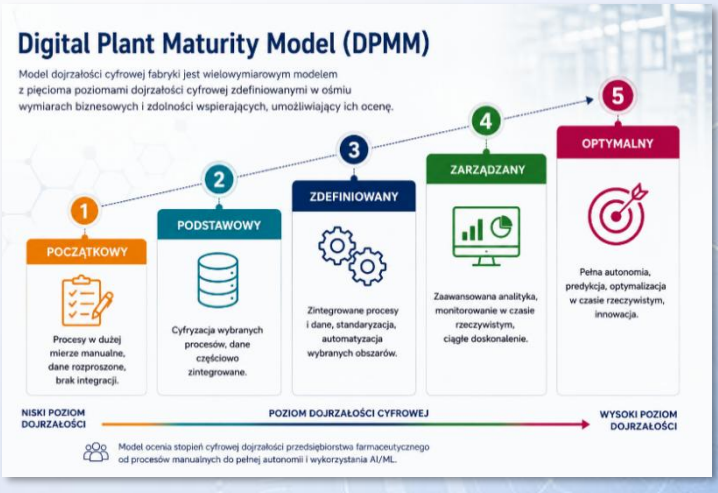
d) Ujednolicone raportowanie incydentów.

Zadania konieczne do wykonania to zdefiniowane progi istotności zgodne z NIS 2, przypisane role (Dyrektor ds. Bezpieczeństwa Informacji- CISO, Zapewnienie Jakości - QA, lokalny koordynator ds. NIS), przygotowane szablony zgłoszeń i scenariusze symulacji sytuacji kryzysowych, tak aby 24-godzinne okno raportowe było wykonalne, bez naruszania wymogów integralności danych i tajemnicy przedsiębiorstwa.

Bardzo ważna współpraca w zespołach multidyscyplinarnych.

Wdrożenie zmian w obszarze cyberbezpieczeństwa, to nie tylko, jak potocznie się słyszy „sprawa Działów IT". Co może pójść nie tak opisałam m.in. w artykule „Zmień niewiedzę i wątpliwości w pewność" w Świat Przemysłu Farmaceutycznego (nr 04/2025). Należy dokładnie przedyskutować zakres i potrzeby walidacji oraz specyfikacji, wymagań od dostawców i producentów oprogramowania i architektury rozwiązań, która ma działać w obszarach krytycznych dla GxP i cyberbezpieczeństwa.

Różny poziom kultury jakości w firmach farmaceutycznych, zróżnicowanie procesów jak i poziomu modernizacji linii wytwarzania oraz Laboratoriów Kontroli Jakości badających różne postacie leków sprawia, że nie ma jednego dobrego scenariusza wdrożenia i doskonalenia rozwiązań z zakresu cyberbepieczeństwa oraz utworzenia jednej odpowiedniej architektury do przetwarzania danych dla wszystkich. Kluczowe jest przygotowanie danych dla rozwiązań korzystających z narzędzi Sztucznej Inteligencji i Uczenia Maszynowego. Wykonywanie tych zadań bez odpowiedniej komunikacji przy chociażby nadawaniu dostępu w zależności od ról i uprawnień, może być bardzo wymagającym zadaniem.



Warto moim zdaniem przypomnieć Digital Plant Maturity Model (DPMM) opracowany w biofarmacji. Model dojrzałości cyfrowej fabryki jest wielowymiarowym modelem z pięcioma poziomami dojrzałości cyfrowej zdefiniowanymi w ośmiu wymiarach biznesowych i zdolności

INTROL Automatyka Sp. z o.o.
ul. Kościuszki 112
40-519 Katowice

Monika Wolańczyk
+48 785 901 227
mwolanczyk@introlautomatyka.pl

wspierających, umożliwiający ich ocenę. Model opracowano, aby ocenić aktualny status cyfryzacji wytwórcy i zaprojektować rozwój w oparciu o dostępne technologie procesowe i informatyczne a potem monitorować i mierzyć postęp techniczny i technologiczny. Osoby zainteresowane odsyłam do artykułu pt. „Planowanie rozwoju cyfrowego wytwórcy farmaceutycznego w oparciu o sprawdzony model DPMM stosowany w biofarmacji"; „Świat Przemysłu Farmaceutycznego" nr (04/2020) To model oceny, jak bardzo zakład produkcyjny jest zdigitalizowany i zintegrowany — od papieru do pełnej autonomii.

Najczęściej obejmuje obszary:

- Procesy produkcyjne
- Dane i ich wykorzystanie
- Automatyka i IT/OT
- Integracja systemów
- Decyzyjność (manualna vs data-driven)

Zainspirowana tym modelem opracowałam **Ocenę poziomu dojrzałości wdrożenia NIS2 w firmie farmaceutycznej** ułatwiającą stworzenie i dopasowanie tzw. mapy drogowej dla transformacji między poziomami, aby wskazać obszary wymagające doskonalenia w pierwszej kolejności lub wykazania posiadania wysokiej zgodności i wdrożenia zabezpieczeń zgodnie z NIS 2. Zapraszam do skorzystania z kodu QR na naszym stanowisku i wykonania samooceny dostępnej na stronie www.introlautomatyka.pl/farmacja/uslugi lub pod linkiem **Ocena poziomu dojrzałości wdrożenia NIS2**

Metodyka oceny poziomu dojrzałości wdrożenia NIS 2 w firmie farmaceutycznej

Ocena została oparta na wynikach uzyskiwanych na podstawie odpowiedzi na pytania zapisanie w formie - checklisty obejmującej obszary:

- zarządzania ryzykiem cyberbezpieczeństwa,

INTROL Automatyka Sp. z o.o.
ul. Kościuszki 112
40-519 Katowice

Monika Wolańczyk
+48 785 901 227
mwolanczyk@introlautomatyka.pl

- ładu organizacyjnego i odpowiedzialności zarządczej,
- bezpieczeństwa systemów IT i danych GxP,
- reagowania na incydenty i ciągłości działania,
- nadzoru nad dostawcami i chmurą.

Każdy obszar oceniany jest pod kątem:

- formalizacji (polityki, procedury),
- wdrożenia operacyjnego,
- audytowalności,
- integracji z systemem jakości (GxP).

Pytania mają charakter audytowy - jest to zgodne z metodą samooceny dojrzałości. W odpowiedzi na każde pytanie należy zaznaczać tyle odpowiedzi – ile opisuje prawidłowo

Średnia ze wszystkich ocen daje wynik ogólny i poziom scharakteryzowany zgodnie z poniższą tabelą:

POZIOM	NAZWA POZIOMU	CHARAKTERYSTYKA
0 0 – 0	**Brak dojrzałości**	Organizacja **nie posiada formalnych zasad TAK. ani procesów związanych z NIS2. Działania są przypadkowe lub nie występują wcale. Brakuje odpowiedzialności, dokumentacji oraz świadomości zagrożeń.**
1 1 – 0,1	**Początkowy**	Podejmowane są pojedyncze działania związane z bezpieczeństwem, jednak mają charakter ad hoc i nie są ustandaryzowane. Świadomość wymagań NIS2 jest ograniczona, a procesy nie są formalnie opisane.
2 2 – 0,25	**Podstawowy**	Organizacja posiada podstawowe polityki i procedury bezpieczeństwa. Część wymagań NIS2 została wdrożona, jednak działania są niespójne lub obejmują tylko wybrane obszary. Brakuje pełnego nadzoru i systematyczności.
3 3 – 0,5	**Zdefiniowany**	TAK. jest integralną częścią strategii organizacji i procesów biznesowych. Organizacja stale doskonali swoje działania, automatyzuje procesy oraz aktywnie reaguje na nowe zagrożenia i wymagania regulacyjne.
4 4 – 0,75	**Zarządzany**	Organizacja monitoruje skuteczność procesów bezpieczeństwa i regularnie je ocenia. Wykorzystywane są wskaźniki, audyty oraz mechanizmy nadzoru. Zarządzanie ryzykiem jest prowadzone w sposób ciągły i świadomy.
5 5 – 1,0	**Optymalny**	Cyberbezpieczeństwo jest integralną częścią strategii organizacji i procesów biznesowych. Organizacja stale doskonali swoje działania, automatyzuje procesy oraz aktywnie reaguje na nowe zagrożenia i wymagania regulacyjne.

INTROL Automatyka Sp. z o.o.
ul. Kościuszki 112
40-519 Katowice

Monika Wolańczyk
+48 785 901 227
mwolanczyk@introlautomatyka.pl

status działań wykonywanych w firmie. Odpowiedź na jedno pytanie będzie zawierała nie tylko 1, ale może 2, 3 lub 4 zaznaczenia na TAK. Brak

Raport z oceny dojrzałości wdrożenia NIS 2, zawiera:

- uśrednioną ocenę poziomu dojrzałości organizacji,
- punktową ocenę poszczególnych obszarów bezpieczeństwa,
- wskazanie obszarów wymagających dalszego doskonalenia,
- rekomendacje kolejności w jakiej należy wykonać działania wspierające zwiększenie poziomu zgodności i odporności cyberbezpieczeństwa.

Raport został opracowany z uwzględnieniem specyfiki sektora farmaceutycznego, w którym szczególne znaczenie mają ciągłość działania, bezpieczeństwo danych oraz zgodność regulacyjna.

Pozwala przygotować dopasowaną do zasobów strategię i plany operacyjne.

Podsumowanie:

Zapraszam do wykonania oceny dojrzałości, by przeanalizować poziom zgodności z NIS 2. Jest to dobry początek i pomoc w monitorowaniu postępu prac w obszarze cyberbezpieczeństwa ze szczególnym uwzględnieniem zgodności z regulacjami GxP.

Statyczne przyglądanie się i czekanie nie rozwiąże problemów długu technologicznego. Związane są z nim ryzyka takie jak:

- regulacyjne – niezgodności z GxP i zatrzymania produkcji lub produktu w obrocie,
- operacyjne – przestojów produkcyjnych i związanych z tym strat finansowych
- konkurencyjne – brak nowoczesnych narzędzi Sztucznej Inteligencji/gromadzenia danych,
- cyber – utrata danych i reputacji,

realnie zagrażają obecnie firmom farmaceutycznym.

Dobra strategia i planowanie rozwoju cyfrowego w firmie pozwala kontrolować i dostosowywać rozwiązania do potrzeb i przeciwdziała kosztownemu chaosowi.