

Bezpieczeństwo systemów internetowych



AGENDA

- Podstawowe informacje o Risco Software
- Przewaga konkurencyjna Risco Software
- Przykładowe zrealizowane projekty
- Postrzeganie bezpieczeństwa systemów internetowych
- Jestem niewinny – dlaczego jestem celem
- Potencjalne obszary zagrożeń
- Czym jest BOTNET
- Jak zapewnić bezpieczeństwo systemów internetowych
- DEMO
- Audyt zewnętrzny

Informacje o Risco Software Sp. z o.o.

- Na rynku od 1999 roku
- Kilkadziesiąt projektów informatycznych wdrożonych z sukcesem w takich branżach jak bankowość, finanse, ubezpieczenia, motoryzacja
- Partnerzy technologiczni: Microsoft, EMC, Oracle, IBM, OpenSpan
- Partnerzy biznesowi: Krajowa Izba Rozliczeniowa S.A.
- Zespół 25 pracowników każdej roli projektowej

Klienci



Główne linie technologiczne - kompetencje



Microsoft

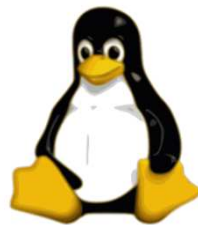
ORACLE



Microsoft
.net



Microsoft
SQL Server



Microsoft
**Windows
Server System**



RISCO
SOFTWARE

Przewaga konkurencyjna Risco Software

- 13-letnie doświadczenie
- optymalny proces produkcji oprogramowania (Craftmanship)
 - nie tylko działające oprogramowanie ale dobrze wytworzone (ciągłe doskonalenie warsztatu)
 - stała refaktoryzacja kodu (w tym proces code review)
 - Continuous Delivery (automatyczne testy, pokrycie kodu testami, continuous integration, continuous deployment)
- optymalny proces utrzymywania systemu (szybkie czasy reakcji i rozwiązania zgłoszenia, wsparcie 24/7/365, wsparcie narzędzi zewnętrznych)
- konkurencyjne ceny
- nowatorskie rozwiązania w zakresie zarządzania przedsiębiorstwem oraz projektami (Lean, Agile)
- optymalna architektura i najlepszy dobór technologii
- pełna elastyczność i dopasowanie do wymagań Klienta

Przykładowe zrealizowane projekty

- Internetowa platforma bankowości elektronicznej
- Interfejs do systemu Express ELIXIR (KIR S.A.)
- Integracje z systemem Ognivo (KIR S.A.)
- Rozwiązania WebServices do komunikacji z klientami korporacyjnymi (standard ISO 20022, e-faktury)
- System wczesnego ostrzegania o niewypłacalności klientów kredytowych
- Centralny system generowania wydruków
- System obsługi procesu kredytowego
- Aplikacje mobilne

Postrzeganie bezpieczeństwa systemów internetowych

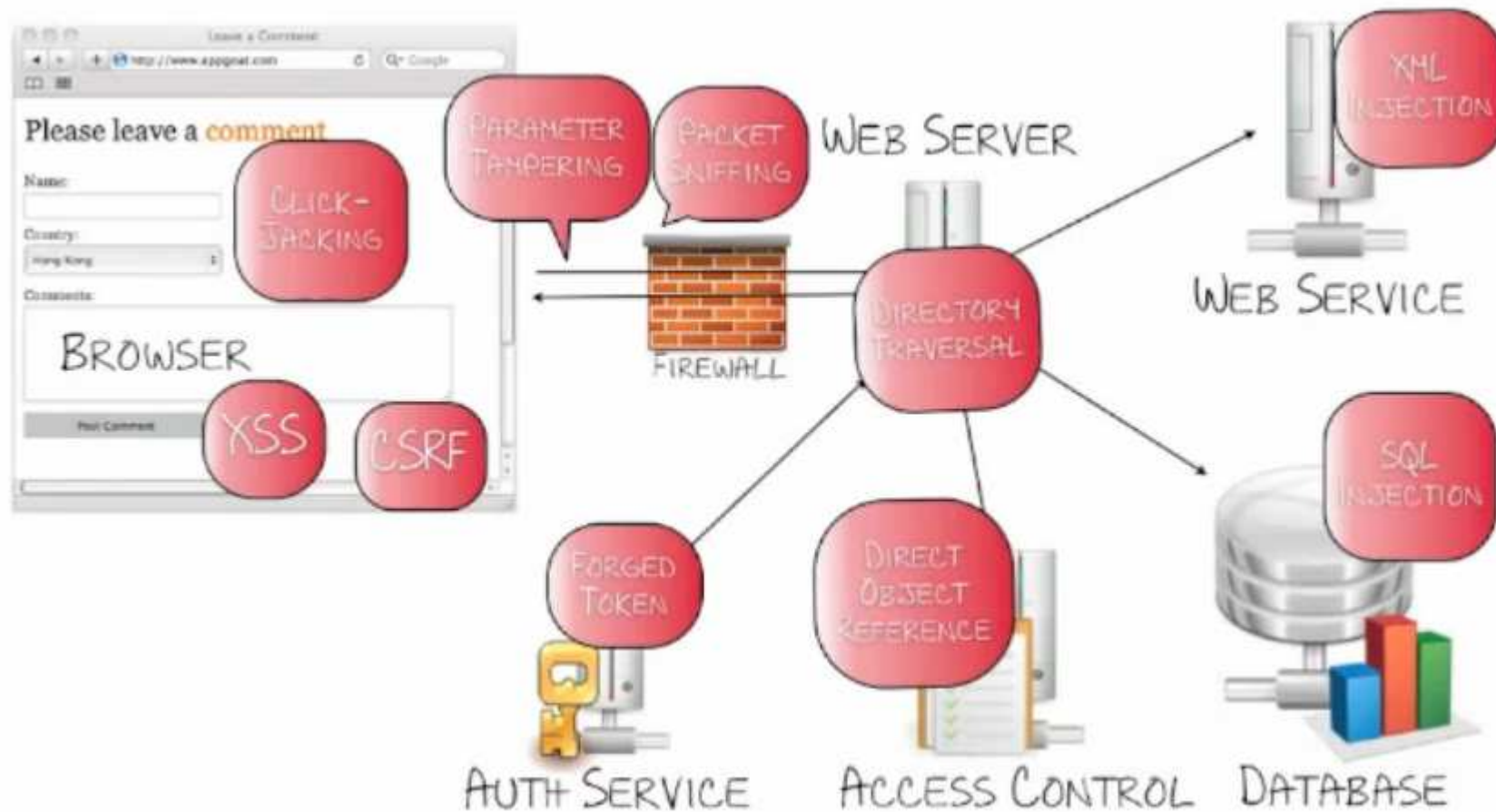
- **Użytkownik końcowy** – aplikacje webowe takie jak bankowość internetowa, płatności elektroniczne, obsługa poczty elektronicznej itp. postrzegane są jako bezpieczne
- **Programista aplikacji webowych** – spora część programistów uważa swoje aplikacje za bezpieczne

Jestem niewinny – dlaczego jestem celem ?

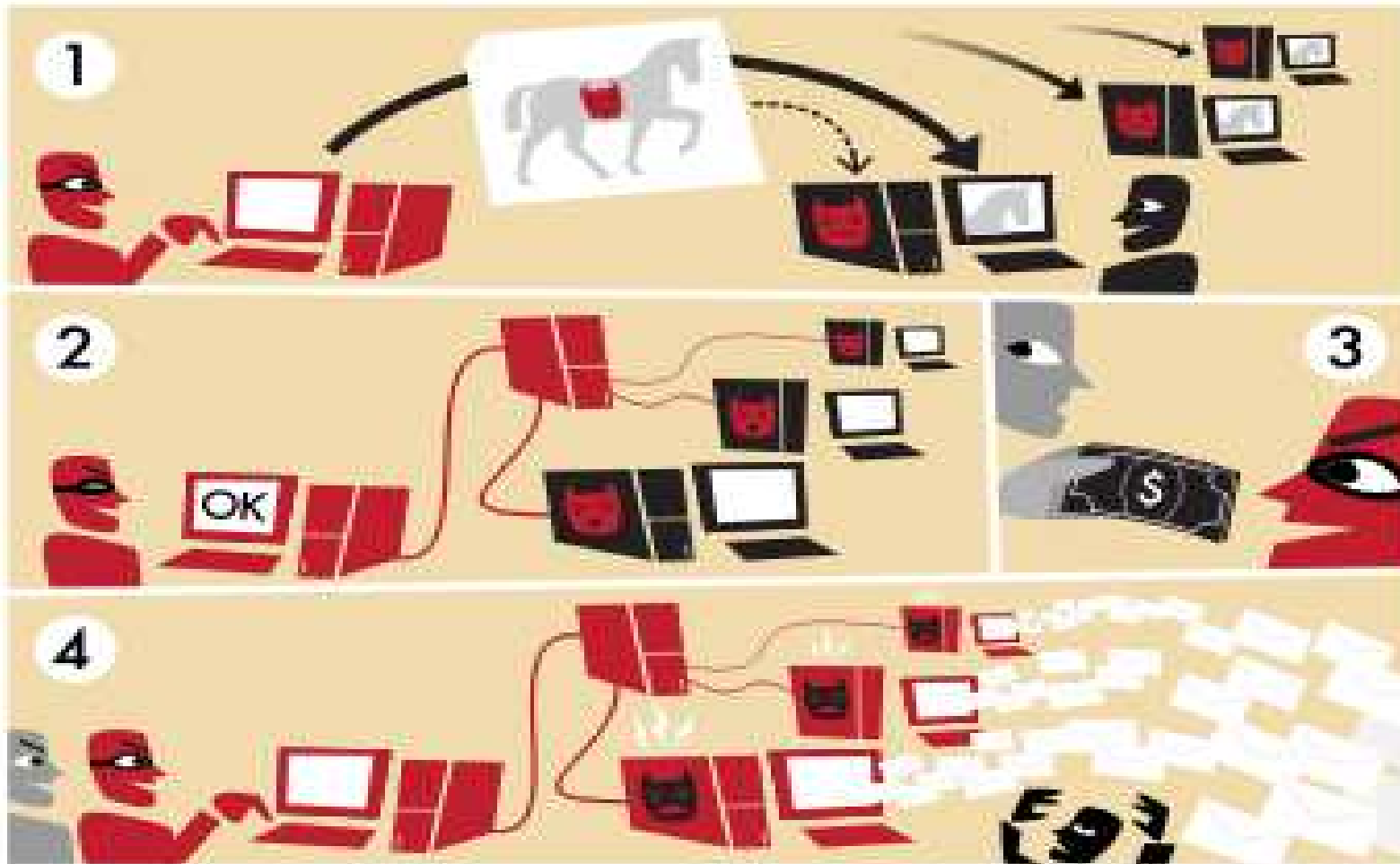
- Paraliż Twoich systemów może być komuś na rękę
- Masz wrażliwe i poufne dane
- Agresor może przejąć Twój komputer aby atakować innych albo wykorzystać Twoje zasoby
- Masz zasoby sprzętowe...



Potencjalne obszary zagrożeń



Czym jest BOTNET ?



Jak zapewnić bezpieczeństwo systemów internetowych ?

- Zapewnić bezpieczeństwo na poziomie infrastruktury
- Zapewnić bezpieczeństwo na poziomie aplikacji
 - Programowanie defensywne - tworzenie oprogramowania z myślą o jego poprawnym działaniu nawet przy nieprzewidywalnych sposobach jego użycia
 - Tworząc aplikacje webowe należy nauczyć się patrzeć na system w sposób w jaki na nasz system patrzył by agresor



OWASP

OWASP – z ang. *Open Web Application Security Project* – jest globalną, profesjonalną fundacją, działającą charytatywnie (non-profit), otwartą dla każdego, kto interesuje się zabezpieczeniami w oprogramowaniu.

Główną ideą stowarzyszenia jest poprawa bezpieczeństwa aplikacji webowych.

Co oferuje OWASP ?

Między innymi:

- OWASP Top Ten
- OWASP Application Security Verification Standard
- OWASP Guide
- ESAPI
- AntiSamy
- XSSer
- WebGoat

DEMO

ETHICAL HACKING – audyt zewnętrzny

Przykłady wykrytych problemów podczas audytu:

- Cache - POST Request Returns 200 OK Server Response
- Application accepts GET instead of POST requests (Pre- Authentication)
- Session ID Cookies Not Marked as Secure
- Browser autocomplete enabled before authentication

Dziękujemy za uwagę

Marcin Werner

Prezes Zarządu

Tel. 22-622-58-33, 502-090-767

marcin.werner@riscosoftware.pl

Radosław Jaszek

Analityk/Programista/OpenSpan Specialist

Tel. 609-02-85-85

radoslaw.jaszek@riscosoftware.pl

Risco Software sp. z o.o.

Al. Jerozolimskie 125/127, 02-017 Warszawa

www.riscosoftware.pl