# Angriff zur Verteidigung
—
# Erfolgsfaktoren für gute Penetrationstests

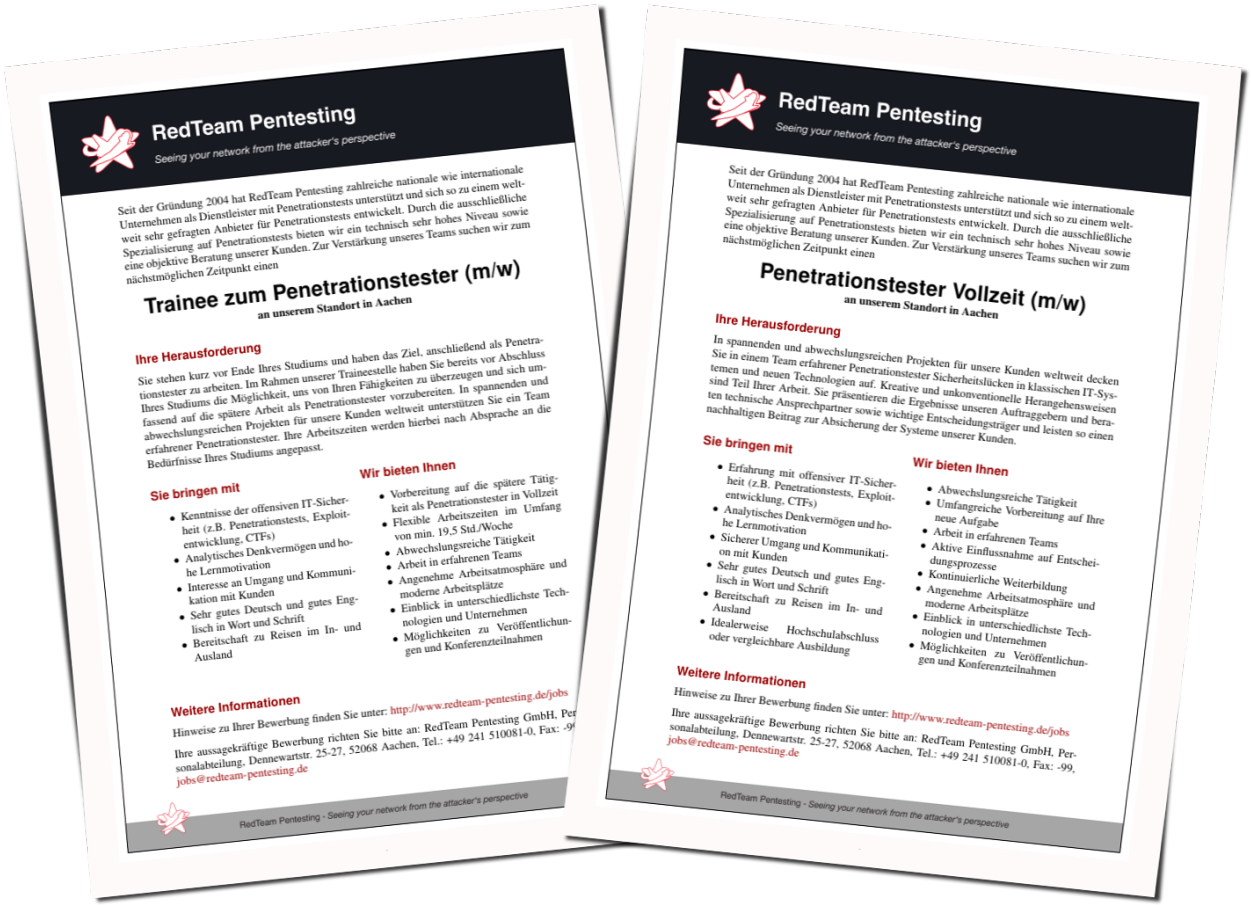
Jens Liebchen - RedTeam Pentesting GmbH
jens.liebchen@redteam-pentesting.de
https://www.redteam-pentesting.de

22. DFN-Konferenz „Sicherheit in vernetzten Systemen“
24./25. Februar 2015, Hamburg

# RedTeam Pentesting, Daten & Fakten

- ★ Gegründet 2004
- ★ 10 Penetrationstester
- ★ Weltweite Durchführung von Penetrationstests
- ★ Spezialisierung ausschließlich auf Penetrationstests

# Wir stellen ein!



RedTeam Pentesting
Seeing your network from the attacker's perspective

Seit der Gründung 2004 hat RedTeam Pentesting zahlreiche nationale wie internationale Unternehmen als Dienstleister mit Penetrationstests unterstützt und sich so zu einem weltweit sehr gefragten Anbieter für Penetrationstests entwickelt. Durch die ausschließliche Spezialisierung auf Penetrationstests bieten wir ein technisch sehr hohes Niveau sowie eine objektive Beratung unserer Kunden. Zur Verstärkung unseres Teams suchen wir zum nächstmöglichen Zeitpunkt einen

## Trainee zum Penetrationstester (m/w)

**an unserem Standort in Aachen**

### Ihre Herausforderung

Sie stehen kurz vor Ende Ihres Studiums und haben das Ziel, anschließend als Penetrationstester zu arbeiten. Im Rahmen unserer Traineestelle haben Sie bereits vor Abschluss Ihres Studiums die Möglichkeit, uns von Ihren Fähigkeiten zu überzeugen und sich umfassend auf die spätere Arbeit als Penetrationstester vorzubereiten. In spannenden und abwechslungsreichen Projekten für unsere Kunden weltweit unterstützen Sie ein Team erfahrener Penetrationstester. Ihre Arbeitszeiten werden hierbei nach Absprache an die Bedürfnisse Ihres Studiums angepasst.

### Sie bringen mit

- Kenntnisse der offensiven IT-Sicherheit (z.B. Penetrationstests, Exploitentwicklung, CTFs)
- Analytisches Denkvermögen und hohe Lernmotivation
- Interesse an Umgang und Kommunikation mit Kunden
- Sehr gutes Deutsch und gutes Englisch in Wort und Schrift
- Bereitschaft zu Reisen im In- und Ausland

### Wir bieten Ihnen

- Vorbereitung auf die spätere Tätigkeit als Penetrationstester in Vollzeit
- Flexible Arbeitszeiten im Umfang von min. 19,5 Std./Woche
- Abwechslungsreiche Tätigkeit
- Arbeit in erfahrenen Teams
- Angenehme Arbeitsatmosphäre und moderne Arbeitsplätze
- Einblick in unterschiedlichste Technologien und Unternehmen
- Möglichkeiten zu Veröffentlichungen und Konferenzteilnahmen

### Weitere Informationen

Hinweise zu Ihrer Bewerbung finden Sie unter: http://www.redteam-pentesting.de/jobs

Ihre aussagekräftige Bewerbung richten Sie bitte an: RedTeam Pentesting GmbH, Personalabteilung, Dennewartstr. 25-27, 52068 Aachen, Tel.: +49 241 510081-0, Fax: -99, jobs@redteam-pentesting.de

RedTeam Pentesting - Seeing your network from the attacker's perspective

RedTeam Pentesting
Seeing your network from the attacker's perspective

Seit der Gründung 2004 hat RedTeam Pentesting zahlreiche nationale wie internationale Unternehmen als Dienstleister mit Penetrationstests unterstützt und sich so zu einem weltweit sehr gefragten Anbieter für Penetrationstests entwickelt. Durch die ausschließliche Spezialisierung auf Penetrationstests bieten wir ein technisch sehr hohes Niveau sowie eine objektive Beratung unserer Kunden. Zur Verstärkung unseres Teams suchen wir zum nächstmöglichen Zeitpunkt einen

## Penetrationstester Vollzeit (m/w)

**an unserem Standort in Aachen**

### Ihre Herausforderung

In spannenden und abwechslungsreichen Projekten für unsere Kunden weltweit decken Sie in einem Team erfahrener Penetrationstester Sicherheitslücken in klassischen IT-Systemen und neuen Technologien auf. Kreative und unkonventionelle Herangehensweisen sind Teil Ihrer Arbeit. Sie präsentieren die Ergebnisse unseren Auftraggebern und beraten technische Ansprechpartner sowie wichtige Entscheidungsträger und leisten so einen nachhaltigen Beitrag zur Absicherung der Systeme unserer Kunden.

### Sie bringen mit

- Erfahrung mit offensiver IT-Sicherheit (z.B. Penetrationstests, Exploitentwicklung, CTFs)
- Analytisches Denkvermögen und hohe Lernmotivation
- Sicherer Umgang und Kommunikation mit Kunden
- Sehr gutes Deutsch und gutes Englisch in Wort und Schrift
- Bereitschaft zu Reisen im In- und Ausland
- Idealerweise Hochschulabschluss oder vergleichbare Ausbildung

### Wir bieten Ihnen

- Abwechslungsreiche Tätigkeit
- Umfangreiche Vorbereitung auf Ihre neue Aufgabe
- Arbeit in erfahrenen Teams
- Aktive Einflussnahme auf Entscheidungsprozesse
- Kontinuierliche Weiterbildung
- Angenehme Arbeitsatmosphäre und moderne Arbeitsplätze
- Einblick in unterschiedlichste Technologien und Unternehmen
- Möglichkeiten zu Veröffentlichungen und Konferenzteilnahmen

### Weitere Informationen

Hinweise zu Ihrer Bewerbung finden Sie unter: http://www.redteam-pentesting.de/jobs

Ihre aussagekräftige Bewerbung richten Sie bitte an: RedTeam Pentesting GmbH, Personalabteilung, Dennewartstr. 25-27, 52068 Aachen, Tel.: +49 241 510081-0, Fax: -99, jobs@redteam-pentesting.de

RedTeam Pentesting - Seeing your network from the attacker's perspective

⇒ `https://www.redteam-pentesting.de/jobs`

# Was ist ein Penetrationstest?

- ★ Angriff auf Netzwerk oder Produkt im Auftrag des Eigentümers
- ★ Ziel: Praxisrelevante Schwachstellen aufdecken
- ★ Kein Audit/Checkliste!

# Probleme bei der Auswahl eines Anbieters

- ★ Beim ersten Test mit einem neuen Anbieter kaufen Sie die berühmte „Katze im Sack“
- ★ Die Dienstleistung Pentest als auch die Anbieter sind nur schlecht vergleichbar!
- ★ Selbst nach Vorauswahl: Kostenunterschiede teilweise um Faktor 10 und mehr
- ★ $\Rightarrow$ ob ein guter Anbieter ausgewählt wurde, sehen Sie erst nach dem Pentest

# Probleme bei der Auswahl eines Anbieters

# Probleme bei der Auswahl eines Anbieters

Auswahl des falschen Dienstleisters:

- ★ Im besten Fall: Viel Geld für schwache Ergebnisse ausgegeben
- ★ Im schlechtesten Fall: Sicherheitsvorfälle oder Risiken werden erst durch den Penetrationstest verursacht

# Einige Hilfestellungen

- ★ Im Folgenden: Verschiedene (nicht-wörtliche) Zitate aus den letzten 10 Jahren
- ★ Quelle: Verschiedene Personen berichten über ihre Erfahrungen mit Penetrationstests
- ★ Ziel: Indizien identifizieren, die vor oder während des Pentests erkennbar sind und darauf hindeuten, dass ein Pentest eventuell nicht den eigenen Erwartungen entspricht

# Einige Hilfestellungen

- ★ Im Folgenden: Verschiedene (nicht-wörtliche) Zitate aus den letzten 10 Jahren
- ★ Quelle: Verschiedene Personen berichten über ihre Erfahrungen mit Penetrationstests
- ★ Ziel: Indizien identifizieren, die vor oder während des Pentests erkennbar sind und darauf hindeuten, dass ein Pentest eventuell nicht den eigenen Erwartungen entspricht

## Disclaimer

Wir bieten Penetrationstests an. Die Erfahrungen unserer Kunden mit anderen Dienstleistern sind nicht repräsentativ.

# Vor dem Pentest/Bei der Beauftragung

## Kunde zitiert aus einem Angebot

„Da können Sie jetzt zwischen dem Silber-, Gold- oder Platin-Paket wählen. . . “

# Vor dem Pentest/Bei der Beauftragung

## Kunde zitiert aus einem Angebot

„Da können Sie jetzt zwischen dem Silber-, Gold- oder Platin-Paket wählen. . . “

- ★ Anbieter erfragte telefonisch lediglich die Anzahl der IP-Adressen
- ★ Anschließend wurden drei Angebote präsentiert, die sich eigentlich nur in den aufgeführten Werkzeugen und der Tagesanzahl unterschieden haben

# Vor dem Pentest/Bei der Beauftragung

- ★ Pentest ohne Detailkenntnisse (technische genauso wie Businessmodel) und ohne Beratung
- ★ Gefahr Fire-and-Forget-Angebot: Standardangebot (mit wenig Aufwand) und erst Gedanken machen, wenn der Kunde das Angebot annehmen will
- ★ Pauschalangebot vs. individuelle Dienstleistung

# Vor dem Pentest/Bei der Beauftragung

## Aus einer Stellenausschreibung eines Pentestdienstleisters

„Suche Studenten zur selbständigen Durchführung von Penetrationstests in Heimarbeit“

# Vor dem Pentest/Bei der Beauftragung

## Aus einer Stellenausschreibung eines Pentestdienstleisters

„Suche Studenten zur selbständigen Durchführung von Penetrationstests in Heimarbeit“

- ★ Schwierig abschließend zu beurteilen
- ★ Penetrationstests als „Fließbandarbeit“?

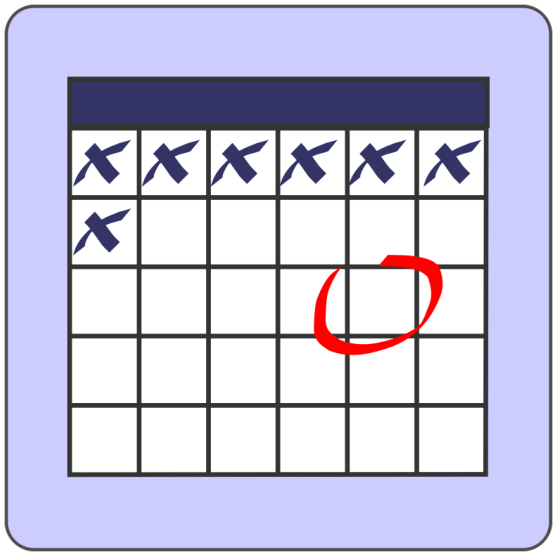
# Vor dem Pentest/Bei der Beauftragung

- ★ Ohne sehr große Erfahrung unwahrscheinlich, dass jemand in kurzer Zeit eingearbeitet werden kann um kreativ auch individuelle Schwachstellen aufzudecken
- ★ Vermutlich Penetrationstests nach Ablaufplan
- ★ Wer führt überhaupt den Pentest durch?
- ★ Heimarbeitsplätze: Datensicherheit und Vertraulichkeit?

# Vor dem Pentest/Bei der Beauftragung

## Kunde erläutert, warum er einen neuen Dienstleister benötigte:

„Zwei Wochen vor dem beauftragten Beginn des Penetrationstests hatte der Pentestdienstleister auf einmal keine Zeit mehr.“



# Vor dem Pentest/Bei der Beauftragung

## Kunde erläutert, warum er einen neuen Dienstleister benötigte:

„Zwei Wochen vor dem beauftragten Beginn des Penetrationstests hatte der Pentestdienstleister auf einmal keine Zeit mehr.“

- ★ Penetrationstest wurde kurzfristig vom Dienstleister abgesagt
- ★ Begründung: Kapazitätsengpässe
- ★ Kunde muss zwei Wochen vor Beginn neu evaluieren und anderen Dienstleister finden
- ★ Insgesamt ca. 3 Monate Projektverzögerung

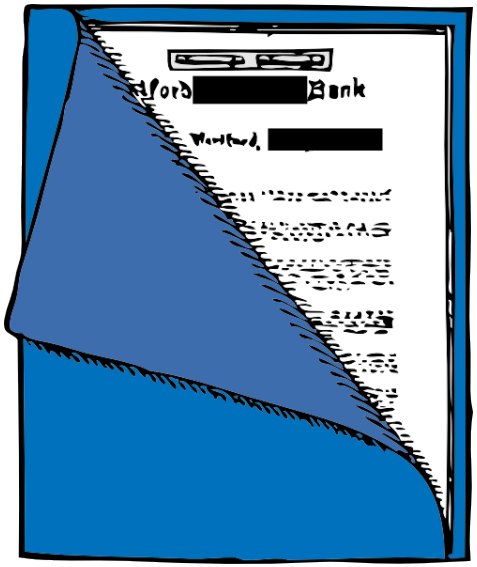
# Vor dem Pentest/Bei der Beauftragung

- ★ Verbindliche Verträge für beide Seiten!
- ★ Lieber einen Dienstleister, der Kapazitäten deutlich kommunziert, als ein Dienstleister, der kurz vor Testbeginn „bemerkt“, dass er keine Kapazitäten hat
- ★ Nicht auf unklare Rücktrittsmöglichkeiten/Erfüllungszeiten im Vertrag einlassen

# Vor dem Pentest/Bei der Beauftragung

## Kunde mit Beispielbericht eines Anbieters

„Diesen Beispielbericht hab ich damals bekommen. . . “



# Vor dem Pentest/Bei der Beauftragung

## Kunde mit Beispielbericht eines Anbieters

„Diesen Beispielbericht hab ich damals bekommen. . . “

- ★ Beispielbericht war geschwärzter echter Bericht
- ★ Schwärzung war unvollständig
- ★ Nach ca. 5 Minuten lesen war klar, dass es sich um eine spezielle NGO handelte, die hier getestet wurde
- ★ Test lag vermutlich ca. 6 Monate zurück, unklar ob Schwachstellen schon alle korrigiert wurden

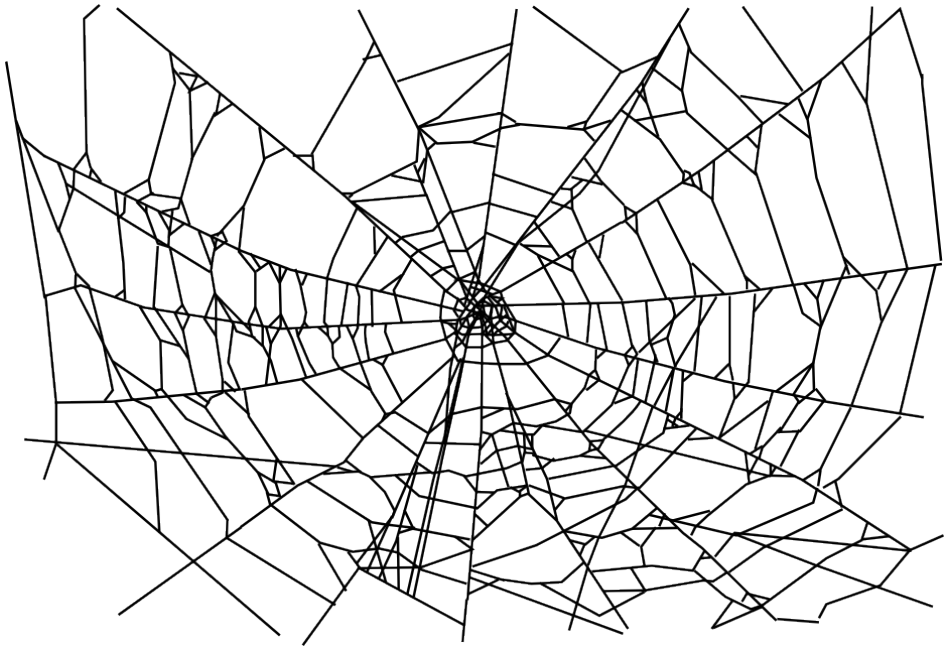
# Vor dem Pentest/Bei der Beauftragung

- ★ Wirft extrem schlechtes Licht auf den Anbieter (Worst-Case: Herausgabe eines fremden Testberichts)
- ★ Lassen Sie sich nicht auf Anbieter ein, bei denen Sie bezüglich der Vertraulichkeit ein schlechtes Gefühl haben!

# Während des Penetrationstests

## Kunde:

„. . . und dann konnten wir keinen mehr erreichen.“



# Während des Penetrationstests

**Kunde:**

„. . . und dann konnten wir keinen mehr erreichen.“

- ★ Laufender Penetrationstest störte das interne Netzwerk
- ★ Penetrationstester waren über mehrere Stunden nicht erreichbar
- ★ Es stellte sich anschließend heraus, dass ein Freelancer von zu Hause aus den Test mit automatisierten Tools durchführte

# Während des Penetrationstests

- ★ Kommunikation(-smöglichkeit) ist für Pentests essentiell
- ★ Vereinbaren Sie Telefonnummern auch für den Notfall
- ★ Schlechte Idee: Penetrationstests der VoIP-Infrastruktur und Kontaktpersonen sind nur per VoIP erreichbar

# Während des Penetrationstests

## Penetrationstester

„Ich arbeite jetzt seit mehreren Jahren als Penetrationstester und brauchte zum Glück noch nie mit Kunden zu sprechen. . . “

# Während des Penetrationstests

## Penetrationstester

„Ich arbeite jetzt seit mehreren Jahren als Penetrationstester und brauchte zum Glück noch nie mit Kunden zu sprechen. . . “

- ★ Penetrationstester arbeitet bei größerem Unternehmen
- ★ Keinerlei direkte Rücksprache während des Pentests?
- ★ Alle Informationen laufen über mehrere Personen
- ★ Auch die Ergebnisse der Tests werden von Leuten vorgestellt, die selber nichts mit dem Test zu tun hatten

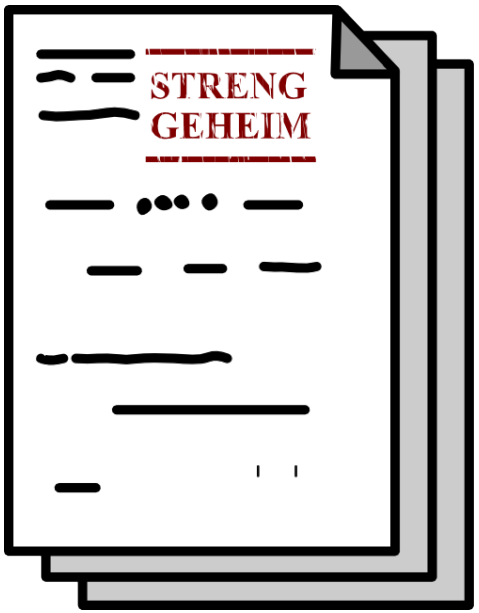
# Während des Penetrationstests

- ★ Unklar, wie ein solches Konzept überhaupt effizient funktioniert
- ★ Rückfragen langwierig
- ★ Ergebnisspräsentation ohne tiefgehende Kenntnisse ist schwierig
- ★ Abschlussbesprechungen finden entweder nicht statt oder haben nur deutlich geringeren Wert

# Während des Penetrationstests

## Penetrationstester

„Wie kommt das denn da hin?“



# Während des Penetrationstests

## Penetrationstester

„Wie kommt das denn da hin?“

- ★ Unsere Penetrationstester entdecken auf wichtigem System eine Datei mit anscheinend ausgelesenen Passwort-Hashes und teilweise auch direkt den zugehörigen Passwörtern
- ★ Verdacht: Kunde wurde in der Vergangenheit bereits unbemerkt erfolgreich angegriffen
- ★ Produktionsstillstand von ca. 4 Stunden für die Analyse

# Während des Penetrationstests

- ★ Fazit: Daten stammten aus vorangegangenem Test (nicht mit uns)
- ★ Tester ließen Daten offen liegen
- ★ Vereinfacht weitere Angriffe enorm ⇒ Kunde war nach dem ersten Test unsicherer als vorher

# Nach dem Penetrationstest

## Kunde beim Betrachten des Abschlussberichts

„Aber wir betreiben doch gar keinen FTP-Server?“

# Nach dem Penetrationstest

## Kunde beim Betrachten des Abschlussberichts

„Aber wir betreiben doch gar keinen FTP-Server?“

- ★ Pentest wurde aus Kostengründen nach Indien outgesourced
- ★ Zahlendreher im IP-Netzwerk blieb bis zum Schluss unbemerkt
- ★ Es wurde ein anderes (branchenfremdes) Unternehmen ohne Einwilligung getestet

# Nach dem Penetrationstest

- ★ Sprachschwierigkeiten verhinderten, dass Tester den offensichtlichen Fehler bemerkten
- ★ Saubere (schriftliche) Dokumentation und mehrfache Prüfung der Zieladressen kann helfen
- ★ Bei sehr günstigen Anbietern liegt der Verdacht nah, dass an vielen Stellen gespart werden muss (unter anderem zum Beispiel an der Vorbereitung des Tests)

# Nach dem Penetrationstest

## Kunde berichtet von den Ergebnissen des letzten Penetrationstests

„. . . und dann kam der Bericht unverschlüsselt per E-Mail.“

# Nach dem Penetrationstest

## Kunde berichtet von den Ergebnissen des letzten Penetrationstests

„. . . und dann kam der Bericht unverschlüsselt per E-Mail.“

- ★ Penetrationstests durchgeführt von einer großen Unternehmensberatung
- ★ Nach Abschluss der Testzeit erhielt der Kunde ohne Absprache den Bericht per E-Mail
- ★ E-Mail wie auch Bericht wurden unverschlüsselt übertragen

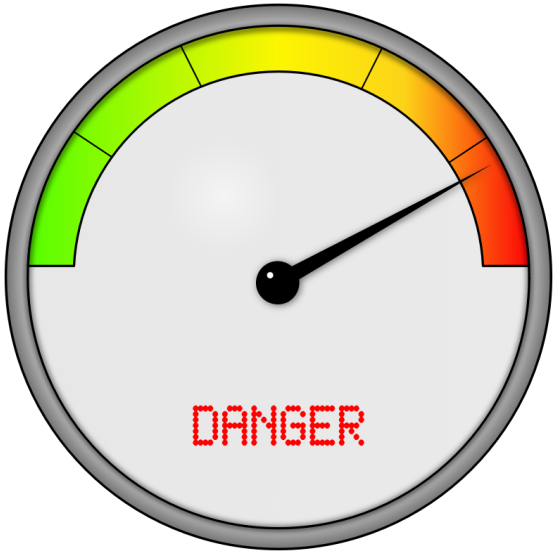
# Nach dem Penetrationstest

- ★ Bericht enthielt noch nicht korrigierte Schwachstellen
- ★ Unverschlüsselte Übertragung gefährdete Auftraggeber zusätzlich
- ★ Wenn selbst der Bericht schon unverschlüsselt übertragen wird, wie geht der Dienstleister ansonsten mit den vertraulichen Daten um?
- ★ $\Rightarrow$ Vorfall hat sehr ungutes Gefühl beim Kunden hinterlassen

# Nach dem Penetrationstest

## Kunde berichtet von den Ergebnissen des letzten Penetrationstests

„Der Bericht enthielt 18 Schwachstellen, 14 davon waren angeblich unsichere weil selbstsignierte Zertifikate.“



# Nach dem Penetrationstest

## Kunde berichtet von den Ergebnissen des letzten Penetrationstests

„Der Bericht enthielt 18 Schwachstellen, 14 davon waren angeblich unsichere weil selbstsignierte Zertifikate.“

- ★ Es wurde 14mal eine angebliche Schwachstelle für verschiedene IP-Adressen mit den gleichen Textbausteinen bemängelt
- ★ Genauere Informationen insbesondere zur Gefährdung durch die Schwachstelle enthielt der Bericht nicht
- ★ Aussage: Selbstsigniertes Zertifikat ist immer unsicher

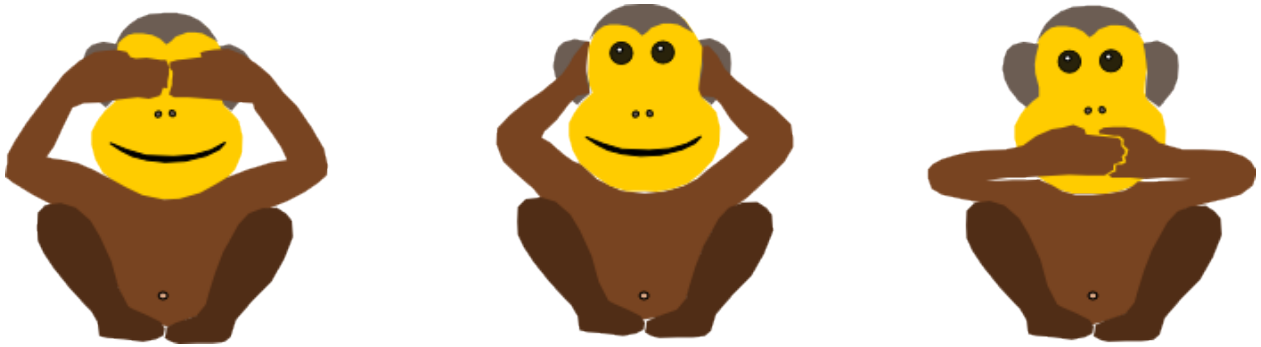
# Nach dem Penetrationstest

- ★ Kunde analysiert und stellt fest: Keine 14 Zertifikate, sondern 14 mal das gleiche Zertifikat
- ★ Nicht genutzte IP-Adressen, werden auf Standard-Host weitergeleitet
- ★ Die Webseite dahinter zeigt lediglich eine (gewollte) Fehlermeldung an
- ★ Überhaupt keine Schwachstelle, trotzdem ca. 2/3 des Berichtumfangs
- ★ Gutes Beispiel für Penetrationstest ohne Interpretation der Ergebnisse

# Nach dem Penetrationstest

## Kunde mit Fragen zum Bericht

„Für Nachfragen hierzu habe ich nie mehr jemanden erreicht.“



# Nach dem Penetrationstest

## Kunde mit Fragen zum Bericht

„Für Nachfragen hierzu habe ich nie mehr jemanden erreicht.“

- ★ Nach der Übergabe der Ergebnisse konnte der Kunde keinen kompetenten Ansprechpartner mehr erreichen
- ★ Selbst (für Penetrationstester) sehr einfache Fragen konnten nicht beantwortet werden

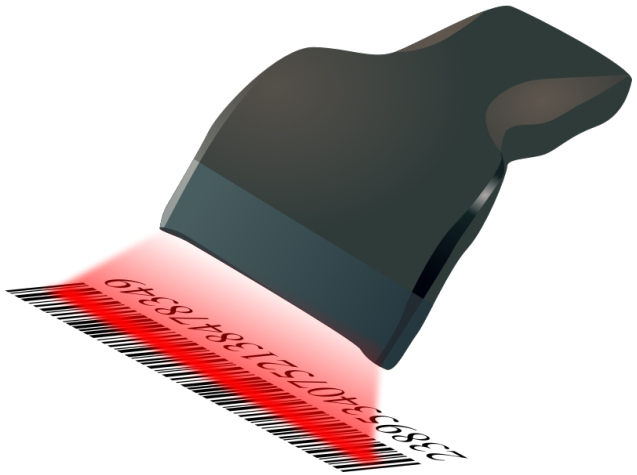
# Nach dem Penetrationstest

- ★ Es blieb das Gefühl, dass der Dienstleister sich zu seinen eigenen Aussagen nicht mehr äußern wollte
- ★ Es blieb unklar, warum
- ★ Erreichbar blieb lediglich der Account Manager, der aber offensichtlich den Bericht der eigenen Pentester nicht deuten konnte

# Nach dem Penetrationstest

## Überraschende Testverläufe

„Nessus kann ich auch selber.“



# Nach dem Penetrationstest

## Überraschende Testverläufe

„Nessus kann ich auch selber.“

- ★ Statt Penetrationstest lediglich Schwachstellen-Scan durchgeführt
- ★ In einem Fall: Rechnung enthielt sogar eine Lizenz für den Schwachstellenscanner

# Nach dem Penetrationstest

- ★ Es existieren Anbieter, die (anscheinend erfolgreich) Schwachstellen-Scans für einen fünfstelligen Betrag verkaufen
- ★ Vorher abklären, dass Vorstellungen bezüglich des Penetrationstests deckungsgleich sind
- ★ Kompetenz des Dienstleisters klären, leider aber schwierig im Vertrag fixierbar
- ★ Gute Penetrationstester kennen das Problem und helfen sicherlich weiter

# Fazit

- ★ Wie überall anders auch: Dienstleister unterscheiden sich deutlich
- ★ Über schlechte Erfahrungen mit Penetrationstests und Dienstleistern wird allerdings häufig geschwiegen
- ★ Eine schlechte Auswahl des Dienstleisters birgt Gefahren

# Fazit

- ★ Wie überall anders auch: Dienstleister unterscheiden sich deutlich
- ★ Über schlechte Erfahrungen mit Penetrationstests und Dienstleistern wird allerdings häufig geschwiegen
- ★ Eine schlechte Auswahl des Dienstleisters birgt Gefahren

⇒ Wie also den richtigen Partner finden und auswählen?

# Tipps zur Dienstleisterauswahl

- Sprechen Sie mit möglichen Kandidaten
- Stellen Sie Fragen:
  - Wie läuft der Test ab?
  - Was wären typische Schwachstellen?
  - Wo sitzen die Mitarbeiter, die den Test durchführen?
  - Wie können wir mit ihnen während des Tests kommunizieren?
  - ...
- Lassen Sie sich nicht von Firmennamen blenden, der Bekanntheitsgrad einer Firma sagt nichts über die Qualität aus
- Hören Sie auf Ihr Bauchgefühl

# Tipps zur Dienstleisterauswahl (Datenschutz)

- ★ Sprechen Sie über Datenschutz und Vertraulichkeit
- ★ Wo werden Daten gespeichert, wer hat Zugriff, gibt es Richtlinien bezüglich der Löschung etc.
- ★ $\Rightarrow$ Klassische Datenschutzthemen
- ★ ADV-Vereinbarungen passen allerdings i.A. nicht auf Penetrationstests (Weisungsbefugnis ist problematisch)
- ★ Ein guter Dienstleister berät Sie gerne und hat Lösungen auch für schwierige Situationen

# Tipps zur Dienstleisterauswahl (Ausschreibungen)

- ★ Vorsicht mit Ausschreibungen
- ★ Anhand von klassischen Kriterien lassen sich Penetrationstests nicht vergleichen
- ★ Falls möglich, versuchen Sie vor einer Ausschreibung mit mehreren Anbietern zu sprechen, um sich auch explizit beraten zu lassen, was sinnvoll im Test untergebracht werden sollte
- ★ Versuchen Sie Pflichtkriterien so zu gestalten, dass Sie keine Dienstleister ungewollt ausschließen
- ★ Versuchen Sie zu vermeiden, dass Sie Standardangebote bewerten müssen

# Dienstleisterauswahl aus Anbietersicht

- ★ Gute Anbieter lassen sich Ihr Geschäftsmodell erklären!
- ★ Sie werden Ihre Vorstellungen bzgl. des Pentests mit den Möglichkeiten in der Praxis übereinbringen oder Ihnen erklären, warum manche Vorstellungen so nicht sinnvoll umsetzbar sind
- ★ Ein erster Pentests muss und sollte nicht *alles* abdecken
- ★ Ein gute Anbieter arbeitet transparent, dies lässt sich leicht erfragen

# Dienstleisterauswahl aus Anbietersicht

## Last but not least:

Lassen Sie Penetrationstests durchführen! Bei guten Anbietern gilt: Die Erkenntnisse schlagen die zusätzlichen Risiken deutlich!

# Zeit für Ihre Fragen!

Vielen Dank für Ihre Aufmerksamkeit.