FUNDACJA
bezpieczna
cyberprzestrzeń

# FUNDACJA BEZPIECZNA CYBERPRZESTRZEŃ
# KATALOG USŁUG IERTowych

**IERT – Infoops Emergency Response Team**
(zespół reagowania na incydenty w środowisku informacyjnym):

Ochrona środowiska informacyjnego jest realizowana poprzez wykonanie usług z obszarów: rozpoznania, analizy i planowania oraz działań aktywnych w środowisku informacyjnym.

**www.cybsecurity.org**

Fundacja Bezpieczna Cyberprzestrzeń pod koniec 2016 uruchomiła projekt badań nad zjawiskiem manipulowania polskim środowiskiem informacyjnym przez obce ośrodki propagandowe. Projekt koncentruje się na identyfikacji i przeciwdziałaniu zjawiskom dezinformacji oraz kampanii propagandowych w polskiej przestrzeni informacyjnej. Cele te realizowane są przez rozpoznanie operacji informacyjnych, psychologicznych w korelacji z cyberatakami. Projekt obejmuje badanie nad zjawiskiem propagandy, dezinformacji, manipulacji środowiskiem informacyjnym, w tym środowiskiem poznawczym.

- Rozpoznanie i analiza polskiej przestrzeni informacyjnej
- Działalność publicystyczna
- Publikowanie ostrzeżeń o zidentyfikowanych incydentach w środowisku informacyjny
- Rozwój technicznych narzędzi wsparcia działań IERT
- Prowadzenie ćwiczeń i szkoleń

Kontakt:
ul. Solec 22, 00-410 Warszawa,
tel: +48 22 112 0 800,
e-mail: kontakt@cybsecurity.org

FUNDACJA bezpieczna cyberprzestrzeń

# Usługi JAKOŚCIOWE

**Analiza ryzyka** IERT wykonujący tę usługę przeprowadza lub asystuje w analizach ryzyka dotyczących bezpieczeństwa środowiska informacyjnego. Ocenia zagrożenia dla środowiska jak również ryzyk dla skutków i efektów realizacji procesu IERT i incydentów.

**Doradztwo w zakresie bezpieczeństwa** Usługa polega na wykorzystaniu IERTu do udzielania porad, wskazówek, najlepszych praktyk bezpieczeństwa do wdrożenia w "constituency". IERT w tej usłudze zaangażowany jest w przygotowanie rekomendacji, udzielanie wskazówek i pomocy w opracowywaniu polityki bezpieczeństwa i dostosowania procesu IERT na potrzeby organizacji.

**Edukacja i szkolenia** Usługa ta polega na dostarczaniu "constituency" informacji o bezpieczeństwie środowiska informacyjnego poprzez seminaria, warsztaty, kursy i tutoriale. Tematy mogą obejmować wytyczne do raportowania incydentów, odpowiednie metody reagowania, narzędzia do reagowania na incydenty, metody zapobiegania incydentom oraz inne. IERT przygotowuje rekomendacje dla szkoleń i dystrybuuje informacje o nich. IERT ustala plan szkoleniowy w porozumieniu z Klientem.

**Działania uświadamiające** Usługa polega na stałym poszukiwaniu możliwości zwiększenia świadomości bezpieczeństwa „constituency" przez opracowywanie artykułów, plakatów, biuletynów, stron www lub innych materiałów przekazujących najlepsze praktyki i zalecenia. Usługa polega również na planowaniu cyklicznych spotkań i seminariów w celu informowania „constituency" o aktualnych procedurach i trendach w bezpieczeństwie środowiska informacyjnego.

**Planowanie działań zapewniających ciągłość działań i odtworzeniowych**
IERTy z zaadresowaną usługą są zaangażowane w system zarządzania ciągłością działania i przygotowanie planu działań niwelujących skutki i efekty incydentów w środowisku informacyjnym, jak również scenariusze potencjalnego zakłócenia ciągłości działania.

**SŁOWNIK POJĘĆ:**

- IERT – Information Environment Emergency Response Team
- Obiekt informacyjny: utrwalona, niezależnie od formy, informacja występująca w środowisku informacyjnym w wymiarze wirtualnym lub fizycznym.
- Obiekt oddziaływania: uczestnik środowiska informacyjnego do którego jest skierowane oddziaływanie informacyjne
- Obszar informacyjny: fragment środowiska informacyjnego.
- Oddziaływanie informacyjne: wszelka aktywność w środowisku informacyjnym kierowana do określonej grupy odbiorców. Aktywność ta może być realizowana w następujących wymiarach: wirtualnym, fizycznym i poznawczym.
- Obsługa incydentu informacyjnego: działania IERT polegające na analizowaniu środowiska informacyjnego, planowaniu, oddziaływaniu i ocenie tych działań, w celu uzyskania wpływu na środowisko informacyjne.
- Kontrola / Sterowanie informacyjne: stan, w którym IERT uzyskał kontrolę nad i efektami incydentu w środowisku informacyjnym lub kontrolę nad środowiskiem informacyjnym.
- Skutek informacyjny: stan w środowisku informacyjnym, będący następstwem incydentu lub oddziaływania IERT
- Efekt informacyjny: efekt w wymiarze kognitywnym obiektu oddziaływania
- Środowisko informacyjne: przestrzeń, w której informacja jest pozyskiwana, wytwarzana, przetwarzana i przekazywana do odbiorców. Środowisko informacyjne funkcjonuje w wymiarach: wirtualnym, fizycznym i poznawczym.
- Dysponent incydentu: obiekt, lider opinii posługujący się informacją kształtującą incydent w środowisku informacyjnym

FUNDACJA
bezpieczna
cyberprzestrzeń

# Usługi REAKTYWNE
## Usługi wykrycia i obsługi incydentu w środowisku informacyjnym

**Alerty i ostrzeżenia** Usługa odnosi się do rozpowszechnienia ostrzeżenia w związku z przewidywanym lub zidentyfikowanym incydentem w środowisku informacyjnym wraz z zespołem doraźnych zaleceń sposobu obsługi incydentu jeżeli obsługa incydentu następuje poza zespołem IERT. Alert lub ostrzeżenie jest rozpowszechniane jako reakcja na wykryty lub bieżący, obsługiwany incydent w środowisku informacyjnym.

**Obsługa incydentów** Usługa obejmuje rozpoznanie incydentu w środowisku informacyjnym, ocenę, analizę, planowanie oraz obsługę incydentu przez zespół działań aktywnych zespołu IERT, z uwzględnieniem oddziaływania informacyjnego.

**Analizy incydentu** Analizy elementów składowych incydentu. Analiza oddziaływania informacyjnego, analiza efektów oddziaływania, skutków i efektów informacyjnych generowanych przez incydent. Analiza obejmuje badanie incydentu, efektów w wymiarach: technicznym, wirtualnym, fizycznym i kognitywnym.

**Zbieranie dowodów** Zbieranie, przechowywanie i analiza materiału informacyjnego, wzorca działania będącego elementem incydentu z uwzględnieniem danych technicznych.

**Śledzenie, namierzanie. rozpoznanie** Rozpoznanie cech szczególnych incydentu. Próba zidentyfikowania dysponenta, beneficjenta incydentu. Rozpoznanie rozwoju incydentu, określenie potencjalnych wzorców oddziaływania incydentu.

**Reagowanie na incydenty na miejscu** Zespół IERT zapewnia bezpośrednią pomoc w obsłudze incydentu u klienta jeżeli tego wymagają okoliczności. Zespół IERT posiada zdolność obsługi incydentu u klienta jeśli IERT nie znajduje się w tej samej lokalizacji co systemy, członkowie IERTu udają się na miejsce.

**Wsparcie reagowania na incydenty** IERT asystuje i doradza ofierze ataku poprzez dostępne środki komunikacji. Asysta techniczna w interpretacji zgromadzonych danych, pomoc w realizacji procesu IERT, udostępnienie samodzielnie pozyskanych danych nt. incydentu Klientowi. Przekazywanie informacji o strategiach postępowania. Usługa nie oznacza bezpośredniej obsługi incydentu.

**Koordynacja reagowania na incydenty** IERT posiada zdolność koordynacji i wsparcia procesu reakcji na incydent przez personel poszkodowanego, innych IERTów, służb PR. W usłudze tej IERT zbiera informacje, powiadamia strony o potencjalnym zagrożeniu, umożliwia komunikację, wymianę i analizę danych. Zapewnia komunikację z organami ścigania, służbami PR. Usługa nie oznacza bezpośredniej obsługi incydentu.

**Obsługa artefaktów** Artefakt – każda istotna pod względem informacyjnym i technicznym cecha incydentu informacyjnego, materiał informacyjny, (wzorzec retoryczny, wzorzec działania), obiekt informacyjny uczestniczący w incydencie informacyjnym lub zidentyfikowany w korelacji z innymi incydentami spoza obszaru "constituency" .

**Analiza artefaktów** Analiza techniczna, wzorca działania, lingwistyczna, skutku i efektu oddziaływania w środowisku informacyjnym w celu wyodrębnienia cech szczególnych, artefaktu.

**Koordynacja reagowania na artefakty** Udostępnianie i synteza informacji z analizy lub/i mówiących o strategiach postępowania wobec artefaktu.

FUNDACJA
bezpieczna
cyberprzestrzeń

# Usługi PREWENCYJNE
## Działania na rzecz poprawy bezpieczeństwa obszaru odpowiedzialności. Działania wyprzedzające w obsłudze incydentów w środowisku informacyjnym.

**Powiadomienia** Usługa powiadomień obejmuje m.in. ostrzeżenia o incydentach, porady bezpieczeństwa. Powiadomienia te informują o nowych wydarzeniach, których skutki mogą być krótko, średnio i długoterminowe (np. nowe incydenty, kampania nie będąca incydentem ale mogąca być jego elementem w przyszłości – np.: przygotowanie informacyjne).

**Reakcja** Usługa obejmuje realizację wybranych elementów procesu IERT w celu niwelacji incydentu lub niedopuszczenia do zaistnienia incydentu w przypadku identyfikacji działań wyprzedzających wystąpienia incydentu w środowisku informacyjnym.

**Aktualności technologiczne** IERT monitoruje nowe rozwiązania techniczne, narzędzia, działania legislacyjne, działania polityczne/społeczne, obiekty informacyjne tematycznie związane z obszarem odpowiedzialności. Dokonuje przeglądu i oceny informacji mogących mieć znaczenie dla bezpieczeństwa środowiska informacyjnego lub „constituency". Komunikuje się z innymi organizacjami. Sporządza ogłoszenia, wytyczne, rekomendacje średnio i długoterminowe.

**Audyty bezpieczeństwa** Usługa dostarcza szczegółowych analiz bezpieczeństwa systemów i procesów zarządzania incydentami w środowisku informacyjnym. Szczególną formą realizacji audytu mogą być ćwiczenia wg ustalonego scenariusza.

**Konfiguracja i obsługa narzędzi, aplikacji, infrastruktury i usług zapewniających bezpieczeństwo** IERT wskazuje lub dostarcza odpowiednie wytyczne do właściwej konfiguracji i utrzymania narzędzi, aplikacji, itp. używanych przez "constituency". IERT aktualizuje proces obsługi środowiska informacyjnego, narzędzia i usługi IERT.

**Rozwój narzędzi bezpieczeństwa** Usługa oznacza tworzenie nowych, dopasowanych do potrzeb „constituency" procedur i narzędzi, które są wymagane lub potrzebne zespołom IERT do kompleksowej i efektywnej realizacji procesu IERT.

**Powiadomienia dotyczące bezpieczeństwa** Usługa dostarcza wszechstronne repozytorium użytecznych informacji: wytycznych, listy kontaktowej, archiwum alertów, ostrzeżeń, ogłoszeń, dobrych praktyk, polityk, procedur, checklist, i FAQ procesu IERT.