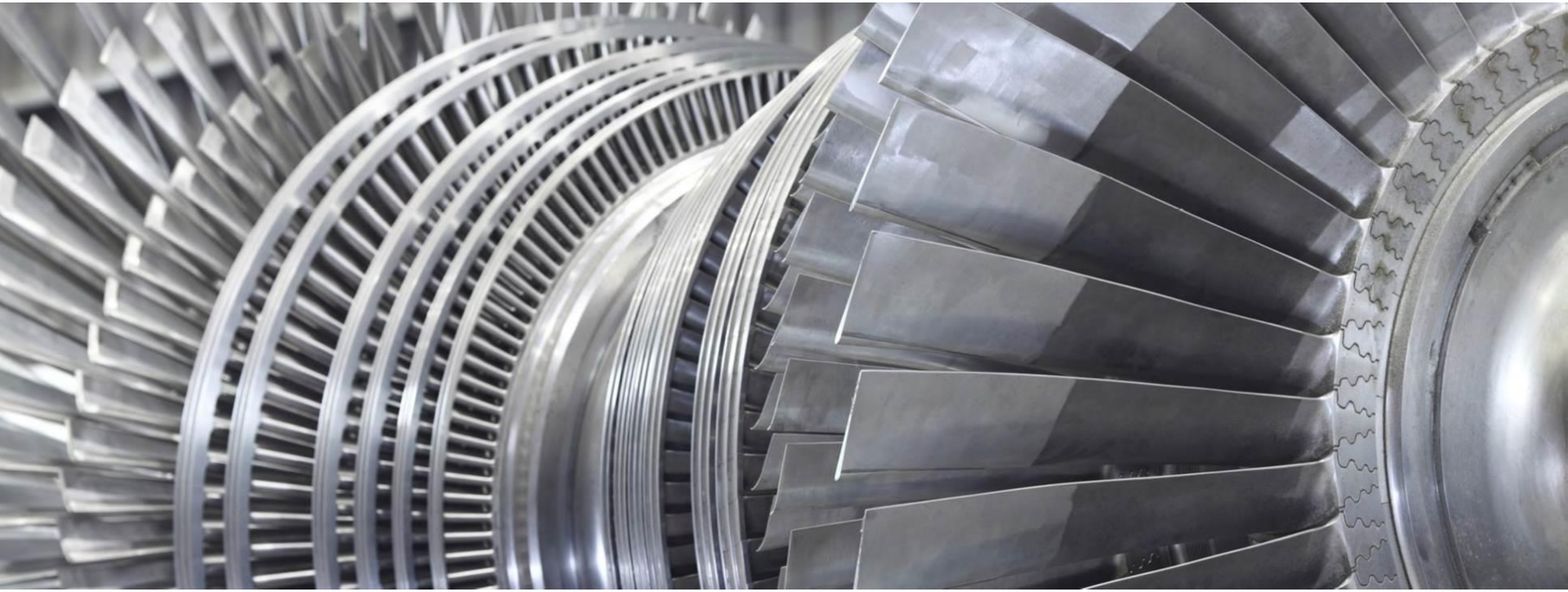
Baker McKenzie.

Penetration Testing bei Mitbewerbern
Zwischen Security Research und Industriespionage

RA Dr. Lukas Feiler, SSCP, CIPP/E

Security Forum 2017, 6. April 2017



Agenda

1 **Motivationslage für Penetration Tests**

Von „mal sehen …“ bis „hoffentlich finden wir was“

2 **Penetrationstests fremder IT-Systeme**

Rechtliche Risiken für das testende Unternehmen

Abwehrmaßnamen für „getestete“ Unternehmen

3 **Sicherheitstests bei fremder Software**

Blackbox Tests & Reverse Engineering

Rechtliche Risiken für das testende Unternehmen

1 Motivationslage für Penetration Tests

Warum wird getestet?

- Sicherheit zunehmend kaufentscheidend
- Unternehmensstrategische Maßnahmen vs. Einzelgängeraktionen
- Arten von Angreifern
  - Einzelne Mitarbeiter der Konkurrenz
  - Unmittelbare Konkurrenz am lokalen Markt
  - Ausländische Großkonzerne und Geheimdienste
- Unternehmensdaten als Ziel?
  - Als Nachweis für Sicherheitslücke oder zur weiteren Verwendung?

2 Penetrationstests fremder IT-Systeme

Rechtliche Grenzen beim Penetrationstest fremder IT-Systeme – 1 von 3

- Industriespionage (§§ 123 und 124 StGB)
  - Auskundschaften eines Geschäftsgeheimnisses mit dem Vorsatz es zu verwerten, einem anderen zur Verwertung zu überlassen oder der Öffentlichkeit preiszugeben
  - Was ist ein Geschäftsgeheimnis?
    - Tatsachen und Erkenntnisse kommerzieller oder technischer Art
    - nur begrenzten Zahl von Personen bekannt
    - wirtschaftliches Interesse an Geheimhaltung
    - Geheimhaltungswille erkennbar
    - ~~angemessen geschützt~~ (OGH 25.10.2016, 4 Ob 165/16t)
- Inlands- vs. Auslandsspionage

Rechtliche Grenzen beim Penetrationstest fremder IT-Systeme – 2 von 3

- Hacking (§ 118a StGB)
  - Zugangsverschaffung zu einem Computersystem (od. einem Teil davon), über das der Täter nicht oder nicht allein verfügen darf
  - indem spezifische Sicherheitsvorkehrungen im Computersystem überwunden werden
  - Sofern der Täter handelt mit
    - Spionageabsicht hinsichtlich personenbezogenen Daten oder
    - Schädigungsabsicht (durch Verwendung ausspionierter Daten oder durch Verwendung des Computersystems)
  - Strafdrohung: bis zu 6 Monate; bis zu 2 Jahre bei kritischer Infrastruktur; bis zu 2 Jahre im Falle einer kriminellen Vereinigung

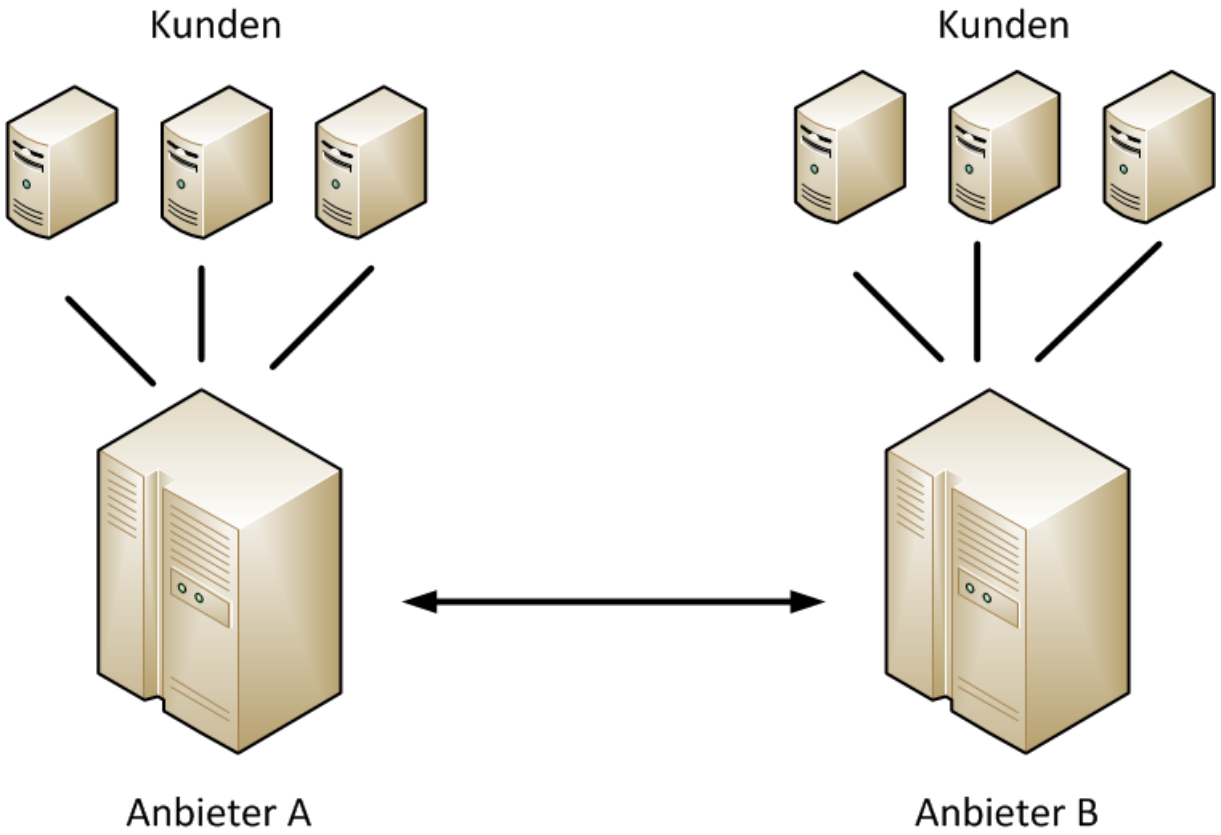
Rechtliche Grenzen beim Penetrationstest fremder IT-Systeme – 3 von 3

- Zivilrechtliche Grenzen: Besitzstörung (OGH 6 Ob 126/12)
  - Stellvertretende Ressortleiter der Tageszeitung „Österreich“ versuchte (erfolglos) Web-Mail-System der „Kronen Zeitung“ zu „hacken“
  - Kronen Zeitung konnte durch WHOIS-Datenbank IP-Adresse zu Konzernmutter der „Österreich“-Mediengruppe zurückverfolgen
  - Kronen Zeitung klagte Konzernmutter der „Österreich“ auf Unterlassung
  - OGH:
    - Hacking ist Besitzstörung
    - Konzernmutter zur Unterlassung verurteilt, da sie Gehilfin der Besitzstörung ist (ihre IP-Adresse)
  - Schadenersatz: bei wissentlich gefährlichen Mitarbeitern

Möglichkeiten der Täterausforschung

- Technische Möglichkeiten
  - WHOIS-Datenbank
  - Received-Header in E-Mails
- Anspruch auf Auskunft über Inhaberschaft einer IP-Adresse?
  - Nur behördlicher Auskunftsanspruch: Staatsanwalt hat das Recht, von einem Access-Provider Auskunft über Name & Anschrift zu erhalten (§ 76a StPO)
  - Um den Staatsanwalt einzuschalten:
    - Strafanzeige gegen Unbekannt einbringen
    - ggf Ermächtigung zur Strafverfolgung erteilen (zB § 118a StGB)
  - Nicht möglich, wenn nur sog. Privatanklagedelikt (zB § 123 StGB)

Case Study – Neugieriger Kinokassendienstleister



3 Sicherheitstests bei fremder Software

Rechtsrahmen für das Testen fremder Software

- Jedes Ausführen einer Software stellt eine Vervielfältigung dar → Nutzungsrecht?
  - Lizenzbedingungen des Herstellers
  - Bestimmungsgemäße Nutzung als freie Werknutzung (§ 40d UrhG)
    - Blackbox Tests?
  - Reverse Engineering als freie Werknutzung nur zur Herstellung von Interoperabilität (§ 40e UrhG)

Rechtsbehelfe bei Urheberrechtsverletzungen

- Verschuldensunabhängiger Anspruch des Rechtsinhabers auf:
  - Unterlassung (§ 81 UrhG)
  - Beseitigung (§ 82 UrhG)
  - Angemessenes Entgelt (§ 86 UrhG)
- Bei Verschulden: Schadenersatz (§87 UrhG)
  - Mindestens: Doppeltes angemessenes Entgelt
  - Plus darüber hinausgehender Schaden inkl. entgangenem Gewinn
- Haftung des Unternehmensinhabers
  - Angemessenes Entgelt – Auch ohne Kenntnis des Unternehmers, wenn im Betrieb des Unternehmens begangen

Baker McKenzie.

Baker McKenzie.

Dr. Lukas Feiler, SSCP, CIPP/E
Senior Associate

Baker & McKenzie
Diwok Hermann Petsche
Rechtsanwälte LLP & Co. KG

Schottenring 25
1010 Wien

T: +43 1 2 42 50 450
M: +43 664 6 06 46 450
lukas.feiler@bakermckenzie.com

www.bakermckenzie.com