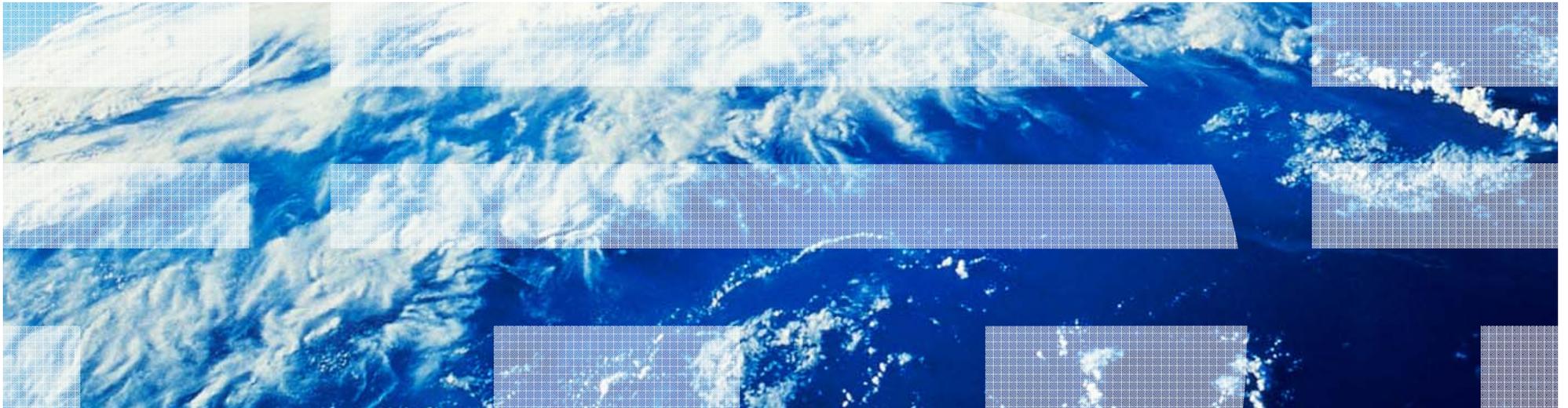


Vertrauen ist gut ...

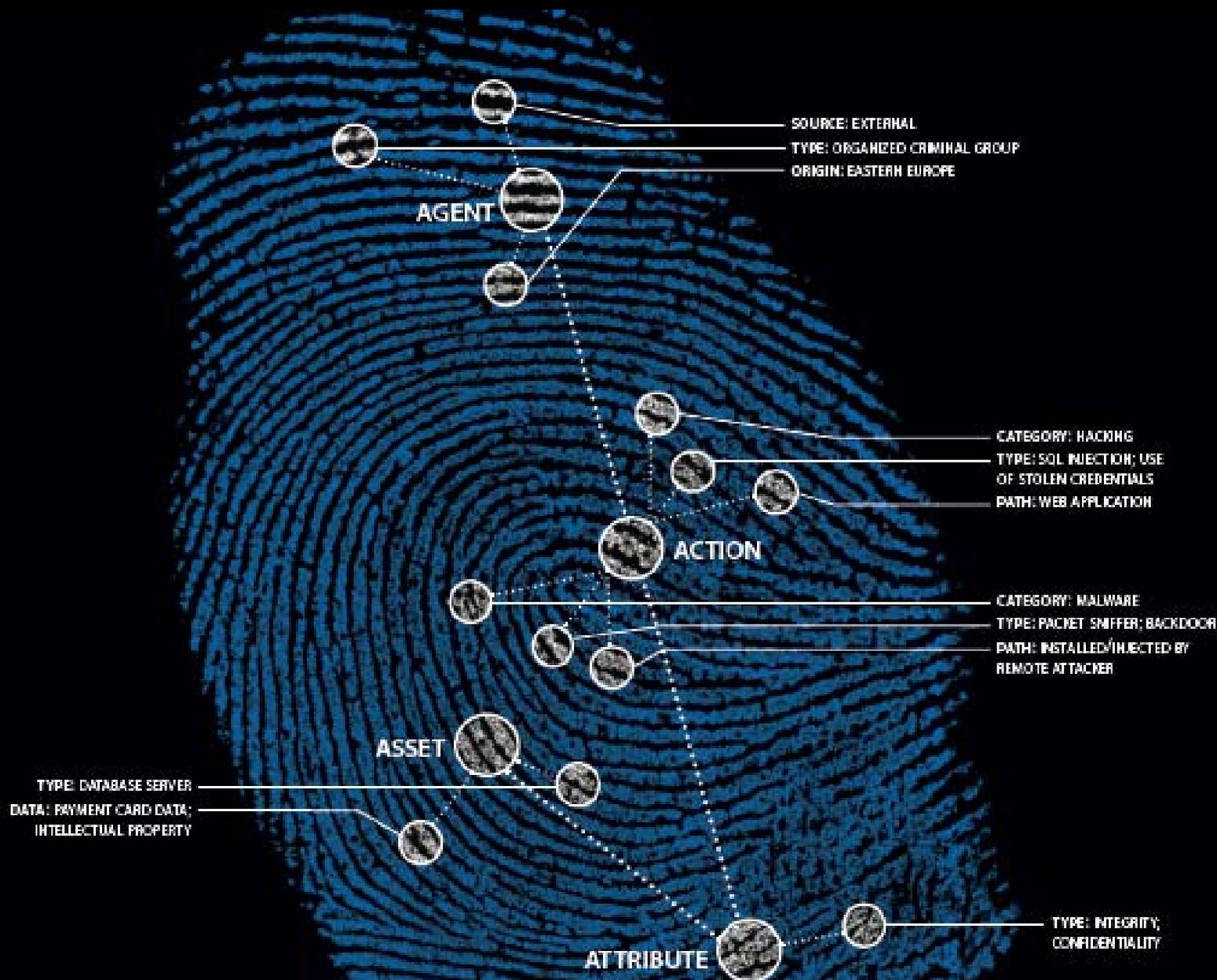
... Kontrolle ist besser



**Vertrauen ...**



# Kontrolle ...



# Das ist das Problem!

Fünf-Euro-Gutschein

## Schlecker entschuldigt sich für Datenpanne



**WELT ONLINE** Nachrichten | Debatte | Schön  
Politik | Wirtschaft | Geld | Sport | Wiss

In den Nachrichten: Thilo Sarrazin | Karstadt | Lottozahlen | Apple

01.09.10 | COMPUTERKRIMINALITÄT 👍 📧 📄 💬 (14)

### Datendiebe kosten deutsche Unternehmen Milliarden

Mittwoch, 11. Februar 2009, 15:00  
Einfacher Hackerangriff reicht  
COMPUTER BILD bei „Deutschland

Drogeriemarktkette Schlecker: Nach Datenpanne An:



enleckerstar"

## Investigators Reveal 'Massive' World Cup Data Breach

By [Chris Wright](#) on September 6th, 2010 - [1 Comment](#)



### Datenpanne bei Bank Austria

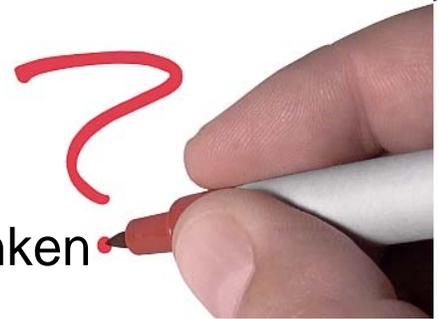
Am 5.10.2010 konnten beim Bank Austria Online-Banking Portal eingeloggte Kunden, die Finanzdaten anderer, ebenfalls angemeldeter Personen einsehen. Nach Informationen der Bank lag der Grund bei fehlerhaften Zuordnungen von Benutzersitzungen auf Grund eines Hardwareproblems. Die betroffenen Kunden wurden über den Vorfall informiert. Überweisungen sollen nicht möglich gewesen sein, so die Bank Austria.

Quelle: Weser Kurier ([Link](#))

nung. rber ellen nit

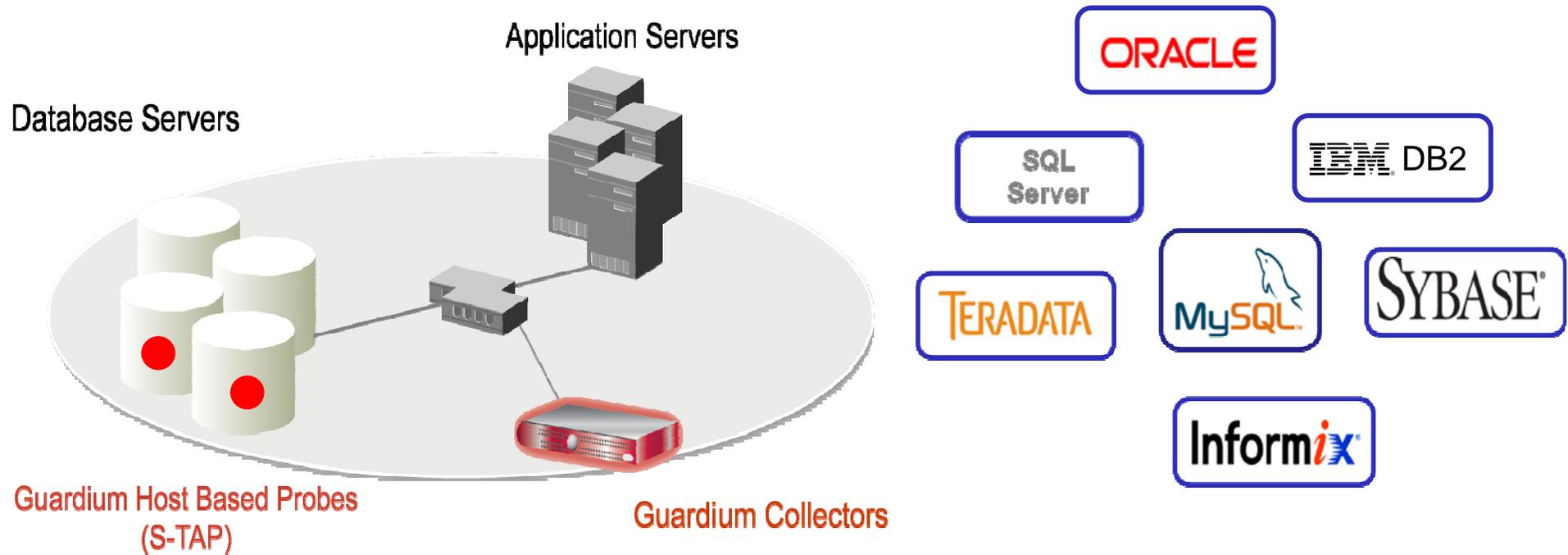
It should come as no surprise to any football fan with even a passing contempt for the game's governing body that FIFA have yet again dropped a sizeable bollock, a bollock that stands a very good chance of ruining many innocent supporters' lives.

## Sind Ihre Daten sicher ?



- Wie kann ich identifizieren und sicherstellen, ob meine Datenbanken sicher *konfiguriert* und kritische *Patches* eingespielt sind?
  
- Wo befinden sich unsere sensiblen Daten und wie vermeide ich, dass Dienstleister sensible Informationen sehen können?
  
- Wie können wir sicherstellen und überwachen, dass DBAs und andere privilegierte Nutzer ihre Zugriffsrechte nicht missbrauchen?
  
- Wie können wir in Echtzeit feststellen, wenn z.B.
  - + Mehr als 3 fehlgeschlagene Loginversuche auftreten?
  - + Jemand unautorisiert eine sicherheitsrelevante Tabelle z.B. in SAP ändert?
  - + Verdächtige Zugriffe aus dem Anwendungsserver-Account auftreten?

# Datenbanküberwachung in Echtzeit



- Nicht-invasive Architektur
  - Außerhalb der Datenbanken
  - Minimaler Einfluss auf Performance (2-3%)
  - Keine Änderungen der DBMS oder Anwendungen
- Unterstützung heterogener Systemlandschaften
- Zentralisiertes Auditing im Guardium Collector
- 100% Transparenz inkl. Zugriffe lokaler DBAs
- Realisiert Vier-Augen-Prinzip (Separation of duties)
- Verlässt sich nicht nur auf lokale DBMS logs die von Angreifern gelöscht werden können
- Granulare Regeln & Echtzeit Auditing
  - *Wer, Was, Wann, Wie*
- Automatisiertes Compliance Reporting, sign-offs & Eskalationen (SOX, PCI, NIST, etc.)

# Guardium 8 - Funktionsübersicht

- Verhindern von Cyber-Attacken
- Überwachen & Blockieren priv. Nutzer
- Erkennen von Betrugsversuchen über die Anwendungsschicht
- Änderungskontrollen
- Real-time Alerts
- Forensische Datenanalyse
- SIEM Integration

**Überwachen & Umsetzen**

- Automatisierte & zentralisierte Kontrollen
- Datenbankübergreifendes AuditRepository
  - Vorkonfigurierte Regeln/ Berichte
    - Sign-off Verwaltung
    - Archivierung (Retention)
    - Keine Datenbankänderungen
    - Keine Beeinflussung der Laufzeit

**Audit & Bericht**

- Auffinden & Klassifizieren sensiblen Daten
- Kontinuierliche Aktualisierung der Regeln
- Erkennen von Schadsoftware

**Finden & Klassifizieren**

- Feststellen von DB Schwachstellen (VA)
- Auditing von DB Konfigurationen
- Verhaltensbasierte Schwachstellen
- Vorkonfigurierte Tests basierend auf Best Practices & Standards (STIG, CIS)

**Bewerten & Verbessern**

# Peanuts ...

