POLSKIE TOWARZYSTWO INFORMATYCZNE

Zarząd Główny, ul. Solec 38 lok. 103, 00-394 Warszawa, tel.: + 48 22 838 47 05, tel./fax: + 48 22 636 89 87, e-mail: pti@pti.org.pl, www.pti.org.pl

W/353/ZG/16

Warszawa, 08.03.2016 r.

Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Szanowni Państwo

Polskie Towarzystwo Informatyczne w związku z zaopiniowaniem kolejnego programowego dokumentu Ministerstwa Cyfryzacji z satysfakcją ocenia fakt szerokich konsultacji takich materiałów.
W odniesieniu do dokumentu „Założenia strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej" stwierdzamy co następuje.

Założenia przedstawiają analizę stanu obecnego zgodną z naszymi obserwacjami, szczególnie w zakresie rozproszenia organizacyjnego jak i ułomności prawa. Proponowane w dalszych częściach dokumentu rozwiązania organizacyjne i legislacyjne likwidujące wyspowy charakter działań w zakresie cyberbezpieczeństwa zdecydowanie popieramy.

Po rozważeniu przytoczonych statystyk z roku 2014 opublikowanych przez firmę Symantec i obrazujących wagę problemów cyberbezpieczeństwa uważamy, iż znacznie korzystniejszym dla odbiorcy byłoby przedstawienie aktualnych statystyk dotyczących w większym zakresie naszego kraju, np. wykonanych przez CERT Polska.

Przy uwagach odnoszących się do powszechnej dostępności narzędzia umożliwiającego tworzenie oprogramowania złośliwego zabrakło nam krótkiego omówienia zjawiska „przestępstwo jako usługa" (*crime as a service*), które pozwala na zakup dedykowanego szkodliwego oprogramowania czy też usługi blokowania konkretnych usług sieciowych.
W opiniowanym dokumencie słusznie podkreślono znaczenie analizy ryzyka oraz zauważono brak spójności w ich szacowaniu. Pragniemy zwrócić uwagę, iż brak jest też publikacji odpowiednich statystyk incydentów, na podstawie których można by szacować ryzyko zagrożeń.

W głównych założeniach budowy systemu ochrony cyberprzestrzeni RP na str. 6, w punkcie 1 umieszczono warunek „wypracowanie konkretnych struktur organizacyjnych odpowiedzialnych za obsługę incydentów". Uważamy, że należałoby uzupełnić go o następujący fragment „w tym procedur ich zgłaszania". Zdarzało się, że zgłoszony incydent do CERT Polska nie wywołał żadnej reakcji, zaś procedura zgłaszania incydentu do Rządowego Zespołu Reagowania na Incydenty Komputerowe ze względu na niejasny formularz oraz konieczność szyfrowania skutecznie zniechęcała do jej stosowania.

Kategorię 1 z punktu 3 według nas należy uzupełnić o sektor odpowiedzialny za odpady i nieczystości.
Kategoria 3 jak i 5 wymaga naszym zdaniem doprecyzowania o jaki system teleinformatyczny, serwis czy usługę chodzi.
Za podstawą skutecznego zwalczania cyberataku przyjęto łańcuch wyszczególnionych na stronie 11 działań. Proponujemy zmianę ich kolejności, tak aby bezpośrednio po wykryciu ataku następowało przekazanie informacji o nim w systemie powiadamiania.

Za podstawą skutecznego zwalczania cyberataku przyjęto łańcuch wyszczególnionych na stronie 11 działań. Proponujemy zmianę ich kolejności, tak aby bezpośrednio po wykryciu ataku następowało przekazanie informacji o nim w systemie powiadamiania. Nawet jeśli informacja ta została już wcześniej wprowadzona, to kolejna będzie wskazywała na zakres i zasięg ataku. Rozwiązanie te wiąże się jednak z koniecznością budowy systemu o dużej wydajności i dostępności. Wyposażenie SOC lub LZR w kompetencje pozwalającą na izolowanie systemu lub jego części od cyberprzestrzeni w krytycznych przypadkach to pomysł wart uwagi.

W związku z tym uważamy, że końcowy dokument założeń powinien zawierać odniesienie do kwestii możliwości technicznych i wpływu obciążeniowego izolacji na infrastrukturę, np. jako stwierdzenie o konieczności przeprowadzenia dla infrastruktury o krytycznym znaczeniu dla państwa badania możliwości technicznej takiej izolacji oraz potencjalnego wpływu jaki wywarłaby taka izolacja na działanie tej infrastruktury.

W omawianym dokumencie wspomniano o problemach w ustalaniu progów wyzwolenia (uruchomienia) procedur i związanych z „ciemną liczbą" ataków. Pragniemy zwrócić uwagę, że równie wiele ataków pozostaje niezgłoszona choćby ze względu na chęć utrzymywania dzięki temu reputacji zaatakowanych organizacji. Należałoby naszym zdaniem rozważyć wprowadzenia dla jednostek administracji publicznej oraz innych organizacji istotnych dla cyberbezpieczeństwa państwa obowiązku prowadzenia jawnego rejestru incydentów cyberbezpieczeństwa, zawierającego na właściwym poziomie ogólności informacje m.in. o wykorzystanej podatności, jej przyczynach, skutkach i sposobach ich usunięcia oraz podjętych/zaplanowanych działaniach zapobiegawczych/naprawczych. Jest to konstrukcja zbieżna (poza jawnością) z wymaganiem p. A.16 *Zarządzanie incydentami związanymi z bezpieczeństwem informacji* załącznika do normy ISO 27001, wskazywanej jako referencyjna w założeniach. Konstrukcja taka według nas jest prosta do wdrożenia i może być wstępem do wdrożenia normy 27001 w całości, choć oczywiście wymóg jawności rejestru niewątpliwie byłby dla jednostek administracji jego cechą kłopotliwą. Jednocześnie byłby bodźcem do wyegzekwowania w administracji wymagań wskazanego dalej rozporządzenia RM z 12 kwietnia 2012 r., które generalnie nie jest respektowane.

Omawiając aspekty prawne i finansowe (podrozdział 3.5), wspomina się o procesie weryfikacji producentów i stosowanych rozwiązań w ramach sieci teleinformatycznych organów administracji państwowej. Uważamy, iż należy włączyć w proponowane rozwiązanie jednostki samorządowe, a nawet wszystkie organizacje infrastruktury krytycznej. Jest to zasadne, gdyż w tym samym kontekście, w podrozdziale 4.5 *Niezbędne zmiany kompetencyjne, organizacyjne i legislacyjne* na str. 31 mówi się już o certyfikacji produktów informatycznych (sprzętu lub oprogramowania) Podrozdział 4.1 *Proponowany podział kompetencji i struktury* określa wymóg wydzielenia w podmiotach realizujących zadania publiczne komórek organizacyjnych podległych bezpośrednio kierownikowi podmiotu, których zadaniem będzie organizacja i utrzymywanie systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami zawartymi w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Oznacza to m.in., co zresztą jest też podkreślane w innych miejscach założeń, wdrażanie wymagań norm ISO serii 27000. Podejście takie zdecydowanie popieramy pomimo tego, że respektowanie w administracji tego rozporządzenia jest znikome i jeszcze oczekuje na dobre zmiany. stosowanych w systemach podmiotów sfery publicznej i w zainteresowanych podmiotach prywatnych.

Prowadzone przez Polskie Towarzystwo Informatyczne badania dotyczące wdrożenia przytoczonego rozporządzenia w jednostkach samorządowych wykazały, iż tylko nieliczne z nich wdrożyły system zarządzania bezpieczeństwem informacji. Raport ze wspomnianych badań, obecnie w opracowaniu, zostanie przekazany do Ministerstwa Cyfryzacji w drugiej połowie marca 2016 roku.
Podrozdział 4.2 *Organizacja systemu wczesnego ostrzegania i reagowania* wspomina o dedykowanej stronie internetowej, zawierającej informacje o zagrożeniach, która powinna być dostępna również dla wszystkich użytkowników cyberprzestrzeni. Popierając takie oczywiste rozwiązanie podkreślamy konieczność zapewnienia zrozumiałości formy przekazu tych informacji, gdyż np. obecnie dostępne statystyki systemu ARAKIS są dla przeciętnego internauty mało czytelne.
W odniesieniu do przewidzianych przez założenia tworzenia komórek Lokalny Zespół Reagowania stwierdzamy, iż niejasne jest kto będzie je powoływał, więc należy to doprecyzować. Ze swej strony nie widzimy możliwości aby w najbliższej przyszłości organizacje samorządowe poniżej szczebla powiatu były w stanie podołać temu zadaniu.

35 lat PTI
POLSKIE TOWARZYSTWO INFORMATYCZNE

Według naszej opinii w systemie ochrony cyberprzestrzeni nie przewidziano jakiejkolwiek roli zwykłych obywatele, w tym hakerów (rozumianych jako pasjonatów komputerowych), którzy często znacznie szybciej doświadczają lub wykrywają nieprawidłowości związane z atakiem na instytucje publiczne. Z tego względu powinien być utworzony obywatelski centralny punkt zgłaszania odkrytych podatności. W zakończeniu naszej opinii zwracamy uwagę na wartą podkreślenia troskę o polską terminologię w dokumencie państwowym i maksymalnie szerokie stosowanie w opiniowanym dokumencie założeń polskich określeń zamiast literalnych angielskich, co spełnia też pozytywną dla języka ojczystego rolę słowotwórczości normatywnej. Oczywiście zdajemy sobie sprawę z trudnością takiego podejścia, zwłaszcza dla określeń najnowszych, więc tym bardziej jest to godne poparcia. Dlatego też proponujemy, aby odważniej porzucać określenia połowicznie polskie, czyli „mail" i stosować określenia „mejl", jak też używać określenia „program złośliwy" zamiast „malware" i „użytkownikoprzyjazny" zamiast „userfriendly".

Opracowanie: dr inż. Przemysław Jatkiewicz, mgr Janusz Żmudziński; uzupełnienia i redakcja dr inż. Janusz Dorożyński

Opinia w wersji dostępnej do kopiowania znajduje się na platformie opiniowania PTI WSTOIn pod adresem https://wstoin.pti.org.pl/wiki/16-02.01#Opinia

Z poważaniem

WICEPREZES
Polskiego Towarzystwa Informatycznego
Janusz Dorożyński