Cybercrime-Straftatbestände

Ausspähen von Daten

Abfangen von Daten

Vorbereiten des Ausspähens und Abfangens von Daten

Datenveränderung

Fälschung beweiserheblicher Daten

Computerbetrug

Computersabotage

Bundeskriminalamt

Herausgeber

Bundeskriminalamt
Referat SO41
65173 Wiesbaden
Tel.: 0611/55-15873
E-Mail: SO41-NKC@bka.bund.de

Gestaltung: Agentur Luh Media, www.luh-media.de – Fotos: S.1 Luh Media, S. 21 Franz Pfluegl, www.fotolia.de

Bundeskriminalamt

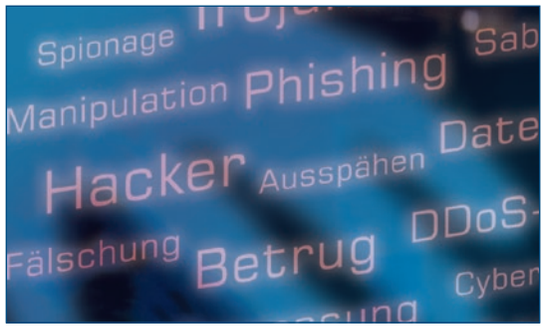
Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime

cybercrime

Handlungsempfehlungen

für die Wirtschaft

in Fällen von Cybercrime



[1] Eine vergleichbare Studie der IHK Schleswig-Holstein und dem LKA Schleswig-Holstein aus dem Jahre 2008 kam zu dem Ergebnis, dass 96% der Unternehmen keine Strafanzeige erstatteten

[2] Die Definition der KPMG zu e-Crime – analog zu Cybercrime – aus 2010 lautet folgendermaßen: „e-Crime bezeichnet die Ausführung von wirtschaftskriminellen Handlungen unter Einsatz von IKT-Systemen zum Schaden eines Unternehmens. Dies kann zur Verletzung von Sachwerten sowie Verfügungsrechten an immateriellen Gütern führen und/oder die auf IKT-Systeme basierenden Prozesse eines Unternehmens beeinträchtigen."

[3] Damit die Handlungsempfehlung lesbar bleibt, wird auf eine explizite Nennung der weiblichen Form im Weiteren verzichtet. Sämtliche Ausdrücke die männlich formuliert sind, gelten sinngemäß auch für Frauen.

[4] Gemäß der Cybercrime Konvention des Europarates aus dem Jahr 2001 sind u. a. nachfolgende Straftaten vom Begriff der Cybercrime umfasst:
- Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -Systemen
- Computerbezogene Straftaten (computerbezogene Fälschung und Betrug).

Zentrale Ansprechstellen der Polizeien des Bundes und der Länder für Cybercrime:

Bundeskriminalamt
Referat SO41
65173 Wiesbaden
Tel.: 0611/55-15684
E-Mail: SO41-NKC@bka.bund.de
Internet: www.bka.de

Bayerisches Landeskriminalamt
SG 541 – Zentralstelle Cybercrime
Maillinger Str. 15
80636 München
Tel.: 089/1212-3300
E-Mail: zac@polizei.bayern.de

Landeskriminalamt Baden-Württemberg
Zentrale Ansprechstelle Cybercrime
Taubenheimstraße 85
70372 Stuttgart-Bad Cannstatt
Tel.: 0711/5401-2444
E-Mail: cybercrime@polizei.bwl.de

Landeskriminalamt Berlin
LKA 24
Martin-Luther-Str. 105
10825 Berlin
Tel.: 030/4664-924924
E-Mail: zac@polizei.berlin.de

Landeskriminalamt Brandenburg
LKA 121 –
Dezernat Cybercrime
Tramper Chaussee 1
16225 Eberswalde
Tel.: 03334/388-8600
E-Mail: cybercrime.fdlka@polizei.brandenburg.de

Landeskriminalamt Bremen
K53 / IuK - Kriminalität
In der Vahr 76
28329 Bremen
Tel.: 0421/362-19820
E-Mail: k53@polizei.bremen.de

Landeskriminalamt Hamburg
LKA 54
Bruno-Georges-Platz 1
22297 Hamburg
Tel.: 040/4286-75401
E-Mail: zac@polizei.hamburg.de

Landeskriminalamt Hessen
SG 331 – Zentrale Ansprechstelle Cybercrime
Hölderlinstraße 5
65185 Wiesbaden
Tel.: 0611/83-3377
E-Mail: zac.hlka@polizei.hessen.de

Landeskriminalamt Niedersachsen
Zentrale Ansprechstelle Cybercrime
Am Waterlooplatz 11
30169 Hannover
Tel.: 0511/26262-3804
E-Mail: zac@lka.polizei.niedersachsen.de

Landeskriminalamt Nordrhein-Westfalen
Zentrale Ansprechstelle Cybercrime
Völklinger Str. 49
40221 Düsseldorf
Tel.: 0211/939-4040
E-Mail: cybercrime.lka@polizei.nrw.de

Landeskriminalamt Mecklenburg-Vorpommern
Retgendorfer Str. 09
19067 Rampe
Tel.: 03866/64-4517
(Hotline im Regeldienst)
E-Mail: cybercrime.lka@polmv.de

Landeskriminalamt Rheinland-Pfalz
Dezernat 47 – Cybercrime
Valenciaplatz 1-7
55118 Mainz
Tel.: 06131/65-2565
E-Mail: lka.cybercrime@polizei.rlp.de

Landespolizeipräsidium Saarland
Direktion LPP 222
Zentrale Ansprechstelle Cybercrime
Hellwigstraße 8–10
66121 Saarbrücken
Tel.: 0681/962-2448
E-Mail: cybercrime@polizei.slpol.de

Landeskriminalamt Sachsen
Zentrale Ansprechstelle Cybercrime
Neuländer Str. 60
01129 Dresden
Tel.: 0351/855-3461
E-Mail: zac.lka@polizei.sachsen.de

Landeskriminalamt Sachsen-Anhalt
Cybercrime Competence Center
Lübecker Str. 53–63
39124 Magdeburg
Tel.: 0391/250-2244
E-Mail: ermittlungen.4c@polizei.sachsen-anhalt.de

Landeskriminalamt Schleswig-Holstein
Zentrale Ansprechstelle Cybercrime
Sachgebiet 231
Mühlenweg 166
24116 Kiel
Tel.: 0431/160-4545
E-Mail: cybercrime@polizei.landsh.de

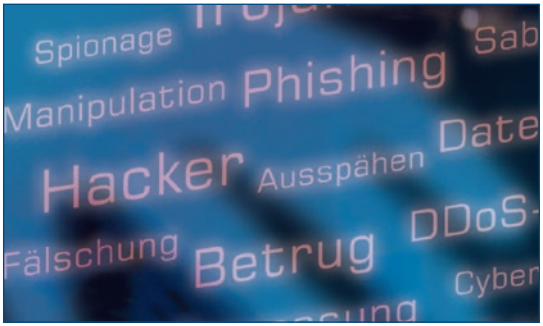
Landeskriminalamt Thüringen
Zentrale Ansprechstelle Cybercrime Dezernat
Kranichfelder Straße 1
99097 Erfurt
Tel.: 0361/341-1425
E-Mail: cybercrime.lka@polizei.thueringen.de

Cybercrime

Handlungsempfehlungen

für die Wirtschaft

in Fällen von Cybercrime



[1] Eine vergleichbare Studie der IHK Schleswig-Holstein und dem LKA Schleswig-Holstein aus dem Jahre 2008 kam zu dem Ergebnis, dass 96% der Unternehmen keine Strafanzeige erstatteten

[2] Die Definition der KPMG zu e-Crime – analog zu Cybercrime – aus 2010 lautet folgendermaßen: „e-Crime bezeichnet die Ausführung von wirtschaftskriminellen Handlungen unter Einsatz von IKT-Systemen zum Schaden eines Unternehmens. Dies kann zur Verletzung von Sachwerten sowie Verfügungsrechten an immateriellen Gütern führen und/oder die auf IKT-Systeme basierenden Prozesse eines Unternehmens beeinträchtigen."

[3] Damit die Handlungsempfehlung lesbar bleibt, wird auf eine explizite Nennung der weiblichen Form im Weiteren verzichtet. Sämtliche Ausdrücke die männlich formuliert sind, gelten sinngemäß auch für Frauen.

[4] Gemäß der Cybercrime Konvention des Europarates aus dem Jahr 2001 sind u. a. nachfolgende Straftaten vom Begriff der Cybercrime umfasst:
– Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -Systemen
– Computerbezogene Straftaten (computerbezogene Fälschung und Betrug).

Eine 2013 von der Industrie- und Handelskammer (IHK) Nord durchgeführte Befragung von 713 Unternehmen kommt zu dem Ergebnis, dass auf 33% der befragten Unternehmen in den vorangegangenen 12 Monaten ein oder mehrere Cyber-Angriffe durchgeführt worden sind. Die Angriffsrate war hierbei relativ gleichmäßig auf alle Branchen verteilt (33,3% der Angriffe gegen Industrie und Handel, 32,8% auf die Dienstleistungswirtschaft). Bei einer Differenzierung nach der Betriebsgröße ist eine leichte Tendenz zur Betroffenheit größerer Unternehmen (>250 Mitarbeiter) zu verzeichnen. Das Anzeigeverhalten der betroffenen Unternehmen ist hierbei weiterhin schwach ausgeprägt, wenngleich eine Verbesserungstendenz festgestellt werden kann[1]. Nur 5,9% der befragten Unternehmen erstatteten im Untersuchungszeitraum nach eigenen Angaben in allen Angriffsfällen Strafanzeige, weitere 2,9% taten dies in der Mehrheit der Angriffsfälle und weitere 4,4% erstatteten in weniger als der Hälfte der bekannten Angriffsfälle Strafanzeige.

Auch die „e-Crime[2] Studie 2015" der Wirtschaftsprüfungs- und Beratungsgesellschaft KPMG bestätigt eine hohe Betroffenheit der deutschen Wirtschaft durch Delikte der e-Crime. Demnach waren in dem zweijährigen Untersuchungszeitraum 40% aller 505 befragten Unternehmen von entsprechenden Delikten betroffen. KPMG stellt hierbei eine besondere Betroffenheit der Finanzdienstleister fest (55% der Unternehmen aus dem Finanzsegment waren nach eigenen Angaben betroffen, bei den übrigen Dienstleistungen waren es lediglich 33%).

Insgesamt sehen 89% der Umfrageteilnehmer/-innen[3] Cybercrime[4] als tatsächliches Risiko für ihre Unter-

nehmen an. 70% rechnen ferner damit, dass die Risiken in Zukunft weiter steigen werden.

Festgestellt werden kann, dass von einer erhöhten Professionalisierung und Internationalisierung von Cyberstraftaten ausgegangen wird. 90 % der Befragten vertraten die Ansicht, dass die entsprechenden Tathandlungen komplexer und schwerer zurückzuverfolgen sind. Des Weiteren ist seitens der Unternehmen ein Rückgang des Vertrauens in die eigene Reaktionsfähigkeit zu erkennen. Abhängig von der Branche äußerten 18-44% der befragten Unternehmen, dass Versäumnisse in der Reaktionsphase auf Fälle von e-Crime gemacht wurden (Fußnote einfügen: in der Vorgängerstudie 2013 äußerten noch 99% der Unternehmen, auf Cyber-Angriffe stets richtig reagiert zu haben).

Obgleich die Unternehmen stärker in vorbereitende Sensibilisierungs- und Schulungsmaßnahmen investierten, wird weiterhin von einer Vielzahl der befragten Unternehmen eine starke Unachtsamkeit (88%) und ein mangelndes Risikoverständnis (77%) der Mitarbeiter festgestellt.

Aus diesem und weiteren Gründen wissen oder bemerken Unternehmen häufig nicht, dass sie Opfer einer Straftat aus dem Bereich der Cybercrime geworden sind. Aber selbst wenn solche Straftaten festgestellt werden, gelangen diese nur in wenigen Einzelfällen zur Anzeige und somit zur Kenntnis der Sicherheits- und Strafverfolgungsbehörden.

Nach Gesprächen mit einigen Wirtschaftsvertretern und aus den o. a. Umfragen sind die nachfolgenden Gründe ursächlich für die Nichterstattung von Anzeigen:

- Es handelt sich oftmals um Innentäter, so dass eine firmeninterne Regulierung bevorzugt wird.
- Die Angriffe werden abgewehrt bzw. bleiben erfolglos.
- Häufig sind zunächst keine Schäden erkenn- oder messbar.
- Fehlende Sensibilisierung/Awareness bei den Verantwortlichen auf Leitungsebene
- Keine Anzeigen aus Sorge vor Imageschäden durch befürchtete Presseveröffentlichungen.
- Befürchtete negative Auswirkungen unter Konkurrenz-/Wettbewerbsaspekten.
- Die Strafverfolgung dauert aus Sicht der Unternehmen zu lange bzw. es wird die Erfolglosigkeit der polizeilichen Ermittlungen angenommen.
- Insbesondere kleinere Firmen befürchten, dass die Polizei Firmenrechner sicherstellt und diese erst nach einem längeren Zeitraum wieder aushändigt.
- Teilweise verfügen Unternehmen nicht über lizenzierte Software, so dass die Angst vor einem Strafverfahren gegen die Firma überwiegt. Gleiches gilt bei einem bekannten oder angenommenen Vorhandensein illegaler Dateien auf den Computern oder Profilen einzelner Beschäftigter der Firma.

Aus Sicht der Polizeibehörden verhindern die zuvor genannten Gründe einen offeneren Umgang mit dem Thema und damit letztlich eine erfolgreichere Bekämpfung der Cybercrime.

Ziel:

Mit dieser Broschüre möchte Ihnen die deutsche Polizei eine Hilfestellung bieten, wenn Sie – selbst unter Beachtung einschlägiger Sicherheitsempfehlungen[5] – in Ihrem Unternehmen von Cybercrime-Straftaten betroffen sind.

Wir wollen Ihnen Empfehlungen zum Umgang mit solchen Angriffen geben, Sie dazu ermutigen, solche strafrechtlich relevanten Vorfälle bei Ihrer Polizei anzuzeigen und Sie auch darüber informieren, was Sie in solchen Fällen von uns erwarten können.

[5] Z. B. zum IT-Grundschutz; herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik (BSI).

2.1 Polizeiliche Zuständigkeiten

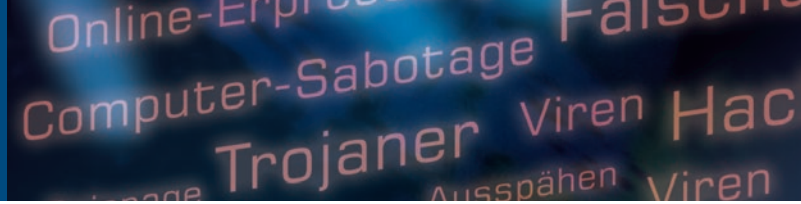
Bei den Landespolizeien werden Cybercrime-Delikte in der Regel durch örtliche Fachdienststellen bearbeitet oder – z. B. bei schwerwiegenden und überregionalen Fällen – auch durch das jeweilige Landeskriminalamt (LKA).

Das Bundeskriminalamt (BKA) unterstützt die Polizeien der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder sonst erheblicher Bedeutung. In bestimmten Fällen kann auch das BKA selbst die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung wahrnehmen und Ermittlungsverfahren führen.

2.2 Gesetzesgrundlagen

Mit dem Inkrafttreten der Cybercrime Konvention in Deutschland am 01.07.2009 wurde das deutsche Strafrecht an die aktuellen Entwicklungen im Bereich der Internet- und Computerstraftaten angepasst.

Die folgende Darstellung soll einen Überblick über die einschlägigen Straftatbestände des Strafgesetzbuches (StGB) geben.



Straftatbestände	Inhalt (Kurzbeschreibung)
§202a StGB Ausspähen von Daten	Das unbefugte Verschaffen eines Zugangs zu Daten, die nicht für den Täter bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung.
§202b StGB Abfangen von Daten	Das unbefugte Verschaffen von Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage unter Anwendung von technischen Mitteln.
§202c StGB Vorbereiten des Ausspähens und Abfangens von Daten	Das Vorbereiten einer o. g. Straftat durch das Herstellen, Verschaffen, Verkaufen, Überlassen, Verbreiten oder Zugänglichmachen von Passwörtern, Sicherheitscodes oder Computerprogrammen, deren Zweck die Begehung einer solchen Tat ist.
§263a StGB Computerbetrug	Das Schädigen des Vermögens eines Anderen durch Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf.
Des Weiteren das Vorbereiten einer solchen Tat durch Herstellung, Verschaffung, Feilhalten, Verwahren oder Überlassung eines Computerprogramms, deren Zweck die Begehung einer solchen Tat ist.	
Das Speichern oder Verändern beweiserheblicher Daten zur Täuschung im Rechtsverkehr, so dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder das Gebrauchen solcher Daten.	**§269 StGB Fälschung beweiserheblicher Daten**
Das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten.	**§303a StGB Datenveränderung**
Das erhebliche Stören einer Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, durch 1. Begehung einer Datenveränderung (§ 303a), 2. Eingabe oder Übermittlung von Daten in der Absicht, einem anderen Nachteil zuzufügen, oder 3. Zerstörung, Beschädigung, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers.	**§303b StGB Computersabotage**

3 Verhaltensempfehlungen bei Betroffenheit von Cybercrime-Delikten

Die nachfolgenden Informationen sollen Ihnen Ratschläge und Tipps an die Hand geben, wie Sie sich zunächst im Vorfeld von Cyberangriffen auf solche Szenarien vorbereiten bzw. nach einem eingetretenen Schadensfall verhalten sollten.

3.1 Firmenleitung/Geschäftsführung

Vor Eintritt eines Schadensfalls

Sie sollten in Ihrem Unternehmen bzw. in Ihrem Verantwortungsbereich bereits Verfahrensweisen oder Anleitungen zum Umgang mit Vorfällen bzw. Straftaten aus dem Bereich der Cybercrime vorbereitet haben. Insbesondere sollten die Compliance- und Datenschutzbeauftragten in die Planungen eingebunden werden.

Die Verfahrensweisen oder Anleitungen sind regelmäßig zu überprüfen und allen Mitarbeitern zugänglich zu machen, die Verantwortung für die Systemsicherheit haben. Die Verfahren sollten konkrete Anweisungen insbesondere zu folgenden Punkten enthalten:

1. Wer hat im Unternehmen welche Verantwortung für die interne Reaktion auf einen Schadensfall?
2. Wer ist die Ansprechstelle für interne und externe Kontakte?
3. Wer sollte innerhalb und außerhalb der Firma unmittelbar verständigt werden?
4. An welchem Punkt sollten die Strafverfolgungsbehörden informiert werden?

Hilfreich ist es auch, firmenintern bereits im Vorfeld festzustellen und erforderlichenfalls festzulegen, welche Protokolle bzw. Logdaten ggf. routinemäßig vom System wie lange erfasst und gespeichert werden und somit im Bedarfsfall als Beweismittel zur Verfügung stehen.

Nach Eintritt eines Schadensfalls

Eventuelle Benachrichtigung von weiteren Geschädigten oder Verkäufern
Wenn Sie von einer bestehenden Schwachstelle in einem Produkt bzw. in einem System erfahren, die gerade ausgenutzt wird, sollten sie potentiell Betroffene (z. B. Hersteller/Entwickler, andere Nutzer o. ä.) informieren oder dafür sorgen, dass diese gewarnt werden. Diese sind darüber hinaus vielleicht in der Lage, Informationen über den Zwischenfall bereitzustellen, von denen Sie selbst keine Kenntnis hatten (z. B. verborgene Codes, laufende Ermittlungen in anderen Bereichen). Somit lassen sich damit vielleicht weitere Schäden an anderen Systemen verhindern.

Benachrichtigung von Betroffenen und der zuständigen Aufsichtsbehörde
Wenn von Ihren Systemen bestimmte personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und dadurch schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdige Interessen der Betroffenen drohen, sind Sie gemäß § 42a Bundesdatenschutzgesetz (BDSG) verpflichtet, dieses der zuständigen Aufsichtsbehörde[6] sowie den Betroffenen mit-

[6] Siehe hierzu § 38 Ziffer 6 BDSG. In der Regel handelt es sich dabei um die Datenschutzbeauftragten in den einzelnen Bundesländern.

zuteilen. Die Benachrichtigung der Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen wurden und die Strafverfolgung nicht mehr gefährdet wird.

Melden von Straftaten an Strafverfolgungsbehörden
Wenn Sie im Zusammenhang mit einem Vorfall den Verdacht haben, dass dieser eine Straftat darstellen könnte, sollten Sie sich an die dafür festgelegte bzw. vorgeschriebene Vorgehensweise in Ihrer Firma halten und unverzüglich die zuständige Strafverfolgungsbehörde informieren.

Folgende Umstände können auf das Vorliegen eines strafrechtlich relevanten Sachverhalts hinweisen:

- Ein unberechtigter Nutzer hat sich in das System eingeloggt bzw. nutzt das System.
- Es laufen ungewöhnliche Prozesse auf dem System, die große Mengen an Systemressourcen in Anspruch nehmen.
- Das System ist von einem Schadprogramm (z. B. Virus, Wurm, Trojaner) befallen.
- Ein Nutzer versucht von außerhalb, z. B. durch intensives Portscanning, in das System einzudringen.
- Innerhalb kurzer Zeit erreicht eine große Menge an Datenpaketen (von einem oder verschiedenen Absendern) das System.

3.2 Systemadministratoren

Erste Feststellung und Beurteilung des Zwischenfalls
Zunächst sollte festgestellt werden, wie viele und welche Systeme auf welche Weise betroffen sind. Gute Indikatoren sind Nachweise, dass auf Dateien oder Protokolle zugegriffen wurde, dass Dateien oder Protokolle erstellt, verändert, gelöscht oder kopiert wurden oder dass Nutzerkonten bzw. Nutzerrechte hinzugefügt oder verändert wurden.

Unter Verwendung der Protokollinformationen können nach Möglichkeit

- der unmittelbare Ausgangspunkt des Angriffs,
- die Kennung der Server, zu denen eigene Daten ggf. übertragen wurden und
- die Identität weiterer Geschädigter bestimmt werden.

Sie sollten daran denken, dass ein Eindringling möglicherweise mehrere Programme oder Daten auf dem System installiert hat. Das System kann so mit Schadsoftware verseucht sein, dass es schwierig ist, bestimmte Datei- oder Konfigurationsänderungen zu erkennen.

Es sollte nach Möglichkeit darauf geachtet werden, dass die getroffenen Maßnahmen keine Veränderungen am Systembetrieb oder den gespeicherten Daten herbeiführen, durch die der Angreifer feststellen kann, dass er entdeckt wurde. Durch das Einspielen von Sicherungskopien können zudem Spuren vernichtet werden und es besteht keine Gewähr, dass nicht auch schon die Sicherungskopien durch Schadsoftware kompromittiert wurden.

Maßnahmen zur Minimierung anhaltender Schäden

Zur Unterbindung anhaltender Schädigungen durch einen aktuellen Angriff auf das Netzwerk sollten beispielsweise Filter zur Abwehr von Denial-of-Service-Angriffen installiert oder die betroffenen Systeme vollständig oder teilweise vom Rest des Netzwerkes isoliert werden. Im Fall eines unberechtigten Zugriffs sollte entweder der weitere illegale Zugriff blockiert oder die illegale Handlung beobachtet werden, um die Quelle des Angriffs und/oder das Ausmaß des Schadens festzustellen.

Bei der Abwägung der Handlungsoptionen sollte bedacht werden, dass der Angreifer bemerken könnte, dass er entdeckt wurde. Er könnte seine Spuren auf den Systemen löschen oder möglicherweise auch aus Vergeltung gezielte Angriffe starten, um seinen Zugang zu schützen oder Sie später mit erlangten Firmendaten zu erpressen. Beraten Sie sich daher frühzeitig mit den Entscheidungsträgern in Ihrem Unternehmen, um zu entscheiden, ob ein Abkoppeln des Netzes geschäftlich und rechtlich durchführbar und zweckmäßig ist.

Sie sollten ausführliche Nachweise über die Kosten führen, die der eigenen Firma durch die Maßnahmen zur Begrenzung der Schäden aus dem Angriff entstehen, sowie Nachweise über die konkreten Aktivitäten zur Abmilderung des Angriffs. Diese Informationen können im Hinblick auf die Erlangung von Schadenersatz und für spätere strafrechtliche Ermittlungen von Bedeutung sein.

Verzicht auf ein Eindringen in den Quellcomputer bzw. eine Beschädigung des Quellcomputers

Eigene offensive Gegenmaßnahmen, wie z. B. das Zugangverschaffen zum Computer eines Angreifers können – unabhängig vom Motiv – rechtlich unzulässig sein. Da Angriffe häufig auch von kompromittierten Systemen unwissender Dritter ausgehen, kann durch das „Zurückhacken" somit eventuell das System eines an der Tat letztlich Unschuldigen beschädigt werden.

Wenn erkennbar ist, dass Angriffe aus dem Bereich anderer (als seriös einzuschätzender) Firmen oder Institutionen erfolgen, sollten Sie versuchen, mit den dortigen Verantwortlichen Kontakt aufzunehmen und um Hilfe bei der Abwehr des Angriffs bzw. bei der Feststellung der ursprünglichen Quelle des Angriffs bitten.

Aufzeichnen und Sammeln von Informationen[7]

Erstellen Sie zunächst eine identische Kopie des betroffenen Systems für eine spätere Analyse und als Nachweis für das durch einen Angriff geschädigte System, insbesondere auch zur Aufstellung der entstandenen Schäden und der Kosten für deren Beseitigung. Solche Kopien können bei der Identifizierung von ausgenutzten Schwachstellen, gelöschten Daten und installierten Schadprogrammen sowie zur Unterstützung der Rückverfolgung des Angreifers hilfreich sein. Der Vorteil dieser bitgenauen Sicherungskopien liegt darin, dass sie auch verborgene Dateien und Ver-

[7] Weitergehende Informationen siehe Leitfaden IT-Forensik des BSI – http://www.bsi.bund.de/ContentBSI/Themen/Internet_Sicherheit/IT-Forensik/it-forensik.html.

zeichnisse, Austauschdaten, gelöschte Daten und Informationen im Speicher umfassen, die Hinweise für die Ermittlung des Angreifers geben können. Wenn zu diesem Zeitpunkt bereits der Verdacht auf strafbare Handlungen vorliegt, sollten Sie schon jetzt die Strafverfolgungsorgane informieren, damit diese die Möglichkeit haben, auch Kopien zu forensischen Zwecken anzufertigen (siehe Nr. 4).

Bei Eintritt eines Schadensfalls sollten darüber hinaus Maßnahmen zur Beschreibung und Feststellung aller Ereignisse (Ereignisprotokoll) im Zusammenhang mit dem Schadensfall ergriffen werden. Sie sollten u. a. Folgendes festhalten bzw. veranlassen:

- Sicherung aller relevanten, bereits bestehenden Protokolle bzw. Logdaten.
- Zeitpunkte, d. h. Daten und Uhrzeiten (einschließlich Zeitzone), an denen relevante Ereignisse entdeckt wurden bzw. stattfanden.
- Angaben (Namen, Daten, Uhrzeiten) zu relevanten Telefonanrufen, E-Mails und anderen Verbindungen.
- Identität der Personen, die Aufgaben im Zusammenhang mit dem Schadensfall bearbeiten, eine Beschreibung dieser Aufgaben und der Zeitaufwand.
- Kennung der von dem Angriff betroffenen Systeme, Konten, Dienste, Daten und Netze sowie die Art der Beeinträchtigung.
- Angaben zu Umfang und Art des entstandenen Schadens.

Diesen Nachweisen sollten Kopien aller Systemprotokolldateien und verdächtiger Dateien beigefügt werden. Denken Sie daran, dass Protokolle an verschiedenen Orten abgespeichert sein können (z. B. lokal oder auf zentralen Servern). Die Uhrzeit- und Datumsangaben in den Protokollen sind sehr wichtig, um einen Angreifer zurückzuverfolgen und ihn zu überführen. Daher sollte darauf geachtet werden, dass diese Angaben in den Protokolleinträgen korrekt und mit den jeweiligen Zeitzonen enthalten sind.

Hinweise zum Informationsaustausch

Infizierte Systeme sollten grundsätzlich nicht dazu verwendet werden, um sich über einen Angriff oder die Reaktion darüber auszutauschen. Falls das kompromittierte System (mangels Alternativen) doch für einen Informationsaustausch verwendet werden muss, sollten zumindest alle relevanten Mitteilungen verschlüsselt werden.

Die zuständigen Personen in Ihrer Firma sollten unverzüglich über den Angriff und alle Ergebnisse der bisherigen Analyse informiert werden. Hierzu zählen – gemäß der unter Nr. 3.1.1. im Vorfeld beschriebenen Festlegungen – z. B. Sicherheitskoordinatoren, Manager oder Rechtsberater. Bei Verbindungsaufnahme wird empfohlen, nur geschützte bzw. zuverlässige Kommunikationskanäle zu benutzen. Sollte der Verdacht bestehen, dass der Angreifer ein Insider ist oder eventuell über Insider-Informationen verfügt, können Sie Informationen über den Zwischenfall streng nach dem Grundsatz „Kenntnis nur, wenn nötig“ begrenzen.

4 Zusammenarbeit mit der Polizei

4.1 Anzeigenerstattung

Die Polizei ist sehr an einer vertrauensvollen Zusammenarbeit mit der Wirtschaft interessiert. Jede Polizeidienststelle kann und wird eine Strafanzeige entgegennehmen. Es empfiehlt sich jedoch, sich direkt an die inzwischen in mehreren Bundesländern eingerichteten Fachdienststellen für Cybercrime-Delikte zu wenden. Darüber hinaus stehen auch in vielen Landeskriminalämtern oder im Bundeskriminalamt zentrale Ansprechstellen zur Verfügung. Zur Identifizierung der für Sie geeigneten Ansprechpartner wird bereits im Vorfeld konkreter Anlässe eine Verbindungsaufnahme mit Ihrer für Cybercrime-Delikte zuständigen Fachdienststelle der Polizei empfohlen.

4.2 Ermittlungen und Tatortarbeit

Die Polizei führt auf Grundlage der Strafprozessordnung (StPO) die Ermittlungen zur Erforschung des Sachverhalts im Auftrag der zuständigen Staatsanwaltschaft. Diese besitzt die Verfahrenshoheit bis zu einer späteren Abgabe an das Gericht.

Es ist das Bestreben der Polizei, im Rahmen ihrer Ermittlungs- und Tatortarbeit jede unnötige Erregung firmeninterner oder öffentlicher Aufmerksamkeit oder unnötige Störungen der Geschäfts-/Betriebsabläufe zu vermeiden. So ist die Geschäftsleitung einer Firma grundsätzlich erster Ansprechpartner bei allen polizeilichen Ermittlungstätigkeiten, die in Ihrer Firma stattfinden.

Der Polizei ist die Interessenlage der Firmen zu dem Aspekt „Imageschaden“ bekannt. Dem wird versucht, durch entsprechende Anpassung der polizeilichen Maßnahmen zu begegnen. So ist die Polizei grundsätzlich bestrebt, mit nur so vielen Beamten vor Ort zu erscheinen, wie es für Durchführung der zu treffenden Maßnahmen notwendig ist. Wenn es vermeidbar ist, wird auf den Einsatz von uniformierten Beamten verzichtet. Abhängig von der Ausgangsposition besteht die Möglichkeit, dass der Anzeigenerstatter die Polizei bei der Pforte als Geschäftstermin anmeldet. Neben dem Gespräch mit der Geschäftsführung kann es notwendig sein, Sicherheitsbeauftragte und/oder Systemadministratoren einzubinden. Dann entscheidet sich, ob und inwieweit weitere Beschäftigte der Firma befragt bzw. vernommen werden müssen. Befragungen/Vernehmungen können zur Wahrung der Diskretion wahlweise am Arbeitsplatz oder einem anderen Ort erfolgen.

Als weitere polizeiliche Maßnahmen kann es erforderlich sein, Daten vor Ort von Firmencomputern zu sichern. Dies geschieht in der Regel durch eine so genannte Spiegelung der Daten, d.h., die als grundsätzlich beweisrelevant eingeschätzten Daten der Firma werden vor Ort auf einen von der Polizei mitgebrachten Datenspeicher kopiert. Die Firmencomputer müssen also nicht zwingend sichergestellt bzw. beschlagnahmt werden. Der laufende Betrieb der Firma wird somit im Normalfall nicht weiter beeinträchtigt.

Im Anschluss werden die so sichergestellten Daten insbesondere zur Feststellung tatrelevanter Spuren, zur Gewinnung weiterer Beweismittel bzw. zur Identifizierung von Tatverdächtigen ausgewertet.

Potenzielle Beweismittel, wie z. B. Datenträger, Computerausdrucke oder digital gespeicherte Informationen, können dabei von einer Firma bzw. deren Vertreter als Gewahrsamsinhaber auch freiwillig – ausdrücklich oder stillschweigend – an die Polizei herausgegeben werden. Haben jedoch mehrere Personen Mitgewahrsam, so müssen alle einwilligen, sofern nicht eine alleine verfügungsberechtigt ist.

Im Falle einer solchen freiwilligen Herausgabe oder auch dann, wenn der Gewahrsamsinhaber nicht bekannt ist, stellt die Polizei die Beweismittel in der Regel formlos sicher.

Eine (förmliche) Beschlagnahme ist hingegen grundsätzlich nur dann erforderlich, wenn die Sachen nicht freiwillig vom Gewahrsamsinhaber herausgegeben werden.

Sollte sich der Tatverdacht gegen einen in der Firma beschäftigten Mitarbeiter richten, wird es ggf. erforderlich sein, seinen Arbeitsplatz zu durchsuchen und sein persönliches Netzwerkprofil sowie seinen E-Mail-Account zu sichern. Die Geschäftsleitung wird grundsätzlich über entsprechende Ermittlungshandlungen in der Firma rechtzeitig informiert.

Während laufender Ermittlungen erfolgt durch die Polizei bzw. die Staatsanwaltschaft in der Regel keine Öffentlichkeitsarbeit.

Die Polizei kann nur die Straftaten aufklären, von denen sie Kenntnis erhält. Die Ermittlung, ggf. Festnahme und die Anklage von Straftätern kann neben der Erfüllung des Strafanspruches auch eine abschreckende

Wirkung auf andere potenzielle Nachahmungs- oder Wiederholungstäter entfalten und damit einen wichtigen Beitrag für die Sicherheit im Internet darstellen. Darüber hinaus dienen die Erkenntnisse aus Strafverfahren den Sicherheits- und Strafverfolgungsbehörden als Grundlage zur Optimierung bestehender und Entwicklung neuer Präventions- und Bekämpfungsstrategien und tragen somit letztlich zu einem erhöhten Schutz aller Nutzer von informationstechnischen Systemen bei.

Insoweit tragen auch Wirtschaftsunternehmen eine besondere Verantwortung, um im Sinne eines ganzheitlichen Ansatzes bei der Bekämpfung der Cybercrime in Deutschland den permanent und immer schneller wachsenden Herausforderungen in diesem Phänomen erfolgreich zu begegnen.

Die Polizei ist Ihr Partner – kommen Sie auf uns zu!

Nützliche Links

Nützliche Links zum IT-Grundschutz und zur Sicherheit in Unternehmen z.B.:

https://www.bsi.bund.de
https://www.sicher-im-netz.de
https://bitkom.org
http://www.bmwi.de
http://asw-online.de