Computerkriminalität

I. Viren

▪Die Vorsätzliche Programmierung und Verbreitung von Viren ist strafbar. (§§ 303 a, b StGB)
▪Eine Freiheitsstrafe von bis zu 5 Jahren kann verhängt werden.
▪Die fahrlässige Computersabotage durch Viren ist nicht strafbar.▪Vorsicht beim Austausch von Datenträgern zwischen Unternehmen:
„billigend in Kauf nehmen" ist auch vorsätzlich
▪Überprüfungspflicht auf Viren
▪Landgericht Kleve: bei einem Handelsgeschäft besteht Prüfungspflicht auf Viren (zumindest dann wenn das Unternehmen „vom Fach" ist)▪Vorsorgemaßnahmen aus rechtlicher Sicht:
-Regelmäßiger Einsatz eines Virenscanners
-stichprobenartige Überprüfung ausgehenden Datenträger
-Protokoll über Prüfungen führen
-Mitarbeiter über Notwendigkeit der Maßnahmen informieren
-Verantwortlichen bestimmen (sonst Organisationsverschulden)

II. Computerspionage

▪Strafbar ist:
-die Mitteilung geheimer Firmendaten (bei Mitarbeitern) (§ 17 I UWG)
-die Anwendung technischer Mittel zur Erlangung oder Herstellung einer verkörperten Wiedergabe von firmeninternen Daten (§ 17 II UWG)
-der unberechtigte Zugriff auf Daten die gegen eines solchen Zugriff besonders geschützt sind (z.B. Passwort) (§ 202 a StGB)▪Für Mitarbeiter gilt:
Computerspionage ist ein schwerwiegender Vertrauensbruch, fristgemäße Kündigung ist gerechtfertigt

III. Computersabotage

▪Die vorsätzliche Störung der Datenverarbeitung durch-Datenveränderung-Zerstörung-Beschädigung-unbrauchbar machen-Beseitigung oder-Veränderung ▪einer Anlage oder eines Datenträgers ist strafbar, Freiheitsstrafe bis zu 5 Jahre (§ 303 b StGB)
▪Die vorsätzliche Manipulation von Daten durch
-löschen
-unterdrücken
-unbrauchbar machen oder
-verändern
▪ist strafbar, Freiheitsstrafe bis zu 2 Jahre (§ 303 a StGB)▪Programmsperren/expiration dates:
-Einbau einer Programmsperre um eine Wartung zu erzwingen

-Oberlandesgericht Bremen: Das Unterbringen eines expiration dates ist eine vorsätzliche sittenwidrige Schädigung.

IV. Computerbetrug

▪Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs durch
-unrichtige Gestaltung eines Programms
-Verwendung unrichtiger oder unvollständiger Daten
-unbefugte Verwendung von Daten
-unbefugte Einwirkung auf den Ablauf des Programms
▪Der Täter muss mit der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, handeln. (§ 263 a StGB)
▪Absicht ist die gesteigerte Form des Vorsatzes: Die Tathandlung wird vorgenommen um zu betrügen

V. Zeitdiebstahl

▪früher: unbefugte Nutzung der begrenzten Ressource Rechenzeit
▪heute: unbefugte Nutzung einer Datenübertragungsstrecke, z.B. Standleitung▪Nach herrschender Meinung ist der Zeitdiebstahl nicht strafbar, da keine Norm für solche Taten existiert.
▪Zivilrechtliche Schadensersatzansprüche sind gegeben.

VI. Computererpressung

▪Verschlüsselung fremder Daten, Entschlüsselung nur gegen Bezahlung eines bestimmten Betrages
▪Wird als Erpressung und Computersabotage strafrechtlich erfasst.

VII. Raubkopien

▪Kopien, die entgegen dem Urheberrecht oder verwandten Schutzrechten hergestellt oder verbreitet werden
▪Besser: “Schwarzkopie”, da kein Raub oder Diebstahl vorliegt

a. Unterschied Film/Musik zu Software

▪Film/Musik:
-Keine Umgehung des Kopierschutzes erlaubt
-Privatkopie gestattet (nur an enge Verwandte/Freunde) nach §53 UrhG und nach gängiger Rechtssprechung max. 7 Stück
-Kopien von ausgeliehenen Medien erlaubt
-Mitschnitte von frei empfangbarem Radio und TV ebenfalls gestattet, aber auch davon max. 7 Kopien an Verwandte/Freunde
-Keine Kopie von “offensichtlich rechtswidrig hergestellten Vorlagen”, z.B. bei Daten aus Filesharing-Programmen
▪Software:
-Umgehung des Kopierschutzes gestattet
-Keine Weitergabe, kein Verkauf ohne das Original

b. Strafbarkeit der Erstellung einer Raubkopie

▪jede Verletzung des Urheberrechts ist strafrechtlich relevant
-Privater Missbrauch: Geldstrafen sowie Freiheitsstrafen bis zu 3 Jahren
-Gewerblicher Missbrauch: Geldstrafen sowie Freiheitsstrafen bis zu 5 Jahren
-Umgehung von Kopierschutz: Geldstrafen bis zu 100.000 €, bis zu 1 Jahr Freiheitsstrafe
▪Sonstige Gefahren für Unternehmen:
-Imageverlust
-Geschäftsausfall (z.B. durch Einziehung der gesamten EDV-Anlage nach §110 UrhG i.V.m. §74e StGB)
-Abmahn-/Gerichtskosten
-Geld-/Haftstrafen der verantwortlichen Mitarbeiter

c. Software-Schutz

▪europaweite Richtlinie
▪Deutschland: §§69a bis 69g UrhG
▪Gegenstand des Schutzes:
-Alle Ausdrucksformen eines Programms, inklusive der Entwürfe
-Ideen und Grundsätze sind nicht geschützt
▪Rechte des Rechtsinhabers:
-Vervielfältigen
-Laden, Anzeigen, Ablaufenlassen, Übertragen, Speichern
-Verbreiten, Vermieten
▪Rechte des Benutzers:
-Vervielfältigen und Modifizieren des Programms, um Fehler des Programms zu berichtigen oder um das Programm lauffähig zu machen, nach §69d UrhG

d. Mehrfach- / Netzwerkinstallationen

▪Netzwerkinstallationen erlaubt
-Nutzungsberechtigter muss gewährleisten, dass nicht mehrere Nutzer auf eine gekaufte Software gleichzeitig zugreifen können à soviele Lizenzen wie Nutzer werden benötigt
▪Heimkopie nicht erlaubt
-gleichzeitige Nutzung einer Software an 2 Orten wäre sonst möglich
▪Sicherungskopie/Backup erlaubt
-konkludent nach §69d UrhG
-laut Gesetz nur, falls "für die Sicherung künftiger Benutzung erforderlich"

e. Frei verfügbare Programme

▪Anbieten von Downloads nur bei Software erlaubt, an der man die Rechte besitzt bzw. von Public-Domain-Programmen
▪Public-Domain-Programme:
-Softwareprodukte, an denen der Rechteinhaber seine Rechte ausdrücklich abgegeben hat
-dürfen vervielfältigt, verbreitet und benutzt werden
-keine Gewährleistungsansprüche

▪Shareware:
-kein Rechteverzicht des Urhebers, sondern nur Gestattung einer kostenlosen Probenutzung
-gewerbliche Nutzung und Weitergabe kann vom Autor verboten werden

f. Umgehung eines Dongles

▪Dongle: Hardwarestecker, der zum Betrieb eines Programms unverzichtbar ist
-soll Erstellung von Software-Kopien erschweren
▪Probleme:
-Dongle kann abhanden kommmen
-Dongle kann das System oder andere Programme stören
▪Entfernung eines Dongles dennoch Verstoß gegen das Urheberrecht
-keine dem Verwender eingeräumte Nutzung im Sinne des §69d UrhG

g. Manipulation von Software

▪Rechtssprechung:
-der berechtigte Anwender darf Programm zur Beseitigung von Störungen untersuchen, testen und ändern (nach §69d UrhG)
▪sonstige Manipulation verstößt gegen §69c UrhG
▪Weiterentwicklung oder Neuprogrammierung nicht erlaubt
▪Dekompilierung nur, um Informationen zur Herstellung der Interoperabilität zu erlangen (nach §69e UrhG)
-Dekompilierer muss Lizenznehmer sein
-Dekompilierung nur auf das notwendige Maß beschränkt