§ 202a - 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.

1. Tatbestandsmerkmale :

Objektiv:

- Daten
- nicht unmittelbar wahrnehmbar
- Unbefugtheit
- Nicht für den Täter bestimmt
- Gegen unberechtigten Zugriff besonders gesichert
- Zugang verschaffen
- Überwindung der Zugangssicherung

Subjektiv:
-Vorsatz

Rechtwidrigkeit:
Rechtfertigunsgründe?

Schuld:
Schuldausschließeungsgründe?

Strafantrag
vgl.: §205 StGB

2. Auslegung der Tatbestandsmerkmale :

Objektiver Tatbestand:

Daten:
Daten i.S. des § 202a StGB sind vgl. Abs. 2
→ Nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden

nicht unmittelbar wahrnehmbar:
Daten müssen kodiert vorliegen
→ Ein Auslesen der Daten darf nur mit zusätzlicher Technik möglich sein, wie Verstärkern, Sensoren oder Bildschirmen
z.B. Das Schreiben auf Papier zählt nicht zu dieser Definition nach Daten

Unbefugtheit:
Verwendung ist unbefugt, wenn die Verwendung der Daten gegen den Willen des Berechtigten der Daten ist. Dafür muss der Personenkreis der Berechtigten klar definiert sein.

Nicht für den Täter bestimmt:

Der Täter ist kein Berechtigter um diese Daten einzusehen. Die Einsichtnahme richtet sich gegen den Willen des Berechtigten oder Datenbesitzers.

Gegen unberechtigten Zugriff besonders gesichert:
Vorkehrungen die einen Zugriff auf Daten für Unberechtigte ausschließen oder zumindest erschweren. Techniken, die einen nicht unerheblichen Aufwand für den Datenzugang erzeugen für unbefugte Zugriffe. Dazu zählen digital geschützte Daten (mittels Passwort oder biometrischen Kennungen) oder auch das Verschließen des Datenträgers hinter physischen Sicherungen (wie z.B. Safes)

Zugang verschaffen:
Der Täter muss Zugang zu den Daten erlangen.
Ausreichend ist, dass er oder ein Dritter die Möglichkeit hat auf die Daten zuzugreifen. Er muss sie nicht zwingend betrachten oder zur Kenntnis nehmen.

Unter Überwindung der Zugangssicherung
Der Zugang zu den Daten muss kausal darauf zurückzuführen sein, dass der Täter die Zugangssicherung überwunden hat. Das Überwinden der Sicherung muss aktiv und mit Vorsatz erfolgen. Der unerhebliche Aufwand ist dabei objektiv zu betrachten und nicht subjektiv durch den Täter zu beurteilen.

Subjektiver Tatbestand:

Vorsatz i.S.d. §15 StGB
mindestens Dolus eventualis (bedingter Vorsatz) bzgl der objektiven Tatbestandsmerkmale (Der Taterfolg muss bei entsprechendem Handeln zu erwarten sein)

Rechtswidrigkeit:
- Keine Notwehr nach §32 StGB ; kein rechtfertigender Notstand nach §34 StGB (keine Notlage)

Schuld:

Schuldunfähigkeit des Kindes §19 StGB

Schuldunfähigkeit wegen seelischer Störungen §20 StGB
→ verminderte Schuldunfähigkeit nach §21 StGB

Kein Notwehrexzess nach §33 StGB
Kein Entschuldigender Notstand nach §35 StGB

Strafantrag:

Gemäß §205 StGB: relatives Strafantragsdelikt; die StA kann bei vorliegendem besonderen öffentlichen Interesse ein Einschreiten von Amts wegen für geboten halten.

3. Cybercrimephänomene (Beispiele):

- Keylogger
- Spyware
- Sniffing / Port Scanning

Kommentar Nachbearbeitung:
→ Weder Sniffing noch Port Scanning sind nach § 202a StGB im regulären Maße strafbar

Sniffing fällt rein nach Definition nicht unter das reine Ausspähen von Daten, sondern unter das Abfangen von Daten, da passiv im Netzwerkdatenverkehr mitgeschnitten wird.

Port Scanning ist ebenso nicht nach § 202a StGB strafbar, da Ports eine öffentlich einsehbarer Quelle darstellen und keine besondere Zugangssicherung bei Port Scanning überwunden wird. Zum Zeitpunkt des Scannens hat sich der Täter noch keinen Zugang zu für nicht bestimmten Daten verschafft.

Anderes Beispiel, welches noch unter § 202a StGB fällt:
- Brute-Force Angriffe auf Passwörter erfüllt das TBM der Umgehung einer besonderen Zugangssicherung

4. Rechtsgutachterliche Prüfung eines Beispiels:

BEISPIEL:

In einem Unternehmen ist eine Kundendatenbank mit Passwort und Firewall hinsichtlich eines unberechtigten Zugriffs gesichert. Mitarbeiter A hat aufgrund seiner Stellung im Unternehmen keinen Zugang zu diesen Daten. Mitarbeiter B (Abteilungsleitung) hat Zugang zu diesen Daten. Mitarbeiter A sieht wie Mitarbeiter B seine Zugangsdaten aufschreibt und in seinem persönlichen Notizbuch hinterlegt. A verschafft sich widerrechtlich Zugang zur Kundendatenbank indem er die Zugangsdaten des Kollegen B verwendet die sich in dessen persönlichen Notizen befinden. A möchte die Telefonnummer und Adresse eines Kunden in Erfahrung bringen.

Daten:
Daten aus der Kundendatenbank (elektronisch gespeichert, nicht unmittelbar wahrnehmbar)

Nicht für den Täter bestimmt:
A ist kein Abteilungsleiter und hat daher keine Zugangsdaten zur Kundendatenbank

Gegen unberechtigten Zugriff besonders gesichert:
Die Kundendatenbank mit Passwort und Firewall hinsichtlich eines unberechtigten Zugriffs gesichert

Zugang verschaffen:
Der A nimmt die Zugangsdaten des B um damit auf die Daten zuzugreifen.

Unter Überwindung der Zugangssicherung
Er umgeht mit den widerrechtlich genutzten Zugangsdaten des A den Passwortschutz und die Firewall.

Subjektiver Tatbestand:
Vorsatz i.S.d. §15 StGB
Der A möchte auf die Kundendatenbank zugreifen. Er möchte gezielt die Daten eines bestimmten Kunden in Erfahrung bringen. Er handelt daher mit direktem Vorsatz.

Rechtswidrigkeit:
Es gibt keine Rechtfertigungsgründe.

Schuld:
Es sind keine Schuldausschließungsgründe ersichtlich.

→ A könnte sich nach § 202a StGB strafbar gemacht haben.