



Lista kontrolna Audyt dostawcy ICT **NIS2 i DORA**

wersja 20240808

Ustalając, czy nasz dostawca nie wprowadza żadnych zagrożeń w zakresie cyberbezpieczeństwa i utrzymania ciągłości działania pomocna może być weryfikacja poniższych obszarów. **Każda odpowiedź NIE wymaga weryfikacji**, choć nie w każdym przypadku oznacza problem.

Pierwszym krokiem jest przeprowadzenie analizy ryzyka i ustalenie, którzy z naszych dostawców i podwykonawców są istotni dla naszej działalności operacyjnej. Na podstawie **mapy ryzyka** określamy, których dostawców i poddostawców traktujemy w sposób szczególny i z wysokim priorytetem, a których możemy pominąć. Prawdopodobnie dla produktów i usług krytycznych pojawi się konieczność prześledzenia kolejnych podmiotów w łańcuchu dostaw. W wielu miejscach wystarczy oświadczenie dostawcy, ale u dostawców krytycznych i ważnych należy przeprowadzić audyt na miejscu. Jednocześnie określimy, czy ważne jest dla nas bezpieczeństwo i ciągłość działania dostawcy lub podwykonawcy, czy też ważne jest bezpieczeństwo i ciągłość działania dostarczonego produktu.

Badając stabilność i odporność na zagrożenia podwykonawcy warto zacząć od następujących pytań w poszczególnych obszarach.

1 WIARYGODNOŚĆ DOSTAWCY/PODWYKONAWCY

- ☐ Czy dostawca jest wiarygodny, tj. czy posiada:
 - ☐ wiedzę?
 - ☐ doświadczenie?
 - ☐ możliwości produkcyjne?
 - ☐ możliwości formalne?
- ☐ Czy nie ma ograniczeń prawnych i innych, które utrudniają lub uniemożliwiają współpracę?
- ☐ Czy siedziba i miejsce wykonywania pracy (usług) przez dostawcę jest dostępne i pozwala na przeprowadzenie audytu?

2 SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

- ☐ Czy dostawca ma świadomość, na odpowiednim szczeblu zarządzania, konieczności posiadania takiego systemu?
- ☐ Czy są wyznaczone osoby, które odpowiadają za całość systemu, za poszczególne polityki i procedury?
- ☐ Czy każdy z zasobów informacyjnych ma właściciela (osobę odpowiedzialną)?
- ☐ Czy istnieje polityka zarządzania bezpieczeństwem informacji, jako oficjalny dokument wewnętrzny, który jest regularnie przeglądany i aktualizowany?
- ☐ Czy istnieją procedury związane z bezpieczeństwem informacji w poszczególnych obszarach, czy są regularnie przeglądane i aktualizowane?
- ☐ Czy pracownicy na poszczególnych stanowiskach pracy mają świadomość jakie zasady ich obowiązują i czy się do nich stosują?
- ☐ Czy dostawca opracował mapę ryzyka, czy wyznaczył osoby za nią odpowiedzialne, czy dokonuje regularnych jej przeglądów i aktualizacji?
- ☐ Czy efekty prowadzenia mapy ryzyka mają przełożenie na działania praktyczne?

- ☐ Czy istnieje rejestr przeglądów dokumentacji związanej z systemem bezpieczeństwa informacji, czy są wyznaczone osoby odpowiedzialne za te przeglądy, czy przeglądy odbywają się regularnie?
- ☐ Czy istnieje rejestr procesów wykonywanych cyklicznie w ramach zarządzania bezpieczeństwem informacji, czy procesy te są wykonywane, czy mają przypisane osoby odpowiedzialne?
- ☐ Czy poddostawca jest zgodny z normą ISO/EIC 27001 (lub podobną), czy jest to potwierdzone wiarygodnym audytem i czy zakres wdrożenia odpowiada naszym potrzebom?

3 CIĄGŁOŚĆ DZIAŁANIA I ŚWIADCZENIA USŁUG DOSTAWCY

- ☐ Czy dostawca posiada zidentyfikowane mapy zagrożeń dotyczących ciągłości działania (świadczenia usług)?
- ☐ Czy posiada polityki i procedury monitorowania i aktualizowania map ryzyka?
- ☐ Czy do poszczególnych zadań i obszarów są przypisane osoby odpowiedzialne?
- ☐ Czy wnioski z analiz ryzyka przekładają się na sposób działania dostawcy, czy istotne zagrożenia są zaadresowane operacyjnie?
- ☐ Czy analizy ryzyka i wdrożone rozwiązania obejmują:
 - ☐ łańcuch dostaw?
 - ☐ bezpieczeństwo fizyczne?
 - ☐ cyberbezpieczeństwo?
 - ☐ personel?
 - ☐ infrastrukturę?
- ☐ Czy istnieją plany awaryjne, czy są regularnie przeglądane i aktualizowane, czy mają przypisane osoby odpowiedzialne?
- ☐ Czy są opracowane plany i procedury na wypadek wystąpienia sytuacji kryzysowe?
- ☐ Czy możliwe sytuacje kryzysowe są poprawnie zidentyfikowane?
- ☐ Czy istnieje system zapewnienia ciągłości podejmowania decyzji w sytuacjach nagłych i kryzysowych?

- ☐ Czy dostawca ma wdrożony znormalizowany system zarządzania ciągłością działania według normy ISO 22301 lub podobny, który jest audytowany i certyfikowany przez wiarygodną organizację?
- ☐ Czy zakres wdrożenia systemu zarządzania ciągłością działania jest zgodny z naszymi potrzebami jako klienta?

4 PERSONEL (PRACOWNICY, WSPÓŁPRACOWNICY, KONSULTANCI) DOSTAWCY

- ☐ Czy istnieje procedura zatrudniania personelu, która ma właściciela i jest regularnie przeglądana i aktualizowana oraz wdrożona w praktyce?
- ☐ Czy dostawca weryfikuje kompetencje i wiarygodność personelu przed i po zatrudnieniu?
- ☐ Czy umowy podpisywane z personelem we właściwy sposób regulują kwestie własności intelektualnej, odpowiedzialności oraz poufności?
- ☐ Czy wnioski z analiz ryzyka przekładają się na sposób działania dostawcy, czy istotne zagrożenia są zaadresowane operacyjnie?
- ☐ Czy dostawca ma wystarczający kontakt z pracownikami, pozwalający na zapewnienie bezpieczeństwa organizacji i produktu?
- ☐ Czy wpływ pracowników zdalnych, zewnętrznych i podlegających słabej kontroli, na bezpieczeństwo organizacji i produktu (błędy, pomyłki, sabotaż) jest zminimalizowany?
- ☐ Czy szkolenia dla personelu (wstępne i cykliczne) zapewniają wystarczający poziom bezpieczeństwa i ciągłości działania?
- ☐ Czy dostawca monitoruje poziom motywacji i dobrostan personelu kluczowego dla bezpieczeństwa i ciągłości działania?
- ☐ Czy utrzymywanie aktualnej wiedzy i znajomości zasad i procedur personelu jest adekwatne do potrzeb organizacji w zakresie bezpieczeństwa i ciągłości działania?

- ☐ Czy wiedza ta jest sprawdzana i uzupełniana cyklicznie i w miarę potrzeb?
- ☐ Czy szkolenia personelu uwzględniają bezpieczeństwo i ciągłość działania?
- ☐ Czy organizacja pracy, w tym przydzielanie i odbieranie dostępów i uprawnień oraz sprzętu, jest właściwa z perspektywy bezpieczeństwa i ciągłości działania?
- ☐ Czy są wdrożone i czy działają poprawnie procedury zwalniania personelu?

5 REJESTR INCYDENTÓW

- ☐ Czy dostawca prowadzi rejestr incydentów dotyczących bezpieczeństwa i ciągłości działania?
- ☐ Czy rejestr ten jest dostępny dla osób, które powinny incydenty zgłaszać?
- ☐ Czy procedura zgłaszania, obsługi i zamykania incydentów jest ustalona i stosowana w praktyce oraz czy ma sens z naszego punktu widzenia?
- ☐ Czy statystyki dotyczące rejestru incydentów wykazują na faktyczne używanie i użyteczność tego narzędzia?

6 BEZPIECZEŃSTWO FIZYCZNE

- ☐ Czy siedziba, biura i miejsca pracy dostawcy są zgodne z naszymi oczekiwaniami i potrzebami w zakresie wymagań prawnych oraz z punktu widzenia bezpieczeństwa i ciągłości działania?
- ☐ Czy pomieszczenia są wystarczająco zabezpieczone przed niepowołanym dostępem?
- ☐ Czy istniejące zabezpieczenia fizyczne faktycznie działają i chronią przed kradzieżą lub sabotażem?

- ☐ Czy pomieszczenia są wystarczająco zabezpieczone przed zdarzeniami losowymi typu pożar, powódź, brak zasilania?
- ☐ Czy usytuowanie drzwi, okien, przejść względem monitorów, tablic i ekranów zapewnia bezpieczeństwo informacji?
- ☐ Czy ściany drzwi i stropy wystarczająco tłumią dźwięk, aby co najmniej chronić przed przypadkowym podsłuchaniem rozmowy/spotkania?

7 INFRASTRUKTURA ICT

- ☐ Czy używane przez dostawcę urządzenia takie jak komputery, czy telefony są wykorzystywane w sposób gwarantujący wystarczający poziom bezpieczeństwa przed:
 - ☐ niepowołanym dostępem?
 - ☐ utratą danych i informacji?
 - ☐ cyberatakami, w tym przejęciem w celu dalszego wykorzystania?
 - ☐ sabotażem?
- ☐ Czy urządzenia sieciowe i serwery są zabezpieczone zgodnie ze standardami obowiązującymi w danym sektorze?
- ☐ Czy istnieją procedury, narzędzia, osoby odpowiedzialne dotyczące monitorowania bezpieczeństwa i ciągłości działania?
- ☐ Czy oprogramowanie jest na bieżąco i w sposób bezpieczny aktualizowane?
- ☐ Czy są prowadzone testy penetracyjne i podobne i czy ich wyniki mają wpływ na infrastrukturę?
- ☐ Czy wszystkie elementy infrastruktury mają przypisane osoby odpowiedzialne?
- ☐ Czy zasady przydzielania dostępów i weryfikacji użytkowników, autoryzacji i autentykacji są zgodne ze współczesnymi standardami i stosowane?

8 PERSONEL DS. BEZPIECZEŃSTWA

- ☐ Czy istnieje w organizacji zespół odpowiedzialny za bezpieczeństwo i ciągłość działania?
- ☐ Czy struktura organizacyjna, w której funkcjonuje ten zespół, spełnia nasze potrzeby?
- ☐ Czy zakres uprawnień i obowiązków członków tego zespołu jest zgodny z potrzebami (tj. czy zespół na faktyczny wpływ na utrzymanie bezpieczeństwa)?
- ☐ Czy osoby niepowołane, w szczególności z zewnątrz, NIE mają możliwości ustalenia tożsamości osób mających faktyczny wpływ na działanie systemu bezpieczeństwa (tj. czy tożsamość osób mających realny wpływ na krytyczne obszary systemu bezpieczeństwa jest dostatecznie chroniona)?

W zakresie bezpieczeństwa **produktu** (na przykład oprogramowania lub urządzenia z oprogramowaniem lub usług) należy sprawdzać dodatkowo i niezależnie aspekty wymienione poniżej. W wielu przypadkach – jeśli zakup produktu kończy nasze relacje z dostawcą – tylko bezpieczeństwo produktu końcowego ma znaczenie.

9 BEZPIECZEŃSTWO OPROGRAMOWANIA (PRODUKTU LUB USŁUG)

- ☐ Czy procedury produkcji, testowania, wdrażania i utrzymania są zgodne z realnymi potrzebami i aktualnymi praktykami w zakresie bezpieczeństwa i ciągłości działania?
- ☐ Czy na podstawie posiadanych informacji możemy stworzyć skuteczny plan zapewnienia ciągłości działania?
- ☐ Czy warunki utrzymania i wsparcia (SLA) są znane i akceptowalne ze względu na poziom ryzyka?
- ☐ Czy zakres znanych z rynku i przekazanych przez dostawcę informacji pozwala na stworzenie mapy ryzyka związanej z wdrożeniem i utrzymaniem produktu?

- ☐ Czy istnieje w organizacji zespół odpowiedzialny za bezpieczeństwo i ciągłość działania?
- ☐ Dla produktów/usług powszechnie dostępnych i sprawdzonych na rynku:
 - ☐ Czy na podstawie historii stosowania produktu możliwa jest ocena podatności na cyberataki i stabilności tego rozwiązania i czy ta ocena odpowiada naszym potrzebom?
- ☐ Dla produktów usług na zamówieni lub jednostkowych:
 - ☐ Czy procedury bezpieczeństwa w procesie produkcji (świadczenia usług) gwarantują odpowiednie parametry produktu?
 - ☐ Czy proces produkcji i wdrażania jest zabezpieczony przed sabotażem?
 - ☐ Czy architektura i zastosowane rozwiązanie uwzględniają oczekiwany poziom bezpieczeństwa i ciągłości działania produktu?
 - ☐ Czy wymagania dotyczące wdrożenia i wykorzystania uwzględniają wymagania w zakresie bezpieczeństwa i ciągłości działania?
- ☐ Czy istniejące w umowach „gwarancje bezpieczeństwa i ciągłości działania” mają znaczenie praktyczne, w szczególności, czy wykraczają poza rozwiązania formalne i obejmują proaktywne podejście do tematu (tj. inne niż kary umowne).

Powyższa lista ma charakter orientacyjny i powinna być ograniczana lub rozszerzana zgodnie z faktycznymi potrzebami.

Nowe przepisy wymuszają na wielu organizacjach zapewnienie podwyższonego poziomu cyberbezpieczeństwa. Przepisy, szczególnie NIS2, nie są jak dotychczas zbyt szczegółowe, jeśli idzie o wymagania techniczne, systemowe, czy organizacyjne. Zalecają natomiast działania zgodne z dobrymi praktykami, czy zasadami sztuki w danym momencie. Pierwszym krokiem i naturalnym krokiem będzie przygotowanie rozwiązań formalnych i dokumentacji, która zdejmie z nas odpowiedzialność lub przeniesie część tej odpowiedzialności na inne podmioty, czy też wykaże, że dochowaliśmy wystarczającej i należytej staranności.

Prawdziwe wyzwanie wiąże się z tym, że zagrożenia cyberatakami, czy nawet sabotaże są realne, pewnie będą się zdarzać, a poza skutkami samego zdarzenia grożą nam dotkliwe i odstraszające kary nakładane w konsekwencji wdrożenia przepisów UE. Prawdziwym testem wdrożonych przez nas rozwiązań będzie nie tylko przejście audytu, ale również faktyczna ciągłość działania (lub jej brak). Co oznacza, że do wszelkich zagrożeń powinniśmy podejść bardzo praktycznie i pragmatycznie. Szukając rozwiązań optymalnych ze względu na koszty i faktyczną skuteczność.

Zainteresowanych praktycznym podejściem do kwestii bezpieczeństwa i ciągłości działania w obszarach związanych z ICT prosimy o kontakt.



CISO

Adam Dawidziuk



+48 660 401 200



a.dawidziuk@7bulls.com