Zaufanie i bezpieczeństwo w Europejskiej Agendzie Cyfrowej.

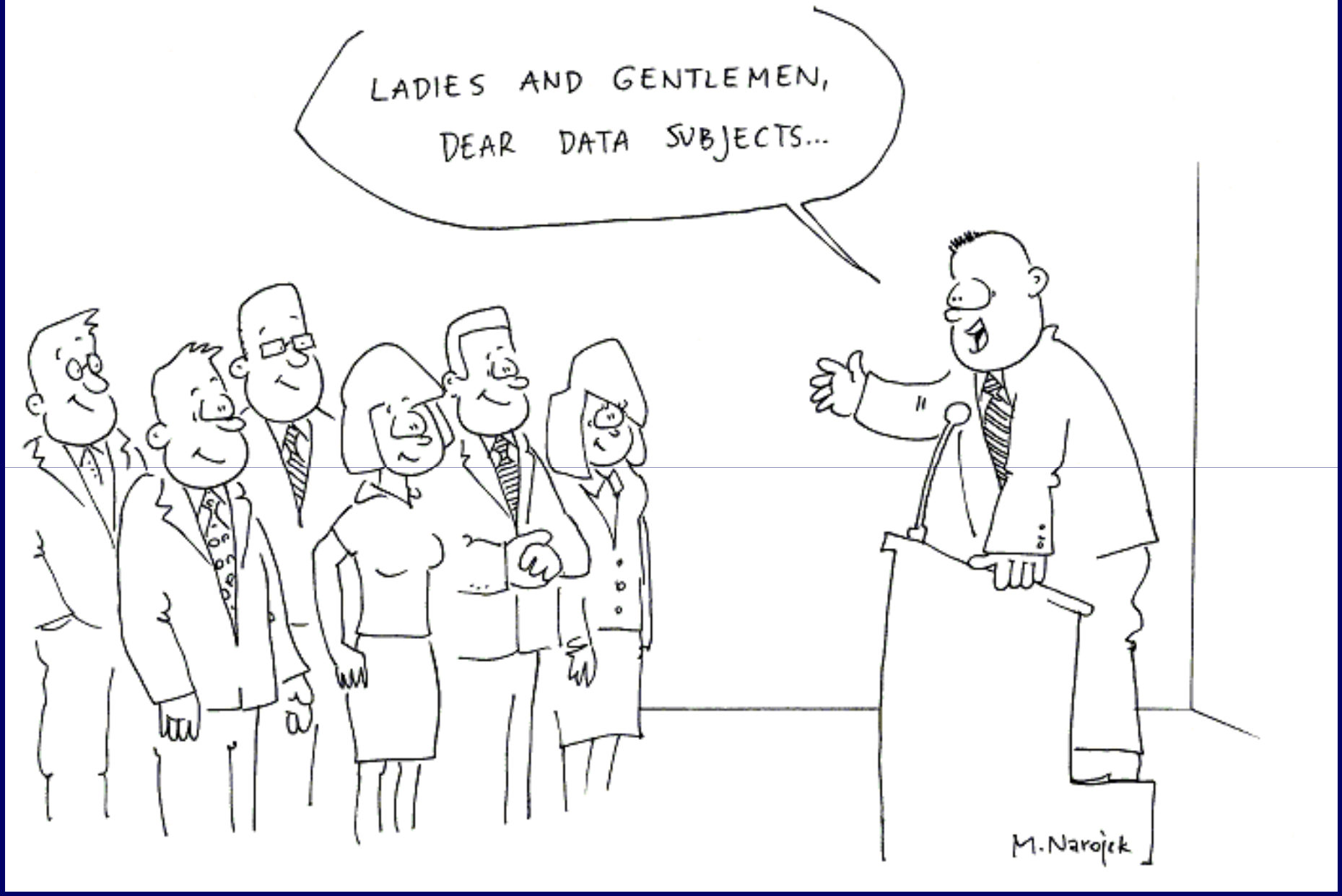
Od idei do wdrożenia

XVII Forum Teleinformatyki
Sesja „Europejska droga do nowego ładu informacyjnego”

22-23 września 2011 r.
Miedzeszyn

dr Wojciech R. Wiewiórowski – WPiA Uniwersytet Gdański, Generalny Inspektor Ochrony Danych Osobowych

Nota:
Niniejsza prezentacja stanowi uzupełnienie wykładu prezentowanego
podczas XVII Forum Teleinformatyki
w czasie sesji „Europejska droga do nowego ładu informacyjnego”.
Forum zorganizowano w Miedzeszynie pod Warszawą
w dniach 22-24 września 2011 r.



Zaufanie i bezpieczeństwo

Europejczycy nie będą korzystać z technologii, którym nie ufają. Epoka cyfrowa to nie „wielki brat” ani „cybernetyczny dziki zachód”.

- Cyberprzestępczość
- Spam
- Malware
- Cyberterroryzm

Czy to jest odpowiedź ?

USTAWA z dnia … 2011 r.
o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw

„1a. Przez zewnętrzne zagrożenie państwa, o którym mowa w ust. 1, rozumie się celowe działania, w tym o charakterze terrorystycznym, godzące w niepodległość, niepodzielność terytorium lub w ważny interes gospodarczy Rzeczypospolitej Polskiej, a także zmierzające do uniemożliwienia lub zakłócenia wykonywania przez organy państwowe ich funkcji, podejmowane przez zewnętrzne w stosunku do niej podmioty, na lądzie, wodzie, w przestrzeni powietrznej, przestrzeni kosmicznej lub cyberprzestrzeni.
1b. Przez cyberprzestrzeń, o której mowa w ust. 1a, rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.”.

Prawo do prywatności i ochrony danych osobowych należą do zasadniczych praw w UE.
Muszą one być skutecznie egzekwowane, również w internecie, przy użyciu szeregu środków, od szerokiego zastosowania zasady poszanowania prywatności od samego początku w stosownych technologiach TIK, po zastosowanie w stosownych przypadkach zniechęcających sankcji.

Zmienione ramy UE dotyczące komunikacji elektronicznej precyzują obowiązki operatorów sieci i dostawców usług, w tym ich obowiązek powiadamiania o naruszeniach ochrony danych osobowych.

Przegląd ogólnych ram ochrony danych obejmie ewentualne rozszerzenie obowiązku powiadamiania o naruszeniach bezpieczeństwa danych.

Wdrażanie zakazu rozsyłania spamu zostanie wzmocnione
dzięki wykorzystaniu sieci współpracy w dziedzinie ochrony konsumentów

Skuteczne i szybkie wdrożenie planu działania UE w zakresie ochrony krytycznej infrastruktury informatycznej oraz programu sztokholmskiego pozwoli na podjęcie szeregu środków w zakresie bezpieczeństwa sieci i informacji oraz walki z cyberprzestępczością.

Należy ustanowić w Europie dobrze funkcjonującą i szerszą sieć zespołów ds. reagowania kryzysowego w dziedzinie informatycznej (Computer Emergency Response Teams – CERT), obejmującą instytucje europejskie, która byłaby w stanie reagować w czasie rzeczywistym.

Należy również stworzyć system punktów kontaktowych w celu zwalczania cyberprzestępczości i umożliwienia podejmowania odpowiednich reakcji w sytuacjach kryzysowych, takich jak ataki cybernetyczne. **Europie potrzeba również strategii dotyczącej zarządzania tożsamością**, w szczególności w odniesieniu do bezpiecznych i skutecznych usług e-administracji.

Komisja podejmie następujące kroki:

• **Główne działanie 6:**
Przedstawienie w 2010 r. środków ukierunkowanych na prowadzenie na wysokim szczeblu udoskonalonej polityki w zakresie bezpieczeństwa sieci i informacji, w tym inicjatyw ustawodawczych, takich jak np.

- unowocześnienie Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA)
- przedstawienie środków umożliwiających szybsze reagowanie na wypadek ataków cybernetycznych, w tym CERT dla instytucji UE;

Główne działanie 7:

Przedstawienie do 2010 r. środków, w tym inicjatyw ustawodawczych, ukierunkowanych na **zwalczanie ataków cybernetycznych na systemy informatyczne oraz powiązanych przepisów dotyczących jurysdykcji w** cyberprzestrzeni na szczeblu europejskim i międzynarodowym (do 2013 r.).

Inne działania:

• Ustanowienie do 2012 r. europejskiej platformy walki z cyberprzestępczością;

• Do 2011 r. analiza możliwości ustanowienia **europejskiego centrum ds. walki z cyberprzestępczością;**

W ramach modernizacji unijnych ram prawnych dotyczących ochrony danych osobowych w celu poprawy ich spójności i zwiększenia pewności prawnej, zbadanie możliwości rozszerzenia zakresu przepisów dotyczących powiadamiania o naruszeniu bezpieczeństwa;

Do 2011 r. wydanie wytycznych dotyczących wdrożenia nowych ram prawnych dotyczących telekomunikacji w odniesieniu do **ochrony prywatności i danych osobowych obywateli;**

Wsparcie **punktów powiadamiania o nielegalnych treściach w internecie** (gorących linii) oraz kampanii uświadamiających dotyczących bezpieczeństwa dzieci w sieci, prowadzonych na szczeblu krajowym, oraz wzmocnienie współpracy paneuropejskiej i wymiany najlepszych praktyk w tym obszarze;

• Wspieranie wielostronnego dialogu oraz samoregulacji wśród europejskich i globalnych dostawców usług (np. portale społecznościowe, dostawcy łączności ruchomej), w szczególności w odniesieniu do korzystania nieletnich z ich usług.

Do 2012 r. ustanowić **dobrze działającą sieć CERT na szczeblu krajowym,** obejmującą całą Europę;

• We współpracy z Komisją **przeprowadzać symulacje ataku na dużą skalę i testować** strategie łagodzenia skutków ataku od 2010 r.;

• W pełni wdrożyć **numery interwencyjne służące do powiadamiania o obraźliwych lub szkodliwych treściach internetowych, organizować kampanie uświadamiające** dotyczące bezpieczeństwa dzieci w internecie, oferować szkołom kursy bezpiecznego korzystania z internetu oraz zachęcać dostawców usług internetowych do wdrażania środków w zakresie samoregulacji dotyczących bezpieczeństwa dzieci w internecie do 2013 r.;

• Począwszy od 2010 r., a przed końcem 2012 r., stworzyć **krajowe platformy ostrzegania lub dostosować je do platformy ostrzegania o cyberprzestępczości** prowadzonej przez Europol.


EXPECTATIONS
REGULATIONS
REQUIREMENTS
COMPETITION
IT'S GAINING ON US!
NOW YOU UNDERSTAND WHAT CONTINUAL IMPROVEMENT IS ALL ABOUT!
ISO 9000
ISO 14000

I tym optymistycznym akcentem

kończąc

zachęcam do zadawania pytań