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

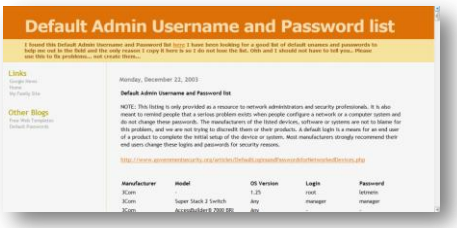
- Próba wskazania 10 najistotniejszych wyzwań i obszarów zagrożeń bezpieczeństwa w polskich realiach na podstawie:
  - Prognoz firm analitycznych
  - Prognoz producentów produktów bezpieczeństwa
  - Opinii uznanych światowych ekspertów ds. bezpieczeństwa
  - Wyników realizowanych przez nas audytów bezpieczeństwa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

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

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

Wyzwanie #6

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

Anonymous speaks: the inside story of the HBGary hack

By Peter Bright | Last updated 11 days ago

It has been an embarrassing week for security firm HBGary and its HBGary Federal offshoot. HBGary Federal CEO Aaron Barr thought he had unmasked the hacker hordes of Anonymous and was preparing to name and shame those responsible for co-ordinating the group's actions, including the denial-of-service attacks that hit MasterCard, Visa, and other perceived enemies of WikiLeaks late last year.

When Barr told one of those he believed to be an Anonymous ringleader about his forthcoming exposé, the Anonymous response was swift and humiliating. HBGary's servers were broken into, its e-mails pillaged and

Increase text size
Reduce text size
Print this story
Leave a comment (393)
Make a correction

Premier features (learn more):
View on single page
Configure these features

LATEST TOP STORIES
Random defendant outlawyers P2P attorney, gets lawsuit tossed
Week in Apple: Verizon iPhone shootout, Thunderbolt makes its debut
Week in tech: more HBGary fallout, rooting your Nook Color, and more
Week in gaming: *Bulletstorm* PC, Geohot cash, *Tiny Wings*
Week in science: don't fear the mosqorpion
Colbert Report features Ars

prevenity

Wyzwanie #7

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

Haker wykorzystał hasła i ukradł 40 tys. złotych

ag

2011-02-23, ostatnia aktualizacja 2011-02-23 14:15

gazeta Rzeszów

Mieszkaniec Jarosławia stracił 40 tys. zł podczas przelewania pieniędzy ze swojego internetowego konta bankowego. Haker wykorzystał hasła do konta, które poszkodowany wysyłał mu przez telefon.

Fot. Archiwum

Mężczyzna podczas logowania się na portal banku, w którym posiada konto, został poproszony o podłączenie swojego telefonu komórkowego do komputera. Na ekranie pojawił się napis, który mówił o autoryzacji klienta poprzez podłączoną komórkę. Jarosławianin podłączył się do sieci i zalogował się na stronę swojego banku, by dokonać przelewu ze swojego konta, wtedy nastąpiło nieautoryzowane wgranie oprogramowania szpiegującego do komórki.

-Smsy z hasłami dostępu do konta bankowego, które niezbędne są do wykonania przelewu, zostały przesłane na telefon komórkowy innej osoby. W efekcie z konta zawiadamiającego zostały wypłacone pieniądze w kwocie 40 tys. zł bez jego wiedzy - informują policjanci.

Właściciel konta zorientował się, że został oszukany, ponieważ nie otrzymał na swój telefon żadnego sms-a z kodami, a to było niezbędne do wykonania przelewu z konta.

Zgłosił sprawę policję i teraz policjanci z wydziału do walki z przestępczością gospodarczą ustalają okoliczności popełnienia tego przestępstwa. Jak wynika z policyjnych ustaleń, mechanizm działania tego typu oszustw jest taki, że zamiast prawdziwej strony pojawia się na ekranie tzw. kalka strony, którą w sieć wprowadza sprawca bądź sprawcy tych przestępstw.

- Apelujemy do wszystkich użytkowników bankowych kont internetowych o ostrożność podczas logowania się do systemu. Zwracajmy szczególną uwagę na to, gdy polecenia administratora strony są zupełnie inne niż te, które funkcjonowały do tej pory - przestrzegają policjanci.

Źródło: Gazeta Wyborcza Rzeszów

prevenity

Wyzwanie #8

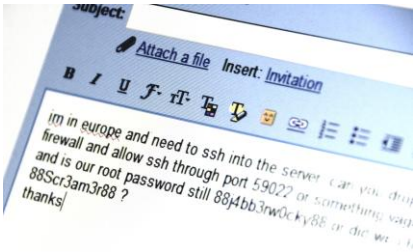
- Aplikacje klienckie
  - Podatności bezpieczeństwa
    - Przeglądarki internetowe
    - Plug-in'y do przeglądarek
    - Przeglądarki PDF
    - Odtwarzacze multimediów
    - Aplikacje
  - Szyfrowane połączenia TLS/SSL
  - Nieautoryzowane sieci VPN (np. Hamachi)

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...



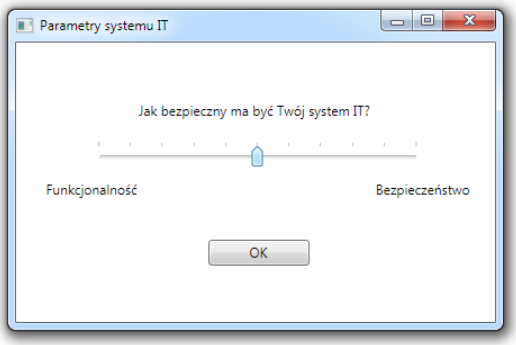
Quo vadis, security?

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 uwagę

artur.maj@prevenity.com

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