

# Penetration Test

Ivan Buetler  
Compass Security AG



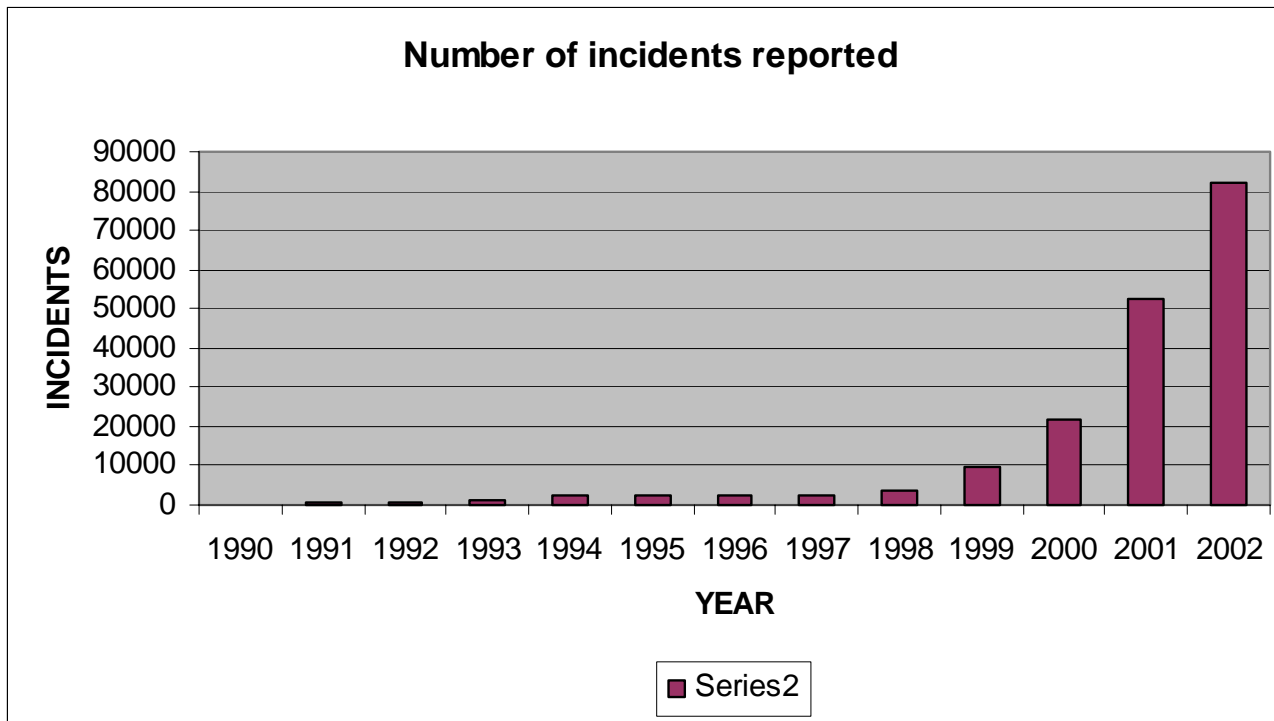
# Agenda

- Intro
- Was ist ein Security Assessment?
- Was ist ein Penetration Test?
- Was ist ein Security Review?
- Sonstige Rahmenbedingungen
- Marketing
- Planung und Durchführung
- Rechtliche Aspekte
- Schluss

# Lernziele

- Sie kennen die Schlagworte rund um das Thema „Security Assessment“ und können diese einordnen
- Sie verstehen den „Penetration Test“ als eine Methode des Security Assessments
- Sie kennen die wesentlichen Merkmale eines Penetration Test und dessen Ausprägungen
- Sie kennen rechtliche Abhängigkeiten in Bezug auf einen Penetration Test
- Sie erhalten Evaluationskriterien für Penetration Tests

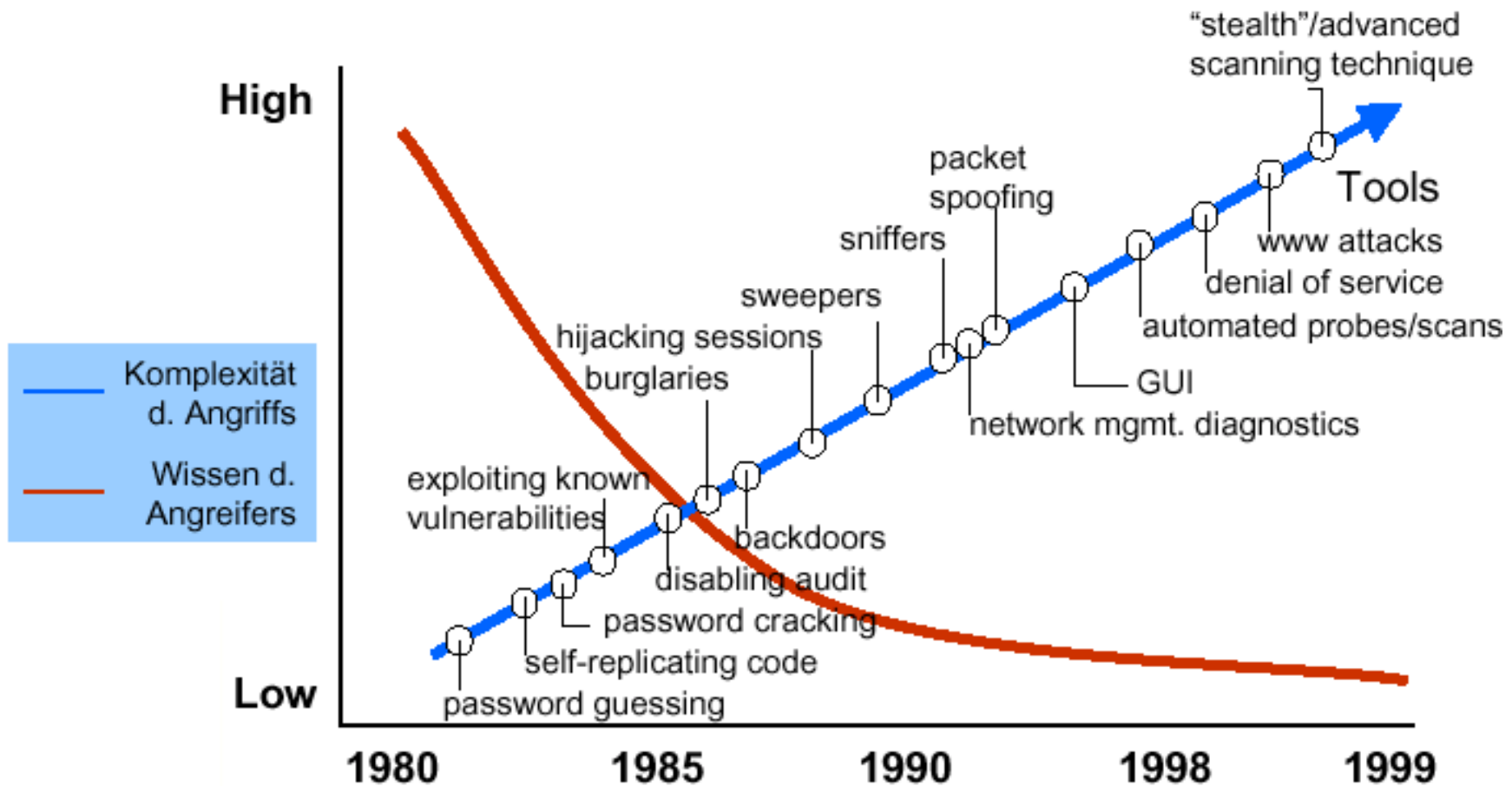
# Entwicklung Hackerangriffe



1990	252
1991	406
1992	773
1993	1334
1994	2340
1995	2412
1996	2573
1997	2134
1998	3734
1999	9859
2000	21756
2001	52658
2002	82094

Quelle: <http://www.cert.org/stats/#incidents>

# Entwicklung Hacker Fähigkeiten

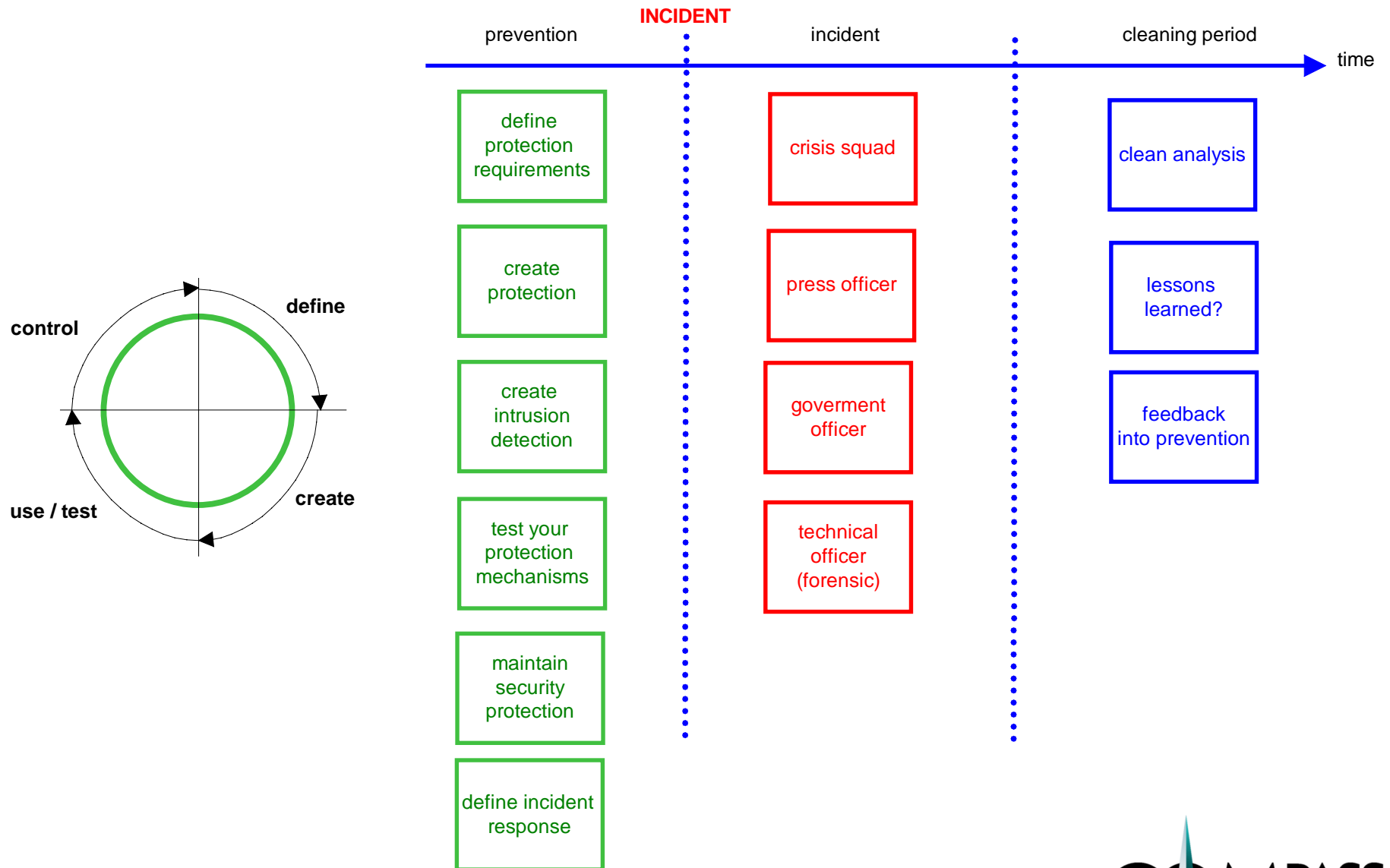


Quelle: CMU/SEI-99-TR-028

# Kapitel: Was ist ein Security Assessment



# Übersicht Sicherheits Aktivitäten



define  
protection  
requirements

create  
protection

create  
intrusion  
detection

test your  
protection  
mechanism

maintain  
security  
protection

define incident  
response

# Security Assessment

- Ein Security Assessment wird *präventiv* eingesetzt
- Dient zur Beurteilung der IST Situation
  - Technik (Vulnerabilities)
  - Organisation (Incident Handling)
- Gehört zur Klasse „test your protection mechanism“

# Begriffe

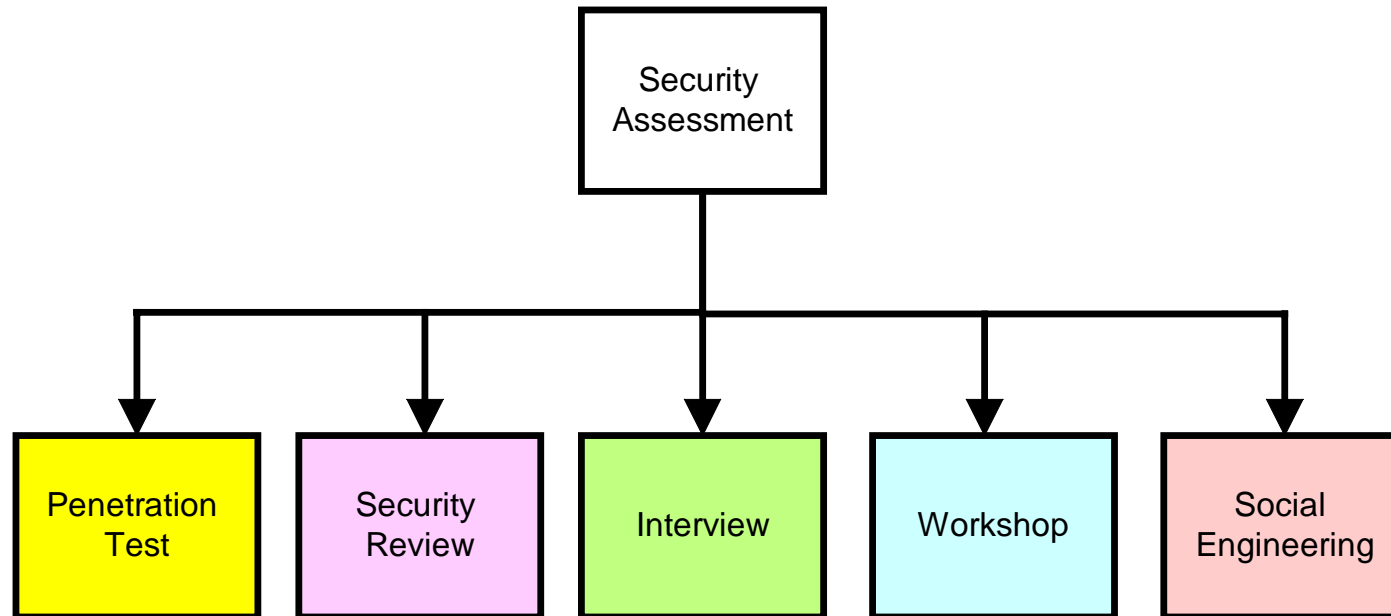
- Methoden

- Unter Security Assessment Methoden sind grundlegende Ansätze zu verstehen, die für die Durchführung eines Assessments angewendet werden können.
- Die Erklärung von Methoden folgt auf den nächsten Folien ...

- Tätigkeiten

- Unter Security Assessment Tätigkeiten sind Arbeitsschritte zu verstehen, die für die Erfüllung eines Security Assessments angewendet werden.
- Die Erklärung der Tätigkeiten folgt auf den nächsten Folien ...

# Übersicht Security Assessment *Methoden*



# Übersicht Security Assessment *Tätigkeiten*

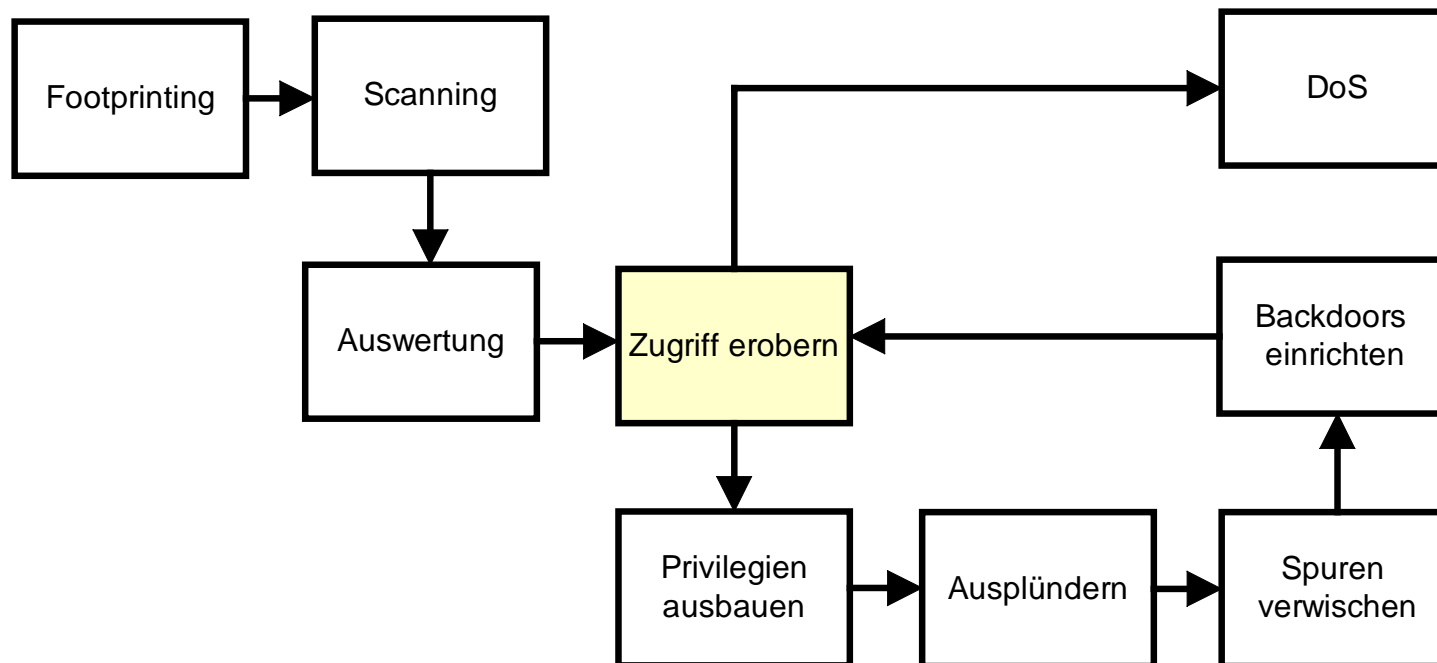
- 01 Aktives Information Gathering
- 02 Passives Information Gathering
- 03 Service Identification
- 04 Vulnerability Research
- 05 Exploitation
- 06 Manual Hacking
- 07 Configuration Review
- 08 Concept Review
- 09 Source Code Analyse
- 10 Interview

# Kapitel: Was ist ein Penetration Test?



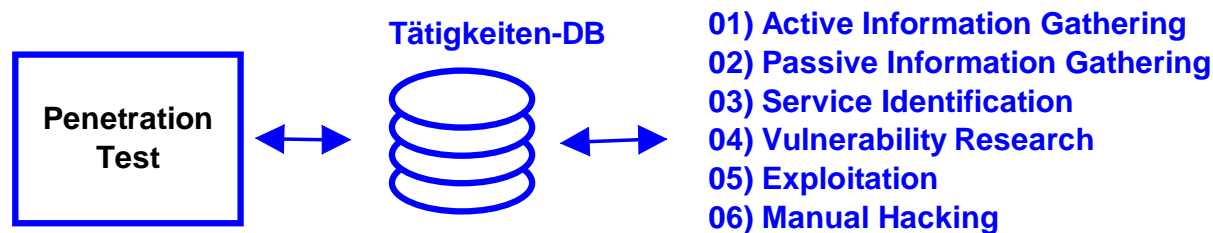
# Anatomie eines Hacker-Angriffes

- Quelle: Das Anti-Hacker Buch (letzte Seite)



# Penetration Test *Tätigkeiten*

- Ein klassischer Penetration Test besteht aus folgenden Tätigkeiten:  
01/02/03/04/05/06



- Es kann aber durchaus sein, dass ein Penetration Tests auf 05/06 verzichtet
- Die Tätigkeiten 01/03/04 werden oftmals durch Vulnerability Scanner wie ISS, Retina, Nessus, Satan, Vigilante etc. durchgeführt. Man findet bei Anbietern dann auch den Begriff „Vulnerability Assessment“

# 01 Aktives Information Gathering

- Aktivitäten
  - Portscanning, DNS Analysen
  - Social Engineering, (Telefon, Fax, E-Mail)
  - Wardialing
  - Wardriving
  - Spezielle Spy-Mails, User Tracking Techniken
- Resultate
  - Überblick über die Infrastruktur und Komponenten (Anordnung, Anzahl)
  - Detektieren von Eintritts- bzw. Austrittspunkten in eine Unternehmung
    - LAN
    - Telefon
    - X25
    - Wireless
    - Bluetooth
    - ...
  - Bewusstsein über das schwächste Glied in der Kette erlangen
  - Identifikation der unterstützten Protokolle

# 02 Passives Information Gathering

- Aktivitäten
  - Lauschattacken / Sniffen
    - Passive OS Fingerprinting
    - Login Credential Stealing
  - Geschäftsberichte lesen
    - E-Mail Adressen
    - Korrekte Anschriften
  - Whois und RIPE abfragen
    - Netzwerke aufspüren
  - Googling
    - Profile erstellen (Privacy Agent)
  - Mailing Listen durchsuchen
    - Eingesetzte Produkte
- Resultate
  - Identifikation von eingesetzten Produkten und Infrastrukturen
  - Identifikation von Mitarbeitern in der Unternehmung
  - Input für das Aktive Information Gathering

# 03 Service Identification

- Aktivitäten
  - Eingesetzte Versionen des „Opfers“ identifizieren
    - Banner Grabbing
    - Analyse von Fehlermeldungen
  - Auswertung von Protokoll-Dateien
    - Mail Headers
    - Logdateien bei Webservern
- Resultate
  - Feststellen der eingesetzten Produkte und Versionen. Diese Informationen dienen als Grundlage für das Vulnerability Research

# 04 Vulnerability Research

- Aktivitäten
  - Parrot Methode
    - Suchen in öffentlich zugänglichen Systemen nach bekannten Sicherheitslücken
    - Nutzung von Vulnerability Assessment Tools (haben diese Vuln-DB bereits eingebaut)
    - Mailing Listen, Bugtraq, CERT
    - Security Advisories
  - Advanced Methode
    - Aktive Suche nach Sicherheitslücken in den zu untersuchenden Produkten und Versionen (z.B. snmp stress test 2002)
    - Reverse Engineering, Code Analyse, Stress Tests
- Resultate
  - Identifikation von „*vulnerable*“ Services. Die Aussagen nach dem Vulnerability Research sind theoretisch und nicht plausibilisiert! Man muss von False-Positives ausgehen.

# 05 Exploitation

- Tätigkeiten
  - Exploit beschaffen, analysieren und im Labor austesten
  - Exploit am Kundensystem anwenden und validieren der Resultate
  - Ausnützen von „**Standard**“ Sicherheitslücken mit dem Exploit
- Resultate
  - Lesezugriff
  - Ausführen von vorinstallierten Tools (Lesen & Ausführen)
  - Ausführen von Malicious Mobile Code (Buffer Overflow)
  - Ausführen von Malicious Mobile Code, indem diese Crackertools zuerst auf das System installiert wurden (Unicode Exploit)
  - Denial of Service

# 06 Manual Hacking

- Tätigkeiten
  - Funktionsweise des „vulnerable“ Service untersuchen. Damit kann auch die Beschaffung des Service mit Tests im Labor gemeint sein
  - Attacke planen
  - Entwicklung des Exploits
  - Ausnützen von „**individual**“ Sicherheitslücken durch den Exploit
- Resultate
  - Lesezugriff (read only)
  - Schreibzugriff (read and write only)
  - Ausführen von vorinstallierten Tools (read and execute)
  - Ausführen von Malicious Mobile Code (inject and execute)
  - Ausführen von Malicious Mobile Code, indem diese Crackertools zuerst auf das System installiert wurden (write and execute)

# Zeitliche Planung von Penetration Tests

- Durchführung von Security Assessments „während“ dem Betrieb existierender Anwendungen und Infrastrukturen
- Typische Penetration Tests
  - E-Mail Gateway
  - Internet Auftritt
  - Prüfen Krisenmanagement (Eskalationsmanagement)

2001		2002											
Dec.	Jan.	Feb.	Mar.	Apr.	May.	June	July	August	Sept.	Oct	Nov.	Dec.	
Security Exercise Q4			Security Review Q1			Security Review Q2			Security Review Q3			Security Review Q4	
cont-scan		cont-scan		cont-scan		cont-scan		cont-scan		cont-scan		cont-scan	
cont-scan	Continuos Scanning												
ass'sment	Security Assessments												

# Stärken/Schwächen des Penetration Test

- Schwächen

- Vorhandene Sicherheitslücken können durch einen Penetration Test nur *teilweise* gefunden werden
- Ein Penetration Test ist nicht umfassend (Stichprobe)
- Ein erfolgloser Einbruchversuch ist lediglich der Beweis dafür, dass das System gegenüber einer speziellen Attacke immun ist
- Es besteht die Gefahr für eine „*Scheinsicherheit*“

- Stärken

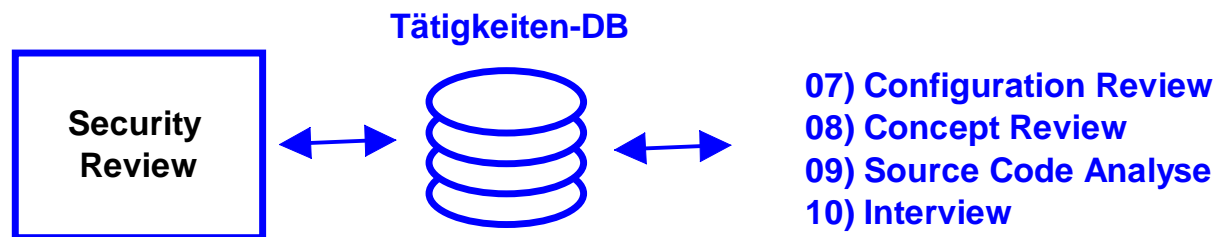
- Relativ kostengünstig
- Falls ein „Beweis“ für Budgets hilfreich ist
- Testen der Alarm Mechanismen und Incident Handling
- Sensibilisierung des Management

# Kapitel: Was ist ein Security Review



# Security Review *Tätigkeiten*

- Ein Security Review besteht aus folgenden Tätigkeiten:  
07/08/09/10



- Ein Security Review verlangt die aktive Teilnahme und Unterstützung des Kunden
- Ein Security Review basiert sowohl auf selbst erhobenen Grundlagen (Configuration Review), als auch auf Fremdaussagen (Interview)

# 07 Configuration Review

- Tätigkeiten
  - Prüfung der Berechtigungen von Prozessen und Files
  - Prüfung der Admin Zugänge (telnet, ftp, ssh, VNC, PCAnywhere, ...)
  - Identifikation der installierten Patches (Vergleich mit SOLL Patchlevel)
  - Prüfung ob Integrity Checking gemacht wird (HIDS)
  - Prüfung, ob Samples und unnötige Komponenten entfernt wurden
  - Prüfung der Passwort Qualität
  - Prüfung Hardening
- Resultate
  - Erkennen von Mängel im Hardening. Das Hardening soll sicherstellen, dass einem Hacker ein möglichst „hacker-unfriendly“ System zur Verfügung steht, falls eine Sicherheitslücke mit Exploit publiziert wird
  - Prüfung, ob das Ersetzen von Binaries auf dem System erkannt wird (Integrity Checking)
  - Prüfen ob die Attacken überhaupt erkannt werden
  - Validierung der Logeinträge. Werden die wesentlichen Teile aufgezeichnet?
  - Prüfung der Zeitsynchronisation (Forensik Anforderung)

# 08 Concept Review

- Tätigkeiten
  - Studium des Konzeptes
  - Erkennen von Gefahren (Analyse)
  - Beurteilung des Konzeptes (Gutachten)
- Resultate
  - Identifikation von Gefahren im Konzept
  - Grundlage für Design Änderungen

# 09 Source Code Analyse

- Tätigkeiten
  - Studium der kritischen Komponenten im Source Code wie:
    - Input Validation (Cross-Site Scripting / SQL Injection)
    - Authentisierung, Password-Management
    - Authorisierung, Datenisolierung
    - Session Management
    - Verwendung von Kryptographie
    - Admin-Seiten / Backdoors
    - Back-End Anbindungen (DB, Host, etc.)
    - Unnötiger Code
- Resultate
  - Erkennen von unsicheren Programmteilen
  - Nicht offensichtliche Schwachstellen können entdeckt werden

# 10 Interview

- Tätigkeiten

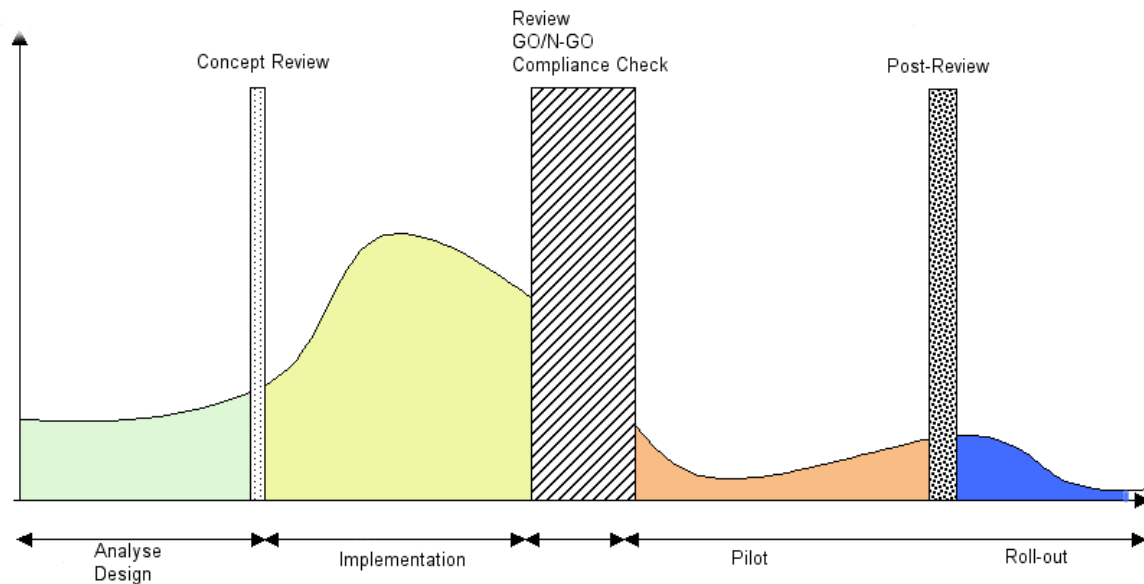
- Befragung der Verantwortlichen/KnowHow Träger
  - Projektleiter
  - System Administratoren
  - Entwickler
  - IT Security Officer
  - Storage Gruppe, Backup Team

- Resultate

- Einarbeitung und Verständnis über Infrastruktur/Applikation
- Die Methode Interview ist vor allem dann sinnvoll, wenn eine sehr grosse Dokumentation vorliegt und ein Gespräch effizienter zum Ziel führt als ein Concept Review (Verkürzung der Einarbeitungszeit)

# Zeitliche Planung von Security Reviews

- Durchführung von Security Reviews „vor“ dem Einsatz von neuen Technologien (Releases)
- Entscheidung, ob ein neuer Release in Produktion darf



# Stärken/Schwächen des Security Review

- Schwäche
  - Zeitintensiv und damit eher teuer
  - Arbeitszeit des Auftraggeber wird alloziert
- Stärke
  - Umfassendere Sicht möglich. Die Qualität der Gefahrenanalyse ist damit besser
  - Aufdeckung von „Security by Obscurity“ Problemen ist möglich
  - KnowHow Transfer wird einfacher

# Kapitel: Wichtige Randbedingungen



# Blackhat vs. Whitehat Approach

- Blackhat Approach (Red Teaming)
  - Ohne Insider Kenntnisse
  - Simulation „Internet“ Angriff
  - Wer die Tätigkeiten als Blackhat Typ durchführen will, der ist an einer „äusseren Sicht“ interessiert.
- Whitehat Approach (Blue Teaming)
  - Mit Insider Kenntnissen
  - Review Firewall Regeln
  - Topologie und Architektur wird offen gelegt
  - Effizienzsteigerung beim Penetration Test
  - Zugriff mit hohen Privilegien
- Ob ein Whitehat oder Blackhat Approach gewünscht und sinnvoll ist, wird zu Beginn bei der Formulierung der Ziele definiert.

# Approach der Security Assessment *Methoden*

	<b>Blackhat</b>	<b>Whitehat</b>
Penetration Test	X	X
Security Review		X
Interview		X
Workshop		X
Social Engineering	X	X

# Approach der Security Assessment *Tätigkeiten*

#	Tätigkeiten	Wie werden Grundlagendaten erhoben?	self	foreign
01	Aktives Info Gathering	Die Grundlagendaten werden durch den Auditor selbst erhoben	x	
02	Passives Info Gathering	Die Grundlagendaten werden durch den Auditor selbst erhoben	x	
03	Service Identification	Die Grundlagendaten werden durch den Auditor selbst erhoben	x	
04	Vulnerability Research	Die Grundlagendaten werden durch den Auditor selbst erhoben	x	
05	Exploitation	Die Grundlagendaten werden durch den Auditor selbst erhoben	x	
06	Manual Hacking	Die Grundlagendaten werden durch den Auditor selbst erhoben	x	
07	Configuration Review	Die Grundlagendaten werden durch den Auditor selbst erhoben	x	
08	Concept Review	Die Grundlagendaten basieren auf Dokumenten. Diese können von der Realität abweichen		x
09	Source Code Analyse	Die Grundlagendaten werden durch den Auditor selbst erhoben	x	
10	Interview	Die Grundlagendaten basieren auf Aussagen von Gesprächspartnern. Diese können von der Realität abweichen		x

# Tätigkeiten-Matrix

#	Methode	Tätigkeiten	Ziel
01	Pen-Test	Aktives Info Gathering	Entscheid für Hacker, ob es sich um ein lohnendes Ziel handelt Optimierung des Angriffes
02	Pen-Test	Passives Info Gathering	siehe Ziel 01
03	Pen-Test	Service Identification	Optimierung des Angriffes. Der Hacker kann einen Angriffs-Plan erstellen
04	Pen-Test	Vulnerability Research	Optimierung des Angriffes. Der Hacker kann einen Angriffs-Plan erstellen
05	Pen-Test	Exploitation	Aktive Ausnützung einer produktspezifischen Sicherheitslücke. Diese werden in den Advisories bekannt
06	Pen-Test	Manual Hacking	Aktive Ausnützung einer individuellen Sicherheitslücke. Diese ergeben sich durch unsicheres Programmieren von zum Beispiel Webapplikationen
07	Review	Configuration Review	Prüfung der Konfiguration am System. Dieses Modul kann Input für 05 oder 06 darstellen
08	Review	Concept Review	Prüfung des Konzeptes. Dieses Modul kann Input für 05 und 06 darstellen.
09	Review	Source Code Analyse	Prüfung von Programmteilen, die selbst entwickelt wurden. Typischerweise Login, Logout, Session Handling, Verschlüsselung.
10	Review und Social Eng.	Interview	Auditor will auf das KnowHow der Verantwortlichen zugreifen, da dieses allenfalls schriftlich nicht vorliegt (kein Konzept).

# Nutzen eines Security Assessment (1)

- Man prüft die Effizienz der geplanten oder implementierten Schutzmassnahmen
- Es sollen Gefahren identifiziert werden, die sich durch den Einsatz der gewählten Architektur und Technologie ergeben
- Man versucht das schwächste Glied in einer vernetzten und komplexen Umgebung zu finden
- Man versucht Sicherheit messbar, und damit steuer- und kontrollierbar zu machen

# Nutzen eines Security Assessment (2)

- Fachlich
  - **Qualität:** der Auftraggeber kann die Leistung des Lieferanten bezüglich Security besser beurteilen
  - **Entscheide:** der Auftraggeber erhält Entscheidungsgrundlagen für ein GO oder NO-GO in Produktion
  - Wissen, was ein „Hacker“ in einer gewissen Zeit erreichen kann
  - Wissen über die Wirksamkeit der gewählten Schutzsysteme (Rest-Gefahren)
  - Validierung der Alerting Mechanismen und entsprechende Erkenntnisse betreffend Eskalationsmanagement
  - Sicherstellen, dass „bekannte“ Sicherheitslücken geschlossen sind
- Politik
  - Der Auftraggeber sichert sich persönlich ab
  - Der Auftraggeber kann Gründe für Budgets schaffen
- Rechtliche
  - Beweis für die Erfüllung des Datenschutz

# Gefahrenanalyse oder Risikoanalyse?

- Ein *Penetration Test* oder *Security Review* weist potenzielle Gefahren aus, die durch Hacker ausgenutzt werden könnten. Diese sind vom Begriff „Risiko“ getrennt zu betrachten. *Risiko* beinhaltet die Wertung der Gefahr mit einer Wahrscheinlichkeit und einem potenziellen Schaden.
- Die Bewertung des *potenziellen Schadens* ist in der Praxis sehr sehr schwierig. Falls das trotzdem gemacht wird, dann meist durch Personen und Fachkundige, die das Business der Firma kennen.
- Die Bewertung der *Eintretenswahrscheinlichkeit* ist ebenfalls schwierig. Hier muss man sich darauf stützen, wie „leicht“ oder „schwierig“ es für einen Angreifer ist, eine gewisse Attacke auch real durchzuführen.

# Beispiel Risikoanalyse

- Gefahr: OpenSSL Buffer Overflow

Sicherheitslücke	OpenSSL Buffer Overflow bei Apache Webserver
Gefahr	Ausführen von beliebigem Code aus dem Internet
Angriff	Datenbank auslesen (Kreditkarten Diebstahl)
Schaden	Direkte oder indirekte Schäden kosten 250'000.--
Eintretenswahrscheinlichkeit pro Jahr	Einmal in 10 Jahren
Risiko	$(1 * 250'000.--) / 10 \text{ Jahre} = 25'000.-- \text{ pro Jahr}$

# Beispiel von Compass Security Report

## 4.1 Application Checks

Nr.	Reference	Weakness	Threat	Elimination	Rating	Comments
1	6.2	Brute force attacks on passwords are possible.	An attacker might gain a valid password that he could use to access the application.	<ul style="list-style-type: none"> <li>Lock the account after several unsuccessful <u>log-in</u> attempts. An administrator has to unlock the account.</li> <li>Insert an increasing delay after each wrong <u>log-in</u>. This hinders brute force attacks.</li> </ul>	🚩🚩🚩	
2	6.2	There is no log-out mechanism in the application. A session is valid as long as the browser stays open.	If an attacker manages to steal the user's cookie, the session seems to be valid for a long time.	<p>Implement a log-out mechanism.</p> <p>Set appropriate session timeout values.</p>	🚩🚩	
3	6.2	A user cannot change his password. The password is defined by the administrator and is not changed regularly.	Brute forcing a given account can gain a valid password.	Implement a mechanism for users to change their passwords but require them to choose passwords containing numbers, letters (upper and lower case) and special characters.	🚩🚩	
4	6.1	The session is valid for an undefined time span.	If an attacker can steal the session cookie, he would then be able to use the application for a long time.	Set the session timeout to a specific time (eg. 30 minutes).	🚩	
5	6.1	The session cookie is not set to "Server Secure".	If an attacker is able to enforce communication via HTTP rather than HTTPS, he could sniff the session cookie.	Set "Cookie Secure = True" in the administration interface under "session tracking".	🚩	

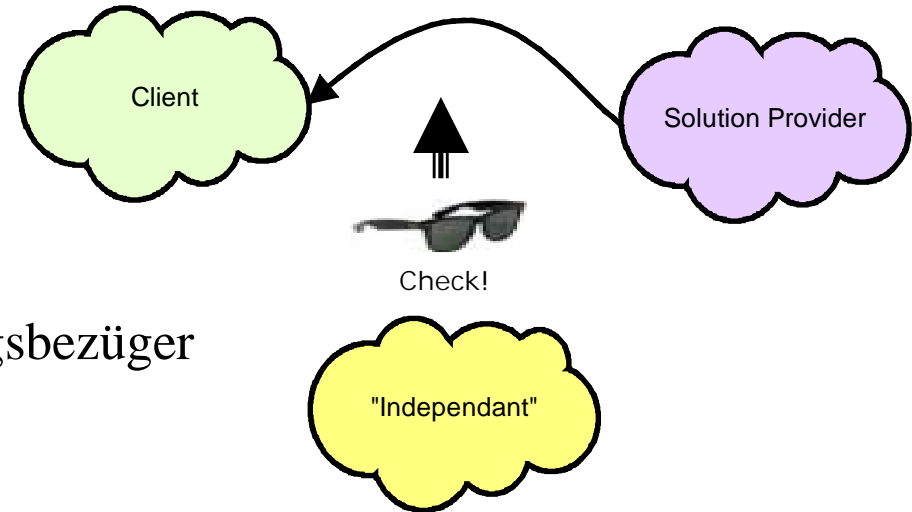
# Kapitel: Marketing



# Der Markt

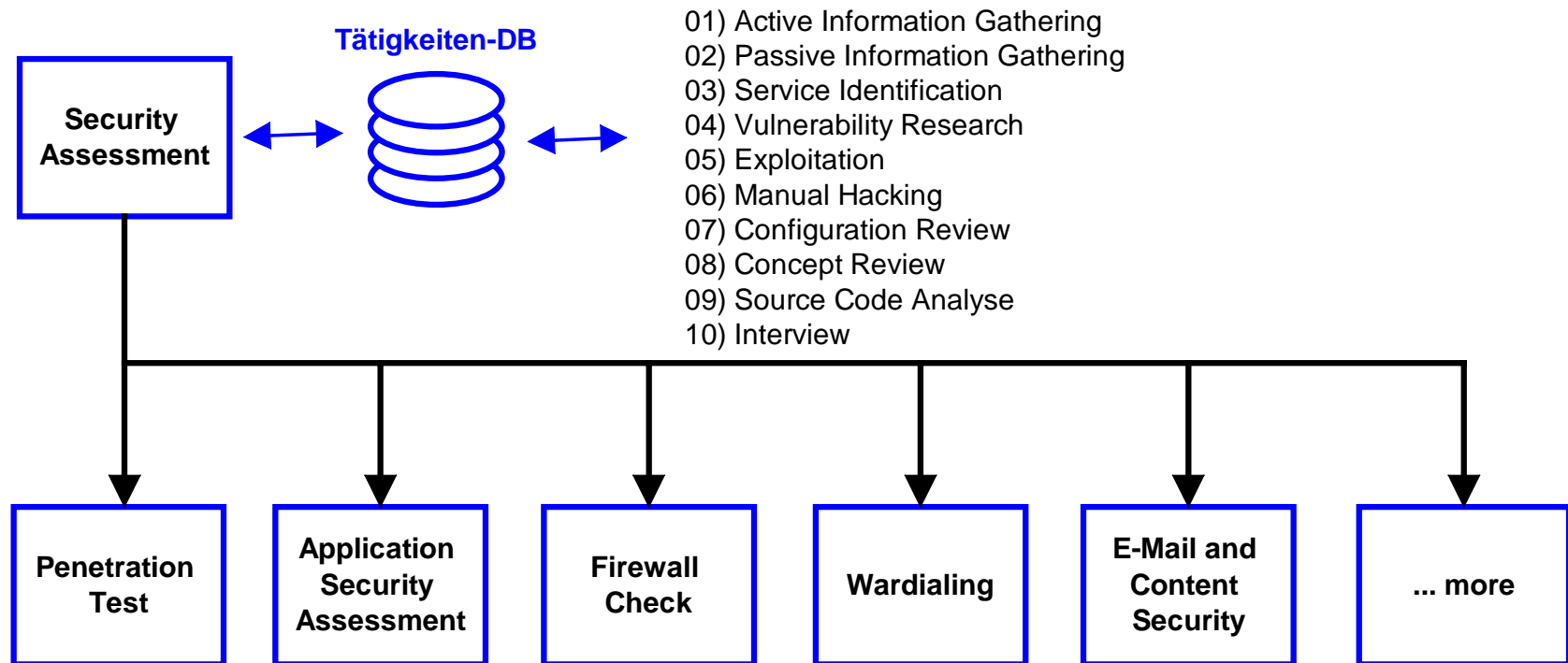
- Marktteilnehmer

- Client – das ist der Leistungsbezüger einer Leistung
- Solution Provider – das sind Leistungserbringer (Vendor), die den Kunden beim Aufbau einer Lösung unterstützen.
- Independant – diese Firmen „*beurteilen*“ die Leistung der Solution Provider und sind sowohl finanziell unabhängig als auch produkteneutral



# Security Assessment

- Marketing Sicht

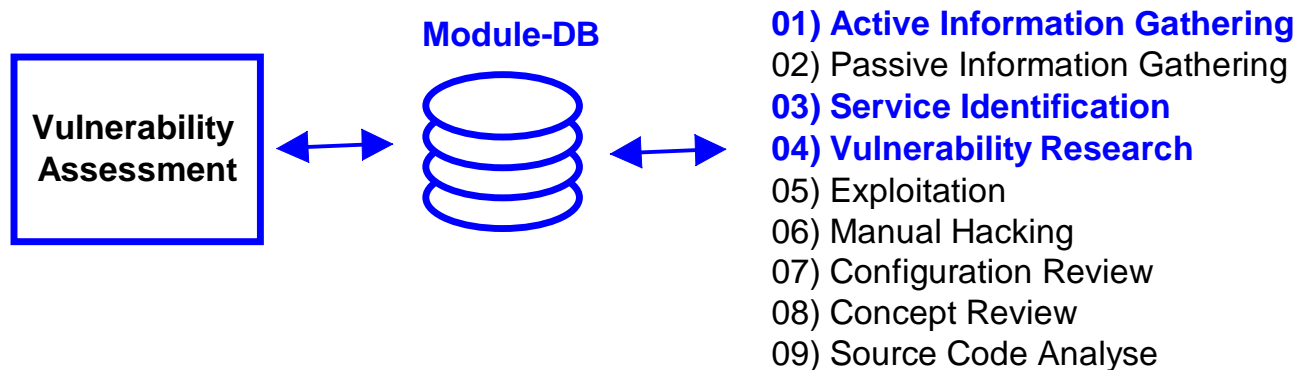


# Marketing – Vorsicht!

- Jeder Anbieter versteht etwas „anderes“ unter einem Penetration Test
  - Inhalt
  - Vorgehen
  - Tiefe
  - Mit oder ohne Exploitation
- Verwechslungsgefahr zwischen Vulnerability Assessment und Penetration Test!

# Definition Vulnerability Assessment

- Ein klassisches Vulnerability Assessment besteht aus folgenden Tätigkeiten: 01/03/04



- Identifikation von Sicherheitslücken
- Meist ohne Plausibilisierung (False-Positives)
- Ohne aktive Ausnutzung der Schwachstelle

# Kriterien an Security Assessment Partner

- Ist der Anbieter vertrauenswürdig?
- Ist der Anbieter neutral (sonst besteht die Gefahr, dass der Anbieter bei den Empfehlungen voreingenommen ist)
- Bietet der Anbieter Security Assessments zusätzlich an, oder ist das seine Kern Kompetenz?
- Ist der Anbieter international vertreten? (grosse Konzerne)
- Wie positioniert sich der Anbieter?
  - Parrot (Proxy für Advisories)
  - Parrot (Wiederverwendung von bekannten Exploits)
  - Expert (findet selbst Sicherheitslücken – Applied Research)
  - Expert (Kundenspezifische Tests – Eigene Programme)

# Kriterien für Security Assessment Partner

Quelle: [http://www.sans.org/rr/penetration/third\\_party.php](http://www.sans.org/rr/penetration/third_party.php)

- # Find vendors that ask to see the company's security policy before they make any recommendations.
- # Use an established and well-known firm.
- # Deploy a fake honey pot and see if they can detect it.
- # Ask about types of tools used and what operating systems they are used on and how many.
- # Do they ask for a cutout?
- # Get references, no matter what.
- # Get the proposal in writing.
- # What other services do they promise? (follow-ups etc.)
- # Ask to see their certification.
- # Do they use the bait and switch technique?
- # Do they employ hackers?
- # Meet with the forensic engineers one on one.
- # Ask for a security clearance.
- # Ask them where will the data be stored after the test is over and for how long.
- # Be there on site all the time!
- # Run a background check on them yourself if there is any doubt.
- # Get what you pay for.
- # Perform follow up checks on their IP address range destined to your network



# Kapitel: Planung und Durchführung



# Klarwerden über die Zielsetzung des Assessment

- Mit oder ohne Insiderwissen?
  - Blackhat oder Whitehat Approach?
- Penetration Test oder Security Review?
  - Stichprobe oder umfassende Security Sicht erwünscht?
  - Phase 1 als Penetration Test, Phase 2 als Security Review?
- Was ist die Motivation für ein Assessment?
  - Persönliche Absicherung
  - Argumente für Budget finden (Security Investment)
  - Erkennen tatsächlicher Gefahren und auch Bereitschaft, die Findings beheben zu lassen
  - KnowHow Transfer
  - Grundlagen für Compliance Meeting (GO/N-GO Meetings)

# Wichtige Fragen (1)

- **„Welche“** Attacken will man verhindern
  - Sprungbrett Attacke
  - Daten lesen, verändern oder zerstören
  - Ausfall der Systeme
  - Ressourcen für Dritte (z.B. als Plattform für Porno-Bilder)
- **„Was“** will man schützen?
  - Anzahl Systeme
  - Assets (Daten, Dokumente, Konten, etc.)

# Wichtige Fragen (2)

- Vor „**wem**“ will man sich schützen?
  - Angriffe von anonymen Benutzern
  - Angriffe von „normal“ registrierten Benutzern
  - Angriffe von Script Kiddies, Joy Rider, Wirtschaftskriminalität,
- Von „**wo**“ erwartet man den Angriff?
  - Angriffe von Aussen (Internet, Telefon, X25, Wireless, Bluetooth)
  - Angriffe von Daten-Lieferanten (Mietleitungen, Feeds)
  - Angriffe von Innen (eigene Mitarbeiter, externe Berater)
  - Angriffe aus einer DMZ (Szenario Hacking)
  - Angriffe via Administration Workstations
  - Angriffe via Backup Zugänge

# Tätigkeiten des Kunden bei der Durchführung

- Unterlagen bereitstellen
- Zugangsberechtigungen erteilen
- Arbeitsplätze bereitstellen
- Informationskanäle festlegen
- Notfallnummern definieren
- Vertraulichkeitserklärung einfordern
- Täglich Statusinformationen einholen
- Tagesentscheide treffen, falls interaktiv die weiteren Schritte von ersten Ergebnissen abhängen

# Probleme bei der Durchführung

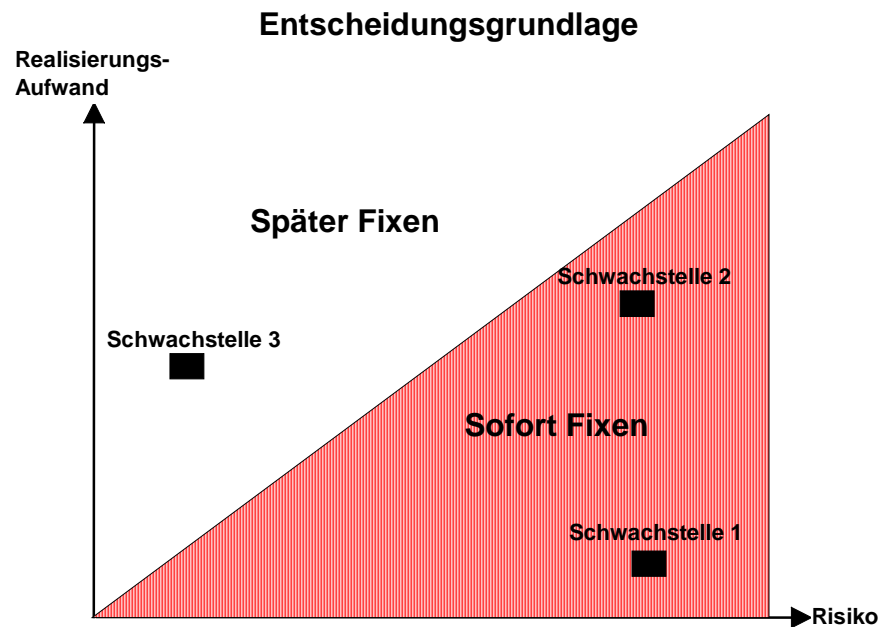
- Der Test wird auf die Testumgebung durchgeführt. Oftmals argumentieren die Hersteller damit, dass diese oder jene Sicherheitslücke in der Produktion behoben ist
- Moving Target (zu testende Ziele sind noch in der Entwicklung)
- Penetration Test Partner hat die Test-Tools auf seinem eigenen Laptop installiert – die Firmen Policy verbietet aber den Anschluss von fremden Geräten
- Fingerprinting – man sucht einen Schuldigen
- Abgrenzung der korrektiven Massnahmen. (z.B. die Erstellung eines Konzeptes)
- Fehlen einer SOLL-Referenz (kein Security Konzept)

# Anforderung an die Resultate

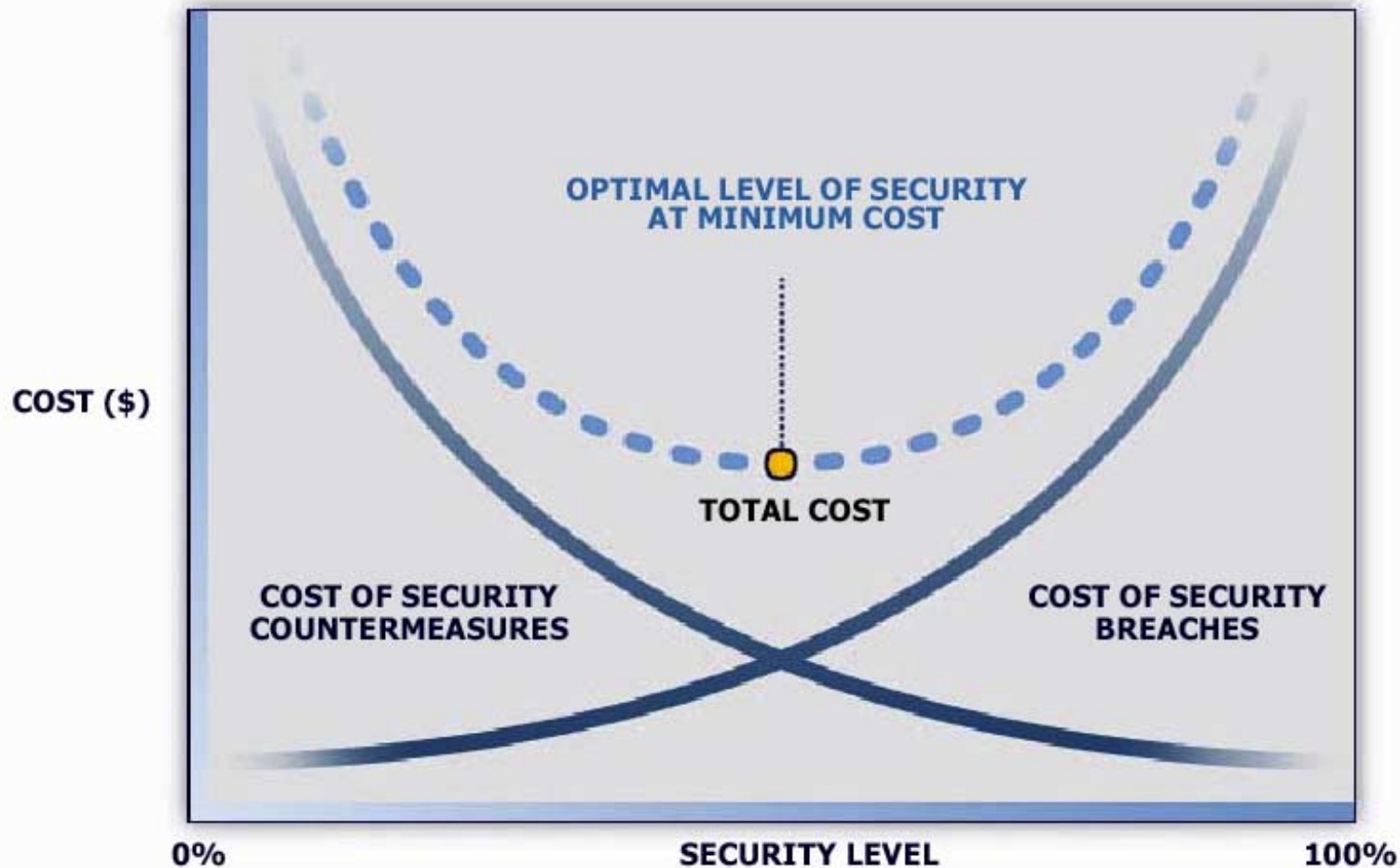
- Rasche Auslieferung des Report nach dem Test (1 Woche)
- Plausibilisiert
- Versehen mit einer Erklärung, was die Sicherheitslücke bewirken könnte
- Vorschlag für korrektive Massnahmen
- Selbständige Bewertung der Resultate
- Allenfalls eine Nachprüfung (Recheck), falls eine grosse Anzahl und schwerwiegende Mängel identifiziert wurden

# Was machen mit den Resultaten?

- Es braucht jemand innerhalb des Auftraggebers, der die Ergebnisse bewertet, entscheidet und entsprechende Massnahmen einleitet



# Was machen mit den Resultaten?



# Kapitel: Rechtliche Aspekte



# Vertrag

- Für den Vertrag eines Security Assessments, insbesondere beim Penetration Test sind folgende Aspekte zu beachten
  - Schriftliche Form (auch Änderungen bei Durchführung)
  - Genaue Bezeichnung der Vertragspartner und einen Ansprechpartner pro Partei (Unterlieferanten?)
  - Genaue Bezeichnung des Vertragsgegenstand. Insbesondere von Ziel, Verfahren, eingesetzten Technologien
  - Vertraulichkeitserklärungen
  - Einverständniserklärung für ein Security Assessment

## Besonders zu beachten (Erfahrungsbericht)

- Einverständniserklärungen einholen vom Serverbetreiber, wenn der zu penetrierende Server nicht dem Auftraggeber gehört. Abklären ob auf den Servern noch Services von anderen Kunden installiert sind
- Siehe Beilage CDROM: Musterreglement für die Internet- und E-Mail Überwachung am Arbeitsplatz  
(<http://www.edsb.ch/d/doku/leitfaeden/internet/index.htm>)

# Schweizerisches Recht (auf einen Blick)

- Datenschutzgesetz (DSG) vom 19. Juni 1992
  - Art. 7: Datensicherheit
- Strafgesetzbuch (StGB)
  - Art. 143: Unbefugte Datenbeschaffung
  - Art. 143: Unbefugtes Eindringen in ein Datenverarbeitungssystem
  - Art. 143: Datenbeschädigung
  - Art. 179 novies 142 : Unbefugtes Beschaffen von Personendaten
- Obligationenrecht (OR)
  - Allgemeines Vertragsrecht

# Datenschutzgesetz (DSG) vom 19. Juni 1992

- Art. 7: Datensicherheit

<sup>1</sup> Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.

# Strafgesetzbuch (StGB)

- Art. 143: Unbefugte Datenbeschaffung

<sup>1</sup> Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, sich oder einem andern elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.

<sup>2</sup> Die unbefugte Datenbeschaffung zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

# Strafgesetzbuch (StGB)

- Art. 143: Unbefugtes Eindringen in ein Datenverarbeitungssystem

Wer ohne Bereicherungsabsicht auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

# Strafgesetzbuch (StGB)

- Art. 143: Datenbeschädigung

1. Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

Hat der Täter einen grossen Schaden verursacht, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden. Die Tat wird von Amtes wegen verfolgt.

2. Wer Programme, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 genannten Zwecken verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonstwie zugänglich macht oder zu ihrer Herstellung Anleitung gibt, wird mit Gefängnis oder mit Busse bestraft.

Handelt der Täter gewerbsmässig, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden.

# Strafgesetzbuch (StGB)

- Art. 179 novies 142: Unbefugtes Beschaffen von Personendaten

Wer unbefugt besonders schützenswerte Personendaten oder Persönlichkeitsprofile, die nicht frei zugänglich sind, aus einer Datensammlung beschafft, wird auf Antrag mit Gefängnis oder mit Busse bestraft.

# Anhang: Leitfaden Eidg. Datenschutzbeauftragter

- Eidgenössischer Datenschutzbeauftragter  
Leitfaden über Internet- und E-Mail-Überwachung am Arbeitsplatz  
<http://www.edsb.ch/d/doku/leitfaeden/internet/index.htm>
- Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes  
<http://www.edsb.ch/d/doku/leitfaeden/tom.pdf>

# Anhang: Links

- Sicherheitsüberprüfungen von IT-Systemen mit Hilfe von “Tiger-Teams”  
<http://www.isaca.ch/download/tigerteam/tigerteam.pdf>
- Eidgenössisches Justiz- und Polizeidepartement  
Rechtsinformatik und Informatikrecht  
<http://www.ofj.admin.ch/d/index.html>
- Eidgenössischer Datenschutzbeauftragter  
<http://www.edsb.ch/>  
Fallbeispiele: <http://www.edsb.ch/d/themen/internet/bsp.htm>
- Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG)  
[http://www.admin.ch/ch/d/sr/c235\\_1.html](http://www.admin.ch/ch/d/sr/c235_1.html)
- Schweizerisches Strafgesetzbuch  
<http://www.admin.ch/ch/d/sr/31.html#311.0>

# Kapitel: Schluss



# SANS Readings

- <http://www.sans.org/rr/penetration/>
- <http://www.sans.org/rr/audit/>
- <http://www.sans.org/rr/social/>
- <http://www.sans.org/rr/appsec/>
- <http://www.sans.org/rr/practice/>
- <http://www.sans.org/rr/incident/>



# Compass Security Network Computing

<http://www.csnc.ch/>

## Professional Ethical Hacking

Ivan Buetler. Dipl. El. Ing. HTL, STV  
Ivan.buetler@csnc.ch



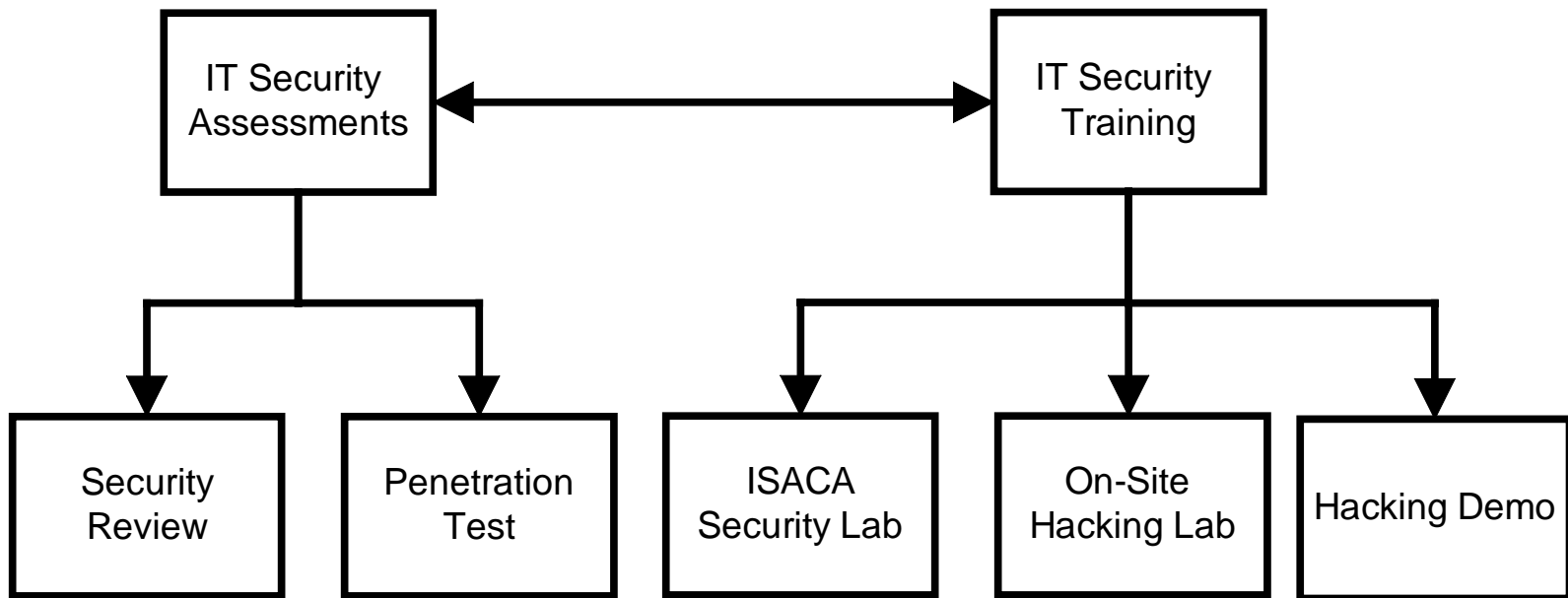
# Who is who: Compass Security

- Compass Security Network Computing AG (csnc)
  - 1999: founded by Walter Sprenger and Ivan Bütler
  - 6 Security experts
  - 3 development engineers (each approx. 30% FTE)
  - Independent security assessments around IT security
    - Penetration tests
    - Security reviews
    - Security training
  - Know how transfer to Fachhochschule Rapperswil
    - [www.sicherheitstest.ch](http://www.sicherheitstest.ch)
- Ivan Bütler, Dipl. El.-Ing. HTL, STV
  - working for Compass since startup, partner
  - was working for r3 security engineering ag



# Compass Security AG

- Unsere Dienstleistungen



Compass Security AG  
Glärnischstrasse 7  
Postfach 1671  
8640 Rapperswil

info@csnc.ch

<http://www.csnc.ch/>

Tel: 055 214 41 60

Fax: 055 214 41 61

