ORACLE®

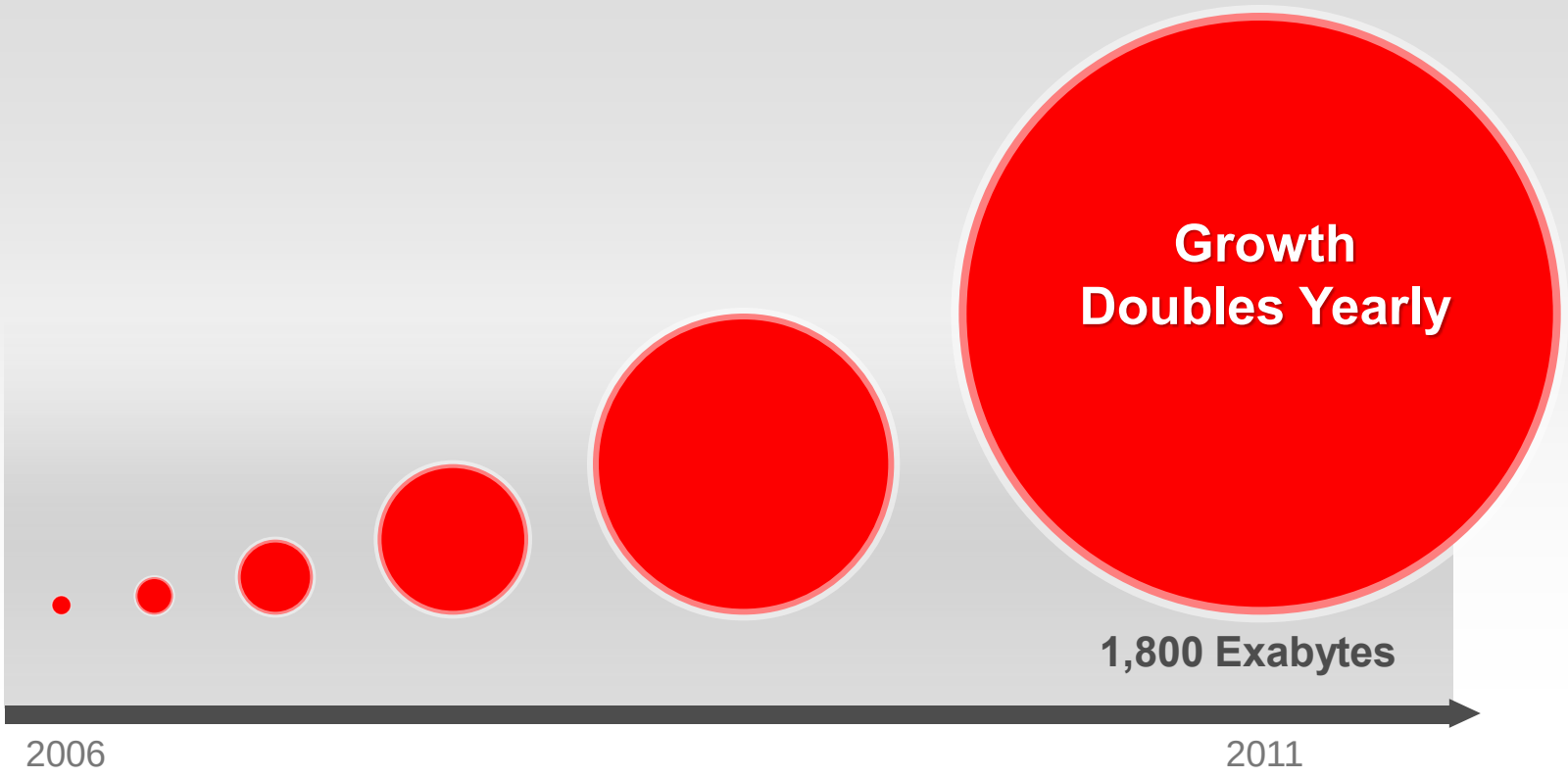
Hacking Oracle – myths and facts

Michał Jerzy Kostrzewa
EECIS Director Database Technologies
Michal.Kostrzewa@Oracle.com

Agenda

- Todays security challenges
- Who is dangerous for our business ?
- How do we get „attacked“ ?
- How can we protect ourself ?

More data than ever…

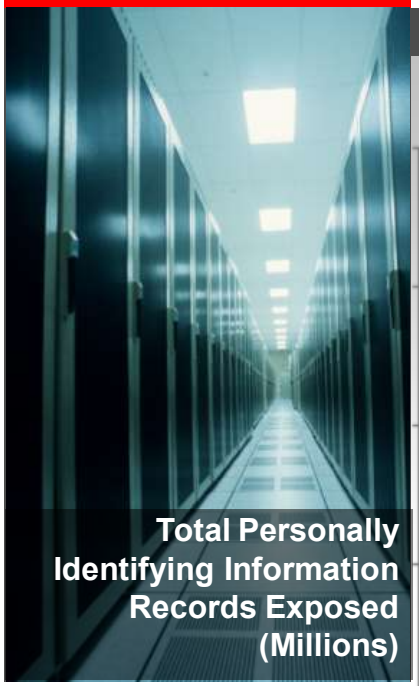


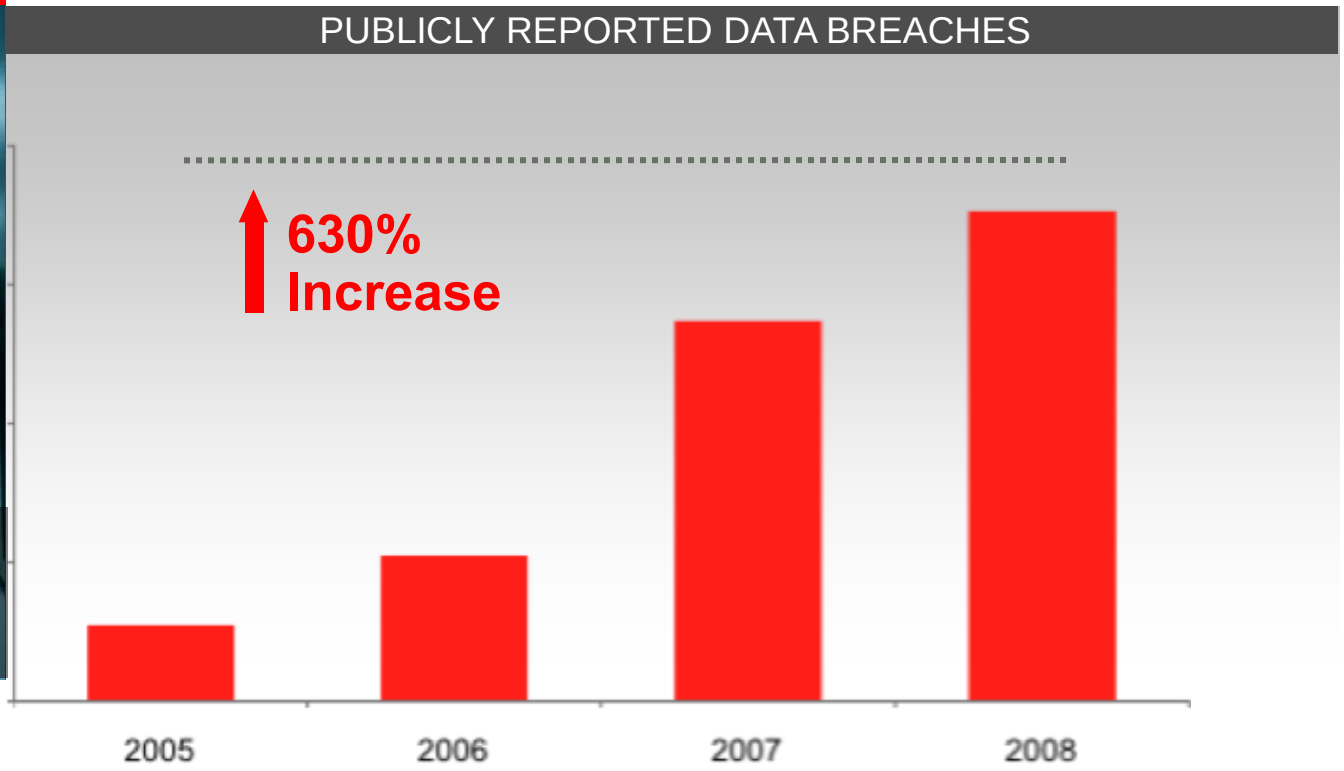
Source: IDC, 2008

More breaches then ever…

Data Breach

Once exposed, the data is out there – the bell can't be un-rung





Source: DataLossDB, 2009

More threats than ever…

More Regulations Than Ever…

90% Companies behind in compliance

Source: IT Policy Compliance Group, 2009.

Market Overview: IT Security In 2009/2010

There has been a clear and significant shift from what was the widely recognized state of security just a few years ago. Protecting the organization's information assets is the top issue facing security programs: data security (90%) is most often cited as an important or very important issue for IT security organizations, followed by application security (86%).

#1 Source of Breached Data:

92% of Records from Compromised Database Servers

Table 7. Types of compromised assets by percent of breaches and percent of records*

Type	Category	% of Breaches	% of Records
Database server	Servers & Applications	25%	92%
Desktop computer	End-User Devices	21%	1%
Web app/server	Servers & Applications	19%	13%
Payment card	Offline Data	18%	<1%
POS server (store controller)	Servers & Applications	11%	<1%
Laptop computer	End-User Devices	7%	<1%
Documents	Offline Data	7%	<1%
POS terminal	End-User Devices	6%	<1%
File server	Servers & Applications	4%	81%
Automated Teller Machine (ATM)	End-User Devices	4%	<1%
FTP server	Servers & Applications	2%	3%
Mail server	Servers & Applications	2%	4%
Customer (B2C)	People	2%	<1%
Regular employee/end-user	People	2%	<1%

verizon business

2010 Data Breach Investigations Report

Organizations Don't Protect Databases

The 2010 IOUG Data Security Report

Only 24%
can "prevent" DBAs from reading or tampering with sensitive data

68%
can not detect if database users are abusing privileges

Less than 30%
monitoring sensitive data reads/writes

48%
not aware of all databases with sensitive data

44%
say database users could access data directly

70%
use native auditing, only **25%** automate monitoring

Only 28%
uniformly encrypting PII in all databases

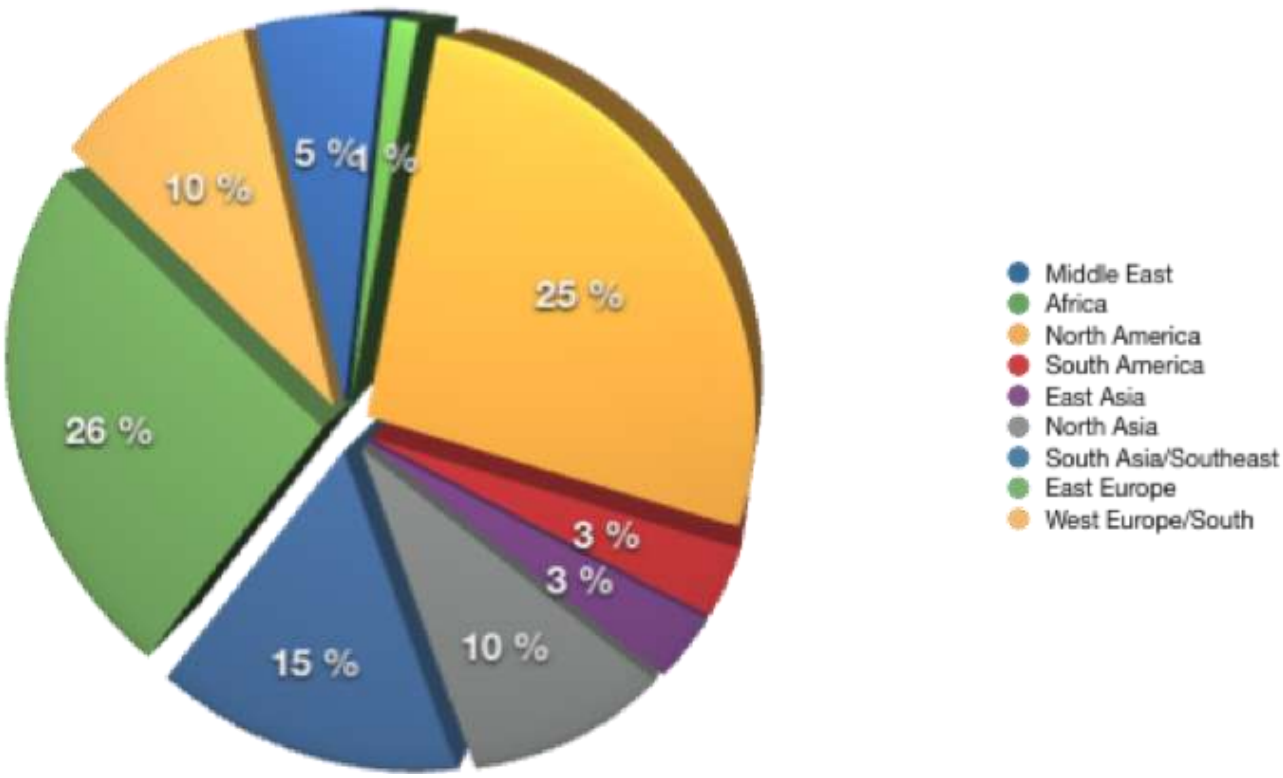
66%
not sure if web applications subject to SQL injection

63%
don't apply security patches within 3 months of release

Agenda

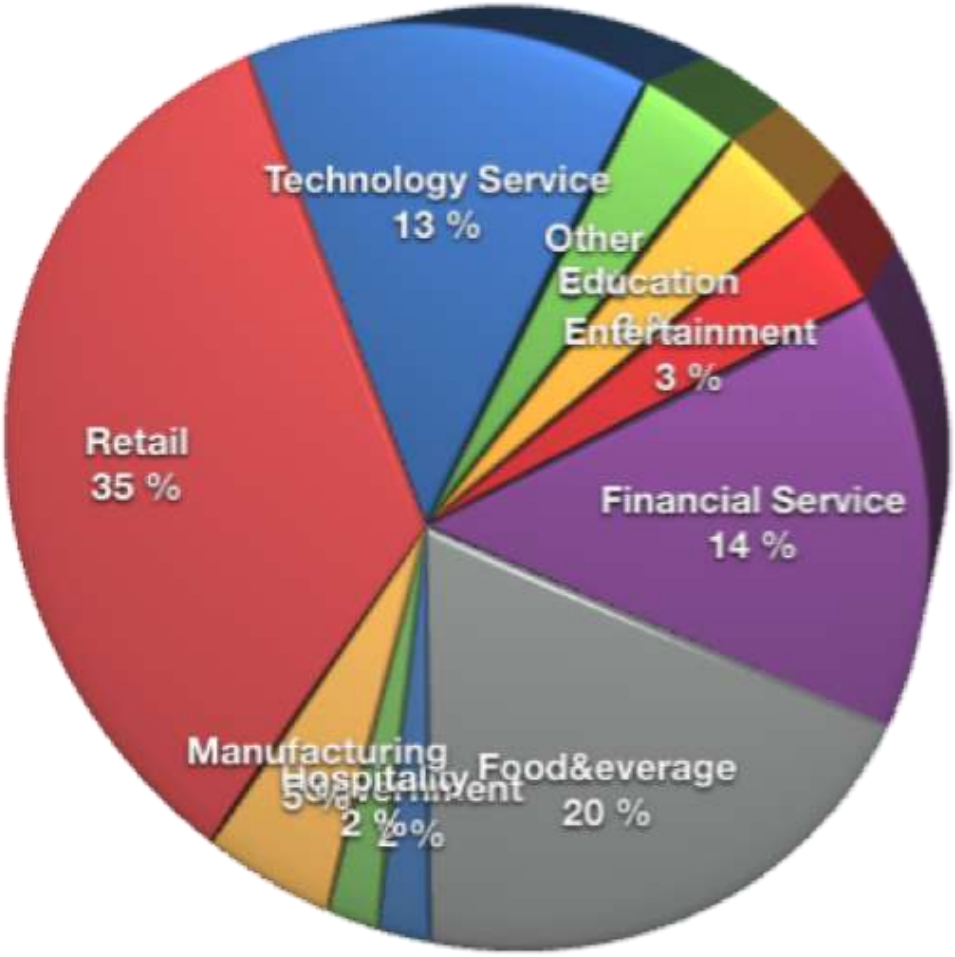
- Todays security challenges
- Who is dangerous for our business ?
- How do we get „attacked“ ?
- How can we protect ourself ?

Where does the attacks come from ?



Source: Verizon Data Breach Report 2009

Who is the target ?



Source: Verizon Data Breach Report 2009

Who is attacking us ?

Hack3rs

Insiders

Information Security Has Changed

1990

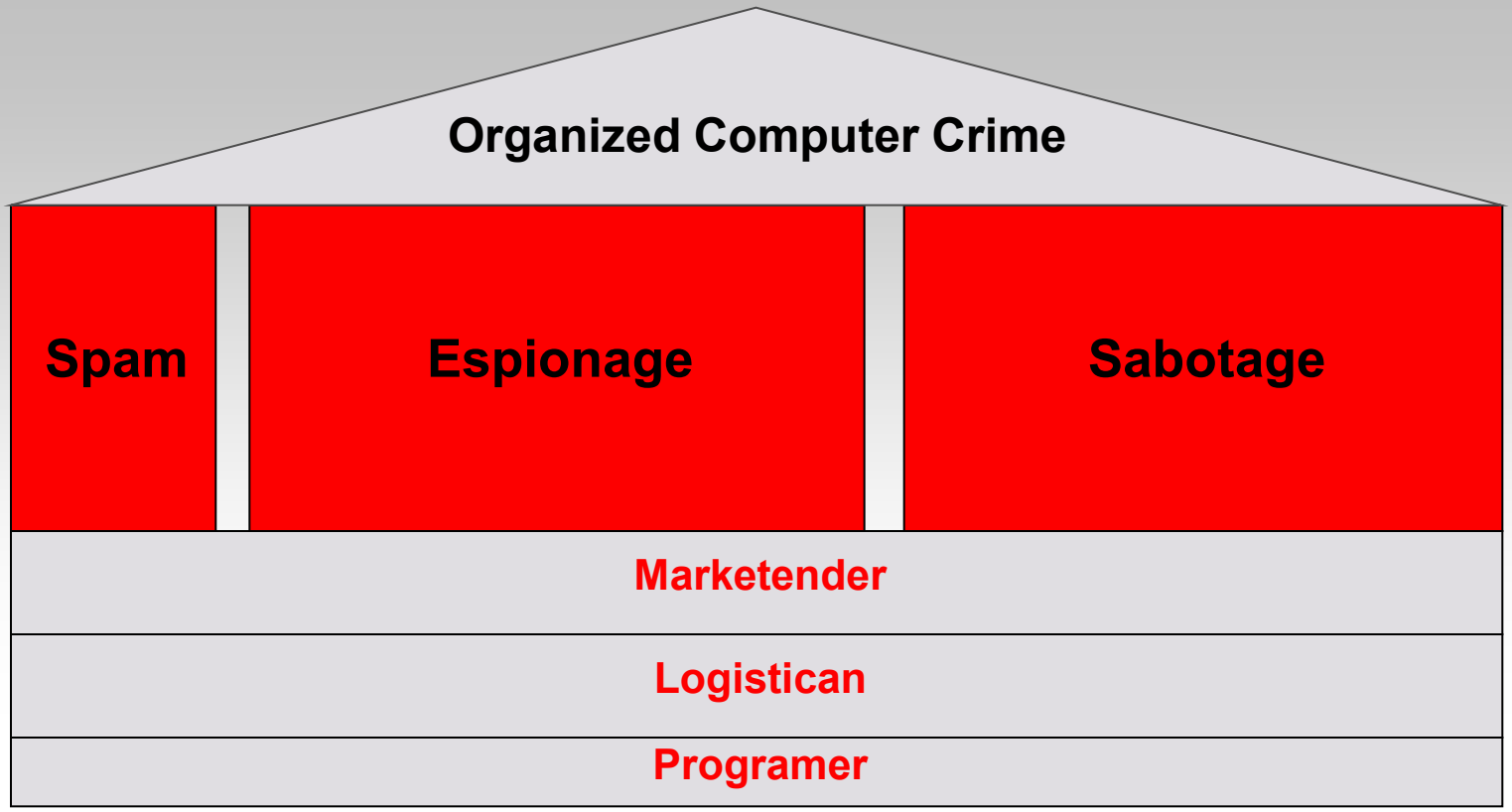
- Hobby Hackers
- Web Site Defacement
- Viruses
- Infrequent Attacks

2010

- **Rentable professional Hackers**
- Criminals
- Denial of Service
- Identity Theft
- Constant Threat

Mythos Hacker

Underground organisation



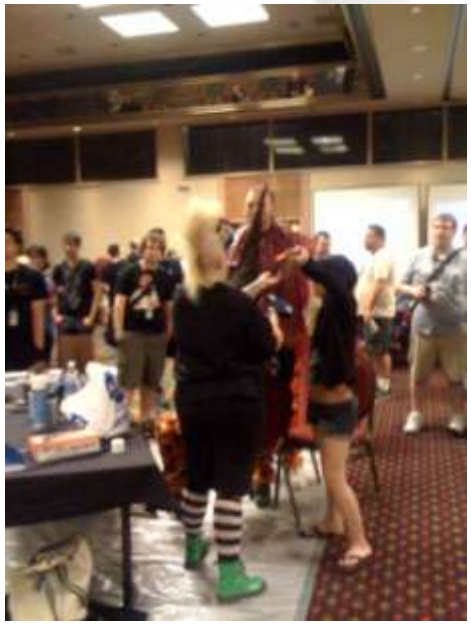

CAESARS
PALACE


USA 2010


WARNING
YOU ARE UNDER
SURVEILLANCE


DEFCON
CTF


CRACK ME IF YOU CAN
KoreLogic




blackhat

Hacking Steps

Preparation Phase	Planing Phase	HACK
• Targeting • Information collection • Social engineering • Social networking • Underground scene consolidation	• Detailed planning • Risk analysis • Staffing • Alternative plans • Methods • Techniques • Choose precautions	• Attack • Backdoor installation • Track cleaning

Official statistics
Secret Service Germany

- **Dramatical increas of the computer crime since the last 12 years (professionalism)**
- **Bigest damage by insiders (sabotage, spying, Information selling)**
- **Typical Hacker is male and over 21; BUT starts with 14 !!!**

Source: BND Sicherheitsreport 2008

Profiling Hack3rs

Criminal Energie

Classic Criminal

Prof. Hackers
Industry Spy
Secret Service

Insider

Script Kiddies

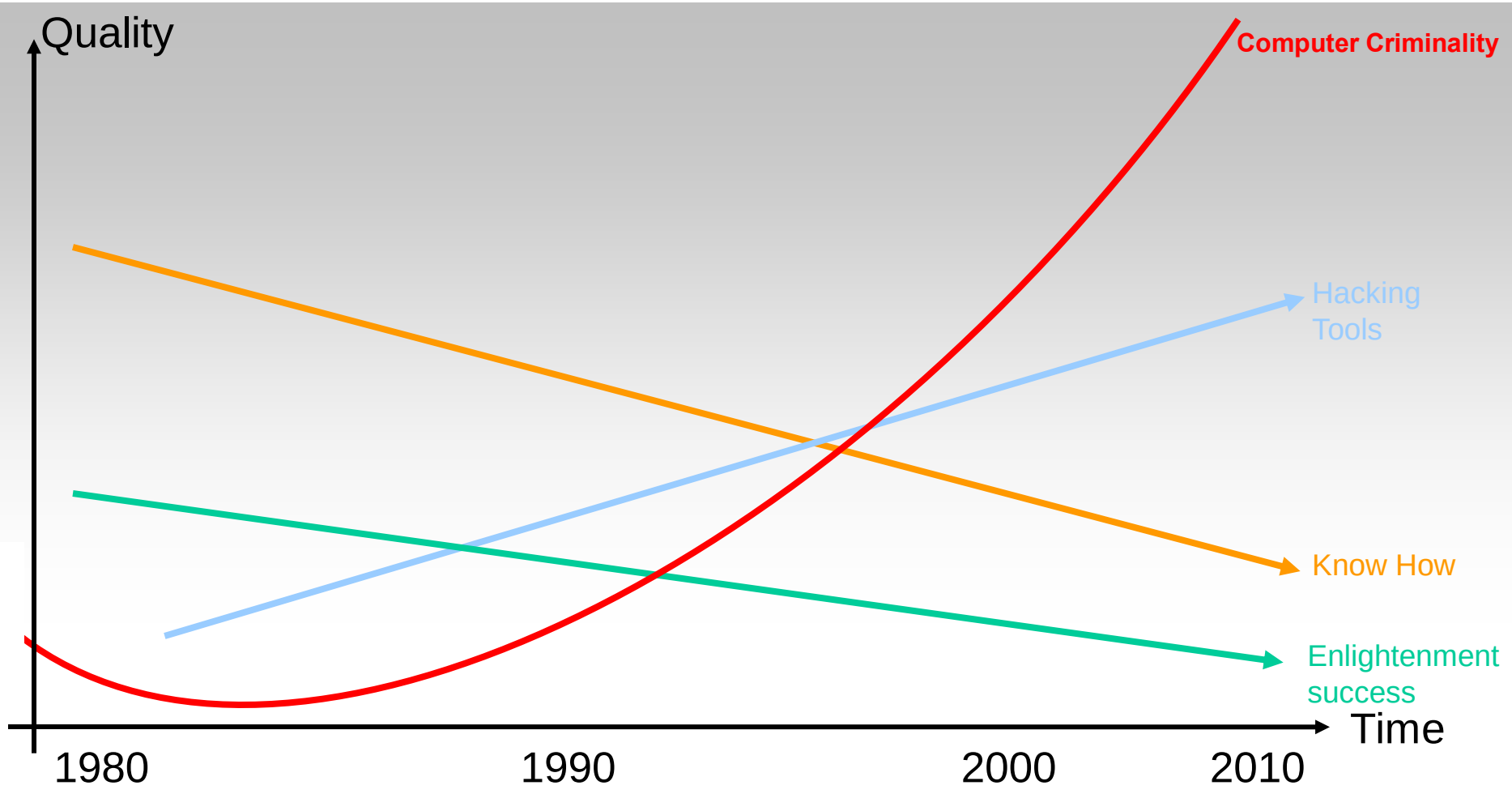
Interested computer users

Classic Hacker

discovered Hacks by police and secret service

Know How

Computer Crime Development



Source: BND Sicherheitsreport 2008

Short Facts

87 % of all Databases are compromised over the Operating System

80 % of the damage is caused by insiders

1 % of all professional hacks are only recognized

10 % of all “standard hacks” are made public

Highscore List

Source: Black Hat / Defcon (unofficial)

30sec Windows Vista

40sec Windows XP SP2

55sec Windows Vista

63sec Windows NT4.0 WKST, SP4

70sec Windows 2003 Server

140sec Linux (latest kernel)

190sec Sun Solaris with rootkit

…

List includes also AIX, HPUX, OS2, OSX, IRIX, …

Shopping List 2007/2008

Source: heise security

50.000 $	Windows Vista Exploit (4000$ for WMF Exploit in Dec2005)
7 $	per ebay-Account
20.000 $	medium size BOT network
30.000 $	unknown security holes in well known applications
25-60 $	per 1000 BOT clients / week

Crisis Shopping List 2009

Source: heise security

100.000 $	Destruction of competitor image
250.000 $	Full internal competitor database
25 $	per credit card account (+sec code + valid date)
20.000 $	medium size BOT network (buy or rent)
2000 $	stolen VPN connection
5000 $	contact to “turned around” insider

Target List 2010

Source: Black Hat / Defcon (unofficial)

Targets:

- Financial information (to sell to governments)

- Complete digital identities (personal details, financial informations, employer data, social network details, insurance and health system informations.....)

- Espionage & Sabotage (foreign industries)

- Information warfare

- Cloud based Bot-Networks

Who is attacking us ?

Hack3rs

Insiders

Insider examples !!!

European headlines 2008-2010:

- lost top secret document about Al Quaida (public train)
- stolen data of thousand prisoners and prison guards
- personal information of 70Mio people unencrypted on DVD‘s lost
- bank employee gambled with 5.4Bio US$
- 88% of admins would steal sensitive corporate informations
- Industry espionage by insiders increased dramatically
- biggest criminal network (RBN) still operating
- Tousends of stolen hardware equipement @ US Army
- US Army lost 50.000 personal data of former soliers
- Chinas „Red Dragon“ organization cracked german gov network
- Lichtenstein Affaire – Insider vs. Secret Service
- Swiss Tax DVD sold to government
- ...

Insider Threat

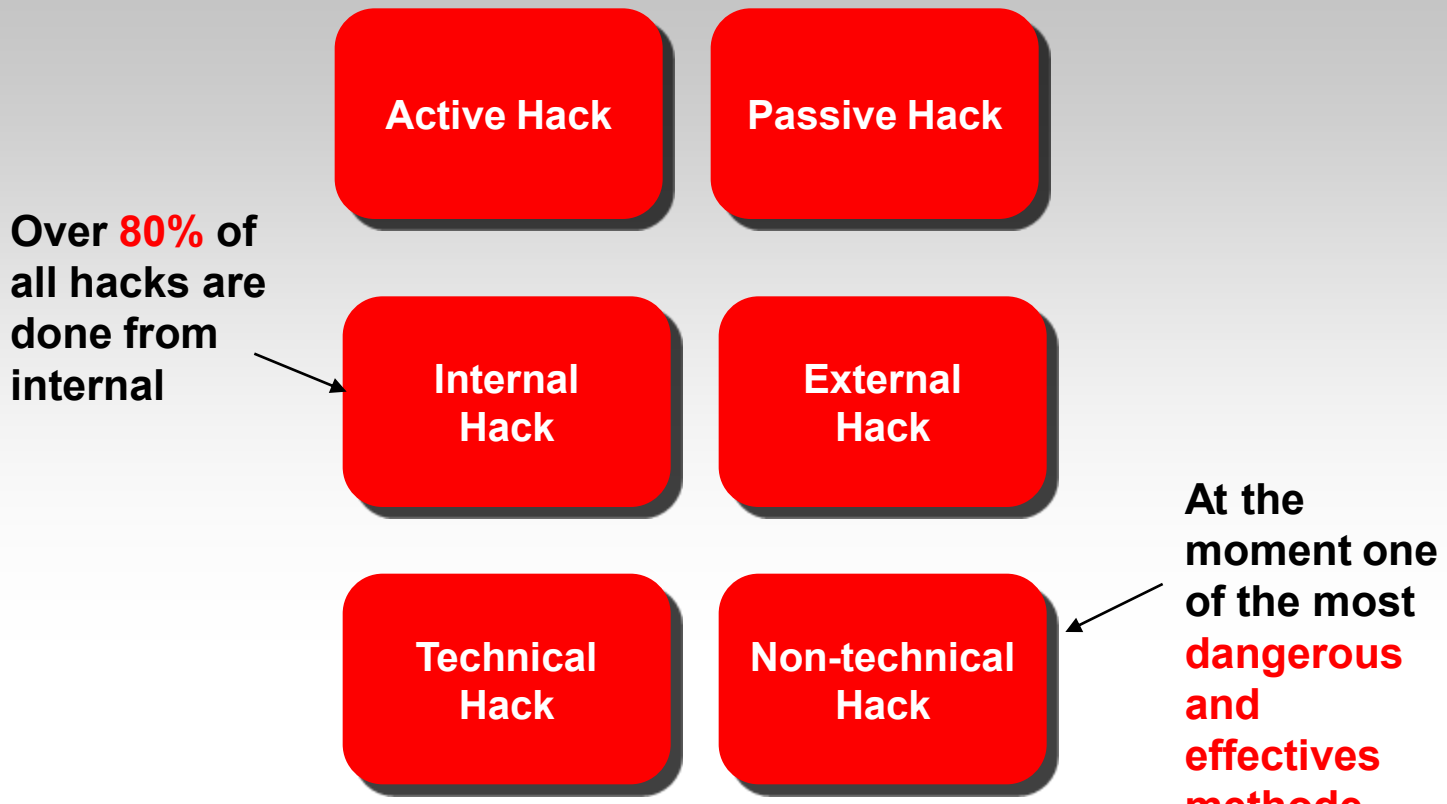
- Companies: min. requirements = max. security
- Outsourcing and off-shoring trend
- Large percentage of threats go undetected

  - huge internal know how
  - powerful privileges
  - track cleaning
  - „clearance“ problem
  - foreign contact persons / turnovers

Agenda

- Todays security challenges
- Who is dangerous for our business ?
- How do we get „attacked“ ?
- How can we protect ourself ?

How we get attacked



How we get attacked -- REALITY

>90%

- Standard configuration
- Misconfiguration
- Misunderstanding of security
- Human errors
- Process/Workflow errors
- “old” versions / no patches
- Known/published wholes/bugs/workarounds
- Downloadable cracking software (script kiddies)

- High quality/knowledge hack

Agenda

- Todays security challenges
- Who is dangerous for our business ?
- How do we get „attacked“ ?
- How can we protect ourself ?

Protection

> 90%

of our security problems

could be solved !!!

Think …

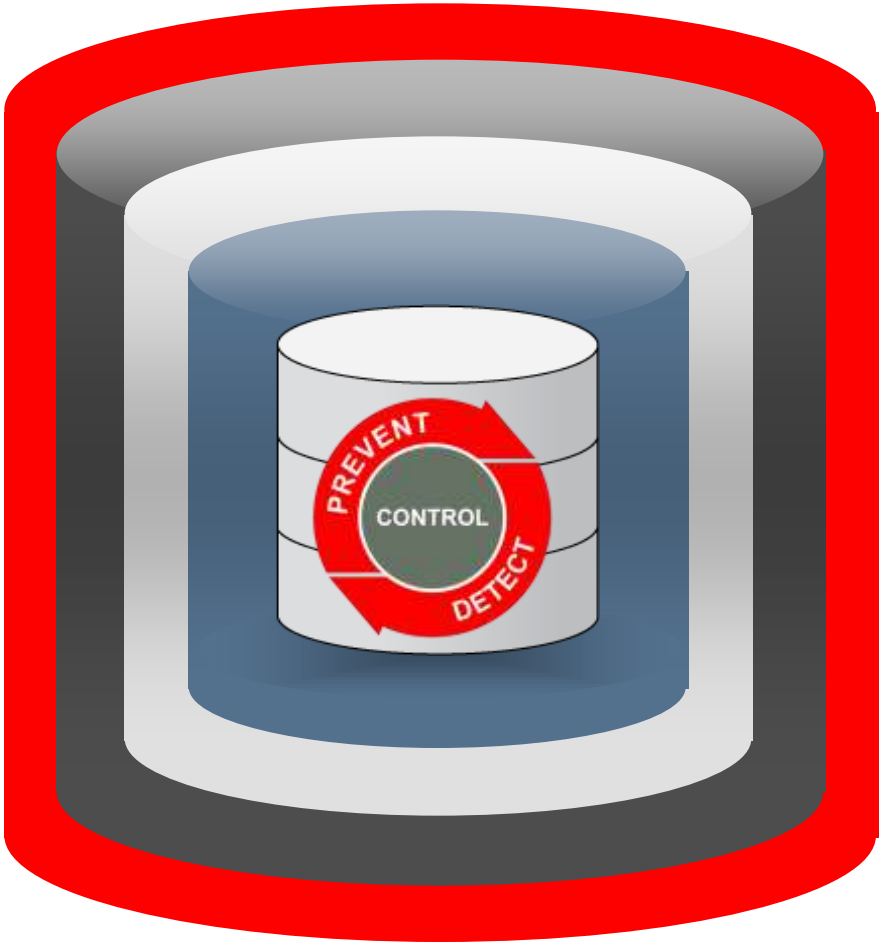
- Security is a „race“, if you stop running you‘ll lose
- Security IS NOT a product; it‘s an ongoing living process
- Train your employees
- Security IS an intelligent combination of more areas
  -> „Big picture“
- Focus on your data, not only on the technic
- Start with the basics

Think about Solutions…

Problem	Oracle Solution	Oracle Security Product
• External Attackers • Internal Threats • Image Damage • Internal Security Regulations • Regulatory Compliances • .. • .	• **Separation of duties** • **Insider threat protection** • **Strong access authentication** • **Strong encryption (DB/OS/Net)** • **Fine grained real time external auditing** • **Data consolidation control** • **High availability + Security combination** • **Firest line of defence**	• Oracle Firewall • Advanced Security Options (ASO) • Network encryption • Transparent data encryption • Strong authentication • Database Vault • Audit Vault • Secure Backup • Virtual Privat Database (VPD) • Oracle Label Security (OLS) • Data Masking • Total Recall

Oracle Database Security Solutions

Inside. Outside. Complete.



Encryption & Masking

- Advanced Security
- Secure Backup
- Data Masking

Access Control

- Database Vault
- Label Security
- Identity Management

Monitoring

- Configuration Management
- Audit Vault
- Total Recall

Database Firewall


ORACLE®