



Compass Security

Company Profile

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch
www.csnc.ch

Agenda



Who is Compass Security AG?

Service Portfolio

Know-how Management

Why Compass Security?



Who is Compass Security?

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch
www.csnc.ch

The Team



Facts and Figures



Foundation	1999
Executive Directors	Walter Sprenger & Ivan Bütler
Turnover per Year	~ CHF 2.5 Mio
Location	Rapperswil-Jona SG 
Size	24 employees
Focus	Security Review - Penetration Testing - Forensics



Service Portfolio

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch
www.csnc.ch

Service Portfolio



Security Assessments



Security Assessments

- ✦ Penetration Tests
- ✦ Ethical Hacking
- ✦ Reviews

Characteristics

- ✦ Attacks from outside
- ✦ Attacks from inside
- ✦ Attacks by anonymous users
- ✦ Attacks by registered users
- ✦ Attacks with insider knowledge
- ✦ Attacks without insider knowledge



Forensic Analysis



Forensic Analysis

- ✦ Phishing Victims
- ✦ Website Defacements
- ✦ Compromised Server
- ✦ Forgery of Documents
- ✦ Insider Knowledge

Goals

- ✦ WHAT happened
- ✦ HOW did it happen
- ✦ WHO was the initiator/victim
- ✦ WHY
- ✦ HOW can you protect yourself



Security Trainings



Course Modules

- ✦ Internet Security - Firewall
- ✦ Web Application Security
- ✦ Content Security
- ✦ Forensics

Characteristics

- ✦ Public Courses (ISACA)
- ✦ E-Learning & E-Lab
- ✦ Company Courses (in-house)
- ✦ Compass Events
- ✦ Hack & Learn
- ✦ Universities of Applied Science
- ✦ Live Hacking Demos
- ✦ Awareness Programs



Security Analysis

- ✦ New Attack Techniques
- ✦ New Defence Methods
- ✦ Proof of Concept Tools

Publications & Tools

- ✦ 2008: WebApp Threat Matrix
- ✦ 2007: BHO (Browser Helper Objec
- ✦ 2007: SIP Proxy Attack
- ✦ 2007: USB U3 Virus Attacks
- ✦ 2006: SmartCard Insecurity

Goal

- ✦ Staying up to date
- ✦ Cutting edge hacking techniques



FileBox



- ✦ Secure web-based document exchange platform
- ✦ Strong authentication – SMS token
- ✦ Hosting Model
- ✦ Source Code Model





Know-how Management

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch
www.csnc.ch

Where does the knowledge come from?



Know-how planning

- ✦ Each employee gets at least 10 training days per year
- ✦ Project experience -> internal checklists
- ✦ Compass research -> advisories or TIGER-INFO
- ✦ Compass research -> publications
- ✦ 2 employees per year visit BlackHat/DefCon in Las Vegas

Characteristics

- ✦ Know-how goals are defined per employee
- ✦ Know-how development is a major component at Compass

Where does the knowledge come from?



Assistant Lecturer HSR

- ✦ Studies/Bachelor/Diploma Thesis at the department for Computer Science

Lectures at HSW (University of Applied Sciences, Lucerne)

- ✦ Courses in MAS INS (Master of Advanced Studies)

Guest Speaker at HTW Chur

- ✦ Internet Technologies and Applications

Applied Research

- ✦ Publications Heise, iX, hackin9
- ✦ Guest speeches at Security Events, Euroforum
- ✦ Compass Security Events (once a year)
- ✦ Hack&Learn (Swiss Wargames)



Compass Security – the right partner?

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch
www.csnc.ch

Yes, because...



Swiss Company – Near, Transparent, Trust

IT Security Specialists – Know-how

Ample Experience – Technology and Methods

Know-how Transfer – Reports – Downloads

Cutting Edge in terms of Hacking Methods - Tools

Customer-oriented – Individual



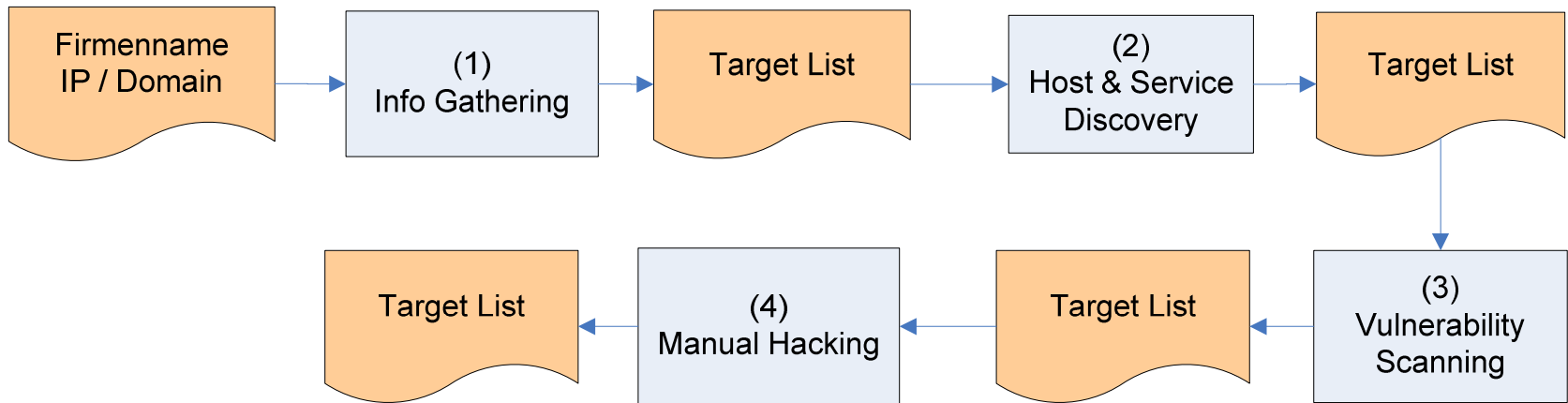
Appendix

Compass Report Attack Methodology

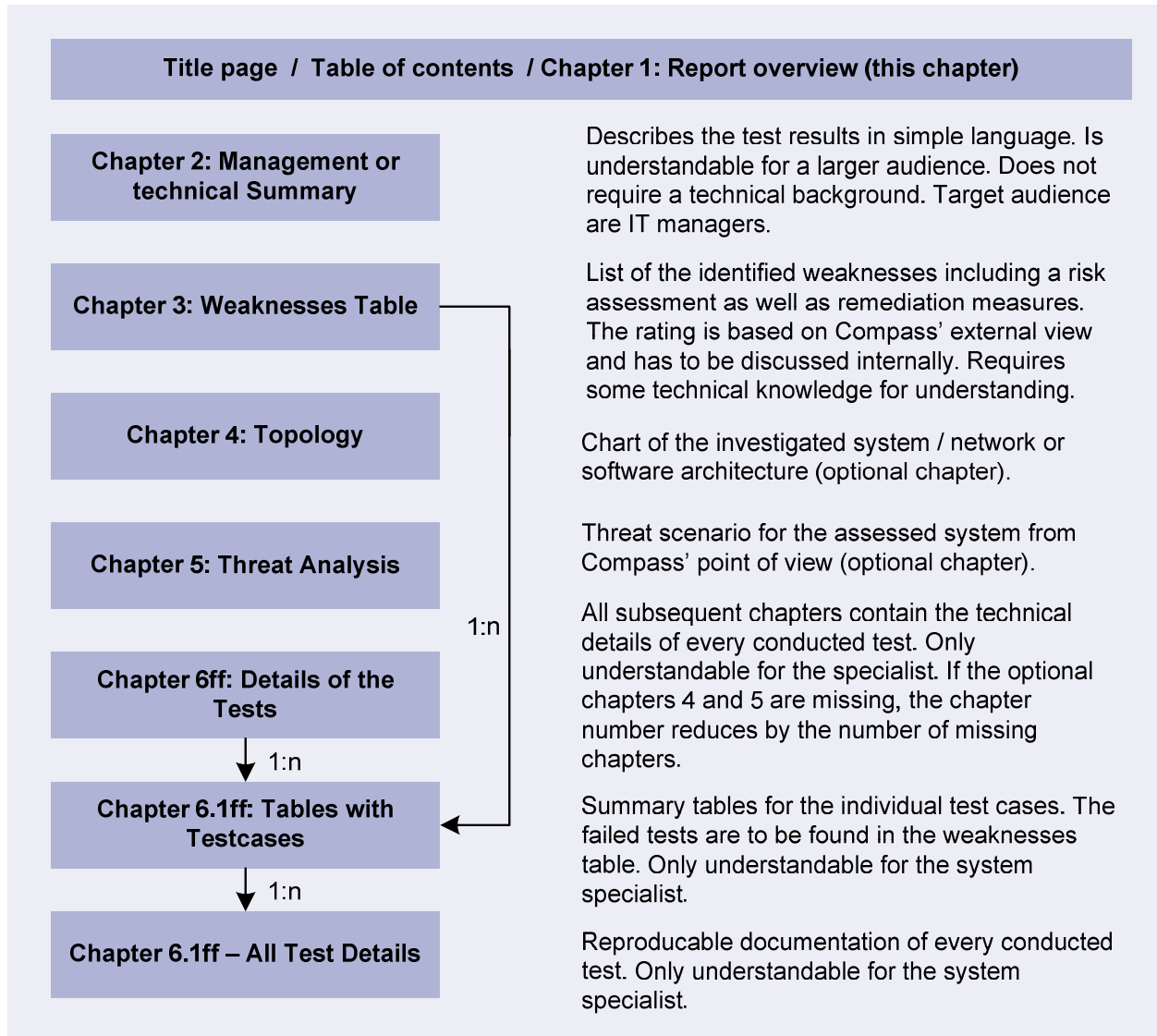
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel.+41 55-214 41 60
Fax+41 55-214 41 61
team@csnc.ch
www.csnc.ch

Penetration Test Process



Report – Structure



Report - Weaknesses Table



3 Vulnerabilities and Remediation

The tables in this chapter summarize the security issues found during the security review or penetration test. A definition for each column is given here:

No.	Reference	Weakness	Threat	Remediation	Rating	Comments
Each issue is consecutively numbered.	Reference to the corresponding test case in the following chapters	Explains the vulnerability or weakness found during testing.	Explains what could happen if the weakness is exploited	Recommendation on how to correct the vulnerability.	Compass rating of the weakness and the corresponding threat: ●* : Low ●*●* : Medium ●*●*●* : High	Normally left blank. The customer's comment regarding this issue.

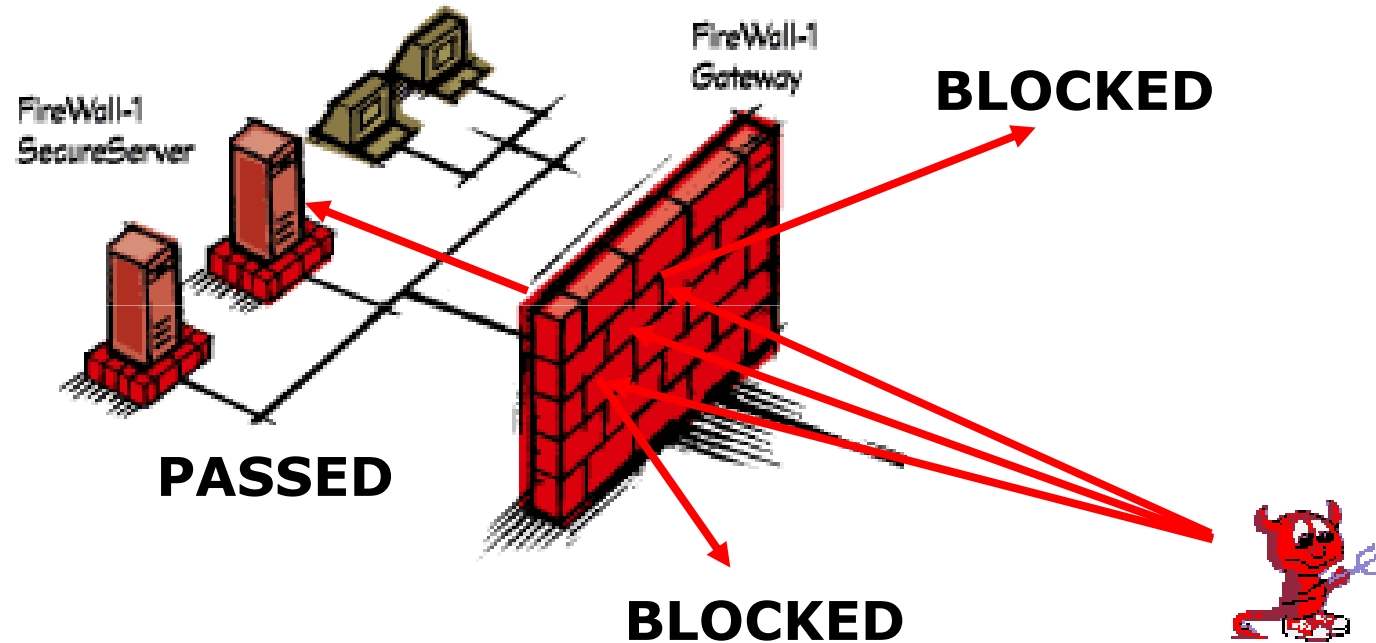
3.1 Online Banking

No.	Reference	Weakness	Threat	Remediation	Rating	Comments
1.	6.10.3 #3	Login servlet is vulnerable to the response-splitting attack.	Attacker is able to inject self-defined http headers within a victim's request. Session hijacking attack.	Input filtering. Escape CR, LF, (%0A, %0D) before processing the request.	●*●*●*	
2.	7.10.4 #4	SQL injection vulnerability (search servlet).	Dump search index table	Input filtering.	●*●*●*	
3.	8.1.1 #2	Apache TRACE	There are known attacks based on the http TRACE command.	Disable TRACE by mod_rewrite regexp expressions.		

Direct Attacks



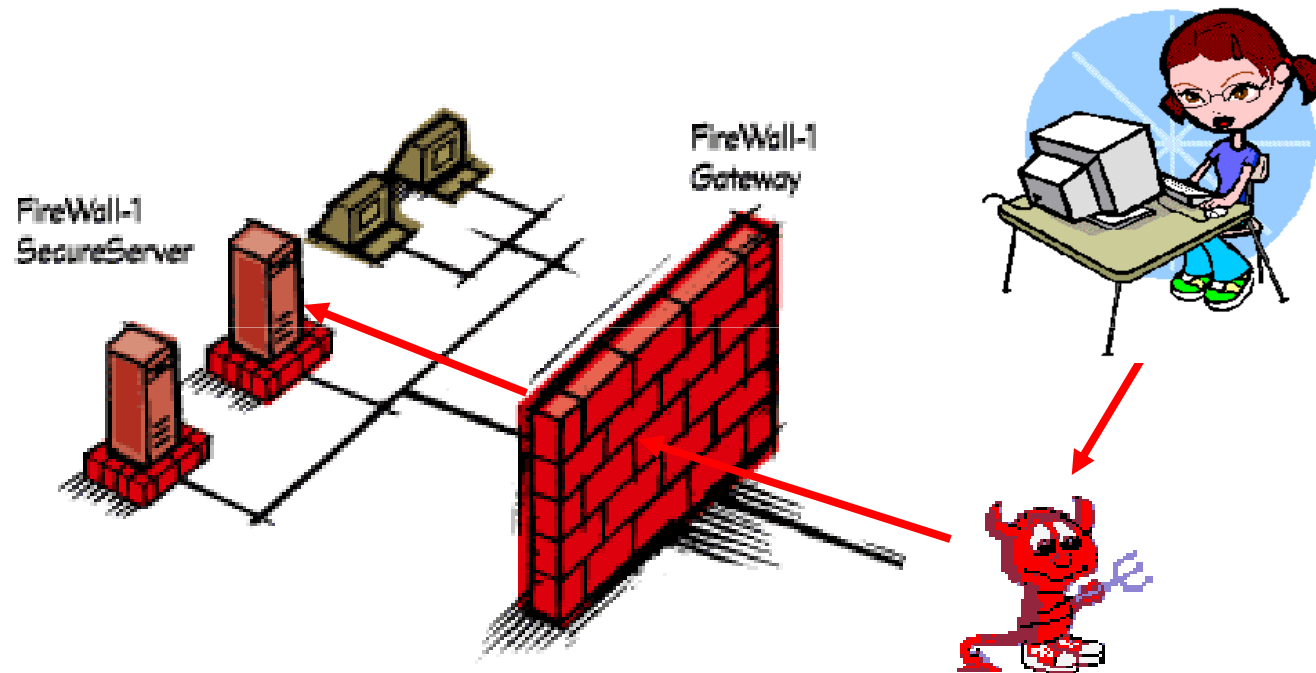
Where do you expect the attacker?



Indirect Attacks (I)



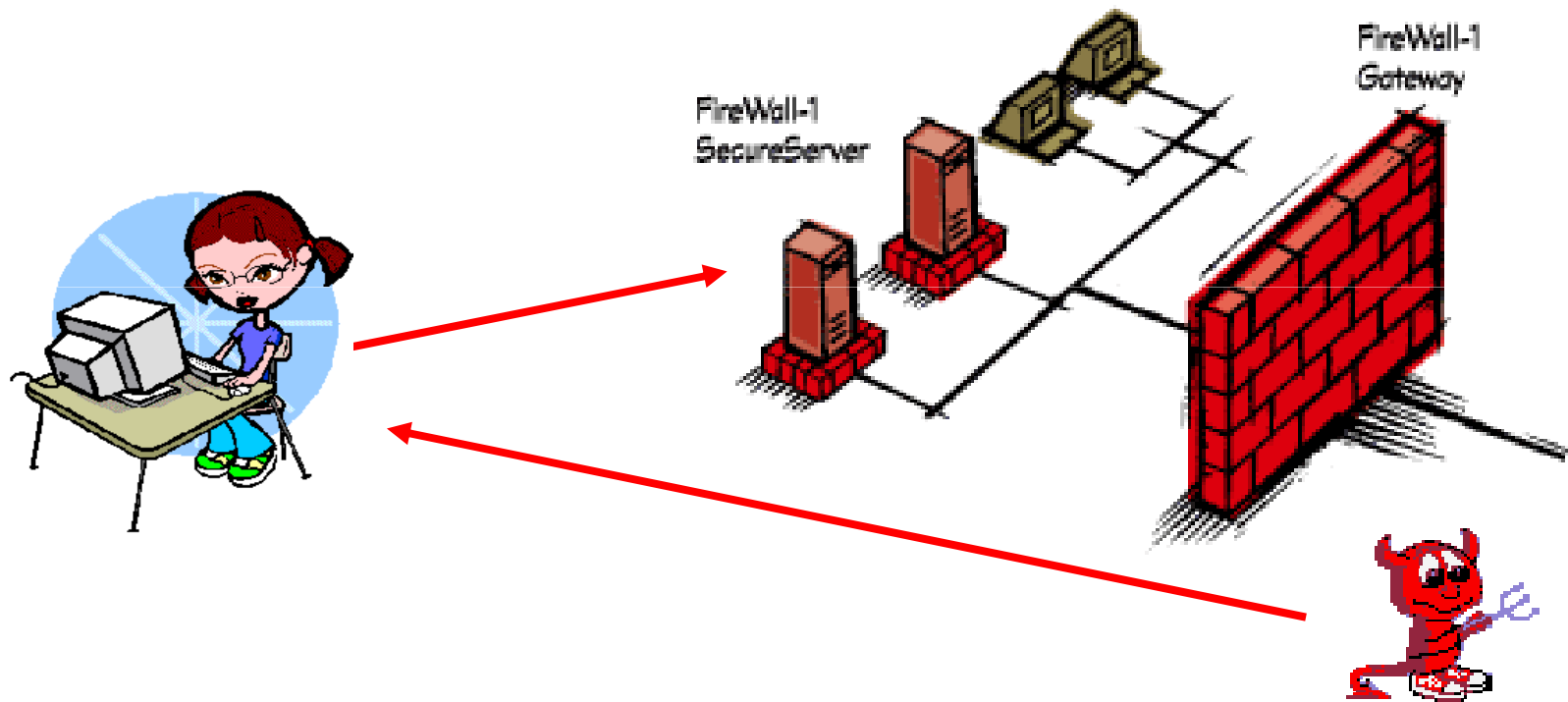
Man in the Middle – Phishing



Indirect Attacks (II)



Virus – Trojan Horse – Reverse Shell

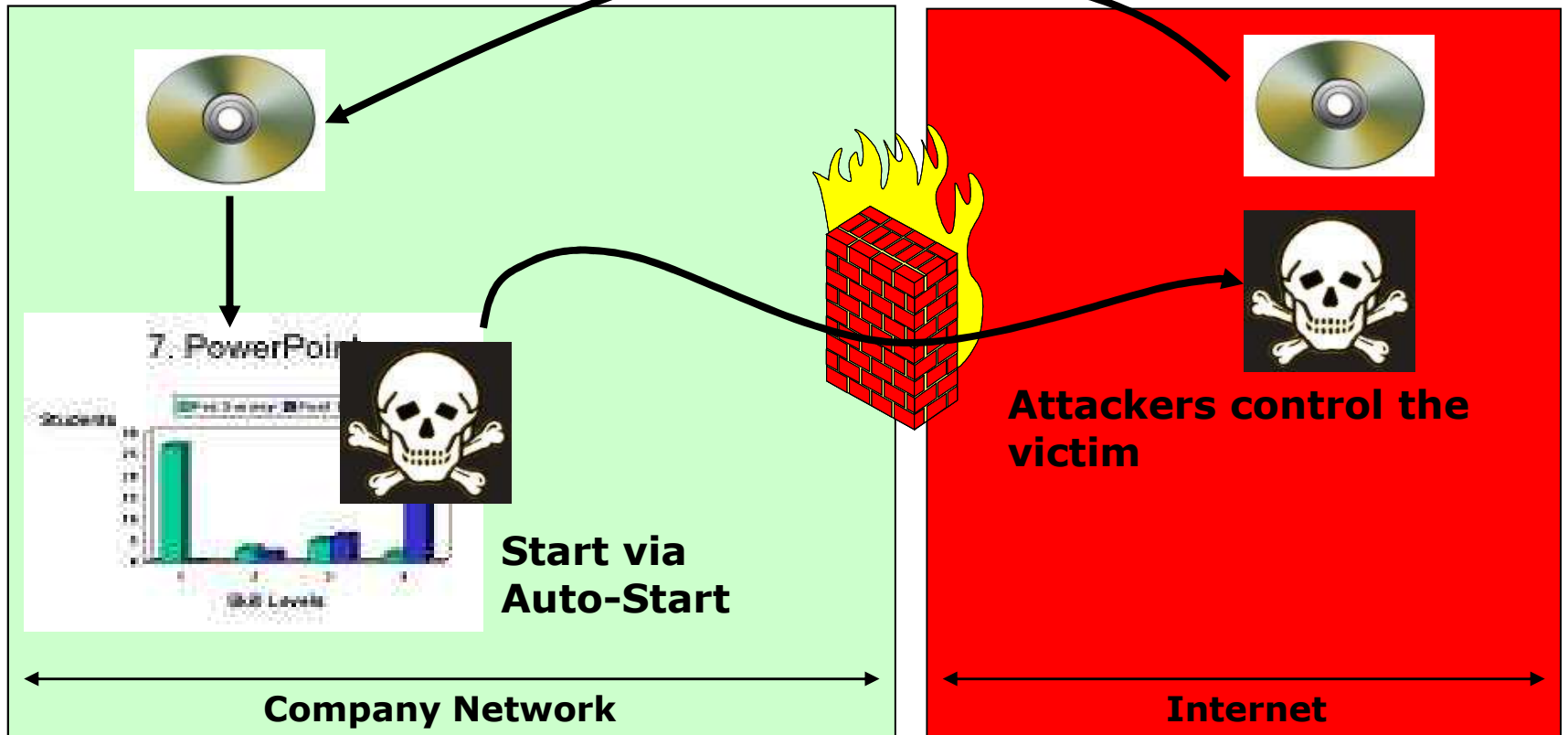


Indirect Attacks (III)



Covert Channel

Delivery through CDROM



Contact



Compass Security Network Computing AG

Werkstrasse 20

P.O. Box 2037

CH - 8645 Jona SG

Tel. +41 55 214 41 60

Fax +41 55 214 41 61

team@csnc.ch

www.csnc.ch

