sentrigo™

Hedgehog:

Datenbankmonitoring, Zugriffsschutz und –protokollierung

DOAG Regionaltreffen Nürnberg 31.03.2011

sentrigo™

Hedgehog:

McAfee to Acquire Sentrigo to Enhance Database Security Portfolio

Companies to Deliver Best-of-Breed Solutions for Database Protection, Compliance and Monitoring

SANTA CLARA, Calif., March 23 - McAfee announced its intention to acquire privately-owned Sentrigo, a leading provider of database security and compliance, assessment, monitoring and intrusion prevention solutions. Sentrigo of , database activity mo npacting performanc

McAfee has rogram and in 201(Databases, McAfee Dat uisition, McAfee will ction of databases, and activity monitoring of databases.

The proposed transaction will bring together best-in-class technologies to:

McAfee®

DOAG Regionaltreffen Nürnberg 31.03.2011

The Sentrigo name, the Sentrigo logo and Sentrigo's product names and logos are trademarks of Sentrigo Inc.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates.
Microsoft is a trademark of the Microsoft group of companies.
Other names appearing in this presentation may be trademarks of their respective owners.

31.03.2011

Why All These Database Breaches?

- Willie, why do you rob banks?
- Because that's where the money is.

William 'Willie' Sutton

1901 - 1980

Datenbankbedrohungen im Laufe der Zeit (1)

- Datenbankverletzungen sind nichts Neues
- SB1386 (July 2003), ein US-Gesetz in dem unter anderem die Offenlegung von Sicherheitsvorfällen geregelt ist.
- In 2005 gab es Dutzende von umfangreichen Vorfällen (Choicepoint – 163.000 Sätze, Guidance SQ – 3800 Kreditkarten Infos, Lexis Nexis, DSW….)

Datenbankbedrohungen im Laufe der Zeit (2)

- 2007 "Mega"-Vorfälle mit Millionen von gestohlenen Datensätzen (TJX, Fidelity und mehr
- 2009 die bisherige Spitze: Heartland Payment Systems: mehr als 135 Millionen Datensätze

Niemand ist sicher...

Reported	Institution	Data Breached
July 2010	UCSF Medical Center	Employee used colleagues' SSNs, PII to fill out hundreds of surveys and redeem Amazon.com vouchers
July 2010	Buena Vista University	PII for applicants, students, staff, and donors going back to 1987 stolen from BVU database
June 2010	Univ. of Maine	Hackers stole PII/clinical data for 3,500 students
June 2010	Digital River, Inc.	Hackers (and possibly insiders) copy 200,000 personal records
Mar 2010	TSA	Terminated developer placed malware in terrorism suspect DB
Feb 2010	Wyndam Hotels	??? Number of customer names and payment card details
Feb 2010	Ceridian	Attack yielded SSNs and bank account data for 27,000 employees of 1,900 companies from payroll processor
Jan 2010	Iowa Racing & Gaming Comm.	Hacker gained access to database containing PII of more than 80,000 employees
Dec 2009	Rock You	SQL injection resulted in breach of 32 million user passwords
Nov 2009	T-Mobile	Employee sold millions of customer records to rival carriers
Aug 2009	Heartland	130 Million+ credit/debit card records

Source: Privacy Rights Clearinghouse

Deutsche Behörden kaufen gestohlene Daten

- Februar 2010 – Deutsche Steuerbehörden kaufen Informationen über 1.500 Kunden einer Schweizer Bank
- Deutschland bezahlt 2,5 Millionen Euros

Schwarzmarktpreise für gestohlene Online-Banking-Daten ermittelt

Die Rendite ist offenbar enorm: 700 US-Dollar muss ein Krimineller für die Zugangsdaten zu einem Bankkonto bezahlen, mit dem sich ein garantiertes Guthaben von 82.000 Dollar erwirtschaften lässt. Für weniger belastbare Konten muss man laut einem Bericht (PDF-Datei) des AV-Herstellers Panda nur 80 US-Dollar ausgeben.

Panda hat sich nach eigenen Angaben in kriminelle Netzwerke eingeschlichen, in denen mit gestohlenen Daten gehandelt und Dienstleistungen feilgeboten werden. Insgesamt 50 solcher "Online-Shops" hat der AV-Hersteller ausgekundschaftet und dabei weitere interessante Preise ermittelt. Die Kosten für Kreditkarteninformationen belaufen sich beispielsweise auf 2 bis 90 US-Dollar, je nach Kreditrahmen.

Wer damit nicht nur im Internet einkaufen möchte, kann sich mit den Daten auch eine Kreditkarte nachmachen lassen. Kostenpunkt: 30 US-Dollar für eine einfarbige Karte, eine unverdächtige bunte Kreditkarte macht 90 US-Dollar – zuzüglich der Kosten für die aufgespielten Daten.

Wer sich nicht selbst traut, mit den Daten online einkaufen zu gehen, kann für 30 bis 300 US-Dollar einen Transaktionsdienst in Anspruch nehmen. Einen Fernseher mit geklauten Daten vom Strohmann einkaufen und an die eigene Adresse schicken zu lassen, schlägt laut Panda mit 100 US-Dollar zu Buche.

Die Shops bieten auch Zubehör für Skimmer. Aufsätze für die Karteneinzüge von Diebold- und NCR-Bankautomaten kosten rund 3000 Euro. Komplette nachgemachte Bankautomaten, etwa zum Aufstellen im belebten Einkaufszentrum, sollen für 35.000 US-Dollar zu haben sein.

Laut Panda funktionieren die Online-Stores von Internet-Kriminellen nach dem Vorbild von legalen Online-Shops. Neben den Preiskatalogen finden Kunden dort auch Sonderangebote, Mengenrabatte, Try&Buy-Angebote und individuelle Dienstleistungen, für die der Kunde sogar Kostenvoranschläge erhält. Umtausch und Reklamation (sic!) soll auch möglich sein. Die Bezahlung funktioniert allerdings etwas abweichend von üblichen Gepflogenheiten: Statt Kreditkarten werden nur Zahlungen über Dienste wie Western Union, Liberty Reserve und WebMoney akzeptiert. Erreichbar ist die Online-Mafia über Chats und Soziale Netze. Das deutsche, in der Vergangheit mehrfach gehackte Untergrund-Forum carders.cc etwa hat einen eigenen Twitter-Account und sogar eine Fangruppe auf Facebook. (dab)
Heise-News-Meldung vom 04.02.2011:
www.heise.de/security/meldung/Schwarzmarktpreise-fuer-gestohlene-Online-Banking-Daten-ermittelt-1183524.html

Schwarzmarktpreise für gestohlene Online-Banking-Daten ermittelt

Artikel	Preis US $
Zugangsdaten Bankkonto („Erwirtschaftung“ eines garantiertes Guthaben von 82.000 $)	700
Kreditkarteninformationen	2 bis 90
Monochrome Kreditkarte	30[1)]
Bunte „echt“ aussehende Kreditkarte	90[1)]
Serviceleistungen: Einkaufen mit gestohlenen Kreditkarteninfos über Strohmänner	100
Skimmer für Geldautomaten	3.000
Kompletter Geldautomat	35.000

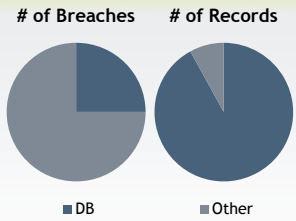
[1)] Zuzüglich der Kosten für das Aufspielen der Daten

→Sonderangebote, Mengenrabatte, Try&Buy, Kostenvoranschläge, Umtausch und Reklamation
→Bezahlung nicht mit Kreditkarten sondern über Western Union, Liberty Reserve, WebMoney

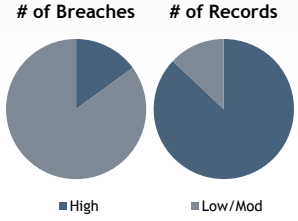
Heise-News-Meldung vom 04.02.2011:
www.heise.de/security/meldung/Schwarzmarktpreise-fuer-gestohlene-Online-Banking-Daten-ermittelt-1183524.html

Wo ist die “Ausbeute” am größten ?

- **Database servers** are involved in 25% of all breaches
- **Database breaches** account for 92% of all records breached



- **Sophisticated attacks** make up 15% of all attacks
- **Sophisticated attacks** account for 87% of all records breached

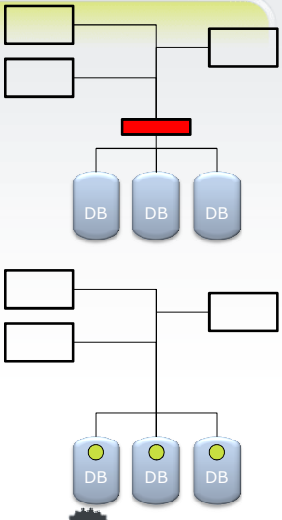


- Source: Verizon Business Study 2010

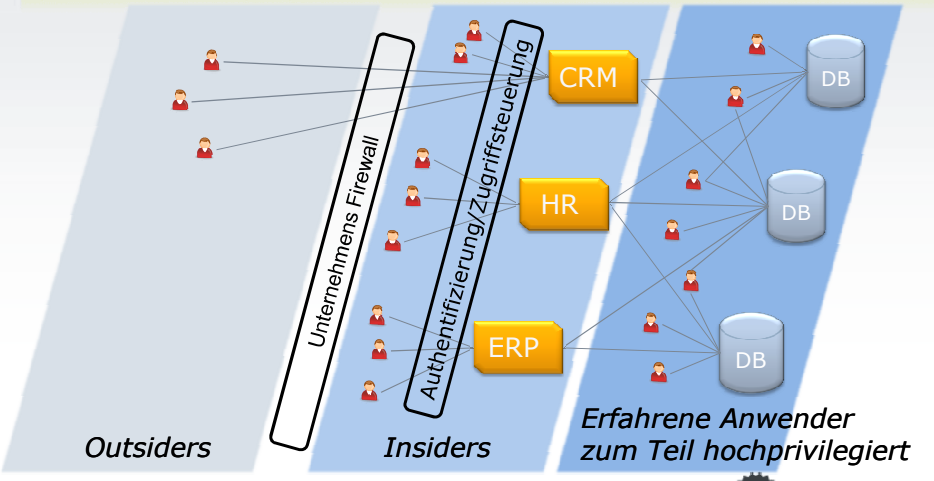
Data Security Lösungen von Sentrigo

Netzwerk- vs. Serverbasiert

- Netzwerkbasiert
  - "sieht" SQL-Statement
  - ? Verschlüsselung / Verschleierung
  - Appliance im Netzwerk
  - tw. Mitschneiden Ergebnismengen
  - ? Lokale Zugriffe
- Serverbasiert
  - "sieht" SQL-Statement
  - und alle davon betroffenen Datenbankobjekte
  - Unabhängig von Zugriffspfad + Verschlüsselung

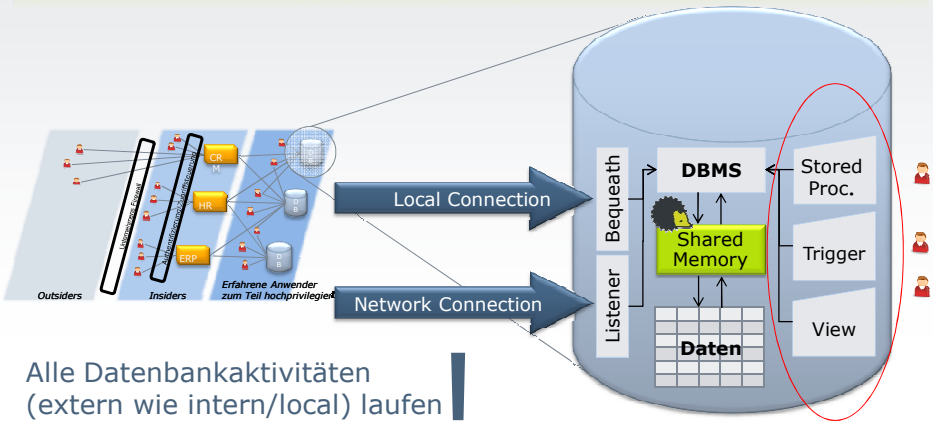


Ausgangslage



Commercially Classified

Monitoring aller Datenbankaktivitäten



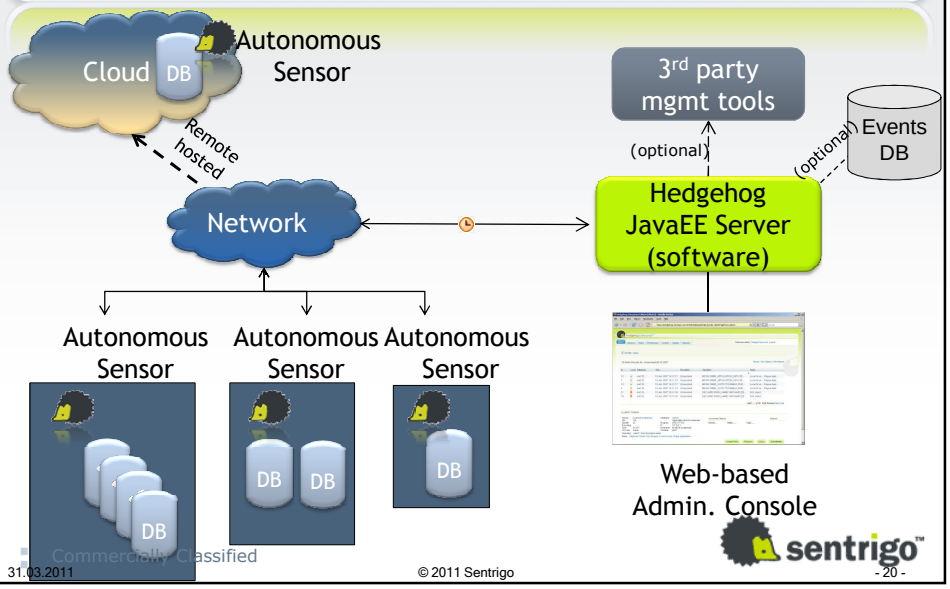
Alle Datenbankaktivitäten (extern wie intern/local) laufen über "Shared Memory" !

Commercially Classified

Hedgehog Enterprise: Monitoring und Schutz in Echtzeit

- Prinzip: Schutz der Daten, nicht des Zugriffpfades
- HE "sieht" die Aktivitäten, unabhänging vom Auslöser, ist nahe genug dran um einzugreifen
- Unabhängig von Zugriffspfaden und -methoden, Umgebungsvariablen und Datenkomplexität
- Datenbanksitzungen können beendet und Benutzerkonten in Quarantäne gestellt werden
- Geringe Performancebelastung, normalerweise weniger als 3% einer einzigen CPU
- Virtuelles Patchen

Hedgehog: Deployment Architecture



Hedgehog Enterprise: Datenbanken / Betriebssystem

- Skalierbar bis > 1.000 Datenbanken
- Datenbanken:
  - Oracle 8.1.7 or newer, Microsoft SQL Server 2000/2005/2008, Sybase ASE 12.5
- Betriebssysteme:
  - Microsoft Windows 2000 or newer, Sun Solaris 7 or newer, IBM AIX 5.2 or newer, HP-UX 11.11 or newer (11.23 or newer on IA64), RHEL, SUSE

download – install – use/test

D E M O

About Sentrigo

- Patent-pending innovator in **database security**, with solutions for vulnerability assessment, activity monitoring, breach prevention and compliance
- Headquarters in Silicon Valley, CA
- More than 1,700 installations
- Red Team conducts independent database security research:
  - Discovers vulnerabilities in DBMS systems, and delivers virtual patches
  - Credited by Oracle in 6 of last 7 patches
  - Works with leading researchers around the globe, including Pete Finnigan, Alexander Kornbrust, and Paul Wright

RED HERRING N. AMERICA WINNER 100 · Info Security Products Guide 2010 GLOBAL PRODUCT EXCELLENCE AWARDS CUSTOMER TRUST ★★★★★ · SC MAGAZINE AWARDS 2010 FINALIST Honored in the U.S. · CLOUD COMPUTING WORLD SERIES AWARDS · NETWORKWORLD SECURITY COMPANIES TO WATCH · SC MAGAZINE AWARDS 2008 WINNER Honored in the U.S.

sentrigo

Q & A ?✓

Franz Hüll
Senior Security Consultant & Sales

Sentrigo Inc.

Mobile: +49 (171) 76 66 475

franzh@sentrigo.com
www.sentrigo.com

sentrigo