Deutsche Stiftung für Recht und Informatik

Schutz der unternehmenseigenen IT-Infrastruktur durch Penetrationstests und Bewältigung rechtlicher Hürden

Florian Groothuis, Roman Schildbach
ByteLaw Rechtsanwälte, Frankfurt am Main

Herbstakademie 2025

Agenda

I. Einführung

II. Einordnung und Ablauf von Pentests

III. Zivil- und strafrechtliche Implikationen

IV. Datenschutzrechtliche Rahmenbedingungen

V. Fazit und Ausblick

I. Einführung

Schäden für deutsche Wirtschaft durch Cyberkriminalität 2024:

178,6 Milliarden Euro

Entspricht den Baukosten von über 200 Elbphilharmonien

Quelle:
Bitkom e.V., Studie Wirtschaftsschutz 2024

I. Einführung

Pentests als Bestandteil der IT-Sicherheitsstrategie

- Regelmäßige Überprüfung auf Schwachstellen durch Penetrationstests (Pentests)
- Teil der „Offensive Security“
- Ziel: Stärkung IT-Sicherheit

II. Einordnung und Ablauf von Pentests

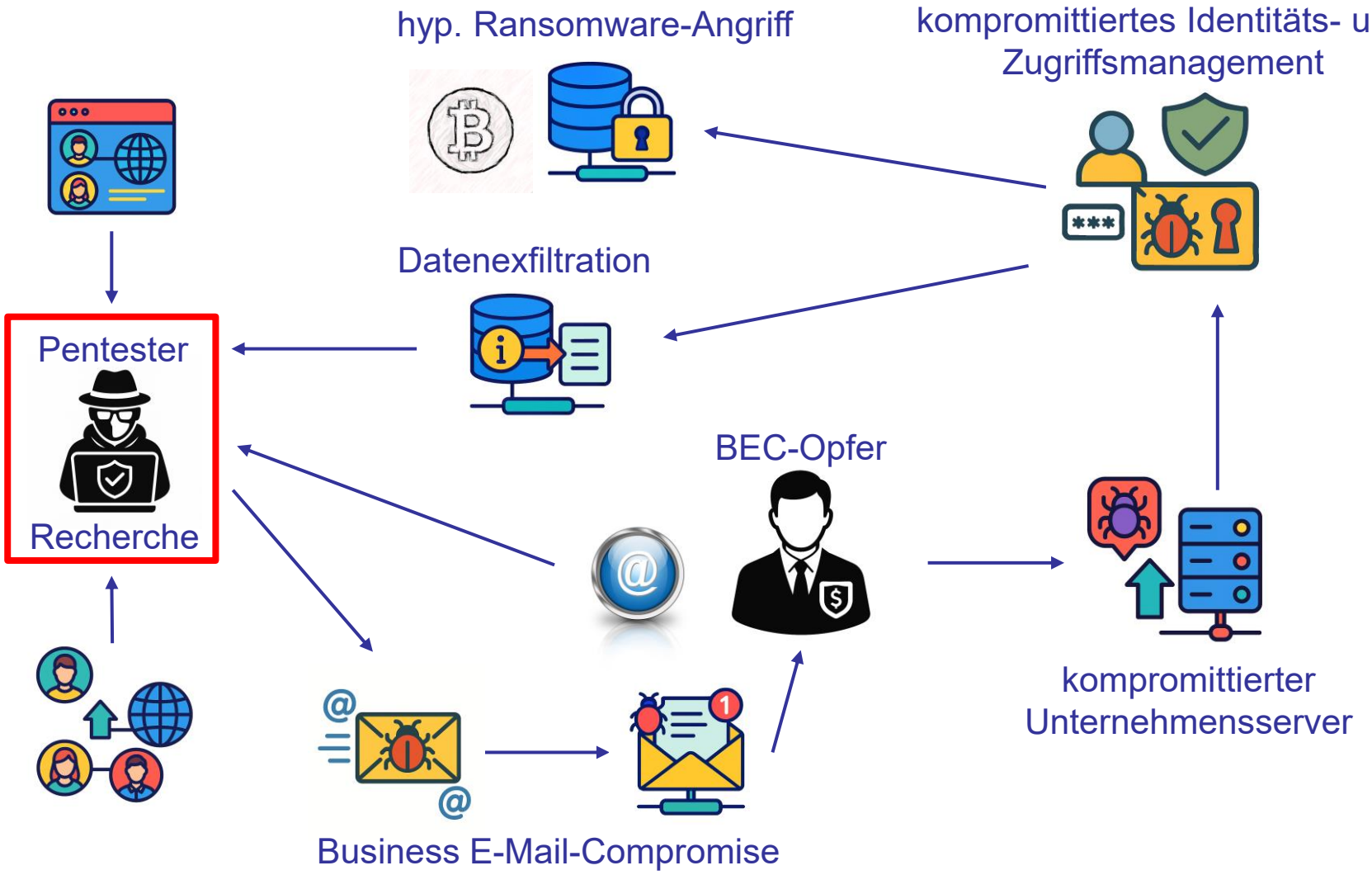
Mittelbare oder unmittelbare Pflicht zu Pentests

- Allgemeine Pflicht zu IT-Sicherheitsmaßnahmen (mittelbare Pflicht): Art. 32 DSGVO, Art. 21 NIS-2-Richtlinie
- Bereichsspezifische Pentestingpflichten (unmittelbare Pflicht): Bankensektor (DORA), Digitale Gesundheitsanwendungen (DiGAV)
- Behörden (ENISA, EDSA) empfehlen regelmäßige Pentests

Paradoxe Rechtslage

- Risiko unbeabsichtigter Rechtsverstöße trotz staatlicher Empfehlung (Strafrecht, Datenschutz)

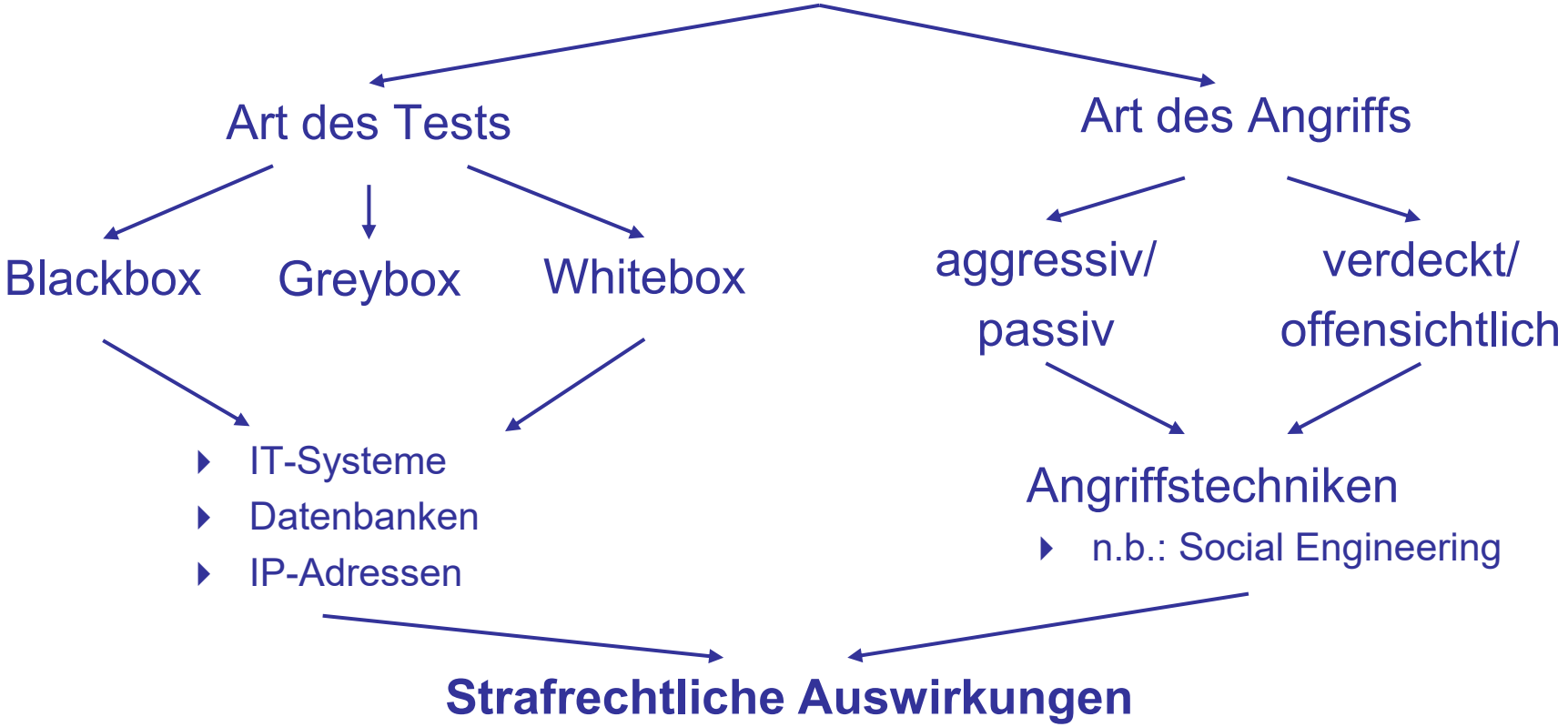
II. Einordnung und Ablauf von Pentests



III. Zivil- und strafrechtliche Implikationen

Vertragsgegenstand

Ermittlung und Analyse von Schwachstellen in IT-Systemen



III. Zivil- und strafrechtliche Implikationen

Strafbarkeitsrisiken u.a. nach § 202a StGB - Ausspähen von Daten

- Unbefugtes Verschaffen von Zugang
- zu besonders gesicherten,
- nicht für den Angreifer bestimmten Daten.

III. Zivil- und strafrechtliche Implikationen

Mitigierende Maßnahmen

- Tatbestandsausschluss durch Einverständnis
  - Erlaubnis des Pentesters zum Ausnutzen von Sicherheitslücken
  - Verfügungsbefugnis des Auftraggebers begrenzt die Einverständniserklärung
  - Restrisiko bei privaten Daten von Mitarbeitern: „OneDrive-Wildwuchs“

III. Zivil- und strafrechtliche Implikationen

Nicht umgesetzte Reform des Computerstrafrechts:

- „*Wer IT-Sicherheitslücken schließt, hat Anerkennung verdient – nicht Post vom Staatsanwalt*“,
  Marco Buschmann – Justizminister a.D.

- § 202a Abs. 3 StGB-E: Strafbarkeitsausschluss durch Befugnisfiktion
  - Feststellungsabsicht
  - Unterrichtungsabsicht
  - Erforderlichkeit

- Aktuell: Stillstand im Gesetzgebungsverfahren

IV. Datenschutzrechtliche Rahmenbedingungen

Verantwortlichkeit / Auftragsverarbeitung bei externen Pentestern:

- Auftraggeber ist Verantwortlicher (Entscheidung über Zwecke und Mittel – zur Sicherstellung der IT-Sicherheit mittels eines Pentests)
- Pentester ist i.d.R. Auftragsverarbeiter (wenn im Auftrag / weisungsgebunden / ohne Entscheidungskompetenz über Zwecke und Mittel)
- **Konsequenz**:
  - Auftragsverarbeitungsvertrag zu schließen
  - Keine eigene Rechtsgrundlage des Pentesters nötig

IV. Datenschutzrechtliche Rahmenbedingungen

Rechtmäßigkeit der Datenverarbeitung:

- Wenig geeignet:
  Einwilligung, Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO

- Denkbar:
  Interessenabwägung, Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO

- Überzeugend:
  Rechtliche Pflicht, Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO
  - Teilweise unmittelbare Pflicht zu Pentesting (DORA etc.)
  - Auch die implizite Pflicht aus Art. 32 DSGVO muss genügen; Argument: Einheit der Rechtsordnung; wenn Gesetzgeber Sicherheit personenbezogener Datenverarbeitungen vorschreibt, muss er auch dazu erforderliche Verarbeitungen erlauben

IV. Datenschutzrechtliche Rahmenbedingungen

Umgang mit besonderen Datenkategorien:

- „Erhebliches öffentliches Interesse“ i.S.v. Art. 9 Abs. 2 lit. g DSGVO?
- **Rechtsunsicherheit**:
  IT-Sicherheit eines Unternehmens von erheblichem öffentlichem Interesse oder reines Individualinteresse?
- **Vorschlag**: auch private IT-Sicherheit als öffentliches Interesse anerkennen, da sonst Widersprüche drohen (besonders sensible Daten dürfte weniger gut geschützt werden)
- **Datenschutzaufsicht**: Hinweise wünschenswert

V. Fazit und Ausblick

- Zunehmende Cyberangriffe machen Pentests unverzichtbar
- Minimierung von Risiken unbeabsichtigter Rechtsverstöße:
  - Vertragliche Regelung samt Einverständniserklärung der verfügungsbefugten Stelle
  - Abschluss eines Auftragsverarbeitungsvertrags
- Wünschenswert:
  Klarstellung durch Behörden (Pentests und sensible Daten) und Gesetzgeber (Reformbedarf im Computerstrafrecht)
- In Zukunft vermehrt relevant: Bei KI-gestützten Pentests zusätzlich Anforderungen der KI-Verordnung (insbesondere Transparenz- und Sicherheitspflichten)