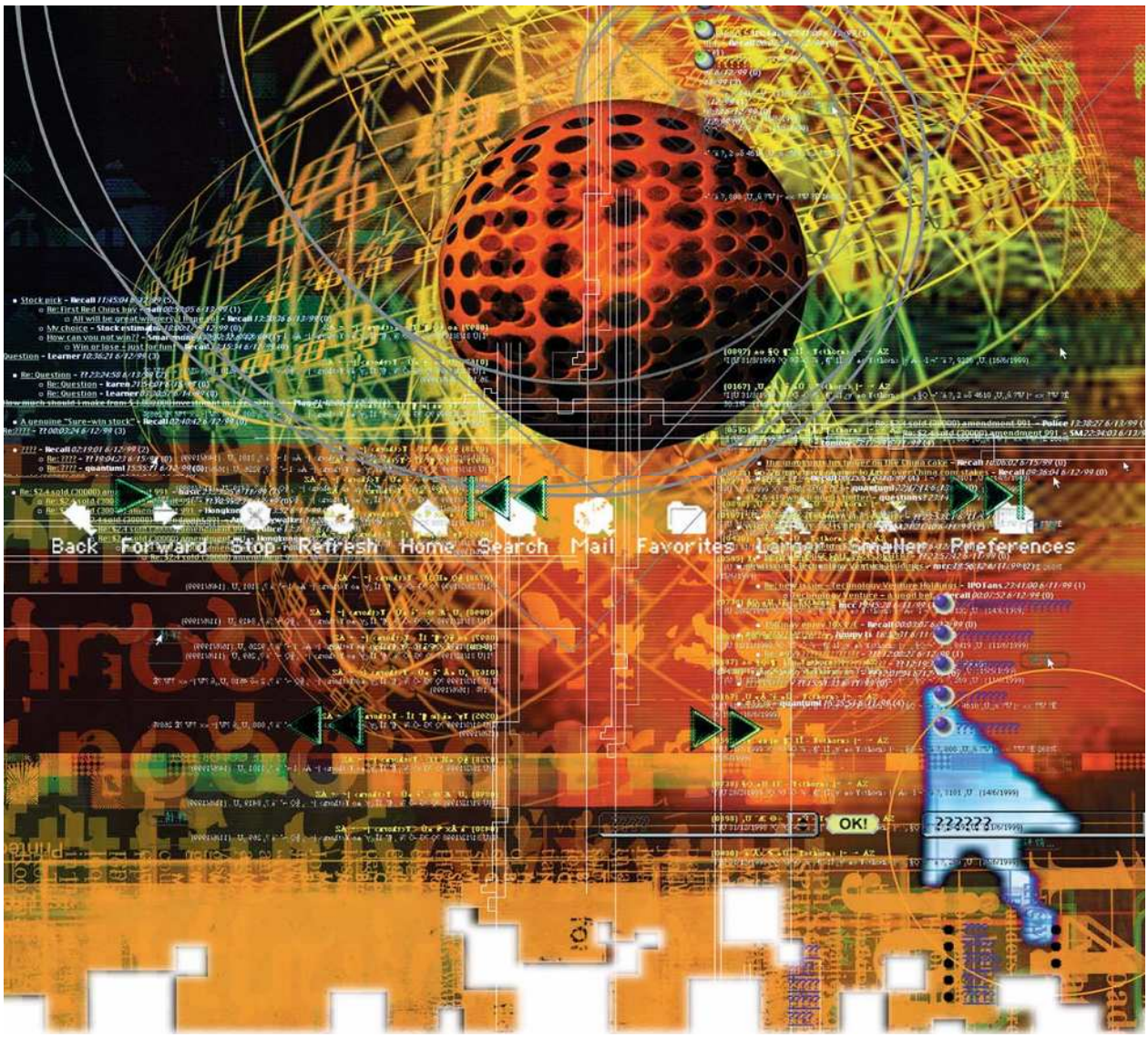


Środki bezpieczeństwa dostawców usług – Część 2

Środki bezpieczeństwa i narzędzia antyspamowe dostawców usług łączności elektronicznej – stan obecny i tendencje

Dokument 4.2.b Programu Roboczego 2006
ENISA/TD/SP/06/118

Carsten Casper i Pascal Manzano

Sekcja Strategii Bezpieczeństwa – Departament Techniczny Europejskiej Agencji Bezpieczeństwa Sieci i Informacji ENISA

Spis treści

1 Streszczenie

Gdy mowa o bezpieczeństwie w Internecie, dostawcy usług łączności elektronicznej znajdują się w centrum uwagi. Obywatele europejscy i przedsiębiorstwa muszą im zaufać, zanim zdecydują się na zawarcie handlowej czy społecznej transakcji on-line. Incydenty związane ze spamem i bezpieczeństwem jednak nadal szkodzą tej komunikacji Brak zaufania ma ogromny wpływ na społeczeństwo informacyjne w Europie. Z myślą o poprawieniu tej sytuacji UE stworzyła ramy prawne dla usług łączności elektronicznej i ich zabezpieczenia.

Niniejszy raport opisuje, w jaki sposób dostawcy usług uwzględnili te wymogi prawne i co można zrobić, by w przyszłości zabezpieczać europejskie sieci i usługi. Jest on oparty na ankietach, które ENISA przeprowadziła wśród dostawców usług, a także na informacjach zdobytych na konferencjach i warsztatach. Skupiono się raczej na ostatnich osiągnięciach i tendencjach niż na szczegółowych danych statystycznych. Fakty, wnioski i propozycje zawarte w tym raporcie podzielono według trzech głównych tematów:

Zarys badań

Coraz większa przejrzystość	Definicja odpowiedniego bezpieczeństwa	Tworzenie standardów
• Powiadamianie o naruszeniach bezpieczeństwa • Uświadamianie sobie problemu związanego z bezpieczeństwem i spamem	• Określenie obecnej sytuacji i kosztów wdrażania Bezpieczeństwo poczty elektronicznej a prywatność	• Techniczne i organizacyjne środki bezpieczeństwa Środki zwalczania spamu

Coraz większa przejrzystość

Powiadamianie o naruszeniach bezpieczeństwa – w USA powiadamianie jest w pewnym stopniu obowiązkowe, natomiast w UE jest ono w większości dobrowolne. Odpowiednie statystyki i wspólne dane na temat incydentów naruszenia bezpieczeństwa są konieczne przy zwiększaniu przejrzystości bezpieczeństwa informacji i przy planowaniu odpowiednich i skutecznych środków zaradczych.

Uświadamianie sobie problemu związanego z bezpieczeństwem i spamem – nadal nie zauważa się wielu problemów związanych z bezpieczeństwem. Podczas gdy widoczny poziom spamu wciąż jest bardzo wysoki, zmienia się rodzaj zagrożenia. Coraz więcej spamu przesyłają komputery obywateli, bez ich wiedzy, działając jak tzw. „zombie"„. Nazwy stron są przywłaszczane, a podejrzani rejestratorzy oszukują właścicieli domen. Niektórzy dostawcy usług patrzą na dane o zagrożeniach jak na informacje posiadane na własność, dające im przewagę nad konkurencją. Ponadto wielu nadal polega całkowicie na skargach klientów, a nie na aktywnym monitorowaniu sieci. Nie informują oni również klientów o kosztach środków zaradczych. Dostawcy usług muszą pogłębić analizę incydentów, natomiast Europa ogólnie potrzebuje mechanizmu ostrzegawczego, by móc określać nadchodzące zagrożenia i by im przeciwdziałać.

Definicja odpowiedniego bezpieczeństwa

Określenie obecnej sytuacji i kosztu wdrażania – większość dostawców usług postępuje zgodnie z tzw. najlepszą praktyką w branży. Wielu oferuje darmowe filtrowanie spamu lub linie interwencyjne, nawet gdy wiąże się to z olbrzymim kosztem dla nich. Zbieranie danych o szkodach spowodowanych incydentami naruszenia bezpieczeństwa jest rzadkie, co utrudnia analizę wydajności kosztów. Dostawcy usług muszą również zadbać o większe zaufanie klienta, wykazując na przykład, że postępują zgodnie z certyfikatami bezpieczeństwa. Konieczne są dalsze badania na poziomie unijnym.

Bezpieczeństwo poczty elektronicznej a prywatność – dostawcy usług dostrzegają konflikt między świadczeniem bezpiecznych usług a ochroną prywatności. Opinia 118 Grupy Roboczej Art. 29 w sprawie prywatności pomaga odnaleźć właściwą równowagę między tymi sprzecznymi celami. Koszt powszechnego, dopasowanego do klienta filtrowania jest jednak ogromny. Konieczny jest dalszy dialog między rzecznikami ochrony prywatności a orędownikami bezpieczeństwa.

Tworzenie standardów

Techniczne i organizacyjne środki bezpieczeństwa – nie trzeba określać celu, ale raczej dopracować środki bezpieczeństwa. Kwarantanna zainfekowanych komputerów, zabezpieczanie usługi rejestracji i utrzymywania nazwy domeny i ochrona sąsiednich sieci powinny być elementem technicznego programu działania. Dostarczanie dokładnych danych osobowych, zapewnianie szczegółowych wskazówek dla subskrybentów i zwiększanie świadomości na temat kradzieży tożsamości wspiera bezpieczną komunikację z organizacyjnego punktu widzenia. Szkolenia konsumenckie mogłyby być realizowane przez partnerstwa publiczno-prywatne. Środki zależą od rodzaju działalności, rozmiaru i zaawansowania dostawcy usług.

Środki zwalczania spamu – w UE różne przepisy antyspamowe są gotowe do wdrożenia. Jest to wyzwanie na dziś - zastosować je w Europie i poza nią. OECD Anti-Spam Toolkit (zestaw narzędzi antyspamowych OECD), kodeksy postępowania dla dostawców usług, techniki uwierzytelniania nadawcy, grzywny dla spamerów i inicjatywy gromadzenia danych o spamie – wszystko to odgrywa ważną rolę. Obawa przed procesami wytaczanymi przez spamerów, szansa na dodatkowy dochód z podejrzanych mailowych usług marketingowych i uciążliwość powiadamiania o przypadkach spamowania jest nadal wyzwaniem dla dostawców usług. Świadomość na temat spamu i związanych z nim zagrożeń dla bezpieczeństwa musi pozostać wysoka.

Poniższy raport jest dokumentem Programu Roboczego 2006 ENISA. Badania te będą kontynuowane w 2007 r.

2 Wstęp

2.1 Uzasadnienie

Obywatel Europy nie czuje się jeszcze bezpieczny korzystając z Internetu, choć wiele już zrobiono, by uczynić z sieci bezpieczniejsze miejsce komunikacji, w którym mógłby porozumiewać się z rządami i prowadzić działalność gospodarczą. Należy udokumentować podjęte środki bezpieczeństwa i przedstawić wyniki tych ulepszeń europejskiemu społeczeństwu.

Główną rolę w zabezpieczaniu Internetu odgrywają w szczególności dostawcy usług internetowych (zwani dalej „dostawcami"), firmy telekomunikacyjne i inni dostawcy informacji i usług internetowych. Wdrożyli oni szereg środków bezpieczeństwa i narzędzi antyspamowych, nie tylko w wyniku własnej oceny ryzyka i analizy wydajności kosztów, ale także w odpowiedzi na krajowe ustawodawstwo i wskazówki odnośnie do bezpieczeństwa informacji. Wiele z tych ostatnich znalazło się w europejskich dyrektywach, w szczególności w europejskiej dyrektywie 2002/58/WE („dyrektywa o prywatności i łączności elektronicznej") oraz w dyrektywach ramowych o łączności elektronicznej (2002/19-22/WE).

Niniejszy wynik sprawozdań ENISA traktuje o obecnym stanie bezpieczeństwa w Europie i nakreśla tendencje na przyszłość. Ma na celu zwiększenie zaufania do łączności

elektronicznej między branżami, rządami i obywatelami Europy, prowadząc do większego uznania usług eAdministracji i handlu elektronicznego. Jest to konieczne do osiągnięcia celów inicjatywy i2010 poprzez utworzenie otwartego i konkurencyjnego, wspólnego rynku dla społeczeństwa informacyjnego i usług medialnych w obrębie Unii Europejskiej.

2.2 Metodologia

Dokument niniejszy jest drugą częścią dokumentu 4.2.b Programu Roboczego 2006 ENISA, który określa się jako *„Badanie wyszczególniające środki przyjęte i udostępnione przez dostawców usług łączności elektronicznej w celu zastosowania się do prawnych wymogów dotyczących technicznych i organizacyjnych środków zapewniania bezpieczeństwa ich usług"*, które zostało przewidziane na drugi kwartał 2006 r. Pierwsza część została wydana w lutym 2006 r. jako reakcja na wniosek Komisji Europejskiej (20051103_COM) o jak najszybsze rozpoczęcie prac w tym zakresie i dostarczenie wyników przed pierwotnie zaplanowanym ostatecznym terminem (II kwartał 2006 r.). To pierwsze badanie przeprowadzone pod koniec 2005 r. i na początku 2006 r. zwane jest dalej *„Ankietą ENISA"*. Jego numer referencyjny to ENISA/TD/SP/06/0055.

W związku z powyższym ENISA dostosowała założenia niniejszego raportu. Uzupełniono pierwsze badanie większą ilością danych i w pewnym stopniu dostosowanych pytań. Sprawozdanie to jest oparte na danych z pierwszego badania, z licznych warsztatów i konferencji, w których ENISA uczestniczyła począwszy od chwili jej powstania oraz na szeroko zakrojonej analizie Internetu.

Raport został zorganizowany wokół sześciu głównych tematów – najistotniejszych, najbardziej zaniedbanych lub najbardziej kontrowersyjnych. Przy każdym temacie przedstawiono fakty i obserwacje, oceny i wnioski oraz rady i propozycje.

Część dotycząca faktów i obserwacji jest podsumowaniem własnych badań ENISA i innych źródeł danych. Zamiast wyliczać wszystkie dostępne dane, część ta skupia się na obecnych tendencjach i interesujących wartościach. Informacji nie zmieniano, podano krótkie odniesienie do źródła. Szczegółowa lista odniesień, wraz z linkami, została umieszczona w załączniku.

Część dotycząca ocen i wniosków przedstawia opinie ENISA. Poza faktami opisuje, jakie rozumowanie skłoniło ENISA do wyszczególnienia wspomnianych wartości. Jest to przygotowanie do części trzeciej. Nie zawsze istnieje bezpośrednia więź między zawartością trzech części; jest jednak kilka stwierdzeń, które należy rozważać razem.

Część poświęcona radom i propozycjom przedstawia zarys rozwiązań. Można je uszeregować od wczesnej koncepcji, która wymaga omówienia z zainteresowanymi stronami i partnerami ENISA do konkretnej propozycji, której wdrożenie ENISA będzie wspierać zgodnie ze swoją pozycją w europejskiej zbiorowości zajmującej się bezpieczeństwem. Może to utorować drogę dla ulepszonego ustawodawstwa lub przynajmniej da początek dodatkowym projektom, warsztatom i wynikom samej ENISA.

Należy zauważyć, że zalecenia w tym sprawozdaniu nie zastępują zaleceń umieszczonych w sprawozdaniu z lutego 2006 r.

Raport miał na celu dostarczyć wykształconej zbiorowości zajmującej się bezpieczeństwem informacji zwięzłych i przy odrobinie szczęścia nowych informacji. Nie jest to ani ostateczny zapis najlepszej praktyki, ani ogólny plan dla przyszłego ustawodawstwa w zakresie bezpieczeństwa. Jest to zaledwie próba przybliżenia wyzwań, jakie stoją przed dostawcami usług, zarys rozwiązań, jakie stosują czołowi dostawcy – a które inni mogą chcieć zastosować – i próba skłonienia czytelnika do (ponownego) zaufania łączności elektronicznej w Europie.

2.3 Ogólny zarys

Bezpieczeństwo usług łączności elektronicznej jest złożonym zagadnieniem. Posiada ono aspekty techniczne, prawne, organizacyjne, polityczne i rynkowe. Kwestia blokowania spamu jest również złożona, a przy tym nawet bardziej dynamiczna, biorąc pod uwagę fakt, że zagrożenia i środki zaradcze szybko ewoluują. Nie istnieje jedno rozwiązanie. Każdy dokument dotyczących tych tematów musi zmierzyć się z różnorodnymi perspektywami i opiniami.

Niniejszy dokument opisuje obecną sytuację bezpieczeństwa i spamu w usługach łączności elektronicznej i przewiduje potencjalny rozwój w ciągu dwóch najbliższych lat. Dokonuje tego dzieląc dziesiątki spraw, obserwacji i propozycji według trzech głównych tematów:

„Coraz większa przejrzystość" została uznana przez ENISA za najbardziej zasadniczą kwestię. Zbiorowość zajmująca się bezpieczeństwem informacji nadal musi się wiele nauczyć na temat obecnej sytuacji w europejskich sieciach i motywów działania wszystkich graczy. Jest to szczególnie istotne, gdyż jest obecnie w toku kilka projektów, które mogłyby zwiększyć przejrzystość. Aktualne cele są w zasięgu ręki.

„Definicja odpowiedniego bezpieczeństwa" była celem co najmniej od powstania dyrektywy 2002/58/WE. Jednak z powodu kosztów i obecnej sytuacji, często poprzestaje się na gołosłownych deklaracjach, a gdy nawet istnieją plany procesów mających na celu tworzenie definicji bezpieczeństwa, rzadko się jej wykonuje. Ciężko spostrzec, jak zasadniczych postępów można dokonać w krótkim okresie, choć widoczne są pewne osiągnięcia w obrębie zagadnienia „prywatność a bezpieczeństwo".

„Tworzenie standardów" jest ciągle omawianym zagadnieniem. W tym przypadku wyzwanie polega na obserwowaniu obecnych inicjatyw i osiągnięć, zarówno pod względem technicznym, jak i politycznym. Osiągnięto znaczny postęp w ciągu ostatnich trzech lat, ale jeszcze nie pora zmieniać przedmiot zainteresowania: Środki bezpieczeństwa i narzędzia antyspamowe wymagają nieustannej uwagi.

Podstawową wytyczną dla tego sprawozdania jest europejska dyrektywa 2002/58/WE. Została wykorzystana przy konstruowaniu kwestionariusza, który był podstawą pierwszej ankiety. Ponadto niektóre kwestie poruszone w niniejszym raporcie łączą się bezpośrednio z dyrektywą, szczególnie z art. 4 i 13. Jednak dyrektywa ta nie ma bezpośredniego zastosowania do dostawców usług łączności elektronicznej, którzy są główną, omawianą w tym dokumencie grupą. 25 państw członkowskich Unii Europejskiej transponuje dyrektywę do krajowych ustaw i dopiero te ustawy są wiążące dla dostawców usług w UE. Dodatkowo istnieje kilka grup inicjatyw w grupie użytkowników zajmującej się bezpieczeństwem informacji, które dostarczają dodatkowych wskazówek w stosunku do dyrektywy, ustaw i ich wdrożeń przez dostawców usług.

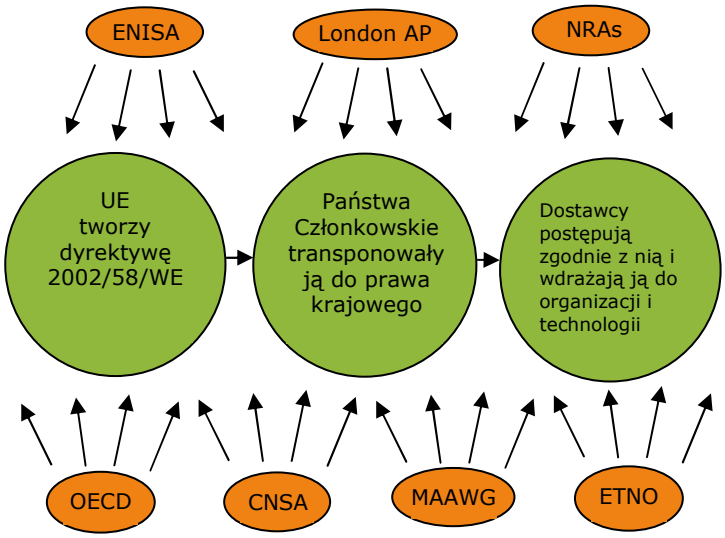
3 Coraz większa przejrzystość

„Jeśli nie jesteś w stanie czegoś zmierzyć, nie możesz tym zarządzać" – jest to znana mądrość stosowana w zarządzaniu przedsiębiorstwami. Jak można zarządzać bezpieczeństwem informacji, jeśli nadal istnieje tak mało danych i – co ważniejsze – jeśli nie są one porównywalne? Jak można decydować o środkach zaradczych, jeśli nie istnieje jasny – i bieżący – obraz problemu? Uświadamianie sobie zagrożeń dla bezpieczeństwa jest koniecznym punktem wyjścia; dzielenie się informacjami z partnerami lub powiadamianie o nich oficjalnie to dodatkowa kwestia.

3.1 Powiadamianie o naruszeniach bezpieczeństwa

Powiadamianie o naruszeniach bezpieczeństwa jest delikatnym i powszechnie dyskutowanym tematem. Nie tylko nie ma porozumienia co do tego, czy i jak powinno się powiadamiać o naruszeniach, ale także nie istnieje powszechnie akceptowana definicja tego, czym jest naruszenie bezpieczeństwa. Skanowanie określonego portu, wytropione hasło, niszczenie strony internetowej i oszustwo przy użyciu karty kredytowej na szeroką skalę mogą być uważane za naruszenia. Należy również zauważyć, że jest różnica między „naruszeniem" (udanym atakiem) a „ryzykiem naruszenia" (narażeniem na niebezpieczeństwo), jak to zostało określone w europejskiej dyrektywie 2002/58/WE.

Schemat środków bezpieczeństwa informacji i środków antyspamowych w Europie



Podstawową wytyczną dla tego sprawozdania jest europejska dyrektywa 2002/58/WE. Została wykorzystana przy konstruowaniu kwestionariusza, który był podstawą pierwszej ankiety. Ponadto niektóre tematy tego sprawozdania łączą się bezpośrednio z dyrektywą, szczególnie z art. 4 i 13. Jednak dyrektywa ta nie ma bezpośredniego zastosowania do dostawców usług łączności elektronicznej, którzy są główną, omawianą w tym dokumencie grupą. 25 państw członkowskich Unii Europejskiej transponuje dyrektywę do krajowych ustaw. Tylko te ustawy są wiążące dla dostawców usług w UE. Ponadto istnieje kilka grup inicjatyw w społeczności zajmującej się bezpieczeństwem informacji, które dostarczają dodatkowych w stosunku do dyrektywy, ustaw i ich wdrożeń przez dostawców usług inicjatyw.

Powiadamianie o naruszeniach bezpieczeństwa

- Upowszechnianie powiadamiania o naruszeniach i sprawienie, że dane te będą porównywalne
- Uzasadnianie badań nad słabymi punktami
- Promowanie wskaźników
- Udzielanie informacji klientom
- Spam przychodzący a spam wychodzący
- Promowanie wymiany informacji

Fakty i obserwacje

• Większość dostawców usług sama decyduje, czy i jak informować subskrybentów i inne osoby. Około połowa dostawców usług **informuje klientów** o ryzyku naruszenia przy wykorzystaniu prywatnych kanałów (tj. prywatnej strony internetowej, poczty elektronicznej lub tradycyjnej poczty). Bardzo niewielu powiadamia całe społeczeństwo (np. poprzez publikację na stronie internetowej lub notatkę w prasie). Tylko w Finlandii dostawcy usług są proszeni o powiadamianie o naruszeniach fińskiego krajowego organu nadzorującego (KON). (Ankieta ENISA z 2006 r.)

• Kalifornijska Ustawa Stanowa 1386, która wprowadziła obowiązek **powiadamiania o naruszeniach bezpieczeństwa**, związanych z kalifornijskimi obywatelami, weszła w życie 1 lipca 2003 r. Za tym przykładem poszło 30 innych stanów USA wprowadzając podobne ustawy. 20 z nich weszło w życie między 1 stycznia 2006 r. a 1 stycznia 2007 r. W wyniku tego upublicznione zostały poważne naruszenia i zwiększyła się w Stanach świadomość na temat kradzieży tożsamości.

• **Badanie słabych stron** staje się coraz bardziej skomercjalizowane. Rynek rozwija się tam, gdzie badacze bezpieczeństwa nie informują społeczeństwa, ale raczej dostarczają informacji tylko firmom zajmującym się bezpieczeństwem, które im płacą (Sprawozdanie *Symantec's Internet Threat Report*, III kwartał 2006 r.)

• „**Czas do momentu naruszenia**" opisuje, jak długo system komputerowy bez ochrony może być podłączony do Internetu zanim zostanie zainfekowany. Jest to wskaźnik ilustrujący potrzebę aktualizacji. Czas do momentu naruszenia jest różny dla różnych systemów, w zależności od strategii ISP (dostawcy usług internetowych) i zasad filtrowania sąsiednich systemów. (Sprawozdanie *Symantec's Internet Threat Report*, III kwartał 2006 r.)

• Choć większość brytyjskich podmiotów posiada procedury zapisu i reakcji na incydenty naruszenia bezpieczeństwa (83 %), tylko niewielka ich część zachowuje dowody stosowania się do norm prawnych (21 %) lub jest w stanie reagować na skargi na to, że ktoś z zewnątrz przejął kontrolę nad siecią (22 %). (Sprawozdanie DTI 2006)

• By promować ujawnianie i wymianę informacji o bezpieczeństwie cybernetycznym między przedsiębiorstwami rząd federalny USA wsparł utworzenie wielu podzielonych według gałęzi przemysłu ośrodków wymiany i analizy informacji **Information Sharing & Analysis** Centers (ISAC) zgodnie z prezydencką dyrektywą 63 („Konsekwencje ekonomiczne rozpowszechniania informacji o bezpieczeństwie", 2005).

Oceny i wnioski

- Wydaje się, że powiadamianie o naruszeniach bezpieczeństwa zwiększa przejrzystość, działa na rzecz środków zaradczych i pozwala zmniejszyć ogólną liczbę naruszeń. Jednak nie istnieją porównywalne dane liczbowe, które potwierdziłyby to przypuszczenie. W większości państw europejskich powiadamianie o naruszeniach nie jest uważane za obowiązkowe i nie jest sformalizowane. Jeśli nie istnieje wspólne podejście w zakresie zbierania danych i powiadamiania o niebezpieczeństwach, nie można wymieniać między sobą danych.
- Rynkowe badania nad słabymi punktami mają dwa skutki. Z jednej strony zachęca to do poświęcania czasu i innych zasobów na badania, co pozwala zbiorowości na określenie problemów związanych z bezpieczeństwem. Z drugiej strony informacje na temat podatności systemu na zagrożenia nie są już wymieniane bezpłatnie między badaczami, tak więc trudniej jest ocenić ryzyko. Ważne, by istniał skoordynowany proces publikacji na temat słabości systemów, tak by sprzedawcy mieli wystarczającą ilość czasu na wprowadzanie aktualizacji.
- Istnieje kilka środków, które dostawcy usług mogliby zastosować, by pomoc w identyfikowaniu naruszeń bezpieczeństwa i powiadamianiu o nich – na przykład mogliby zainstalować tzw. *honey-pots* (przynęty) i *honey-nets* (sieci przynęt), by namierzyć działalność hakerów i monitorować nieużywane adresy IP. ISP mógłby również mierzyć czas do momentu naruszenia dla wybranych zagrożeń w regularny sposób i udostępniać te informacje lub publikować je. To pozwoliłoby dostawcom usług koordynować strategie, nagradzać tych dostawców usług, którzy przyczyniają się do zwiększania czasu do infekcji i wystrzegać się tych, którzy tego nie robią. To pozwoliłoby krajom również, do pewnego stopnia, opisać ich stan bezpieczeństwa, zakładając, że dostawcy usług stosują środki w obrębie granic geograficznych.

Rady i propozycje

- **Dostawcy usług** powinni zacząć dobrowolnie powiadamiać KONy lub zaufane osoby trzecie o naruszeniach przy użyciu zestawu uznanych wskaźników.
- **Państwa członkowskie** powinny wspierać powiadamianie o naruszeniach bezpieczeństwa lub wymagać go.
- **UE** powinna wprowadzić szereg wytycznych i/lub przepisy, które Zachę-

całyby dostawców usług do powiadamiania o naruszeniach bezpieczeństwa, czy nawet czyniłyby z tego obowiązek.

- **ENISA** powinna rozpocząć współpracę w zakresie gromadzenia informacji o tendencjach i rozmiarach naruszeń bezpieczeństwa; przy tym sama ENISA mogłaby działać jako ośrodek wymiany i analizy informacji.
- Regulowanie rynku badań nad podatnością systemów na zagrożenia nie jest obecnie możliwe. Jednak UE musi kontrolować rozwój na rynku. Skoordynowany proces publikacji na temat podatności systemów na zagrożenia jest ważny, pozwala odnaleźć równowagę między pełnym ujawnianiem informacji (co wywiera nacisk na sprzedawców, by tworzyli aktualizacje) a kontrolowanym ujawnianiem informacji (co umożliwia w szczególności zabezpieczenie krytycznych elementów infrastruktury przed upublicznieniem słabości systemu).

3.2 Uświadamianie sobie problemu bezpieczeństwa lub spamu

Zanim dostawca może powiadomić o naruszeniu bezpieczeństwa lub problemach związanych z masowo rozsyłanym spamem, musi je sobie uświadomić. Najlepiej byłoby, gdyby dostawca zbadał źródło, przyczynę i wpływ problemu na jego własną infrastrukturę. Dostawca może aktywnie monitorować sieć lub czekać, aż ktoś powiadomi o problemie.

Uświadamianie sobie problemu bezpieczeństwa lub spamu

- 80% wszystkich e-maili stanowi spam
- Większość spamu jest obecnie wysyłana przez komputery „zombie”
- Kraje UE otrzymują więcej spamu niż wysyłają
- Sieci „zombie” stają się coraz mniejsze
- Dostawcy wciąż za bardzo polegają na skargach

Fakty i obserwacje

- Prawie dwie trzecie wszystkich e-maili **otrzymywanych** przez europejskich dostawców stanowi spam, podczas gdy **wychodzący spam** stanowi zaledwie 5% wszystkich e-maili (Ankieta ENISA 2006). Jednak niektóre sprawozdania wykazują, że ponad 20% całego spamu na świecie pochodzi z Europy (zobacz część „Środki zwalczania spamu”).
- **80% wszystkich e-maili stanowi spam**, na podstawie oceny około 390 milionów skrzynek mailowych na całym świecie. (Messaging Anti-Abuse Working Group (MAAWG) Email Metrics Program 1Q2006)
- 80% spamu jest **wysyłane przez komputery „zombie”**, zgodnie z raportem sprzedającego z 2004 roku (Sandvine). Dane te są nadal powszechnie uznawane. (Konferencja MAAWG)
- W procesie uświadamiania sobie problemów związanych ze spamem lub bezpieczeństwem dostawcy w znacznej mierze polegają na skargach subskrybentów. Ponadto dostawcy podają skargi innych dostawców jako źródło informacji. (Ankieta ENISA 2006)
- Ponad połowa dostawców informuje klientów o środkach zaradczych, jakie mogą podjąć, lecz bardzo **niewielu dostawców informuje** klientów o **kosztach**, jakie środki te pociągają za sobą. (Ankieta ENISA 2006)
- Dostawcy obserwują również więcej złośliwego oprogramowania napisanego z myślą o ataku na określone grupy użytkowników. Hakerzy planują takie złośliwe oprogramowanie tak, by miało krótką żywotność i korzystają tylko z kilkuset komputerów „zombie”, które **pozostają pod kontrolą** programów monitorujących sieć. (Konferencja MAAWG)
- Niektórzy dostawcy postrzegają informacje o oszustach itd. jako informacje zastrzeżone i konkurencyjne i nie chcą się nimi dzielić.

- Jest więcej niż sto **przechwyconych marek**, kilkaset niepowtarzalnych aplikacji o złośliwym kodzie, kradnących hasła dostępu, ponad tysiąc URL o złośliwym kodzie, kradnących hasła dostępu oraz do dziesięciu tysięcy nowych stron przechwytujących informacje w ramach phishingu każdego miesiąca. (Anti-Phishing Working Group **(**APWG), Phishing Activity Trends Report, February 2006)
- Pewni **wątpliwi administratorzy DNS** próbują również podstępem nakłonić posiadaczy domeny do zmiany administratora i zarejestrowania się u nich. Tego typu oszustwo prawie nie różni się od phishingu.
- W ICANN (*The Internet Corporation for Assigned Names and Numbers* - Internetowa Korporacja ds. Nadawania Nazw i Numerów) trwają dyskusje na temat **zamknięcia publicznego dostępu do bazy danych Whols** w celu ochrony prywatności właścicieli domen. Bazy danych Whols są ważnym pierwszym krokiem w procesie identyfikowania spamerów. Według Spamhaus nawet fikcyjne zapisy w bazie danych Whols pomagają w identyfikowaniu spamerów. (Konferencja MAAWG)

Oceny i wnioski

Zgodnie z obserwacjami ENISA stosunek spam/e-mail w Europie jest tylko trochę korzystniejszy od pomiaru MAAWG (która to grupa zdominowana jest przez Stany Zjednoczone). Dane osiągnęły wysoki poziom i skrzynka elektroniczna nie posiadająca żadnej ochrony przed spamem jest praktycznie bezużyteczna.

- Podczas gdy niektóre raporty wskazują na to, że ilość spamu pochodzącego z Europy zmniejszyła się, z innych raportów wynika, że ilość ich rośnie. Obie te wiadomości mogą być prawdziwe. Sytuacja prawna sprawia, że spamerom trudno jest ukryć się w UE. Jednak technicznie ich e-maile mogą nadal pochodzić z Europy – i coraz częściej ma to miejsce. Należy to przypisać zwiększonemu poziomowi infekcji typu botnet, którym sprzyja coraz większa liczba zryczałtowanych, stałych łączy szerokopasmowych w Europie. Oznacza to, że mimo iż spamerzy znajdują się poza UE, infrastruktura, której używają - botnety przechwyconych komputerów osobistych używanych przez konsumentów – znajduje się w państwach takich jak Francja, Hiszpania i Polska.
- Problem spamu jest wielowymiarowy. Radzenie sobie ze spamem wymaga podejścia technicznego zarówno po stronie wysyłającej (tj. w odniesieniu do botnetów), jak i po stronie otrzymującej. Do skutecznej walki ze spamerami niezbędna jest podstawa prawna, która byłaby egzekwowana i która umożliwiałaby legalny marketing bezpośredni i odbierała spamerom motywację, tj. określała kary pieniężne, które stanowiłyby prawdziwą przeciwwagę dla dochodu otrzymywanego ze spamu.
- Coraz częściej naruszanie bezpieczeństwa i spam nie są oddzielnymi kwestiami. Naruszenie ma miejsce, gdy zainfekowany załącznik do e-maila instaluje w komputerze Trojana. Z kolei spam często wysyłany jest z botnetu, który jest wynikiem kilku incydentów naruszenia bezpieczeństwa.
- Występujące i pojawiające się zagrożenia, takie jak oszustwa związane z darmowym rejestrowaniem domen na kilka dni (tzw. domain kiting) lub rejestracją domeny, szybko ewoluują (zobacz część „Określenie sposobu i kosztu wdrażania"). Aby znaleźć właściwą polityczną, prawną lub techniczną odpowiedź, Europa potrzebuje szybkich i skoordynowanych mechanizmów ostrzegania i informowania.
- Niektórzy dostawcy polegają tylko na skargach od subskrybentów. Aby zareagować w samą porę, konieczne jest bardziej aktywne podejście, polegające nie tylko na uwzględnianiu skarg od subskrybentów, ale również na ciągłym monitorowaniu ruchu. Rzeczywiście większość dostawców stosuje taką mieszaną strategię. Pokrzepiające jest to, że dostawcy reagują również na skargi innych dostawców. Jednakże stosunek pomiędzy skargami partnerów, skargami subskrybentów i problemami zidentyfikowanymi w wyniku monitoringu nie jest jeszcze jasny i wymaga dalszej analizy.

Rady i propozycje

- Jeśli chodzi o zidentyfikowanie problemu, **dostawcy** powinni polegać przede wszystkim na swoich własnych możliwościach monitorowania, w dalszej kolejności na skargach innych dostawców i dopiero na końcu na skargach subskrybentów.
- **UE** powinna popierać pozytywną

identyfikację nadawców e-maili (np. SIDF, DKIM). Dostawcy powinni wdrożyć ją tak szybko jak to możliwe w opłacalny sposób.

- Należy zachęcać **dostawców** do (jeśli nie wymagać od nich) czynnego monitorowania swoich sieci zamiast reagowania wyłącznie na skargi klientów.
- **ENISA** powinna pogłębić badania sposobów, w jakie dostawcy dowiadują się o incydentach z zakresu bezpieczeństwa i trendach związanych ze spamem.
- Należy stworzyć w **Europie** mechanizm ostrzegawczy służący do identyfikacji pojawiających się zagrożeń i radzenia sobie z nimi.

4. Definicja odpowiedniego bezpieczeństwa

Przez długi czas powszechnie uznawanym celem działań z zakresu bezpieczeństwa informacji było maksymalne podniesienie poziomu tego bezpieczeństwa. Obecnie sytuacja wygląda inaczej. Odchodzenie od zaostrzonych środków bezpieczeństwa usprawiedliwiane jest dobrem interesów, podczas gdy wciąż prawdą jest to, że cięcia w budżecie przeznaczonym na niezbędne środki zagrażają bezpieczeństwu i interesom. Ponadto środki bezpieczeństwa często są sprzeczne z prawem obywateli do prywatności. Znalezienie równowagi i udostępnienie dostawcom informacji wystarczających do podjęcia właściwej decyzji jest dziś głównym celem.

4.1 Określenie sposobu i kosztów wdrażania

Informacje dotyczące tego, co jest możliwe, właściwe i na co można sobie pozwolić, mogą pochodzić z różnych źródeł. Żadne źródło nie jest doskonałe, a zatem wszystko zależy od tego, w jakim stopniu ufa się danym i wskazówkom opracowanym przez konkretną jednostkę. Oczywiście autorytet i zasięg tej jednostki również mają znaczenie.

Fakty i obserwacje

- Większość dostawców **po prostu postępuje zgodnie z „najlepszą praktyką w branży”**. Około połowa dostawców postępuje zgodnie z międzynarodowymi normami. Krajowe przepisy i porady krajowej organizacji bezpieczeństwa komputerowego lub krajowego organu nadzorującego odgrywają mniejszą rolę. (Ankieta ENISA 2006)
- Około połowa dostawców przeprowadza wewnętrzną ocenę ryzyka, ale niewielu wdraża określony **proces zarządzania ryzykiem** lub porozumienie na poziomie usług. (Ankieta ENISA 2006)
- Wielu dostawców oferuje **bezpłatne** filtrowanie spamu. (Ankieta ENISA 2006)
- **Koszty związane z prowadzeniem linii interwencyjnych** są już bardzo wysokie i odbieranie telefonów związanych z bezpieczeństwem stanowi dodatkowe obciążenie dla dostawców. (Konferencja MAAWG)

- Kilka branżowych ankiet zawiera **dane dotyczące szkód** (np. raport FBI/CSI w Stanach Zjednoczonych, ankieta DTI w Zjednoczonym Królestwie, raport AUS/CERT w Australii, światowa ankieta Deloitte), lecz dane te różnią się znacznie i nie są porównywalne. (Raport #2982 firmy META Group)
- Eksperci ds. bezpieczeństwa często podważają **przydatność danych statystycznych dotyczących szkód** wynikających z naruszenia bezpieczeństwa. Na przykład, w raporcie Computer Security Institute (CSI) z 2006 roku stwierdzono, że koszty incydentów z zakresu bezpieczeństwa zmniejszają się, natomiast analityk rynkowy Gartner szybko zakwestionował takie dane. Nadal nie ma ogólnie akceptowanego systemu pomiaru. (CSI/Gartner)
- Większość ludzi uważa, że korzystne jest pokazywanie **pieczęci zaufania** na stronie internetowej, zgodnie z raportem z 2006 roku. (Goodmail Systems)
- Wiele nazw domen rejestrowanych jest bezpłatnie tylko na kilka dni (**'domain name kiting'**), co może prowadzić do oszustw zwanych click-fraud, polegających na klikaniu reklam internetowych w celu generowania opłat. Z drugiej strony rozstrzygnięcie sporu dotyczącego nazw domen jest bardzo złożone i kosztowne i często angażuje Światową Organizację Własności Intelektualnej (World Intellectual Property Organisation, WIPO, zobacz www.wipo.int), ICANN (zobacz www.icann.org), administratorów DNS i firmy prawnicze. A zatem, podczas gdy wielu ponosi koszty, tylko nieliczni odnoszą korzyści z tego typu oszustw.
- Ekspertyzy medycyny sądowej dotyczące spamu i incydentów związanych z bezpieczeństwem są złożone (np. utrzymanie łańcucha opieki) i często wykonalne tylko przy użyciu **drogiego** oprogramowania. Wymagają one również wysokiego poziomu kompetencji. (Konferencja MAAWG)

Oceny i wnioski

- Chociaż opublikowano różne sprawozdania dotyczące kosztu środków bezpieczeństwa (i potencjalnego kosztu nie wdrażania ich), nadal nie ma wspólnej podstawy dokonywania pomiarów, a tym samym sposobu porównywania różnych danych.
- W gospodarce globalnej sposób dbania o bezpieczeństwo informacji ewoluuje na poziomie międzynarodowym. Inicjatywy krajowe powinny raczej koncentrować się na współpracy niż konkurencji w dziedzinie najbardziej odpowiednich środków.
- Decyzję odnośnie do tego, czy dane środki są opłacalne i odpowiednie można podjąć tylko w określonym kontekście. Na przykład, większość dostawców uznała za właściwe sponsorowanie filtrowania antyspamowego, usiłując zdobyć i utrzymać zaufanie klientów i udział w rynku.
- Inwestycja w bezpieczeństwo informacji powinna stanowić dodatkową zaletę dostawcy, lecz w wielu przypadkach dostawcy nie pokazują i nie sprzedają tej zalety w odpowiedni sposób. Pieczęć lub świadectwo zaufania pomaga w zapewnieniu subskrybenta o wiarygodności usługi i uzasadnieniu realizowanych inwestycji.
- Stosowność środków i kosztów związanych z bezpieczeństwem informacji jest ruchomym celem. Stosowanie metodologii zarządzania ryzykiem nie zapewnia bezpośrednio odpowiedzi, ale pomaga w znalezieniu rozwiązań i sprawia, że proces może być powtarzalny.

Rady i propozycje

- Jeśli chodzi o dyskusje dotyczące zarządzania Internetem, **Komisja Europejska** powinna mieć świadomość istniejącego konfliktu pomiędzy prostą rejestracją nazwy domeny (pomagającą w rozwoju rynku) i szczegółową rejestracją nazwy domeny (pomagającą w zwalczaniu phishingu i masowego rozsyłania spamu).
- **UE** mogłaby zachęcić do badań i innych projektów, które wspierają rozwój i rozpowszechnianie narzędzi dochodzeniowych.
- **UE** mogłaby pomóc w przeanalizowaniu pewnych aspektów strategii bezpieczeństwa wdrażanych przez państwa europejskie w celu zwiększenia ogólnej wydajności w całej Europie.
- **ENISA** powinna nadal zapewniać wskazówki dotyczące metodologii oceny ryzyka i zarządzania ryzykiem (zobacz *Implementation Principles and Inventories for Risk Management/Risk Assessment*, czerwiec 2006).
- **Państwa członkowskie** powinny wspierać i promować stosowanie metodologii oceny ryzyka i zarządzania ryzykiem, aby pomóc w lepszym

zrozumieniu stosunku kosztów do korzyści w dziedzinie bezpieczeństwa informacji.

4.2 Bezpieczeństwo poczty elektronicznej a prywatność

Główną zasadą prywatności jest bezpieczne przechowywanie i przekazywanie danych. Nikt nie powinien mieć dostępu do osobiście zaadresowanych informacji oprócz odbiorcy. Lecz co się dzieje wówczas, gdy odbiorca nie chce mieć dostępu do tych informacji? Tak jak w przypadku zasady nieoznaczoności Heisenberga, zgodnie z którą nie można z dowolną dokładnością wyznaczyć jednocześnie położenia i pędu cząsteczki, podobnie niemożliwe jest sprawdzanie prywatnych e-maili pod kątem bezpieczeństwa, bez naruszania prawa osoby fizycznej do prywatności, przynajmniej w pewnej mierze.

Bezpieczeństwo poczty elektronicznej a prywatność

- Istnieje konflikt pomiędzy obowiązkami ISP i prywatnością
- Blokowanie prywatnych komputerów jest często uznawane za nielegalne
- Opinia Grupy Roboczej Art. 29 dopuszcza głównie filtrowanie
- Dostawcy chcieliby uzyskać więcej informacji na temat przepisów dotyczących spamu

Fakty i obserwacje

- Prawie dwie trzecie dostawców odpowiedziało, że uważają, iż istnieje konflikt pomiędzy obowiązkami ISP w zakresie dostarczania wiadomości/ ochrony prywatności i stosowaniem filtrów spamu, które blokują pewne wiadomości. (Ankieta ENISA 2006)
- Zwalczanie botnetów przysparza dostawcom problemów, gdyż blokowanie legalnych łączy, opłacanych przez konsumentów, którzy nie są świadomi infekcji swoich prywatnych komputerów, może stanowić naruszenie przepisów dotyczących prywatności i często uważane jest za nielegalne.
- Grupa Robocza Art. 29 omówiła temat równowagi pomiędzy prywatnością i bezpieczeństwem w Opinii 2/2006 (WP118). Mówiąc w skrócie, filtrowanie poczty elektronicznej jest dozwolone pod pewnymi warunkami w bardziej oczywistych przypadkach (tj. ochrona przed wirusami i spamem), lecz w innych rozwijających się dziedzinach (np. usługi na indywidualne zlecenie) konieczna jest bardziej dogłębna analiza. (Opinia Grupy Roboczej Art. 29)
- Umożliwienie subskrybentom wycofania się (opt-out) z filtrowania jest wyzwaniem od strony technicznej. Jeśli filtrowanie wdrażane jest w szkielecie sieci na poziomie IP, dostawca albo przepuszcza wszystkie e-maile z przefiltrowanej sieci (w tym spam), albo subskrybent nie może otrzymywać żadnej poczty z tej sieci. Sprecyzowane filtrowanie (tj. polegające na przepuszczaniu e-maili przychodzących z konkretnego adresu) jest wykonalne jedynie wówczas, gdy użytkownikowi wolno zobaczyć wszystkie e-maile, co jest bardzo kosztowne dla dostawcy, który musi przenieść wszystkie e-maile (w tym spam) i zapewnić mechanizm otrzymywania/odrzucania określonych e-maili. (Konferencja MAAWG)
- Większość dostawców chciałaby uczestniczyć w warsztatach, na których uzyskaliby informacje o przepisach i problemach prawnych dotyczących spamu. (Ankieta ENISA 2006)

Oceny i wnioski

- Zwalczanie spamu wiąże się z filtrowaniem, lecz obowiązkiem Dostawców jest dostarczanie e-maili. Jeśli chcą pomóc klientom, ponoszą stałe ryzyko postępowania niezgodnie z prawem.
- Niektórzy dostawcy nieoficjalnie poinformowali ENISA, że nie chcą odpowiadać na naszą ankietę, ponieważ zawarte w niej pytania są kłopotliwe. Powiedzieli również, że filtrują e-maile, lecz nie chcą, aby wiedzieli o tym klienci.
- Zawsze będzie istniał konflikt pomiędzy „ochroną osoby fizycznej" (prywatność) a „ochroną przed osobą fizyczną" (bezpieczeństwo), lecz istnieją różne rozwiązania umożliwiające znalezienie równowagi pomiędzy tymi dwiema kwestiami. Zanim Grupa Robocza Art. 29 wydała opinię, zakres rozwiązań prawnych nie był jasny, co powodowało niepewność dostawców.
- Zadanie rozwiązania problemu prawnych sprzeczności nie należy do dostawców; potrzebują oni jasnych wskazówek mówiących o tym, co jest, a co nie jest dozwolone. Opinia 2/2006 opublikowana w lutym 2006 roku w dużej mierze wyjaśnia prawne aspekty filtrowania. Wydaje się, że dokument Grupy Roboczej Art. 29 dotyczący ochrony poczty elektronicznej nie jest jeszcze dobrze znany.

Rady i propozycje

- **Dostawcy** powinni wziąć pod uwagę Opinię 2/2006 dotyczącą ochrony poczty elektronicznej.
- **ENISA** powinna promować stanowisko opisane w Opinii 2/2006 i mogłaby zorganizować warsztaty poświęcone przepisom i prawnym aspektom Dotyczącym spamu.
- **ENISA** powinna zachęcić państwa członkowskie do pogłębiania wiedzy obywateli na temat blokowania osobistych komputerów w tym sensie, że brak możliwości uzyskania połączenia z Internetem może być spowodowany złośliwą infekcją komputera należącego do obywatela.
- **UE** powinna promować Opinię 2/2006 dotyczącą ochrony e-maili i zapewnić dalsze objaśnienia odnośnie do tego, kiedy filtrowanie treści jest dozwolone, opierając się na opinii Grupy Roboczej Art. 29.
- **UE** (a dokładnie Grupa Robocza Art. 29) i dostawcy powinni rozpocząć rozmowy mające na celu znalezienie równowagi pomiędzy kosztami i skutecznością ukierunkowanego filtrowania z opcją opt-out.

5. Tworzenie standardów

Określenie odpowiednich środków jest często zbyt trudne lub kosztowne. Zamiast tego dostawcy przyglądają się temu, co robią inni, mając nadzieję, że uśrednione rozwiązanie będzie zarówno opłacalne, jak i odpowiednie z perspektywy bezpieczeństwa informacji. Jeśli coś się nie powiedzie, sądy i opinia publiczna przynajmniej potwierdzą próbę usilnych starań.

5.1 Techniczne i organizacyjne środki bezpieczeństwa

Dostawcy muszą zabezpieczyć swoje usługi, ale w znacznej mierze to oni decydują o szczegółach. Techniczne środki bezpieczeństwa mogą odnosić się do urządzenia użytkownika końcowego lub infrastruktury sieciowej znajdującej się w siedzibie dostawcy. Środki organizacyjne mogą mieć

wpływ na wszystkie zainteresowane strony i mogą obejmować zarówno jednokierunkowe informacje, jak i wielostronną współpracę.

Techniczne i organizacyjne środki bezpieczeństwa

- Większość dostawców stosuje różne techniki
- Nacisk kładziony jest na ochronę własnej sieci
- W Szwecji stosuje się DNSSEC
- Dostawcy poddają kwarantannie zainfekowane komputery
- Użytkownicy postępują bardziej nierozważnie w pracy

Fakty i obserwacje

- Większość **dostawców stosuje kombinację** od 3 do 5 różnych technik ochrony. (Ankieta ENISA 2006)
- Filtrowanie pakietów wychodzących z sieci (ochrona innych sieci) jest znacznie rzadziej stosowane niż filtrowanie pakietów przychodzących (**ochrona własnej sieci)** Większość dostawców oferuje dane kontaktowe na wypadek nadużycia poczty elektronicznej; około 15 % dostawców nie praktykuje tego. (Ankieta ENISA 2006)
- W Szwecji stosuje się **DNSSEC**, rosyjska domena najwyższego poziomu .RU jest podpisana, natomiast w Meksyku i Holandii przeprowadzono testy (zobacz www.dnssec.net/news oraz www.ripe.net/disi
- Dwie trzecie dostawców **poddaje kwarantannie zainfekowane komputery**. (Ankieta ENISA 2006)
- Około połowa dostawców stosuje rozwiązanie Business Contingency lub Disaster Recovery (często wprowadzane przez firmowe wymogi zarządzania). Jednak dostawcy przyznają, że rozwiązania te są rzadko testowane. (Ankieta ENISA 2006)
- Tylko połowa dostawców **informuje subskrybentów regularnie** i szczegółowo, np. przy pomocy pisemnych wskazówek lub regularnych informacji umieszczanych na stronie internetowej, wysyłanych pocztą elektroniczną lub tradycyjną pocztą. (Ankieta ENISA 2006)
- W Stanach Zjednoczonych 48 % pracowników przyznaje, że prędzej otworzą podejrzane e-maile lub strony internetowe **w komputerach w pracy niż w domu**, powiedziało, że jest to spowodowane tym, że w pracy jest dział IT, który może pomóc im, gdy stanie się coś złego. Niemcy (39%) i Japonia (28%) odnotowały podobne wyniki. (studium Trend Micro, 2005)
- Wielu oszustów **nie obawia się odkrycia ich tożsamości**, ponieważ często żyją w krajach, w których nie spodziewają się kary.

Oceny i wnioski

- Środki zaradcze zależą od rodzaju firmy, wielkości i dojrzałości dostawcy. Zależą również od rodzaju klienta, na którym skupiają się działania dostawcy. Klienci firmowi (którzy często wymagają pewnej niezależności w działaniu) mają inne wymagania niż konsumenci (którzy często szukają najtańszej usługi). Rozróżnienie pomiędzy klientami firmowymi a konsumentami może być problematyczne w przypadku małych przedsiębiorstw, które często postępują tak jak konsumenci (brak wiedzy na temat bezpieczeństwa), ale jednocześnie wymagają wydajności na poziomie firm (stałe łącze).
- Ponieważ wielu dostawców w kwestii uświadamiania sobie problemów związanych z bezpieczeństwem polega na skargach klientów, większość z nich udostępnia klientom dane kontaktowe.
- Dostawcy nadal nie podchodzą wystarczająco poważnie do szkolenia i pogłębiania wiedzy oraz rzadko oferują kursy. Można by stwierdzić, że nie leży to w gestii dostawców infrastruktury, choć mają ku temu odpowiednie warunki, biorąc pod uwagę to, że utrzymują kontakt z dużą liczbą użytkowników Internetu. Oni również skorzystaliby z wykształcenia użytkowników dzięki zmniejszeniu zagrożenia złośliwych incydentów u tych użytkowników.

- Alternatywnym rozwiązaniem jest kontrola rządowa. Przykłady w niektórych krajach udowodniły, że w eHandlu odnosi się korzyści, gdy użytkownicy umieją korzystać z nowej technologii (np. wprowadzenie karty eID w Belgii).
- Wdrożenie w kraju DNSSEC jest procesem złożonym, a ogólna penetracja DNSSEC jest niska.

Środki zwalczania spamu

- Wiele środków zaradczych ma charakter prawny.
- W UE obowiązują przepisy antyspamowe
- Dostawcy obawiają się procesów sądowych ze strony spamerów
- Dostawcy odrzucają bezpośrednie SMTP
- Dane statystyczne są zróżnicowane
- Opublikowano OECD Anti-Spam Toolkit
- Istnieje kilka kodeksów postępowania dla dostawców

Rady i propozycje

- ENISA – przy współpracy z dostawcami powinna stworzyć platformę wymiany informacji o środkach zabezpieczających komunikację elektroniczną.
- UE i ENISA powinny promować określone środki, takie jak poddawanie komputerów kwarantannie (zgodnie z przepisami o prywatności), dostępność danych kontaktowych w związku z kwestią bezpieczeństwa i na wypadek nadużycia poczty elektronicznej, filtrowanie i DNSSEC.
- Konsumenci potrzebują więcej indormacji i lepszego szkolenia z zakresu określonych kwestii związanych z bezpieczeństwem. Najlepszym sposobem zapewnienia informacji i szkoleń o możliwie najszerszym zasięgu byłyby partnerstwa publiczno-prywatne zrzeszające jednostki rządowe i dostawców.

5.2 Środki zwalczania spamu

Początkowo spam uznawano wyłącznie za uciążliwość, a nie problem związany z bezpieczeństwem. Jednakże zmieniający się krajobraz zagrożeń (en. threatscape) sprawia, że kwestionuje się to założenie, w miarę jak phishing, spyware i botnety (zwane również crimeware) rozprzestrzeniają się drogą poczty elektronicznej i często są nie do odróżnienia od zwykłego spamu. Do złożonego charakteru krajobrazu zagrożeń przyczynia się również masowe rozsyłanie spamu w telefonii (spamming in telephony – SPIT) i komunikacji Nawychmiastowej (spamming in instant messaging - SPIM).

Fakty i obserwacje

- Większość środków podejmowanych przez dostawców w celu zapobiegania rozsyłaniu przez subskrybentów spamu ma **charakter prawny**, np. „zakazanie masowego rozsyłania spamu zgodnie z warunkami" oraz „informowanie subskrybentów o prawnych konsekwencjach masowego rozsyłania spamu". Najczęściej stosowaną techniką ograniczania spamu w otrzymywanej poczcie elektronicznej jest korzystanie z czarnej listy. (Ankieta ENISA 2006)
- Prawie we wszystkich krajach UE obowiązują **przepisy antyspamowe**. Jednakże na poziomie międzynarodowym tylko w 23% krajów wcielono przepisy antyspamowe, natomiast 64% krajów nie ma takich przepisów. (Ankieta Międzynarodowego Związku Telekomunikacyjnego (International Telecommunications Union, ITU) dotycząca przepisów antyspamowych na świecie)
- Czasem dostawcy **obawiają się procesów sądowych ze strony spamerów** na skutek blokowania ich działań. W niektórych rozwijających się krajach egzekwowanie prawa (antyspamowego) postrzega się jako trudne, gdyż kraje te nie mają wystarczających kompetencji dochodzeniowych. (Konferencja MAAWG)
- W dziewięciu krajach europejskich **nałożono kary pieniężne** na spamerów, wynoszące od około jednego tysiąca euro do dziesięciu tysięcy euro (z wyjątkiem dwóch bardzo niskich kar). (CNSA)
- Niektórzy dostawcy przyznają, że wśród ich **klientów są spamerzy**. (Ankieta ENISA 2006)
- Statystyki sprzedawców oprogramowania filtrującego dotyczące spamu są bardzo zróżnicowane i szybko się zmieniają. Często na liście krajów rozsyłających znajduje się tylko kilka państw członkowskich UE (np. www.Spamhaus.org, 21.06.2006, tylko Zjednoczone Królestwo na miejscu #8, odpowiadające za 3% spamu), natomiast dłuższa jest lista krajów otrzymujących spam (np. cztery kraje UE otrzymują 21% spamu rozsyłanego na całym świecie, na podstawie danych Trend Micro, czerwiec 2006). We wszystkich przypadkach Stany Zjednoczone są na pierwszym miejscu.
- 25% **dostawców odrzuca bezpośrednie połączenia SMTP**. Liczba ta rośnie, w miarę jak coraz więcej dostawców decyduje się na „zarządzanie" portem 25. Bardzo wielu dostawców oferuje bezpłatne filtrowanie antyspamowe w swojej sieci, niektórzy oferują je odpłatnie, około 20% nie oferuje żadnego oprogramowania filtrującego (ani za opłatą, ani bezpłatnie). Kanadyjscy dostawcy również z powodzeniem stosowali tę metodę ograniczania spamu.
- W 2006 roku Organizacja Współpracy Gospodarczej i Rozwoju (OECD) opublikowała **OECD Anti-Spam toolkit.** Dokument ten zawiera zalecenia dotyczące środków z zakresu kontroli, egzekwowania przepisów, inicjatywy sterowanej przemysłem, technologii, kształcenia i świadomości, partnerstwa opartego na współpracy, pomiaru spamu i globalnej współpracy. (OECD Anti-Spam toolkit)
- BIAC (Komitet doradczy ds. biznesu i przemysłu) w połączeniu z MAAWG (w ramach OECD toolkit), Australia, Finlandia i Włochy (oraz inne kraje) opracowały dla dostawców **kodeksy postępowania** dotyczące zwalczania spamu.
- Choć miały miejsce **inicjatywy związane z białymi listami** w związku z marketingiem bezpośrednim poprzez pocztę elektroniczną (np. Certified Sender Alliances zainicjowane przez eco w Niemczech), większość sprzedawców stosujących taki marketing radzi sobie z tą kwestią, rozpatrując konkretne przypadki.
- **Techniki uwierzytelniania nadawcy,** takie jak SIDF i DKIM, łączą adres IP lub wiadomość z nazwą domeny. Choć techniki te mają wady (spamerzy też je stosują, aby uwierzytelnić swoje e-maile), stanowią część rozwiązania problemu i można je uzupełnić systemami opiniowania przez użytkowników. Uwierzytelnianie nadawcy znalazło już swoje zastosowanie; przede wszystkim duża liczba nadawców e-maili może być objęta rekordami zawierającymi informacje uwierzytelniające dla popularnych domen takich jak eBay, Yahoo, Hotmail, Gmail, PayPal. Gdy takie firmy zwrócą się do swoich klientów o pomijanie wszystkich e-maili z ich domeny, które nie są podpisane, wywrze to większy nacisk na inne firmy, aby również zastosowały uwierzytelnianie nadawcy. (Konferencja MAAWG)
- UE zainicjowała sieć kontaktową krajowych organów odpowiedzialnych za walkę ze spamem (Contact Network of Spam Authorities - **CNSA**), zrzeszając, w zależności od kraju, organy ochrony danych i krajowe organy nadzorujące. CNSA dysponuje informacjami na temat pojawiających się problemów, powiadomień o spamie oraz prowadzonych spraw sądowych dotyczących spamu. Dotychczas przyłączyło się 21 krajów. CNSA jest podobna do Londyńskiego Planu Przeciwdziałania Spamowi (London Action Plan – LAP), światowej inicjatywy prowadzonej przez Zjednoczone Królestwo i Stany Zjednoczone. CNSA i LAP ściśle współpracują ze sobą.
- Jest kilka **inicjatyw związanych z gromadzeniem danych dotyczących spamu**. „Spotspam" jest inicjatywą finansowaną przez UE, podjętą przez niemieckie stowarzyszenie eHandlu (eCommerce – eco) wspólnie z polską Naukową i Akademicką Siecią Komputerową (NASK). „Signal Spam" jest analogicznym projektem we Francji, wspieranym przez kilka francuskich ministerstw. Ostatnio podpisano Memorandum Porozumienia pomiędzy obiema inicjatywami. Digital Phishnet jest inicjatywą podjętą przez Stany Zjednoczone.
- W niektórych krajach **zgłaszanie spamu jest uciążliwe**, np. różne organy są odpowiedzialne za różne rodzaje spamu lub skargi można składać jedynie tradycyjną pocztą. Z drugiej strony w Holandii zgłaszanie spamu ułatwiono dzięki formularzowi internetowemu, w wyniku czego organy otrzymują dużą liczbę zgłoszeń. (CNSA)
- Powiadamianie o spamie przez konsumentów stanowi problem. Nawet jeśli proces zgłaszania jest ułatwiony, prostszym rozwiązaniem jest usuwanie spamu. **Spadek** liczby powiadomień o spamie **nie oznacza spadku ilości spamu**. (CNSA)

Oceny i wnioski

- Ilość spamu przychodzącego do Europy kształtuje się na poziomie wyższym niż średni, a jednocześnie państwa europejskie są rzadziej źródłem pochodzenia spamu. Jednakże sytuacja może się zmienić. Spamerzy coraz częściej wykorzystują botnety do rozsyłania spamu z krajów europejskich. Są one instalowane w osobistych komputerach konsumentów, które są wyposażone w stałe łącze szerokopasmowe.
- Sytuacja ze spamem jest analogiczna do sytuacji związanej z zaporami sieciowymi w początkowym etapie stosowania ich. Wówczas pierwsza strategia stosowania zapór sieciowych polegała na blokowaniu całego złośliwego ruchu, podobnie jak w przypadku czarnych list spamerów. Takie podejście sprawdza się, pod warunkiem, że rodzaj i wielkość złośliwego ruchu są rozumiane i dają się kontrolować. Później strategia związana z zaporami sieciowymi zmieniła się z default-allow (domyślne umożliwianie wszystkich połączeń) na default-deny (domyślne odrzucanie wszystkich połączeń), co przypomina filtrowanie na zasadzie białej listy i uwierzytelnianie poczty elektronicznej.
- Dostępne są szczegółowe techniczne i organizacyjne wskazówki dotyczące zwalczania spamu.
- Z perspektywy prawnej spam pochodzący z Europy nie jest problemem; problem stanowi brak przepisów antyspamowych i egzekwiowania tych przepisów poza Europą. W obrębie Europy bardziej istotny jest konflikt prawny pomiędzy poufnością komunikatów (prywatność) a filtrowaniem komunikatów (bezpieczeństwo).
- Należy zauważyć, że spam nie jest po prostu problemem dostawców usług internetowych. Jest to raczej cały ekosystem składający się z dużych i małych dostawców połączeń, firm hostingowych wynajmujących aplikacje i platformy, DNS, dostawców poczty elektronicznej i innych usług. Zmiany techniczne i prawne wpływają na cały ten system.

Rady i propozycje

- **Dostawcy** powinni skoncentrować się na zwiększaniu współdziałania i standaryzacji, zwłaszcza w zakresie mechanizmów uwierzytelniania nadawcy.
- **Dostawcy** powinni zarządzać połączeniami SMTP poprzez port 25.
- **Państwa członkowskie** powinny pomóc w wykształceniu użytkowników końcowych w dziedzinie problemów i rozwiązań dotyczących spamu. Można by to zrealizować na poziomie państw członkowskich, w połączeniu z inicjatywą i2010 i eAdministracją.
- Kampanie w ramach szerzenia wiedzy, organizowane przez **państwa członkowskie** również powinny podkreślać fakt, iż zgłaszanie spamu ma wpływ na zwalczanie go.
- **ENISA** powinna promować korzystanie ze „Spotspam” i analogicznych projektów.
- Zważywszy na liczbę dostępnych poradników dotyczących najlepszych praktyk, **ENISA** wyłącznie podsumuje najlepsze praktyki i w inny sposób odniesie się do istniejących poradników.

6. Załącznik

6.1 Terminy i definicje

Czarna lista	Czarna lista to mechanizm kontroli dostępu, który oznacza wpuszczanie każdego poza członkami czarnej listy. Źródło: Wikipedia
Filtrowanie treści	Filtrowanie treści to najbardziej rozpowszechniony zespół metod filtrowania w kontekście problemów związanych z bezpieczeństwem (np. wirusy). Działanie filtrów treści obejmuje albo treść, tzn. informacje zawarte w samym e-mailu, albo nagłówki e-maili (takie jak „Temat") i ma na celu klasyfikację, przyjęcie lub odrzucenie e-maila. Źródło: Wikipedia/ENISA
DKIM	Domain Keys Identified Mail (DKIM) zapewnia metodę potwierdzania tożsamości przypisywanej określonej wiadomości w momencie, kiedy wiadomość ta przekazywana jest przez Internet. Tożsamość ta może być wówczas odpowiedzialna za wiadomość. Źródło: http://mipassoc.org/dkim/
DNSSEC	DNSSEC (DNS Security Extensions) zwiększa bezpieczeństwo DNS (Domain Name System – System Nazw Domenowych) używanego w sieciach IP. Stanowi on zbiór rozszerzeń DNS, które zapewniają uwierzytelnianie źródła danych DNS, integralność danych i uwierzytelnione zaprzeczenie istnienia (tj. uwierzytelnioną odpowiedź o nieistnieniu). DNSSEC zaprojektowano w celu ochrony Internetu przed pewnymi atakami, takimi jak zatruwanie DNS. Wszystkie odpowiedzi w DNSSEC są cyfrowo podpisywane. Sprawdzając podpis, DNS jest w stanie sprawdzić, czy informacje są identyczne (poprawne i kompletne) z informacjami na autorytatywnym serwerze DNS. Źródło: Wikipedia, w oparciu o RFC 4033-4035
Sieć łączności elektronicznej	Sieć łączności elektronicznej oznacza systemy transmisyjne, oraz stosownie do okoliczności, urządzenia przełączające i routingowe oraz inne zasoby, które umożliwiają przekazywanie sygnałów przewodowo, za pomocą radia, środków optycznych lub innych elektromagnetycznych środków, w tym sieci satelitarnych, stacjonarnych (komutowanych i pakietowych, w tym Internetu) i naziemnych sieci przenośnych, elektrycznych systemów kablowych, w takim zakresie, w jakim są one wykorzystywane do przekazywania sygnałów, w sieciach nadawania radiowego i telewizyjnego oraz sieciach telewizji kablowej, niezależnie od rodzaju przekazywanej informacji. Źródło: Dyrektywa 2002/21/WE
Usługa łączności elektronicznej	Usługa łączności elektronicznej oznacza usługę zazwyczaj świadczoną za wynagrodzeniem, polegającą całkowicie lub częściowo na przekazywaniu sygnałów w sieciach łączności elektronicznej, w tym usługi telekomunikacyjne i usługi transmisyjne świadczone poprzez sieci nadawcze; nie obejmuje jednak usług związanych z zapewnianiem albo wykonywaniem kontroli treści przekazywanych przy wykorzystaniu sieci lub usług łączności elektronicznej. Spod zakresu niniejszej definicji wyłączone są usługi społeczeństwa informacyjnego w rozumieniu art. 1 dyrektywy 98/34/WE, jeżeli nie polegają one całkowicie lub częściowo na przekazywaniu sygnałów w sieciach łączności elektronicznej. Źródło: Dyrektywa 2002/21/WE
Środki	Środki bezpieczeństwa informacji ograniczające wpływ spamu i innego złośliwego oprogramowania oraz zabezpieczające usługi komunikacji elektronicznej. Źródło: własna definicja ENISA
Opt-in	Dopuszczanie niechcianych wiadomości dla celów marketingu

	bezpośredniego wyłącznie za zgodą subskrybenta. Źródło: własna definicja ENISA
Opt-out	Dopuszczanie niechcianych wiadomości dla celów marketingu bezpośredniego, o ile subskrybent nie wyraził życzenia, aby nie otrzymywać tych wiadomości. Źródło: własna definicja ENISA
Dostawcy	Dostawcy sieci i usług łączności elektronicznej, tacy jak dostawcy usług internetowych (Internet Sernice Providers – ISP), firmy telekomunikacyjne, dostawcy hostingu i podobnych usług. Źródło: własna definicja ENISA
Poddawanie komputera kwarantannie	Poddawanie komputera kwarantannie oznacza odizolowanie komputera w specjalnej sieci, dopóki nie osiągnie pewnego poziomu bezpieczeństwa. Aktualizacje antywirusowych plików sygnatur lub patche są udostępniane do zainstalowania. Źródło: własna definicja ENISA
Sender ID	Sender ID potwierdza pochodzenie poczty elektronicznej poprzez weryfikację adresu IP nadawcy w porównaniu z rzekomym właścicielem domeny wysyłającej. Źródło: Microsoft
SIDF	Sender ID Framework (SIDF) jest protokołem technologii uwierzytelniania poczty elektronicznej łączącym Sender Policy Framework (SPF) z Sender ID firmy Microsoft w jeden standard. Źródłó: Microsoft
Sender Policy Framework (SPF)	Sender Policy Framework (SPF) jest rozszerzeniem SMTP (Simple Mail Transfer Protocol), standardowego protokołu internetowego służącego do przekazywania poczty elektronicznej. Źródło: Wikipedia
Biała lista	Biała lista jest mechanizmem kontroli dostępu, który oznacza brak dostępu dla kogokolwiek poza członkami białej listy. Źródło: Wikipedia
Zombie	Zombie to komputer podłączony do Internetu, który został zainfekowany przez hakera, wirus komputerowy lub konia trojańskiego. Zazwyczaj zainfekowane urządzenie jest tylko jednym z wielu w „botnecie" i wykorzystywany jest do różnego rodzaju złośliwych działań zdalnie kontrolowanych. Większość właścicieli komputerów zombie jest nieświadoma, że ich system wykorzystywany jest w ten sposób. Ponieważ wektor zazwyczaj jest nieświadomy, komputery te są przenośnie nazywane zombie. Źródło: Wikipedia

6.2 Lista odniesień

Ankieta ENISA 2006 (Survey on Industry Measures) – ankieta dotycząca środków branżowych podejmowanych w celu stosowania się do krajowych środków wdrażających Przepisy ram regulacyjnych dla sieci i usług łączności elektronicznej w związku z ubezpieczeń-stwem usług (ENISA/TD/SP/06/0055, luty 2006) - www.enisa.eu.int/doc/pdf/deliverables/enisa_security_spam.pdf

OECD Anti-Spam Toolkit – dokument opublikowany przez Organizację Współpracy Gospodarczej i Rozwoju (OECD), Grupę Roboczą ds. Spamu – kwiecień 2006 - www.oecd-antispam.org/

Grupa Robocza Art. 29 – Opinia 2/2006 (WP118) - http://ec.europa.eu/iustice_home/fsi/privacy/docs/wpdocs/ 2006/wp118 en.pdf

Contact Network of Spam Authorities (CNSA), - http://europa.eu.int/rapid/pressReleasesAction.do?reference=1P/05/146&format=HTML&aged=0&language=EN&guiLanguage=en

Ankieta ITU dotycząca przepisów antyspamowych na świecie (ITU Survey on Anti-Spam legislation worldwide) - www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf

Konferencja MAAWG - www.maawg.org

Raport **MAAWG Metrics -** www.maawg.org/about/FINAL_1Q2006_Metrics_Report.pdf

Sprawozdanie APWG dotyczące trendów w phishingu (APWG Phishing Activity Trends Report), luty 2006 - www.antiphishing.org/reports/apwg_report_feb_06.pdf

Sprawozdanie DTI dotyczące naruszania bezpieczeństwa (DTI Report on Security Breaches) - www.pwc.com/extweb/pwcpublications.nsf/docid/7FA80D2B30A116D7802570B9005C3D16

Raport Computer Security Institute (CSI) i FBI dotyczący Ankiety o przestępczości i bezpieczeństwie komputerowym (**Computer Security Institute and FBI report on Computer Crime and Security Survey**) - www.gocsi.com/

Komentarz Gartnera na temat raportu CSI (**Gartner comment on CSI report**)- www.gartner.com/DisplayDocument?doccd=141622

Raport # 2982 firmy META Group (META Group Research Note #2982) **-** www.metagroup.com/us/displayArticle.do?oid=48913

Raport firmy Symantec dotyczący zagrożeń internetowych 302006 (Symantec's Internet Threat Report 302006) **-** www.symantec.com/enterprise/threatreport/index.jsp

Studium firmy Trend Micro – Odkrycia dotyczące ryzykownego zachowania użytkownika końcowego w związku z korzystaniem z Internetu w pracy (End-User Revelations About Risky Online Behavior at Work), opublikowane w 2005 roku - www.trendmicro.com/en/about/news/pr/archive/2005/pr09_1305.htm

Sandvine – Analiza trendów związanych ze spamem/ trojanem (Spam/Trojan Trend Analysis), 2004 - www.theregister.co.uk/2004/06/04/trojan_spam_study

Ekonomiczne konsekwencje dzielenia się informacjami z zakresu bezpieczeństwa (**The Economic Consequences of Sharing Security Information)** - Esther Gal-Or & Anindya Ghose, 2005. Industrial Organisation 0503004, EconWPA- http://ideas.repec.org/p/wpa/wuwpio/0503004.html - 2005

Goodmail Systems - www.goodmailsystems.com/certifiedmail/

6.3 Dodatkowe odnośniki

Najlepsza praktyka

- Dobra praktyka w dziedzinie zwalczania masowo rozsyłanej niechcianej poczty elektronicznej
- www.ripe.net/docs/spam.html
- Najlepsza praktyka MAAWG and APWG w zakresie antyphishingu
- www.maawg.org/about/publishedDocuments/Anti_Phishing_Best_Practice.pdf
- Najlepsze praktyki BIAC i MAAWG dla ISP
- www.oecd-antispam.org/article.php3?id_article=232

Statystyki

- Statystyki MAAWG – www.maawg.org/about/FINAL_1Q2006_Metrics_Report.pdf
- Spamhaus – www.spamhaus.org/statistics/countries.lasso
- Trend Micro – www.trendmicro.com/spam-map/default.asp
- Sophos – www.sophos.com/pressoffice/news/articles/2006/07/dirtydozjul06.html

Inne

- Portal Cybersecurity Gateway Międzynarodowego Związku Telekomunikacyjnego (ITU) - www.itu.int/cybersecurity/
- Organizacja Anti-Phishing Working Group (APWG) – www.antiphishing.org/
- Organizacja Digital PhishNet – www.digitalphishnet.org

Adnotacja prawna

ENISA - European Network and Information Security Agency

P.O. Box 1309

71001 Heraklion

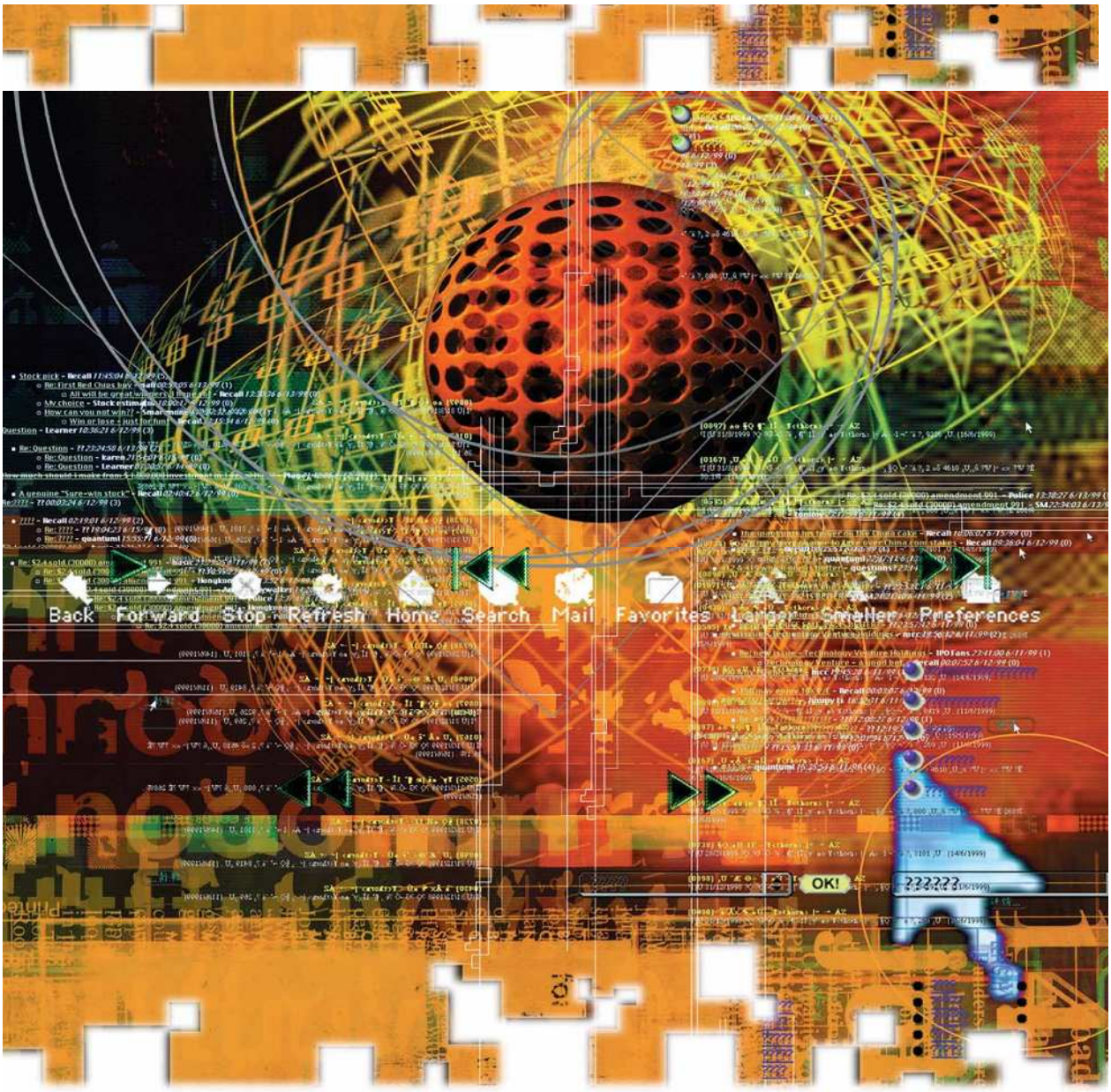
Crete

Greece

Tel.: +30 28 10 39 1280

Faks: +30 28 10 39 1410

E-mail: info@enisa.europa.eu



Provider Security Measures Part 2

Security and Anti-Spam Measures of Electronic Communication Service Providers - Status and Outlook

Deliverable 4.2.b of ENISA's Work Program 2006
ENISA/TD/SP/06/118

Carsten Casper & Pascal Manzano

European Network and Information Security Agency
Technical Department – Section Security Policies

June 2006

enisa
European Network and Information Security Agency

ENISA – European Network and Information Security Agency
P.O. Box 1309
71001 Heraklion
Crete
Greece

Tel: +30 28 10 39 1280
Fax: +30 28 10 39 1410
Email: info@enisa.europa.eu