Zamień niewiedzę i wątpliwości w pewność

Monika Wolańczyk
Starszy Specjalista ds. Walidacji
Introl Automatyka

Czy wiesz, że wytwórców farmaceutycznych i kontraktowych, jak i dystrybutorów obowiązują w Europie i Polsce specjalne dedykowane przepisy prawne odnoszące się do systemów skomputeryzowanych, z jakich korzystają? **Pytanie to warto obecnie zadać producentom i dostawcom systemów skomputeryzowanych wdrażanych w obszarze cyberbezpieczeństwa**..

Regulacje obowiązujące wytwórców farmaceutycznych a także wytwórców kontraktowych wymagają zgodności z wymaganiami prawnymi tzw. Dobrej Praktyki Wytwarzania (DPW). (Dz.U. 2022 poz. 1273 Obwieszczenie Ministra Zdrowia z dnia 28 kwietnia 2022 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Ministra Zdrowia w sprawie wymagań Dobrej Praktyki Wytwarzania)

Przepisy te odnoszą się bezpośrednio do systemów skomputeryzowanych – Aneks 11 oraz walidacji i kwalifikacji – Aneks 15. Wytwórcy muszą je spełniać, aby uzyskać i utrzymać zezwolenie na wytwarzanie. Spełnianie tych regulacji jest weryfikowane przez inspekcję farmaceutyczną przed wydaniem Zezwolenia na wytwarzanie, jak i podczas systematycznych inspekcji wykonywanych co najmniej co 3 lata, po uruchomieniu działalności. W zależności od typu i zakresu prowadzonej działalności, wymagania te również dokładnie sprawdzają/kontrolują Audytorzy zewnętrzni firm zlecających różne usługi w ramach kontraktowego wytwarzania (np. produkcji, pakowania, kontroli jakości itp.).

Łańcuch dystrybucji produktów leczniczych i wyrobów medycznych w Europie podlega również dedykowanym przepisom, które wymagają walidacji i kwalifikacji systemów skomputeryzowanych, z jakich korzysta dystrybutor, pośrednik w obrocie, hurtownia farmaceutyczna. (Dz.U. 2022 poz. 1287 Obwieszczenie Ministra Zdrowia z dnia 24 maja 2022 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Ministra Zdrowia w sprawie wymagań Dobrej Praktyki Dystrybucyjnej – DPD). Regulacje te opisuje punkt 3.5 odnoszący się do Systemów skomputeryzowanych i 3.6 Kwalifikacja i Walidacja.

W Aneksie 11 DPW zapisana Reguła wprost wskazuje, że dotyczy wszystkich rodzajów systemów skomputeryzowanych stosowanych w działalności podlegającej działaniom DPW. Z tego względu możemy mieć pewność, że zastosowanie modernizacji czy wprowadzenie nowych rozwiązań podnoszących poziom bezpieczeństwa w zakresie sprzętu i oprogramowania sieciowego oraz systemów operacyjnych wspierających działanie aplikacji w ramach infrastruktury, jak też aplikacji działających na określonej platformie czy sprzęcie komputerowym, to przepisy w randze branżowych uszczegóławiających. **Należy je powiązać zgodnie z ich zakresem z wymaganiami NIS 2 dotyczącymi cyberbezpieczeństwa w EU**.

Każde wykorzystywane oprogramowanie, jak i infrastruktura podlegają kwalifikacji i nie mogą zwiększać ogólnego ryzyka dla jakości produktu leczniczego, poziomu kontroli procesu oraz zapewnienia jakości. Zapisy prawne Aneksu 11 odnoszą się do całego cyklu życia systemu, co oznacza wszystkie etapy funkcjonowania systemu skomputeryzowanego od wymagań wstępnych przez projektowanie, specyfikację, programowanie, testowanie, instalację w środowisku docelowym, eksploatację i utrzymanie, aż do wycofania włącznie.

W związku z powyższym dostawcy i usługodawcy wspierający firmy farmaceutyczne w zakresie oprogramowania zwiększającego cyberbezpieczeństwo, powinni zapoznać się z nimi, aby wiedzieć, jakie wymagania muszą spełnić dodatkowo w tym obszarze.

Każdy z dostawców i usługodawców podlega ocenie jego kompetencji i rzetelności. W ramach Kwalifikacji dostawców lub producentów oprogramowania oraz usług sprawdzana/weryfikowana jest: dokumentacja, informacje dotyczące systemu jakości, podejście do kwalifikacji i walidacji systemu, aby udowodnić, że system skomputeryzowany został stworzony zgodnie z odpowiednim Systemem Zarządzania Jakością. W zależności od oceny ryzyka wymagane jest przeprowadzenie audytu, którego wyniki muszą być dostępne na żądanie inspektorów do spraw wytwarzania Głównego Inspektoratu Farmaceutycznego. Jest to wpisane w wymagania Aneksu 11.

Na potrzeby kwalifikacji dostawców rozwiązań z zakresu cyberbezpieczeństwa polecam wykorzystanie metodologii Gamp 5 ed. 2. Dostarcza ona w sposób syntetyczny opis niezbędnych działań, jakie należy podjąć, aby uzyskać zgodność z przepisami regulacyjnymi uwzględniając specyfikę działania systemów skomputeryzowanych i różne ich kategorie. Pomaga w tworzeniu uzasadnienia dla różnych podejść w kwalifikacji i zakresu dokumentacji dla systemów.

Wdrażanie wymagań związanych z cyberbezpieczeństwem może prowadzić do zakłóceń operacyjnych.

Narzędzia cyberbezpieczeństwa nie mogą być zaimplementowane bez procesu rozwoju i testowania oprogramowania, również pod kątem cyberbezpieczeństwa, ponieważ mają ten sam potencjał wprowadzania błędów jak każde inne oprogramowanie.

W zależności od architektury oprogramowania może spowodować ono i wywołać szeroki zakres zakłóceń w działaniu usług do katastrofalnych włącznie.

Rolą dostawców rozwiązań zabezpieczających w ramach infrastruktury operacyjnej jest przedstawienie metod zapobiegania temu zagrożeniu i pomóc opracować plan łagodzenia jego skutków.

Pojawia się konieczność przygotowania dodatkowej strategii obniżania ryzyka w celu oceny i przeciwdziałania potencjalnym zagrożeniom wynikającym ze stosowania oprogramowania zabezpieczającego.

Zabezpieczenie łańcucha dostaw oprogramowania

Szybki postęp w technologii cyfrowej i tempo rozwoju spowodowały, że projekty programistyczne są bardzo złożone. Wdrażane aplikacje często zawierają kod i zależności pochodzące z różnych źródeł (komercyjnych, open source i komponentów od różnych poddostawców). Korzystanie z oprogramowania z różnych źródeł pomaga tworzyć i wdrażać szybciej, efektywniej, ograniczając koszty oraz zwiększa skalowalność i interoperacyjność. Stwarza to jednak rozległą płaszczyznę do wykorzystywania luk w zabezpieczeniach przez złośliwe podmioty.

„Coroczny raport firmy Synopsys "Open Source Security and Risk Analysis", w którym przeanalizowano bazy kodu pod kątem luk w zabezpieczeniach i konfliktów licencji, wykazał, że 96% z około 1700 przeskanowanych baz kodu zawierało komponenty open source. Ale chociaż wiele aplikacji opiera się na bibliotekach open source, ten kod może nie być całkowicie godny zaufania”.

Zapewnienie bezpieczeństwa wymaga posiadania wyczerpującej listy wszystkich bibliotek kodu, komponentów i zależności używanych w tworzeniu projektów oprogramowania.

Taka kompleksowa inwentaryzacja pod nazwą SBOM (Software Bill of Materials) – zestawienia materiałów oprogramowania – stała się kluczowym elementem bezpiecznego cyklu życia tworzenia oprogramowania.
SBOM zawiera co najmniej informacje o każdym składniku oprogramowania:

- nazwa, data wydania i numer wersji,
- nazwa dostawcy i dane kontaktowe,
- zależności przechodnie,
- informacje o licencjonowaniu,
- lista skojarzonych znanych luk w zabezpieczeniach i ich środków zaradczych.

Raporty SBOM mogą być tworzone ręcznie, przez zespoły zaangażowane w proces tworzenia oprogramowania lub automatycznie, za pomocą narzędzia do generowania oprogramowania.

Chociaż posiadanie aktualnych SBOM bezpośrednio nie zapobiega cyberatakom na systemy IT, to pomaga złagodzić potencjalne wektory ataków. Mając wgląd we wszystkie komponenty, można śledzić zabezpieczenia i luki w czasie rzeczywistym, zanim wykorzystają to cyberprzestępcy.

Pozwala też na szybką identyfikację naruszonych komponentów w przypadku incydentu związanego z bezpieczeństwem, skracając czas potrzebny na zbadanie i rozwiązanie zaistniałego problemu.

Nowe i zmieniające się przepisy dotyczące bezpieczeństwa wymagają obecnie od dostawców oprogramowania spełnienia tych surowych wymagań.

Utrzymanie zgodności z wymaganiami prawnymi GxP zmian wdrażanych na potrzeby cyberbezpieczeństwa

Warto więc włączyć powyższe wymaganie do audytu dostawców rozwiązań, oprogramowania i usług z zakresu cyberbezpieczeństwa dla procesów GxP. Dopiero pozytywny wynik pozwala na zawieranie umów zakupu, wdrożenia i serwisowania oprogramowania oraz usług (Serwis Lewel Agreement – SLA). **Chcąc utrzymać zgodność z Aneksami 11 i 15 przy wdrażaniu cyberzabezpieczeń, należy wykonać stosowną ocenę w procesie kontroli zmian.**

Działania te związane są z wdrożeniem zmian dotyczących obszaru GxP i wymagają przeglądu oraz modyfikacji dokumentacji związanej z zarządzaniem ryzykiem, specyfikacjami infrastruktury czy oprogramowania, a także przetwarzania danych przy zachowaniu ich integralności i bezpieczeństwa.

Musimy tu uwzględnić oprócz rekwalifikacji i rewalidacji związanej z testowaniem integracji również testowanie bezpieczeństwa danych.

Należy pamiętać o uzupełnieniu listy oprogramowania działającego w zakresie procesów podlegających wymaganiom Dobrej Praktyki Wytwarzania, bo jest to również wymóg prawny.

Integracja działań pozwalających spełniać wymagana NIS2 i GxP dotyczy całego cyklu życia systemu skomputeryzowanego i należy ją wdrożyć od etapu wyboru rozwiązań, na podstawie wyników z przeprowadzenia testów penetracyjnych.

Przy wyborze producenta i dostawcy oprogramowania ważne jest potwierdzenie, czy wprojektowywanie bezpieczeństwa (Secure by Design) traktował priorytetowo przy rozwoju produktu.

Etap projektowania w nowych technologiach informatycznych, w tym generatywnej sztucznej inteligencji (Generative Artificial Intelligence – GenAI) powinien uwzględniać bezpieczeństwo.

Eksperci z zakresu cyberbezpieczeństwa stwierdzają, że nowe technologie i nowe produkty niestety nie zabezpieczają nas przed popełnianiem tych samych błędów.

Sprzedaż niepewnych produktów i zarabianie dodatkowo na ich zabezpieczeniach, wskazują na dbanie tylko o poziom własnych dochodów.

Dowodzi to, że nie kierowano się zasadą zaprojektowania bezpiecznego oprogramowania sprzedawanego klientom od początku stosując bezpieczny cykl życia oprogramowania (System Development Life Cycle – SDLC).

Firmy farmaceutyczne jako klienci, wdrażając produkty oprogramowania zabezpieczającego, ufają, że zapobiega ono atakom i potrafi wyeliminować całe klasy wad. Natomiast jeśli przeciwnicy zdołają nam zagrozić, to producent i/lub dostawca szczerze i otwarcie będą się z nami komunikować, aby przeciwdziałać tym zagrożeniom.

Certyfikowany Audytor Systemów Informatycznych (Certified Information Systems Auditor, CISA) powinien wspierać te działania w zakresie standaryzacji bezpieczeństwa już na etapie projektowania.

Sztuczna Inteligencja (Artificial Intelligence – AI) w rozwiązaniach na potrzeby zapewnienia cyberbezpieczeństwa zapewnia jeszcze przewagę obrońcom, ponieważ jest trenowana zarówno w oparciu o zachowania w punkcie końcowym, jak i w chmurze, zamiast wykrywania opartego na sygnaturach.

Generatywna sztuczna inteligencja (GenAI) przy zwiększaniu siły roboczej, mocy i produktywności jednostek, wspiera i daje przewagę SOC (Security Operations Center) – centrum obrony i bezpieczeństwa, co ma na celu zwiększenie produktywności i umożliwienie AI podejmowania decyzji obronnych pod nadzorem ludzi.

Kwestie bezpieczeństwa AI w rozumieniu mechanizmów przeciwstawnych, których można użyć do manipulowania systemami GenAI są dopiero w bardzo wczesnej fazie badań. Natomiast zabezpieczenie aplikacji internetowych nie daje 100% pewności skuteczności. Pewnym rozwiązaniem na teraz jest AI jako wewnętrzna stacja robocza, do której nie mają dostępu zewnętrzni przeciwnicy.

Wszystko dlatego, że nie rozumiemy w pełni jak możemy zostać zmanipulowani i jak do końca działają te systemy. Jesteśmy w fazie obserwacji co się dzieje, jak szybko działać, jeśli wykryjemy nową manipulację.

Zespół do zarządzania bezpieczeństwem powinien współpracować z zespołem oceniającym bezpieczeństwo techniczne i technologiczne oraz osobnym zespołem audytowym.

Brak realnego zarządzania ryzykiem lub działania pozorowane sprawią prędzej niż później, że ryzyko zacznie zarządzać nami.

Podsumowanie

Do obecnej sytuacji wymagającej wdrożenia zmian podnoszących bezpieczeństwo cybernetyczne w firmie działającej w obszarze regulacji GxP możemy podejść dwojako. Możemy przyjąć postawę ofensywną – działać predykcyjnie i wykonać przegląd pod kątem bezpieczeństwa, współpracować z zespołem cyberbezpieczeństwa, komunikować oraz rejestrować zmiany, oceniać ryzyko i wpływ zmian na działalność podlegającą regulacjom GxP. Dobre planowanie z udziałem firm mających doświadczenie we wdrażaniu systemów skomputeryzowanych zgodnie z GxP i kompetentnych w zakresie zapewnienia cyberbezpieczeństwa, to rozsądnie podejście pozwalające dodatkowo zaoszczędzić czas i pieniądze, aby wybrać dopasowane do potrzeb klienta rozwiązania zgodne z GxP i NIS2.

Natomiast postawa pasywna opiera się na pozostawieniu systemów z obszaru GxP i posiadanej dokumentacji bez wdrożenia i zrozumienia wpływu istotnych zmian w całej firmie przez NIS2. Grozi to poważnymi brakami w dokumentacji (w szczególności dotyczy to rekwalifikacji, rewalidacji, wycofania ryzykownych systemów, dostępu do danych rejestrowanych przez usuwane systemy itp.), bez testowania oraz monitorowania wpływu zmian, zgodnie z Aneksem 11, w odpowiednim zakresie.

Narażać to będzie firmy na utratę komunikacji, przestoje wynikające z wprowadzenia działań po audycie bezpieczeństwa bez konsultacji i prezentacji wymagań środowiska i systemów skomputeryzowanych działających w obszarze GxP. Działanie reaktywne skierowane wyłącznie na awarie i incydenty lub negatywne raporty z inspekcji GIF czy audytów, będą bardziej kosztowne, jeśli chodzi chociażby o straty w wyniku przestojów, kary za niespełnianie wymagań, konieczność zakupu innych rozwiązań, utrata środków na systemy niespełniające wymagań NIS2 i GxP w konsekwencjach mogą zagrozić płynnej działalności firmy. ■