

# Hunt for the digital crown jewels ... using a door handle



## Introduction to computer security

# Agenda

- Hacking and information security revisited
- Case
- Lessons learned
- Questions and Answers

# Hacking and information security revisited

# Hacking and information security revisited

“Hacking” is often associated with:

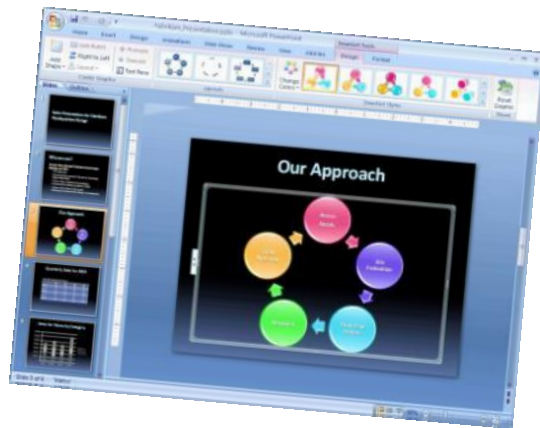
- Internet
- Threats from outside an organization
- Breaking technical systems / controls



# Hacking and information security revisited

But information is often accessible via different access paths:

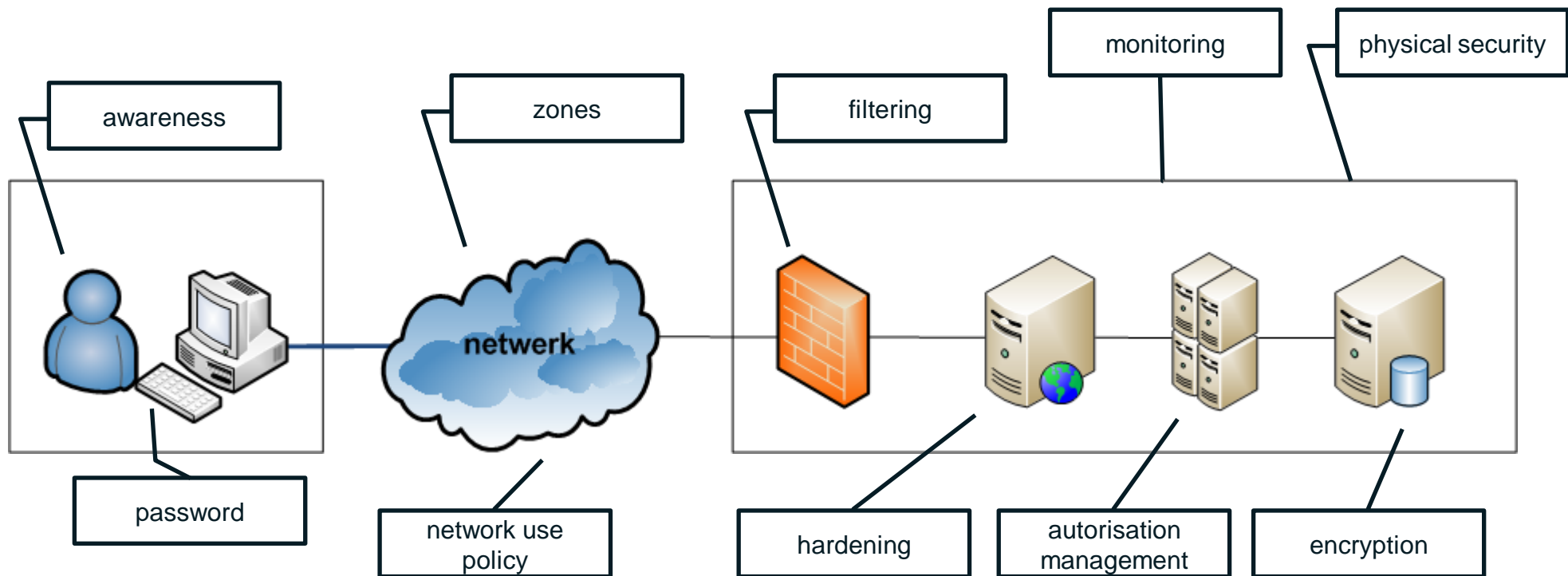
- Internet
- Extranet
- Local network
- On paper
- Social media



# Hacking and information security revisited

How to secure information:

- Defense in depth – layers of security
- Measures on both people, process and technology level
- Combination of preventive and detective measures



# Hacking and information security revisited

Hacking (or securing information) from a purely technical point of view and a single access path is probably insufficient

- Weaknesses in non-technical measures can lead to circumvention of technical measures
- Non-trivial access paths may provide interesting opportunities
- Isolated issues in not-so-important security controls may not always lead to problems – combine them and they probably will

# Case

# Hacking case

## Hunt for the digital crown jewels ... using a door handle

- Use of multiple “hacking” methods
- Combine issues in various levels of security (people, process, technology)

# Hacking case

The situation:

- Organization with around 200 employees
- Office and IT environment in 1 large building
- Part of the building is accessible for customers
  
- Newly appointed IT Director
- Inheritance of an IT infrastructure with a variety of systems
  
- Concerns regarding the security of the organization's "digital crown jewels" (sensitive information)
- Information is stored in several applications



or



# Hacking case

## Objectives:

- Determine level of security for digital crown jewels
- Simulate an “external” attack

## Client requirements:

- Limited number of days
- No prior information provided on IT infrastructure or office building
- Test will not be announced (only IT Director and 1 other person knew)
- Testers were provided with a visitor’s badge



# Hacking case

Our overall approach:

## *External*

- Penetration tests on internet-connected systems (IP and telephony)

## *Internal*

- Obtain access to office
  - Social engineering / observation
  - Limited physical penetration testing
- Penetration tests on the internal network
  
- “Get our of jail, free” letter in my pocket



# Hacking case

## External penetration testing approach

- From “stealth” to “intrusive” – would the client have security monitoring in place?
- Information gathering internet-facing systems
  - Public sources such as RIPE
- Reconnaissance internet environment
  - Port scanning / war dialing
- Identification of vulnerable systems
  - Vulnerability testing
- Exploitation
  - Manual verification of vulnerabilities found
  - Find a path to the internal network!



# Hacking case

## External penetration testing results

### Technical results

- Limited set of internet-facing systems
- 1 modem with standard user / password
- A number of websites with out-dated, vulnerable software
- No path to the internal network ☹ ☹

### Non-technical results

- Post of IT admins on various internet forums
- No indication security monitoring in place

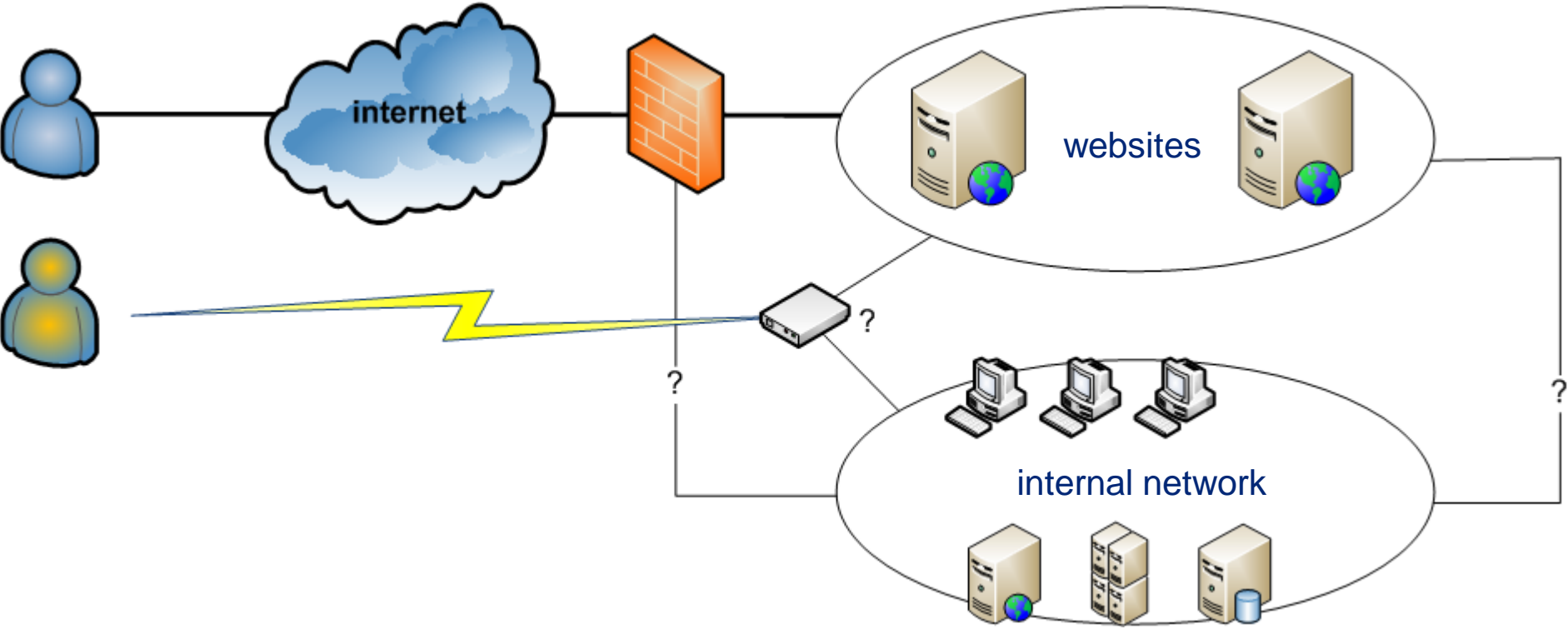
Conclusion: digital crown jewels are protected from an external attack?



# Hacking case

## External penetration testing results

Schematic overview of organizations internet environment



# Hacking case

## Internal penetration testing approach

### •Attack plan:

- Use visitor's badge
- Find a place to "work"
- Perform internal penetration test
- Gain access to the digital crown jewels

•Do not use "get out of jail, free" letter 😊

### •Tools:

- 1 visitor's badge
- 1 test laptop
- 1 friendly smile and charming personality



# Hacking case

## Internal penetration testing – day 1

- Visitor's badge opens access gate on ground floor
- Elevator with access badge system:
  - Access to floor 1 and 2 with visitor's badge
  - Floors 3-5 restricted
  - Elevator extremely crowded around 8.30am
- Stairs – badge reader per floor (identical to elevator access restrictions)
- Floor 1 and 2
  - Large chambers with >4 persons: crowded
  - Work without raising suspicion: not a chance
- The coffee machine
  - Serious shortage of office space (employee)
  - Announcement of network upgrade (internal newsletter)
  - Susan turned 40 and invited everyone for cake (notice board)



# Hacking case

## Internal penetration testing – day 2

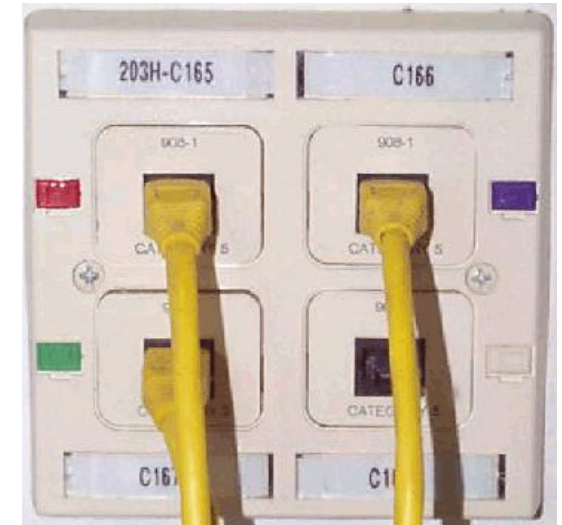
- Gain access to the 3<sup>rd</sup>, 4<sup>th</sup> or 5<sup>th</sup> floor:
  - Step into a crowded elevator
  - Get out at ... floor 4
- Find myself a place to work with a network connection
  - Office doors closed, door handles missing (?)
  - Some office open, but crowded ☹
- The coffee machine
  - “Steal-an-office-prevention” by removing door handles (employee)
  - “By the way: what are you doing here?” ☹
  - The story: gathering network statistics to prepare for upcoming network upgrade (making the network super fast)
  - “You are my hero!”
    - “Finally!”
    - “You are very very welcome”
    - “Network is extremely slow”
  - I was escorted to the secretary in charge of the door handles



# Hacking case

## Internal penetration testing – day 2

- Got myself an office on the 4<sup>th</sup> floor:
  - A desk with a PC 😊
  - Multiple network connections
- First steps (non-intrusive)
  - Password reset on PC – admin access to local PC (required opening up the PC)
  - Use MAC address spoofing to connect my test laptop to the internal network (not sure if MAC address filtering was in place)
  - Network sniffing on the internal network (sniff authentication traffic, plaintext communication)
- Offsite analysis of information gathered
  - Shortlist of interesting systems (based on sniffing results)
  - Password cracking of sniffed password hashes
  - Plan next steps, focus on interesting systems
  - Limit the number of onsite visits required



No.	Time	Source	Destination	Protc
1	0.000000	192.168.0.2	Broadcast	ARP
2	0.299139	192.168.0.1	192.168.0.2	NBNS
3	0.299214	192.168.0.2	192.168.0.1	ICMP
4	1.025659	192.168.0.2	224.0.0.22	IGMP
5	1.044366	192.168.0.2	192.168.0.1	DNS
6	1.048652	192.168.0.2	239.255.255.250	UDP
7	1.050784	192.168.0.2	192.168.0.1	DNS
8	1.055053	192.168.0.1	192.168.0.2	UDP
9	1.082038	192.168.0.2	192.168.0.255	NBNS
10	1.111945	192.168.0.2	192.168.0.1	DNS
11	1.226156	192.168.0.2	192.168.0.1	ICMP
12	1.227282	192.168.0.1	192.168.0.2	TCP

Frame 11 (62 bytes on wire, 62 bytes captured)  
Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear\_  
Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.

# Hacking case

## Internal penetration testing – day 3

- Next steps (non-intrusive)

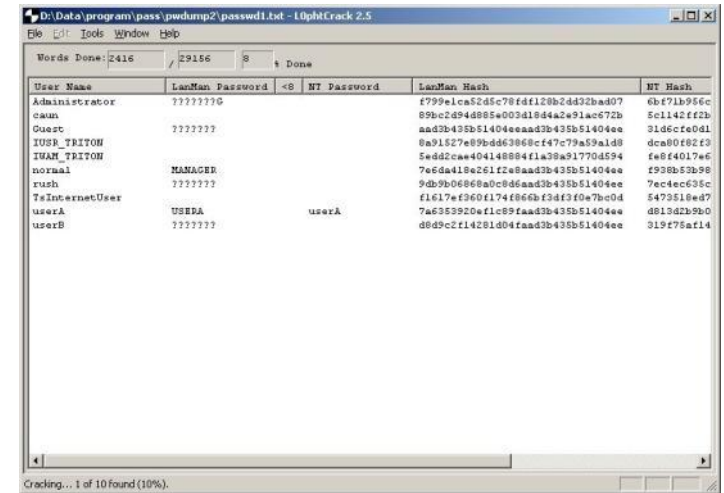
- Use cracked passwords to explore network and applications
- Obtained access to e-mail of users using the PC in the room

- Results

- Access to subset of the digital crown jewels in applications (via cracked passwords)
- Access to subset of digital crown jewels via e-mail messages and network shares (export by users and copied to share)

- And of course

- Enthusiastic response from employees to my “network sta gathering” activities 😊
- Access to 4<sup>th</sup> floor via elevator (easy, if timing is right)



The screenshot shows the L0phtCrack 2.5 interface with a list of cracked passwords. The status bar at the bottom indicates 'Cracking... 1 of 10 found (10%)'.

User Name	LANMan Password	<S	NT Password	LANMan Hash	NT Hash
Administrator	????????			f799e1ca52d5c78fd120b2dd32bad07	6bf71b956c
Guest	????????			89bc2894d895e003d18d4a2e91ac672b	5c1142ff2b
IUSP_TRTON				aa32b435b51404eaa335435b51404ee	310cfe0d1
IHAM_TRTON				8a31527e899d463866cf47c79a59a1d8	dca8048e23
normal	MANAGER			5ed2cae404148884f1a38a91770d594	fe8f40174c
rush	????????			7e6da418e261f2a8aad3b435b51404ee	f938b53b99
TaInternetUser				9db9b06868a0c8d6aad3b435b51404ee	7ec4ec635c
userA	USERA		userA	f1e17ef3660f174f866bf3d43f0e7bc0d	5473518ed7
userB	????????			7a635920e1c89faad3b435b51404ee	d813d2b9b0
				d8d9c2f14281d04faad3b435b51404ee	319c78a1f4



# Hacking case

## Internal penetration testing – day 4

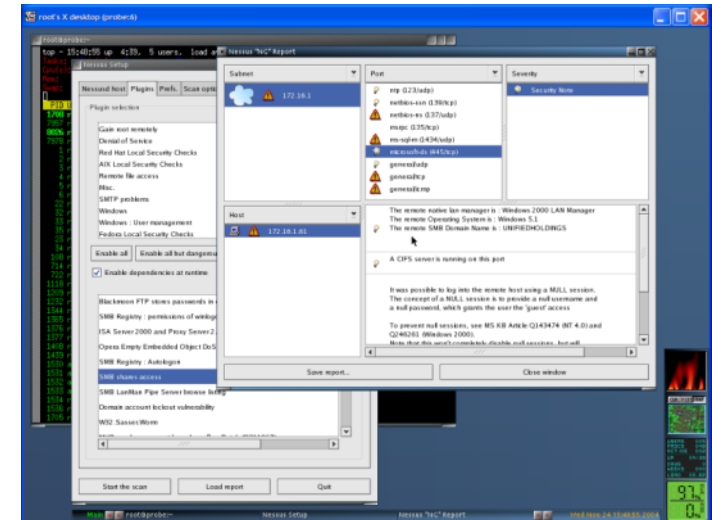
### •Next steps (intrusive)

- Port scanning of “interesting” systems → identification of database server
- Vulnerability scan on subset of these systems
  - Cracked password of the Windows account of user X turned out to belong to the database admin (remember the internet forum posts?)
  - The password had been used on various systems

### •Results

- Security of systems was fairly well hardened, but ...
- Cracked password of user X worked on various systems ...
- Including the database with the full set of crown jewels!

### •Mission accomplished!



# Hacking case

## Internal penetration testing

### *Summary of results*

- Various technical security measures in place:
  - PC with physical and logical security measures
  - Hardened application server configurations
  - Password policy
  - MAC filtering on network
- Weaknesses in various non-technical layers of security provided opportunities to circumvent technical measures
- Lack of detective measures
- Result: full access to the complete set of digital crown jewels



# Lessons learned

# Hacking case

## Internal penetration testing

### *Weakness*

- Technical
  - Limited measures to prevent sniffing: MAC address filtering in place, no switched network
  - Use of outdated / plaintext protocols
- Procedural / human factor:
  - Card reader process not optimal 😊
  - Access procedure for office room not waterproof
  - PC was left in unused room
  - No security monitoring
  - Export of subsets of digital crown jewels to other locations
  - Using the same password for management of various systems
  - Lack of user awareness (I was hardly challenged being a complete stranger in the building)
  - Admin published detailed information about IT management on internet

GOOD  
NEWS,  
BAD  
NEWS

# Hacking case

## Hunt for the digital crown jewels ... with a door handle

• Using a hacking approach aimed at people, process and technology resulted in:

- Unintended access paths to digital crown jewels
  - Insight in the layers of measures protecting the digital crown jewels – and weaknesses in them
  - Very concrete actions to take (combinations of) measures to enhance the overall level of security
- Interesting materials for internal security awareness trainings ...



# Questions and answers

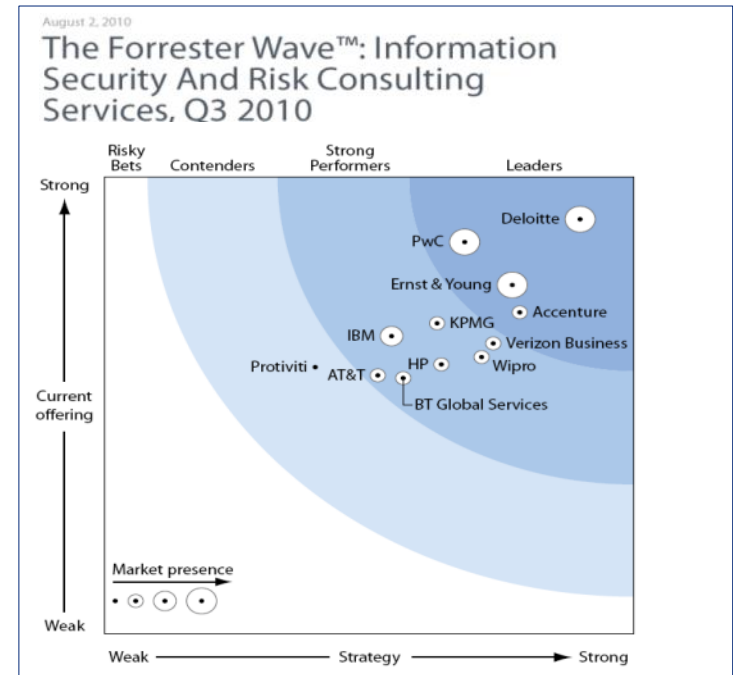
# Last, but not least ...

- Deloitte is looking for new Security & Privacy consultants
- We are offering internships for students interested in Information Security
  - Penetration testing
  - Cloud computing security
  - Data leakage prevention
  - Security management
  - ...

Service Area	Sample Projects	
	Audit/Review/Test	Advise/Implement
Security Management & Transformation	<ul style="list-style-type: none"> <li>• ISO27001 review</li> <li>• Review of policies &amp; procedures</li> <li>• Security Audits</li> </ul>	<ul style="list-style-type: none"> <li>• ISMS/ISO27001 implementation</li> <li>• Business Continuity Management</li> <li>• Security Awareness Program</li> <li>• GRC Solutions</li> <li>• Identity &amp; Access Management</li> </ul>
Security Operations & Infrastructure	<ul style="list-style-type: none"> <li>• Penetration testing</li> <li>• Source code review</li> <li>• O/S, DB, Network audits</li> </ul>	<ul style="list-style-type: none"> <li>• Security baseline definition</li> <li>• ITGC Data Analytics</li> <li>• Secure software development</li> </ul>
Data Protection	<ul style="list-style-type: none"> <li>• Privacy Audits</li> <li>• PCI Compliance Audits</li> <li>• Cloud computing Audits</li> </ul>	<ul style="list-style-type: none"> <li>• Information leakage solutions</li> <li>• PCI implementation</li> <li>• Cloud computing implementation</li> </ul>
SAP / Oracle Security	<ul style="list-style-type: none"> <li>• SAP / Oracle Audit (SoD / GITC)</li> <li>• SAP / Oracle Project Quality Assurance</li> </ul>	<ul style="list-style-type: none"> <li>• SAP / Oracle Security &amp; Controls implementation</li> <li>• SAP / Oracle Data Analytics</li> </ul>

# Contact details

- Contact me if you have any further questions / ideas
- <http://werkenbijdeloitte.nl/vacature/86232/Consultant-Security-and-Privacy.html>



*“In Forrester’s 75-criteria evaluation of information security and risk consulting service providers, we found that Deloitte led the pack because of its maniacal customer focus and deep technical expertise.”*

## Deloitte.

Laan van Kronenburg 2  
1183 AS Amstelveen  
The Netherlands

**Tom Schuurmans CISSP CEH**

Security & Privacy Services

Mobile: + 31 65 585 3822  
tschuurmans@deloitte.nl

Member of  
**Deloitte Touche Tohmatsu**

Regions	Deloitte professionals
North America	> 4,500
EMEA	> 1,600
Asia Pacific	> 2,500
Rest of the World	> 1,300
The Netherlands	>75

Approximately 10,000 IT risk management and Security & Privacy professionals globally. Many of them are certified CISA, CISSP and/or RE (NL only).



**Disclaimer:**

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms.