T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting

Frankfurt a.M., 10. - 11.11.2016

Penetrationstests Aussagekraft und Grenzen

Patrick Sauer

binsec GmbH

Agenda

- Vorstellung
- Penetrationstests: Die Sicht des Kunden
- Penetrationstests: Die Realität

Agenda

- Vorstellung
- Penetrationstests: Die Sicht des Kunden
- Penetrationstests: Die Realität

Vorstellung
Patrick Sauer

Patrick Sauer

- Seit 2013 Geschäftsführer der binsec GmbH
- Qualifikationen
  - M.Sc. Security Management
  - Diplom Wirtschaftsinformatiker (FH)
  - Zertifikate: CISSP, CISM, OSCP, CPSSE, TISP, DSB-TÜV
  - Dozent der TH Brandenburg und Hochschule Darmstadt

Vorstellung
binsec GmbH

binsec GmbH

- Security Consulting
- Penetration Testing
- Business Security Checkup
- Security Training

E-Mail: info@binsec.com

Telefon: +49 69 2475607 0

Webseite: www.binsec.com

Agenda

- Vorstellung
- Penetrationstests: Die Sicht des Kunden
- Penetrationstests: Die Realität

Penetrationstests:
Die Sicht des Kunden

Handzeichen: Wer hat schon Pentests in Auftrag gegeben?

Penetrationstests:
Die Sicht des Kunden

Handzeichen: Wer davon hat sich "sicherer gefühlt"?

Penetrationstests:
Die Sicht des Kunden

Potentieller Kunde fragt:

"Bekommen wir eine Garantie,

dass wir nach einem Pentest sicher sind?"

Penetrationstests:
Die Sicht des Kunden

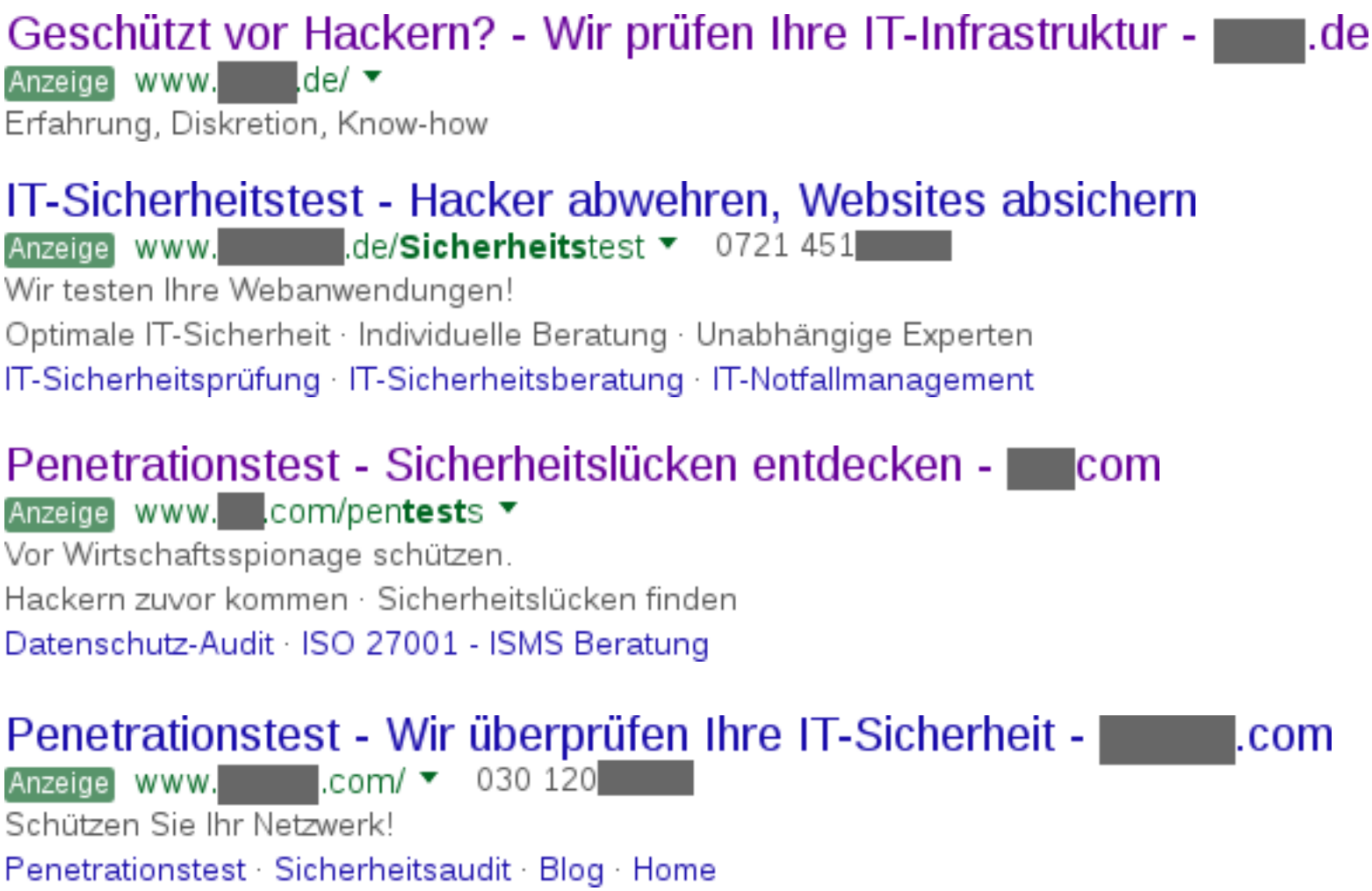
Potentieller Kunde fragt:

"Bekommen wir eine Garantie,

dass wir nach einem Pentest sicher sind?"

Publikumsfrage: Was ist die richtige Antwort?

Penetrationstests:
Die Sicht des Kunden



Geschützt vor Hackern? - Wir prüfen Ihre IT-Infrastruktur - [redacted].de
Anzeige www.[redacted].de/
Erfahrung, Diskretion, Know-how

IT-Sicherheitstest - Hacker abwehren, Websites absichern
Anzeige www.[redacted].de/**Sicherheits**test 0721 451[redacted]
Wir testen Ihre Webanwendungen!
Optimale IT-Sicherheit · Individuelle Beratung · Unabhängige Experten
IT-Sicherheitsprüfung · IT-Sicherheitsberatung · IT-Notfallmanagement

Penetrationstest - Sicherheitslücken entdecken - [redacted]com
Anzeige www.[redacted].com/pen**test**s
Vor Wirtschaftsspionage schützen.
Hackern zuvor kommen · Sicherheitslücken finden
Datenschutz-Audit · ISO 27001 - ISMS Beratung

Penetrationstest - Wir überprüfen Ihre IT-Sicherheit - [redacted].com
Anzeige www.[redacted].com/ 030 120[redacted]
Schützen Sie Ihr Netzwerk!
Penetrationstest · Sicherheitsaudit · Blog · Home

Penetrationstests:
Die Sicht des Kunden

Publikumsfrage: Welche Erwartungen haben Kunden?

Penetrationstests:
Die Sicht des Kunden

Die (oftmals) subtile Erwartung:

Wir zahlen ein paar Tausend Euro,

und Sie finden dafür alle Schwachstellen.

Wir beheben alle und sind dann sicher!

Penetrationstests:
Die Sicht des Kunden

Die optimale Erwartung wäre:

Wir zahlen ein paar Tausend Euro und dafür

werden bekannte Schwachstellen identifiziert, indem

Tools & Techniken eines typischen Angreifers benutzt werden.

Penetrationstests:
Die Sicht des Kunden

Die optimale Erwartung wäre:

Wir zahlen ein paar Tausend Euro und dafür

werden bekannte Schwachstellen identifiziert, indem

Tools & Techniken eines typischen Angreifers benutzt werden.

Publikumsfrage: Was wird ein Kunde im Gegensatz zu seinen Erwartungen bekommen?

Agenda

- Vorstellung
- Penetrationstests: Die Sicht des Kunden
- Penetrationstests: Die Realität

Penetrationstests: Die Realität

Charakteristika professioneller Pentests:

- individuelle Projektgestaltung (Scoping!)
- standardisierte Vorgehensweise
- Tool-Set & Manuelle Tests
- hohes Know-How
- Qualitätssicherung
- detaillierter und verständlicher Bericht
- angemessenes Preis-/Leistungsverhältnis

Penetrationstests:
Die Sicht des Kunden

Publikumsfrage: Welche Aussagekraft haben Pentests?

Penetrationstests: Die Realität

Die Aussagekraft professioneller Pentests:

- keine low hanging fruits mehr
- keine Chancen mehr für Script Kiddies
- keine Chancen mehr für automatisierte Angriffe
- erfolgreicher Angriff nur mit viel mehr finanziellen und zeitlichen Aufwand möglich
- Aussage über das Sicherheitsniveau des Ziels

Penetrationstests:
Die Sicht des Kunden

Publikumsfrage: Welche Grenzen haben Pentests?

Penetrationstests: Die Realität

Die Grenzen professioneller Pentests:

- Zero Day Exploits
- Advanced Persistent Threats
- Gültig bis? Gestern, weil:
  - Veränderungen an den Zielsystemen
  - neue Angriffe
  - neue Schwachstellen

Penetrationstests: Die Realität

Fazit:

- Pentests machen keine IT-Systeme "100%" sicher
- Transparente Zielsetzung notwendig
- Pentests erhöhen das Sicherheitsniveau
  - Identifizierung von konkreten Schwachstellen
  - Identifizierung von strukturellen Sicherheitsproblemen
  - Abschätzen von internem Weiterbildungsbedarf
- Berichte mit "0" Findings sind extrem selten

Danke für Ihre Aufmerksamkeit

Fragen?