FUNDACJA bezpieczna cyberprzestrzeń

ROZWÓJ CSIRT A OBSZAR DZIAŁAŃ INFO OPS

7.12.2017

Idea tworzenia i działania zespołów typu CSIRT/CERT w przyszłym roku będzie odchodzić 30 rocznicę. Krótko po tym jak 2 listopada 1988 roku Morris Worm „zainfekował cały internet" na Carnegie Mellon University w Pittsburghu powołano CERT Coordination Center. Od tego czasu takich zespołów powstało setki. Największa organizacja zrzeszająca je – FIRST liczy blisko 400 członków.

Zakres działania CSIRT-ów przez te wszystkie lata mocno się zmienił. Powstały nowe zagrożenia, nowe techniki ataków, które wymusiły zmiany po stronie reagujących na incydenty. W tym kontekście ciekawym przykładem staje się obszar INFOOPS, czyli operacji informacyjnych. Jest on z pewnością nowym obszarem dla specjalistów technicznych od cyberbezpieczeństwa. Jednocześnie trudno zaprzeczyć oczywistym faktom, że „tradycyjne" ataki w cyberprzestrzeni (CYBEROPS) coraz częściej są zsynchronizowane z operacjami informacyjnymi, tworząc de facto jedną wspólną operację.

Na chwilę obecną trudno jednoznacznie stwierdzić na ile specjaliści CSIRT zaangażują się bezpośrednio w zarządzanie incydentami powiązanymi z operacjami informacyjnymi. Jest jednak bardzo prawdopodobne, że proces taki będzie musiał nastąpić i skończy się on co najmniej wypracowaniem ścisłych zasad współpracy pomiędzy specjalistami z obydwu obszarów – CYBEROPS i INFOOPS.

W Fundacji Bezpieczna Cyberprzestrzeń od dawna zauważamy konieczność tej współpracy. Uruchomiliśmy specjalny projekt temu poświęcony – INFOOPS. Kolejnym, bardzo praktycznym przykładem naszego zaangażowania było zorganizowanie dedykowanych ćwiczeń z tego zakresu, właśnie dla specjalistów CSIRT. Ćwiczenia odbyły się 23 listopada w Kiszyniowie. Zostały zorganizowane we współpracy z ITU (International Telecommunication Union) i były częścią "ITU Joint Alert Cyber Drill for Europe and CIS (Common Independent States)"

> NA ILE SPECJALIŚCI CSIRT ZAANGAŻUJĄ SIĘ W ZARZĄDZANIE INCYDENTAMI POWIĄZANYMI Z OPERACJAMI INFORMACYJNYMI? BARDZO PRAWDOPODOBNE, ŻE TO NASTĄPI I SKOŃCZY SIĘ WYPRACOWANIEM ŚCISŁYCH ZASAD WSPÓŁPRACY POMIĘDZY SPECJALISTAMI Z OBYDWU OBSZARÓW – CYBEROPS I INFOOPS.

ĆWICZENIA – SCENARIUSZ, ZAŁOŻENIA I PRZEBIEG

Podstawowym celem ćwiczenia było sprawdzenie na ile tradycyjne zespoły CERT-owe rozumieją naturę operacji informacyjnych i na ile, jako zespoły mające w swoim składzie technicznych specjalistów od reagowania na incydenty, są w stanie wspomóc analityków INFOOPS w ich analizach, które to mają bardziej charakter analizy treści niż analizy technicznej.

W ramach ćwiczenia zdecydowano się na nowatorskie rozwiązanie polegające na przeprowadzeniu treningu operacji informacyjnych (INFOOPS) będących odpowiedzią na towarzyszące zwykle atakowi technicznemu działania adwersarza w środowisku informacyjnym. Ćwiczona operacja informacyjna miała na celu eskalację negatywnych emocji w społeczności powiązanej z atakowanym podmiotem (np.: klientów banku, czy nawet obywateli danego państwa), poprzez aktywne wpływanie na środowisko informacyjne, w szczególności media społecznościowe. Ćwiczenie zwróciło uwagę na rolę tego typu operacji, które w istocie są integralną częścią większości zaawansowanych operacji CYBEROPS. W ramach ćwiczenia zwrócono szczególną uwagę na możliwości kształtowania negatywnych postaw wśród odbiorców informacji, dezawuację systemu bankowości krajowej, dezawuację państwa poprzez wykazywanie jego niezdolności do zagwarantowania bezpieczeństwa systemom bankowym, a w konsekwencji obywatelom.

W ramach ćwiczenia zwrócono szczególną uwagę na korelacje czasowe pomiędzy operacjami INFOOPS i CYBEROPS. W tym celu wytworzono w mediach społecznościowym trzy wektory narracji, z czego dwa były pozornie przeciwstawne. Pozwoliło to zobrazować typowy sposób wpływania na środowisko informacyjne (INFOOPS), w czasie poprzedzającym atak techniczny (CYBEROPS) na system bankowy. Taki sposób wpływania na środowisko informacyjne ułatwia jego skryte kształtowanie, tak aby stanowiło tło pod właściwe operacje informacyjne (atak informacyjny) z potencjałem uzyskania supremacji informacyjnej po ataku technicznym.

Zadaniem zespołów obsługujących incydent było zidentyfikowanie operacji informacyjnej i jej celu, obiektów będących narzędziami oddziaływania przeciwnika oraz podjęcie przeciwdziałania zgodnego z uwarunkowaniami prawnymi, tak aby uniemożliwić przeciwnikowi osiągniecie zakładanego przez niego celu. Zespoły miały do dyspozycji wskazane narzędzia analizy sieci społecznościowych. Służyły one do identyfikacji samej operacji informacyjnej, identyfikacji podmiotów (kont w serwisie Twitter) uczestniczących w dystrybucji informacji powiązanej z tą operacją i przede wszystkim poprawnej identyfikacji tych z kont, które były za nią odpowiedzialne za intencjonalne prowadzenie operacji, w odróżnieniu od tych, które uczestniczyły w tej operacji w sposób nieświadomy. Przede wszystkim jednak uczestnicy mieli podjąć próbę skutecznego powstrzymania prowadzonej operacji informacyjnej.

Scenariusz zakładał, że specjaliści z CSIRT otrzymują prośbę o wsparcie od analityków INFOOPS. Mieli oni dostarczyć argumentów natury technicznej, które pozwolą szybciej zidentyfikować operację, ustalić źródła za nią odpowiedzialne i pomóc ostatecznie ją zneutralizować.

Szczegółowy zakres tych zadań stanowią poniższe punkty, które jednocześnie można potraktować jako dobry zestaw zakresu szkolenia:

a. Identyfikacja słów kluczowych wykorzystywanych w czasie operacji
b. Identyfikacja komunikacji pomiędzy uczestnikami operacji
c. Identyfikacja uczestników „alpha", czyli inicjatorów operacji
d. Identyfikacja profili behawioralnych uczestników operacji
e. Identyfikacja profili zautomatyzowanych (botów)
f. Przeprowadzenie działań zmierzających do skutecznej blokady uczestników operacji o statusie „alpha"

Dodatkowymi zadaniami, które wkraczały w obszar działań specjalistów od INFO OPS były:

a. Analiza treści komunikatów generowanych w czasie operacji, w celu identyfikacji motywów i szczegółowych celów działania
b. Zaplanowanie własnej kampanii informacyjnej, neutralizującej negatywne skutki operacji informacyjnej
c. Przeprowadzenie kampanii informacyjnej zbieżnej z planem komunikacji

Ćwiczenia przeprowadzane były z dwóch miejsc. Na miejscu, w Kiszyniowie, jeden członek zespołu zarządzającego ćwiczeniami przedstawiał ich założenia i koordynował przebieg. Podstawowa praca operacyjna, tj. działania symulujące prowadzoną operację informacyjną, przeprowadzane były przez trzyosobową grupę specjalistów w Warszawie. Całość poprzedzona była tygodniową aktywnością w sieci, również z wykorzystaniem botów, dzięki której pojawił się w internecie zestaw informacji stanowiących operację poddaną analizie przez uczestników ćwiczeń.

PODSUMOWANIE ĆWICZEŃ

Ćwiczenia przeprowadzone w Mołdawii miały charakter pilotażowy. Przede wszystkim miały ograniczony czas trwania: dwie godziny wspólnej pracy, poprzedzone tygodniowym przygotowaniem zespołu i krótkim okresem zaznajomienia się z narzędziami przez uczestników ćwiczeń. W praktyce przebieg ćwiczeń w dużej mierze był instruktażem postępowania. Poszczególne, najważniejsze zadania, kończyły się demonstracją poprawnego działania. Taki pilot nie pozwala na jednoznaczną, rzetelną ocenę na ile specjaliści CSIRT, sprawnie poruszający się w obszarze reagowania na CYBEROPS, są przygotowani do realnego wsparcia analityków INFOOPS. Szacunek dotyczący rozwiązania zadań wskazuje na skuteczność na poziomie 20-30%. To oczywiście mało. Dlatego nie ma wątpliwości, że dalsza praca nad rozwijaniem tych umiejętności jest konieczna, tym bardziej, że nikt nie kwestionował sensu włączania się specjalistów CSIRT do prac związanych z INFOOPS. Pilot pozwolił również nam na wyklarowanie wizji docelowego, pełnego ćwiczenia, które planujemy w przeszłości przeprowadzić. Niewykluczone, że we współpracy z ITU, którego przedstawiciele bardzo pozytywnie ocenili wprowadzenie nowego obszaru ćwiczeniowego do koncepcji „ITU Joint Alert Cyber Drill" i już zaprosili Fundację do dalszej współpracy.

Autorzy:
Mirosław Maj – Prezes Fundacji Bezpieczna Cyberprzestrzeń
Rafał Kasprzyk – Wojskowa Akademia Techniczna
Kamil Basaj – Kierownik projektu INFOOPS Fundacji Bezpieczna Cyberprzestrzeń.

Śledź nas na:
TT: @cybsecurity_org
Facebook: **@FundacjaBezpiecznaCyberprzestrzen**