»IT-Sicherheit für klein- und mittelständische Unternehmen«

Veranstaltung der IHK Cottbus im TGZ Wildau (12.06.2008)

Die rechtlichen Herausforderungen der IT-Sicherheit

Referent: Rechtsanwalt Peter K. Baake
Kanzlei Baake Berlin

Hinweise

- Die Inhalte dieses Handouts dienen lediglich den Zuhörern des Seminars als Gedächtnisstütze.
- Die Informationen erheben keinen Anspruch auf Vollständigkeit. Sie können und sollen eine rechtliche Einzelfallberatung nicht ersetzen.
- Bearbeitungsstand: 11.06.08

Überblick

- Neuregelungen des Computerstrafrechts
- Rechtliche Risiken des Einsatzes von Anti-Spam-/Anti-Viren-Software
- Notwendigkeit eines »*IT-Sicherheitsbeauftragten*«*?*
- Datensicherung

Strafverschärfungen

durch das StrÄndG (08/2007) zur Bekämpfung der Computerkriminalität

- modifiziert: § 202a StGB („Ausspähen von Daten“)
- modifiziert: § 202b StGB („Abfangen von Daten“)
- **neuer »*Hackerparagraph*«: § 202c StGB** („Vorbereitung des Ausspähens und Abfangens von Daten“)
- modifiziert: § 303b StGB „Computersabotage“

Wortlaut »Hackerparagraph«, § 202c StGB:

»Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. *Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder*
2. *Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,*

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.« (...)

Aus didaktischen Gründen stark verkürzte Tatbestandskomprimierung des § 202c Nr. 2:

Wer sich Computerprogramme verschafft, deren Zweck die Begehung einer Straftat nach § 202a oder § 202b ist, wird bestraft.

Praxisprobleme des § 202c StGB

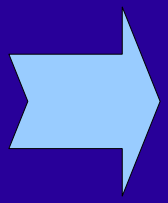
Woran merkt man, dass ein Programm das Ausspähen oder Abfangen von Daten **bezweckt**?

Ab wann überschreitet man die Schwelle zur »**Vorbereitungshandlung**«?

Können wenigstens noch **firmeneigene Sicherheitheitstests** straflos durchgeführt werden?

1. Woran merkt man, dass ein Programm das Ausspähen oder Abfangen von Daten **bezweckt?**

- Maßstab: ***„objektivierte Zweckbestimmung"***
- Problem: Wer bestimmt diesen Zweck objektiv?
  - Programmierer/Benutzer? Zu willkürlich!
  - Richter? Zu wenig sachnah!
  - Sachverständiger? Jedenfalls bei sog. »**dual-use**«-Programmen zu unsicher?



Gefahr von willkürlichen Ergebnissen!

2. Ab wann überschreitet man die Schwelle zur »**Vorbereitungshandlung**«?

- Das Ausspähen oder Abfangen von Daten muss in groben Zügen in Aussicht genommen werden.
- Dabei ist unerheblich, ob die Vorbereitung geeignet ist, die Tat später auch tatsächlich durchzuführen.

3. Können wenigstens noch **firmeneigene Sicherheitheitstests** straflos durchgeführt werden?

- »*Freibrief*« für IT-Verantwortliche?

  Denkbar, da es zum Aufgabenbereich gehört (juristisch: »konkludente Einwilligung«).

- Besser: Ausdrückliche Einwilligung (z.B. im Arbeitsvertrag)

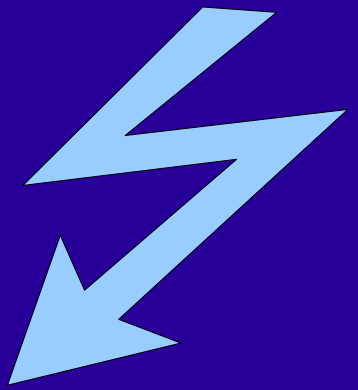
Rettung durch fehlenden Vorsatz?

- Doppelter Vorsatz erforderlich:
  1. dass Programm zur Tatbegehung geeignet
  2. es sich verschaffen (etc.) zu wollen
- Ergo: Je größer die Spezialkenntnisse über die Leistungsfähigkeit des Programms, desto eher wird Vorsatz unterstellt werden können!

Besondere Gefahr für IT-Experten!

Warum sollte mich das interessieren?
Bisher lief doch auch alles reibungslos?!

- straf-/zivilrechtliche Haftung des Geschäftsführers / Inhabers
- Wesentlich praxisrelevanter: **arbeitsrechtliche Auswirkungen!** Schlimmstenfalls Anlass / Grund für fristlose Kündigung!



Bewertung: § 202c StGB praxistauglich?

- Zahlreiche seit Jahren verbreitete Anwendungen und Testverfahren können zur tickenden Zeitbombe werden!
- Spielwiese für Juristen, aber hindernisreicher Trampelpfad für IT-Verantwortliche!
- Gegebenenfalls sogar Verstoß gegen strafrechtliches Bestimmtheitsgebot (Art. 103 Abs. 2 GG)

Praktische Konsequenzen

- Firmeninterne Sicherheitstests nur mit entsprechender **Freigabe** der Geschäftsführung (konkludent, besser aber ausdrücklich)
- Genaue **Protokollierung** und **Dokumentation** erforderlich, möglichst veränderungssicher!
- **Keine Weitergabe** von Software zum Auffinden von Sicherheitslöchern an Dritte!

Rechtliche Risiken des Einsatzes von Anti-Spam-/Anti-Viren-Software

- Anti-Spam/Anti-Viren-Software unverzichtbar, andernfalls Haftung aus Organisationsverschulden
- ABER: strafrechtlich relevante Datenunterdrückung (§§ 303a, 206 StGB) bei Löschung privater E-Mails?

OLG Karlsruhe v. 10.01.2005, 1 WS 152/04

*»**Unter Umständen kann es** daher **gerechtfertigt sein**, eine E-Mail herauszufiltern, beispielsweise dann, wenn eine E-Mail mit **Viren** behaftet ist, so dass bei deren Verbreitung Störungen oder Schäden der Telekommunikations- und Datenverarbeitungssysteme eintreten.«*

Lösungsansätze

»Holzhammer«-Methode:

- private E-Mail-Nutzung generell untersagen
- Gleiches gilt auch privates „Surfen“ und Speicherung von externen Programmen oder Daten
- Verbot muss zudem regelmäßig überwacht werden, um keine stillschweigende Duldung zu fingieren.

Probleme der »Holzhammer«-Methode:

- Praktikabilität?
- Mitarbeiterzufriedenheit?
- Durchsetzbarkeit?
- Kontrollierbarkeit?
- Verletzung des Gleichbehandlungsgrundsatzes?

Alternative 1: separate Spam-Postfächer

- Vorteil: Strafrechtlich wohl zulässig
- Was aber ist mit »Ausreißern«?
- Wer haftet hierfür?
- Gefahr durch Viren/Trojanern für gesamte IT nicht gebannt!

Alternative 2: modifizierter »Holzhammer«

- Untersagung der privaten E-Mail-Nutzung (Vorteil: Arbeitgeber wird nicht zum »*Diensteanbieter*« im Sinne des TKG - str.)
- Gestattung von privatem »Surfen« im moderaten Maße (Vorteil für Mitarbeiter: Nutzung von »Webmail« möglich; Vorteil für Arbeitgeber: unter Umständen keine Aussortierungspflicht von privaten E-Mails nach einem Ausscheiden des Mitarbeiters)

IT-Sicherheitsbeauftragter

- Keine zwingende Regelung im Gesetz
  (außer TK-Anlagenbetreiber...)
- Zuständig für Ausarbeitung und Einhaltung von Sicherheitskonzepten
- Haftungsprivileg gilt nur für Arbeitnehmer, nicht für externe Dienstleister!
  Interner Mitarbeiter hat in der Regel Freistellungsanspruch gegenüber Arbeitgeber
- Geheimhaltungspflichten

Datensicherung

- Von der Rechtsprechung aufgestellte Mindestanforderungen hinsichtlich der Häufigkeit von Sicherungskopien (Backup)
- Bei Nichteinhaltung: unter Umständen kein Schadensersatz für Kosten der Datenrekonstruktion (OLG Hamm 01.12.2003 (13 U133/03))

OLG Hamm 01.12.2003 (13 U133/03)

- »Wie dargelegt, gehört es im gewerblichen Anwenderbereich heute zu den vorauszusetzenden Selbstverständlichkeiten, dass eine zuverlässige, zeitnahe und umfassende Datenroutine die Sicherung gewährleistet. (...) Die Sicherung hätte **täglich** erfolgen müssen, die **Vollsicherung** mindestens einmal **wöchentlich**.«
- Gegebenenfalls auch Haftung des Geschäftsführers gegenüber den Gesellschaftern

Exkurs:

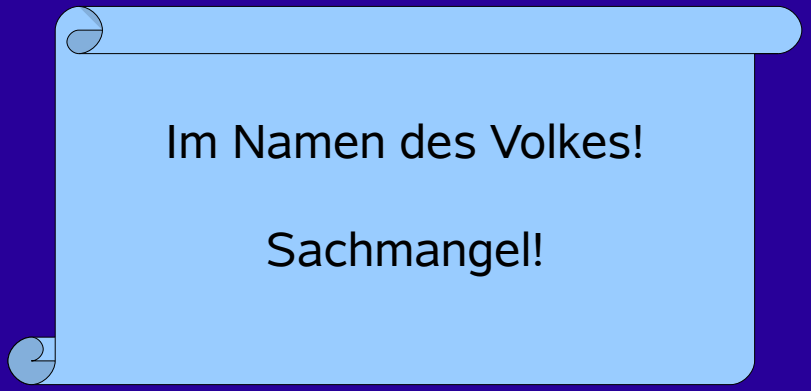
Tadellose Sicherungskopie, aber unregelmäßig auftauchende (unzutreffende) Meldung:

»Während des Prüflesens der Systemsicherung wurde ein Fehler festgestellt.
Die Systemsicherung ist unbrauchbar!«

Sachmangel der Datensicherungseinheit?!

Exkurs (Auflösung)

- OLG Koblenz Urt. v. 19.09.2007 - 1 U 1614/05:



- Grund: manuelle Überprüfung nicht zumutbar!

Fazit:

- Rechtliche Anforderungen an IT-Experten in vielen verschiedenen Gesetzen verankert.
- Dimensionen von Gesetzesänderungen auch von Experten nicht immer absehbar.
- Oberstes Gebot beim Austesten von IT-Sicherheitsrisiken: Freigabe & Dokumentation
- Nutzungsmöglichkeiten mit Arbeitnehmern im Vorfeld regeln

Vielen Dank für Ihre Aufmerksamkeit!

Rechtsanwalt Peter K. Baake

Kanzlei Baake

Gardeschützenweg 139

12203 Berlin

☎ 030 / 245 36 22 - 0

peter.baake@kanzlei-baake.de

Handout-Download

www.kanzlei-baake.de

Kanzlei Baake

Die von Rechtsanwalt Peter K. Baake im April 2004 gegründete Berliner Kanzlei beschäftigt sich schwerpunktmäßig mit Fragen des Immaterialgüter-, Wettbewerbs- und Internetrechts und vertritt hierbei mittelständische Mandanten sowohl gerichtlich wie auch außergerichtlich.

Rechtsanwalt Baake ist Mitglied der Arbeitsgemeinschaft Informationstechnologie (DAV IT) im Deutschen Anwaltverein (DAV) e.V.