
ORACLE®

ORACLE®

E-usługi a bezpieczeństwo w sieci

XVI Forum Teleinformatyki

Identity and Access Managment Architect
Aleksander Jachowicz

Agenda

- Zagrożenia w obszarze dostępu do e-usług
- Projektowanie architektury rozwiązań „bezpiecznych”
- Jednorodna kontrola dostępu do wszystkich e-usług
- Zarządzanie tożsamością obywatela – konta i uprawnienia
- Wykrywanie i zapobieganie nadużyciom

Zagrożenia – zewnętrzne

- Phishing - Spoofing
- Pharming
- Wirusy, trojany – logowanie pisania na klawiaturze
- Brak uwierzytelniania aplikacji internetowych

Ataki na systemy webowe

Technology news and Jobs › Information Technology News › [redacted] loses $1.14 million to online fraud (update)

[redacted] Bank loses $1.14 million to online fraud (update)

User Rating: ○○○○○ / 0

Poor ○ ○ ○ ○ ◉ Best Rate

Written by Alex Zaharov-Reutt

McAfee has described the phishing attack as "the biggest ever" online bank heist, throwing new light on just how effective hackers are at using phishing techniques to illegally earn the big bucks.

BOOKMARK

First name

Last name

email

Country

Australia

Please enter the text you see on the right.

9QTYG4

iTWire

Subscribe

Subscribe to iTWire's FREE daily e-newsletter

BONUS Get a 12 month License to LiveProject valued at $99 USD

McAfee have told ZDNet UK this phishing attack is 'the biggest ever'. Surely, even bigger attacks are in store for 2007, and are likely being planned, or may even be in progress right now.

While banks around the world have been under attack from phishing emails for months now, with the phishers using increasingly clever techniques to get people to voluntarily divulge their usernames and passwords without realizing they are giving them straight to 'the bad guys', calling into qusetion the security systems that everyone relies on daily to do business online.

250 customers have been affected so far, with at least 121 more customer accounts under investigation. The hackers used a phishing email that advised bank customers to download a "spam fighting" program called 'raking.zip' or 'raking.exe' that loaded what security companies are calling the haxdoor.ki Trojan.

Related stories

MailMarshal claims 99.5 percent spam detection

The Road from Windows - Online email

IT jobs market to continue boom through 2008 says

Ochrona systemów webowych

Witaj, [redacted].

Czy wiesz, że hasło jest kluczem do Twojego konta? Tak jak klucze do mieszkania nie może dostać się w niepowołane ręce, dlatego:

- **nie zapisuj** swojego hasła - zapamiętaj je;
- zawsze **wyloguj się** po zakończeniu przeglądania stron [redacted] (zwłaszcza jeśli korzystasz z kafejek internetowych);
- pod żadnym pozorem **nie podawaj swojego hasła, nawet osobom, które podają się za pracowników** [redacted]. Jeżeli otrzymasz taką prośbę, nie odpowiadaj na nią, ale skontaktuj się z nami.

Jak możesz zadbać o to, by Twoje konto było bezpieczne?

- Stwórz mocne hasło:
  - ułóż je z kombinacji cyfr oraz małych i wielkich liter;
  - nie stosuj słów podobnych do Twojej nazwy użytkownika, imienia itp.;
  - nie używaj informacji, które łatwo zdobyć, np. daty Twoich urodzin.
- Sprawdzaj, czy logujesz się na oryginalnej stronie [redacted] (zobacz, jak to zrobić).

W naszym Centrum Bezpieczeństwa znajdziesz instrukcje, jak zbudować łatwe do zapamiętania, a jednocześnie trudne do odgadnięcia hasło.

Przydatne informacje

- Jeżeli korzystasz już z hasła, które łatwo odgadnąć - zmień je na stronie *Moje* [redacted] > *Ustawienia* > *Moje Dane*.

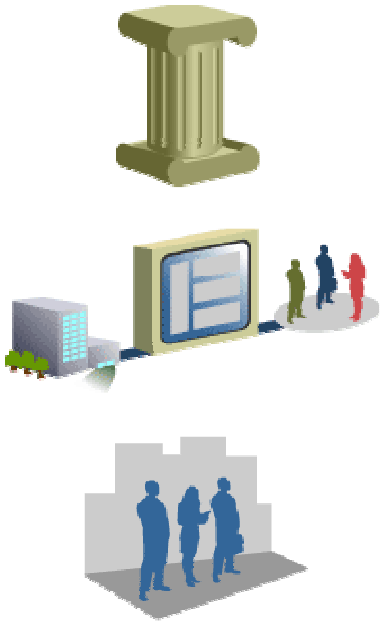
Zagrożenia - architektura

- Duża ilość miejsc przechowywania użytkowników – brak jednorodnej bazy
- Brak integracji między różnymi systemami w wielu instytucjach
- Brak mechanizmu pojedynczego logowania
- Skala rozwiązania – nadawanie uprawnień dla dużej ilości użytkowników
- Rozbudowa systemów – skalowalność
- Funkcjonalności bezpieczeństwa jako część systemu a nieintegrowany moduł
- Brak centralnego audytowania

Architektura

- Wykorzystanie standardów – łatwa integracja
- Jednorodne mechanizmy uwierzytelniania użytkowników – wykorzystanie istniejących i planowanych metod (PL.ID)
  - Pojedyncze logowanie do portali i aplikacji
  - Łatwa integracja (eUsługi, ePUAP)
- Silne, kontekstowe uwierzytelnianie oparte na analizie ryzyka
- Centralizacja baz użytkowników
- Federacja domen pojedynczego logowania
- Zapewnienie łatwej skalowalności wraz ze wzrostem bazy użytkowników
- Zarządzanie użytkownikami i uprawnieniami – automatyzacja, samoobsługa i delegowanie uprawnień administracyjnych
- Scentralizowane możliwości audytowe

Jak Oracle może pomóc?



- Dostarczyć bezpieczne metody dostępu do internetowych usług administracji publicznej bazujących na silnym uwierzytelnianiu, autoryzacji opartej o analizę ryzyka i ochronie danych dotyczących tożsamości
  - Access Manager
  - Adaptive Access Manager
- Umożliwić wsparcie dla efektywnego wdrożenia rozwiązań zgodnych z przepisami (np. Ustawa o ochronie danych osobowych)

- Usprawnić zarządzanie i dystrybucję uprawnień dla dużej liczby użytkowników ze wsparciem dla usług samoobsługowych i delegowania czynności administracyjnych
  - Oracle Identity Manager
  - Oracle Identity Analitics
- Ułatwić integrację w obszarze zarządzania tożsamością i bezpieczeństwem pomiędzy agencjami, departamentami, urzędami, ministerstwami
  - Oracle Identity Federation

Przykład - Norwegia

MinID

• Rząd Norweski wdrożył usługę MinID – identyfikatory dla obywateli do logowania do serwisów publicznych

Ministerstwo Rolnictwa

• Potrzeba wdrożenia elastycznej platformy zarządzania tożsamością i dostępem do aplikacji webowych (głównie dla rolników)

• Wymagana integracja z państwowym systemem MinID

• Automatyzacja zarządzania tożsamością użytkowników zewnętrznych

Poczta Norweska

• Znaleźć następcę dla obecnego niewydajnego systemu zarządzania tożsamością i dostępem

• Umożliwić zarządzanie dostępem dla obywateli do zarządzania swoimi danymi pocztowymi (zmiana adresu, przekierowanie poczty, itp.)

• Wdrożyć platformę. która umożliwi integrację z MinID

• Zapewnienie zgodności z lokalnymi regulacjami

Rozwiązanie Oracla

Ministerstwo Rolnictwa

• Oracle Identity and Access Managements Suite

• Użycie Fereracji, Access Managera i Identity Managera

Poczta Norweska

• Oracle Identity and Access Managements Suite

• Access Manager do kontroli dostępu dla użytkowników zewnętrznych i wewnętrznych

• Identity Manager do zarządzania użytkownikami wewnętrznymi

Rezultaty

Ministerstwo Rolnictwa

• Federacja z uwierzytelnianiem MinID

• Integracja SSO dla aplikacji wewnętrznych

• Platforma do zarządzania użytkownikami zewnętrznymi

Poczta Norweska

• Skalowalna platforma do zarządzania dostępem dla użytkowników zewnętrznych (1M) i wewnętrznych (20K)

• Zarządzanie tożsamością dla wszystkich użytkowników wewnętrznych (Oracle HR, AD, eBS)

• Aktualnie wdrożenie federacji z MinID

Przykład – Szwedzki urząd skarbowy Skatteverket

Wdrożenie dla 9 milionów obywateli

Skatteverket

Wymagania i problemy

- Potrzeba zmniejszenia kosztów administracji do 0.5% od zebranych podatków
- Wymagane zwiększenie bezpieczeństwa nowych usług internetowych wykorzystywanych przez obywateli
- Istniejące rozwiązanie SSO zrealizowane wewnętrznie było drogie w utrzymaniu i nie było wystarczająco skalowalne
- Potrzeba obsługi różnych metod uwierzytelniania: kody PIN, certyfikaty (CRL/OCSP)

Rozwiązanie Oracla

- Oracle Access Manager
- Oracle Internet Directory
- OAM SDK zostały w łatwy sposób zintegrowane z JAAS na WebLogic
- Integracja z partnerskimi rozwiązaniami, takimi jak „Nexus MultiID Server” do weryfikacji autentyczności certyfikatów (CRL/OCSP)
- Automatyczne tworzenie kont i uprawnień w trakcie uwierzytelniania, aby zapobiec pre-populacji 9 milionów obywateli

Rezultaty

- Pojedyncza platforma dostępu dla szwedzkich obywateli (początkowo 2,5 miliona docelowo 9 milionów)
- Krótszy czas wdrażania nowych usług internetowych i zwiększenie bezpieczeństwa
- Zmniejszenie kosztów obsługi systemu i jego rozwoju

Przykład – Helse Vest, Okręgowy Urząd Zdrowia południowo-wschodniej Norwegii

Wymagania i problemy

- Zabezpieczenie portala pracowniczego dostępnego przez internet
- Zmniejszenie kosztów operacyjnych
- Zapewnić zgodność z przepisami dotyczącymi opieki zdrowotnej
- Wymagana centralizacja administracji dla dużego okręgu zdrowotnego
- Rozwiązanie musi łatwo integrować się z istniejącą infrastrukturą

Rozwiązanie Oracla

- Oracle Adaptive Access Manager do bezpiecznego wieloelementowego uwierzytelniania
- Bezproblemowa integracja z istniejącymi aplikacjami internetowymi

Rezultat

- OAAM pozwolił na przyjazne dla użytkownika uwierzytelnianie, które spełniają wymagania stawiane przez przepisy dotyczące opieki zdrowotnej
- Nie potrzeba rozwiązań sprzętowych jak „tokeny”, karty
- Obniżenie kosztów administracyjnych
- Rozwiązanie umożliwiło dostęp do portalu pracowniczego bez zwiększania ryzyka

Minimalizacja kosztów – ROI

Koszty całkowite								
Koszty	**Początkowe**		**1 rok**		**2 rok**		**3 rok**	**Suma**
Koszty licencji	$	500 000	$ -	$	-	$ -	$	500 000
Roczne utrzymanie	$	-	$ 75 000	$	75 000	$ 75 000	$	225 000
Koszty wdrożenia	$	357 500	$ 70 000	$	60 000	$ -	$	487 500
Koszty wewnętrzne- Planowanie, Projekt	$	250 000	$ -	$	-	$ -	$	250 000
Koszty wewnętrzne- Wsparcie operacyjne	$	-	$ 405 000	$	315 000	$ 180 000	$	900 000
Sprzęt	$	250 000	$ -	$	-	$ -	$	250 000
	$	-	$ -	$	-	$ -	$	-
Suma	**$**	**1 357 500**	**$ 550 000**	**$**	**450 000**	**$ 255 000**	**$**	**2 612 500**

Korzyści całkowite								
Korzyści	**1 rok**		**2 rok**		**3 rok**		**Suma**	
Wydajność nowo przyjętych pracowników	$	540 000	$	540 000	$	540 000	$	1 620 000
Prowizjonowanie aplikacji i resetowanie haseł	$	800 000	$	800 000	$	800 000	$	2 400 000
Resetowanie haseł, czas połączeń do helpdesk	$	1 000 000	$	1 000 000	$	1 000 000	$	3 000 000
oszczędności kosztów pracy: recertyfikacja dostępu, wnioski o nowe konta, atestacja, wsparcie audytu	$	400 000	$	400 000	$	400 000	$	1 200 000
Zwiększenie wydajności: audyty, atestacja	$	300 000	$	300 000	$	300 000	$	900 000
Unikanie kosztów wynikających z audytu	$	250 000	$	250 000	$	250 000	$	750 000
Oszczędności na licencjach niewykorzystanych	$	250 000	$	250 000	$	250 000	$	750 000
Suma korzyści	**$**	**3 540 000**	**$**	**3 540 000**	**$**	**3 540 000**	**$**	**10 620 000**

ORACLE IS THE INFORMATION COMPANY