ABUSE-Forum

Przemek Jaroszewski
NASK / CERT Polska

Co to jest ABUSE-Forum?

- Grupa robocza dla zespołów zajmujących się nadużyciami u polskich dostarczycieli Internetu i contentu
- Powstała w 2003, początkowo dla ISP
- Rozszerzona o dostawców treści (m.in. Allegro, Agora, Onet.pl, nasza-klasa, Gadu Gadu), CERT.GOV.PL, WBBiŁ, …
- Początkowe cele – poznanie się, swoich problemów, sposobów pracy
- Współpraca z organami ścigania, wspólne inicjatywy, dyskusje…

Zasady

- Spotkania 3x w roku (potencjalna kolokacja z jesiennym PLNOG)
- Lista mailingowa, lista kontaktów
- Członkowstwo osobiste
  - Tylko osoby związane z bezpieczeństwem, obsługą nadużyć, incydentów
  - Najlepiej osoby operacyjne, nie management
  - E-mail wyłącznie „firmowy”
  - Osoba wskazana przez dotychczasowego członka z tej samej instytucji
  - Nowa instytucja: rekomendacja + brak sprzeciwu
- Wymagana aktywność!
- Brak formalnego statusu

Blackholing

- … bo nam nie jest wszystko jedno
- Cele
  - ograniczenie komunikacji z kontrolerami botnetów
  - ograniczenie dostępu do stron stanowiących zagrożenie techniczne
  - ograniczanie skutków ataków DDoS
  - wspólna realizacja i wymiana informacji
- Kto powinien decydować?
  - każdy w zakresie swojej sieci
  - eksperci
  - ??

BGP Blackholing

- Bardziej „ryzykowny” ale łatwy w implementacji i skalowalny
- Zasady:
  - Każdy operator może dodawać prefiksy /32 z własnej sieci
  - CERT Polska dołącza dodatkowe listy
  - Każde źródło identyfikowane osobnym community
- W produkcji od 2007
- Nie ma przeszkód w korzystaniu niezależnie z innych źródeł czy innych projektów, np. blackholing.pl

DNS Blackholing

- „Miękki”, może być łatwo wdrożony jako opcjonalna funkcjonalność
- Proponowane rozwiązanie: domyślne serwery „kłamią”, dodatkowe serwery dla „wymagających” klientów
- Brak standardowych protokołów wymiany informacji
- NASK przymierza się do wprowadzenia produkcyjnie i stworzenia pilota

Ogólne wnioski ze statystyk

- Statystyki pomiędzy operatorami trudno jest porównać ze względu na:
  - różne systemy klasyfikacji
  - pomijanie wielu rodzajów zgłoszeń
  - brak rozróżnień między zgłoszeniami i incydentami
- Ogromna większość zgłoszeń to przypadki rozsyłania spamu
- Druga najliczniejsza grupa to naruszenia praw autorskich
- Stosunkowo dużo zgłoszeń phishingu
- Część zespołów zgłasza zastrzeżenia co do prawnych możliwości weryfikacji i obsługi niektórych rodzajów zgłoszeń

Pozbywamy się IE6

- Konsekwencja krytycznej luki 0day z 14.01.2010 (MSA 979352)
- IE6 to przeglądarka przestarzała, niewspierana przez producenta, uciążliwa w obsłudze dla programistów WWW
- Aktualny odsetek użytkowników IE6: 4-7%
- Microsoft żywotnie zainteresowany eliminacją tej wersji przeglądarki
- Wspólny komunikat jako podsumowanie spotkania AF
- Zachęta do
  - Umieszczania informacji we własnych serwisach / przekazania jej klientom
  - Dedykowanego ostrzeżenia dla użytkowników IE6
  - Zaprzestania wspierania przeglądarki we własnych serwisach

Abuse-forum jest otwarte

- info@cert.pl
- przemek@cert.pl

- Dołącz, powiedz kolegom, zorganizuj spotkanie ;)

CERT POLSKA

zgłaszanie incydentów: cert@cert.pl

strona internetowa: www.cert.pl

tel. +48 22 380 82 74

fax +48 22 380 83 99

adres pocztowy:

NASK - CERT Polska

ul. Wąwozowa 18

02-786 Warszawa

Polska

DZIĘKUJEMY ZA UWAGĘ

ZMYEL TELEKOMUNIKACJI

NASK

CERT POLSKA