NASK
Cyber POLICY

Skoordynowane ujawnianie informacji o podatnościach

Coordinated Vulnerability Disclosure (CVD)

Podsumowanie sesji “Together-safer, stronger, smarter”

Wstęp

Szanowni Państwo,

Z nieukrywaną przyjemnością, przedstawiam Państwu publikację podsumowującą sesję zamkniętą "Together-safer, stronger, smarter". Wydarzenie, w którym wzięli udział przedstawiciele krajowych i międzynarodowych instytucji zajmujących się cyberbezpieczeństwem zostało zorganizowane przez NASK Państwowy Instytut Badawczy 21 października 2021r. Głównym tematem sesji był proces skoordynowanego ujawniania informacji o podatnościach, lukach i błędach (ang. *Coordinated Vulnerability Disclosure – CVD*).

Wydarzenie było okazją nie tylko do wymiany doświadczeń i dobrych praktyk, ale także do wzmocnienia współpracy pomiędzy NASK PIB i europejskimi ekspertami działającymi w obszarze CVD. W spotkaniu wzięli udział przedstawiciele polskich i europejskich agencji rządowych i organizacji zajmujących się cyberbezpieczeństwem.

Podczas spotkania prelegenci przedstawili krajowe podejścia, doświadczenia i dobre praktyki w obszarze CVD. Wszyscy zgodnie podkreślili istotną rolę, jaką odgrywają tzw. dobrzy hakerzy, (ang. *positive hackers*) a także inne podmioty (producenci i dostawcy), którzy zajmują się wyszukiwaniem informacji o podatnościach, lukach i błędach. Ich działalność wpływa na zwiększenie poziomu bezpieczeństwa systemów, urządzeń i procesów ICT. Nie może jednak być prowadzona bez jakiejkolwiek kontroli. Dlatego ważne, aby ustanowić jasne ramy i zasady współpracy pomiędzy podmiotami wyszukującymi podatności, a właścicielami systemów. Zasadne wydaje się również zapewnienie tym podmiotom ochrony przed odpowiedzialnością karną na bazie już istniejących przepisów lub poprzez wprowadzenie nowych.

Poniżej znajdziecie Państwo, przykłady różnych rozwiązań zaprezentowanych w trakcie sesji zamkniętej przez naszych kolegów – przedstawicieli NCSC z Niderlandów, BSI z Niemiec, NBU ze Słowacji i CCB z Belgii.

Życzę miłej lektury i inspiracji w podejściu do tematu CVD.

Krzysztof Silicki

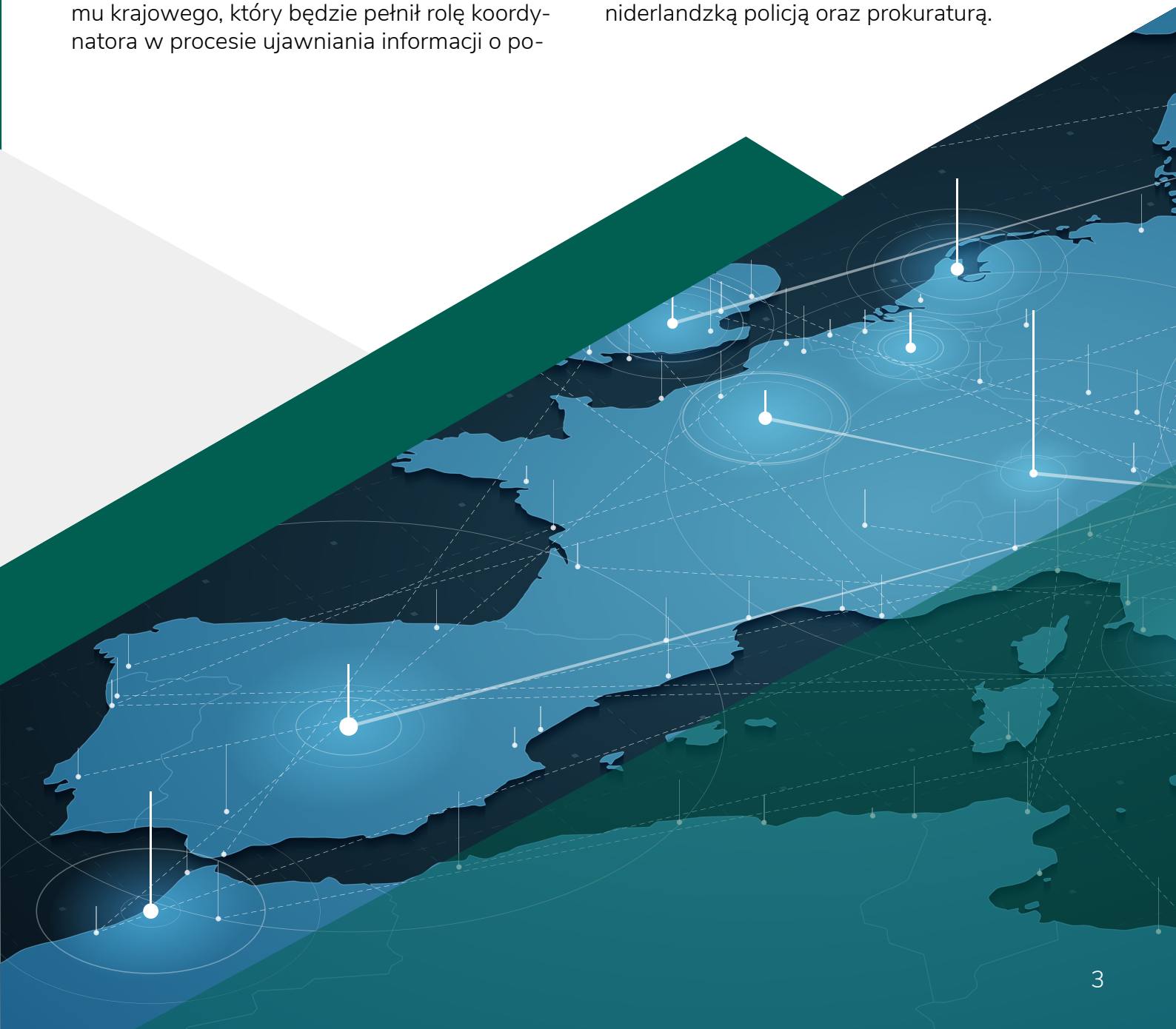
Z-ca Dyrektora NASK
Dyrektor ds. Cyberbezpieczeństwa i Innowacji

CVD na poziomie Unii Europejskiej

W dniu 16 grudnia 2020 r. Komisja Europejska przedstawiła nowy pakiet cyberbezpieczeństwa, którego częścią, poza nową Strategią Cyberbezpieczeństwa i Dyrektywą o odporności krytycznych podmiotów, jest propozycja Dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii Europejskiej – tzw. Dyrektywa NIS 2. CVD jest na tyle istotnym zagadnieniem, że Komisja Europejska postanowiła włączyć ten temat do projektu Dyrektywy.

W artykule 6 KE zobowiązała każde państwo członkowskie do wyznaczenia CSIRT-u poziomu krajowego, który będzie pełnił rolę koordynatora w procesie ujawniania informacji o podatnościach, lukach i błędach oraz zaufanego pośrednika, ułatwiającego interakcje pomiędzy podmiotem zgłaszającym a producentem lub dostawcą produktów lub usług ICT. Przyjęcie takiego podejścia istotnie wzmocni rolę CSIRT w procesie budowy partnerstw publiczno–prywatnych w obszarze cyberbezpieczeństwa.

W dniu 9 października 2018 roku ENISA wraz zqq National Cyber Security Center (NCSC, Niderlandy) przedstawiła wytyczne dotyczące CVD – Coordinated Vulnerability Disclosure: The Guideline. Dokument jest efektem 5 lat współpracy pomiędzy przedsiębiorstwami i społecznością sektora ICT, instytucjami rządowymi, NCSC, a także z organami ścigania – niderlandzką policją oraz prokuraturą.



CVD – doświadczenia krajów europejskich. Podsumowanie sesji zamkniętej “Together- safer, stronger, smarter”

21 października 2021 r. odbyła się sesja zamknięta “Together – safer, stronger, smarter”. Wydarzenie zorganizował NASK Państwowy Instytut Badawczy w ramach SECURE, jednej z najstarszych konferencji dotyczących bezpieczeństwa teleinformatycznego w Polsce.

Już po raz czwarty przedstawiciele krajowych i międzynarodowych instytucji zajmujących się cyberbezpieczeństwem spotkali się, aby wymienić się wiedzą, wnioskami i dobrymi praktykami. W tym roku tematem sesji zamkniętej był proces CVD. Prezentacje o narodowych doświadczeniach przygotowali prelegencji z Belgii, Słowacji, Niderlandów i Niemiec. Dodatkowo w dyskusji wzięli udział eksperci z Rumunii, Czech oraz Polski.

Słowację reprezentowali przedstawiciele National Security Authority (NBU), którzy opowiedzieli o motywacji do stworzenia krajowej polityki w zakresie CVD, stanie obecnym, a także wyzwaniach na przyszłość. Do niedawna na Słowacji nie istniała krajowa polityka dotycząca skoordynowanego ujawniania podatności.

Dopiero w 2019 r. Narodowe Centrum Cyberbezpieczeństwa SK-CERT opracowało wytyczne dotyczące CVD. Dokument zawiera zalecenia dla osób zgłaszających podatności, organizacji, a także organów cyberbezpieczeństwa.

Ze strony Niderlandów w sesji uczestniczyli przedstawiciele Narodowego Centrum Cyberbezpieczeństwa (NCSC), którzy zaprezentowali poradnik: Coordinated Vulnerability Disclosure: The Guideline. Zawiera on wytyczne dla procesu CVD dla instytucji przyjmujących zgłoszenie i stron zgłaszających. Odnosi się również do roli NCSC, obszarów odpowiedzialności, a także komunikacji przed, w trakcie, a także po zakończeniu procesu ujawniania informacji. Dokument jest efektem 5 lat współpracy pomiędzy przedsiębiorstwami i społecznością sektora ICT, instytucjami rządowymi, NCSC, a także z organami ścigania – niderlandzką policją oraz prokuraturą.

Natomiast prezentacja przedstawicieli Federalnego Urząd Bezpieczeństwa Teleinformatycznego (BSI) z Niemiec dotyczyła bardziej specjalistycznych zagadnień, związanych z obsługą wykrytych w ramach CVD podatności po stronie klienta.

Eksperci poruszyli kwestię przekazywania komunikatów bezpieczeństwa użytkownikom końcowym, a także problematykę braku spójności w instrukcjach bezpieczeństwa pochodzących od różnych producentów. Zaprezentowali również standard CSAF 2.0, który ma wspomóc w automatyzacji procesu przekazywania informacji na temat bezpieczeństwa zarówno producentom, jak i klientom.

Belgijskie Centrum Cyberbezpieczeństwa (CCB) zaprezentowało krajowe podejście do procesu CVD. W Belgii skoordynowane ujawnianie podatności odbywa się na zasadzie umowy pomiędzy stronami. Istnieją również krajowe wytyczne, które są uwzględnione w belgijskiej strategii cyberbezpieczeństwa. CCB pracuje nad propozycją zmian prawnych, które mają zagwarantować bezpieczeństwo osobom zgłaszającym podatność.

SŁOWACJA
Krajowy Urząd ds. Bezpieczeństwa (NBU)

Proces skoordynowanego ujawniania podatności na zagrożenia.

Motywacja do stworzenia słowackiej polityki krajowej w zakresie CVD

Jako cała społeczność zajmująca się cyberbezpieczeństwem, stajemy w obliczu ogromnego wzrostu liczby podatności w oprogramowaniu, sprzęcie, jak również usługach i procesach. Wykorzystanie podatności będących jednym z powszechniejszych sposobów ataku, może prowadzić do uzyskania pełnego dostępu do zasobów organizacji, w tym do zgromadzonych w jej systemach i serwerach danych i informacji.

Do niedawna na Słowacji nie było jednolitej polityki krajowej w zakresie CVD. Brakowało opracowanych lub określonych zasad postępowania zarówno dla zgłaszających podatności, jak i organizacji. Uzupełnienie tej luki jest kluczowe dla procesu zarządzania podatnościami. Pozwoli na ich wykrywanie niezależnie od standardowych metod, takich jak przeprowadzanie testów penetracyjnych czy regularny monitoring.

Stan obecny

W 2019 roku Narodowe Centrum Cyberbezpieczeństwa SK-CERT opracowało dokument niebędący aktem normatywnym pt. “Wytyczne dotyczące zgłaszania podatności”. Dokument podzielony jest na następujące części:

- cel sporządzenia dokumentu,
- znaczenie CVD
- określenie definicji,
- określenie definicji CVE i CVSS,
- Sformułowanie zasad i wskazania zaleceń:
  - osób zgłaszających (etyczn hakerzy, badacze, zwykli ludzie),
  - organizacji
  - organów cyberbezpieczeństwa
- mapy procesu CVD

Celem dokumentu jest zapewnienie wsparcia dobrym hakerom, badaczom, jak również zwykłym obywatelom, którzy zgłaszają luki w zabezpieczeniach. Dokument wyjaśnia również znaczenie CVD oraz korzyści dla zgłaszających i organizacji wynikające z wdrożenia tego procesu.

Zasady dla zgłaszających określają jak i gdzie zgłaszać podatności oraz jakie działania są niezgodne z prawem. Podmiotom, których dotyczy zgłoszenie podatności, dokument wyjaśnia, co powinny były one wdrożyć i jaka jest właściwa reakcja na zgłoszenie. Organy cyberbezpieczeństwa mogą znaleźć w dokumencie rekomendacje, a także wskazania dotyczące opracowywania zasad i procesów CVD, a także sposobów ich koordynacji.

Wyzwania na przyszłość

W ciągu 2 lat mieliśmy do czynienia zarówno z dobrymi, jak i złymi praktykami w zakresie CVD. Przed nami wciąż wiele wyzwań w tym obszarze. Do przykładowych należy: wdrożenie rekomendacji dotyczących programów typu *bug bounty*, uwzględnienie doświadczeń z przypadków podatności zgłoszonych w ramach CVD i jednocześnie promowanie implementacji i rozwijanie samego procesu skoordynowanego ujawniania podatności.

NIDERLANDY
Narodowe Centrum Cyberbezpieczeństwa (NCSC)

Wytyczne dla procesu odpowiedzialnego ujawniania informacji.

Początek CVD w Niderlandach

Społeczeństwo w coraz większym stopniu ulega cyfryzacji, co stwarza wiele nowych możliwości. Jednocześnie luki lub podatności w systemach informatycznych stanowią potencjalne zagrożenie dla użytkowników, a ich wykorzystanie może powodować poważne skutki.

Na początku obecnej dekady doniesienia o podatnościach nie były dobrze widziane, a cyberprzestępcy chętnie wykorzystywali istniejące luki do ataków na organizacje publiczne i prywatne. Jednak z biegiem czasu podejście się zmieniło i wiele organizacji dostrzegło zalety posiadania wiedzy o podatnościach w swoich systemach.

Przedsiębiorstwa zaczęły publikować regulacje dotyczące sposobu zgłaszania podatności. NCSC przeprowadziło konsultacje, których wyniki opublikowano w 2013 r. w formie „Wytycznych dla procesu odpowiedzialnego ujawniania informacji". Firmy deklarowały, że są otwarte na otrzymywanie informacji o podatnościach na opracowanych przez nich warunkach.

Wypracowane mechanizmy dały możliwość zgłaszania podatności w sposób przejrzysty i bezpieczny dla zgłaszającego. Na spotkaniu wysokiego szczebla UE w sprawie bezpieczeństwa cybernetycznego w 2016 r. 29 organizacji potwierdziło znaczenie polityki radzenia sobie z podatnościami podpisując wspólny dokument.

Skoordynowane Ujawnianie Podatności: Wytyczne

W dniu 9 października 2018 roku ENISA wraz z NCSC przedstawiła wytyczne dotyczące CVD – Coordinated Vulnerability Disclosure: The Guideline. Dokument jest efektem 5 lat współpracy pomiędzy przedsiębiorstwami i społecznością sektora ICT, instytucjami rządowymi, NCSC, a także z organami ścigania – holenderską policją oraz prokuraturą.

Wytyczne zawierają informacje na temat:

- Celu skoordynowanego ujawniania podatności na zagrożenia
- Obszarów odpowiedzialności
- Wskazówek dla instytucji przyjmującej zgłoszenie i strony zgłaszającej
- Roli NCSC
- Komunikacji przed, w trakcie, a także po zakończeniu procesu ujawniania informacji.

W skład dokumentu wchodzą również przykłady ogłoszeń holenderskich firm zawierających zasady ujawniania podatności.

Wnioski z ostatnich lat

W ostatnich latach stało się jasne, że strony zgłaszające są gotowe do pracy zgodnie z warunkami regulacji CVD opracowanej przez NCSC. Sprawozdania są przekazywane bezpośrednio lub pośrednio organizacji przez strony zgłaszające. Praktyka odpowiedzialnego ujawniania informacji wykazała, że podmioty zgłaszające, które działają w dobrej wierze, i organizacje podatne na zagrożenia potrafiły współpracować, a tym samym podjąć kolejny krok w zwiększaniu bezpieczeństwa sieci i systemów informatycznych.

Niemcy
Federalny Urząd ds.Bezpieczeństwa Informacji (BSI)

Automatyzacja ostrzeżeń o podatnościach z wykorzystaniem frameworku CSAF, czyli jak wypełnić lukę między procesem CVD a właścicielami systemów?

Obsługa podatności po stronie klienta

Na koniec procesu CVD (Coordinated Vulnerability Disclosure), zazwyczaj wydawany jest komunikat bezpieczeństwa informujący klientów danego produktu i opinię publiczną o podatności i możliwych sposobach jej usunięcia. Jest to tak naprawdę początek procesu obsługi podatności po stronie właściciela podatnego systemu. Na tym etapie użytkownik końcowy powinien zastosować się do wydanego ostrzeżenia i wykonać zalecane działania (instalacja łatki, aktualizacja, czy inne środki zaradcze). Z uwagi na to, że każde środowisko jest inne, a instalacja aktualizacji czasem może mieć daleko idące konsekwencje, w pierwszej kolejności wskazana jest wcześniejsza ocena ryzyka. W celu dokonania takiej oceny, należy przeanalizować szczegóły podatności opisane w komunikacie.

Ciągłe wyszukiwanie komunikatów bezpieczeństwa dla wielu różnych produktów i ocenianie ich przydatności jest czasochłonne i wymaga wiele wysiłku. Wynika to z jednej strony z faktu, że producenci używają różnych kanałów dotarcia do swoich klientów i opinii publicznej, np.:

- poczta elektroniczna (często z opóźnieniem),
- ostrzeżenia na specjalnie dedykowanym kanale RSS (wymagana subskrypcja)
- strona internetowa (czasem z ograniczonym dostępem)

Z drugiej strony ostrzeżeń bezpieczeństwa jest coraz więcej, a sprawdzenie czy produkty, o których mowa w tych komunikatach, są używane w obszarze, za który odpowiedzialny jest klient, zwykle nie jest łatwe.

Brak spójności w formacie komunikatów

Kolejną problematyczną kwestią jest brak spójności w wydawanych ostrzeżeniach o podatności. Komunikaty, które pochodzą z różnych źródeł zazwyczaj znacznie się od siebie różnią pod względem formatowania, formatu plików, struktury i jakości informacji. Automatyczne przetwarzanie informacji w nich zawartych nie jest zatem możliwe lub jest możliwe jedynie w ograniczonym zakresie.

Z kolei oddelegowanie do tych zadań pracowników niepotrzebnie zajmuje czas wysoko wykwalifikowanym specjalistom. Ponadto ręczna obsługa takich ostrzeżeń nie jest skalowalna wraz ze wzrostem liczby podatności. W praktyce klienci często nie korzystają z komunikatów bezpieczeństwa w sposób ciągły i regularny, a w efekcie nie wdrażają ich na czas. Działają jedynie doraźnie, na przykład po nagłośnieniu sprawy przez media lub za radą krajowego CSIRT, takiego jak BSI.

Standard Common Security Advisory Framework (CSAF) 2.0

W celu zaadresowania tego problemu społeczność międzynarodowa opracowała wspólnymi siłami otwarty standard pod patronatem OASIS Open Foundation – Common Security Advisory Framework (CSAF) w wersji 2.0. Został on oparty na formacie JSON, co pomoże w automatyzacji procesu po obu stronach – zarówno wydawców ostrzeżeń, jak i ich odbiorców.

CSAF zastępując oparty na formacie XML Common Vulnerability Reporting Framework (CVRF) 1.2, określa również dostępność i miejsca dystrybucji komunikatów bezpieczeństwa. CSAF 2.0 definiuje wymagania dla narzędzi z niego korzystających. Autorzy mają nadzieję, że dzięki temu za kilka miesięcy każdy będzie mógł łatwo porównać i wybrać spośród różnych narzędzi dostępnych na rynku.

Z uwagi na to, że proces jest zautomatyzowany, można to narzędzie zastosować w całym łańcuchu dostaw oprogramowania i sprzętu. Informacje o podatnościach znacznie szybciej mogą być przekazywane w dół łańcucha dostaw. Co więcej, możliwe staje się również wyraźne stwierdzenie, że w danym produkcie nie występuje konkretna podatność poprzez użycie profilu VEX (Vulnerability Exploitability eXchange).

Taki mechanizm może pomóc zredukować liczbę fałszywie pozytywnych wyników ze skanerów bezpieczeństwa i co ważniejsze – wesprzeć infolinię poprzez aktywne informowanie klienta, że produkt nie jest podatny.

Członkowie Komitetu Technicznego OASIS rozpoczęli już wdrażanie swoich komunikatów bezpieczeństwa w formacie wymaganym przez CSAF, w tym między innymi Arista, Cisco, Red Hat, czy Siemens. BSI opublikowało już pierwsze narzędzie do tworzenia dokumentów CSAF (Secvisogram) w swoim repozytorium dostępnym na GitHubie. Kolejne narzędzia i wskazówki jak korzystać ze standardu będą pojawiać się w przyszłości.

Najnowsze informacje o standardzie i dostępnych narzędziach typu open source można znaleźć na stronie https://csaf.io. W razie jakichkolwiek pytań prosimy o kontakt z TC lub BSI pod adresem csaf@bsi.bund.de.

Belgia
Centrum Cyberbezpieczeństwa (CCB)

Belgijskie Centrum Cyberbezpieczeństwa (CCB) promuje przyjęcie skoordynowanego procesu ujawniania podatności (CVD) dla podmiotów prywatnych i publicznych m.in. poprzez opublikowanie wytycznych i przedstawienie przykładowej polityki postępowania. Wytyczne te, nie zmieniając istniejących ram legislacyjnych, wyjaśniają sytuację prawną osób zgłaszających podatność w przypadku przyjęcia przez organizację polityki CVD. Przypisują także CCB (jako krajowemu CSIRT) rolę domyślnego koordynatora CVD, nawet jeśli nie istnieje polityka CVD.

Podejście do procesu CVD w Belgii
W Belgii wdrożenie procesu CVD lub bug bounty jest uważane za rodzaj umowy akcesyjnej, którą publikuje się na stronie internetowej. Dokument zawiera postanowienia umowne między organizacją odpowiedzialną a zgłaszającymi (akceptowane przez nich, gdy dobrowolnie decydują się na udział na przedstawionych warunkach), z zastrzeżeniem przestrzegania wzajemnych zobowiązań opisanych w dokumencie CVD. Przyjęcie takiej polityki przez daną firmę oznacza wyrażenie zgody dla osób z zewnątrz na uzyskanie dostępu, lub podjęcia takiej próby, do systemów informatycznych w celu zidentyfikowania ewentualnych słabych punktów lub dostarczenia wszelkich istotnych informacji na temat ich bezpieczeństwa. W takim wypadku, dostęp lub próba dostępu do tych systemów informatycznych są zgodne z prawem, o ile spełnione są wcześniej określone zasady CVD.

Zasady te powinny zapewniać, między innymi, poufność wymienianych informacji oraz stanowić odpowiedzialne i skoordynowane ramy dla ujawniania wykrytych podatności. Termin "ujawnienie" nie musi oznaczać, że luka w zabezpieczeniach zostanie upubliczniona szerszej społeczności, ale raczej, że zgłaszający poinformuje o niej daną organizację.

Zgłaszający jest zobowiązany do przekazania informacji organizacji, której podatność dotyczy, ale publiczne jej ujawnienie (przez zgłaszającego lub daną organizację) jest opcjonalne i musi być wspólnie skoordynowane. Jeśli podatność nie jest jeszcze znana, a może mieć bezpośredni lub pośredni wpływ na inne organizacje, dana instytucja musi poinformować CCB i inne potencjalnie zainteresowane podmioty, nawet jeśli nie chce, aby podatność została podana do publicznej wiadomości.

Krajowe wytyczne dotyczące CVD są uwzględnione w krajowej strategii cyberbezpieczeństwa oraz w podstawowych wymogach bezpieczeństwa CCB dla sektora publicznego. CCB przyjęła, jako przykład dla innych organizacji, politykę CVD dla swojej strony internetowej.

Bezpieczeństwo osób zgłaszających podatności – propozycja legislacji

W kontekście wdrażania unijnej dyrektywy w sprawie ochrony osób zgłaszających naruszenia prawa Unii (potocznie zwanej dyrektywą o ochronie praw sygnalistów) CCB przedstawiła pewne propozycje zmian prawnych, których celem jest zagwarantowanie na określonych warunkach bezpieczeństwa osobom zgłaszającym podatności na zagrożenia, które w pewnych okolicznościach mogłyby pełnić rolę tzw. cyfrowych sygnalistów. Konkretne proponowane warunki, które musiałaby spełnić dana osoba, to:

- Działanie nie miało na celu oszukania ani wyrządzenia szkody;
- Poinformowanie organizacji odpowiedzialnej za system, proces lub kontrolę, nastąpiło tak szybko, jak to było możliwe, a najpóźniej w momencie zgłoszenia do krajowego CSIRT (CCB) informacji o odkryciu potencjalnej podatności;
- Osoba zgłaszająca jest w stanie udowodnić proporcjonalność swoich działań i metod badawczych w odniesieniu do celu, jakim jest poprawa bezpieczeństwa danego systemu, procesu lub kontroli;
- Nie doszło do ujawnienia informacji o odkrytej luce w zabezpieczeniach bez uprzedniej zgody krajowego CSIRT.

NASK

Cyber POLICY