Praktischer Leitfaden für die Bewertung von Software im Hinblick auf den § 202c, StGB

Leitfaden

BITKOM

Impressum

Herausgeber:	BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. Albrechtstraße 10 A 10117 Berlin-Mitte Tel.: 030.27576-0 Fax: 030.27576-400 bitkom@bitkom.org www.bitkom.org
Ansprechpartner:	Lutz Neugebauer Tel.: 030.27576-242 l.neugebauer@bitkom.org
Redaktion:	Lutz Neugebauer, BITKOM e. V. in Zusammenarbeit mit Dr. Rüdiger Peusquens, Deutsche Telekom AG Christoph Puppe, HiSolutions AG RA Bernd H. Harder, Harder Rechtsanwälte Johann Fichtner, Siemens AG Wolfgang Schäfer, DATEV eG
Gestaltung / Layout:	Design Bureau kokliko / Anna Müller-Rosenberger (BITKOM)
Copyright:	BITKOM 2008

Praktischer Leitfaden für die Bewertung von Software im Hinblick auf den § 202c, StGB

Leitfaden

BITKOM

Inhaltsverzeichnis

- § 202c StGB: Vorbereiten des Ausspähens und Abfangens von Daten

  (1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
  Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
  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.

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

1 Einleitung und Hintergrund

Mit der Einführung des § 202 c (sog. Hackerparagraph) und weiterer IT-spezifischer Regelungen in das Strafgesetzbuch (StGB) im August 2007 wurden Vorgaben der Europäischen Union zur Bekämpfung von Computerkriminalität (Cybercrime) in deutsches Recht umgesetzt. Bezogen auf den § 202c StGB bedeutet dies, dass nicht nur das unberechtigte Beschaffen bzw. Manipulieren von Daten Dritter sondern nunmehr bereits die reine Vorbereitungshandlung hierzu unter Strafe gestellt ist. Der Gesetzgeber zielt damit insbesondere auf die Herstellung, Beschaffung oder Verbreitung von Software ab, die dem Anwender der Software auf strafbare Weise Zugang zu Daten verschafft, die nicht für ihn bestimmt sind.

Grundsätzlich begrüßt und unterstützt BITKOM die Absicht des Gesetzgebers, gegen Software-Hersteller, -Nutzer und -Distributoren vorzugehen, die Straftaten gemäß § 202a (Ausspähen von Daten) oder § 303a (Datenveränderung) fördern.

Der Wortlaut des § 202c StGB beschränkt jedoch die Strafandrohung nicht eindeutig auf die vom Gesetzgeber intendierten Fälle. Er lässt vielmehr auch rechtschaffene Software-Anbieter und –Anwender u. U. in die Nähe der Kriminalität geraten, denn der Wortlaut stellt zunächst auf die Herstellung, Beschaffung oder Verbreitung der Software als objektiven Tatbestand ab. Diese Tatbestandsvoraussetzung erfüllen auch Sicherheitsforscher, Netzwerk-Administratoren und Software-Qualitätsprüfer: Sie benötigen Computerprogramme wie in § 202c beschrieben, um IT-Systeme sicher zu gestalten und gerade gegen die mit §§ 202a/b unter Strafe gestellten Angriffe zu schützen. Nur durch – ordnungsgemäße – Nutzung dieser Programme, Exploits etc. lassen sich bestehende oder potentielle Sicherheitslücken erkennen.

Dieser schlechten wie guten Nutzungsmöglichkeit von Computerprogrammen (Dual- Use-Problematik) trägt § 202 c StGB allerdings nicht Rechnung, denn einem Computerprogramm zum Aufspüren von Sicherheitslücken sieht man nicht zwingend an, ob sein „ Zweck die Begehung einer solchen (Straf-)Tat“ ist. Und ob mit der Herstellung, Beschaffung oder Verbreitung eines besagten Computerprogramms nicht das weitere objektive Tatbestandsmerkmal „eine Straftat nach § 202a oder § 202b StGB vorbereitet zu haben“ erfüllt worden ist, hängt durchaus von den Umständen des Einzelfalls ab. Verschärfend kommt vielmehr hinzu, dass § 202c StGB ein Offizialdelikt ist, d.h. erfahren die Strafverfolgungsbehörden von der Existenz derartiger Programme, müssen sie ermitteln. Dabei werden sie den Verdacht, dass eine Straftat nach § 202c StGB vorliegt, zu erhärten oder zu widerlegen versuchen. Vor diesem Hintergrund wurde dieser Leitfaden erstellt.

Zielgruppe dieser Empfehlung sind daher einerseits alle Personen, die mit entsprechenden Computerprogrammen umgehen, sei es als Forscher, Programmierer, Sicherheitsberater, System-Administrator oder Anwender, und andererseits diejenigen Personen, denen die Bewertung der Strafbarkeit obliegt, also Ermittler, Gutachter, Staatsanwälte, Verteidiger und Richter.

2 Wie ist dieses Dokument zu nutzen?

Dieses Dokument hat zwei unterschiedliche Zielgruppen.

- Zum einen sollen sich **Personen, die sich im Rahmen der Strafverfolgung mit dem § 202c StGB auseinandersetzen müssen**, einen detaillierten Überblick über die Funktionen und Einsatzgebiete von Software-Werkzeugen verschaffen können, die im Rahmen der IT-Sicherheit zum Einsatz kommen (Kapitel 3 und 4).

- Auf der anderen Seite sollen Personen, **die beruflich mit dem Thema IT-Sicherheit befasst** sind, auf wichtige Vorsichtsmaßnahmen hingewiesen werden. Diese wurden in Kapitel 5 als Best Practice zusammengestellt.

Um dem Leser eine bessere Orientierung im Dokument zu geben, folgt nun eine kurze Übersicht über die nachfolgenden Kapitel:

Das in Kapitel 3 vorgestellte Bewertungsschema soll helfen eine Software[1] hinsichtlich seiner Relevanz bezüglich der Strafbarkeit einzuordnen. Die Verfasser dieses Dokuments schlagen hierfür einen Dreierschritt vor:

- 1. Funktionen einschätzen
- 2. Einsatzzweck feststellen
- 3. Intention der handelnden Person ermitteln

Nach Prüfung dieser drei Schritte steht mit hoher Wahrscheinlichkeit fest, ob im Einzelfall eine strafbare Handlung zu vermuten ist.

In Kapitel 4 werden Beispiele für den Einsatz von Sicherheitstools skizziert. Dies soll dem Leser das Thema noch anschaulicher darstellen.

In Kapitel 5 werden Hilfestellungen für die zweite Adressatengruppe dieser Publikation vorgestellt. Diese bekommt hier Hinweise für ein Best Practice im Umgang mit entsprechenden Programmen.

1 Die Begriffe „Software“, „Tool“ und „Programm“ werden in dieser Publikation synonym verwendet.

3 Bewertungsschema

Ob der Umgang mit einer Software als strafbar zu bewerten ist, ist von mehreren Faktoren abhängig. Einerseits spielen die tatsächlichen **Funktionen** der Software (auch die Kombination bestimmter Funktionen) eine Rolle. Darüber hinaus ist aber auch **der Einsatzzweck** von Bedeutung. Und schließlich lässt sich aus der **Intention** des Nutzers ableiten, ob hier ein Straftatbestand gemäß §§ 202 c StGB vorliegt. Die Verfasser dieses Dokuments schlagen daher drei Schritte vor, mit denen konkrete Anlässe betrachtet werden sollten.

Schritt 1: Funktionen einschätzen

Um eine Software richtig bewerten zu können, müssen zunächst die Funktionen der Software betrachtet werden. Erst danach kann eine Einschätzung getroffen werden, ob diese Software zur Begehung einer Straftat nach §§ 202 a/b oder §§ 303 a/b StGB geeignet ist. Die Einordnung der Einzelfunktionen kann nach einem sehr einfachen Schema erfolgen:

- Kritisch
  Diese Funktion ist zur Begehung einer Straftat geeignet.
- Unkritisch
  Diese Funktion ist nicht zur Begehung einer Straftat geeignet.

Der Anwender der nachfolgenden Bewertungsmatrix kann in diesem Abschnitt schnell alle Programme aussortieren, deren Funktionen nicht „kritisch“ sind.

Die hier aufgeführten Funktionen gelten insbesondere immer dann als „kritisch“, wenn sie ohne Einwilligung oder Benachrichtigung des legitimen Nutzers des IT-Systems ausgeführt werden können.

Von besonderer Bedeutung ist hier auch die Formulierung „dem angegriffenen Rechner“ Es handelt sich hier um ein IT-System, das dem Nutzer der fraglichen Software nicht gehört bzw. nicht zu seiner legitimen Nutzung überlassen wurde oder bei dem er die legitime Nutzung überschreitet.

Software-Funktion	kritisch	unkritisch
Öffnen einer Kommandozeile auf dem angegriffenen Rechner zur Ausführung eines oder mehrerer Befehle	X	
Installation von Software zur Fernsteuerung oder nicht berechtigte Nutzung des angegriffenen Rechners	X	
Einbringen von eigenem Code durch den Angreifer / Angriffs-Software	X	
Ändern oder Löschen der Daten auf dem angegriffenen Rechner	X	
Auslesen der Daten auf dem angegriffenen Rechner	X	
Starten/Stören/Deaktivieren des angegriffenen Rechners oder seiner Dienste	X	
Angriff anderer Rechner bzw. Unterstützung oder Koordination solcher Angriffe	X	
Analyse von Software-Abläufen (Debugger, Disassembler)		X
Automatisierter Test von Software, um Verhalten im Fehlerfall zu dokumentieren (Fuzzer)		X
Passworte reproduzieren oder erraten	X	
Entschlüsselung von verschlüsselten Daten	X	
Änderung oder Einrichtung von Benutzerkonten und Änderung der Sicherheitskonfiguration	X	
Aufzeigen aktiver Geräte und Dienste im Netz (Portscanner)		X

Software-Funktion	kritisch	unkritisch
Aufzeigen von Sicherheitsschwachstellen im Netz oder in Applikation (Vulnerability-Scanner)		X
Selbstpropagierender Code (sich selbst weiter verbreitender Schadcode - Viren, Würmer, etc inkl. Baukästen)	X	
Umleiten von Netzwerkverkehr	X	
Mithören von Netzwerkverkehr	X	

Schritt 2: Einsatzzweck feststellen

Falls im Schritt 1 die Software mit ihren Funktionen als insgesamt kritisch eingestuft wurde, sollte im zweiten Schritt der primäre Einssatzzweck betrachtet werden. Auch hier kann die Software in der Regel schnell zugeordnet werden.

Einsatzzweck	kritisch	unkritisch
Verwendung von regulär angebotenen Internetapplikationen (z.B. Browser, E-Mail)		X
Technische Qualitätssicherung		X
Administration von Netzen und IT-Systemen (Installation, Betrieb, Wartung)		X
Sicherheitsadministration	X	
Sicherheitstests (Penetrationstest, Entschlüsselung, IT-Forensik, ...)	X	
Sicherheitsforschung (Wirkung von Schadsoftware, ...)	X	

Schritt 3: Intention der handelnden Person ermitteln

Sollte die Software in einem als kritisch eingestuften Szenario zum Einsatz kommen, wäre in einem dritten Schritt die Intention des Anwenders zu hinterfragen. Bestimmte Handlungen beim Umgang mit dieser Software können als Indiz für die **fehlende Intention**, eine Straftat vorzubereiten, gewertet werden. Mögliche Absichten der handelnden Person sind in diesem Abschnitt aufgeführt.

Die nachfolgende „White List“ ist nicht vollständig, sondern stellt häufig vorkommende Beispiele dar:

- Beauftragung durch den Angegriffenen
- Erfüllung des Geschäftszwecks (z.B. als Sicherheitsberater, Softwarehaus)
- Information an den Hersteller über Sicherheitslücken in dessen Produkten (z.B. im Rahmen eines Responsible Disclosure[2])
- Austausch der Ergebnisse unter Sicherheitsexperten
- Realisierung von Software als „Proof of Concept“[3]
- Weitreichende Veröffentlichung (z.B. innerhalb der Responsible Disclosure)

2 Erläuterung „Responsible Disclosure“: Nach den Grundsätzen der Responsible Disclosure wird nach dem Finden einer Schwachstelle als erstes der Hersteller informiert. Nach einer angemessenen Frist wird die Schwachstelle und die diese ausnutzende Software veröffentlicht. Der Hersteller soll damit die Möglichkeit bekommen, das Problem zu beheben, indem er eine neue, sichere Version seiner Software erstellt. Auch soll der Hersteller dadurch in der Lage versetzt werden, die Anwender über die neue Version der Software zu informieren und sie an die Anwender zeitnah auszuliefern.
Die Information über die Schwachstelle und wie man sie ausnutzt sowie die Software zum Ausnutzen wird vom Autor in elektronischen Medien mit hoher Verbreitung (z.B. „Bugtraq“, „Full-Disclosure“ oder spezialisierte Webseiten) öffentlich gemacht.
Wenn der Ersteller einer sicherheitsrelevanten Software bei ihrer Verteilung den Regeln der „Responsible Disclosure“ folgt, kann in der Regel davon ausgegangen werden, dass er damit die Sicherheit im Internet zu verbessern sucht

3 Unter „Proof of Concept“ versteht man den Nachweis der Existenz und schwere einer Schwachstelle

4 Beispiele zur Anwendung

An folgenden, konkreten Beispielen soll eine Einschätzung von mehreren Typen von Programmen exemplarisch durchgeführt werden. Es wird eine kurze Einleitung mit einer Beschreibung der Software gegeben und die daraus folgende Einschätzung nach dem Bewertungsschema in Kapitel 3 dargestellt.

4.1 Passwort-Cracker

Diese Software wird entwickelt, um verschlüsselte Passwörter oder Schlüssel zur Dateiverschlüsselung auf ausreichenden Schutz zu untersuchen. Die Software nutzt entweder Fehler im eingesetzten Algorithmus aus oder probiert eine große Anzahl möglicher Schlüssel oder Passwörter („Brute Force Attacke"). Durch beide Ansätze werden Schlüssel und Passwörter gefunden, die nicht ausreichend komplex sind, um den notwendigen Schutz sicher zu stellen. Die Software gibt für jeden Schlüssel oder jedes Passwort eine Meldung aus, ob es erraten werden konnte. Zur Überprüfung der Sicherheit von komplexen Installationen ist es teilweise notwenig auch den gefundenen Schlüssel oder das gefundene Passwort im Klartext anzuzeigen. Diese Funktion haben die meisten derartigen Programme.

Funktionen	Bewertung
Passwörte reproduzieren oder erraten	Kritisch
Entschlüsselung von verschlüsselten Daten	Kritisch
Erläuterung	
Nach dem Bewertungsschema weist die Software klar Funktionen auf, die als kritisch anzusehen sind. Nur der Inhaber der Daten oder der Benutzer des Zugangs, für den das Passwort gebrochen wird, darf eine solche Maßnahme durchführen oder durchführen lassen.	

Einsatzzweck	Bewertung
Die Software kann für Penetrations-Tests und Angriffe nach §§ 202 a/b und §§ 303 a/b StGB eingesetzt werden.	Kritisch
Erläuterung	
Da dieses Tool im Rahmen eines strafrechtlich unbedenklichen Penetrationstests, aber auch für kriminelle Aktivitäten eingesetzt werden kann, ist der Einsatzzweck als kritisch einzustufen.	

Intention	Bewertung
Viele Administratoren und alle Sicherheitsberater benötigen diese Funktion für ihre Arbeit. Auch für private Anwender ist der Test, ob ein gewähltes Passwort sicher ist, empfehlenswert und wird häufig durchgeführt	Unkritisch
Erläuterung	
Die Überprüfung der Passwört-Güte dient der Verbesserung des Zugangsschutzes. Besitzer verschlüsselter Daten können mit diesem Tool zudem bei Verlust des Passworts die Verfügbarkeit ihrer Informationen sicherstellen.	

Zusammenfassung	Abschl. Bewertung
Im Regelfall ist von einer legitimen Nutzungsabsicht auszugehen. Der Besitz dieses Tools allein begründet keinen Verdacht auf einen Verstoß gegen § 202 c StGB.	Unkritisch

4.2 Portscanner / Vulnerability Assessment

Portscanner sind Programme, die dem automatisierten Finden von Schwachstellen dienen. Die Software will entweder im Netzwerk einer Organisation alle IT-Systeme (z.B. PCs, Server, Router, Firewalls, etc) finden, auf denen Software mit bekannten Sicherheitslücken installiert ist, oder für alle IT-Systeme feststellen, welche Dienste diese IT-Systeme anbieten.

Auch Details der Konfiguration, wie Netzwerkadresse, Ort der Aufstellung (physisch und im Netzwerk) oder weitere Netzwerkparameter können mit dieser Software in Erfahrung gebracht werden.

Funktionen	Bewertung
Aufzeigen aktiver Geräte und Dienste im Netz (Portscanner)	Unkritisch
Aufzeigen von Sicherheitsschwachstellen im Netz oder in Applikation (Vulnerability Scanner)	Unkritisch
Erläuterung	
Vulnerability Assessment bzw. Portscanning wird in sicherheitsbewussten IT-System-Verwaltungen, sowie in der Überprüfung der IT-Sicherheit durch Sicherheitsberater (z.B. Penetrationstests) ständig durchgeführt.	

Zusammenfassung	Abschl. Bewertung
Derartige Software dient der Verbesserung der Sicherheit und ist nicht von vornherein für ein Verfahren nach §§ 202 c StGB relevant.	Unkritisch

4.3 Software Analyse Werkzeuge

Derartige Werkzeuge können zur Suche nach neuen Verwundbarkeiten von Anwendungen genutzt werden. Die zu untersuchende Software wird von dieser Software auf unterschiedliche Art und Weise untersucht. Die Vorgehensweise ist von der zu untersuchenden Software abhängig.

Generell können die folgenden Typen von Software zur Analyse unterschieden werden:

- Fuzzer
  Die zu untersuchende Software wird mit Hilfe von durch die Fuzzing-Software erzeugten Eingaben aufgerufen. Die Eingaben sollen Fehler in der zu untersuchenden Software auslösen.
- Disassembler
  Eine als Maschinencode vorliegende Software wird in eine für Menschen lesbare Form gebracht. Mit automatisierten Mechanismen wird nach potentiellen Sicherheitsproblemen gesucht.
- Debugger
  Eine als Maschinencode vorliegende Software wird durch Eingaben dazu gebracht Fehler zu machen. Durch den Debugger kann erforscht werden, ob der Fehler der Software als Sicherheitslücke ausgenutzt werden kann.

Funktionen	Bewertung
Analyse von Software-Abläufen (Debugger, Disassembler)	Unkritisch
Automatisierter Test von Software, um Verhalten im Fehlerfall zu dokumentieren (Fuzzer)	Unkritisch
Erläuterung	
Diese Arten von Software sind bei Forschern und Sicherheitsberatern ständig im Einsatz	

Zusammenfassung	Abschl. Bewertung
Derartige Software dient zur Verbesserung der Sicherheit und ist nicht von vornherein für ein Verfahren nach §§ 202 c relevant.	Unkritisch

4.4 Zero-Day Exploits

Ein „Zero-Day Exploit“ ist eine Software, die noch nicht allgemein bekannte Sicherheitslücken ausnutzt, um in fremde IT-Systeme einbrechen zu können. Die Software, wie auch das Wissen um die Schwachstelle, werden geheim gehalten. Der Hersteller erhält damit keine Chance, das Problem zu beheben und eine korrigierte Version der verwundbaren Software an seine Kunden zu verteilen (sog. „Patch“).

Funktionen	Bewertung
Öffnen einer Kommandozeile auf dem angegriffenen Rechner, um einen oder mehrere Befehle auszuführen	Kritisch
Einbringen von eigenem Code durch den Angreifer / Angriffs-Software	Kritisch
Erläuterung	
Nach dem Bewertungsschema weist die Software klar mehrere Funktionen auf, die als kritisch anzusehen sind.	

Einsatzzweck	Bewertung
Die Software kann für Angriffe nach §§ 202 a/b und §§ 303 a/b StGB eingesetzt werden. Eine Verwendung bei Penetrationstests ist kaum möglich, da die Software nicht frei verfügbar ist.	Kritisch

Intention	Bewertung
Es ist keiner der oben aufgeführten Hinweise auf eine fehlende Intention eine Straftat durchzuführen oder vorzubereiten erkennbar.	Kritisch
Erläuterung	
Besonders die Verteilung einer solchen Software ist ein Indiz: Der Hersteller der verwundbaren Software wird nicht über die Sicherheitslücke informiert, da diese Lücke ausgenutzt werden soll. Die Verteilung findet in kleinem Kreis statt. Mitglieder einer Gruppe geben Software dieser Art ausschließlich untereinander weiter	

Zusammenfassung	Abschl. Bewertung
Funktionen, typischer Einsatzzweck und Art der Verbreitung legen den Verdacht nahe, dass die Absicht besteht, eine Straftat zu begehen und nicht die Sicherheit des Internets zu verbessern. Ein Verfahren nach §§ 202 c StGB ist angebracht.	Kritisch

5 Best Practice – Leitfaden für Anweisungen in Unternehmen

5.1 Prinzipielle organisatorische Regelungen im Unternehmen

- Interne Tests brauchen einen klaren internen Auftrag durch das Management und einen klar definierten internen Personenkreis, der diese durchführen darf.
- Die Durchführung von Tests und der Umgang mit entsprechender Software sollten in der offiziellen Aufgabenbeschreibung oder Rollenbeschreibungen des Mitarbeiters oder aber der Abteilung niedergelegt sein.
- Toolset, Scanpolicies und Lizenzen werden durch eine hierfür verantwortliche Abteilung gepflegt und zur Verfügung gestellt
- Die bei Sicherheitsuntersuchungen eingesetzten Werkzeuge sollen nur für den mit Sicherheitstests beauftragten Personenkreis zur Verfügung gestellt werden.
- Eine Nutzung selbsterstellter oder extern beschaffter Tools außerhalb der dienstlichen Tätigkeit ist nicht erlaubt.
- Die Durchführung interner Penetrationen und die Weitergabe von Passworten durch interne Stellen betreffen auch arbeitsrechtliche bzw. betriebsverfassungsrechtliche Aspekte und sind entweder durch eine Stellen- bzw. OE-Aufgaben-Beschreibung vorgegeben oder durch ein anderes Gremium zu genehmigen.

5.2 Vorbereitung des Tests

- Die Beschaffung und der Test von sog. Hackertool auf Test-IT-Systemen, können als weniger kritisch bewertet werden, sollten aber mit der jeweiligen Führungskraft abgestimmt sein.
- Bei der Durchführung von Tests ist besondere Sorgfalt geboten, um die Schädigung Dritter zu vermeiden. Hierzu ist schon bei der Vorbereitung auf die Auswahl geeigneter Tools und Werkzeuge zu achten.
- Dem Test muss ein mit dem Systemeigner abgestimmter Testplan zugrunde liegen.
- Vor Testbeginn muss das Einverständnis des Systemeigners eingeholt werden.

5.3 Testdurchführung

- Tests für interne oder externe Kunden dürfen erst nach schriftlicher Beauftragung durch den Kunden begonnen werden.
- Der Auftrag muss dabei Angaben zur Art und Umfang der geplanten Tests sowie eine genaue Benennung der zu testenden IT-Systeme beinhalten. Weiterhin ist die Benennung der Mitarbeiter, die mit der Testdurchführung betraut sind, erforderlich.
- Zum Nachweis der Sorgfalt sind aussagekräftige Protokolle während der Testdurchführung anzulegen, aus denen insbesondere das Testziel und möglichst die Konfigurationsdaten der eingesetzten Testwerkzeuge ersichtlich sind.
- Die Rechner, von denen aus Scans durchgeführt werden, sind sorgfältig zu sichern. Insbesondere sind die Scan-Ergebnisse gegen einen Zugriff durch unbefugte Dritte zu schützen.
- Erfolgt eine Testdurchführung nicht aus den Räumlichkeiten des beauftragten Unternehmens, sollten die Mitarbeiter, die mit der Testdurchführung betraut worden sind, im eigenen Interesse eine Kopie des Auftrages mit sich führen. Diese Kopie dient als Nachweis des Auftrages für den Fall strafrechtlicher Ermittlungen vor Ort.
- Sofern es erforderlich ist, für die Durchführung von Testaufträgen nicht dienstliche Accounts zu verwenden, muss durch eine geeignete Dokumentation der dienstliche Bezug erkennbar sein.

- Tests, die Verhaltenskontrollen von Mitarbeitern oder Einsicht in deren private Daten ermöglichen, müssen genehmigt werden. Hierfür ist in der Regel die Arbeitnehmervertretung einzubeziehen.
- Alle Informationen im Zusammenhang mit dem Test unterliegen der Geheimhaltungsverpflichtung. D.h. sie dürfen nur zu den Zwecken verwendet werden, zu denen sie erlangt wurden, und sie dürfen wie eigene Betriebsgeheimnisse gegenüber Dritten nicht zugänglich gemacht werden.
- Einschlägige gesetzliche Regelungen sind zu beachten (z. B. in Deutschland: Datengeheimnis gemäß § 5 Bundesdatenschutzgesetz (BDSG), Fernmeldegeheimnis gemäß § 88 und 89 Telekommunikationsgesetz (TKG), Abhörverbot/Geheimhaltungspflicht der Betreiber von Empfangsanlagen gemäß § 86 TKG).

5.4 Testabbruch bei versehentlicher Schädigung Dritter

- Sollte bei der Testdurchführung versehentlich in ein Netz oder ein System eines Dritten eingedrungen worden sein, so muss der Test sofort abgebrochen werden.
- Der betroffene Dritte ist, sofern identifizierbar, unverzüglich zu informieren und bei der Behebung von eventuellen Schäden zu unterstützen.
- Die Ursache des Fehlers bei der Testdurchführung ist zu analysieren.
- Der Gesamtvorgang muss dokumentiert werden, insbesondere was zur Schadensbegrenzung unternommen wurde und aus welchen Gründen der Mitarbeiter davon ausging, dass er einen Dritten nicht treffen würde.
- Ergibt sich im Verlauf eines Tests die Möglichkeit zum Zugriff auf Daten Dritter (z.B. Kundenanwendungen auf Hostingplattformen) so darf auf diese Daten nicht zugegriffen werden. Für derartige Analysen auf den eigenen Plattformen sollten „Testkunden“, ausschließlich zum Zweck der Testdurchführung, angelegt werden.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.200 Unternehmen, davon 900 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org