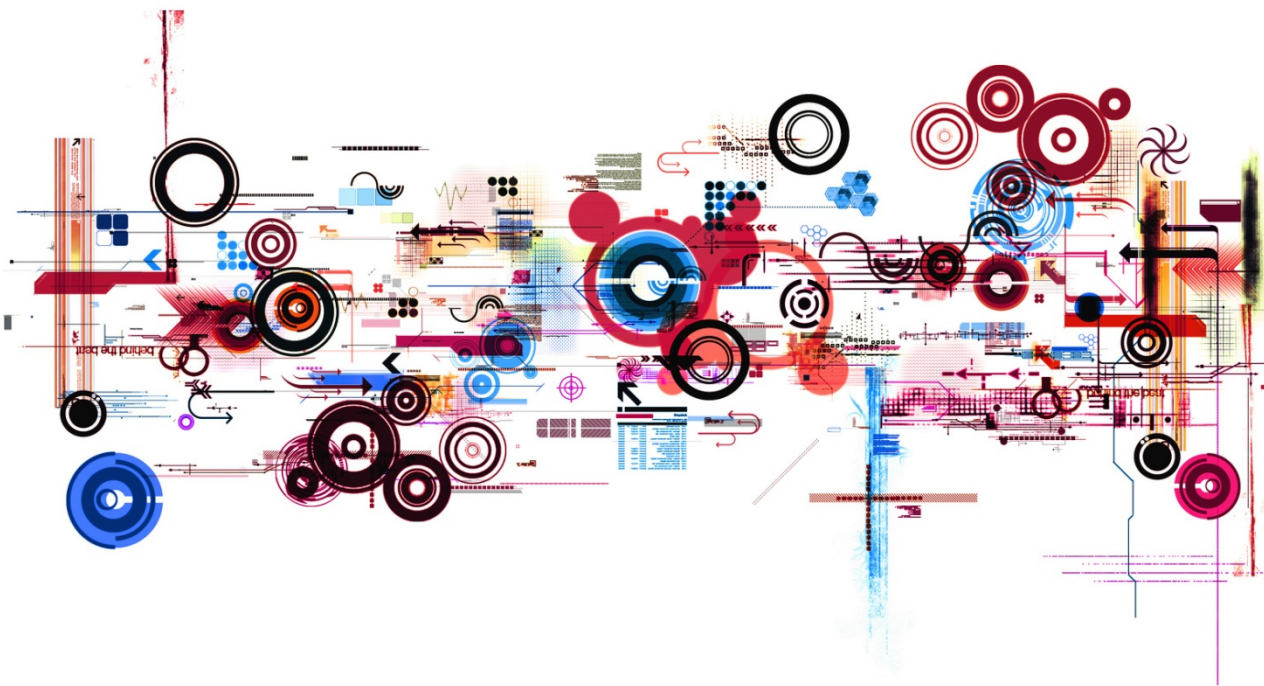


Der unbefugte Zugriff auf gesicherte Daten unter näherer Betrachtung des § 202a StGB



24.07.2015 18:20

« Vorige | Nächste »

Nach Fernsteuerungs-Hack ruft Fiat Chrysler 1,4 Millionen Autos zurück

urlesen / MP3-Download



Während ein Journalist im Wagen saß, konnten die Angreifer das Fahrzeug steuern. (Bild: Screenshot)

Fiat Chrysler ruft die Software...

Ashley Madison: Hacker veröffentlichen zweiten großen Datensatz

Zum zweiten Mal innerhalb weniger Tage sind interne Daten des Seitensprungportals AshleyMadison.com veröffentlicht worden. Im neuen Paket finden sich offenbar auch Quellcode sowie die E-Mails des Chefs.

damit

Suche

Tools Foren

DIE WELT

Home Politik Wirtschaft Geld Sport Wissen Panorama Feuilleton ICON Reise PS WELT Regional Meinung Videos Markt

Panorama > Weltgeschehen > Tausende Webcams und Babyphones gehackt

INTERNET-SKANDAL

Hacker knacken Tausende Webcams und Babyphones

20.11.14

Auf einer russischen Webseite haben Hacker Videos veröffentlicht, Tausende von privat und geschäftlich genutzten Internet-Kameras sind betroffen, sogar Babyphones. Das Material stammt aus 250 Ländern.

How it Works FAQ

Media

ago

Beirut, Lebanon

Emerging Technology From the arXiv

April 24, 2015

Security Experts Hack Teleoperated Surgical Robot

The first hijacking of a medical telerobot raises important questions over the security of remote surgery, say computer security experts.

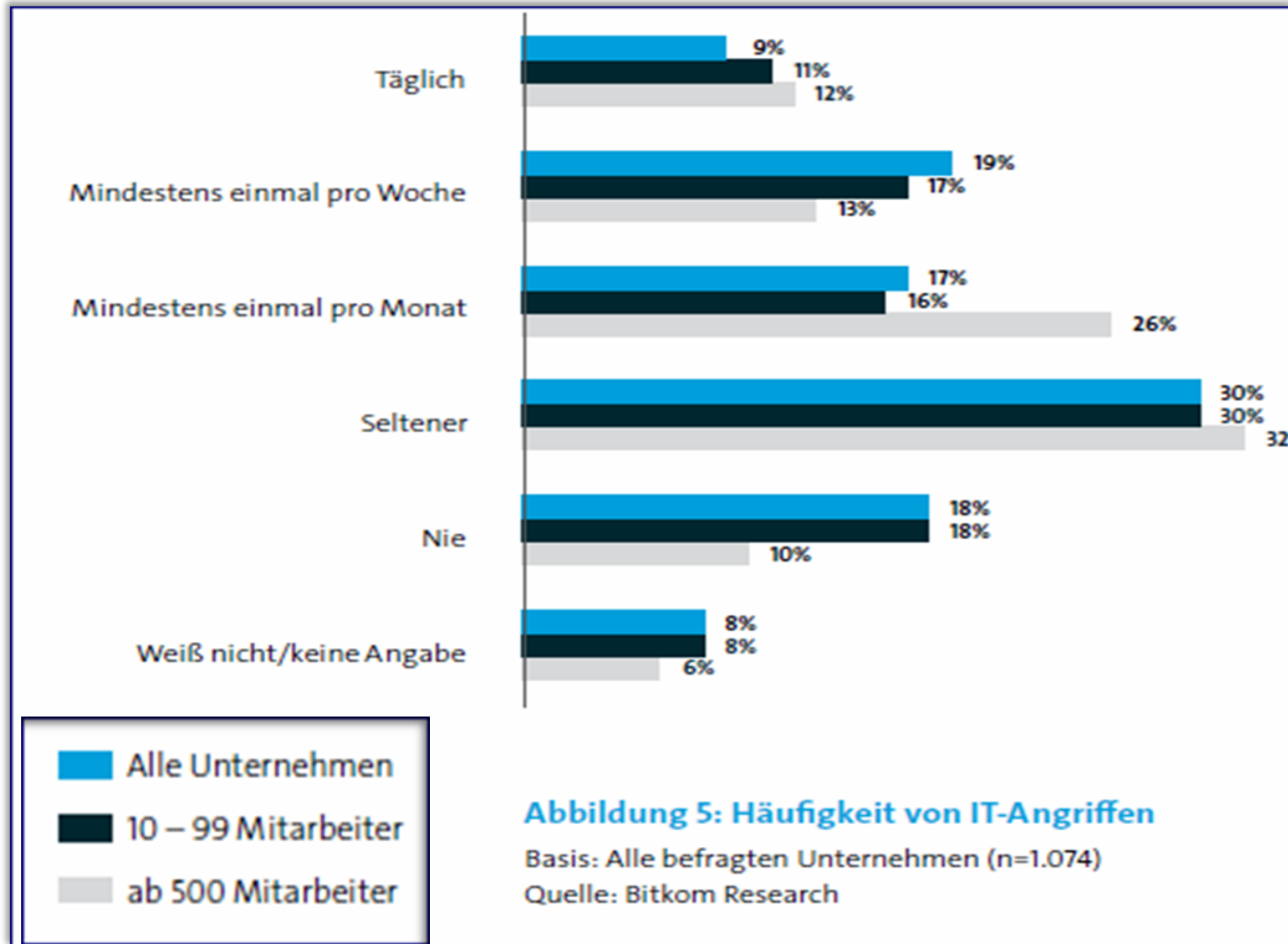
Der unbefugte Zugriff auf ge...
Betrachtung des § 202a StGB

Beratungsbedarf im IT-Strafrecht

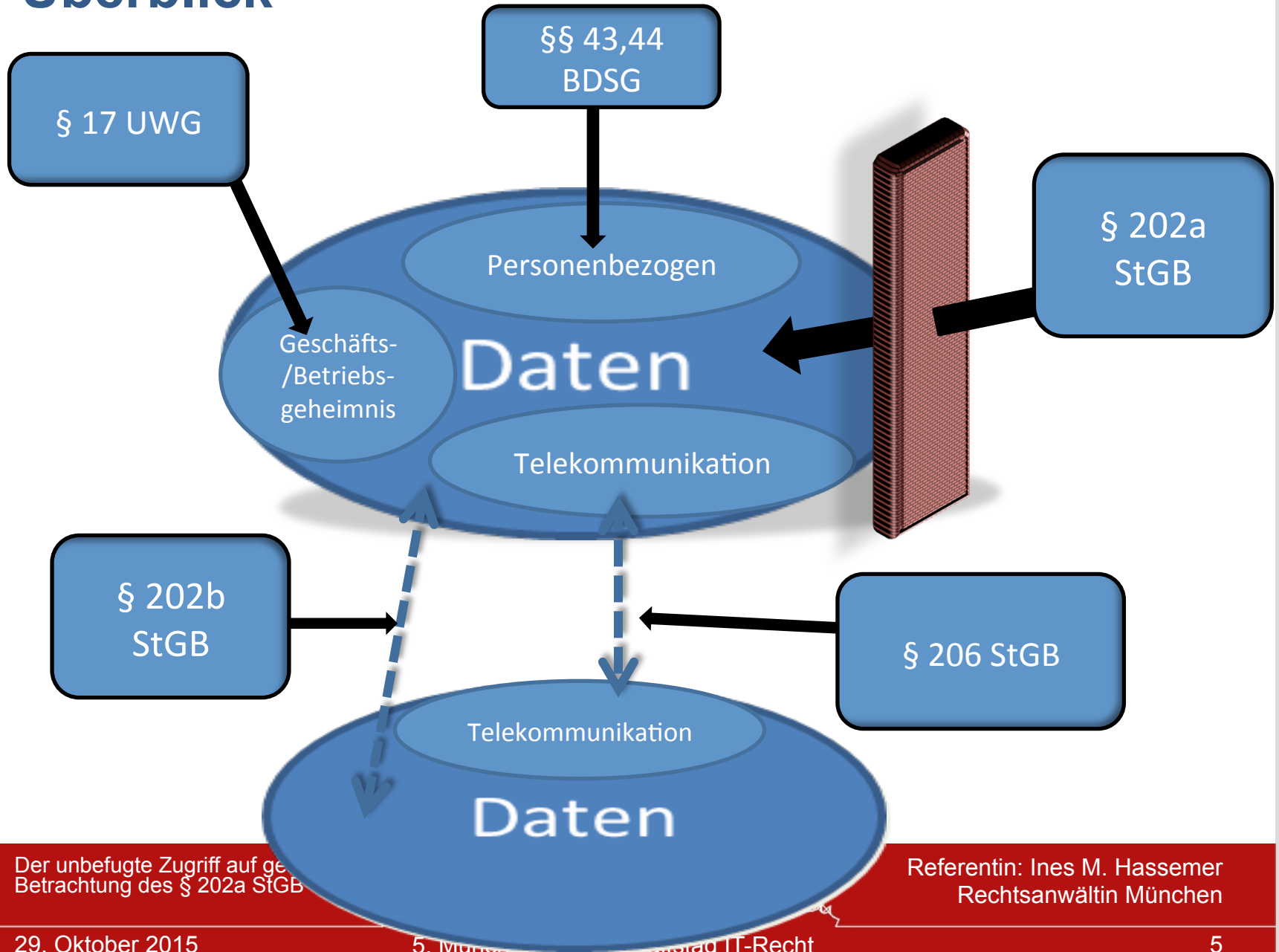
- ✓ **Strafrechtskonforme Regelungen im Unternehmen**
 - Compliance
 - EDV Betreuung
 - IT- Sicherheit

- ✓ **Fachgerechte Beratung im Strafverfahren**
 - Richtige Analyse des Sachverhalts
 - Korrekte Strafanzeigen
 - Beachtung der einschlägigen Formalien, insbesondere: Strafantragsfristen
 - Adäquate Verteidigungsstrategie
 - Zuziehung einer/s FA für Strafrecht

IT-Angriffe auf Unternehmen



Überblick



Der unbefugte Zugriff auf ge...
Betrachtung des § 202a StGB

Referentin: Ines M. Hassemer
Rechtsanwältin München

§ 202a StGB Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

Daten, die für den Täter nicht bestimmt sind

- Daten: § 202a Abs. 2 StGB
- Ausschlaggebend: Rechtsmacht zur Verfügung über die Daten.
- Nicht tatbestandsgemäß: Zweckwidriges Verwenden.
Fallbeispiel: Der Handelnde darf grundsätzlich über die Daten verfügen, handelt jedoch gegen den Willen bzw. die Weisung des Berechtigten.
- Auf den Inhalt kommt es nicht an. Insofern nicht erforderlich:
 - Personenbezug
 - Betriebs- oder Geschäftsgeheimnis

Gegen unberechtigten Zugang besonders gesichert

- Vorkehrungen, die den Zugang zu Daten ausschließen bzw. nicht unerheblich erschweren (≠ strenge Regelungen gem. Anlage 1 zu § 9 BDSG)
- Berechtigter dokumentiert sein Interesse an der Geheimhaltung (Signalwirkung)
- Sicherung zum Zweck der Zugangsverhinderung bzgl. der Daten

Zugangssicherung

+	—
Geheimes Passwort	Öffentliches Passwort
Zugangstür mit Kontrollsystem für Befugte (Beispiel: Rechenzentrum)	Brandschutztür (ohne Bezug zu den gesicherten Daten)
Biometrische Erkennungsverfahren	Genehmigungsvorbehalt, Allg. Registrierungspflicht
Verschlüsselung	„Verstecken“ der Dateien

Verschaffen unter Überwindung der Zugangssicherung

- Systemsicherung muss zum Zeitpunkt des Überwindens wirksam sein.
- Fallbeispiel:
Arbeitnehmergerät ist gesichert – Kopie liegt auf Unternehmensserver

Unbefugtes Handeln/Rechtswidrigkeit

Der Täter muss unbefugt handeln, im Sinne der Rechtswidrigkeit (allgemeines Deliktsmerkmal).

Doppelfunktion:

- Keine Befugnis (ansonsten Tatbestandsausschluss)
- Keine Rechtfertigungsgründe
- Beispiele: IT-Sicherheitsprüfungen

Compliance

IT Sicherheit

IT Sicherheitsprüfungen beinhalten das Risiko einer Strafbarkeit gem. § 202a StGB für Auftragnehmer und Auftraggeber. Folgende Aspekte sollten vorab geprüft werden:

- Ist die private Nutzung erlaubt?
- Auf welche Datenspeicher wird zugegriffen?
- Wer ist Eigentümer der betroffenen Datenspeicher?
- Wo werden Sicherungen überwunden?
- Auf welche Daten wird zugegriffen?
- Wem gehören die betroffenen Daten – Rechtsmacht?
- Liegen umfassende und wirksame Einverständniserklärungen vor, welche die Überwindung von Zugangssicherungen bzw. den Zugriff auf gesicherte Daten ausdrücklich erfassen?

Brennpunkt Compliance

Wird ein Zugriff auf gesicherte AN-Datenspeicher im Rahmen von Compliance Maßnahmen in Erwägung gezogen, sollte vorab geprüft werden:

- Ist die private Nutzung grundsätzlich erlaubt?
- Gibt es ausreichende Einverständniserklärungen?
- Wem gehören die betroffenen Daten – Rechtsmacht?
- Wer ist Eigentümer der betroffenen Datenspeicher?
- Warum ist der Zugriff erforderlich?
(Verhältnismäßigkeitsprüfung)

Strafantragserfordernis gem. § 205 Abs. 1 S. 2 StGB

- Gem. § 77 ff StGB muss der Verletzte innerhalb von 3 Monaten nach Kenntnisaufnahme von Tat und Täter einen Strafantrag stellen.
- Anderenfalls besteht das Risiko, dass die Tat nicht mehr verfolgt wird, es sei denn, die Strafverfolgungsbehörde hält wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten.

Vielen Dank für Ihre Aufmerksamkeit.

SSW SCHNEIDER SCHIFFER WEIHERMÜLLER
Rechtsanwälte Steuerberater Wirtschaftsprüfer

Ines M. Hassemer
Rechtsanwältin und Fachanwältin für Strafrecht
Beethovenstraße 6
80336 München

Ines.Hassemer@ssw-muc.de

