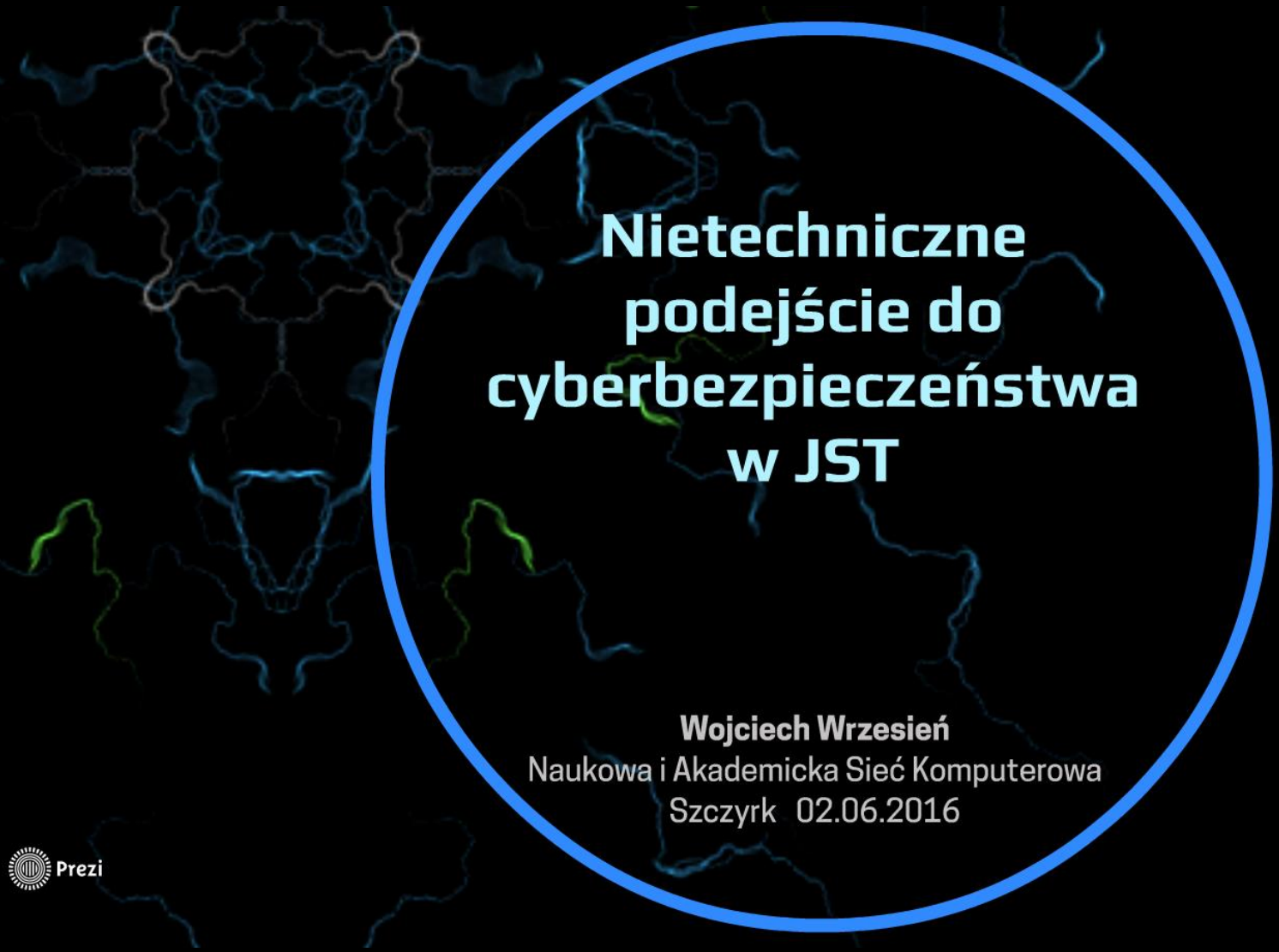


Nietechniczne podejście do cyberbezpieczeństwa w JST

Wojciech Wrzesień
Naukowa i Akademicka Sieć Komputerowa
Szczyrk 02.06.2016

Cyberprzestrzeń

obecne terndy w zagrożeniach

Czy Polska jest zauważalna w światowej sieci Internet ?

Mapa: http://www.nominet.uk/mapping-the-online-world/


Prezi

Powierzchnia
- *całkowita 12 km²*

Liczba ludności (2008) 234. na świecie
- *całkowita 1433[1]*
- *gęstość zaludnienia 119 osób/km²*

Pozycja	Rejestr krajowy	Liczba nazw w domenie (w mln)
1.	Tokelau (.tk)	28,6*
2.	Chiny (.cn)	16,4
3.	Niemcy (.de)	16,0
4.	Wielka Brytania (.uk)	10,7
5.	Holandia (.nl)	5,6
6.	Rosja (.ru)	5,0
7.	Brazylia (.br)	3,7
8.	Australia (.au)	3,0
9.	Francja (.fr)	2,9
10.	Włochy (.it)	2,9
11.	Polska (.pl)	2,7

Źródło: Rynek nazw domeny .PL szczegółowy raport NASK za czwarty kwartał 2015 roku na podstawie „ Domainwire global tld stat report q4 2015".

Jak zmienia się świat?

Odrobina danych od EY i PwC

Media społecznościowe

Przetwarzanie w chmurze

Internet rzeczy

Urządzenia mobilne

Big Data

Sztuczna inteligencja AI

Wydruki 3D

$ 626 mld płatności mobilnych w 2018

Źródło: Goldman Sachs 2014

99% urządzeń nie włączonych do sieci

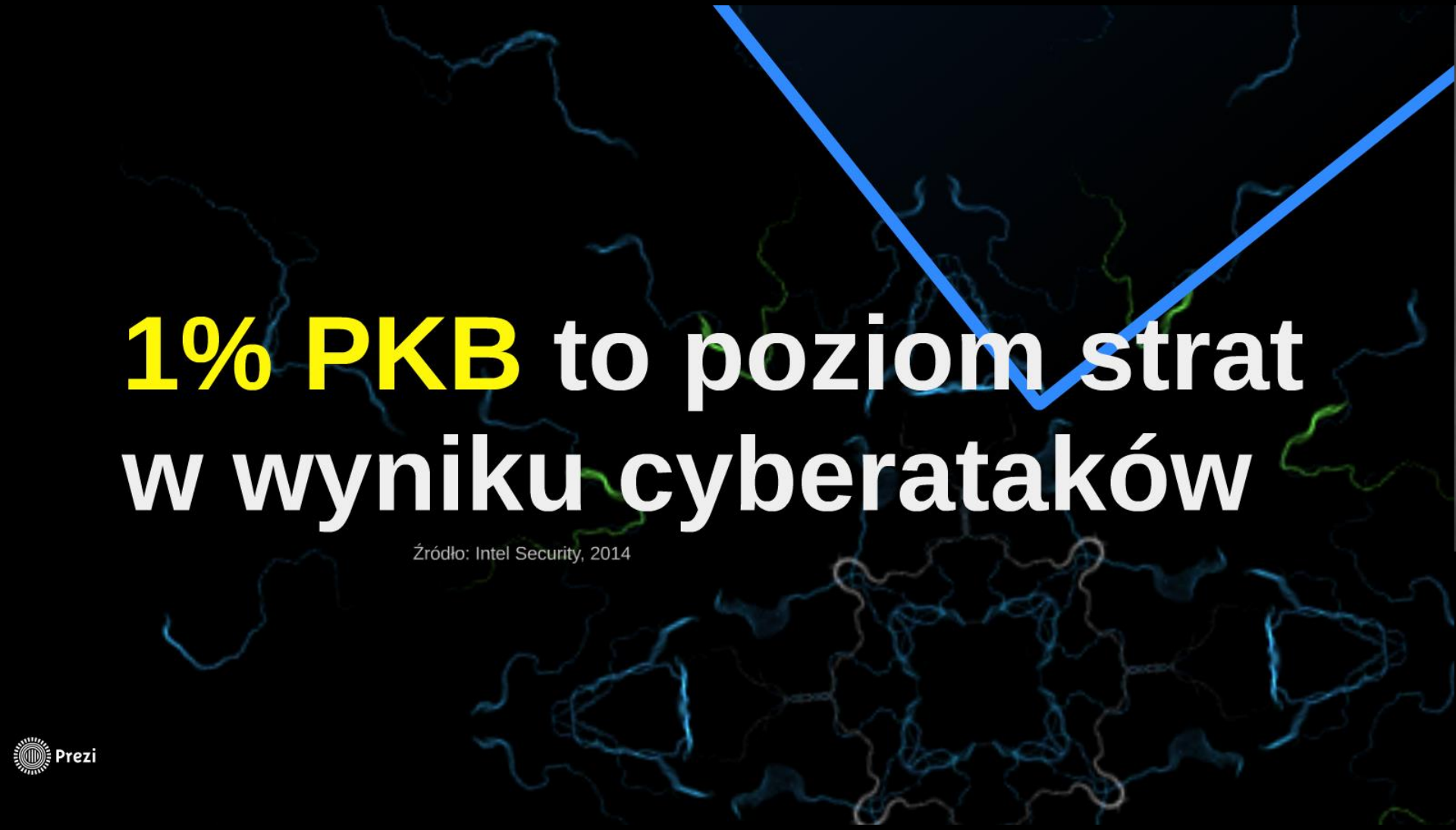
Źródło: Cisco, Rob Soderbury 2013

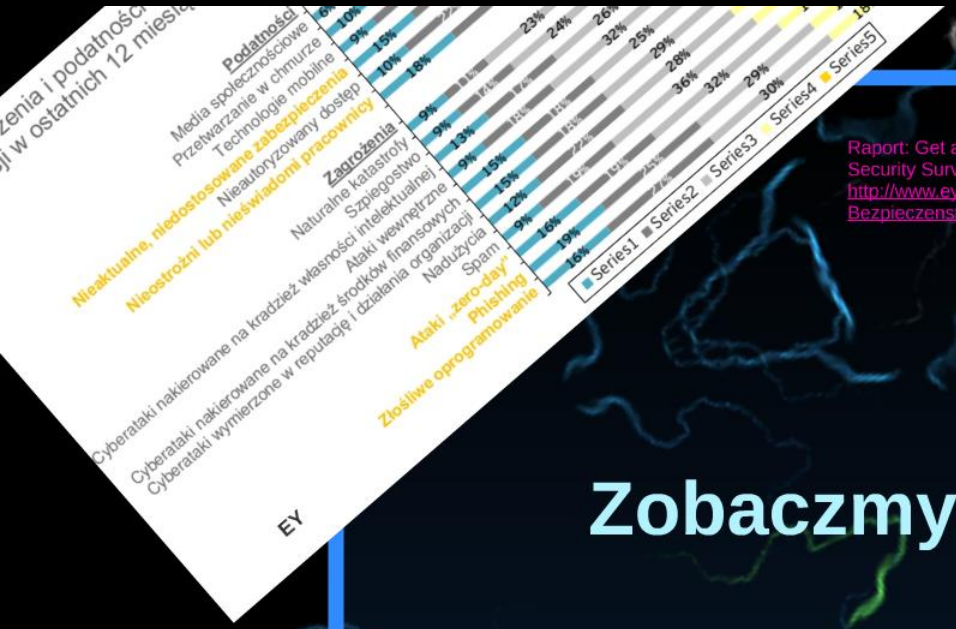
źródło: Report: Get ahead of cybercrime - EY's Global Information Security Survey 2015
http://www.ey.com/PL/pl/Services/Advisory/EY-Swiatowe-Badanie-Bezpieczenstwa-Informacji-2015

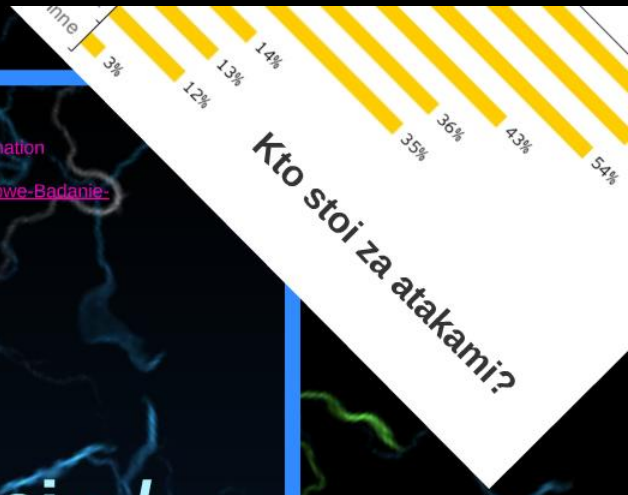
Prezi

85% relacji biznesowych
bez interakcji z człowiekiem w 2020

Źródło: Gartner Group 2011


1% PKB to poziom strat
w wyniku cyberataków
Źródło: Intel Security, 2014



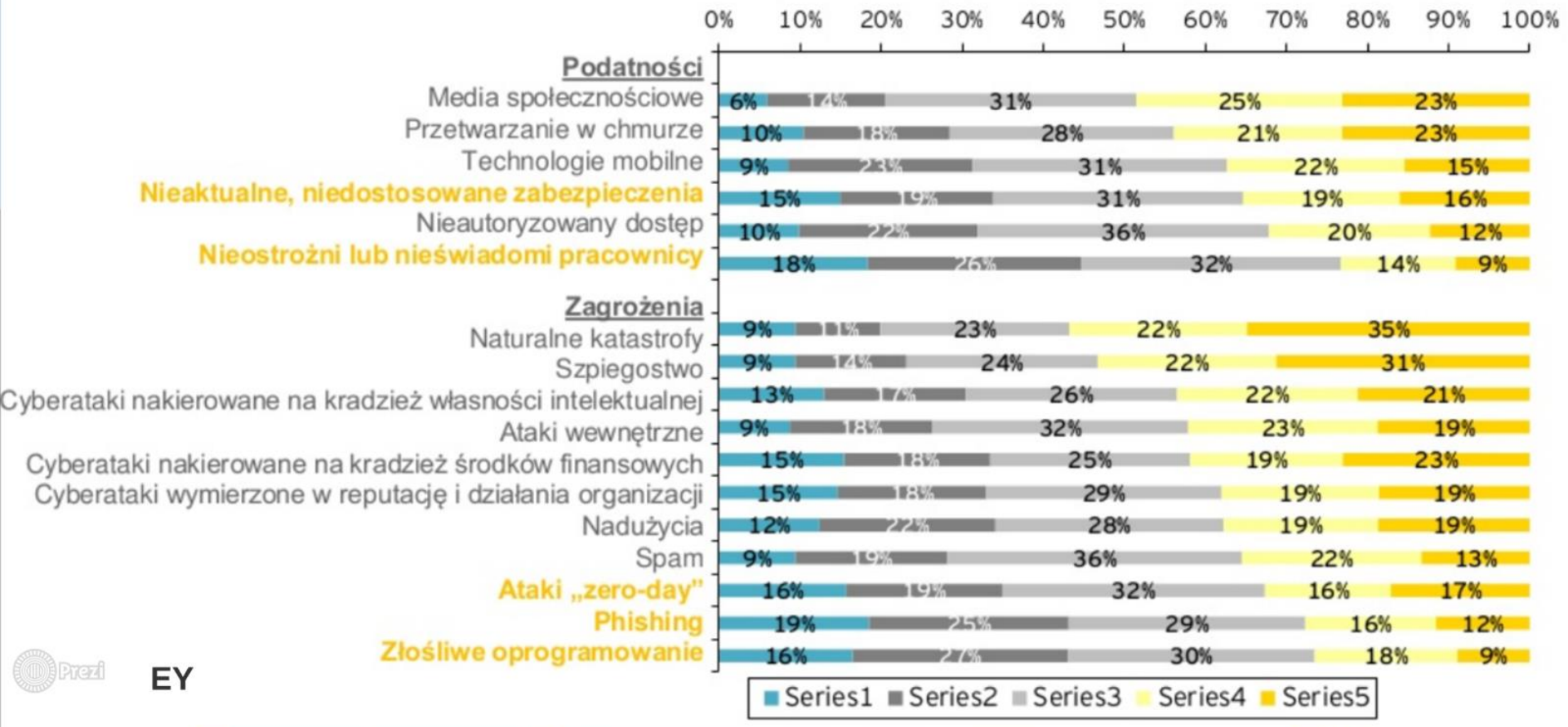


Raport: Get ahead of cybercrime - EY's Global Information Security Survey 2014,
http://www.ey.com/PL/pl/Services/Advisory/EY-Swiatowe-Badanie-Bezpieczenstwa-Informacji-2014

Zobaczmy dokładniej :-/

Dlaczego polskie firmy są tak łatwym celem dla cyberprzestępców?
http://www.slideshare.net/PwCPolska/dlaczego-polskie-firmy-s-tak-atwym-celem-dla-cyberprzestpcw

Jakie zagrożenia i podatności w największym stopniu zwiększyły poziom ryzyka w organizacji w ostatnich 12 miesiącach? (1 w największym, a 5 w najmniejszym stopniu)



EY

Kto stoi za atakami?

EY


Utrata klientów
33%
Straty finansowe
33%
Ujawnienie lub modyfikacja danych
31%
Ujawnienie lub utrata reputacji
16%
Strata ponad 1 mln zł z powodu cyberataków
5%
Przestój w działalności na 5 dni
4%
Konsekwencje...
PwC

Prezesi światowych firm wskazują na zagrożenia związane z cyberbezpieczeństwem jako na **drugie** najważniejsze ryzyko mogące zagrozić prowadzonym interesom

4 godziny - tyle średnio hakerowi zajmuje uzyskanie nieautoryzowanego dostępu do systemów i danych

W najbliższych latach firmy będą musiały liczyć się z możliwością kary w wysokości do **4% globalnych obrotów** za uchybienia w ochronie danych osobowych

Udział wydatków na cyberbezpieczeństwo w budżecie IT w polskich firmach wzrósł w ubiegłym roku z **5,5%** do **10%**. Na świecie ten odsetek wynosi **19%**

30% polskich firm nie planuje wprowadzać szkoleń dla pracowników podczas gdy w **70%** przypadków to właśnie pracownicy są głównym źródłem cyberataku

Jedynie **70%** polskich firm deklaruje zgodność z polską Ustawą o Ochronie Danych Osobowych

PwC

O JAKICH ŹRÓDŁACH ZAGROŻEŃ MÓWIMY ?

Raport Cert Polska 2015-> http://www.cert.pl/PDF/Raport_CP_2015.pdf

W 2015 roku CERT Polska...

... zebrał informacje o 2 484 incydentach dotyczących przeprowadzonych ataków DoS/DDoS z polskich sieci.

... przyjął zgłoszenia dotyczące ponad 3 070 000 unikalnych adresów IP, na których znajdowały się błędnie skonfigurowane serwery i usługi w Polsce.

... obsłużył 881 504 zgłoszenia phishingu w polskich sieciach, dotyczące 29 762 adresów URL w 4 535 domenach, na 1 822 adresach IP.

... otrzymał zgłoszenia dotyczące 20 769 308 unikalnych złośliwych URL-i.

Nazwa instytucji będącej celem	Liczba stron phishingowych
Paypal	286
Wells Fargo	147
Bank of America	132
Google	116
Apple	115
Yahoo	113
Dropbox	77
Alibaba	50
AOL	35
Netflix	35
Chase	34
Amazon	23
Westpac	22
American Express	21
Bradesco	20
NatWest Bank	20
Inne banki	233

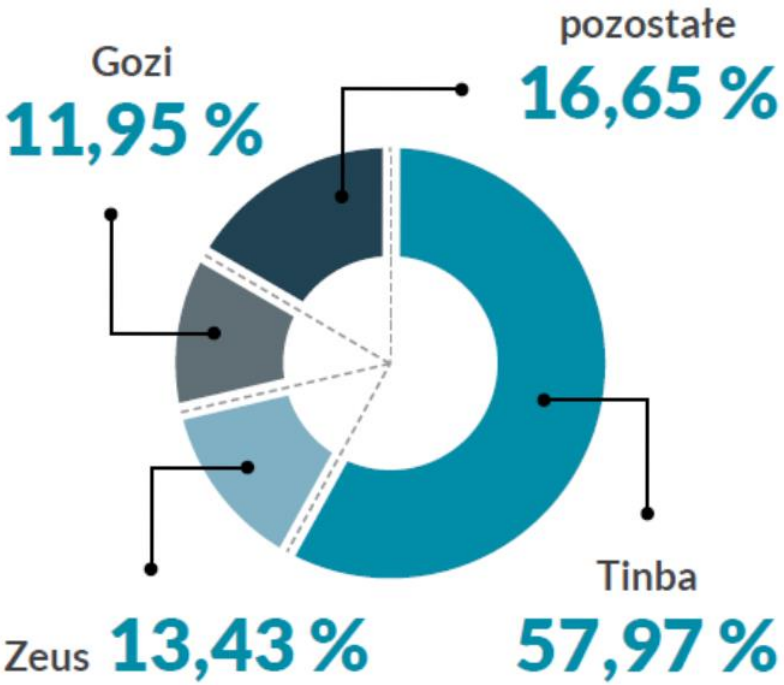
Tabela 11. Instytucje będące celem phishingu

Lp.	Liczba unikalnych adresów URL	Kraj
1	375 344	Polska
2	143 955	Francja
3	28 385	Holandia
4	13 896	Stany Zjednoczone
5	10 496	Niemcy
6	3 998	Hiszpania
7	1 471	Wielka Brytania
8	360	Czechy
9	282	Rosja
10	206	Kanada

Tabela 25. Kraje, w których hostowano najwięcej złośliwych adresów URL w domenie .pl

Największe trojany bankowe w Polsce

W większości trojanów bankowych wykorzystywany jest mechanizm modyfikacji strony internetowej na zainfekowanym komputerze, przez co przestępcy mają pełny dostęp do konta ofiary i mogą przelewać środki znajdujące się na nim.



APT, czyli *Advanced Persistent Threat*, to nazwa nadawana zaawansowanym technicznie atakom teleinformatycznym na cele polityczne, ekonomiczne, techniczne i wojskowe. Głównym zadaniem takich ataków jest wykradanie informacji. Według Richarda Bejtlicha[37] APT należy rozumieć jako:

- **Advanced** (zaawansowane) – ponieważ atakujący wykorzystują różne techniki i metody skutecznego przełamania zabezpieczeń, wykorzystując znane podatności, ale także wynajdując nowe, specjalnie do przeprowadzenia danego ataku,

- **Persistent** (przedłużone, trwałe, uporczywe) – ze względu na formalne zadanie przeprowadzenia skutecznego ataku. Ma on być wykonany tak, aby nie zwrócić niczyjej uwagi, a po uzyskaniu dostępu do jednego systemu ofiary poszerzyć kontrolę o kolejne, w sposób umożliwiający długotrwałą i stałą obecność oraz dozór.

- **Threat** (zagrożenie) – bowiem atakujący to zorganizowana grupa z odpowiednim zapleczem technicznym oraz budżetem. Zagrożenie jest stałe, dopóki atakujący posiada motywację (polityczną, ekonomiczną) do wykradania informacji ofiary. To nie użyte oprogramowanie jest niebezpieczne, a ludzie stojący za nim.

Najważniejsze kampanie APT w 2015:

- Grupa Pocztowa
- Atak na LOT
- Atak na PlusBank
- Atak na polskie konsulaty na Białorusi
- Atak na kancelarie prawne

Wyciąg z opisów ataków

Grupa pocztowa

Celem przestępców było skłonienie użytkowników do zainstalowania złośliwego oprogramowania: Andromedy lub TorrentLockera dla Windows, albo OpFake dla Androida. Przestępcy zarabiali też pieniądze przez program partnerski internetowych kasyn, reklamowanych w spamowych wiadomościach.

Instalowany przez przestępców TorrentLocker to program szyfrujący dane użytkownika dla okupu (*ransomware*), mający jednocześnie funkcje wykradania ustawień kont pocztowych. Drugi z wykorzystywanych botów, Andromeda, używany był tylko jako kanał instalacji jeszcze innego złośliwego oprogramowania – Slave, prostego bota wykonującego ataki na bankowość internetową za pomocą typowej techniki modyfikacji treści stron internetowych w przeglądarce użytkownika. Slave kradnie też kryptowalutę BitCoin poprzez podmienianie w schowku przeklejanych przez użytkownika adresów bitcoin (odpowiedników numerów kont).

Kancelarie prawne

W minionym roku na większą skalę miały miejsce również nieco bardziej wyrafinowane ataki, których grupa odbiorców była ściśle określona. Na uwagę, z kilku względów, zasługują ataki wymierzone przeciwko kancelariom prawnym. Atakujący podszywali się pod firmę, która rzekomo chciała nawiązać współpracę w zakresie obsługi prawnej. Przestępcy przygotowali również stronę, która udawała witrynę internetową firmy. Następnie na adres kancelarii wysyłana była wiadomość z prośbą o odpowiedzenie na kilka podstawowych pytań. W przypadku reakcji ze strony kancelarii, następowała dalsza korespondencja (nierzadko prowadzona z wykorzystaniem innego konta pocztowego), która miała już na celu infekcję rozmówcy złośliwym oprogramowaniem. W szerzej opisywanym przypadku, (m. in. w serwisie Zaufana Trzecia Strona[54]) wektorem infekcji nie był załącznik zawierający złośliwe oprogramowanie, lecz w treści wiadomości znajdował się odnośnik prowadzący do strony, na której rzekomo miał znajdować się plik, będący w rzeczywistości złośliwym oprogramowaniem.

Atak na konsulaty

Atakowany jest system e-konsulat[52], który miał rozładować kolejki, jednak po jego wdrożeniu okazało się, że wszystkie dostępne spotkania są natychmiast rezerwowane, a w białoruskich miastach zaczęły się pojawiać firmy, które oferowały rejestrację wszystkich wniosków wizowych. Za taką usługę pobierały opłatę w wysokości od 150 do 300 dolarów. Dla Białorusinów, którzy na skutek dewaluacji rubla białoruskiego wobec dolara zarabiali jeszcze niedawno równowartość ok. 400 dolarów, była to dość wygórowana cena.

KRAJOBRAZ BEZPIECZEŃSTWA POLSKIEGO INTERNETU

2015

ISSN 2084-9079

NASK

Raport roczny
z działalności CERT Polska

Zatem co jest najtrudniejsze w zachowaniach (cyber) bezpiecznych w organizacji ?

- podatność ludzi na inzynierię społeczną
  - reguły Ciladiniego - wywieranie wpływu na ludzi
  - phishing - jako nośnik złośliwego oprogramowania
  - spearphishing - atak ukierunkowany

1. Zasada wzajemności
2. Zobowiązanie i konsekwencja
3. Społeczny dowód słuszności
4. Sympatia i podobieństwo
5. Autorytet
6. Niedostępność

Robert . B Cialdini

- *Profesor psychologii i marketingu na Uniwersytecie w Arizonie*
- *Autor książki – „Wywieranie wpływu na ludzi", GWP, 1995*

---- Wiadomość oryginalna ----
Temat: Weryfikacja w systemie ING
Wysłano: 22 maj 2016 12:48 PM
Od: ING Online <rulid@bobpeitz.com>
Do: [redacted]gns.pl
DW:

Data: 22.05.2016 r.

Dostęp do Twojego konta ING został zablokowany!

W trosce o bezpieczeństwo naszych klientów zablokowaliśmy twoje konto w systemie ING Bank Śląski, powodem jest nieautoryzowany dostęp do konta.
W celu odzyskania dostępu prosimy o weryfikację właściciela rachunku, logując się na:

www.ingbank.pl/weryfikacja

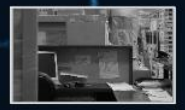
Serdecznie pozdrawiamy,
Zespół ING Bank Śląski S.A.

W przypadku jakichkolwiek pytań prosimy o kontakt z Infolinia 801 601 607

- brak "czujności" pracowników
  - atak na organizację nie jest atakiem na mnie
  - "obcy" w organizacji jest niewidzialny
  - pozostawienie stanowiska pracy bez opieki
  - bałagan na biurku, ważne dokumenty "na widoku"
  - obsługa interesantów, klientów "zbyt dociekliwych"
  - telefon od "przełożonego"

VS

- nieznajomość procedur bezpieczeństwa
  - higiena haseł !!!!!!!!!!!!!!!!!!!!!!!!!!
  - przechowywanie haseł !!!!!!!!!!!!!!!!!!
  - bezpieczeństwo wi-fi
  - przechowywanie dokumentów
  - kopie zapasowe



RANKING HASEŁ

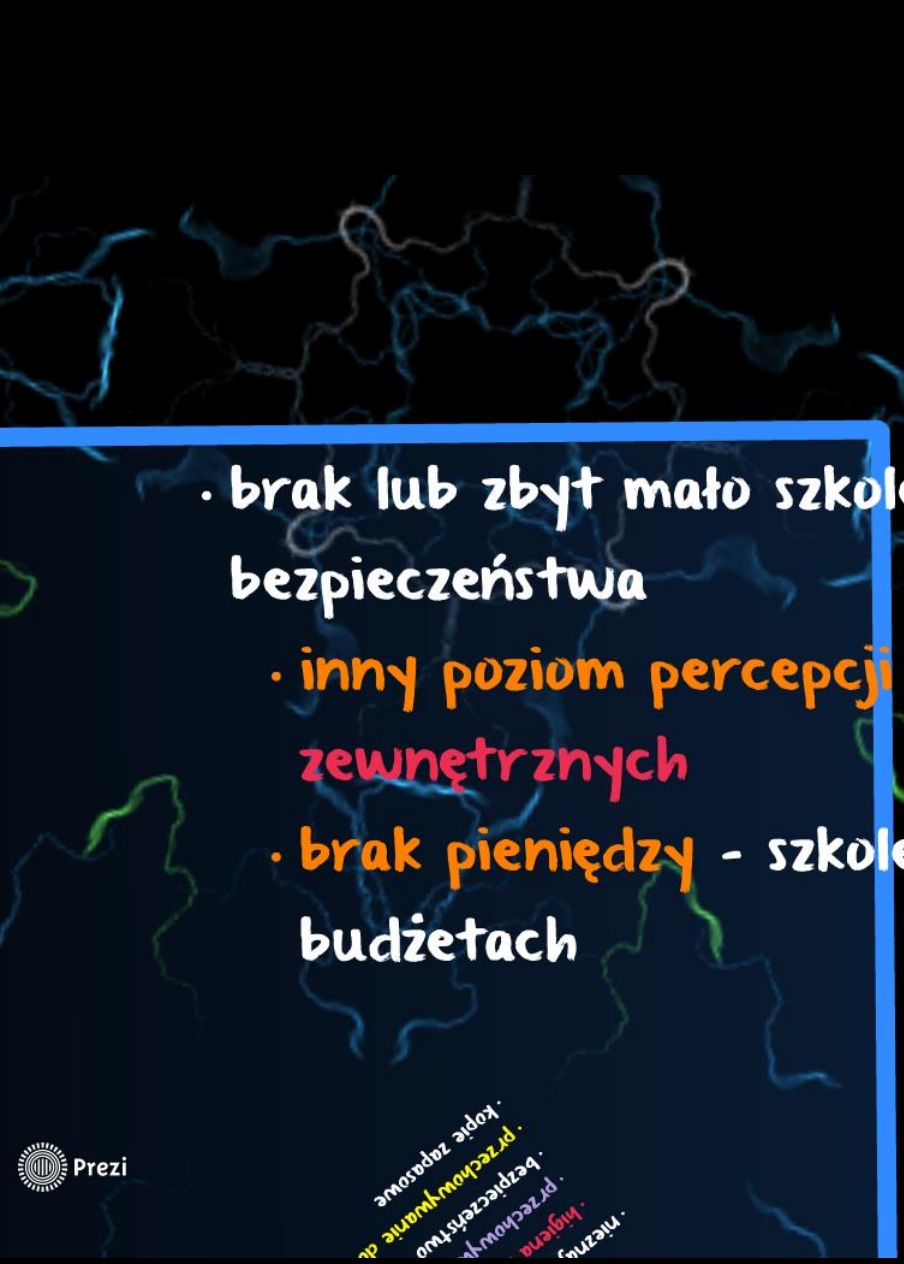
ŚWIAT*	POLSKA**
1. 123456	1. 123456
2. password,	2. polska
3. 12345,	3. matrix
4. 12345678,	4. qwerty
5. qwerty	5. zaq12wsx
6. 123456789	6. monika
7. 1234	7. 12345
8. baseball	8. marcin
9. dragon	9. misiek
10. football	10. master
11. 1234567	11. samsung
12. monkey	12. marcin1
13. Letmein	13. 111111
14. abc123	14. myszka
15. 111111	15. michal
16. admin	16. lukasz
17. iloveyou	17. haslo

*Ranking przygotowany przez firmę Splash Data
** Lista przygotowana przez serwis niebiezpiecznik.pl na bazie wycieku prawie 10 000 haseł z portali onet.pl, wp.pl, interia.pl, o2.pl w 2010 roku.


Nowe hasło
5
abs ZAGATA

- mieszanie obszarów prywatnych i służbowych on-line
  - bezpieczne korzystanie z serwisów społecznościowych czyli jak dużo powiedzieliśmy o sobie w sieci
  - bezpieczna obsługa poczty elektronicznej (prof i priv)
  - serwisy dla profesjonalistów też mogą być nośnikiem ataków

- brak lub zbyt mało szkoleń z podstawowego zakresu bezpieczeństwa
  - inny poziom percepcji dla szkoleń wewnetrznych i zewnętrznych
  - brak pieniędzy - szkolenia tego typu nie ma w budżetach



Podsumujmy:

Cyfryzacja świata postępuje bardzo szybko.

Ataki cybernetyczne były, są i będą.

Przestępcy będą korzystać z luk w zabezpieczeniach bez zahamowań

Wszyscy jesteśmy podatni na ataki socjotechczne

Konieczne są ciągłe kampanie informacyjne

Szkolenia z bezpieczeństwa ogólnego (security awareness) powinny być przeprowadzane i powtarzane jak szkolenia BHP

Uzbrojenie w "sprzęt" security nie zastąpi nieustannego podnoszenia wiedzy pracowników.

"Ucz się, jakby wszystko było jeszcze przed tobą, i ciągle obawiaj się stracić to, czegoś sie nauczył"

Konfucjusz

Dziekuję za uwagę.

wojciech.wrzesien@nask.pl