CYBERBEZPIECZEŃSTWO

Zgłaszanie incydentów według NIS 2 – systemowa odpowiedzialność i procedury

Cyberataki, awarie systemów, wycieki danych to nie odległa przyszłość, ale codzienność wielu organizacji. Nowe unijne regulacje wymagają, by podmioty kluczowe i ważne nie tylko wiedziały, jak radzić sobie z incydentem, ale miały gotowy plan działania, zespoły reagowania i ścieżkę raportowania.

ADW. TOMASZ KAMIŃSKI

wspólnik w Kancelarii Krzysztof Rożko i Wspólnicy

DANIEL NIWIŃSKI

prawnik, ekspert ds. cyberbezpieczeństwa w Kancelarii Krzysztof Rożko i Wspólnicy

Dane o poważnych incydentach związanych z bezpieczeństwem informacji trafiają coraz częściej na pierwsze strony gazet. Wycieki danych osobowych, utrudnienia w dostępie do kont bankowych, przerwy w działaniu usług cyfrowych, to tylko nieliczne przykłady incydentów, o których informacje trafiają do szerokiego grona odbiorców. W czasach wszechobecnej cyfryzacji i rosnących zagrożeń w cyberprzestrzeni pojęcie incydentu zyskało na znaczeniu nie tylko w kontekście samego bezpieczeństwa ICT (technologie informacyjno-komunikacyjne), lecz również w wymiarze prawnym i praktycznym, a zarządzanie ryzykiem wystąpienia incydentu stanowi coraz większe wyzwanie dla wzrastającej liczby podmiotów, które wykorzystują technologie informatyczne do świadczenia usług lub dostarczania produktów.

Dyrektywa (UE) 2022/2555 (NIS 2) przyjęta w celu ustanowienia środków mających na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii, która nakłada wymogi w zakresie zarządzania odpornością cyfrową na tzw. podmioty kluczowe lub ważne, definiuje incydent jako zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych albo usług oferowanych przez sieci i systemy informatyczne bądź dostępnych za ich pośrednictwem. Incydenty mogą mieć różną skalę, od lokalnych awarii technicznych, przerw lub błędów w funkcjonowaniu procesów biznesowych, poprzez zorganizowane cyberataki o zasięgu międzynarodowym.

Zarządzanie incydentami stanowi kluczowy element tzw. systemu zarządzania bezpieczeństwem informacji, do którego wdrożenia na mocy dyrektywy NIS 2 zobowiązane zostały podmioty kluczowe lub ważne. Celem zarządzania incydentami jest zapewnienie szybkiej reakcji na występujące zdarzenie niebezpieczne, minimalizacja skutków tego zdarzenia oraz zapobieganie dalszej jego eskalacji. Brak wdrożenia skutecznych środków reagowania i obsługi incydentów może prowadzić do poważnych konsekwencji, takich jak przerwy w świadczeniu usług, straty finansowe, utrata informacji, utrata zaufania klientów, a także naruszenie przepisów i odpowiedzialność prawna.

W praktyce skuteczne zarządzanie incydentami związanymi z cyberbezpieczeństwem pozwala nie tylko efektywnie reagować na zdarzenia niebezpieczne i ograniczać ich skutki, lecz również dostarczać wiedzę i doświadczenie dla personelu podmiotu, dzięki czemu organizacja jest w stanie ciągle doskonalić i podnosić swoją odporność na nowe zagrożenia.

Obowiązki

Dyrektywa NIS 2 rozszerza zakres obowiązków podmiotów kluczowych i ważnych w zakresie cyberbezpieczeństwa. Pośród wielu wymogów dotyczących cyberodporności kluczowe znaczenie ma właśnie zarządzanie incydentami.

Zgodnie z art. 21 ust. 2 lit. b) NIS 2 podmioty kluczowe i ważne zobowiązane będą wprowadzać odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem, obejmujące m.in. obsługę incydentów.

Dodatkowo art. 23 NIS 2 wprowadza obowiązki w zakresie zgłaszania incydentów – podmioty objęte dyrektywą zobowiązane są do wdrożenia procedur umożliwiających skuteczne wykrywanie, zgłaszanie i reagowanie na incydenty. Obowiązek ten obejmuje:

- identyfikację incydentów mających istotny wpływ na świadczenie usług;
- niewzwłoczne zgłoszenie incydentu do właściwego CSIRT-u lub właściwego organu nadzorczego – najpóźniej w ciągu 24 godzin od momentu uzyskania wiedzy o incydencie;
- uzupełnienie informacji o incydencie w ramach zgłoszeń uzupełniających, w ciągu kolejnych 72 godzin;
- przekazanie raportu końcowego zawierającego ocenę skutków incydentu oraz zastosowane środki zaradcze.

Zarządzanie incydentami

Skuteczne zarządzanie incydentami wymaga solidnego przygotowania i postawienia organizacji w stan gotowości, tak aby nie tylko być w stanie wykrywać i rozpoznawać incydenty, prawidłowo je klasyfikować, ale również właściwie reagować na wystąpienie incydentu, dokumentować przebieg zdarzenia i podjęte środki zaradcze, a także wypełniać obowiązki raportowe i informacyjne.

Procesy związane z obsługą incydentów można podzielić na dwa główne elementy, tj. zarządzenie incydentem (incident management) oraz mitygacja skutków incydentu (incident response).

Zarządzanie incydentem to procesy wykrywania, analizowania, klasyfikacji i obsługi incydentów, które obejmuje w szczególności takie elementy, jak:

- ustanowienie punktów kontaktowych i zespołu reagowania na incydenty;
- ustanowienie prawidłowych kanałów komunikacji i strategii komunikacji zarówno wewnętrznej, jak i zewnętrznej, na wypadek wystąpienia różnego rodzaju zdarzeń, w tym takich, które mogą utrudnić komunikację;
- przygotowanie personelu do prawidłowego rozpoznawania i zgłaszania incydentów;
- zastosowanie narzędzi do monitorowania systemów informatycznych i wykrywania anomalii;
- klasyfikację incydentów zgodnie z kryteriami wpływu i pilności;
- eskalację i dokumentację procedur reakcji;
- obsługę prawną incydentu – obowiązki informacyjne, zgłoszenie incydentu, roszczenia, wypełnienie obowiązków prawnych.

Mitygacja skutków incydentu to procesy mające na celu ograniczenie szkód wynikających z zaistnienia incydentu, które obejmują w szczególności takie elementy, jak:

> „Zarządzanie incydentami to dziś obowiązek prawny, nie tylko dobra praktyka

- niezwłoczne odizolowanie zaatakowanych elementów środowiska;
- przywracanie sprawności zgodnie z planem ciągłości działania;
- współpraca z organami zewnętrznymi, takimi jak np. CSIRT NASK;
- analiza powłamaniowa i wdrożenie środków zaradczych.

Przygotowanie organizacji do obsługi incydentów powinno uwzględniać cykliczne testy, symulacje oraz szkolenia pracowników. Podstawą jest opracowanie zrozumiałych procedur wewnętrznych, a także planów reagowania i przywracania sprawności, które mogą zostać wdrożone niezwłocznie po otrzymaniu pierwszego sygnału o zaistnieniu potencjalnie niebezpiecznego zdarzenia.

Powiadomienie organów

Na gruncie NIS 2 rozszerzony został obowiązek informowania odpowiednich organów o wystąpieniu incydentu w podmiocie kluczowym lub ważnym. Podmioty zobowiązane zostały do przedkładania odpowiedniemu CSIRT lub właściwemu organowi, bez zbędnej zwłoki, w ciągu 24 godzin, wczesnego ostrzeżenia o wystąpieniu incydentu, następnie w ciągu 72 godzin zgłoszenia uzupełniającego. Dodatkowo na wniosek odpowiedniego organu podmioty mogą być zobowiązane do przekazania sprawozdania okresowego na temat odpowiednich aktualizacji statusu związanego z obsługą incydentu. W ciągu miesiąca podmiot zobowiązany będzie do przedstawienia sprawozdania końcowego, zawierającego m.in takie elementy, jak:

- szczegółowy opis incydentu, w tym jego dotkliwości i skutków;
- rodzaj zagrożenia lub pierwotną przyczynę, która prawdopodobnie była źródłem incydentu;
- zastosowane i wdrażane środki ograniczające ryzyko.

Warto zaznaczyć, że NIS 2 nie jest jedyną regulacją, zgodnie z którą należy spełnić obowiązki informacyjne po wystąpieniu incydentu. Jeżeli incydent dotyczył naruszenia ochrony danych osobowych, podmiot będzie zobowiązany również do przekazania powiadomienia w ciągu 72 godzin do prezesa Urzędu Ochrony Danych Osobowych na gruncie rozporządzenia RODO. Ze względu na liczne obowiązki dotyczące informowania o wystąpieniu incydentów istotnym jest stworzenie spójnych procedur wewnętrznych dotyczących komunikacji i przekazywania informacji do organów nadzoru, które uwzględniać będą takie elementy, jak:

- analiza, czy incydent podlega zgłoszeniu w ramach NIS 2, RODO lub ew. innych regulacji;
- ustalenie jasnej ścieżki eskalacji i powiadomień;
- ustalenie ról i odpowiedzialności dotyczących przekazywania informacji do organów nadzoru;
- ustalenie zasad nadawania priorytetu incydentom wielowątkowym;
- zapewnienie zgodności treści raportów ze standardami instytucji nadzorczych.

Kluczowym dla zapewnienia skuteczności procesów związanych z przekazywaniem informacji do organów nadzoru jest zapewnienie współpracy pomiędzy zespołami odpowiedzialnymi za bezpieczeństwo IT, ochronę danych osobowych oraz compliance.

Bezpieczne funkcjonowanie

Zarządzanie incydentami już dawno przestało być jedynie elementem związanym z dobrymi praktykami, a stało się wymogiem prawnym i jednym z głównych filarów cyberbezpieczeństwa wielu instytucji, szczególnie kwalifikowanych jako podmioty kluczowe lub ważne. Wdrożenie wymagań dyrektywy NIS 2 w praktyce związane jest nie tylko z implementacją odpowiednich narzędzi, lecz przede wszystkim opracowania odpowiednich procesów i procedur, a także planów reagowania.

Niezbędnym jest również wyciąganie wniosków z występujących incydentów i ciągłe doskonalenie systemu zarządzania bezpieczeństwem informacji.

Współczesne środowisko cyfrowe charakteryzuje się dużą dynamiką zmian i ewolucją krajobrazu zagrożeń. Organizacje, które chcą nie tylko spełniać obowiązki regulacyjne, lecz również budować zaufanie wśród swoich klientów i kontrahentów, powinny traktować zarządzanie incydentami jako integralny element strategii bezpieczeństwa. /℗