Bundesverband

TeleTrusT
Pioneers in IT security.

TeleTrusT – Bundesverband IT-Sicherheit e.V.

Allianz für Sicherheit der Wirtschaft e.V. - ASW Bundesverband

TeleTrusT/ASW-Workshop "IT-Sicherheit in der Wirtschaft"

Berlin, 23.09.2015

Case Studies: Angriffe und was kann man tun?
- Mehr als 1 Trojaner -

Frank Witte, Senior Manager Cyber Security, Deloitte

Deloitte.

Case Studies: Angriffe und was kann man tun?

- Mehr als 1 Trojaner -

Frank Witte,
Senior Manager Cyber Security

09.09.2015
Wiesbaden

Deloitte.

Deloitte & Touche GmbH
Wirtschaftsprüfungsgesellschaft

Kurfürstendamm 23
10719 Berlin
Deutschland

Frank Witte
Senior Manager

Tel +49 30-25468 266
Mobil +49 151 5800 3781
frwitte@deloitte.de
www.deloitte.com/de/cyber

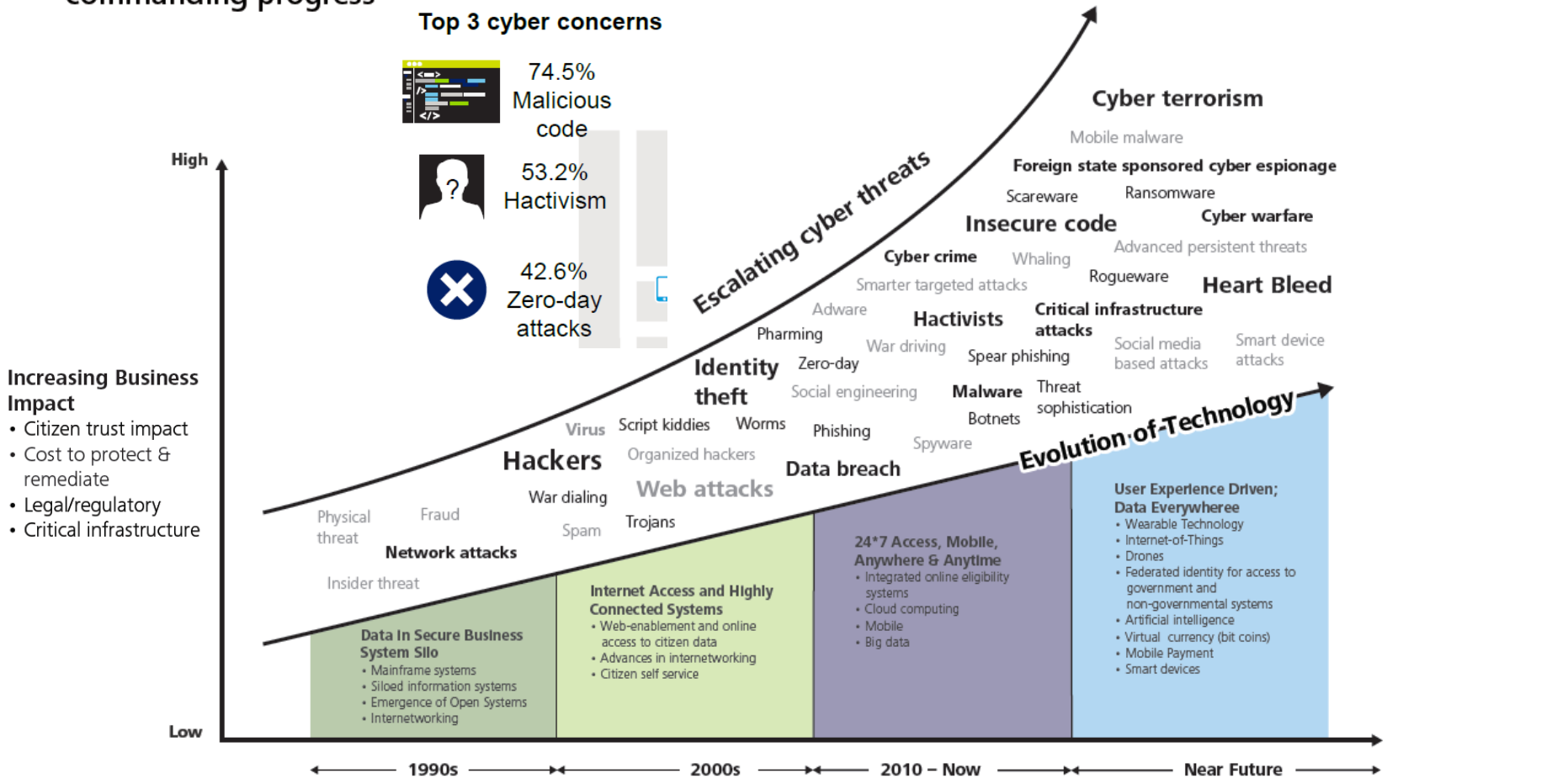
Cyber Risk Services
Öffentliche Verwaltung
& Verteidigung

Member of
Deloitte Touche Tohmatsu

APT gehören zur Cyber-Bedrohung

Komplexität von Cyber-Angriffen nimmt zu

Figure 29: Evolving technology and rapidly escalating cyber threats call for a deliberate approach to make commanding progress



*Quelle: 2014 Deloitte-NASCIO Cybersecurity Study – State government at risk: Time to move forward

© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

APT – keine Modeerscheinung

Ziel der Angriffe nach Industrien

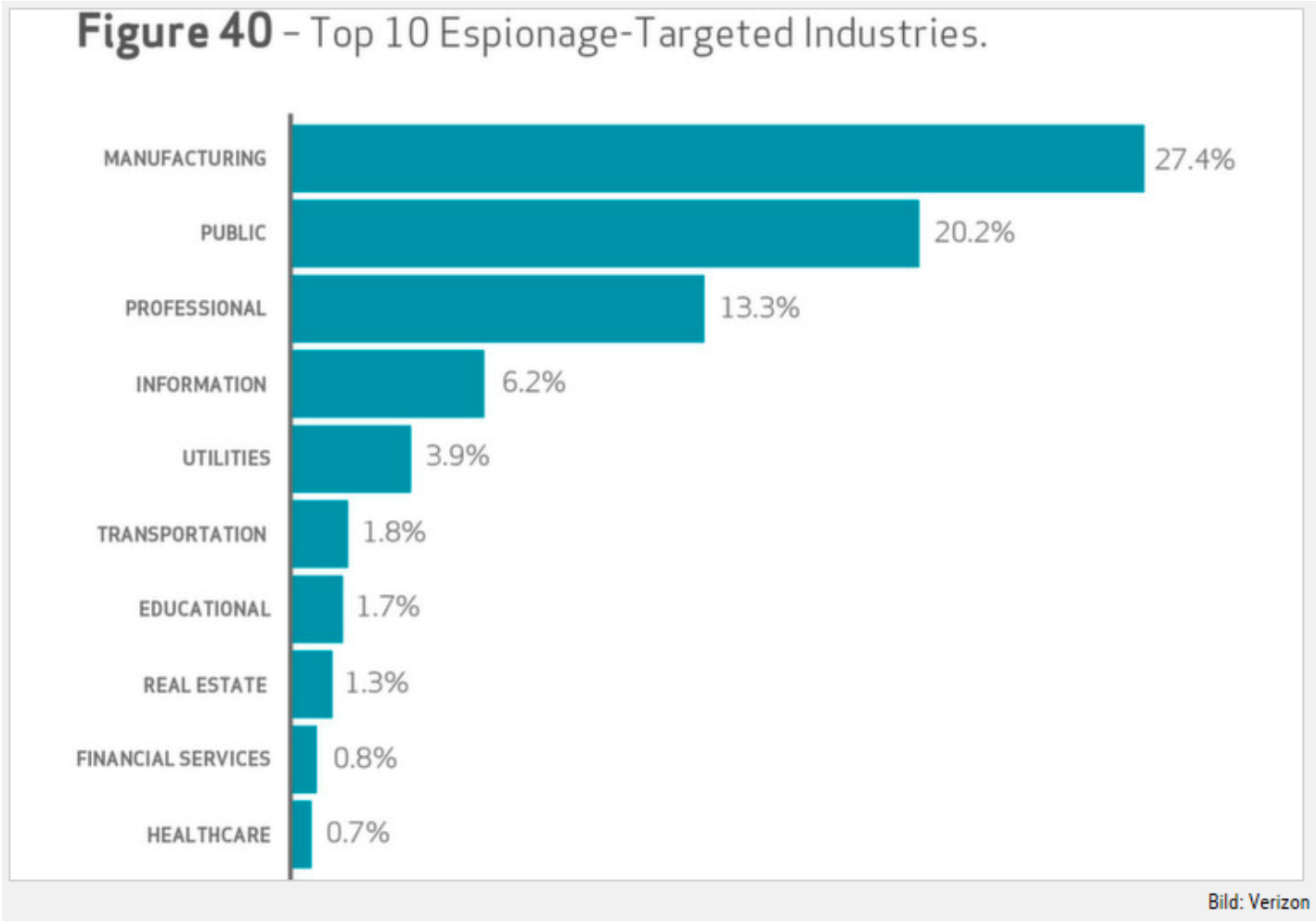


Bild: Verizon

Quelle: Verizon Data Breach Investigation Report 2015 – Security Insider Artikel “Datensicherheit muss auf die Tagesordnung!” vom 07.08.2015

© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

APT – keine Modeerscheinung

Ziel der Angriffe nach Datenkategorien

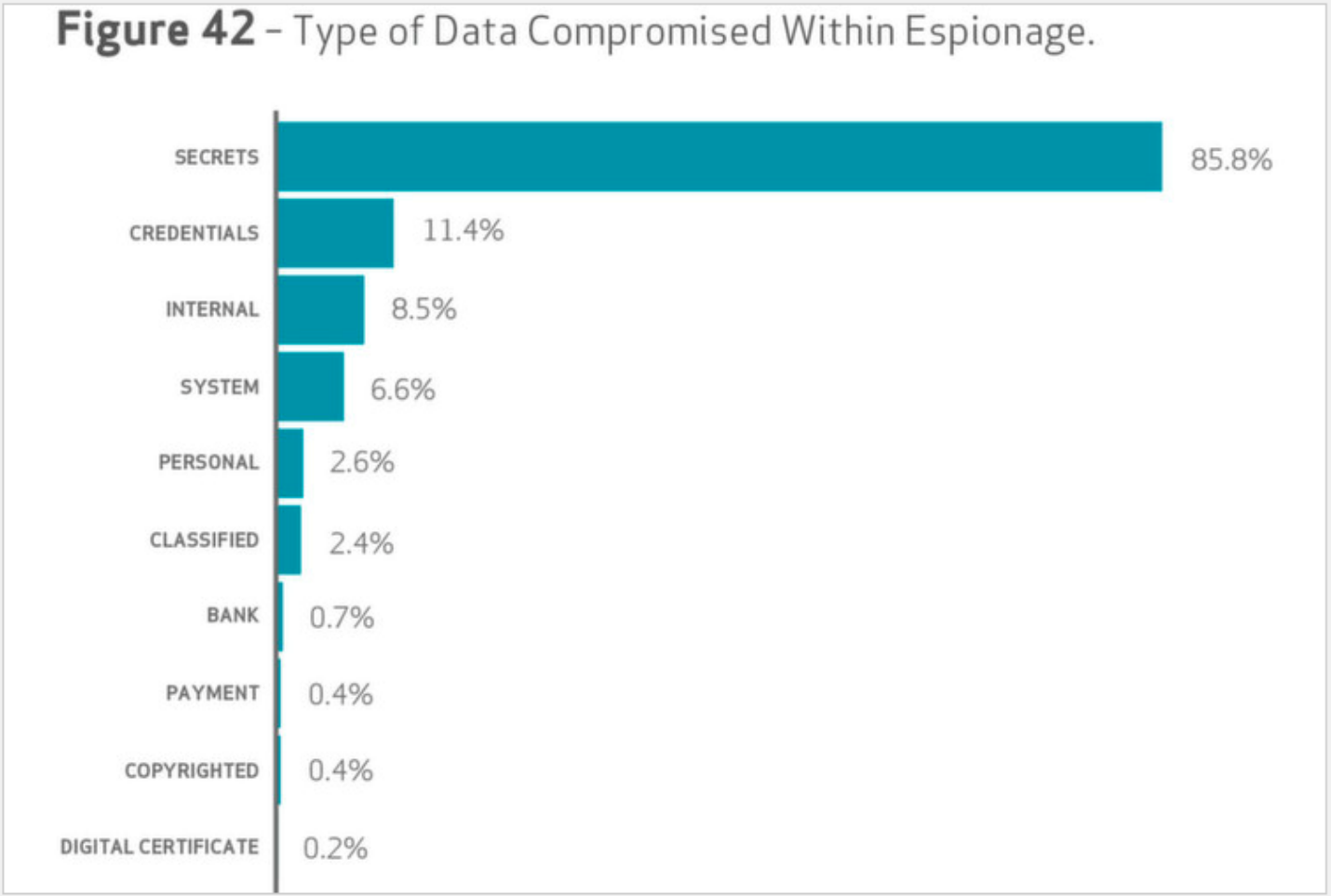


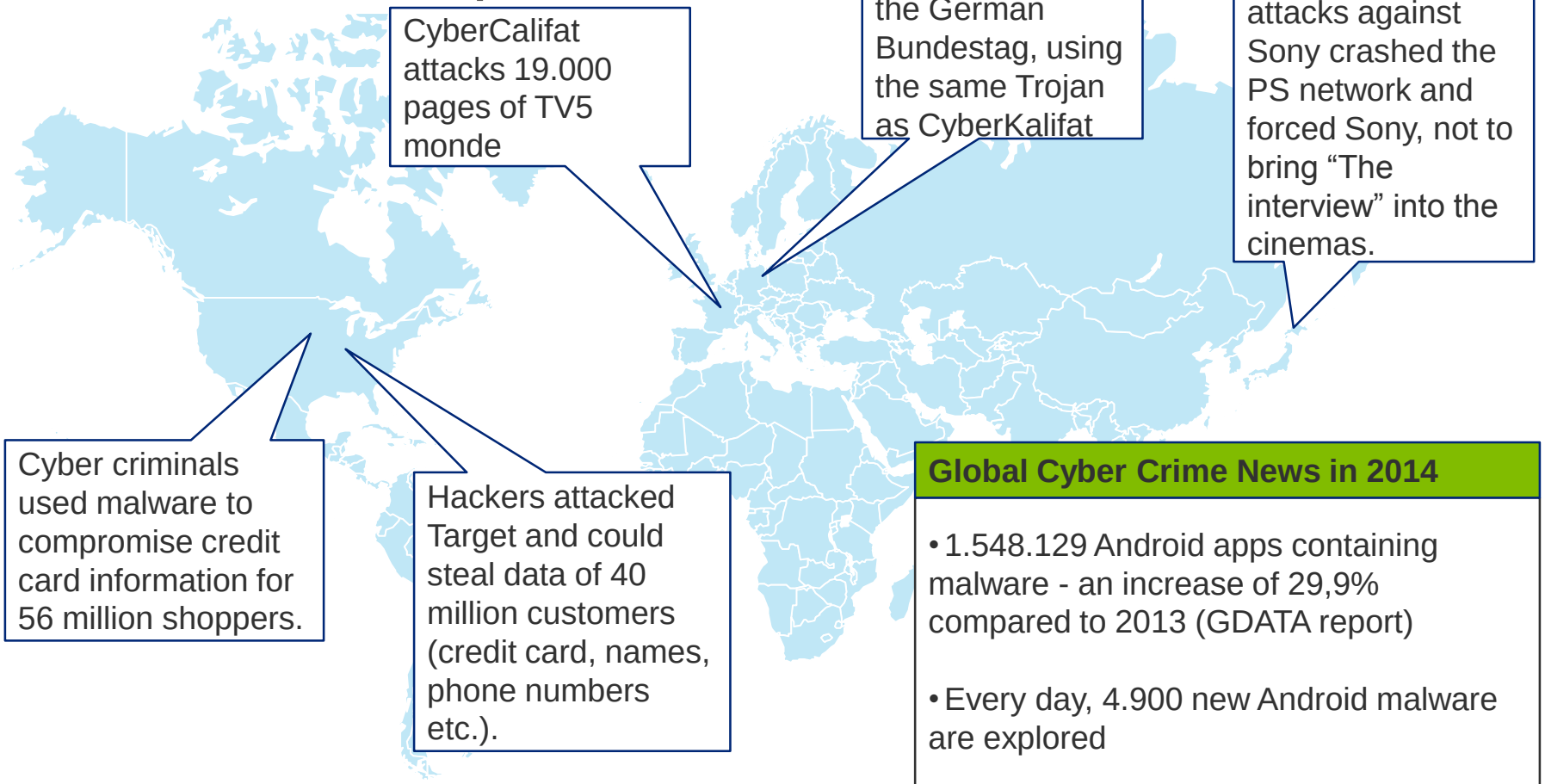
Bild: Verizon

Quelle: Verizon Data Breach Investigation Report 2015 – Security Insider Artikel “Datensicherheit muss auf die Tagesordnung!” vom 07.08.2015

© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

Cyber Bedrohungen

Threat Landscape 2014



2013’s “Cybercrime” statistic of the Bundeskriminalamt counts 64.426 Cyber Crime incidents for 2014 in Germany.

Global Cyber Crime News in 2014

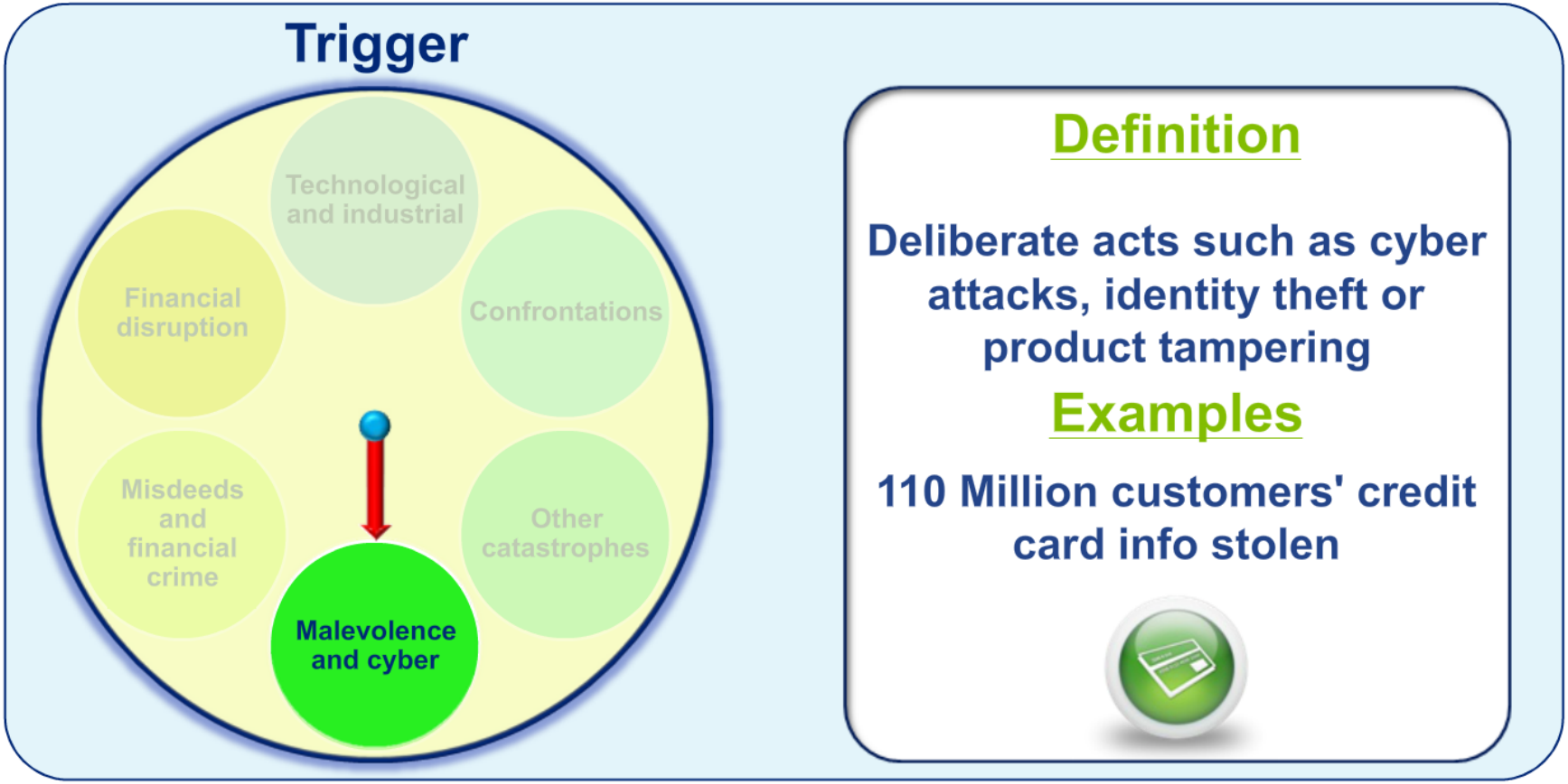
- 1.548.129 Android apps containing malware - an increase of 29,9% compared to 2013 (GDATA report)
- Every day, 4.900 new Android malware are explored
- 312 data breaches have been recorded, with 348.000.000 stolen identities

© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

Cyber – Auslöser einer Krise

APT – 110 Mio. Kreditkartendaten gestohlen

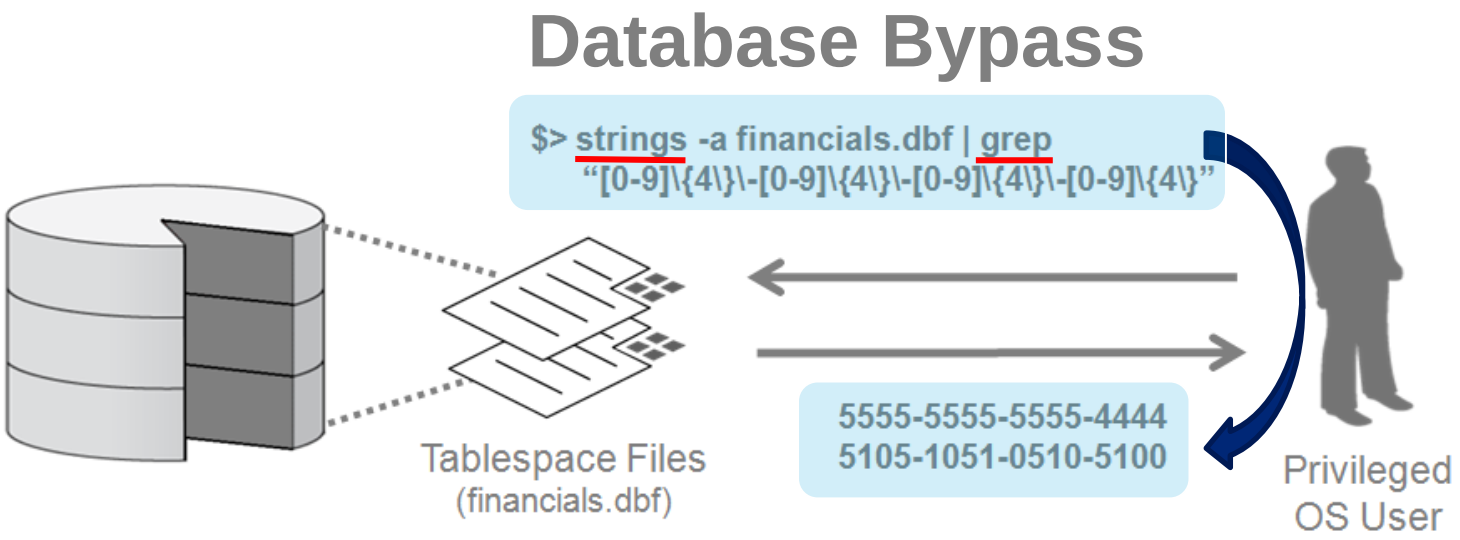
Crisis Triggers



© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

APT – Jenseits der Netze liegen die Kronjuwelen

Extrahieren von Kundenkreditkartennummern von Datenbank-tablespace files (e.g. Oracle Database 12)



30 Sek - Verwendung von Standard Unix- / Linux Betriebssystembefehlen

Zusatz für Windows XP+

© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

APT – Advanced Persistent Threat

Team 1

- Infizierung und Zerstörung der Windows Clients
- Web Attacke - Domäne eine Zeit lang vom Netz nehmen
- Störung des öffentlichen Internet-Auftritts (z.B. Social Media)

Team 2

- Manipulation der Backend Systeme
- Verwischen / Löschen von Spuren
- Ablenkungsmanöver (gegen interne und externe Experten)

Team 3

- Physikalische Angriffe auf kritische Infrastrukturen

© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

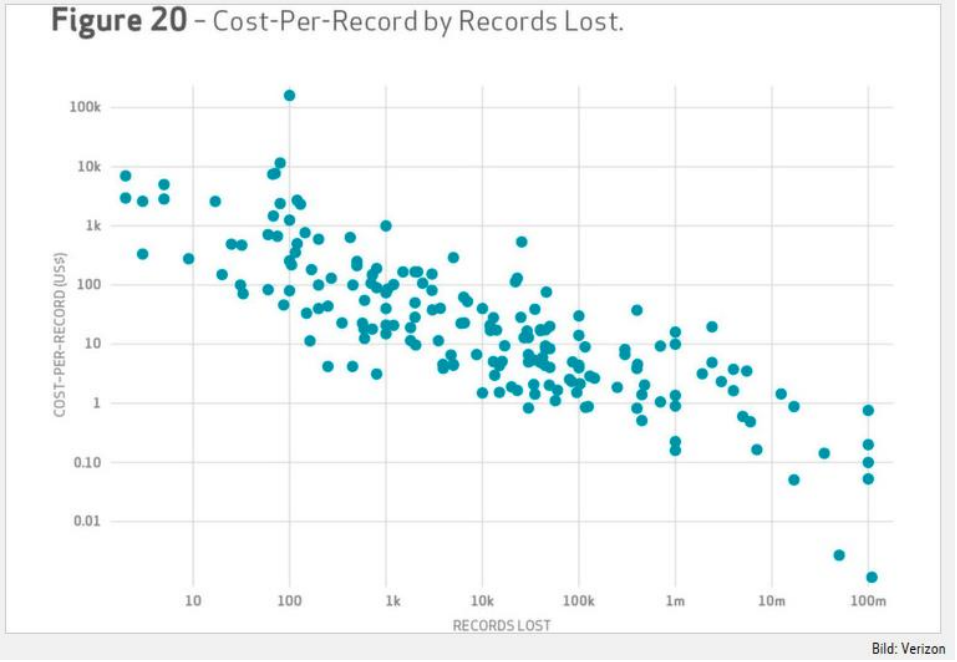
Typische Fehler

- Mangelnde Kompetenz im Sicherheitsbereich (Ablenkung erfolgreich)
- Fokus nur auf externe Sicherheit (First line of defence)
- Sicherheitsprinzip INSIDE-OUT fehlt komplett
- Zu viel Vertrauen in die Mitarbeiter
- Management hat keine Kontrolle über Sicherheit; liegt eher in der Hand von verschiedenen Technikabteilungen
- Backend Systeme hinter den Firewalls völlig ungeschützt
- Kein durchgehendes Auditing/Monitoring/Alarming Konzept
- Security Outsourcing (mehrere kleine lokale Firmen) / Ticketsystem
- Kein Notfallplan
- Keine klare Aufgabenteilung / Kein Emergency-Team
- Kosten: Billige Arbeitskräfte aus Nachbarstaaten; hohe Fluktuation

© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

Berechnung des Schadens pro Datensatz

Monetäre Auswirkung der Angriffe auf die Daten



Quelle: Verizon Data Breach Investigation Report 2015 – Security Insider Artikel “Datensicherheit muss auf die Tagesordnung!” vom 07.08.2015

Proaktiv vs. Reaktiv – Wirtschaftlichkeit Prävention

© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

„I. vs Finnland“: Umkehr der Beweislast

EuGH - “Finnische Krankenschwester”

ECHR 17 July 2008, I v. Finland, Application no. 20511/03.

Nicht die Mitarbeiterin musste beweisen, dass es unberechtigten Zugriff auf das IT-System gegeben hat.

Der Betreiber des Systems (hier: Krankenhaus) muss nachweisen, dass

1. organisatorisch und
2. Arbeitsabläufe entsprechend gestaltet sind und
3. alles nach dem Stand der Technik getan wurde,

um den unberechtigten Zugriff auf die Daten bestmöglich zu verhindern

2010 – 2014+: dies gilt nicht nur für öffentliche sondern AUCH für private ENTITÄTEN

© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

Top 6 Sicherheitsfallen im IDC Kontext

IDC Enterprise Security Survey, 2010

- Ungelöste Trennung von Aufgaben und Funktion (Separation of Duties), welche unbemerkt Accounts „Superuser“ Rechte einräumte
- Fehler in der Kontrolle der Anzahl der Nutzer mit „Superuser“ Rechten, die Zugriff zu Produktions-Databases hatten
- Nicht adäquate Datensicherung bei Kundenapplikationen
- Fehlende Möglichkeit, manuelle Prozesse zu dokumentieren und diese in das genutzte IT System zu überführen
- Nicht adäquate Absicherung des Zugriffs auf Operating Systems und Databases, welche die Finanzapplikationen und Transaktionen des Unternehmens unterstützten
- Mangelnde Überwachung der Aktivitäten von privilegierten Nutzern

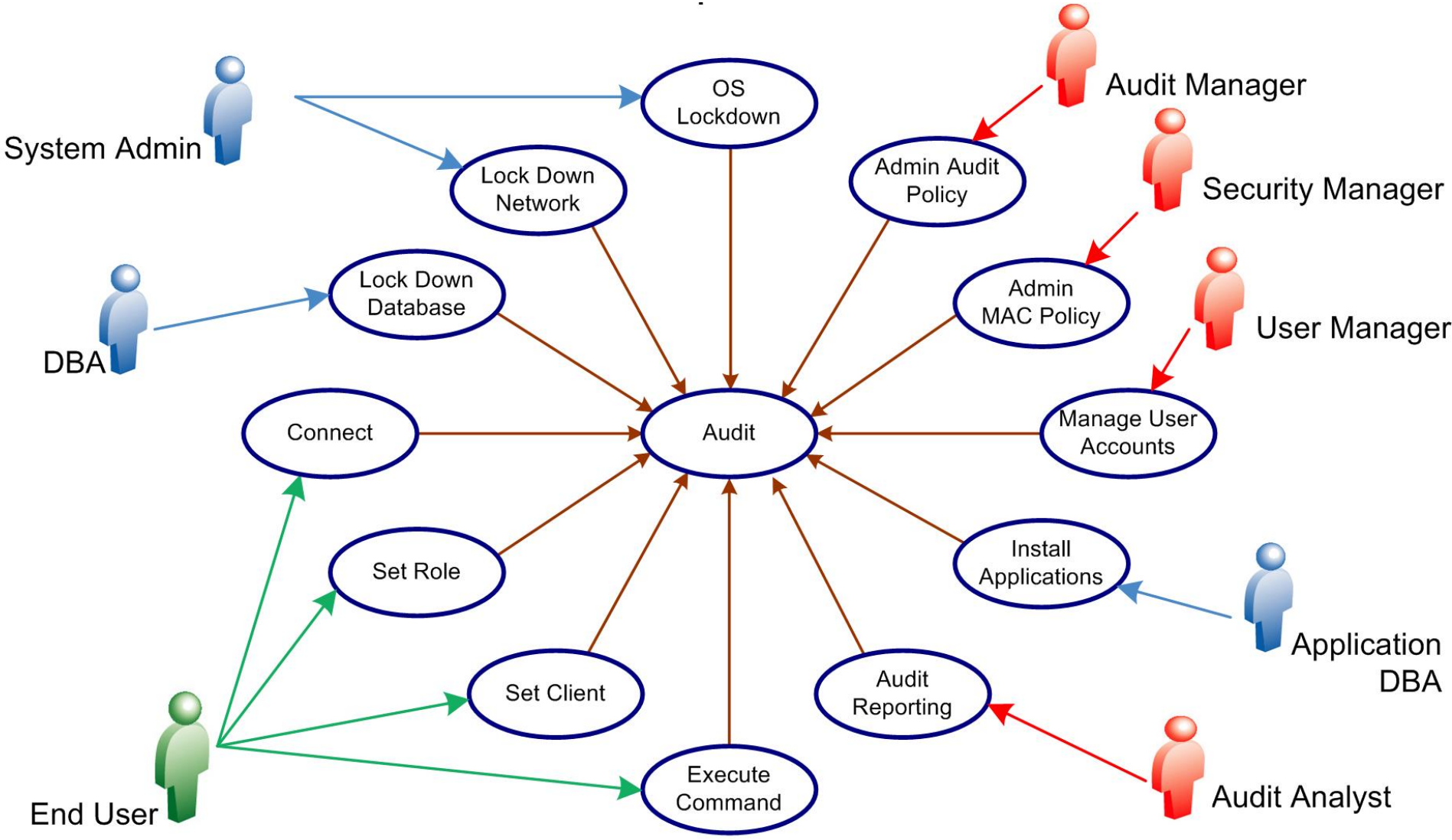
© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

Sicherheit = Datensicherheit

IDC Empfehlungen	Sicherheits-maßnahme(n)	Sicherheitsergebnisse
Database Bypass verhindern	**Verschlüsselung**	• Transparente Datenverschlüsselung für alle Applikationen, Daten oder spezifische, sensible Bereiche (optionale Verschlüsselung für „data leaving over the network“ oder via Backup)
Application Bypass verhindern	**Authorisierung**	• Absicherung von Applikations Daten vor Zugriff von berechtigten Database-Nutzern zur Sicherstellung von Integrität & Privatsphäre • Klassifizierung von Daten und Vermittlung von Datenzugriff auf einer „Need to Know“ Basis– Schutz der Privatsphäre
Zusammengefasste Audits & Compliance Berichte	**Auditierung**	• Sammeln & Zusammenfassen von Auditergebnissen über Databases von verschiedenen Zulieferern. • Application agnostic retainment historischer Daten ohne erneuter Codierung der Applikationen durch automatisches sammeln und speichern der Werte vor und nach Datenupdates als auch Detektion & Reparatur inkorrekter oder schadhafter Änderungen.
Network-Based Database Activity Monitoring & Blocking	**Überwachung & Blockierung**	• Database Firewall und Auditierung
Umfassende Sicherheit für Produktions- & Nicht-Produktionsumgebungen	**Sichere Konfiguration**	• Erkennung & Verhinderung unauthorisierter Kofigurationsänderungen
	Data Masking	• Maskierung von realen Daten mit künstlichen, aber realistischen Daten für die Entwicklung, das Testen oder Teilen mit Outsourcing Partnern.

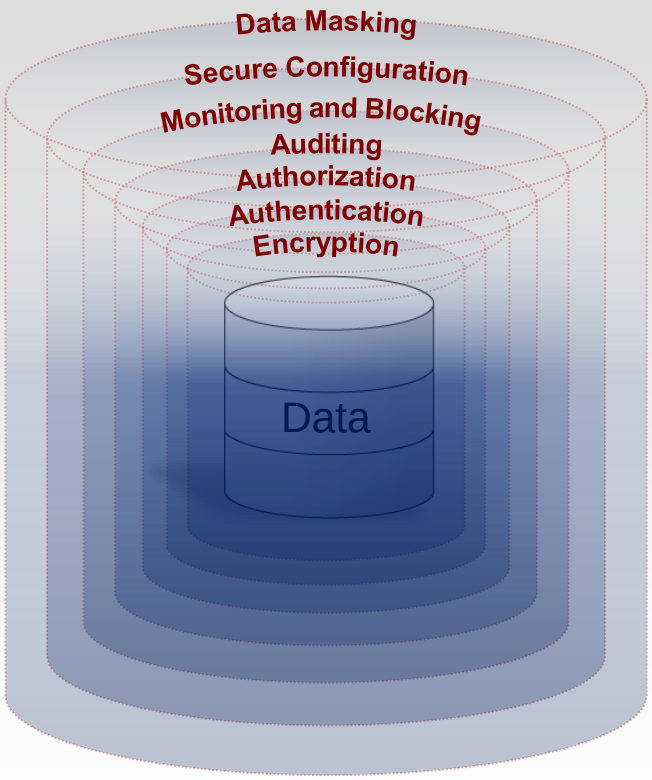
© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

“Trennung von Aufgabe und Funktion”



© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

Database Inside-Out Security

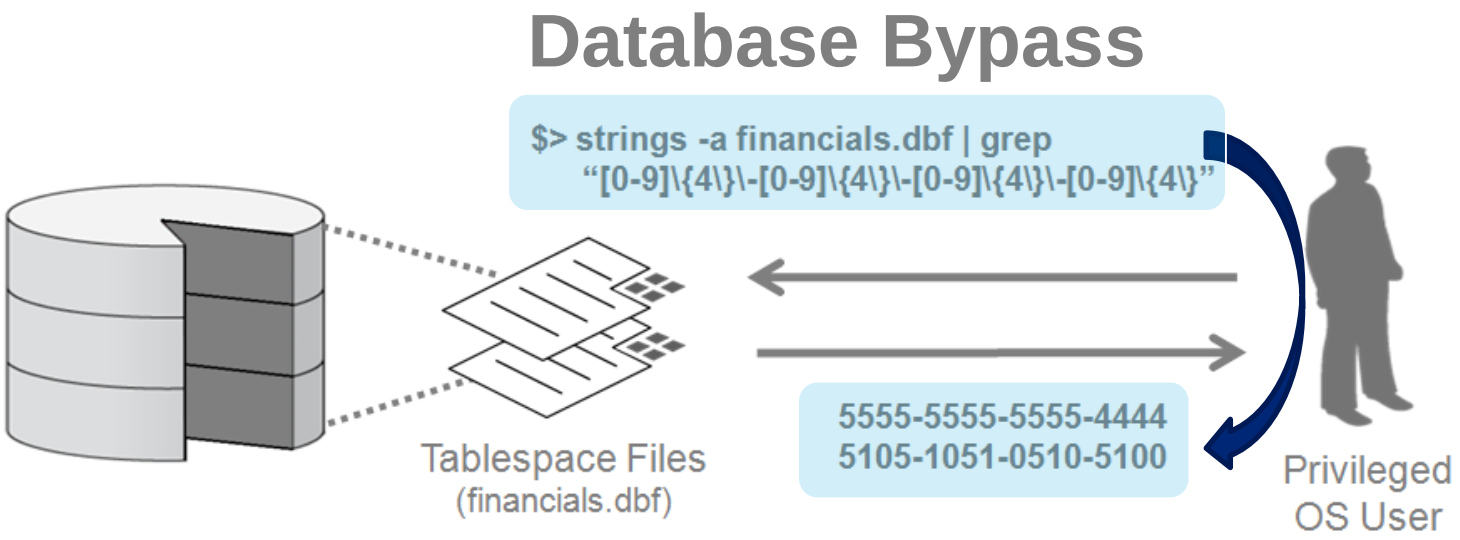


Transparente Datenverschlüsselung für alle Applikationen, Daten oder spezifische, sensible Bereiche (optionale Verschlüsselung für „data leaving over the network“ oder via Backup), Identity-Administration, Access-Management, Directory Services	**Verschlüsselung**
Absicherung von Applikations Daten vor Zugriff von berechtigten Database- Nutzern zur Sicherstellung von Integrität & Privatsphäre, Klassifizierung von Daten und Vermittlung von Datenzugriff auf einer „Need to Know“ Basis– Schutz der Privatsphäre	**Authemtifizierung/ Authorisierung**
Sammeln & Zusammenfassen von Auditergebnissen über Databases von verschiedenen Zulieferern. Application agnostic retainment historischer Daten ohne erneuter Codierung der Applikationen durch automatisches sammeln und speichern der Werte vor und nach Datenupdates als auch Detektion & Reparatur inkorrekter oder schadhafter Änderungen.	**Auditierung**
Database Firewall	**Überwachung & Blockierung**
Erkennung & Verhinderung unauthorisierter Kofigurationsänderungen	**Sichere Konfiguration**
Maskierung von realen Daten mit künstlichen, aber realistischen Daten für die Entwicklung, das Testen oder Teilen mit Outsourcing Partnern.	**Data Masking**

© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

APT – Jenseits der Netze liegen die Kronjuwelen

Extrahieren von Kundenkreditkartennummern von Datenbank-tablespace files (e.g. Oracle Database 12)

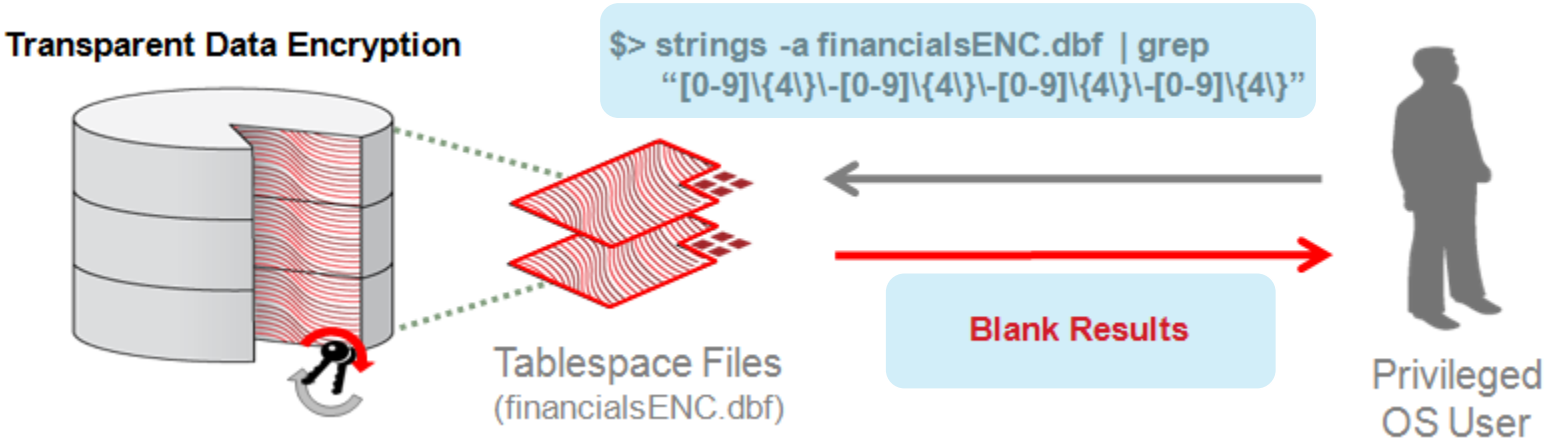


30 Sek - Verwendung von Standard Unix- / Linux Betriebssystembefehlen

© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

Schutz der Daten erhöhen

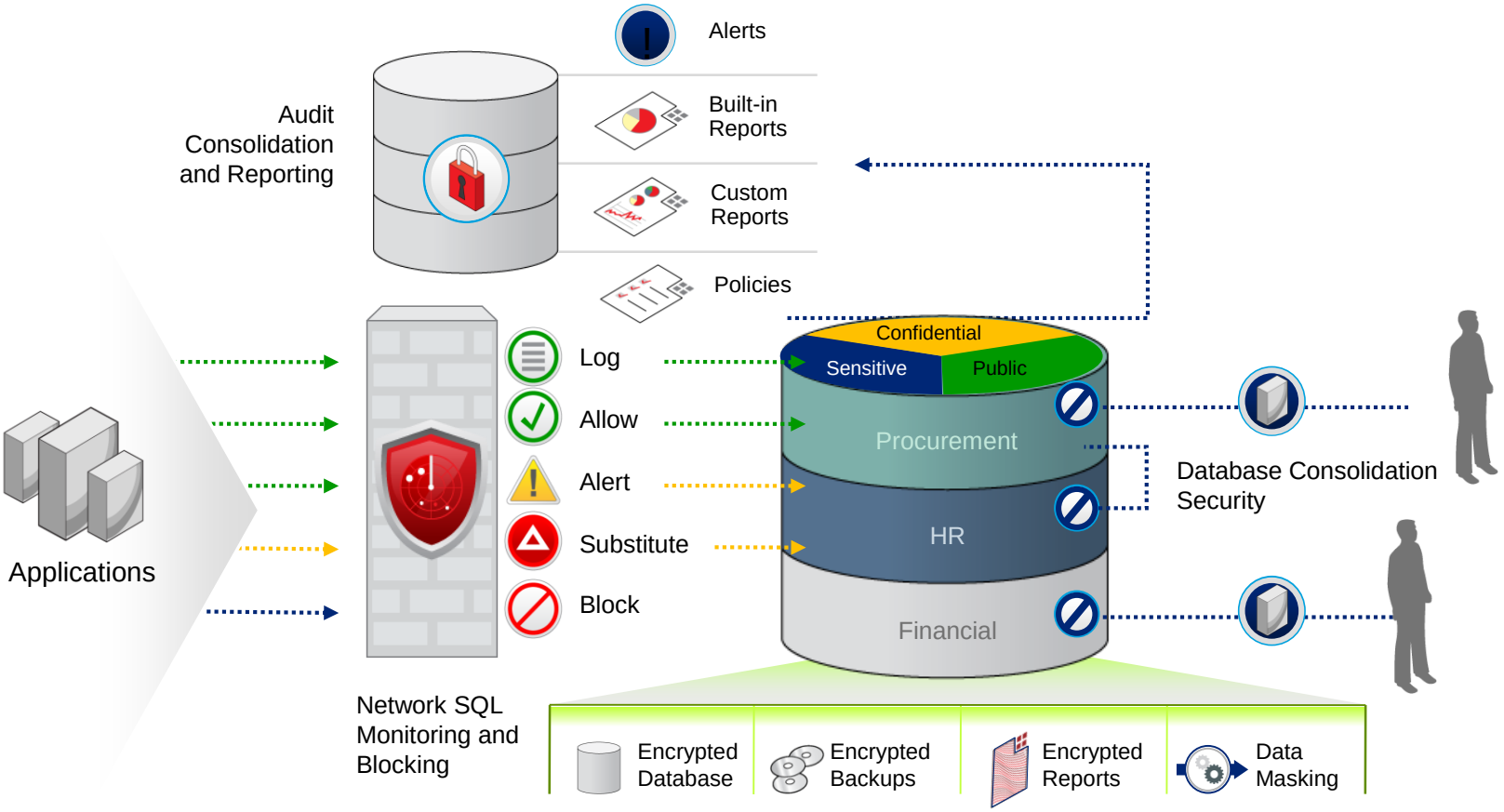
Database Bypass durch Verschlüsselung verhindern



Verschlüsselungs Algorithmus	Hash-Algorithmus (optional)
Advanced Encryption Standars (AES) Schlüssellänge: 128, 192, 256 bits	**Secure Hash Algorithm 1 (SHA 1)** Länge: 160 bits
Triple Data Encryption Standard Schlüssellänge: 168 bits	

© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

Database Security
Database Firewall



© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

Cyber Risk Services – Sicher, wachsam, widerstandsfähig

Deloittes Cyber Risk Services reichen von strategischen Ebenen bis zum globalen 24/7-Betrieb von Sicherheitssystemen mit Fokus auf einem umfassenden Schutz von kritischen materiellen und immateriellen Vermögenswerten einer Organisation (Personen, Informationen, Prozesse, Infrastrukturen und Reputation) gegenüber internen und externen Bedrohungen.

Sicherheitsstrategie und Transformation

- Sicherheitsstrategie, Planung und Nachhaltigkeit
- Organisation und Transformation
- Compliance-Management
- Informationssicherheitsmanagement
- Sicherheitskultur
- Dashboards und Berichtsmodelle

Cyber

- Cyber-Simulation und -Wahrnehmung
- Cyber-Risikobewertung und -Analyse
- Cyber-Management und -Leistungssteigerung

Sicherheits-architekturen

- Informationsschutz
- Anwendungssicherheit
- System-, Netzwerk- und Endgeräteschutz

Identitäts- und Zugriffsmanagement

- Zugriffsmodelle, -kontrolle und -verfolgung
- Autorisierungsmodelle
- Digitale Identität

Bereitschaft und Anpassungsfähigkeit

- Geschäftskontinuitäts-planung u. -management
- Krisenmanagement
- Hochverfügbarkeit, Backup und DRP

Unternehmens-sicherheit

- Integraler Sicherheitsschutz
- Unternehmens-informationen
- Infrastrukturschutz

Neue Bedürfnisse

- Sicherheit von Industriesteuerungen
- Cloud Computing und Virtualisierung
- Social-Media-Risiken
- Sicherheit mobiler Endgeräte
- Schutz kritischer Infrastrukturen

Globale Cyber Operationen

- CyberSOC – 24/7 Überwachung
- D-CIC – Deloitte Global Cyber Intelligence
- D-CIR – Deloitte Cyber Incident Response

Cyber Risk Academy

- Eigene Sicherheitszertifikate
- Fortschrittliche Sicherheitsschulungen
- Sicherheits-Tools und Produktschulungen

© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

Was können wir daraus lernen?

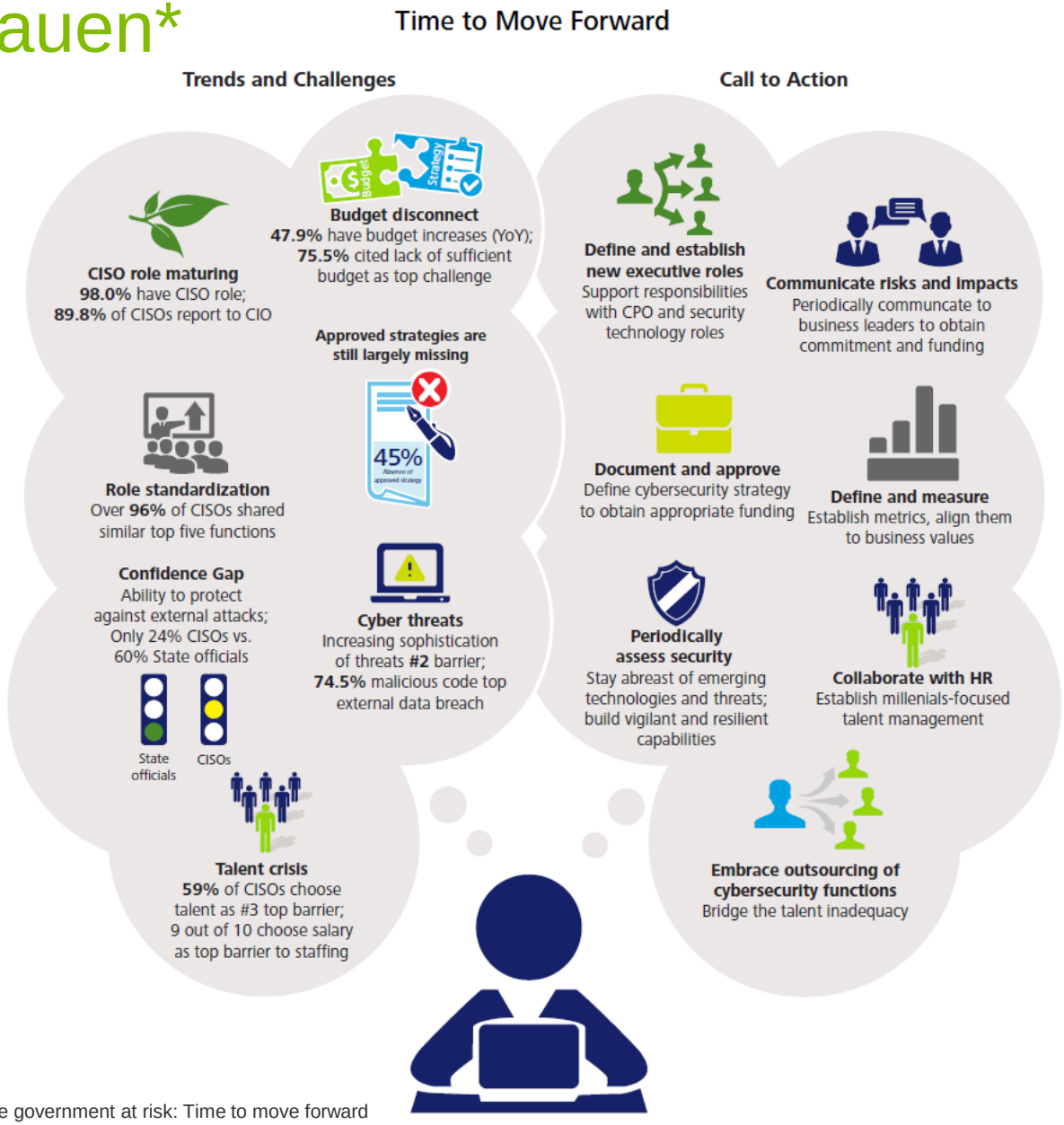
- „Standardangriffe“ werden oft als Ablenkungsmanöver genutzt
- Die Kombination „Firewall + Antivirus“ reicht nicht !!!
- Tiefergehende Analysen und Verwertung der bisherigen Vorfälle: Aus Fehlern der anderen lernen!
- Pro-Aktivität (z.B. Multi-Level Data Sec.) vs. Schadensbegrenzung
- Intensivere Einbindung von Spezialisten aus der Industrie
- Änderung der bisherigen Einstellung: „Minimale Anforderungen (vorgeschriebene Regulatorien) = maximale Sicherheit“
- Intensive Schulung der Mitarbeiter (z.B. Social Engineering)
- Besseres „clearing“ der Mitarbeiter (speziell im Outsourcing Bereich)
- Notfallpläne / Emergency Response Teams
- Schnellere Einbindung von öffentlichen Organen + externen Spezialisten
- „Think like a hacker“ - Man muss seine Feinde und deren Waffen kennen, um ihnen entgegentreten zu können !!!
- SIEM (Information Security and Event Management) kombiniert mit „Stand der Technik“, Prozessen und Organisation von Sicherheit

© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

Nach vorne schauen*

Key Findings:

- Maturing role of the CISO
- Continuing budget-strategy disconnect
- Cyber complexity challenge
- Talent Crisis



*Quelle: 2014 Deloitte-NASCIO Cybersecurity Study – State government at risk: Time to move forward

© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

Deloitte.

Deloitte & Touche GmbH
Wirtschaftsprüfungsgesellschaft

Kurfürstendamm 23
10719 Berlin
Deutschland

Frank Witte
Senior Manager

Tel +49 30-25468 266
Mobil +49 151 5800 3781
frwitte@deloitte.de
www.deloitte.com/de/cyber

Cyber Risk Services
Öffentliche Verwaltung
& Verteidigung

Member of
Deloitte Touche Tohmatsu

Deloitte.

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited („DTTL“), eine „private company limited by guarantee“ (Gesellschaft mit beschränkter Haftung nach britischem Recht), ihr Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen. DTTL und jedes ihrer Mitgliedsunternehmen sind rechtlich selbstständig und unabhängig. DTTL (auch „Deloitte Global“ genannt) erbringt selbst keine Leistungen gegenüber Mandanten. Eine detailliertere Beschreibung von DTTL und ihren Mitgliedsunternehmen finden Sie auf www.deloitte.com/de/UeberUns.

Deloitte erbringt Dienstleistungen aus den Bereichen Wirtschaftsprüfung, Steuerberatung, Consulting und Corporate Finance für Unternehmen und Institutionen aus allen Wirtschaftszweigen; Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Mit einem weltweiten Netzwerk von Mitgliedsgesellschaften in mehr als 150 Ländern und Gebieten verbindet Deloitte herausragende Kompetenz mit erstklassigen Leistungen und steht Kunden so bei der Bewältigung ihrer komplexen unternehmerischen Herausforderungen zur Seite. Making an impact that matters – für mehr als 210.000 Mitarbeiter von Deloitte ist dies gemeinsame Vision und individueller Anspruch zugleich.

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen, die nicht geeignet sind, den besonderen Umständen des Einzelfalls gerecht zu werden und ist nicht dazu bestimmt, Grundlage für wirtschaftliche oder sonstige Entscheidungen zu sein. Weder die Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited, noch ihre Mitgliedsunternehmen oder deren verbundene Unternehmen (insgesamt das „Deloitte Netzwerk“) erbringen mittels dieser Veröffentlichung professionelle Beratungs- oder Dienstleistungen. Keines der Mitgliedsunternehmen des Deloitte Netzwerks ist verantwortlich für Verluste jedweder Art, die irgendjemand im Vertrauen auf diese Veröffentlichung erlitten hat.

© 2015 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft