

Änderungen im Computerstrafrecht – was IT wissen sollte

Autor: Georg Osner, Datenschutzberater und IT-Revisor
November 2007

Bis zuletzt umstritten waren einige Änderungsformulierungen des Strafrechts (StGB), insbesondere zum sog. Hackerparagrafen und dessen Auswirkungen auf die betriebliche Praxis:

Nicht nur die Vorgehensweise beim Einsatz von Sicherheitstools zur Netzwerküberwachung, zur Passwortwiederherstellung oder die Durchführung von Vulnerability-Checks sollten künftig verstärkt hinterfragt werden.

Auch alltägliche Vorgänge wie Passwortweitergaben an die Vertretung oder der Vermerk von Sicherheitscodes in der Nähe Ihres Arbeitsplatzes sind betroffen:

In beiden Fällen wäre eine Überwindung der Zugangssicherung ohne erheblichen Aufwand möglich und die neuen Bestimmungen des § 202 a StGB könnten zur Anwendung kommen – so einige Argumentationen bei der Diskussion der Gesetzesvorlagen.

Auf was sollten IT-Verantwortliche, Administratoren und IT-Nutzer achten, um strafrechtliche Fallen zu umgehen ?

Strafrechtliche Konsequenzen drohen in der Regel immer dann, wenn es sich um einen sog. Vorsatz handelt. Aber Vorsicht !

Auch wenn kein subjektiver Vorsatz vorliegt, kann es im Verdachtsfall im Eigeninteresse notwendig werden, den tatsächlichen Nicht-Vorsatz und ggf. auch eine Nichtbeteiligung unter Beweis zu stellen.

Nicht übersehen werden sollten darüber hinaus auch eine mögliche zivilrechtliche Schadensersatzpflichtigkeit, die schon mit Fahrlässigkeit eintreten kann.

Gestalten Sie klare und nachvollziehbare Abläufe, Prozesse und Regeln und vermeiden Sie dadurch schon im Vorfeld bestimmte Risiken.

Hier einige Handlungshilfen:

- keine Passwortrücksetzungen auf Zuruf
- Keine Weitergabe von Passwörtern, Sicherheitscodes oder Karten an Dritte
- Datei/ Datenlöschungen nur mit schriftlichen Auftrag des Dateiowners
- fremde E-Mails sind grundsätzlich tabu (vergleichbar: Briefgeheimnis)
- Weitergabe von Datenträgern mit Programmen oder Daten nur nach Virenprüfung
- Programmänderungen nur mit nachvollziehbarem Änderungsauftrag
- klare Regeln für den Einsatz von Sicherheitstools (u. a. zur Netzwerküberwachung)
- vermeiden Sie Penetrationstests in Eigenregie ohne entsprechenden Auftrag
- Achten Sie auf die Dokumentation von System-, und Programmänderungen (z.B. Serverdokumentation, Programmdokumentation)
- keine Änderung oder vorzeitiges Löschen von Logdateien/ daten
- Sichern Sie Logdateien vor unbefugten Zugriff (ggf. auf separaten Rechner)
- Beschränken Sie die Installationsmöglichkeiten für Programme (z.B. strenge Systemrichtlinien)
- Auch für Programminstallationen gilt das Prinzip Auftrag und Genehmigung
- Vorsicht beim Einsatz von Entschlüsselungstools
- Hände weg von Keyloggern und Passwortknackern
- Sichern Sie sich ab bei Fernsteuerung von fremden Rechnern (im eigenen Interesse!)

- Hände weg von der Programmierung zwangsweiser Veränderungen der Browsereinstellungen in Internetprogrammen (z.B. über Java oder ActiveX)
- Achten Sie auf die Vollständigkeit der Lizenzen
- Der Einsatz von Tools zum Kopieren z.B. geschützter Musik CDs wie auch Kopierschutzknacker sind unmittelbar strafrechtlich bedroht.

Nutzen Sie strafrechtliche Vorschriften auch zum Schutz Ihrer Unternehmensdaten !

Der Zugriff auf Systeme und Daten muss – falls zum Beispiel § 202 a – Ausspähen von Daten- wirksam werden soll, unter Überwindung einer Zugangssicherung erfolgen, ansonsten besteht kein besonderer Geheimnisschutz. Hierfür notwendig sind beispielsweise Firewalls, Logins, Passwörter und für E-Mails in der Übertragungsphase Verschlüsselung.

Ebenso können grosszügige oder fehlerhafte Dateifreigaben den besonderen Geheimnisschutz aufheben.

Neben dem kürzlich geänderten Strafrecht gibt es schon seit geraumer Zeit eine Reihe weiterer Strafrechtsvorschriften mit Auswirkungen auf die IT, u. a.:

- rechtswidriges Löschen, Unterdrücken, Zerstören oder Verändern von Daten (§ 303a)
- Computersabotage (303b), u. a. auch durch Verbreitung von Viren
- die Fälschung beweiserheblicher Daten (§ 269, §270), wobei beweiserhebliche Daten auch Stammdaten von Geschäftskunden oder Kontenstandsdaten sein können.

Aufzupassen gilt es auch

bei allen Verarbeitungen, Nutzungen und Weiterleitungen von personenbezogenen Daten, u. a. Mitarbeiterdaten und Kundendaten. Hier gelten die Bussgeld-, und Strafbestimmungen des Bundesdatenschutzgesetzes – besonders auch im Hinblick auf missbräuchliche Nutzung.

Für die Bereiche Telekommunikation (Telefon, Internet, E-Mail) gilt es, nicht nur auf die Wirkung des sog. Telefongeheimnisses zu achten, sondern auch auf spezielle Bestimmungen aus dem Telekommunikationsrecht.

Auf dem Gebiet der Telemedien ergeben sich weitere strafrechtliche Risiken nicht nur aus der unmittelbaren Verantwortung für einen dargestellten Inhalt (z.B. Pornographie, Jugendschutz), sondern auch aus abgeleiteter Strafbarkeit, z.B. wegen Unterlassens einer unverzüglichen Sperrung nach deren Kenntnisnahme.

Über das Urheberrecht wurde das Kopieren geschützter Werke (Raubkopien) unter Umgehung eines Kopierschutzes ebenso verboten wie die Herstellung und der Vertrieb von Software, die einen Kopierschutz überwinden kann.

Was wurde im Strafrecht (StGB) konkret geändert ?

Auszug aus den Änderungen im sog. Computerstrafrecht (Die Änderungen sind fett gedruckt.)

§ 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.

§ 202b "Abfangen von Daten"

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c "Vorbereiten des Ausspähens und Abfangens von Daten"

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passworte 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 zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

§ 303a "Datenveränderung"

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend

Weitere detaillierte Informationen finden Sie unter dem Link

<http://www.bmj.bund.de/media/archive/1317.pdf>

Hinweis in eigener Sache:

Die vorliegende Abhandlung erhebt nicht den Anspruch auf Vollständigkeit und hat nicht den Charakter einer Rechtsberatung.