CyberPOLICY
NASK

SKOORDYNOWANE UJAWNIANIE PODATNOŚCI

(COORDINATED VULNERABILITY DISCLOSURE, CVD)

PORADNIK

Publikacja przygotowana we współpracy
z Narodowym Centrum Cyberbezpieczeństwa w Holandii
National Cyber Security Centre (NCSC)

CyberPOLICY NASK

Spis treści

Wstęp

Szanowni Państwo,

Z przyjemnością przedstawiam Państwu Poradnik na temat procesu skoordynowanego ujawniania informacji o podatnościach (ang. Coordinated Vulnerability Disclosure – CVD). Temat ten w świadomości osób zajmujących się bezpieczeństwem teleinformatycznym istnieje właściwie „od zawsze". Podejście do zagadnienia i roli tzw. pozytywnych, etycznie działających hakerów, których działalność wpływa na zwiększenie poziomu bezpieczeństwa systemów, urządzeń i procesów ICT, podlegało ewolucji. Kwestia i wyzwania związane z CVD zostały zauważone i ostatecznie uwzględnione przez Komisję Europejską w projekcie Dyrektywy NIS 2. Niektóre państwa członkowskie już wprowadziły w życie koncepcję CVD, a inne, w tym także Polska, dopiero rozpoczynają prace z tym związane. Poniższy poradnik ma na celu przedstawienie korzyści z wdrożenia całego procesu, a także stworzenie przejrzystych zasad współpracy i komunikacji pomiędzy zgłaszającymi podatności, a organizacjami będącymi adresatem. Publikacja wybiega w przyszłość i uwzględnia zobowiązania wynikające z NIS 2.

Przygotowując Poradnik korzystaliśmy z doświadczenia i dobrych praktyk naszych kolegów z Narodowego Centrum Cyberbezpieczeństwa (NCSC) w Niderlandach, którzy w tej dziedzinie byli pionierami. Dlatego też zdecydowaliśmy się opisać skoordynowane ujawnianie podatności zgodnie z podejściem niderlandzkim, w którym to zachęcamy Organizacje do stworzenia polityki CVD. Pokazujemy również jak zastosować CVD zgodnie z polskim prawem, gdy brak opublikowanej polityki.

Poradnik jest skierowany do wszystkich stron procesu CVD - zarówno producentów sprzętu i oprogramowania, właścicieli firm, administratorów systemów, osób raportujących informacje o podatnościach i błędach konfiguracyjnych, CSIRTów poziomu krajowego zaangażowanych w badanie podatności i propagowanie informacji o zagrożeniach, a także społeczności IT i akademickiej itp. - wszystkich, którzy są zainteresowani CVD.

Dziękuję wszystkim, którzy z oddaniem, poświęceniem i pasją przygotowali poniższy Poradnik, a Państwu życzę miłej lektury i inspiracji do wdrożenia CVD w Państwa organizacjach.

Z poważaniem,

Krzysztof Silicki

Zastępca Dyrektora NASK, Dyrektor ds. Cyberbezpieczeństwa i Innowacji

Czym jest skoordynowane ujawnianie podatności?

Coordinated Vulnerability Disclosure, w skrócie CVD to określenie na skoordynowane ujawnianie informacji o podatnościach.

Pomimo tego, że firmy, organizacje i instytucje zajmujące się bezpieczeństwem od bardzo dawna mierzą się z kwestią efektywnego informowania o wykrytych podatnościach w systemach informatycznych i lukach w zabezpieczeniach to, jak się okazuje, opracowanie standardów i procedur w tym zakresie jest nie lada wyzwaniem. Dość powszechnie stosowane są programy typu bug bounty, które oferują finansową gratyfikację za zgłaszanie wykrytych w oprogramowaniu błędów, a zwłaszcza podatności, dotyczących bezpieczeństwa. Programy te pozwalają Organizacjom i twórcom oprogramowania na zdiagnozowanie i usunięcie błędów, zanim dowie się o nich opinia publiczna, co zapobiega przypadkom nadużyć.

Polityka czy zasady ujawniania informacji o podatnościach lub lukach w zabezpieczeniach mają na celu przejrzyste określenie ram procesu CVD dla wszystkich stron, biorących w nim udział. Należą do nich:

1. Organizacje – mowa tu przede wszystkim o właścicielach systemów teleinformatycznych, w których podatność występuje (czy to przez błąd w konfiguracji, czy w oprogramowaniu), ale także o producentach tych systemów. Na potrzeby niniejszego poradnika podmioty te zostały zbiorczo nazwane “Organizacjami”.

2. Zgłaszający - osoby lub grupy osób, które wyszukują podatności, często określani jako etyczni hakerzy lub badacze bezpieczeństwa.

3. Zaufany Pośrednik – zgodnie z projektem NIS 2, wyznaczony do pełnienia w procesie CVD roli tzw. “zaufanego pośrednika” CSIRT poziomu krajowego.

Skoordynowane ujawnianie podatności to ustrukturyzowany proces, w ramach którego podatności są zgłaszane organizacjom w sposób umożliwiający organizacji zdiagnozowanie i wyeliminowanie danej podatności, zanim szczegółowe informacje dotyczące podatności zostaną ujawnione osobom trzecim lub podane do wiadomości publicznej.

Źródło: The NIS2 Directive: A high common level of cybersecurity in the EU; https://www.europarl.europa.eu/thinktank/pl/document/EPRS_BRI(2021)689333

Zaufany Pośrednik

Zgłaszający ⟷ **Organizacja**

Biorąc pod uwagę, że niezamówione przez właściciela systemu testy bezpieczeństwa kojarzą się raczej z działalnością nielegalną, obie kluczowe strony CVD, czyli Zgłaszający jak i Organizacja, której dotyczy podatność, stały po przeciwnych stronach barykady. Musiało minąć sporo czasu, aby wypracować rozwiązanie satysfakcjonujące obie strony - oparte na przejrzystych warunkach i dobrej komunikacji.

Pionierami w tej dziedzinie w Europie było National Cyber Security Centre (NCSC), które już w 2013 r. opublikowało wytyczne dotyczące odpowiedzialnego ujawniania podatności. Ten dokument podkreślał przede wszystkim rolę organizacji, u której wykryto podatność. Następnie w 2018 r. za pośrednictwem Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA), NCSC opublikowało „Poradnik Skoordynowanego Ujawniania Informacji o Podatnościach". Zasadnicza różnica w nazwie wynikała z odmiennego podejścia do podmiotu raportującego, CVD podkreśla jego rolę. Aby osiągnąć zamierzony cel „pogodzenia" Zgłaszającego i Organizacji potrzebna jest skoordynowana współpraca obu stron.

Poradnik NCSC zawiera definicje, tłumaczy na czym polega proces CVD i pokazuje jak on przebiega. Autorzy wyszli z założenia, że najlepiej, aby organizacje posiadały politykę CVD, która jasno wyznacza zasady współpracy ze Zgłaszającymi. Poradnik zawiera wytyczne jak taką politykę napisać i co powinno się w niej znaleźć. W przypadku braku polityki, NCSC wspiera strony w procesie ujawniania podatności, pełniąc rolę pośrednika. Podkreśla jednak, że to zawsze Organizacja i Zgłaszający są stronami procesu.

Wyzwania związane z tematyką CVD zostały zauważone i nazwane w projekcie Dyrektywy NIS 2, która promuje wdrożenie regulacji CVD na poziomie wszystkich krajów członkowskich UE. W propozycji dyrektywy pojawia się trzecia strona procesu skoordynowanego ujawniania podatności, a mianowicie tzw. Zaufany Pośrednik.

Już na tym etapie legislacji, można stwierdzić, że propozycje rozwiązań i ramy prawne wpływają na zróżnicowanie podejścia do tematu CVD - w zależności od istniejących systemów, czy możliwości i preferencji wyboru np. procesu gratyfikacji.

Poziom zaawansowania prac nad wdrożeniem procesu CVD w krajach członkowskich różni się w dość dużym stopniu. Niektóre kraje mogą podzielić się już swoimi doświadczeniami, a inne, w tym także Polska, są na początku tej drogi.

Globalny zasięg problematyki CVD powoduje, że temat dotyczy także krajów pozaeuropejskich, które stworzyły własne polityki CVD. Wyzwaniem jest spójna integracja regulacji krajowych, europejskich i międzynarodowych w tym zakresie.

Cel i korzyści wynikające z CVD

Nadrzędnym celem CVD jest zwiększenie poziomu bezpieczeństwa sieci i systemów informatycznych. Jednak warto podkreślić, że poprawnie przeprowadzony proces ujawniania podatności przynosi korzyści wszystkim stronom.

Głównym beneficjentem jest Organizacja, ponieważ to ona ponosi bezpośrednią odpowiedzialność za bezpieczeństwo wykorzystywanych systemów teleinformatycznych. Wdrożenie polityki CVD powinno być postrzegane jako uzupełnienie istniejących środków w zakresie bezpieczeństwa informacji.

Osoba, która zgłasza podatność również korzysta na procesie CVD. Z jednej strony może wykorzystać swoją wiedzę i umiejętności, aby przyczynić się do zwiększenia poziomu cyberbezpieczeństwa, a jej wkład może zostać publicznie doceniony (czasem w grę wchodzi również nagroda pieniężna). Z drugiej – działanie w ramach procesu CVD chroni ją przed odpowiedzialnością karną.

Aby ujawnianie podatności mogło zakończyć się sukcesem, warunkiem jest współpraca obu stron, zarówno strony zgłaszającej jak i Organizacji. Polityka CVD ma na celu określenie warunków komunikacji z uwzględnieniem podstaw prawnych obowiązujących obie strony. Każda ze stron posiada również obowiązki i zobowiązania, których powinna przestrzegać.

Komunikacja, przejrzystość i odpowiedzialność przyczynią się do poprawy bezpieczeństwa systemów.

Korzyści płynące z wdrożenia CVD

Dla Organizacji	Dla zgłaszającego
Poprawa bezpieczeństwa wykorzystywanych systemów, a w efekcie ciągłości działania	Możliwość wykorzystania specjalistycznej wiedzy i umiejętności na rzecz zwiększenia poziomu cyberbezpieczeństwa
Przejrzysta komunikacja i potwierdzenie rzetelności i dojrzałości firmy (luki systemowe są i będą w każdym środowisku – nie ma sensu temu zaprzeczać) – korzyści wizerunkowe	Jasne zasady zgłaszania podatności i komunikacji z Organizacją
Pokazanie gotowości do przyjmowania informacji o podatnościach	Możliwość sprawdzenia swoich umiejętności na prawdziwych, często produkcyjnych systemach zgodnie z prawem
Unikanie komplikacji i niejednoznacznych sytuacji w związku z wykryciem podatności (np. żądania gratyfikacji i spełnienia nierealnych oczekiwań)	Ochrona przed konsekwencjami prawnymi, o ile zgłaszający postępuje zgodnie z polityką CVD
Wzrost świadomości przedsiębiorstwa i w obszarze podatności	Publiczna pochwała i możliwość dzielenia się informacjami na temat podatności z szerszą społecznością IT (po upływie czasu na upublicznienie)
„Bezpieczna” przestrzeń do przekazywania informacji - jasne i przejrzyste zasady komunikacji przekazywania informacji o podatnościach	Ewentualna gratyfikacja finansowa lub nagroda rzeczowa

Okiem prawnika

Ramy CVD w projekcie Dyrektywy NIS 2

Tematyka skoordynowanego ujawniania podatności została ujęta w projekcie Dyrektywy NIS 2[1]. Przepisy zawarte w dokumencie wyznaczają role zarówno dla Państw Członkowskich, jak i dla ENISA.

Dyrektywa NIS 2 - Obowiązki Państw Członkowskich

Pierwszym, podstawowym obowiązkiem nakładanym na Państwa Członkowskie w ramach przepisów Dyrektywy NIS 2 (Artykuł 5) jest przyjęcie, w ramach krajowej strategii cyberbezpieczeństwa, polityki mającej na celu promowanie i ułatwianie skoordynowanego ujawniania podatności. Na podstawie Artykułu 6 każdy kraj ma wskazać jeden z krajowych CSIRTów jako koordynatora procesu skoordynowanego ujawniania podatności, pełniącego jednocześnie rolę Zaufanego Pośrednika.

Zaufany Pośrednik, ułatwia, w stosownych przypadkach, interakcję pomiędzy Zgłaszającym a Organizacją. W sytuacji, gdy zidentyfikowana podatność ma charakter transgraniczny i dotyczy grupy takich podmiotów w różnych krajach Unii, wyznaczony CSIRT z każdego Państwa Członkowskiego, w którym ujawniono podatność, współpracuje z siecią CSIRT. Pozostałe krajowe zespoły reagowania na incydenty komputerowe mają w zakresie swoich obowiązków (Artykuł 10) monitorowanie podatności na poziomie krajowym, a także wczesne ostrzeganie podmiotów niezbędnych i istotnych oraz innych zainteresowanych podmiotów.

Znaczna część zadań lub obowiązków państw członkowskich i krajowych podmiotów cyberbezpieczeństwa dotyczy obszaru współpracy lub wymiany informacji, tak w wymiarze krajowym jak i międzynarodowym. Obowiązki te obejmują różne podmioty, pozostające ze sobą w różnych relacjach na gruncie tak krajowych, jak i unijnych przepisów prawa.

Przykładowo CSIRTy (Artykuł 10) mają za zadanie przekazywanie informacji o podatnościach, a także propagują wdrażanie oraz stosowanie wspólnych lub znormalizowanych praktyk, systemów kwalifikacji oraz taksonomii w zakresie skoordynowanego ujawniania podatności.

Natomiast w szerszej i międzynarodowej perspektywie Sieć CSIRT (Artykuł 13) odpowiada za te same zadania na poziomie wymagającym wielostronnej współpracy i przekazywania danych pomiędzy krajowymi CSIRTami państw unijnych. Na podstawie Artykułu 12 grupa współpracy, tworzona przez ekspertów z krajów UE oraz ENISA i pracująca na poziomie strategicznym, ma na gruncie przepisów Dyrektywy NIS 2 za zadanie wymianę najlepszych praktyk i informacji w związku z wdrażaniem dyrektywy oraz innych norm w obszarze cyberzagrożeń i incydentów, w tym m.in. w odniesieniu do podatności.

1 Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylająca dyrektywę (UE) 2016/1148

Kraje UE mają konkretne zadania w zakresie relacji z i pomiędzy podmiotami niezbędnymi i istotnymi, w szczególności zapewnienie możliwości wymiany informacji na temat cyberbezpieczeństwa, w tym odnośnie wykrytych lub zidentyfikowanych podatności, luk i błędów. Co ważne, Państwa Członkowskie zapewniają, aby wymiana informacji odbywała się w ramach zaufanych społeczności podmiotów niezbędnych i istotnych, do których przystąpienie jest dobrowolne, a członkostwo może ustać w dowolnym momencie. Kraje Unii ustanawiają w tym zakresie przepisy i procedury regulujące sposób, a także platformę do przekazywania danych i komunikacji pomiędzy podmiotami.

Państwa Członkowskie na gruncie Artykułu 18 mają także zapewnić odpowiednie i proporcjonalne środki, tak techniczne jak i organizacyjne, zarządzania ryzykiem w cyberprzestrzeni. Mają one obejmować m.in. określenie postępowania w przypadku ujawnienia podatności w celu zapewnienia bezpieczeństwa w procesie zakupowym, rozwoju i utrzymania sieci oraz systemów informatycznych. W kontekście bezpieczeństwa łańcucha dostaw należy ponadto uwzględniać cechy charakterystyczne producentów, dostawców i usługodawców.

Dyrektywa NIS 2 - Obowiązki ENISA

Zasadniczą rolą ENISA, na podstawie Artykułu 6, jest opracowanie i prowadzenie europejskiego rejestru podatności, a także ustanowienie związanych z tym polityk, procedur oraz utrzymanie odpowiednich systemów informatycznych. Ma to w szczególności wspomóc podmioty istotne i niezbędne, a także dostawców sieci i systemów w ujawnianiu i rejestrowaniu podatności, a także zapewnić dostęp do informacji o podatnościach wykazanych w rejestrze. Potencjalnie znajdujące się w tym repozytorium informacje dotyczą:

- produktu lub usług ICT, których ta podatność dotyczy,
- dotkliwości podatności pod względem okoliczności, w jakich może ona zostać wykorzystana,
- dostępności powiązanych z podatnościami łat (ang. patch) dla oprogramowania,
- wytycznych skierowanych do użytkowników produktów i usług, których dotyczy podatność, wskazujących sposoby ograniczania ryzyka wynikającego z ujawnionych podatności.

ENISA ma swoją rolę także w kwestii wymiany informacji o podatnościach podmiotów niezbędnych i istotnych na gruncie Artykułu 26 Dyrektywy NIS 2. Agencja pomaga w ustanowieniu mechanizmów wymiany informacji na temat cyberbezpieczeństwa, a także dzieleniu się najlepszymi praktykami i wytycznymi.

Ujawnianie podatności w prawie polskim

Polskie przepisy karne określają szereg zachowań przestępczych nazywanych potocznie „cyberprzestępstwami", szczególnie tymi związanymi z wykorzystaniem narzędzi informatycznych lub sieci, systemów lub urządzeń informatycznych. Większość wspomnianych przestępstw została zgrupowana w Kodeksie karnym w rozdziale XXXIII „Przestępstwa przeciwko ochronie informacji". Tytuł ten wskazuje na główny przedmiot ochrony przyjęty przez ustawodawcę, a więc ochronę informacji, którą na gruncie współczesnych rozważań dotyczących powiązań pomiędzy ochroną informacji a cyberprzestępczością należy rozumieć jako zapewnienie poufności, integralności oraz dostępności danych informatycznych przetwarzanych w systemach, sieciach i urządzeniach informatycznych.

Zapewnienie tych podstawowych atrybutów bezpieczeństwa i potwierdzenie, że określone systemy, sieci i urządzenia informatycznych są bezpieczne wiąże się oczywiście z ich testowaniem, sprawdzaniem zabezpieczeń oraz skuteczności wdrożonych mechanizmów i procedur ochrony. Rozwój informatyki, w tym także usług testów bezpieczeństwa spowodował, że oprócz złych hakerów oraz pentesterów, których usługi zostały zamówione pojawiła się szara strefa – testerzy, których motywacja nie jest do końca zła, ale których usług nikt nie zamawiał. To z kolei rodzi problemy nie tylko w relacjach pomiędzy testującym a przedsiębiorcą, ale także na gruncie prawa karnego, a konkretnie potencjalnej karalności.

Karalność „dobrych" hakerów - polskie regulacje prawne oraz poglądy doktryny

W Polsce regulacja dotycząca wyłączenia karalności działalności tzw. białych/dobrych hakerów została wprowadzona do kodeksu karnego nowelizacją z 2017 roku z inicjatywy ówczesnego Ministerstwa Cyfryzacji. Celem wprowadzenia regulacji była ochrona przed odpowiedzialnością karną osób testujących urządzenia, oprogramowanie i sieci pod kątem podatności. Sposób sformułowania tych przepisów pozwala jednak na rozszerzenie tego kręgu nie tylko o osoby zatrudnione do przeprowadzenia takich czynności (np. o pracowników przedsiębiorstwa lub wynajętego do tego zadania podmiotu zewnętrznego), ale także wobec osób niebędących w żaden sposób związanych z organizacją.

Wspomniany kontratyp działania w celu wykrycia błędów w zabezpieczeniach systemów informatycznych zawiera określone czynniki wpływające na ocenę czy osoba może skorzystać z uniknięcia odpowiedzialności karnej, czy też nie. Nie został on wyrażony w jednym tylko artykule kodeksu karnego, lecz został umieszczony w oddzielnej jednostce redakcyjnej (art. 269 c) oraz jako element kolejnej (art. 269b par. 1a). W związku z tym na wstępie należy zaznaczyć, że możliwość wyłączenia karalności nie dotyczy każdego z przestępstw przeciwko ochronie informacji, systemów, urządzeń lub sieci informatycznych. Taka ochrona dla potencjalnego białego hakera istnieje w przypadku następujących działań:

- Bezprawnego uzyskania informacji za pośrednictwem urządzenia podsłuchowego, wizualnego albo innego urządzenia lub oprogramowania (art. 267 par. 2 kk)
- Zakłócenia systemu komputerowego (art. 269a kk)
- Wytwarzania programów komputerowych mogących posłużyć do popełnienia przestępstw przeciwko ochronie informacji, systemów, urządzeń lub sieci informatycznych (art. 269b kk)

Ponadto, samo ograniczenie dotyczy także sytuacji, w której można skorzystać z ochrony na podstawie omawianego kontratypu. Dotyczy to działania wyłącznie w celu:

- zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, albo
- opracowania metody takiego zabezpieczenia

Istotne jest także niezwłoczne powiadomienie dysponenta systemu lub sieci o ujawnionych zagrożeniach. Dodatkowo działanie podmiotu, powołującego się na działalność biało-hakerską, nie może naruszać interesu publicznego lub prywatnego i nie może jednocześnie wyrządzać szkody. Określenie w ten sposób niedozwolonego efektu działalności białego hakera jest szerokie i dotyczyć może każdego dobra prawnego.

W doktrynie prawa karnego[1] wskazuje się, że osoba, która odkryła podatność lub lukę powinna przekazać jak najbardziej szczegółową informację o tym fakcie np. poprzez wskazanie potencjalnego wektora ataku ze wskazaniem konkretnej luki i konkretnego systemu / oprogramowania / urządzenia podatnego na działanie z zewnątrz. Sam sposób przekazania informacji nie jest ściśle określony, co oznacza, że w tej kwestii pozostawiono swobodę zgłaszającemu lub podatnemu podmiotowi np. poprzez wskazanie konkretnej metody lub procedury w polityce zgłaszania podatności lub w przypadku braku jakichkolwiek wskazań – dowolną metodą zapewniającą podatnemu podmiotowi możliwość zapoznania się z informacją o potencjalnym zagrożeniu. Dodatkowo, w doktrynie występuje pogląd, że przekazanie informacji powinno być indywidualne[2], skierowane bezpośrednio do podmiotu prywatnie, a nie za pośrednictwem przestrzeni publicznej jak np. fora internetowe lub media społecznościowe.

1 Np. D. Zając [w:] Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212-277d, red. W. Wróbel, A. Zoll, Warszawa 2017, art. 269(c) lub A. Lach [w:] Kodeks karny. Komentarz, wyd. III, red. V. Konarska-Wrzosek, Warszawa 2020, art. 269(c).

2 A. Lach [w:] Kodeks karny. Komentarz, wyd. III, red. V. Konarska-Wrzosek, Warszawa 2020, art. 269(c).

Wskazane powyżej zdanie doktryny prawniczej stanowi jeden z możliwych poglądów w kwestii metod i sposobów ujawniania podatności oraz zaleceń w tej kwestii. Nie jest to pogląd wiążący prawnie, gdyż jak wspomniano wyżej, przepisy polskiego prawa zostawiły swobodę w kwestii określenia procedur informowania o podatnościach przez Zgłaszającego. Zauważyć należy, że wdrożenie przepisów lub procedur uściślających sposób przekazywania informacji o lukach i błędach, rozszerzając go o proces skoordynowanego ujawniania podatności z Zaufanym Pośrednikiem jako nieodzownym jego elementem, nie będzie stanowić naruszenia dotychczas obowiązujących przepisów. Ponadto, przyjęcie szerszych niż do tej pory regulacji prawnych w zakresie ujawniania podatności i wprowadzenie na ich podstawie krajowej polityki CVD zapewni ochronę tak Zgłaszającym, jak i Organizacjom.

Odpowiedzialności karnej nie podlega na gruncie polskich przepisów karnych osoba, której dysponent systemu/sieci/urządzenia powierzył zadanie przeprowadzenia testów lub sprawdzenia bezpieczeństwa, niezależnie czy jest to podmiot zewnętrzny czy delegowany pracownik firmy. Jest tak z uwagi na fakt, iż brak jest spełnienia warunku konstytuującego przestępstwo, czyli braku uprawnień danej osoby.

PODSUMOWANIE:

- Propozycja Dyrektywy NIS 2 nakłada szereg obowiązków i zadań w zakresie wykrywania podatności. Główne zadania wymienione w NIS 2 dotyczą kompetencji w zakresie współpracy i wymiany informacji o zidentyfikowanych w systemach lub sieciach podatnościach. Dotyczy to przekazywania danych pomiędzy podmiotami istotnymi i niezbędnymi oraz pozostałymi, występującymi na gruncie tak przepisów unijnych, jak i krajowych.
- Kluczową rolą ENISA jest opracowanie i prowadzenie europejskiego rejestru podatności, który stanowić będzie punkt odniesienia oraz źródło informacji dla wszystkich Państw Członkowskich.
- Kraje UE mają za zadanie wyznaczenie spośród krajowych CSIRTów jednego Zespołu jako koordynatora i zaufanego pośrednika, którego rola w ramach procesu skoordynowanego ujawniania podatności będzie bardziej wymagająca i ważniejsza niż innych CSIRTów.
- Polskie przepisy karne, wprowadzające kontratyp działania w celu wykrycia błędów w zabezpieczeniach systemów informatycznych, stanowią krok w dobrą stronę, umożliwiający i dający podstawę prawną do tworzenia środowiska wymiany informacji o podatnościach i zagrożeniach z szerszą społecznością IT, bez obawy z ich strony o potencjalną odpowiedzialność karną.
- Kontratyp działania w celu wykrycia błędów w zabezpieczeniach systemów informatycznych nie może zostać zastosowany do jakichkolwiek czynności o charakterze niszczącym lub wywołującymi szkody w systemach, urządzeniach lub sieciach informatycznych.

- Mimo faktu, iż przepisy dają możliwość organom ścigania do niekarania osób, które popełniły wybrane cyberprzestępstwa dla celów zabezpieczenia systemów lub sieci informatycznych, to jest to obwarowane konkretnymi warunkami, które musi spełnić osoba znajdująca podatności lub luki. Bez ich spełnienia nie ma możliwości skorzystania z kontratypu i uniknięcia odpowiedzialności karnej. Ocena ich wypełnienia leży po stronie organów ścigania lub wymiaru sprawiedliwości.

- Ogólne wskazanie warunków do zwolnienia z odpowiedzialności karnej stanowi szansę dla organów krajowego systemu cyberbezpieczeństwa oraz podmiotów prywatnych zainteresowanych wprowadzaniem polityk CVD do samodzielnego, oddolnego określenia warunków, będących możliwymi do zaakceptowania przez jak najszerszy krąg podmiotów i instytucji.

- Sformułowanie polityki lub procedur skoordynowanego ujawniania podatności (CVD) może stanowić znaczące praktyczne uzupełnienie i uszczegółowienie do przepisów wyłączających odpowiedzialność karną w ramach kontratypu działania w celu wykrycia błędów w zabezpieczeniach systemów informatycznych. Przyjęcie jednolitych ram na poziomie krajowym ułatwi organom ścigania oraz wymiaru sprawiedliwości, a także podatnym podmiotom ocenę zachowania osób przekazujących informacje o podatnościach lub lukach.

1 Np. D. Zając [w:] Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212-277d, red. W. Wróbel, A. Zoll, Warszawa 2017, art. 269(c) lub A. Lach [w:] Kodeks karny. Komentarz, wyd. III, red. V. Konarska-Wrzosek, Warszawa 2020, art. 269(c).

2 A. Lach [w:] Kodeks karny. Komentarz, wyd. III, red. V. Konarska-Wrzosek, Warszawa 2020, art. 269(c).

Jak powinien wyglądać proces CVD?

W CVD kluczowa jest współpraca stron. Układa się ona najlepiej wtedy, gdy wszyscy działają w ramach ustalonych zasad. Dlatego tak ważne jest, aby Organizacje wykonały pierwszy krok i pokazały gotowość przyjmowania informacji o podatnościach poprzez opublikowanie polityki CVD. Wtedy proces ujawniania podatności przebiega zgodnie z oczekiwaniami, strony znają swoje prawa i obowiązki na każdym z etapów, a Zaufany Pośrednik udziela wsparcia tylko, gdy istnieje taka potrzeba.

Jest to sytuacja najbardziej pożądana i ma dużo zalet. Jednak trzeba liczyć się z tym, że nie wszystkie Organizacje mają opracowane polityki CVD. W takim przypadku Zgłaszający nadal ma obowiązek poinformować Organizację o znalezionej podatności. Może w tym celu skorzystać z pomocy Zaufanego Pośrednika.

Odpowiedzialność i obowiązki stron w procesie CVD

W CVD każda ze stron ma swoją rolę i zobowiązania.

Obowiązki Organizacji

1. Odpowiedzialność za bezpieczeństwo systemu

Organizacja ponosi odpowiedzialność za bezpieczeństwo systemu, również za informowanie o podatnościach. Jednym ze sposobów wykrycia błędów czy luk jest zaangażowanie do tego osób trzecich (Zgłaszających). Dlatego też zachęcamy Organizacje do publikacji polityki CVD.

2. Zobowiązanie do przestrzegania polityki CVD

Organizacja, która publikuje politykę CVD zobowiązuje się, że będzie przestrzegała jej zapisów, a w szczególności nie będzie składała skargi do organów ścigania, jeżeli Zgłaszający przestrzega zasad polityki.

3. Odpowiedzialność za usunięcie podatności

Po wykryciu podatności, odpowiedzialność za usunięcie luki spoczywa na Organizacji. Zgłaszający nie ma wpływu na wewnętrzne procesy usuwania podatności, dlatego ważne, aby Organizacja poinformowała (bez zbędnych szczegółów) kiedy i w jaki sposób podatność będzie usunięta, a także o sposobie jej upublicznienia.

Obowiązki Zgłaszającego

1. Odpowiedzialność za przestrzeganie polityki CVD

Zgłaszający działa na rzecz zwiększenia bezpieczeństwa systemów IT i dąży do ujawnienia podatności. Jednak powinno się to odbywać w ramach ogłoszonej polityki CVD (najczęściej organizacje umieszczają politykę CVD na ogólnodostępnej stronie internetowej).

2. Obowiązek przestrzegania polskiego prawa

W przypadku, gdy Zgłaszający wykrył podatność w systemie Organizacji, która nie opublikowała polityki CVD, zgodnie z polskim prawem, nadal ma obowiązek przekazać taką informację. Powinien to zrobić bezpośrednio i indywidualnie. W przypadku jakichkolwiek trudności (czy to przy identyfikacji Organizacji, czy też w znalezieniu osoby kontaktowej), Zgłaszający może skorzystać z pomocy Zaufanego Pośrednika.

UWAGA

Wyszukiwanie lub ujawnianie podatności w systemach Organizacji, które nie mają polityki CVD, może wiązać się z naruszeniem przepisów polskiego prawa, a w konsekwencji z możliwym poniesieniem odpowiedzialności prawnej – cywilnej lub karnej. W Polsce brakuje przepisów jednoznacznie chroniących w takich przypadkach osoby zgłaszające podatności, gdyż każdorazowo musi to zostać ocenione pod kątem konkretnych kryteriów: celu działania, czasu od wykrycia podatności do przekazania o niej informacji, a także oceny czy działanie Zgłaszającego nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody.

Obowiązki Zaufanego Pośrednika

1. Pełnienie roli tzw. „Zaufanego Pośrednika” pomiędzy stronami

Projekt Dyrektywy NIS 2 nakłada na państwa członkowskie obowiązek wyznaczenia CSIRTu, pełniącego rolę tzw. „zaufanego pośrednika” / koordynatora, który w razie potrzeby ułatwi interakcję pomiędzy stronami procesu CVD. Zaangażowanie Zaufanego Pośrednika jest szczególnie istotne w sytuacji, gdy organizacja nie opublikowała polityki CVD, a Zgłaszający znalazł podatność przypadkowo, czy to w ramach aktywnych testów systemów.

Do zadań Zaufanego Pośrednika należą:

- Identyfikacja i kontakt z zainteresowanymi podmiotami;
- Wspieranie podmiotów zgłaszających;
- Negocjowanie terminarza ujawnienia podatności;
- Zarządzanie informacją o podatnościach, których skutki dotykają wielu organizacji; (wielostronne ujawnianie podatności).

2. Współpraca z CSIRT z innych państw

W przypadku, gdy podatność dotyczy podmiotów posiadających jednostkę organizacyjną w co najmniej dwóch państwach członkowskich, sieć CSIRT współpracuje w celu wspólnej koordynacji usunięcia podatności.

Rejestr podatności ENISA[2]

Dyrektywa NIS 2 zobowiązuje ENISA do prowadzenia europejskiego rejestru podatności. Rejestr ma zawierać informacje na temat podatności, produktów lub usług, których dana podatność dotyczy. A także dane o sposobie jej wykorzystania, dostępności łat lub wytyczne na temat sposobów ograniczenia ryzyka.

Podmioty istotne, niezbędne oraz ich dostawcy sieci i systemów informatycznych będą mogły, na zasadzie dobrowolności, zgłaszać podatności do rejestru ENISA[3].

2 Agencja Unii Europejskiej ds. Cyberbezpieczeństwa

3 Motyw 30 projektu dyrektywy NIS2

CVD krok po kroku

Proces wdrożenia zasad CVD powinien rozpoczynać się od Organizacji, która jest odpowiedzialna za bezpieczeństwo systemu. Do jej obowiązków należy również monitorowanie podatności, a także naprawa błędów, luk i przygotowywanie aktualizacji.

Organizacja może zwrócić się o pomoc w testowaniu systemu do osób z zewnątrz. W tym celu opracowuje i ogłasza politykę CVD, która zawiera zasady współpracy w obszarze wyszukiwania i zgłaszania podatności.

Następnie Zgłaszający, którzy mają świeże spojrzenie, mogą zaangażować się testowanie systemu i wyszukiwanie błędów i luk. Ich rola jest niezwykle istotna, bo przyczyniają się do wzrostu poziomu cyberbezpieczeństwa. Ważne, aby osoby te postępowały odpowiedzialnie, przestrzegały zasad polityki CVD, współpracowały z Organizacją, a także powstrzymały się od upubliczniania jakichkolwiek informacji zanim podatność zostanie naprawiona.

Zadaniem Zaufanego Pośrednika jest wspieranie komunikacji pomiędzy stronami, a także pomoc w koordynacji zarządzania podatnością, szczególnie gdy dotyczy ona wielu organizacji i/lub organizacji zlokalizowanych w różnych krajach. Należy jednak podkreślić, że rola Zaufanego Pośrednika ma charakter wspierający, a podstawą procesu CVD jest zawsze Organizacja i Zgłaszający.

W przypadku, gdy brakuje polityki CVD, Zgłaszający nadal ma obowiązek poinformować Organizację o znalezionej podatności. Może poprosić o pomoc Zaufanego Pośrednika, który wesprze w dotarciu do Organizacji, znalezieniu osoby kontaktowej, a także ustaleniu zasad dalszej współpracy.

Platformy wspomagające proces CVD

Na rynku działają również komercyjne platformy, które oferują pośrednictwo w procesie CVD pomiędzy dobrymi hakerami, a organizacjami. W ramach wykupionej usługi Organizacje mogą udostępnić swoje systemy do wyszukiwania podatności przez Zgłaszających, zatrudnionych w ramach danej platformy.

Kroki CVD po stronie organizacji

1. Organizacja opracowuje i podaje do publicznej wiadomości politykę CVD – tym samym oświadcza, że jest gotowa na przyjmowanie raportów o podatnościach, na zasadach ogłoszonych w dokumencie.

2. Aby ułatwić zgłaszanie podatności, Organizacja powinna opracować procedurę przyjmowania zgłoszeń, a także zapewnić ich sprawną obsługę. Warto oddelegować w tym celu konkretnych pracowników tak, aby informacje o podatnościach były rozpatrywane najszybciej jak to możliwe.

3. Po przyjęciu zgłoszenia Organizacja informuje zgłaszającego o statusie sprawy. Następnie ustala czas usunięcia podatności. Czas ten zależy bezpośrednio od charakteru podatności i rodzaju systemu. Najczęściej jest to 60 dni (jeśli podatność dotyczy luk w oprogramowaniu) lub nawet 6 miesięcy (jeśli podatność dotyczy wady sprzętu lub też występuje w większej ilości systemów). Po upływie terminu podatność może zostać upubliczniona.

4. Jeżeli podatność dotyczy większej liczby instytucji, Organizacja kontaktuje się z osobami odpowiedzialnymi w tych przedsiębiorstwach. Może skorzystać z pomocy Zaufanego Pośrednika, aby zidentyfikować te instytucje i nawiązać z nimi kontakt.

5. Może się zdarzyć, że ze względu na trudność w usunięciu podatności albo wysokie koszty, Organizacja zdecyduje się nie naprawiać systemu i zaakceptować lukę jako element ryzyka. Taka decyzja powinna być podjęta w porozumieniu z osobą zgłaszającą i nie powinna mieć wpływu na upublicznienie informacji o istnieniu podatności.

6. W dobrym tonie jest nagrodzenie Zgłaszającego. Nagroda zachęca Zgłaszających do wspierania organizacji w wyszukiwaniu luk i błędów w oprogramowaniu, a także stanowi formę podziękowania za wykonaną pracę. Dodatkowo motywuje społeczność tzw. białych hakerów do wykorzystywania wiedzy o podatnościach w dobrym celu, a nie przekazywania jej w niepowołane ręce.

7. Gdy wykrycie podatności odbyło się zgodnie z zasadami polityki CVD, Organizacja powinna odstąpić od pociągania Zgłaszającego do odpowiedzialności karnej.

8. Po konsultacji ze Zgłaszającym, Organizacja upublicznia informację o podatności. Jeśli wszystkie strony wyraziły zgodę, wiedzę na temat szczegółów podatności można udostępnić szerszej społeczności IT. Zgłaszający ma prawo zadecydować, czy przy upublicznieniu podatności zostaną podane jego dane, czy też nie.

9. Organizacja może, na zasadzie dobrowolności, zgłosić podatność do rejestru ENISA[4], a także do Zaufanego Pośrednika, szczególnie jeśli podatność dotyczy popularnego oprogramowania. Gromadzenie informacji na temat podatności produktów i usług ICT, a także sposobów zapobiegania im przekłada się na wzrost bezpieczeństwa w cyberprzestrzeni.

4 Rejestr podatności ENISA – ustanowienie rejestru zostało zapowiedziane w projekcie Dyrektywy NIS 2.

Polityka CVD zawiera:

- jasne wytyczne dotyczące wyszukiwania podatności (m.in. jakie systemy czy elementy systemów podlegają testowaniu, jakie metody są dozwolone);
- sposób raportowania podatności (formularz online, adres e-mail, zasady bezpieczeństwa wysyłanych zgłoszeń, kwestie anonimowości);
- informacje na temat procedury obsługi podatności po stronie Organizacji (w tym czas na usunięcie podatności, zanim zostanie ona upubliczniona);
- zobowiązanie do odstąpienia od pociągania do odpowiedzialności karnej Zgłaszających, którzy przestrzegają zapisów polityki CVD;
- informacje na temat ew. nagrody.

Polityka powinna być ogólnodostępna i łatwa do znalezienia (można ją umieścić, np. na stronie internetowej Organizacji i ogłosić w mediach społecznościowych).

CyberPOLICY NASK

Kroki CVD po stronie zgłaszającego

1. Osoba zgłaszająca jest odpowiedzialna za przestrzeganie polityki CVD, opracowanej przez Organizację. Oznacza to, że nie powinna robić więcej, niż to konieczne, aby wykryć podatność. Jeżeli Organizacja nie posiada polityki CVD, to nadal należy jej zgłosić znaleziony błąd czy lukę (samodzielnie lub z pomocą Zaufanego Pośrednika).

2. Podatność musi być zgłoszona tak szybko, jak to możliwe, aby zapobiec wykorzystaniu błędu przez osoby niepowołane.

3. Zgłaszający ma obowiązek zachowania zasad poufności, aby uniemożliwić innym uzyskanie dostępu do informacji.

4. Zgłaszający powinien współpracować z Organizacją na rzecz jak najszybszego usunięcia podatności, w tym udzielić niezbędnych informacji na temat wykrytego błędu. W przypadku trudności w komunikacji, Zgłaszający może poprosić o wsparcie Zaufanego Pośrednika, który pomoże w nawiązaniu współpracy.

5. Informowanie o podatności, czy dalsze przekazywanie informacji nie może być uzależnione od nagrody. Ustalenie nagrody stanowi inicjatywę Organizacji i jest formą podziękowania, która może zostać ogłoszona już w polityce CVD.

6. Zgłaszający ma prawo do informacji na temat obsługi podatności, a także bierze udział w ustaleniu zasad jej ujawnienia. Jeżeli podatność dotyczy większej liczby instytucji, konieczne może być uzyskanie zgody na jej upublicznienie przez wszystkie zaangażowane strony. Zgłaszający może wyrazić zgodę na ujawnienie swoich danych lub też zachować anonimowość.

7. Jeżeli strony wyrażą chęć, możliwe jest również opublikowanie informacji o szczegółach podatności szerszej społeczności IT.

Rola Zaufanego Pośrednika

1. Podstawą procesu CVD jest zawsze Organizacja i Zgłaszający. Zaufany Pośrednik pełni rolę wspierającą i angażuje się w proces CVD na prośbę którejś ze stron (szczególnie w sytuacji, gdy brakuje polityki CVD).

2. Jeśli Zgłaszającemu zależy na zachowaniu anonimowości i nie chce skontaktować się bezpośrednio z Organizacją, może zrobić to za pośrednictwem Zaufanego Pośrednika.

3. Zaufany Pośrednik podejmie wysiłki w celu zwrócenia uwagi Organizacji na daną podatność i w razie potrzeby zaoferuje pomoc w naprawie błędu. Warto jednak pamiętać, że odpowiedzialność za system informatyczny zawsze spoczywa na Organizacji. Zaufany Pośrednik nie może zmusić Organizacji do usunięcia podatności.

4. W przypadku, gdy mamy do czynienia z wielostronnym ujawnianiem podatności, czyli gdy podatność dotyczy większej liczby systemów lub instytucji, Zaufany Pośrednik może wesprzeć w przekazywaniu informacji i kontakcie z zainteresowanymi stronami.

5. W przypadku, gdy podatność dotyczy podmiotów posiadających jednostkę organizacyjną w co najmniej dwóch państwach członkowskich, Zaufany Pośrednik poprzez sieć CSIRT[5] współpracuje w celu wspólnej koordynacji usunięcia podatności.

6. Zaufany Pośrednik będzie traktować informacje na temat podatności w sposób poufny i nie będzie udostępniać danych osobowych bez zgody obu stron, chyba że wynika to z obowiązku ustawowego.

7. Zaufany Pośrednik w porozumieniu z obiema stronami może zaangażować się w rozpowszechnianie informacji o podatności w szerokiej społeczności IT, np. poprzez publikację informacji lub opracowanie rekomendacji dla konkretnych instytucji czy sektorów.

5 Mowa o sieci CSIRT wg. dyrektywy NIS

CVD krok po kroku

1. Organizacja opracowuje i podaje do publicznej wiadomości politykę CVD.

2. W chwili znalezienia podatności, Zgłaszający kontaktuje się z Organizacją (nawet jeśli nie istnieje polityka CVD). Może zrobić to z pomocą Zaufanego Pośrednika.

3. Organizacja informuje o przyjęciu zgłoszenia, a także o przewidywanym czasie usunięcia luki. Strony ustalają planowany termin upublicznienia podatności.

4. Jeśli jest taka potrzeba, strony angażują Zaufanego Pośrednika jako wsparcie w komunikacji.

5. Po usunięciu podatności następuje upublicznienie informacji, a także podziękowanie i gratyfikacja dla Zgłaszającego.

6. Organizacja dodaje podatność do europejskiego rejestru podatności ENISA, a także do rejestrów krajowych (jeżeli istnieją). Przekazuje również informacje na temat ryzyka, dostępnych łatek i zalecanych działań.

Komunikacja na każdym z etapów

Proces CVD w dużej mierze opiera się na zaufaniu. Organizacja udziela zgody osobom trzecim na testowanie systemu informatycznego w celu wyszukiwania podatności. Z drugiej strony, Zgłaszający wyszukuje błędy wierząc, że jeśli będzie stosować się do zasad, nie zostanie pociągnięty do odpowiedzialności za działanie niezgodne z prawem. Dla każdej ze stron tego procesu ważna jest jasna i czytelna komunikacja.

Etap I – ogłoszenie polityki CVD

Pierwszą formą komunikacji w procesie skoordynowanego ujawniania podatności jest publikacja polityki CVD. Dlatego tak ważne, aby Organizacja przygotowała taki dokument, bo wtedy może ustalić zasady, na jakich chciałaby przyjmować informacje o podatnościach. Polityka może ulegać aktualizacjom, a wiedza o zmianach może być istotna dla Zgłaszających. Dlatego ważne, aby umieścić datę publikacji, a także poinformować o modyfikacjach, czy to w formie podsumowania zmian, czy archiwum zawierającego poprzednie wersje dokumentu.

Warto, aby w polityce CVD zamieścić także informacje na temat kanałów komunikacji pomiędzy stronami (np. poczta elektroniczna, czy formularz online). Szczególnie ważne jest określenie zasad poufności przekazywanych informacji tak, aby nie dostały się one w niepowołane ręce.

Etap II – komunikacja w trakcie ujawniania i obsługi podatności

Zgłaszający, najszybciej jak to możliwe, nawiązuje kontakt z Organizacją w sposób określony w polityce CVD. Jeżeli takiej polityki nie ma, kontaktuje się z Organizacją bezpośrednio, poprzez publicznie dostępne kanały komunikacji (np. adres e-mail, numer telefonu). Może również skorzystać z pomocy Zaufanego Pośrednika.

Ważne, aby w komunikacie przekazać szczegółowe informacje na temat znalezionej podatności. Już na tym etapie Organizacja powinna wysłać potwierdzenie przyjęcia zgłoszenia, a także poinformować o spodziewanym terminie udzielenia odpowiedzi, tak aby Zgłaszający wiedział, kiedy może spodziewać się kolejnego kontaktu. Jeżeli Organizacja nie jest w stanie podać terminu usunięcia podatności, może to zrobić po wstępnej analizie. Ważne jednak, aby poinformować Zgłaszającego, kiedy otrzyma informację zwrotną.

Może się zdarzyć, że Zgłaszający raportując podatność, z góry ustala termin podania jej do wiadomości publicznej, np. z powodu prezentacji na konferencji. W takiej sytuacji ważne, aby Zgłaszający poinformował Organizację, kiedy nastąpi upublicznienie podatności, a także określił, czy istnieje szansa modyfikacji tego terminu, czy też nie.

Jeżeli istnieje taka konieczność, Organizacja kontaktuje się ze Zgłaszającym w celu uzupełnienia zgłoszenia i uzyskania dodatkowych informacji na temat podatności. W dobrym tonie jest regularne informowanie o kolejnych etapach obsługi podatności i planowanych działaniach. Dzięki temu Zgłaszający, mimo że jest spoza Organizacji, może czuć się zaangażowany w proces usuwania błędu. Jeżeli z jakiegokolwiek powodu okaże się, że termin upublicznienia podatności wydłuża się, Zgłaszający będzie o tym wiedział z wyprzedzeniem.

Na każdym z tych etapów można zaangażować Zaufanego Pośrednika, w celu wsparcia którejkolwiek ze stron lub też koordynacji komunikacji, w szczególności, gdy dochodzi do wielostronnego ujawniania podatności (z udziałem wielu organizacji), Organizacja potrzebuje wsparcia w usunięciu podatności lub też Zgłaszający napotkał trudności w kontakcie z Organizacją.

Etap III – komunikacja po usunięciu podatności

Dla wielu Zgłaszających ważne jest publiczne uznanie ich osiągnięć. Dlatego należy z góry ustalić termin ujawnienia podatności, a także docenić tych, którzy przyczynili się do usunięcia błędu. Organizacja powinna bez zbędnej zwłoki wypłacić nagrodę, jeżeli została wyznaczona, a także umieścić podziękowania dla Zgłaszającego na stronie internetowej, czy w mediach społecznościowych. Ważne, aby potwierdzić zgodę na ujawnienie danych osobowych.

Publikacja podatności kończy proces CVD, a tym samym daje stronom prawo do swobodnego przekazywania informacji na ten temat, chyba że strony ustalą inaczej.

Brak polityki CVD – wsparcie Zaufanego Pośrednika

Proces CVD jest najbardziej efektywny wtedy, gdy Organizacja z góry przygotuje się na przyjmowanie informacji o podatnościach i określi zasady współpracy ze Zgłaszającymi w polityce CVD. Jednak, gdy brakuje polityki CVD, ciężar nawiązania kontaktu spoczywa na Zgłaszającym, bo to on, zgodnie z prawem, ma obowiązek poinformować Organizację o znalezionej podatności. Niestety Organizacje nie zawsze chętnie przyjmują takie zgłoszenia, ciężko znaleźć osobę kontaktową i nawiązać współpracę. W takiej sytuacji wsparciem może służyć Zaufany Pośrednik, który z racji pełnienia swojej funkcji, ma większe szanse na dotarcie do Organizacji i znalezienie osób odpowiedzialnych za obsługę podatności.

Instytucja Zaufanego Pośrednika znalazła się w projekcie dyrektywy NIS 2 i oficjalnie zostanie powołana w ramach implementacji dyrektywy do prawa krajowego. Obecnie zgłoszenia podatności przyjmuje zespół CSIRT NASK, z którym można skontaktować się poprzez formularz na stronie: incydent.cert.pl.

Rekomendacje do polityki krajowej

Aktualnie w Polsce nie istnieją jednolite zasady, które porządkują proces skoordynowanego ujawniania podatności. Nieliczne Organizacje posiadają politykę CVD, a podatności zgłaszane są indywidualnie lub też za pośrednictwem CSIRT NASK, który przyjmuje takie zgłoszenia przez formularz na stronie incydent.cert.pl. Sytuacja ta będzie musiała ulec zmianie wraz z implementacją dyrektywy NIS 2, której projekt nakłada na państwa członkowskie obowiązek przyjęcia polityki mającej na celu promowanie i ułatwianie skoordynowanego ujawniania podatności.

Rekomendacje przedstawione poniżej mają na celu wsparcie Polski we wdrożeniu procesu CVD na poziomie krajowym.

Rekomendacje do polskiej polityki krajowej CVD:

- Ustalenie jasnych zasad skoordynowanego ujawniania podatności w Polsce, nie tylko dla podmiotów ujętych w NIS 2, ale dla wszystkich przedsiębiorstw działających na terenie kraju.
- Przyjęcie rozwiązań prawnych, które uregulują kwestie odpowiedzialności Zgłaszających i ich ochronę przed konsekwencjami prawnymi (o ile nie przekroczyli zasad opublikowanych w polityce CVD).
- Ustalenie zasad współpracy stron w sytuacji, gdy Organizacja nie opublikowała polityki CVD.
- Przyjęcie zasad upubliczniania podatności bez konsekwencji (ustalenie obowiązujących terminów, po upływie których Zgłaszający może opublikować informacje o podatności)
- Wyznaczenie CSIRTu poziomu krajowego, który będzie pełnił rolę Zaufanego Pośrednika.
- Zdefiniowanie roli Zaufanego Pośrednika w polityce krajowej, opisanie jego zadań i kompetencji, a także zapewnienie finansowania na realizację tych zadań (w tym etaty dla pracowników, odpowiednie narzędzia).
- Przyjęcie rozwiązań prawnych ułatwiających Zaufanemu Pośrednikowi kontakt z właścicielami podatnych systemów widocznych z internetu, np. przyznanie prawa do uzyskania danych właściciela publicznego adresu IP.
- Opracowanie rozwiązań, które umożliwią Zaufanemu Pośrednikowi wywarcie wpływu na Organizacje w celu usunięcia podatności.

- Utworzenie na poziomie krajowym rejestru podatności produktów i usług ICT, sposobów ich wykorzystania, dostępności łatek/aktualizacji i porad dotyczących ograniczenia ryzyka.

- Stworzenie platformy wymiany informacji i doświadczeń w zakresie CVD.

- Stworzenie kampanii zwiększającej świadomość na temat CVD, która byłaby zachętą dla Organizacji do zaangażowania się w skoordynowane ujawnianie podatności na poziomie krajowym, usuwanie błędów i zgłaszanie podatności do krajowego i europejskiego rejestru podatności produktów i usług ICT.

- Opracowanie pozafinansowego systemu gratyfikacji (np. uznanie zasług, wyróżnienie, gadgety, programy stażowe itp.) dla osób, które zgłaszają podatności do Zaufanego Pośrednika. Obecnie brakuje takiego systemu, co przekłada się na niewielkie zainteresowanie tematem wśród etycznych hakerów.

Zakończenie

Skoordynowane ujawnianie podatności jest sposobem na zwiększenie poziomu cyberbezpieczeństwa, z którego korzyści mogą czerpać zarówno Organizacje, jak i Zgłaszający. Jednak brak jednolitych przepisów i polityki krajowej sprawia, że sytuacja prawna osób wyszukujących podatności jest niejednoznaczna i mogą się one obawiać konsekwencji prawnych. Z drugiej strony Organizacje nie są motywowane do opracowania polityki CVD i nie mają świadomości korzyści takiego rozwiązania. Zespół CERT Polska, który działa w ramach CSIRT NASK i przyjmuje zgłoszenia podatności, spotyka się z brakiem zrozumienia ze strony Organizacji, trudnościami z identyfikacją osób odpowiedzialnych i brakiem chęci współpracy. Dlatego konieczne jest opracowanie krajowej polityki CVD, która zapewni przyjęcie odpowiednich regulacji prawnych dla ochrony Zgłaszających, ustali jasne zasady procesu CVD (w sytuacji, gdy istnieje polityka CVD, a także wtedy, gdy jej nie ma), a także oficjalnie powoła Zaufanego Pośrednika i stworzy rozwiązania, które wesprą jego działalność. Szczególnie, że takie zobowiązania i tak Polskę czekają w ramach implementacji dyrektywy NIS 2. Wprowadzenie ich z wyprzedzeniem pozwoli na szybsze wdrożenie skoordynowanego ujawniania podatności w naszym kraju, co przyczyni się do wzrostu poziomu cyberbezpieczeństwa wszystkich obywateli.