

ORACLE®

Hacking Oracle – myths and facts

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



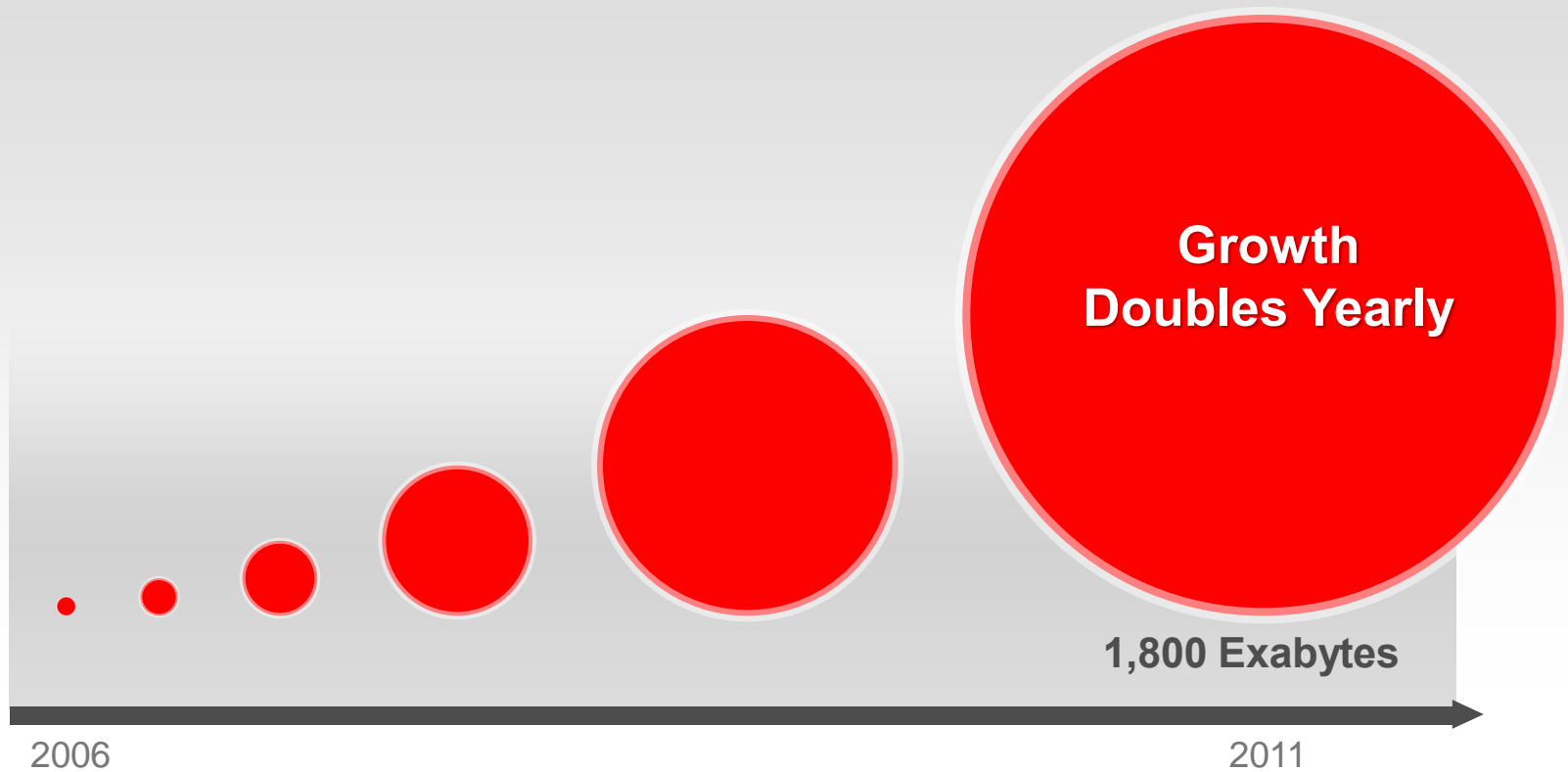
Agenda



Oracle Database Security

- **Today's security challenges**
- Who is dangerous for our business ?
- How do we get „attacked“ ?
- How can we protect ourselves ?

More data than ever...



Source: IDC, 2008

More breaches than ever...

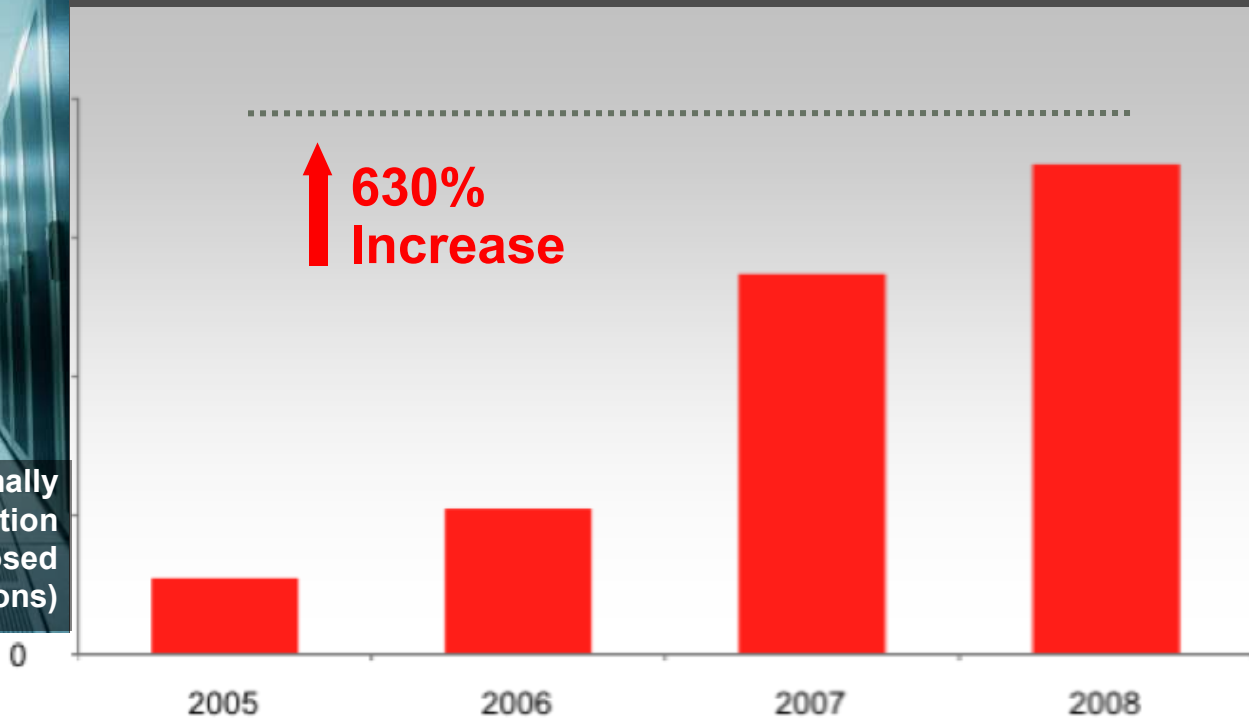
Data Breach

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

PUBLICLY REPORTED DATA BREACHES



Total Personally Identifying Information Records Exposed (Millions)



Source: DataLossDB, 2009

More threats than ever...

CyberInsecure.com
Daily Cyber Threats And Internet Security News Alerts

HOME ARCHIVES CONTACT ABOUT EMAIL SUBSCRIBE ADVERTISE

August 5th, 2008

Countrywide Financial Insider Steals And Sells Thousands Of Private Customer Records

The FBI on Friday arrested a former Countrywide Financial Corp. employee and another man in an alleged scheme to steal and sell sensitive personal information, including Social Security numbers, of as many as 2 million mortgage applicants. The breach in security, which occurred over a two-year

BANK INFO SECURITY
Bank Information Security Articles
Fannie Mae Consultant Indicted
Fired Programmer Accused of Planting Malware
January 30, 2007 - Linda McGlasson, Managing Editor

NETWORKWORLD
News | Blogs & Columns | Subscriptions
Security | LANs & WANs | VoIP | Infrastructure Mgmt | Wireless | Software
Anti-Malware | Compliance & Regulation | Desktop Firewall / Host PS | Enterprise Firewall

Insider theft at New York Police Dept. impacts cops

Former pension fund executive is accused of stealing computer tapes
By Steve Mizer, Network World, 03/06/2008

ShareEmail Buzz up 1 Comment Print

The New York Police Department (NYPD) is telling thousands of police of personal information may be compromised due to a suspected data theft in the police pension fund, according to reports in New York's daily news

Re: Recent Pfizer Data Breach

Dear General Ayotte:

I am writing to give you advance notice of a data privacy breach affecting our client, Pfizer Inc ("Pfizer"), and an estimated 34,000 current employees, former employees, health care professionals and other individuals. It appears that the breach developed when a Pfizer employee wrongfully removed copies of confidential information from a Pfizer computer system

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%



2010 Data Breach
Investigations Report

Organizations Don't Protect Databases



The 2010 IOUG Data Security Report

For the Complete Technology & Database Professional

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

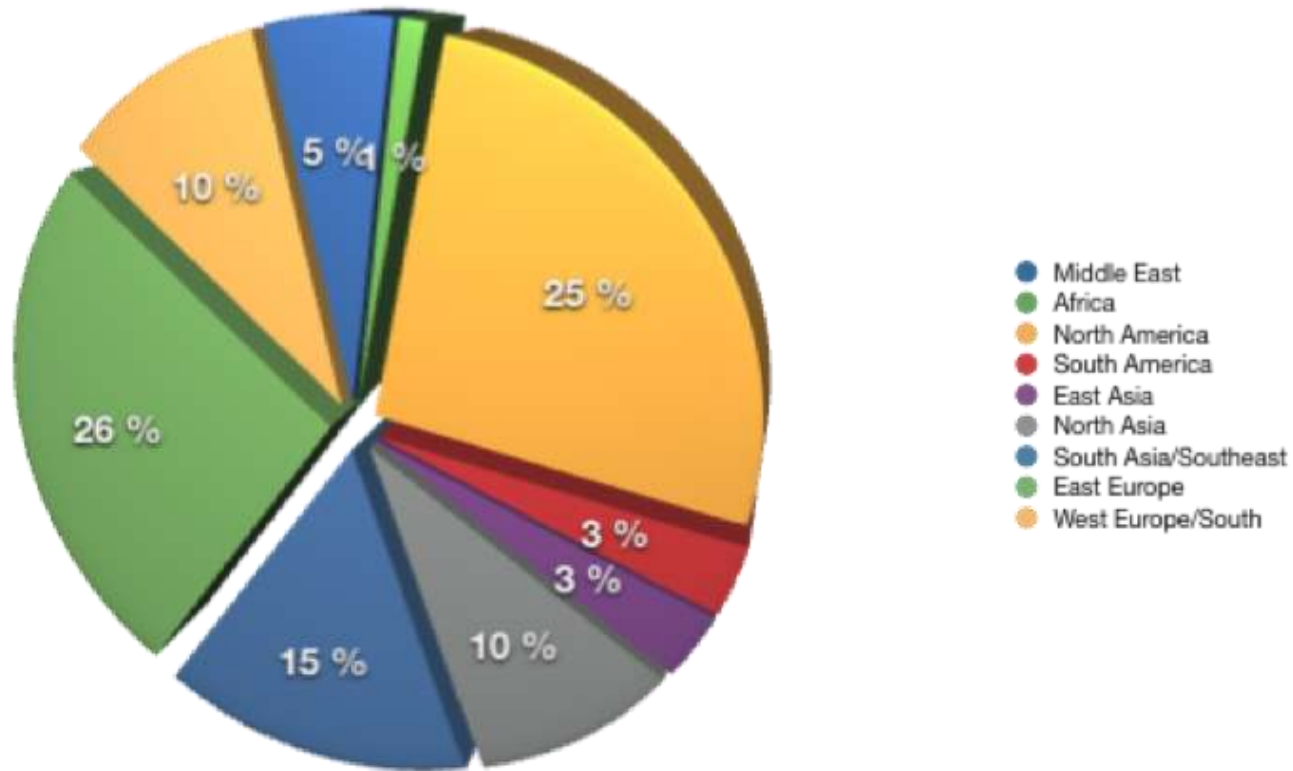
Agenda



Oracle Database Security

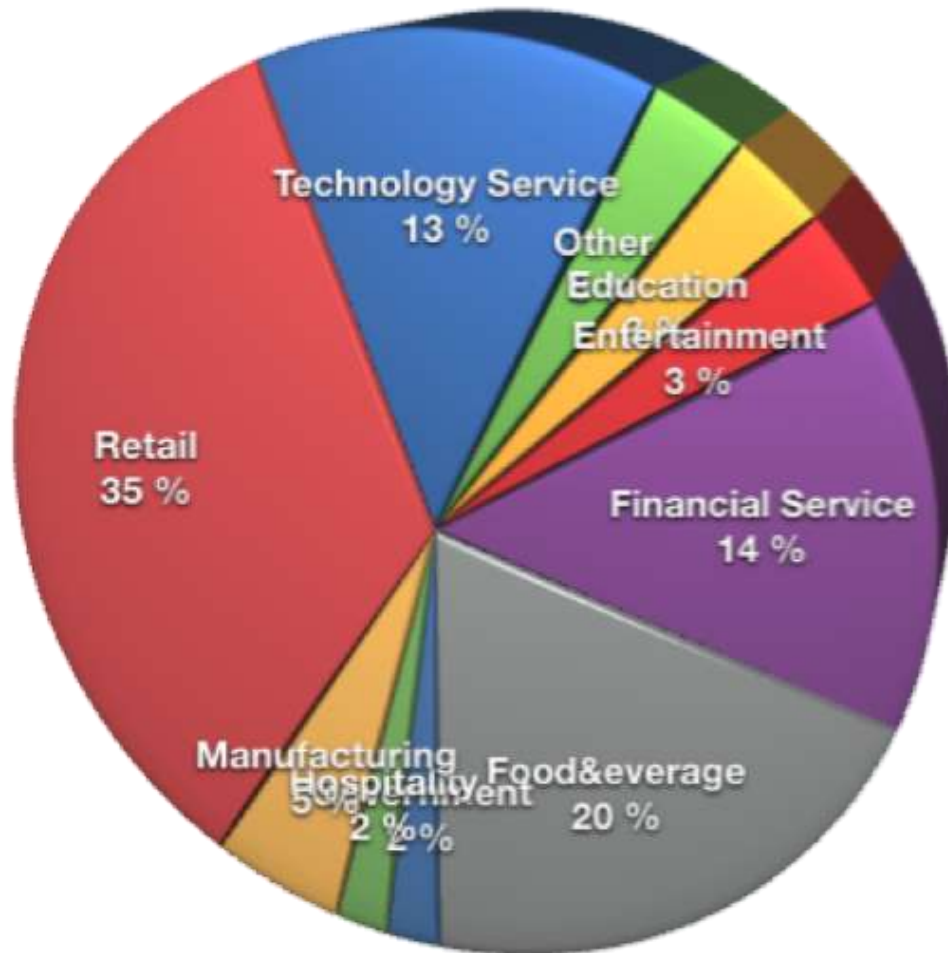
- Today's security challenges
- Who is dangerous for our business ?
- How do we get „attacked“ ?
- How can we protect ourselves ?

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

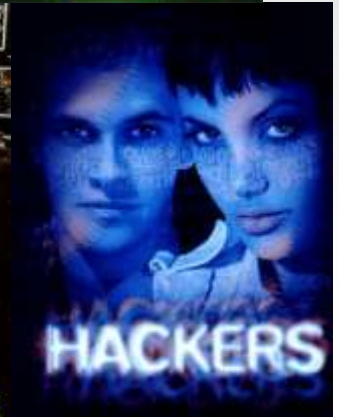
- Hobby Hackers
- Web Site Defacement
- Viruses
- Infrequent Attacks

2010

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

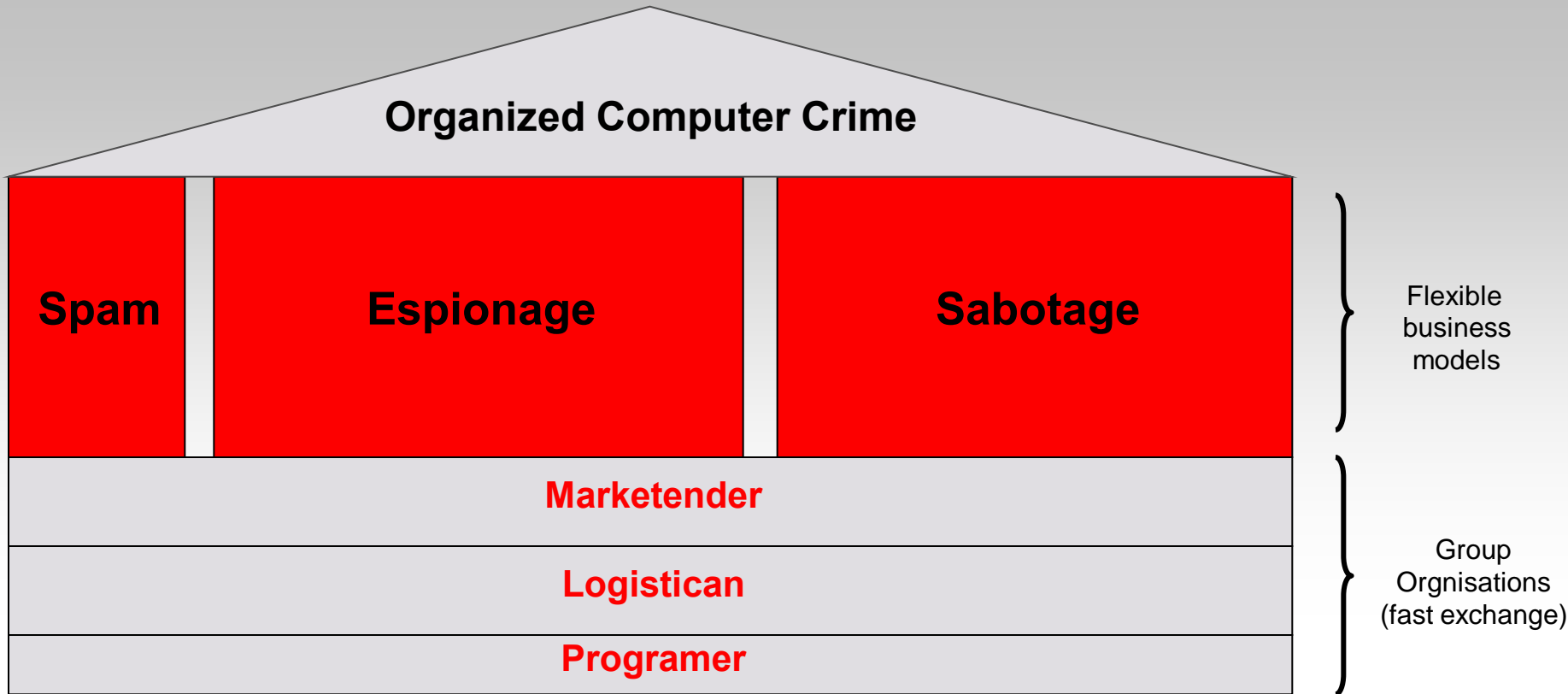


Mythos Hacker





Underground organisation





Hacking Steps

Preparation Phase

- Targeting
- Information collection
- Social engineering
- Social networking
- Underground scene consolidation

Planing Phase

- Detailed planning
- Risk analysis
- Staffing
- Alternative plans
- Methods
- Techniques
- Choose precautions

HACK

- 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 !!!**



Fahndrehung und Aufklärung (Tabelle 61)
Binnen-, Bundespolizei insgesamt

Merkmal	Tatbestandsgruppe	Gesamtfälle		ermittelt		erfolgreich	
		2011	2012	Anzahl	in %	Anzahl	in %
0010	Computerkriminalität - alle Fälle	19.000	22.100	4.637	24,4	4.111	18,6
0011	Diebstahl von Daten einschließlich unbefugter Datenkopie	17.747	21.222	4.280	24,1	40,0	18,9
0012	Computerfälschung (IDK) (MKB)	18.200	13.970	108	0,6	48,0	34,5
0013	Diebstahl von Zugangsdaten/Computer- und Internetkennzeichen	5.822	7.788	16	0,3	11,0	1,4
0014	Fälschung Internetprotokolle (IP), Diebstahl von Kennzeichen bei Datenübertragung (z. B. WWW, FTP, etc.)	2.488	1.802	148	5,9	44,0	24,4
0015	Datenveränderung, Computerfälschung (z. B. VBA, MSN, etc.)	1.672	1.888	30	1,8	20,0	10,6
0016	Angriff von Daten	2.286	2.298	104	4,5	11,0	4,8
0017	Softwarepatente (patentverstoß) z. B. Computerpatent	1.928	2.467	147	7,6	16,0	6,5
0018	Softwarepatente in Form geschützter Werke	121	402	30	24,8	16,0	39,8

Gewalttaten und Abgrenzungen (Tabelle 62)
Binnen-, Bundespolizei insgesamt

Merkmal	Tatbestandsgruppe	Anzahl	Täteralter					
			14-17	18-20	21-25	26-30	31-35	
0010	Computerkriminalität - alle Fälle	19.000	16,1	11,9	1,1	0,8	12,1	16,9
0011	Diebstahl von Daten einschließlich unbefugter Datenkopie	17.747	17,8	13,8	1,8	1,8	12,9	18,0
0012	Computerfälschung (IDK) (MKB)	18.200	18,2	13,8	1,3	0,8	11,9	18,9
0013	Diebstahl von Zugangsdaten/Computer- und Internetkennzeichen	5.822	18,1	14,1	0,8	0,9	12,1	18,0
0014	Fälschung Internetprotokolle (IP), Diebstahl von Kennzeichen bei Datenübertragung (z. B. WWW, FTP, etc.)	2.488	18,2	13,1	0,9	0,7	10,7	18,8
0015	Datenveränderung, Computerfälschung (z. B. VBA, MSN, etc.)	1.672	22,9	18,4	0,1	0,2	1,1	22,9
0016	Angriff von Daten	2.286	14,1	18,1	0,4	0,8	8,7	14,1
0017	Softwarepatente (patentverstoß) z. B. Computerpatent	1.928	14,1	12,9	0,8	0,9	7,7	14,9
0018	Softwarepatente in Form geschützter Werke	121	11,9	18,1	0,9	0,4	7,4	16,0

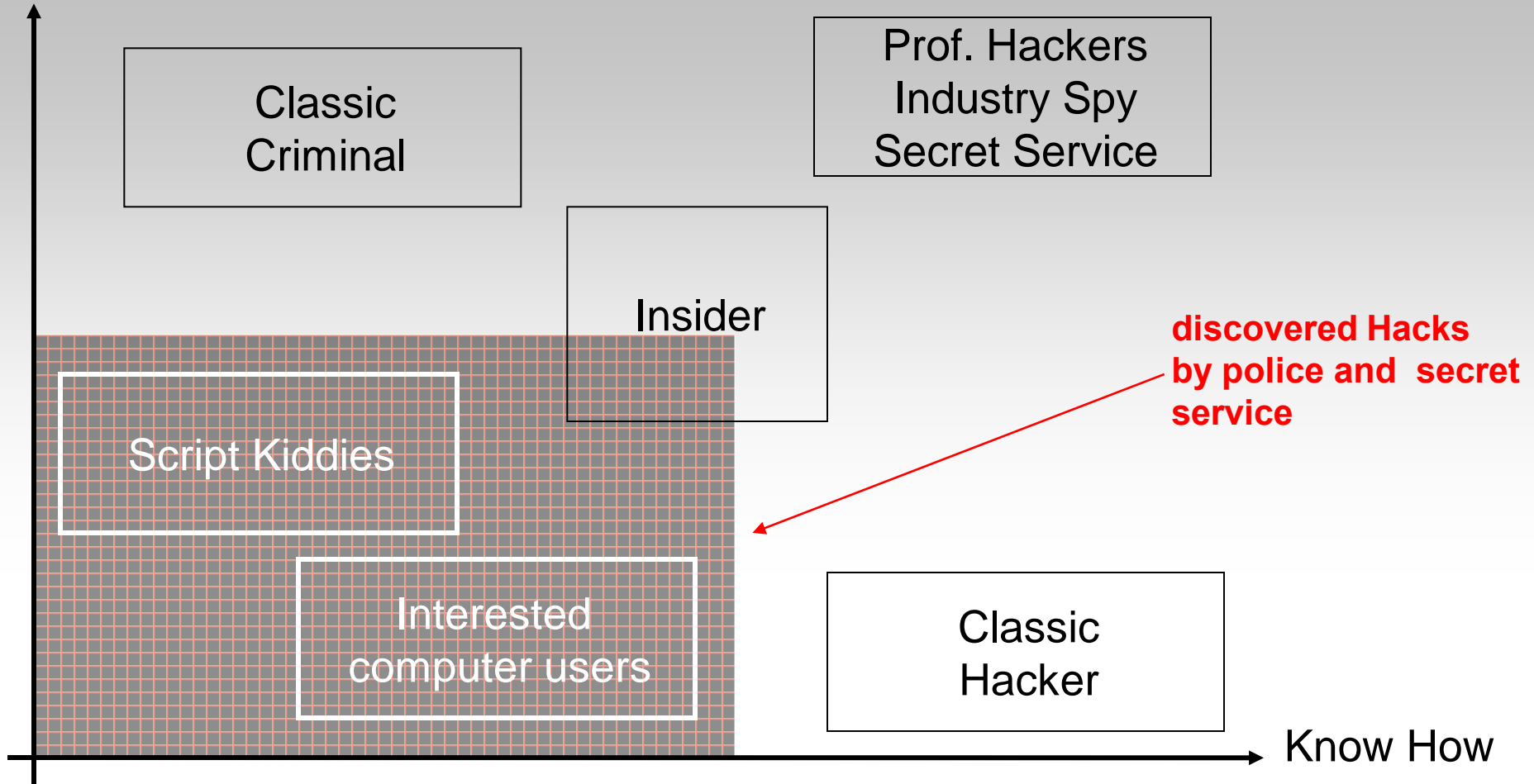
Bei den Computerkriminalität, Diebstahl von Daten einschließlich unbefugter Datenkopie ab 21 Jahren.

Source: BND Sicherheitsreport 2008

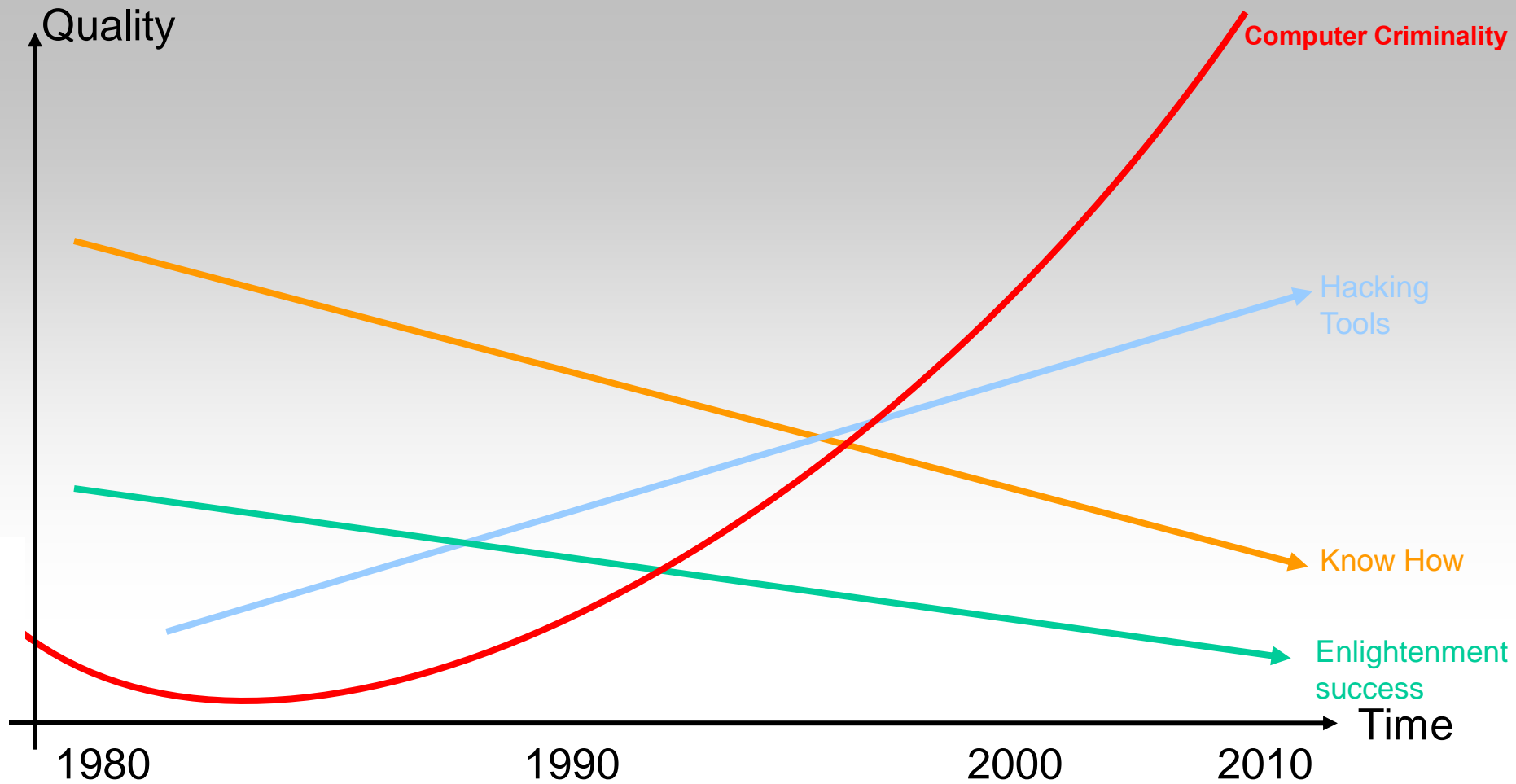
Profiling Hack3rs



Criminal
Energie



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

- 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
- ...

Source: [Black Hat / Defcon](#) (unofficial)

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
- Tousands 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

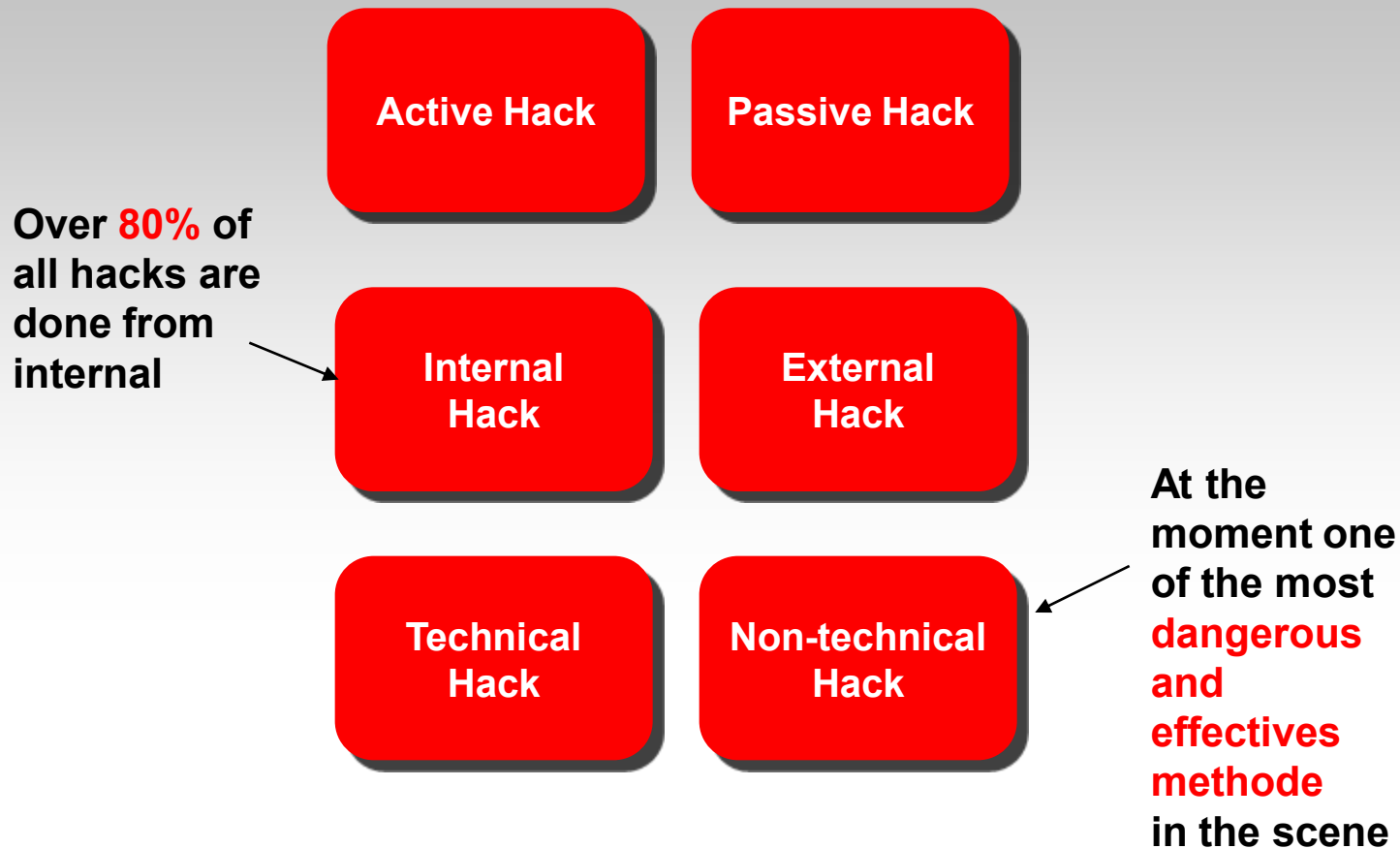
Agenda



Oracle Database Security

- Today's security challenges
- Who is dangerous for our business ?
- How do we get „attacked“ ?
- How can we protect ourselves ?

How we get attacked



How we get attacked -- REALITY

- 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



Oracle Database Security

- Today's security challenges
- Who is dangerous for our business ?
- How do we get „attacked“ ?
- How can we protect ourselves ?

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

- External Attackers
- Internal Threats
- Image Damage
- Internal Security Regulations
- Regulatory Compliances
- ..
- .



Oracle Solution

- **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 Security Product

- 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®