CYBERBEZPIECZEŃSTWO

Wymogi NIS 2 - analiza ryzyka ICT. Implementacja nowych wymagań

Analiza ryzyka ICT oznacza ocenę zagrożeń, podatności oraz skutków potencjalnych incydentów związanych z utratą poufności, integralności, dostępności lub autentyczności danych i systemów.

TOMASZ KAMIŃSKI

Adwokat, Wspólnik w Kancelarii Krzysztof Rożko i Wspólnicy,

DANIEL NIWIŃSKI

Prawnik, Ekspert ds. cyberbezpieczeństwa w Kancelarii Krzysztof Rożko i Wspólnicy

Nowa dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa (dyrektywa NIS 2) stawia przed wieloma podmiotami wyzwania, które wykraczają poza samą technologię. Spełnienie nowych obowiązków wymaga przede wszystkim strategicznego podejścia do ryzyka w obszarze cyberbezpieczeństwa.

Jak zatem zbudować skuteczne procesy związane z analizą ryzyka ICT, aby z jednej strony spełnić wymogi prawa, ale przede wszystkim zwiększyć odporność organizacji na cyberzagrożenia?

Czym jest analiza ryzyka ICT

Analiza ryzyka ICT to proces identyfikacji, oceny i zarządzania ryzykiem związanym z zasobami teleinformatycznymi. W ujęciu cyberbezpieczeństwa – analiza ryzyka ICT oznacza ocenę zagrożeń, podatności oraz skutków potencjalnych incydentów związanych z utratą poufności, integralności, dostępności lub autentyczności danych i systemów.

Ryzyko jest zatem miarą potencjalnej szkody, która może zostać wyrządzona organizacji lub jej klientom, kontrahentom, będąca kombinacją prawdopodobieństwa oraz skutków materializacji tego ryzyka.

Celem przeprowadzenia analizy ryzyka jest umożliwienie podjęcia świadomych decyzji dotyczących zarządzania cyberbezpieczeństwem oraz zapewnienia odpowiednich, adekwatnych środków organizacyjnych i technicznych, mających na celu zabezpieczenie organizacji przed oddziaływaniem zagrożeń.

Do czego służy analiza ryzyka ICT

Analiza ryzyka stanowi fundament skutecznego zarządzania cyberbezpieczeństwem. To dzięki analizie ryzyka, najwyższe kierownictwo organizacji jest w stanie podjąć odpowiednie decyzje związane z:

- priorytetyzacją działań zapobiegawczych, dzięki koncentracji zasobów dookoła najważniejszych zagrożeń powodujących najpoważniejsze potencjalne skutki dla organizacji;
- świadomym zarządzaniem budżetem, poprzez odpowiednie planowanie inwestycji związanych z bezpieczeństwem;
- zapewnieniem zgodności z wymogami przepisów prawa, poprzez implementację odpowiednich procesów oraz wdrożeniem odpowiednich rozwiązań, które pozwolą na wykazanie zgodności z wymaganiami nakładanymi przepisami prawa;
- zarządzaniem incydentami poprzez identyfikację i ocenę krytycznych zasobów oraz opracowanie scenariuszy awaryjnych, związanych z reagowaniem i przywracaniem sprawności.

Analiza ryzyka ICT w dyrektywy NIS 2

Dyrektywa NIS 2 wprowadza wymogi dla podmiotów kluczowych i podmiotów ważnych w zakresie zarządzania cyberbezpieczeństwem, w tym również obowiązek prowadzenia systematycznej analizy ryzyka.

NIS 2 zobowiązuje podmioty kluczowe i ważne do wprowadzenia odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług. Jednym z elementów, które należy przyjąć, w celu spełnienia wyżej wskazanego obowiązku, jest opracowana i wdrożona polityka analizy ryzyka i bezpieczeństwa systemów informatycznych, a także regularne wykonywanie oceny ryzyka z uwzględnieniem ryzyk operacyjnych i ryzyk dotyczących łańcucha dostaw. Oznacza to, iż analiza ryzyka ICT musi obejmować nie tylko wewnętrzne systemy, ale także zależności od dostawców i partnerów technologicznych.

W praktyce podmioty powinny przyjąć wewnętrzną dokumentację dotyczącą analizy ryzyka i bezpieczeństwa systemów informatycznych, uwzględniającą takie elementy, jak:

- opis metody oceny ryzyka,
- określenie zakresu analizy ryzyka – tj. objęcie odpowiednich aktywów, identyfikację zagrożeń, podatności,
- harmonogram przeprowadzania odpowiednich ocen, identyfikacji, a także przeglądu ryzyk,
- opis metody opracowania planu postępowania z ryzykiem, w tym akceptacji ryzyka, minimalizacji, przenoszenia czy też eliminacji ryzyka,
- określenie zakresu obowiązków i odpowiedzialności w ramach realizacji procesów związanych z zarządzaniem ryzykiem ICT.

Jak przeprowadzić analizę ryzyka ICT?

Przeprowadzenie skutecznej analizy ryzyka to wieloetapowy proces, składający się zwykle z następujących kroków:

1. Identyfikacja i klasyfikacja aktywów.

W tym kroku organizacja identyfikuje i określa co zamierza chronić, jakie aktywa mają dla niej wartość oraz dokonuje oceny wartości tych aktywów. Na tym etapie tworzy się rejestry sprzętu, oprogramowania, danych, procesów, a nawet zasobów osobowych. Dane oraz zasoby, na których przetwarzane są dane podlegają dalszej klasyfikacji, zgodnie z zasadami danej organizacji co do klasyfikacji informacji.

2. Identyfikacja zagrożeń i podatności.

Na tym etapie tworzy się scenariusze ryzyka, identyfikuje się potencjalne zagrożenia, które mogą oddziaływać na organizację oraz jej aktywa, a także analizuje się potencjalne podatności, przez które może dojść do materializacji się zidentyfikowanych ryzyk. Jest to często etap długi, wymagający dużej wiedzy oraz doświadczenia. Podczas identyfikacji podatności znacząco pomaga zastosowanie zautomatyzowanych narzędzi do skanowania i monitorowania ewentualnych słabości systemów informatycznych organizacji. Do celów identyfikacji zagrożeń oraz podatności wykorzystuje się w praktyce również często testy penetracyjne oraz analizy podatności przeprowadzane przez doświadczone zespoły pentesterskie. Podmioty, które nie chcą inwestować w utrzymanie własnych zespołów (tzw. RedTeam), często decydują się na outsourcing w tym obszarze.

> „Wyniki analizy ryzyka powinny być również uwzględniane podczas podejmowania decyzji dotyczących szkoleń i przeprowadzania działań uświadamiających, a także w procesach związanych z zarządzaniem incydentami

3. Ocena ryzyka.

Przeprowadzenie oceny ryzyka to etap związany z przypisaniem wartości poszczególnym zidentyfikowanym ryzykom. Na tym etapie poznajemy skwantyfikowany poziom ryzyka w podziale na poszczególne, zidentyfikowane wcześniej aktywa oraz scenariusze ryzyk. W zależności od przyjętej metody oceny ryzyka, najczęściej na tym etapie poznaje się dwie wartości dla każdego scenariusza – tj. ryzyko pierwotne (czyli ryzyko występujące niezależnie od przyjętych w organizacji mitygantów) oraz ryzyko rezydualne (czyli ryzyko, które pozostaje po uwzględnieniu zastosowanych mitygantów).

4. Określenie poziomu ryzyka akceptowalnego.

Przyjmuje się, że ryzyko rezydualne (szczątkowe) występuje zawsze, nawet po zastosowaniu wszelkich znanych środków mitygujących to ryzyko – chyba, że dokonano tzw. wyeliminowania ryzyka, poprzez wprowadzenie takich modyfikacji, że dany scenariusz ryzyka w ogóle przestaje istnieć (np. zidentyfikowaliśmy ryzyko utraty poufności informacji drukowanych na drukarkach firmowych ustawionych w korytarzu – możemy całkowicie wyeliminować to ryzyko, jeżeli zrezygnujemy z tworzenia wydruków na rzecz przetwarzania informacji jedynie w formie cyfrowej, bez fizycznych wydruków). Na etapie określenia poziomu ryzyka akceptowalnego, określa się, które z ryzyk są możliwe do zaakceptowania przez organizację, a które powinny podlegać dalszemu postępowaniu z ryzykiem.

5. Planowanie działań zaradczych – plan postępowania z ryzykiem.

Na tym etapie tworzy się plan postępowania z ryzykiem. Kiedy określono już, które z ryzyk podlegają dalszej mitygacji (czyli nie są akceptowalne), przeprowadza się plan, w którym określa się, jakie działania należy podjąć, aby poziom danego ryzyka zminimalizować, bądź też przenieść to ryzyko na inny podmiot, lub całkowicie je wyeliminować.

6. Dokumentowanie wyników oraz komunikacja.

Raport podsumowujący przeprowadzoną analizę ryzyka powinien zostać przekazany najwyższemu kierownictwu, w celu oczywiście akceptacji, ale również w celu zaangażowania najwyższego kierownictwa w podejmowanie kluczowych decyzji w oparciu o wyniki analizy ryzyka. Raport często bywa również komunikowany niższym szczeblom managementu, aby podnieść poziom świadomości osób zaangażowanych w realizację poszczególnych procesów w organizacji.

7. Monitorowanie i przeglądy.

Ryzyka występujące w organizacji powinny podlegać ciągłemu monitorowaniu, a także powinny być okresowo przeglądane i aktualizowane.

Podstawa decyzji związanych z cyberbezpieczeństwem

Wyniki analizy ryzyka ICT stanowią jeden z podstawowych elementów, który musi być brany pod uwagę podczas podejmowania wszelkich decyzji związanych z cyberbezpieczeństwem.

Pamiętać należy, że analiza ryzyka to proces ciągły. Efekty przeprowadzonych analiz powinny być aktywnie wykorzystywane w tworzeniu lub modyfikacji istniejących polityk i procedur, wdrażaniu rozwiązań technicznych i organizacyjnych, takich jak nowe narzędzia (np. systemy klasy SIEM, EDR, XDR), wdrożeniu odmiennych konfiguracji, segmentacji sieci. Wyniki analizy ryzyka powinny być również uwzględniane podczas podejmowania decyzji dotyczących szkoleń i przeprowadzania działań uświadamiających, a także w procesach związanych z zarządzaniem incydentami, chociażby podczas tworzenia planów reagowania i przywracania sprawności, określania punktów eskalacji, tworzenia planów komunikacji itp.

Ważne, aby analiza ryzyka była przeprowadzona w oparciu o spisaną politykę, opracowaną z uwzględnieniem uznanych standardach, co umożliwia porównywalność wyników, a przez to obserwowanie zmian w obszarze cyberzagrożeń na które narażona jest organizacja. Wykorzystanie wniosków z analizy ryzyka przeprowadzonej na podstawie takiej metodyki wzmacnia kulturę bezpieczeństwa w organizacji i pozwala na elastyczne reagowanie na wciąż zmieniający się krajobraz cyberzagrożeń. /®