NASK

http://www.nask.pl/pl/dzialalnosc/csirt-nask/1551,CSIRT-NASK.html
2019-05-27, 11:55

CSIRT NASK

Ustawa o krajowym systemie cyberbezpieczeństwa z 5 lipca 2018 r. definiuje rolę CSIRT NASK – jednego z trzech CSIRT na poziomie krajowym. Zadania CSIRT NASK realizuje wiele komórek znajdujących się w strukturze NASK PIB . Jedną z nich jest CERT Polska, który prowadzi działania operacyjne, takie jak: monitorowanie zagrożeń cyberbezpieczeństwa, reagowanie na zgłoszone incydenty i koordynacja ich obsługi oraz przeciwdziałanie zagrożeniom cyberbezpieczeństwa, które dotykają wiele sektorów i państw. Dyżurnet.pl to zespół, który reaguje na zgłoszenia dotyczące nielegalnych i szkodliwych treści, w tym materiałów przedstawiających seksualne wykorzystywanie dzieci. Ustawa nakłada na CSIRT NASK również inne zdania m.in. z zakresu edukacji, budowania świadomości oraz tzw. poziomu *policy*.

- Ustawa o krajowym systemie cyberbezpieczeństwa

Jedną z odpowiedzi na cyberzagrożenia we współczesnym świecie są międzynarodowe i krajowe regulacje dotyczące ochrony cyberprzestrzeni. Najważniejszymi aktami prawnymi w tym zakresie są Dyrektywa NIS i jej implementacja do porządku krajowego czyli ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, obowiązująca od 28 sierpnia 2018 r. Jest to pierwszy akt prawny, który w kompleksowy sposób adresuje temat cyberbezpieczeństwa w Polsce. Organizuje krajowy system cyberbezpieczeństwa oraz określa zadania i obowiązki podmiotów wchodzących w skład tego systemu. Ma umożliwić zapobieganie, wykrywanie oraz zwalczanie incydentów cyberbezpieczeństwa, które mogą wpływać na funkcjonowanie państwa.

- Trzy CSIRT poziomu krajowego

Jedną z najważniejszych zmian, które wprowadziła ustawa, jest powołanie trzech zespołów CSIRT na poziomie krajowym. Są to zespoły, które monitorują polską cyberprzestrzeń, reagują na incydenty, koordynują ich obsługę czy szacują ryzyko. Każdy z nich ma swój zakres odpowiedzialności. Są to:
• CSIRT GOV w Agencji Bezpieczeństwa Wewnętrznego - incydenty zgłaszane przez administrację rządową, Narodowy Bank Polski, Bank Gospodarstwa Krajowego oraz operatorów infrastruktury krytycznej;

• CSIRT MON w Ministerstwie Obrony Narodowej (MON) - incydenty zgłaszane przez podmioty podległe Ministrowi Obrony Narodowej i przedsiębiorstwa o szczególnym znaczeniu gospodarczo-obronnym;
• CSIRT NASK w Państwowym Instytucie Badawczym NASK.

• CSIRT NASK

CSIRT NASK koordynuje incydenty zgłaszane przez operatorów usług kluczowych, dostawców usług cyfrowych, samorząd terytorialny oraz wszystkie te podmioty, których nie obsługują CSIRT GOV i MON. Incydenty mogą także zgłaszać zwykli obywatele, jako że CSIRT NASK pełni rolę tzw. CERT *of last resort*, czyli CERT ostatniej szansy.

CSIRT NASK zgodnie z ustawą m.in.:

• monitoruje zagrożenia cyberbezpieczeństwa i incydenty na poziomie krajowym oraz szacuje ryzyko związane z ujawnionymi zagrożeniami;
• współpracuje z podmiotami krajowego systemu cyberbezpieczeństwa, w tym z pozostałymi CSIRT poziomu krajowego, sektorowymi zespołami cyberbezpieczeństwa oraz organami właściwymi ds. cyberbezpieczeństwa;
• bada i ocenia sprzęt lub oprogramowanie stosowane przez podmioty krajowego systemu cyberbezpieczeństwa, a także wnioskuje o wydanie rekomendacji w tym zakresie;
• zapewnia zaplecze analityczne oraz badawczo-rozwojowe, które analizuje złośliwe oprogramowanie oraz podatności, buduje świadomość cyberbezpieczeństwa, opracowuje rekomendacje i dobre praktyki, prowadzi działania edukacyjne, a także rozwija narzędzia i metody zwalczania cyberzagrożeń;
• przyjmuje zgłoszenia oraz analizuje przypadki rozpowszechniania materiałów przedstawiających seksualne wykorzystywanie dzieci.

Zobacz wszystkie zadania CSIRT NASK, które nakłada ustawa o krajowym systemie cyberbezpieczeństwa.

Zadania CSIRT NASK realizują w ramach NASK PIB odpowiednie komórki i zespoły.

Na poziomie operacyjnym są to:
• CERT Polska – przyjmuje zgłoszenia, rozpoznaje je i ocenia, a także koordynuje obsługę incydentów cyberbezpieczeństwa.

• Dyżurnet.pl – reaguje na zgłoszenia i incydenty dotyczące rozpowszechniania nielegalnych i szkodliwych treści, w tym materiałów przedstawiających seksualne wykorzystywanie dzieci.

Na poziomie *policy* CSIRT NASK prowadzi analizy i opracowuje standardy, rekomendacje oraz dobre praktyki w zakresie cyberbezpieczeństwa, a także wspiera podmioty krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności w obszarze cyberbezpieczeństwa.
Więcej informacji o charakterze strategicznym, regulacyjnym oraz organizacyjnym z zakresu cyberbezpieczeństwa dostępnych jest na stronie CyberPolicy.

Wsparcie dla różnego rodzaju podmiotów, w tym także dla podmiotów krajowego systemu cyberbezpieczeństwa, zapewniane jest także w ramach programu Partnerstwo dla Cyberbezpieczeństwa. Celem programu jest budowanie zaufania, które stanowi podstawę aktywnej współpracy, wymiany informacji i doświadczeń oraz budowania szerokiej sieci kontaktów. Współpraca odbywa się w formule partnerstwa publiczno-prywatnego. Umożliwia wszystkim partnerom zwiększenie poziomu cyberbezpieczeństwa na poziomie:

• technicznym - wymiana informacji i doświadczeń,
• strategicznym - wypracowywanie rekomendacji, udział w pracach grup i zespołów zadaniowych,
• kompetencyjnym - spotkania, szkolenia i ćwiczenia procedur reagowania.

Do współpracy zapraszane są podmioty, które świadczą usługi korzystając z systemów teleinformatycznych, a zakłócenie tych usług ma znaczne skutki gospodarcze lub społeczne. Więcej informacji o programie można uzyskać w Zespole Programu Partnerstwo dla Cyberbezpieczeństwa pod adresem pdc@nask.pl.
CSIRT NASK odpowiada także za budowanie świadomości oraz edukację w obszarze cyberbezpieczeństwa. Więcej informacji na ten temat na stronie Akademii NASK.

- Raportowanie incydentów

Najprostszą i najwygodniejszą formą zgłoszenia incydentu jest przesłanie zgłoszenia elektronicznego do CERT Polska, który odpowiada za operacyjną działalność CSRIT NASK. Najlepiej wykorzystać formularz online na stronie https://incydent.cert.pl, który krok po kroku podpowie jakie informacje zawrzeć w zgłoszeniu. Ostatecznie można wysłać zgłoszenie pocztą elektroniczną na adres cert@cert.pl. Formularz do wydruku dostępny jest na BIP NASK.

Zgłoszenie należy wysłać jak najszybciej, przy czym nie później niż w ciągu 24 godzin od momentu wykrycia incydentu. Czas reakcji na zgłoszenie jest bardzo ważny i może wpłynąć na rozwiązanie problemu. Zobacz szczegółową instrukcję dotycząca zgłaszania incydentów.

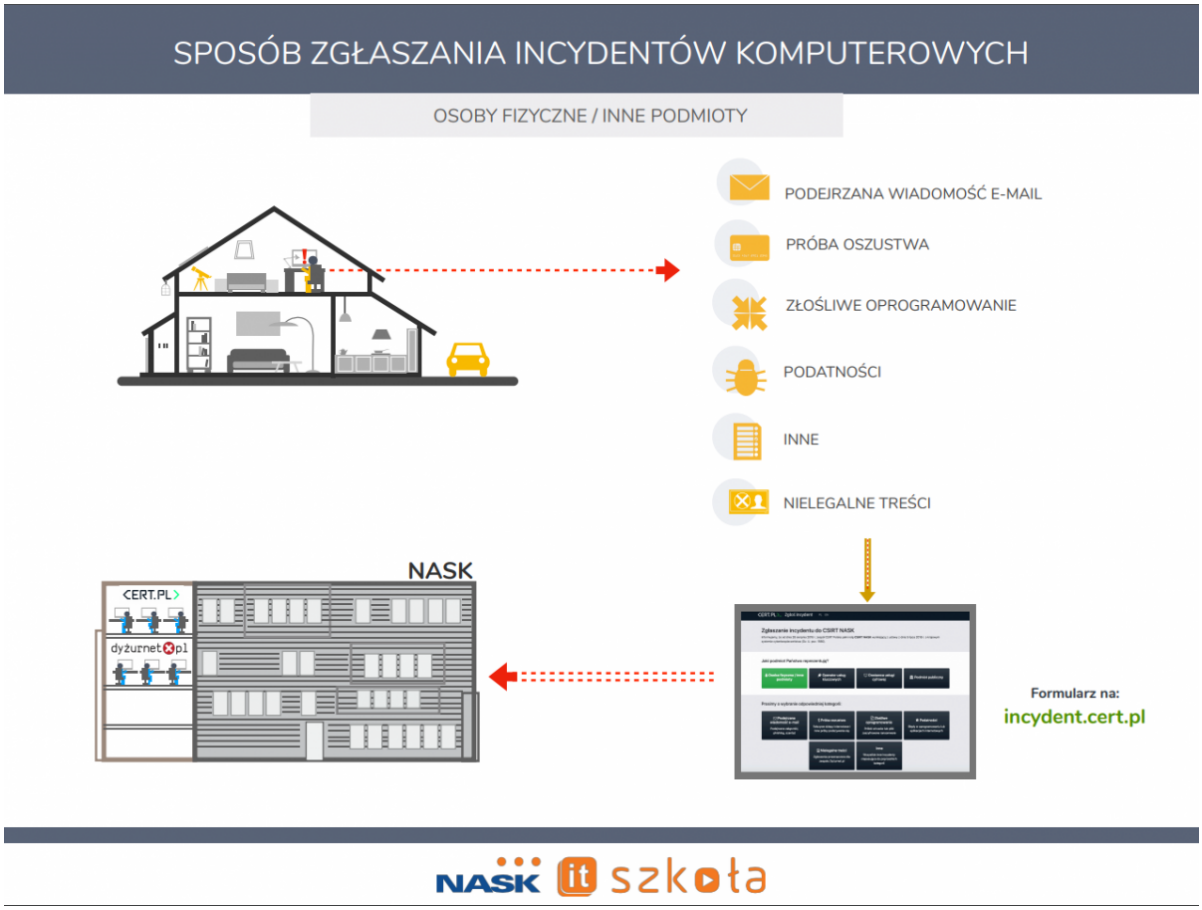
- Zgłoś incydent co CERT Polska
- Zgłoś incydent do Dyżurnet.pl

Kto musi raportować incydenty

Podmiotami krajowego systemu cyberbezpieczeństwa są:

1. Operatorzy usług kluczowych - to firmy lub instytucje świadczące usługi o istotnym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej.
2. Dostawcy usług cyfrowych - podmioty takie jak internetowe platformy handlowe, usługi przetwarzania w chmurze czy wyszukiwarki internetowe.
3. Podmioty publiczne takie jak jednostki sektora finansów publicznych, instytuty badawcze, Narodowy Bank Polski; Bank Gospodarstwa Krajowego; Urząd Dozoru Technicznego; Polską Agencję Żeglugi Powietrznej; Polskie Centrum Akredytacji; Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej; spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej.

O tym, czy dany podmiot lub firma jest operatorem usługi kluczowej decyduje minister, który nadzoruje dany sektor gospodarki. Wymienieni w ustawie ministrowie oraz Komisja Nadzoru Finansowego to tzw. organy właściwe do spraw cyberbezpieczeństwa.



Jakie incydenty należy zgłaszać

Do CERT Polska można zgłosić każdy incydent cyberbezpieczeństwa lub potencjalnie niebezpieczne zjawisko w internecie, takie jak fałszywy sklep online, próba wyłudzenia danych lub pieniędzy, phishing czy złośliwe oprogramowanie. Wszystkie zgłoszenia są analizowane oraz odpowiednio klasyfikowane. Jeżeli znane jest rozwiązanie danego problemu, zgłaszający szybko otrzyma odpowiedź. Na podstawie zgłoszeń powstaje całościowy obraz bezpieczeństwa w sieci. Mając taką wiedzę, dużo łatwiej jest podejmować skoordynowane działania ostrzegawcze, zapobiegawcze lub naprawcze.

Ustawa nakłada obowiązek zgłaszania następujących incydentów:

• Incydent w podmiocie publicznym to incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego;
• Incydent istotny dotyczy tylko dostawców usług cyfrowych. Jest to incydent, który ma istotny wpływ na świadczenie usługi cyfrowej;
• Incydent poważny dotyczy tylko operatorów usług kluczowych. To, czy incydent jest uznawany za poważny, zależy np. od liczby użytkowników dotkniętych incydentem oraz czasu oddziaływania incydentu na świadczoną usługę. Kryteria dla poszczególnych sektorów dostępne są w analizie Rozporządzenia Rady Ministrów w sprawie progów uznania incydentu za poważny.

Wyznaczenie osoby do kontaktu
Każdy podmiot publiczny, który realizuje zadania publiczne zależne od systemu informacyjnego, a także operator usługi kluczowej musi wyznaczyć osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Informację należy wysłać do CSIRT NASK w ciągu 14 dni od daty wyznaczenia takiej osoby. O ewentualnych zmianach również należy poinformować w ciągu 14 dni.
Wiadomość powinna zawierać nazwę podmiotu lub organizacji, sektor, imię, nazwisko, telefon kontaktowy oraz email służbowy osoby kontaktowej. Zgłoszenie należy wysłać:
• E-mail na adres ksc@cert.pl
• Pismo na adres NASK/CERT Polska, ul. Kolska 12, 01-045 Warszawa