URZĄD
OCHRONY
KONKURENCJI
I KONSUMENTÓW

# KODEKS DOBRYCH PRAKTYK ANTYSPAMOWYCH DLA ISP

7 marca 2006 r.

Autorzy:

Justyna Kurek, Łukasz Wroński

# Dlaczego spam jest groźny?

- Poważne awarie, w tym wypadki zatrzymania systemów z powodu samej tylko ilości wysyłanej poczty
- Gorsza jakość systemów poczty elektronicznej dla wszystkich użytkowników, opóźnienia i blokada legalnego ruchu
- Niechciany ruch dla użytkowników
- Dodatkowe koszty utrzymania systemów dla operatorów i dostawców usług internetowych

# Czy możliwa jest LIKWIDACJA zjawiska spamu?

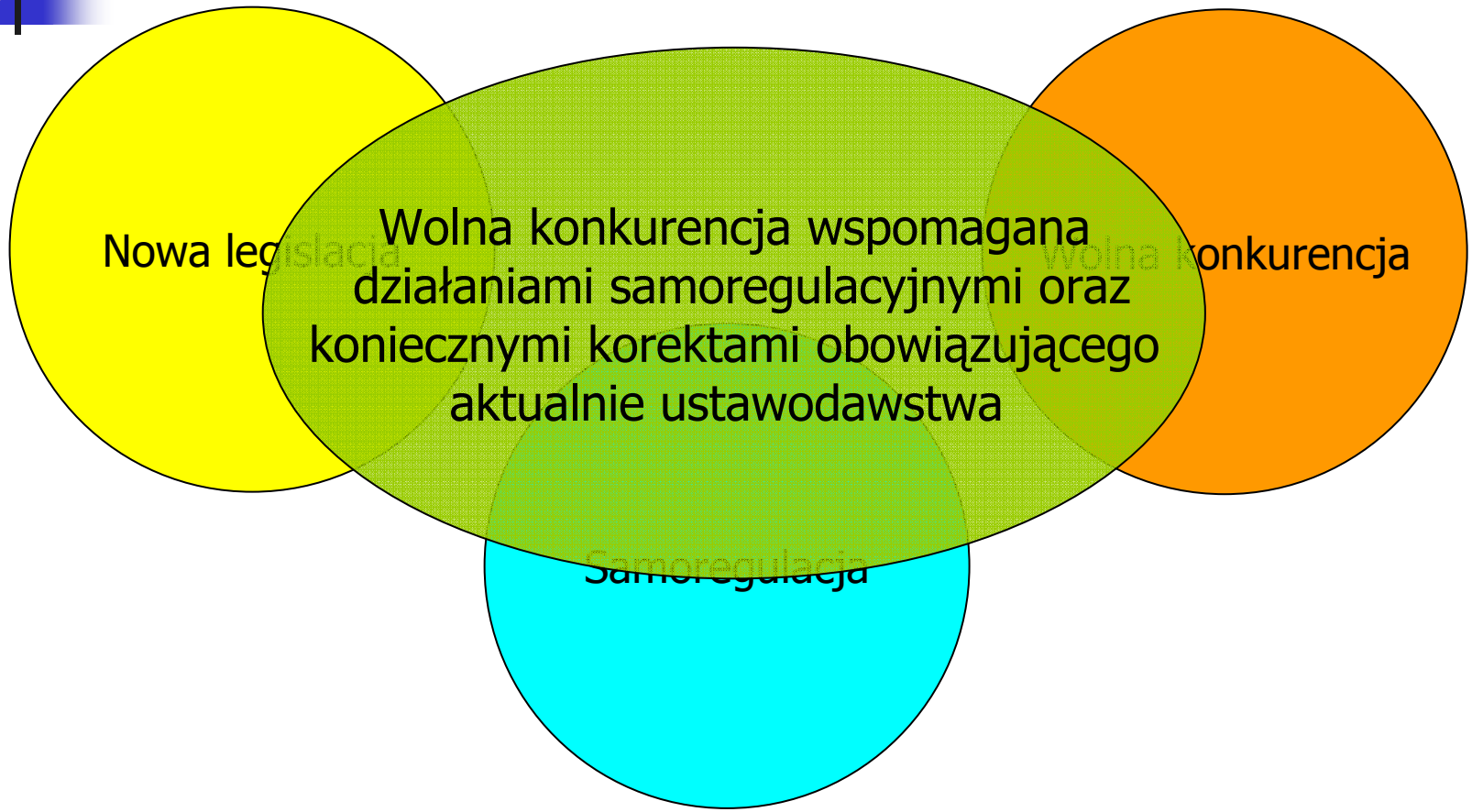
NIE!

Wszelkie działania podejmowane zarówno przez przedsiębiorców, jak też organy administracji mogą mieć na celu tylko i wyłącznie OGRANICZENIE skali zjawiska spamu

# OGRANICZENIE zjawiska spamu

W walce ze zjawiskiem spamu najbardziej praktycznym wkładem operatorów i dostawców usług internetowych może być minimalizacja wysyłania spamu przez swoich klientów lub ze swoich systemów

# Metody walki ze spamem



# Metody walki ze spamem

- Powszechność zastosowania
- Konsolidacja sił
- Współpraca wszystkich podmiotów / uczestników rynku (przedsiębiorcy, organy administracji, użytkownicy)

# Inicjatywy samoregulacyjne dotyczące zjawiska spamu

- Kanada
- Hong Kong
- Wielka Brytania

# Efekty podjętych inicjatyw

Dane przedstawione przez kanadyjsich dostawców usług wskazują na:

- 95 % spadek liczby wysyłanych wirusów
- 98 % spadek raportów o nadużyciach
- zmniejszenie liczby wirusów oraz przechwyconych maszyn używanych do wysyłania spamu
- oszczędności kosztów w zakresie jednostek zarządzania siecią

# Wnioski

- Brak jednego rozwiązania dla spamu. Niezbędne jest stosowanie wielu rozwiązań (organizacyjnych, umownych, technicznych) mających na celu ograniczenie zjawiska spamu
- Rządy państw powinny promować przyjmowanie przez operatorów i dostawców usług internetowych rozwiązań ograniczających zjawisko spamu
- Operatorzy i dostawcy usług internetowych powinni przyjmować i skutecznie wprowadzać w życie kodeksy dobrego postępowania

# Podstawowe założenia kodeksu dobrych praktyk

ISP zapewniają, że

- ich systemy pocztowe nie przekazują dalej poczty od nieautoryzowanych osób trzecich
- można stwierdzić źródło wszystkich przesyłek wygenerowanych w ich sieci
- wszystkie przesyłki wygenerowane w ich sieciach można przypisać konkretnemu klientowi lub systemowi

# Podstawowe założenia kodeksu dobrych praktyk (cd)

- ISP zapewniają odpowiednie procedury przetwarzania doniesień o nadużyciach przekazywanych przez swoich klientów
- W przypadkach nadużyć, ISP podejmują odpowiednie działania powstrzymujące klienta od kontynuowania nadużyć (podstawa prawna, na podstawie której usługi dostarczane są klientowi musi zezwalać na podjęcie takich działań)
- ISP podejmują działania informacyjno-edukacyjne dotyczące zjawiska spamu i związanych z nim zagrożeń

# Zalecane elementy kodeksu dobrych praktyk

- Definicja spamu
- Umowy z użytkownikami
- Rozwiązania techniczne
- Działania operatorów / dostawców usług
- Informacja / edukacja

# Elementy kodeksu – *definicja spamu* – opis

Pod pojęciem spam należy rozumieć informację przesłaną drogą elektroniczną (w tym nie tylko informację handlową), która spełnia łącznie następujące warunki:

- jej treść jest niezależna od tożsamości odbiorcy w związku z tym, że wiadomość ta może być przesyłana do wielu niezależnych odbiorców
- odbiorca nie wyraził wcześniej zgody na otrzymanie wiadomości, przy czym zgoda ta musi być wyrażona w sposób weryfikowalny, świadomy, wyraźny i możliwy do odwołania
- z okoliczności wynika, że wysyłający odniósł niewspółmierną korzyść z faktu wysłania wiadomości w stosunku do korzyści, jaką odniósł odbiorca w związku z jej odbiorem

# Elementy kodeksu – *definicja spamu* – uzasadnienie

- Art. 10 ustawy o świadczeniu usług drogą elektroniczną – przesyłanie niezamówionej informacji handlowej jako czyn nieuczciwej konkurencji
- Wykroczenie zagrożone karą grzywny od 20 zł do 5000 zł, ściganie z wniosku pokrzywdzonego

# Elementy kodeksu – *umowy z użytkownikami* – opis

Operatorzy i dostawcy usług internetowych rozwijają i wprowadzają w życie Politykę Dozwolonego Użytkowania w celu zakazania wysyłania wiadomości spam – i podobnych działań – w swoich sieciach oraz ustalenia sankcji za złamanie zakazów

# Rekomendowane elementy Polityki Dozwolonego Użytkowania:

- Zakaz wysyłania, przesyłania, dystrybucji i dostarczania spamu
- Zakaz fałszowania nagłówków wiadomości i innej manipulacji identyfikatorów mających na celu ukrycie pochodzenia jakiejkolwiek przesyłanej zawartości
- Zakaz wysyłania wiadomości zawierających wirusy lub inne złośliwe kody i programy stworzone w celu uszkodzenia funkcjonalności jakiegokolwiek oprogramowania lub urządzeń

# Rekomendowane elementy Polityki Dozwolonego Użytkowania (cd):

- Prawo operatora lub dostawcy usług internetowych do:
  - podjęcia działań które uzna za stosowne, takich jak zablokowanie wiadomości z konkretnej domeny, serwera pocztowego lub adresu IP
  - natychmiastowego zablokowania dowolnego konta w dowolnej usłudze, która została użyta do przesyłania jakiejkolwiek wiadomości, która narusza reguły przedmiotowej polityki

# Elementy kodeksu - *rozwiązania techniczne* - opis

- Blokada przez operatorów i dostawców usług ruchu wychodzącego poczty elektronicznej użytkowników końcowych przy użyciu portu 25
- Udostępnienie portu 587 do wysyłania wiadomości pocztowych – wyłącznie za pomocą autoryzowanego protokołu SMTP Auth.

Niniejsze zalecenie nie wyklucza użycia innych metod uwierzytelniania wiadomości poczty elektronicznej

# Elementy kodeksu - *rozwiązania techniczne* - uzasadnienie

Celem uwierzytelnienia nadawcy poczty elektronicznej jest zmniejszenie zjawiska podszywania się pod nazwę domeny w wiadomościach poczty elektronicznej (domain-name spoofing), a poprzez to zmniejszenie liczby przypadków wysyłania spamu i prób pozyskania poufnych informacji (phishing)

# Elementy kodeksu - *rozwiązania techniczne* - opis

- Blokada przez operatorów i dostawców usług możliwości przesyłania załączników do wiadomości poczty elektronicznej, które mają rozszerzenie wskazujące na to, że mogą przenosić wirusy

  lub

- Filtrowanie załączników w oparciu o właściwości zawartości

# Elementy kodeksu - *rozwiązania techniczne* - uzasadnienie

Wiele wirusów i robaków jest przenoszonych w załącznikach do wiadomości; najbardziej powszechne rozszerzenia plików przenoszących taki „ładunek” to: .pif, .scr, . exe, .vbs

# Elementy kodeksu – *działania operatorów* – opis

Monitoring przez operatorów i dostawców usług internetowych objętości przychodzącej i wychodzącej poczty w celu stwierdzenia niecodziennej aktywności sieciowej i określenia źródeł takich działań

# Elementy kodeksu – *działania operatorów* – uzasadnienie

Monitorowanie i możliwe ograniczenie ilości wiadomości wysyłanych przez danego użytkownika może być pomocne w zniechęcaniu osób wysyłających wiadomości spam do takiego działania, jak również zapewnia wczesną sygnalizację możliwości infekcji maszyny użytkownika

# Elementy kodeksu – *działania operatorów* – opis

- Stworzenie przez operatorów i dostawców usług internetowych odpowiednich procedur w celu właściwego reagowania na raporty o incydentach pochodzących od innych operatorów – współpraca punktów abuse
- Współpraca z organami administracji i organami ścigania w zakresie przekazywania informacji o stwierdzonych incydentach

# Elementy kodeksu – *informacja i edukacja* – opis

Operatorzy i dostawcy usług internetowych:

- przekazują swoim abonentom założenia polityki bezpieczeństwa i procedury zabezpieczeń, w tym informacje na temat dostępności, używania i odpowiedniego stosowania oprogramowania do filtrowania spamu i wirusów
- prowadzą kampanie informacyjne podnoszące świadomość użytkowników w zakresie tego, jakie działania mogą podjąć w zakresie ograniczenia spamu

# Dziękujemy za uwagę!

Justyna Kurek

jkurek@uokik.gov.pl

Łukasz Wroński

lwronski@uokik.gov.pl