

prevenity

SECURITY SOLUTIONS

Quo vadis, security?

Artur Maj, Prevenity



Agenda

1. Bezpieczeństwo informacji – rys historyczny
2. Najistotniejsze wyzwania bezpieczeństwa - obecnie i w najbliższym czasie
3. Nasze rekomendacje

Bezpieczeństwo - rys historyczny

Bezpieczeństwo – rys historyczny

- Zagrożenia i ataki

	10 lat temu	Obecnie
Ataki	Proste	Złożone
Motywacja intruzów	Sława, rzadko korzyści finansowe	Korzyści finansowe, rzadziej sława
Koncentracja ataków	Strona serwera, np.: - Microsoft IIS, Apache	Strona klienta, np.: - Przeglądarka WWW, PDF
Najpopularniejsze podatności*	Przepełnienie bufora	Cross Site Scripting, SQL Injection
Socjotechniki	Rzadko stosowane	Często stosowane

*Źródło: Open Source Vulnerability Database (<http://osvdb.org>)

Bezpieczeństwo – rys historyczny (cd.)

- Wybrane techniczne środki ochrony

	10 lat temu	Obecnie
Zapory ogniowe	Tradycyjne	Nowej generacji
Osobiste zapory ogniowe	Rzadko stosowane	Często stosowane
Systemy antywirusowe	Samodzielne	Zintegrowane z innymi elementami ochrony
Centralne serwery logów	Rzadko stosowane	Często stosowane, wypierane przez SIEM
Wykrywanie włamań	IDS, rzadko stosowane	IPS, często stosowane
Zdalny dostęp	Szyfrowanie rzadko stosowane	SSH, SSL, IPsec

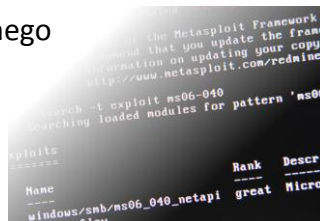
**Najistotniejsze wyzwania
bezpieczeństwa –
obecnie i w najbliższym czasie**

Wyzwania bezpieczeństwa – obecnie i w najbliższym czasie

- Próba wskazania 10 najistotniejszych wyzwań i obszarów zagrożeń bezpieczeństwa w polskich realiach na podstawie:
 - Prognoz firm analitycznych
 - Prognoz producentów produktów bezpieczeństwa
 - Opinii uznanych światowych ekspertów ds. bezpieczeństwa
 - Wyników realizowanych przez nas audytów bezpieczeństwa i testów penetracyjnych
 - Ciągłej obserwacji rozwoju obszaru bezpieczeństwa informacji

Wyzwanie #1

- Zarządzanie poprawkami
 - Brak zainstalowanych lub nieprawidłowo zainstalowane poprawki bezpieczeństwa
 - Na poziomie warstwy sprzętowej
 - Na poziomie środowiska wirtualnego
 - Na poziomie systemu operacyjnego
 - Na poziomie serwera aplikacji
 - Na poziomie aplikacji



```
... the Metasploit Framework
... that you update the fram
... information on updating your copy
... http://www.metasploit.com/redmasc

Search for exploit ms06-040
Searching loaded modules for pattern 'ms06

exploits
-----
Name                               Rank  Descri
-----
windows/smb/ms06_040_netapi great Micros
... flow
```

Wyzwanie #2

- Nieprawidłowa konfiguracja
 - Domyślne nazwy kont i hasła
 - Domyślne ustawienia konfiguracji
 - Nadmiarowe usługi



Wyzwanie #3

- Urządzenia mobilne
 - Kradzież urządzenia
 - Mobile malware
 - Socjotechniki



Wyzwanie #4

- Systemy wbudowane
 - Telewizory z dostępem do Internetu
 - Komputery samochodowe
 - Nowoczesny sprzęt AGD
 - Zastosowania RFID



© 2010 Prevenity Sp. z o.o. Wszelkie prawa zastrzeżone.

prevenity
INTEGRATED SOLUTIONS

Wyzwanie #5

- Cloud Computing
 - Kontrola nad dostępem do danych
 - Kontrola nad fizyczną lokalizacją danych
 - Kontrola nad backupem danych
 - Błędy bezpieczeństwa w aplikacjach Cloud Computing
 - Wyciek danych



© 2010 Prevenity Sp. z o.o. Wszelkie prawa zastrzeżone.

prevenity
INTEGRATED SOLUTIONS

Wyzwanie #6

- Bezpieczeństwo aplikacji WWW
 - Znane typy błędów bezpieczeństwa
 - Nowe zagrożenia
 - HTML 5.0



Wyzwanie #7

- Uwierzytelnianie i autoryzacja
 - Kradzież tożsamości
 - Kradzież danych uwierzytelniających
 - Nieautoryzowane transakcje



Wyzwanie #8

- Aplikacje klienckie
 - Podatności bezpieczeństwa
 - Przeglądarki internetowe
 - Plug-in'y do przeglądarek
 - Przeglądarki PDF
 - Odtwarzacze multimedialnych
 - Aplikacje
 - Szyfrowane połączenia TLS/SSL
 - Nieautoryzowane sieci VPN (np. Hamachi)



Wyzwanie #9

- Sieci społecznościowe i Web 2.0
 - Socjotechniki
 - Dystrybucja złośliwego oprogramowania
 - Wyciek informacji
 - Zagrożenia prywatności
 - SPAM



Wyzwanie #10

- Socjotechniki
 - Phishing (Smishing, Vishing itp.)
 - Skrócone adresy URL
 - Techniki SEO
 - Wiele innych...



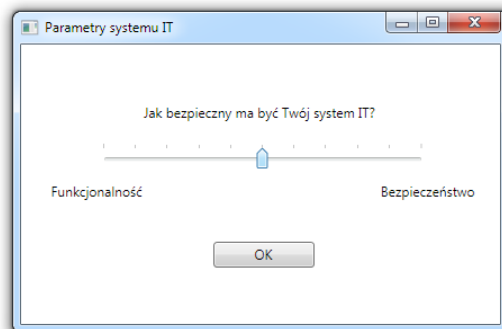
Quo vadis, security?

Quo vadis, security?

- Zarówno teoria jak i doświadczenie pokazuje, że zapewnienie bezpieczeństwa informacji musi być procesem **ciągłym**
- Zadanie to staje się coraz bardziej **złożone, trudniejsze** i jednocześnie **ważniejsze** dla biznesu
- Zagrożenia i ataki zmieniają się w czasie, podobnie jak techniczne środki bezpieczeństwa...
- ... które choć są bardzo ważne, **nie są wystarczające** aby zapewnić skuteczną ochronę

Nasze rekomendacje

- Zapewnienie 100% bezpieczeństwa niepraktyczne a wręcz niemożliwe – sugerujemy skupić się na oszacowaniu ryzyka i jego redukcji do **akceptowalnego poziomu**
- W pierwszej kolejności należy adresować **realne** zagrożenia a nie potencjalne lub „medialne”
- Przy wyborze rozwiązania uwzględnić nie tylko bieżące potrzeby ale również **trendy** i zmieniające się **zagrożenia** bezpieczeństwa
- Rozwiązania techniczne tylko **jednym z wielu** metod ochrony!



Dziękuję z uwagą

artur.maj@prevenity.com