3.1. Podział kompetencji i struktura systemu

Utworzenie trzypoziomowej struktury systemu cyberbezpieczeństwa, gdzie odpowiednie instytucje, komórki organizacyjne czy zespoły odpowiadałyby za bezpieczeństwo cyberprzestrzeni w warstwie strategicznej, operacyjnej i technicznej.

Poziom operacyjny - Instytucje odpowiedzialne za przekazywanie informacji o incydentach transsektorowych oraz agregowanie i analizę informacji o tego typu incydentach

Odpowiedzialność powinna zostać rozszerzona o opracowanie technicznych standardów, tak aby uniemożliwić dowolności w interpretacji (dokumentacja how to). Standard ten pozwoli na łatwe ocenienie konfiguracji/funkcjonowania zabezpieczeń oraz wypełnianie zadań pionu technicznego. Do zadań pionu operacyjnego powinna również należeć kontrola pracy pionu technicznego.

Poziom techniczny: Instytucje odpowiedzialne za bezpośrednie reagowanie na incydentyw poszczególnych instytucjach (zarówno państwowych, jak i prywatnych)

Odpowiedzialność powinna zostać rozszerzona również na wsparcie techniczne (a nawet pomoc konfiguracji/wdrożeniu), kontrolę zabezpieczeń i doradztwo w zakresie bezpieczeństwa. Nie da się reagować na incydenty (first responder) lub przeprowadzać analizy powłamaniowej (forensic) bez znajomości systemu. Doprowadzi to chaosu w procesie podejmowania decyzji.

Poziom techniczny musi mieć realny wpływ na funkcjonowanie systemu tj. Musi istnieć mechanizm wymuszający zastosowanie się do zaleceń.

3.2.3. Ostrzeganie i informowanie

Drugim komponentem systemu ostrzegania i informowania powinien być system monitorowania ruchu w punktach wymiany ruchu internetowego (*Internet Exchange Point* – IXP -Rysunek. 3) Przy czym pod pojęciem IXP należy rozumieć zarówno punkt wymiany pomiędzy operatorami krajowymi jak i punkty wymiany z operatorami zagranicznym

Kolejną trudnością związaną z realizacją monitorowania ruchu sieciowego w punktach wymiany jest wolumen wymienianego ruchu. Monitorowanie nie może prowadzić do obniżenia przepustowości punktu wymiany, a zatem wymagać to będzie zastosowania urządzeń o bardzo dużej mocy obliczeniowej.

Zadanie wydaje się być nieosiągalne oraz może budzić obawy o utratę anonimowości w sieci. W tym przypadku należałoby rozpocząć monitorowanie ruchu tylko do/z chronionych systemów (systemy krytyczne oraz w miarę możliwości reprezentatywny przypadek systemów o niższym priorytecie). Dobrym pomysłem jest również centralizacja usług oraz utworzenie sieci typu honeypot, która będzie zachęcać do wykonywania ataków co umożliwi identyfikacje sprawcy i jego wczesną blokadę.

Podobne rozwiązanie udało się zastosować w Czechach.

CERT/CSIRT narodowy powinien posiadać możliwość umieszczania własnych sond w IXP lub korzystania z narzędzi stosowanych przez operatora.

Rozwiązanie budzi obawy o anonimowość. Sytuacja jest analogiczna do tej, jaka wystąpiła w Stanach Zjednoczonych.

3.3. Procedury, progi reakcji, kanały wymiany informacji

Z uwagi na konieczność reakcji w czasie rzeczywistym, reakcje takie muszą następować według z góry ustalonych scenariuszy ujętych w stosowne procedury. Należy dążyć do tego, aby procedury reakcji zostały ustandaryzowane we wszystkich podmiotach danego poziomu hierarchii reagowania.

W tym miejscu należy nadmienić, że pion techniczny musi mieć możliwość rekonfiguracji urządzeń należących do podmiotu chronionego (musi istnieć współodpowiedzialność). Reakcja, nie może opierać się o ludzi, którzy mają inne obowiązki (tj. spotkania, delegacje) lub nie posiadają kompetencji. W wielu przypadkach administratorzy nie reagują na informacje z SOC, mając nadzieje, że nic nie będą musieli robić, a sprawa ucichnie.

Nie może odbywać się to w taki sposób jak obecnie: CERT rozsyła zalecenia, ale nie ma mocy prawnej aby wymusić ich zastosowanie. Dobrym przykładem jest strona: https://poczta.cba.gov.pl. Wg. zaleceń dostęp do zasobów firmowych powinien odbywać się poprzez połączenie VPN.

W ustalaniu progów wyzwolenia mogą pojawić się trudności związane z „ciemną liczbą” ataków. Dotyczy to w szczególności ataków na komputery osobiste i urządzenia mobilne pojedynczych obywateli lub podmiotów sektora MŚP.

Proszę zwrócić uwagę, że aktywna ochrona nie może obejmować firm czy też prywatnych komputerów. Wiele osób/firm prowadzi własne badania bezpieczeństwa lub uczestniczy w programach bug bunty.

3.4. Rola organizatora systemu

W dłuższym okresie, w oparciu o organizatora systemu i CSIRT-krajowy, uznane w kraju ośrodki badawcze oraz we współpracy z producentami urządzeń i systemów teleinformatycznych, zostanie powołane **Narodowe Centrum Cyberbezpieczeństwa**, które będzie gromadzić dane o zagrożeniach i podatnościach z zakresu bezpieczeństwa teleinformatycznego. Charakter Centrum ma umożliwić pogłębioną analizę niektórych zjawisk (np. do analizy złośliwego kodu), co jednocześnie zracjonalizuje sposób działania zespołów ds. bezpieczeństwa.

Podany przykład analizy kody wydaje się być niewłaściwy. Łatwiej przesłać złośliwy kod do firmy, która tym się specjalizuje, niż utrzymywać osobny zespół. Wiele firm (np. producentów oprogramowania antywirusowego) prowadzi takie badanie. Problem będzie stanowić również utrzymanie kadry. Proponuje tutaj zainwestować w automatyczne oprogramowanie analizujące złośliwe oprogramowanie i udostępnić go wszystkich zainteresowanym.

Podobnie nieopłacalne jest utrzymywanie specjalistów, którzy będą wyszukiwać nieznane dotąd podatności. Lepiej uruchomić program bug bunty. Również w tym przypadku nie uda się znaleźć specjalistów.

3.5. Aspekty prawne i finansowe

Projekt zawiera zobowiązania wobec operatorów kluczowych usług, którzy będą dokonywać oceny zagrożeń cybernetycznych, na jakie są narażeni, oraz do przyjęcia odpowiednich i proporcjonalnych środków mających na celu zapewnienie bezpieczeństwa sieci i informacji. Podmioty te będą zobowiązane do zgłaszania wszelkich incydentów poważnie zagrażających ich sieciom i systemom informatycznym oraz mogących znacząco zakłócić ciągłość działania kluczowych usług.

Zgłaszanie incydentów przez podmioty jest nierealne. Bez należytej kontroli większość problemów zostanie ukryta lub niezauważona ze względu na brak kompetencji pracowników podmiotu.

Ocena zagrożeń musi być dokonana przez pracowników programu oraz maksymalne zautomatyzowanie procesu. Raportowanie musi to się odbywać w pełni automatyczny.

Spójność ze sferą bezpieczeństwa narodowego zostanie również zachowana poprzez uregulowanie np. w ustawie o zamówieniach publicznych i ustawie o Agencji Bezpieczeństwa Wewnętrznego **procesu weryfikacji producentów** i stosowanych rozwiązań w ramach sieci teleinformatycznych organów administracji państwowej oraz świadczonych usług, m.in. w zakresie: zapór sieciowych (firewall), oprogramowania antywirusowego, antyszpiegowskiego, rozwiązań uwierzytelniających, filtrujących, archiwizujących, szyfrujących, rozwiązań monitorujących i wykrywających włamania.

Porównanie konkurencyjnych produktów i wyłonienie kilku (lub jednego) spowoduje protesty producentów, którzy nie zostali wybrani. Na jakiej podstawie te produkty zostaną wybrane? Podmioty zobligowane do zakupu wybranego sprzętu będą musiały przeszkolić odpowiedzialnych pracowników, a proces zdobywania doświadczenia na nowym sprzęcie zajmie dużo czasu.

Najważniejszym czynnikiem jest możliwość integracji z systemem raportowania oraz z systemem automatycznej rekonfiguracji urządzenia/oprogramowania.

Podmiot powinien mieć możliwość wyboru rozwiązania, a pion techniczny powinien zapewnić wymagane wsparcie (jak również dobór odpowiedniego rozwiązania dla konkretnego podmiotu).

Do wypracowania pozostanie nałożenie wymagań regulacyjnych i kontrolnych na dostawców rozwiązań systemów sterowania przemysłowego (OT – ang. *Operational Technology*) i systemów informatycznych (IT – ang. *Information Technology*) dla operatorów kluczowych usług.

Nałożenie wymagań na dostawców rozwiązań systemów jest niemożliwe. Dostawca może nie być zainteresowany wprowadzeniem usprawnień (jako zbyt kosztowne lub bezcelowe). W ostateczności dostawca przestanie świadczyć usługę.

Jedyną możliwością są zachęty finansowe: wprowadzenie poprawek w zamian za zwiększone zakupy.

Tworzenie wymagań krajowych będących kopią wymagań ogólnoprzyjętych jest niepotrzebne. Wprowadzenie jakiekolwiek nowych wymagań nieujętych w wymaganiach światowych niczego nie zmienią. Zostaną one po prostu zignorowane przez globalnych dostawców.

Operatorzy kluczowych usług, o ile nie są już objęci przepisami dotyczącymi sektora publicznego, będą zobowiązani do przyjmowania minimalnych wymagań z zakresu bezpieczeństwa teleinformatycznego, co będzie wiązało się poniesieniem dodatkowych kosztów, np. na wdrożenie standardów bezpieczeństwa teleinformatycznego.

Wymagania z zakresu bezpieczeństwa muszą być jednoznacznie sprecyzowane. W przeciwnym wypadku będą interpretowane na korzyść podmiotu. Np. zapis, że podmiot musi być wyposażonych w system ochrony przed włamaniami nie oznacza, że też ten system musi być poprawnie skonfigurowany. System jest, ale z powodu problemów, których pracownicy podmiotu nie są w stanie rozwiązać, połowa jego funkcji została wyłączona.

Niezależnie od powyższych struktur wykonawczych na poziomie technicznym, w podmiotach realizujących zadania publiczne, muszą zostać wydzielone komórki organizacyjne, podległe 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*

Takie zadania powinny świadczyć piony techniczne. Podmioty mogą ukrywać informację o incydentach. Osoby przydzielone do zadań ze strony podmiotu mogą nie posiadać niezbędnej wiedzy, przez co rozporządzenie nie będzie wykonywane w myśl autora.

Ze strony podmiotu powinna zostać przydzielona odpowiedzialna za wyjaśnianie struktury systemu teleinformatycznego.

4.2. Organizacja systemu wczesnego ostrzegania i reagowania

CERT/CSIRT narodowy musi posiadać możliwość zbierania informacji o anomaliach w ruchu sieciowym odbywającym się zarówno w wymianie międzynarodowej, jak i w wymianie pomiędzy operatorami krajowymi, których usługi zaliczone zostaną do tzw. usług kluczowych.

Sformułowanie anomalia nie jest precyzyjne. Może odnosić się ono do ruchu, który zostaje sklasyfikowany jako atak (np. przez IPS) oraz do odchyleń od standardowego zachowania systemu.

Na styku operatorskim wychwycenie odchyleń od standardowego zachowania systemu będzie niemożliwe.

Może również dochodzić do utraty informacji, ze względu na wysokie obciążenie punktu wymiany.

4.5. Niezbędne zmiany kompetencyjne, organizacyjne i legislacyjne

Dodatkowo w NASK,jako instytucie badawczym mogłoby powstać akredytowane laboratorium dokonujące oceny lub certyfikacji produktów informatycznych (sprzętu lub oprogramowania) stosowanych w systemach podmiotów sfery publicznej i w zainteresowanych podmiotach prywatnych.

W przypadku zastosowania komercyjnych produktów informatycznych dodatkowa certyfikacja nie ma sensu. Część produktów jest certyfikowanych przez niezależne organizacje. Co się stanie jeżeli produkt, który już jest wykorzystywany nie uzyska certyfikatu krajowego? Zostanie wycofany? Kto poniesie koszt wycofania? Jak zmusić producenta aby poprawił swój produkt?

Planuje się również ustanowienie programu motywacyjnego dla specjalistów z obszaru cyberbezpieczeństwa pod roboczą nazwą „Złota Setka”; celem programu będzie zapewnienie stosownych dodatków motywacyjnych dla specjalistów spełniających najwyższe kryteria fachowości potwierdzone stosownymi certyfikatami. Ocenia się że ok. 100 specjalistów z różnych dziedzin informatyki będących w zasobach państwowych struktur (resortów)zaliczonych do programu „Złota Setka” może mieć istotny wpływ na zapewnienie wymaganego poziomu bezpieczeństwa teleinformatycznego sektora rządowego i skutecznie wspierać ważne sektory pozarządowe.

Co oznacza sformułowanie stosowne certyfikaty? Kto decyduje, który certyfikat jest stosowny, a który nie.

Ze względu na wysokie koszty uzyskania certyfikatu promowane będą osoby, które mają wyższe zarobki oraz osoby zatrudnione w instytucjach, które mają większy budżet na informatykę/szkolenia. I w końcu, kto zdecyduje o wysłaniu pracownika na szkolenie.

Szkolenia powinny być prowadzone w ramach programu przez pion techniczny. Zapewni to równomierny transfer wiedzy do wszystkich pracowników oraz uniemożliwi dowolność w wyborze szkoleń.

Dodatki motywacyjne powinny być wypłacane za zaangażowanie w programie. Np. stworzenie standardu, dobrych praktyk, wykrycie zagrożenia itp.

Podsumowanie

Piony techniczny oraz operacyjny powinny działać jak usługodawca (tj. zapewniać kompleksowe bezpieczeństwo), a nie jako podmiot stawiający wymagania oraz monitorujący.

Należy skupić niewielką grupę najlepszych specjalistów w kilku punktach (pionach technicznych i operacyjnym), które wezmą na siebie odpowiedzialność za bezpieczeństwo systemów. Specjaliści ci będą monitorować, pomagać w konfiguracji, w pełni administrować wybrane systemy oraz szkolić działy bezpieczeństwa podmiotów.

Rozproszenie wielu specjalistów w chronionych podmiotach i oparcie na nich bezpieczeństwa jest błędem. Przede wszystkim rynek nie jest w stanie zapewnić tylu specjalistów, co spowoduje braki kadrowe lub zatrudnianie osób nieposiadających wymaganych kompetencji. W tym momencie zagraniczne korporacje mają problem z obsadzeniem stanowisk.

W przypadku mniejszych podmiotów, które ze względu na stan finansowy, nie mogą pozwolić sobie na zakup oprogramowania lub sprzętu, pion techniczny powinien zapewnić dostęp do własnych systemów bezpieczeństwa w ramach usług wspólnych.

Proszę wziąć pod uwagę fakt, iż działy informatyczne mają za zadanie utrzymać pracę systemu. Bezpieczeństwo posiada bardzo niski priorytet. W tym momencie pracownicy IT są przeładowani obowiązkami, i nie są w stanie wykonywać zadań związanych z bezpieczeństwem. Dołożenie dodatkowych obowiązków spowoduje, że sprzęt będzie źle skonfigurowany (niezgodnie z zaleceniami producenta czy też najlepszymi praktykami). Działa, jest dobrze. Źle skonfigurowane urządzenia (być może celowo) nie będą raportować do pionu operacyjnego, a incydenty nie będą zgłaszane. Wszystko to w celu uniknięcia dodatkowych obowiązków.

Znane są mi również przypadki, kiedy przełożony wymusza nie dziale technicznym wyłączenie zabezpieczeń.

Podmioty chronione należy traktować z dużym dystansem, bo z ich punktu widzenia niewiedza jest błogosławieństwem, a „no logs = no problem”