



IT-Brunch



Planung und Durchführung von  
Penetrationstests

Dipl.-Inform. Sebastian Schreiber





- @ Gegründet 1998
- @ 18 Festangestellte + 2 Extern
- @ Sitz in Tübingen
- @ Deutschlandweit und teilweise europaweit/weltweit tätig.
- @ **Dienstleistungen:**
  - @ Penetration Testing & Sicherheitsanalysen
  - @ Incident Response/Schulungen
- @ **Kunden:**

HP, Bosch, Bosch-Rexroth, Siemens, European Commission, Union Investment, Scheffler, TÜV München, T-Systems, T-Com, Neckermann, Lufthansa, Deutsche Flugsicherung, Bundeswehr, SAP AG, BMW, Audi AG, Daimler-Chrysler AG, Innenministerium/LKA Niedersachsen, Schufa, Gebr. Heller Maschinenfabrik, Europäische Zentralbank, Festo AG, Burda Systems, Roland-Rechtsschutz, Basler Versicherung, Kodak, Heller Bank, Baader Wertpapierbank, Fielmann AG, Deka-Bank etc.



- @ Sicherheitsprobleme lassen sich effizient aufdecken.
  - @ Fremdkontrolle ist Selbstkontrolle überlegen.
  - @ Der „bezahlte Hacker“ verfügt über viel Erfahrung und identifiziert Probleme.
  - @ Voraussetzung: Ein Vertrauensverhältnis zwischen Dienstleister und Kunde muss bestehen.
-



- @ **Wissensstand**
  - @ Zero Knowledge Test
  - @ Whitebox Test
- @ **Simulierter Angriffsursprung**
  - @ vom Internet aus
  - @ vom Firmennetz aus
- @ **Aggressivität**
  - @ D.o.S.-Attacken eingeschlossen?
  - @ Ein gewisses Absturzrisiko sollte in Kauf genommen werden.
- @ **Angriffsmittel**
  - @ Rein technische Methoden
  - @ Social Engineering
  - @ Dokumentenanalyse
  - @ Interviews
- @ **Testtiefe / Testfrequenz**
  - @ Ein grober Test vieler Systeme
  - @ Ein fundierter, ausführlicher Test
- @ **Einschränkungen**
  - @ Testzeit (z.B. nur ausserhalb der Geschäftszeit)
  - @ Limit der Bandbreite oder der Scangeschwindigkeit
- @ **Test-Modus**
  - @ Test "im Team"
  - @ Test im Dialog mit dem Kunden ("Tandemtest")



## Angekündigt oder unangekündigt?

	<b>Angekündigt</b>	<b>Unangekündigt</b>
<b>Vorteile</b>	<ul style="list-style-type: none"><li>▪ Schafft Sicherheitsbewusstsein</li><li>▪ Kooperatives Vorgehen vereinfacht Test und Maßnahmenwahl.</li></ul>	<ul style="list-style-type: none"><li>▪ Unverfälschte Bewertungsmöglichkeit</li></ul>
<b>Nachteile</b>	<ul style="list-style-type: none"><li>▪ Evt. leicht verfälschtes Bild</li></ul>	<ul style="list-style-type: none"><li>▪ Schafft Misstrauen</li><li>▪ Administrator fühlt sich hintergangen.</li><li>▪ Reaktanz</li></ul>

### Bsp. aus der Praxis:

1. Zur Aufwandsschätzung eines Projekts wird ein Portscan durchgeführt.
2. Der PenTest wird angekündigt.
3. Bei der Durchführung des Tests stellt sich heraus, dass 30% der Ports nicht mehr erreichbar sind. Darunter sämtliche Netbios- und NFS-Ports.

**Guter Kompromiss:** Grobe Ankündigung des Tests.



<b>Aggressivität</b>	<b>Konsequenz auf die Stabilität der getesteten Systeme</b>
Einfacher Portscan	Minimales Risiko.
Inkl. Attacken mit dem Ziel in Rechner einzudringen. Absturzrisiken werden bewusst in Kauf genommen.	Mit einem geringen, steuerbaren Risiko können Systeme abstürzen.
Inkl. DOS-Attacken	Hohes Risiko.
Inkl. DDOS	Sehr hohes Risiko. Auch ISP kann in Mitleidenschaft gezogen werden. Strafbar/nicht ratsam. Schaden schwer kalkulierbar.

Wenig Risiko aber wenig Erkenntnis



Hohes Risiko, hoher Erkenntnisgewinn

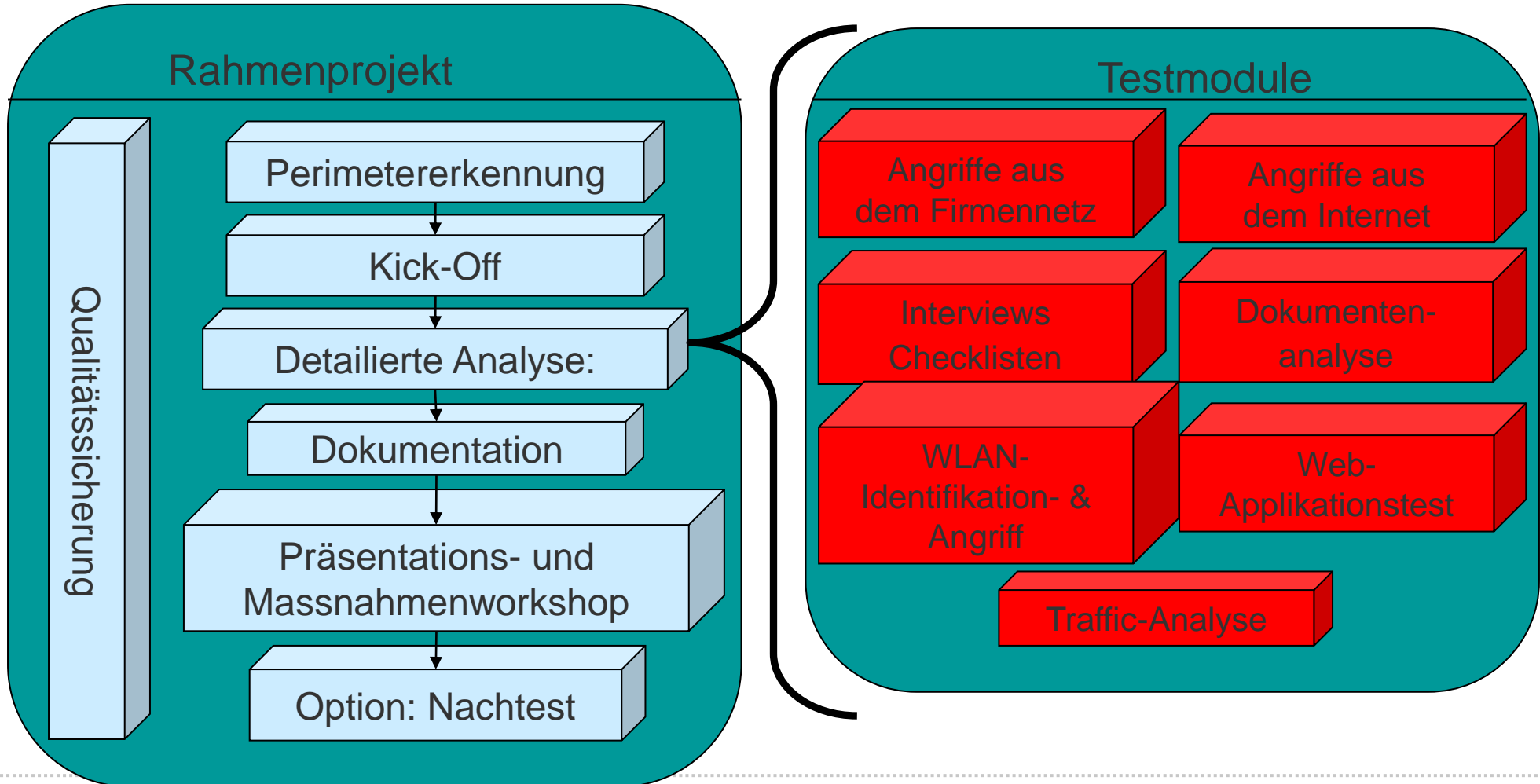
# Unterschiede: externer/interner

	<b>Extern (über das Internet)</b>	<b>Intern (vom Firmennetz aus)</b>
<b>Anzahl möglicher Täter</b>	Sehr hoch	Sehr niedrig
<b>Angriffsfläche</b>	Nur wenige Rechner/Ports erreichbar.	Riesige Masse an erreichbaren Systemen.
<b>Sicherungsmöglichkeit</b>	Hervorragend: Firewalls beschränken den Zugriff auf wenige, gute gewartete Systems.	Leider sehr eingeschränkt.
<b>Konsequenz für Pen-Test</b>	Möglichst genaue Analyse der erreichbaren Dienste.	Eher stichprobenhaft. Suche nach kritischen Fehlern, die überhaupt behebbar sind.

<b>Pro</b>	<b>Contra</b>
Identifiziert Risiken, die in der Realität ausgenutzt werden.	<ul style="list-style-type: none"><li>■ Angriff auf menschliche Eigenschaften</li><li>■ Zerstört Vertrauen</li></ul>

@ Empfehlung:

- @ Nur angekündigt.
- @ Nur nach Security-Awareness-Training  
Idee: Chefsekretärinnen als Multiplikator
- @ Keine Mitarbeiter „ans Messer“ liefern!



# Bewertung der identifizierten Schwachstellen

## **Exploit-Hürde:**

- @ Verfügbar, getesteter Exploit
- @ Proof-of-concept Exploit
- @ Gerücht über einen Exploit
- @ Mögliche Angreifbarkeit (z.B. ein Buffer Overrun)
- @ Risiko nur akademisch/theoretisch vorhanden.

## **Erreichbarkeit schwachen Services:**

- @ Aus dem Internet
- @ Von privilegierten Systemen aus dem Internet
- @ Aus dem Firmennetz
- @ Von privilegierten Rechnern aus dem Firmennetz
- @ Nur von authentifizierten Benutzern (z.B. FTP-Logins)

## **Bewertung der externen Sicherheit (Kennzahlen):**

- @ Anzahl offener Ports
- @ Anzahl *unterschiedlicher Services*
- @ Anzahl der *unterschiedlichen Server*



1. PenTests als Prozess
2. Frühzeitige Terminierung
3. "Dabei sein"
4. Lieber angemeldete Penetrationstests
5. Greybox-Test ist effizient
6. Prüfer: unabhängiger Spezialist
7. Besser eine knappe Prüfung als keine
8. Kein DDOS
9. Clustering
10. Nachtest festzurren



Teilprojekt	Kurzbezeichnung (s. Anhang)	Planungshorizont: 5 Jahre									
		2011		2012		2013		2014		2015	
		Q1	Q3	Q1	Q3	Q1	Q3	Q1	Q3	Q1	Q3
Kick-Off-Workshop (telefonisch)	KICK	ohne Berechnung		ohne Berechnung		ohne Berechnung		ohne Berechnung		ohne Berechnung	
Analyse der IP-Range aus dem Internet Die IP-Range des Kunden wird mit unterschiedlichen Sicherheitsscannern geprüft. False-Positives werden identifiziert. Manuelle Tests folgen. (jährlich)	INTERNET		2	-	2	-	2	-	2	-	2
Analyse der Web-Applikation aus dem Internet (jährlich)	WEB	-	2,75	-	2,75	-	2,75	-	2,75	-	2,75
Analyse der Systeme aus dem Firmennetz (1,5-jährlich)	CN	2,5	-	-	2,5	-	-	2,5	-	-	2,5
Analyse des WLANs (alle 2 Jahre)	WLAN	-	-	-	1	-	-	-	1	-	-
Angriff auf die TK-Anlage (alle 2 Jahre)	TK	-	-	2	-	-	-	2	-	-	-
D.o.S.-Attacke Ausserhalb der Geschäftszeiten wird versucht, die Systeme des Kunden zum Absturz zu bringen. Überlastattacken werden nicht durchgeführt, sondern lediglich logische D.o.S.-Attacken. (alle 2 Jahre)	D.o.S.	1	-	-	-	1	-	-	-	1	-
Dokumentation inkl. Qualitätssicherung	DOKU	2	1,5	1	3	0,5	2,5	2,5	3	0,75	3
Abschlusspräsentation	PRÄS	1 (optional)	1 (optional)	1 (optional)	1 (optional)	1 (optional)	1 (optional)	1 (optional)	1 (optional)	1 (optional)	1 (optional)
<b>Summe der Personentage:</b>		<b>5,5</b>	<b>6,25</b>	<b>3</b>	<b>11,25</b>	<b>1,5</b>	<b>7,25</b>	<b>7</b>	<b>8,75</b>	<b>1,75</b>	<b>10,25</b>
Durchschnittlich erforderliche Personentage pro Jahr:	12,5										

## Test-Tiefe bei Applikationstests

Kalkulationsgrundlage für die reinen Test-Tage für die Prüfung von Web-Applikationen		<b>Komplexität</b> der Applikation gemessen an der Anzahl der Formulare, der Berechtigungsstufen; der Anzahl der Code-Zeilen, etc.			
		<b>Niedrig</b>	<b>Mittel</b>	<b>Hoch</b>	<b>Sehr hoch</b>
<b>Schutzbedarf</b> , gemessen am Erwartungswert für den eintretenden Schaden, der resultieren würde, wenn die Applikation durch einen Dritten kompromittiert würde und die enthaltenen Daten z.B. an einen Wettbewerber gelangen würden oder im Internet veröffentlicht würden.	<b>Niedrig</b>	1	1,5	2	3
	<b>Mittel</b>	1,5	2,5	4	6
	<b>Hoch</b>	2	4	8	10
	<b>Sehr hoch</b>	3	6	10	15



1. Unabhängigkeit
2. Vertraulichkeit
3. Provisionsverbot
4. Vorsicht
5. Professionalität und QM
6. Verbindlichkeit
7. Objektivität und Transparenz
8. Striktes Legalitätsprinzip
9. Respekt vor Menschen
10. Korrektes Zitieren

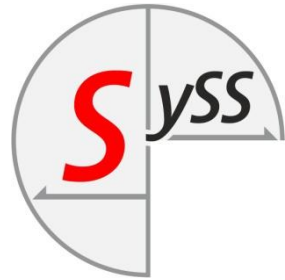


IT-Brunch

## Kontakt

### Firma

SySS GmbH  
Wohlboldstr. 7  
72070 Tübingen



Web [www.SySS.de](http://www.SySS.de)  
Telefon 0 7071-407856-0  
E-Mail [Schreiber@SySS.de](mailto:Schreiber@SySS.de)



IT-Brunch

## Kontakt

### Firma

SySS GmbH  
Wohlboldstr. 7  
72070 Tübingen



Web [www.SySS.de](http://www.SySS.de)  
Telefon 0 7071-407856-0  
E-Mail [Schreiber@SySS.de](mailto:Schreiber@SySS.de)