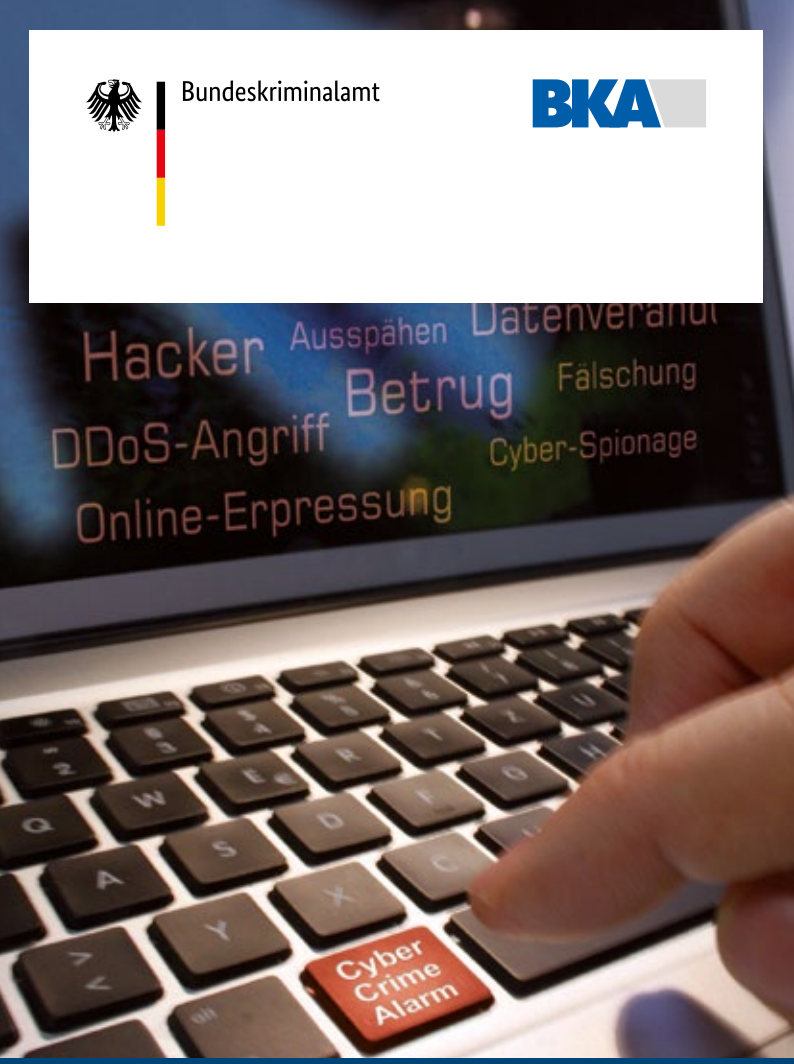
Bundeskriminalamt

BKA



Cybercrime

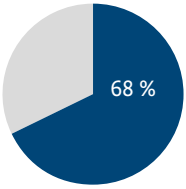
Handlungsempfehlungen für die Wirtschaft

Handlungs-empfehlungen für die Wirtschaft in Fällen von Cybercrime

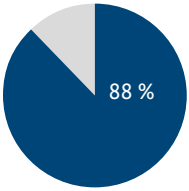
1 Einleitung und Zielsetzung

NEBEN PRIVATPERSONEN STEHEN INSBESONDERE WIRTSCHAFTSUNTERNEHMEN IM ZIELSPEKTRUM VON CYBERKRIMINELLEN.

So führt der Digitalverband Bitkom[1] in seiner 2018 veröffentlichten Studie *„Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie“*[2] aus, dass 68% der Industrieunternehmen in Deutschland in den vergangenen beiden Jahren Opfer von Datendiebstahl, Industriespionage oder Sabotage geworden sind. Hierdurch ist ein Schaden von rund 43,4 Milliarden Euro in den letzten beiden Jahren entstanden.



Die im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) durchgeführte Cyber-Sicherheits-Umfrage 2018[3] kam zu dem Ergebnis, dass 33% der befragten Organisationen von Cyber-Sicherheits-Vorfällen betroffen waren. Fast neun von zehn Institutionen (88%) erwarten von der Digitalisierung eine Verschärfung der Bedrohungslage.



[1] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
[2] Stand: 2018.
[3] Öffentliche Online Umfrage der Allianz für Cyber-Sicherheit u.a. bei IT-Dienstleistern, Finanzdienstleistern, Industrie und Handel sowie im Öffentlichen Dienst, Stand: 18.04.2019.

1 Einleitung und Zielsetzung

Die Wirtschaftsprüfungs- und Beratungsgesellschaft KPMG stellt in ihrer Studie *„e-Crime[4] in der deutschen Wirtschaft 2019“* fest, dass vier von zehn Unternehmen in Deutschland in den vergangenen zwei Jahren von e-Crime betroffen waren.[5] Der Mehrheit der betroffenen Unternehmen entstanden jeweils Schäden zwischen 20.000 € und 150.000 €, wobei einige der Befragten Gesamtschäden von 500.000 € und auch deutlich darüber angeben. Mit zunehmender Unternehmensgröße steigt auch der realisierte Schaden.

Erneut steht der Aspekt *„Unachtsamkeit“* an der Spitze der e-Crime begünstigenden Faktoren. Weiter wird die zunehmende Komplexität der eingesetzten Technologie angeführt und 86 % der Betroffenen sehen in einer mangelnden Sicherheitskultur bzw. mangelndem Risikoverständnis entscheidende Faktoren. Die Bekämpfung des Phänomens sollte daher sowohl bei den technischen, als auch den menschlichen Faktoren ansetzen.

---

[4] Definition e-Crime in der Studie: Ausführung von wirtschaftskriminellen Handlungen unter Einsatz von Informations- und Kommunikationstechnologien zum Schaden einer Einzelperson, eines Unternehmens oder einer Behörde.

[5] Befragt wurden ausgewählte Unternehmen aus den Branchen Industrie, Handel, Finanzdienstleister und andere Dienstleister.

[6] Gemäß der Cybercrime Konvention des Europarates 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).

Unternehmen bemerken häufig nicht, dass sie Opfer von Cybercrime[6] geworden sind. Selbst wenn solche Straftaten festgestellt werden, gelangen diese nur in wenigen Fällen zur Anzeige und somit zur Kenntnis der Sicherheits- und Strafverfolgungsbehörden. Laut der eingangs genannten KPMG-Studie haben lediglich ca. 40% der betroffenen Unternehmen Strafanzeige erstattet.

Aus Gesprächen mit Wirtschaftsvertretern sind die nachfolgenden Gründe ursächlich für die Nichterstattung von Anzeigen:

- Es handelt sich oftmals um Innentäter, sodass eine firmeninterne Regulierung bevorzugt wird.
- Die Angriffe werden abgewehrt bzw. bleiben erfolglos.
- Zunächst keine Schäden erkennbar oder messbar.
- Fehlende Sensibilisierung/Awareness bei den Verantwortlichen auf Leitungsebene.
- Keine Anzeigen aus Sorge vor Imageschäden durch befürchtete Presseveröffentlichungen.

1 Einleitung und Zielsetzung

- Befürchtete negative Auswirkungen unter Konkurrenz- oder Wettbewerbsaspekten.
- Die Strafverfolgung dauert aus Sicht der Unternehmen zu lange bzw. es wird Erfolglosigkeit der polizeilichen Ermittlungen befürchtet.
- Insbesondere kleinere Firmen haben Sorge, dass die Polizei Firmenrechner sicherstellt und diese erst nach einem längeren Zeitraum wieder aushändigt.
- Teilweise verfügen Unternehmen über unzureichend lizenzierte Software, sodass 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 Polizei schränkt eine Nichtanzeige die effektive und erfolgreiche Bekämpfung von Cybercrime erheblich ein.

Ziel:

Mit dieser Broschüre möchte die Polizei Ihnen konkrete Empfehlungen zum Schutz vor Cybercrime geben und aufzeigen, wie Sie bei Betroffenheit durch eine solche Straftat vorgehen können. Zudem wollen wir Sie dazu ermutigen, strafrechtlich relevante Vorfälle bei der Polizei anzuzeigen und Sie darüber informieren, was Sie in solchen Fällen von uns erwarten können. Denn nur durch einen Schulterschluss von Polizei und Wirtschaft können Täter ermittelt, verurteilt und so Cybercrime nachhaltig bekämpft werden. Davon profitieren auch Ihr Unternehmen und Ihre Geschäftspartner.

2 Grundlagen für die Verfolgung von Cybercrime

2.1 POLIZEILICHE ZUSTÄNDIGKEITEN

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

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

Im BKA sowie in den Landeskriminalämtern (LKÄ) wurden speziell für Unternehmen sowie öffentliche und nichtöffentliche Institutionen die sogenannten *„Zentralen Ansprechstellen Cybercrime“* (ZAC) eingerichtet. Diese dienen als *„Single Point of Contact“* (SPoC), um als kompetenter Ansprechpartner Informationen zu IT-Sicherheitsvorfällen direkt von Ihnen entgegenzunehmen und zeitnah Erstmaßnahmen mit anschließender Zuweisung an die zuständigen Ermittlungsstellen zu veranlassen. Die Erreichbarkeiten der ZAC ha-

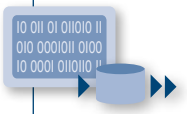
ben wir für Sie am Ende dieser Broschüre zusammengestellt. So erreichen Sie immer direkt Ihren fachkundigen Ansprechpartner bei der Polizei – nicht nur bei Betroffenheit von Cybercrime sondern auch für allgemeine Fragestellungen und Anliegen zum Thema Prävention in diesem Phänomenbereich.

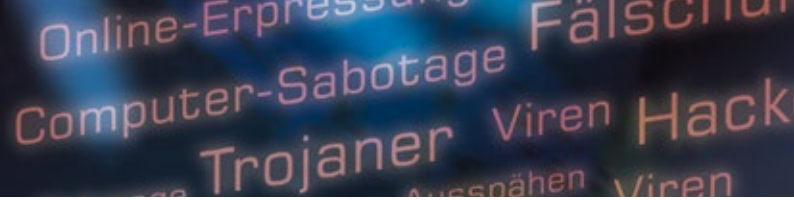
2.2 GESETZESGRUNDLAGEN

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 gibt einen Überblick über die einschlägigen Straftatbestände des Strafgesetzbuches (StGB).

2 Grundlagen für die Verfolgung von Cybercrime

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.
§ 202d StGB Datenhehlerei 	Das sich oder einem anderen Verschaffen, Überlassen, Verbreiten oder Zugänglichmachen von nicht allgemein zugänglichen und durch einen anderen aus einer rechtswidrigen Tat erlangten Daten mit der Absicht, sich oder einen Dritten zu bereichern oder einen anderen zu schädigen.
§ 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, Veräußerung, Verwahrung oder Überlassung eines Computerprogramms, dessen Zweck die Begehung einer solchen Tat ist.	
Das Speichern oder Verändern beweiserheblicher Daten zur Täuschung im Rechtsverkehr, sodass 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, 3. Zerstörung, Beschädigung, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers.	**§ 303b StGB Computersabotage**

3 Verhaltensempfehlungen

Auf Grundlage der Strafanzeigen der letzten Jahre ist festzustellen, dass Unternehmen vor allem von den nachfolgend aufgeführten Szenarien betroffen sind und diese eine maßgebliche Rolle für die hohen Fallzahlen und wirtschaftlichen Schäden spielen:

- Online-Erpressung mittels Ransomware/ Kryptotrojaner
- Online-Erpressung mittels DDoS (Distributed-Denial-of-Service)
- Man-in-the-middle-Angriff
- Datendiebstahl/Veröffentlichung von Daten
- CEO-Fraud

Die nachfolgenden Informationen sollen Ihnen Ratschläge und Tipps an die Hand geben, welche präventiven Maßnahmen Sie bereits im Vorfeld von Cyberangriffen umsetzen können, um sich wirkungsvoll auf solche Szenarien vorzubereiten.

3.1 TECHNISCHE PRÄVENTIONSMASSNAHMEN

Einen hundertprozentigen Schutz gegen Cyberangriffe gibt es nicht. Allerdings können Sie das Risiko durch die Umsetzung der folgenden technischen Maßnahmen deutlich verringern und die Sicherheit Ihrer IT-Infrastruktur erhöhen:

- Informieren Sie sich auf den Internetseiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zum IT-Grundschutz und setzen Sie die dort genannten Maßnahmen in Ihrem Unternehmen um.
- Installieren Sie zeitnah die regelmäßig von den jeweiligen Herstellern bereitgestellten Sicherheitsupdates für Ihr Betriebssystem und die von Ihnen genutzten Programme.
- Setzen Sie ein Virenschutzprogramm ein und aktualisieren Sie dieses regelmäßig.
- Verwenden Sie eine Firewall.
- Nutzen Sie für den Zugriff auf das Internet ausschließlich ein Benutzerkonto mit eingeschränkten Rechten.
- Verwenden Sie sichere, komplexe Passwörter. Eine noch höhere Sicherheit

können Ihnen Zwei-Faktor-Authentifizierungen bieten.
- Verwenden Sie Verschlüsselungsmechanismen (z.B. Verschlüsselung von Datenträgern) und digitale Signaturen ihrer E-Mails im Rahmen der internen und externen E-Mail-Kommunikation.
- Beobachten Sie Ihre Systeme. Infizierte Systeme sollten schnellstmöglich vom Netzwerk getrennt werden, um eine Weiterverbreitung der Malware zu verhindern.
- Erstellen Sie regelmäßig Backups und prüfen Sie deren Verfügbarkeit und Rückspielbarkeit. Bewahren Sie die jeweils durchgeführten Backups über einen längeren Zeitraum auf, bevor Sie diese wieder überschreiben.

3.2 SENSIBILISIERUNG DER MITARBEITER

Den größten Verursacherkreis bilden ehemalige oder aktuelle Mitarbeiter *(„insider threat“)*. Allerdings erfolgen die Taten überwiegend nicht in krimineller Absicht, sondern vielmehr aufgrund von Fahrlässigkeit und mangelndem Problem-

bewusstsein. Daher ist es besonders wichtig ein Sicherheitsbewusstsein sowohl in technischer Hinsicht, aber insbesondere auch mit Blick auf die soziale Komponente zu schaffen, um Ihre Mitarbeiter vor Phishing, Social Engineering und Co zu schützen. Hierzu sind spezielle IT-Sicherheitsschulungen für Ihre Mitarbeiter eine wirksame Maßnahme.

Grundlegende Tipps für Ihre Mitarbeiter sind dabei:

- Halten Sie sich an die IT-Sicherheitsvorschriften Ihres Arbeitgebers, diese dienen Ihrem und dem Schutz des Unternehmens.
- Seien Sie zurückhaltend mit der Weitergabe von vertraulichen und persönlichen Informationen.
- Haben Sie ein gesundes Misstrauen und scheuen Sie sich nicht vor persönlichen Rückfragen, wenn Ihnen etwas ungewöhnlich vorkommt.
- Überprüfen Sie E-Mails auf die richtige Absenderadresse sowie die korrekte Schreibweise der E-Mail-Domain.
- Öffnen Sie keine verdächtigen Mails.
- Seien Sie misstrauisch bei Links oder Anlagen in E-Mails unbekannter Absender.

3.3 ABLAUFORGANISATORISCHE MASSNAHMEN

Sie sollten in Ihrem Unternehmen bzw. in Ihrem Verantwortungsbereich Verfahrensweisen oder Anleitungen zum Umgang mit Vorfällen bzw. Straftaten aus dem Bereich der Cybercrime vorbereiten. Insbesondere sollten die Compliance- und Datenschutzbeauftragten in die Planungen eingebunden werden. Darüber hinaus bietet sich – sofern vorhanden – die Einbindung der Rechtsabteilung, der Presse- und Öffentlichkeitsarbeit sowie des Betriebsrates an. Solche Verfahrensweisen geben Ihren Mitarbeitern Handlungssicherheit im Ereignisfall, helfen Schäden zu begrenzen und die relevanten Akteure innerhalb und außerhalb Ihres Unternehmens frühzeitig einzubinden.

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

- Wie muss bei einem IT-Sicherheitsvorfall Schritt für Schritt und differenziert nach unterschiedlichen Szenarien vorgegangen werden?
- Wer hat im Unternehmen welche Verantwortung für die interne Reaktion auf einen Schadensfall?
- Wer ist die Ansprechstelle für interne und externe Kontakte?
- Wer sollte innerhalb und außerhalb der Firma unmittelbar verständigt werden?
- An welchem Punkt sollten die Strafverfolgungsbehörden informiert werden?

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

Planen Sie zudem eine professionelle Öffentlichkeitsarbeit für den Fall eines IT-Sicherheitsvorfalls. Diese hilft mögliche Reputationsschäden zu vermeiden bzw. zu begrenzen.

4 Verhaltensempfehlungen bei Betroffenheit von Cybercrime-Delikten

Die nachfolgenden Informationen sollen Ihnen Ratschläge und Tipps an die Hand geben, wie Sie sich im Schadensfall verhalten sollten.

4.1 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 derart 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.

4.2 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

[7] Weitergehende Informationen siehe Leitfaden IT-Forensik des BSI: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.html

Identifizierung von ausgenutzten Schwachstellen, gelöschten Daten und installierten Schadprogrammen sowie zur Unterstützung der Rückverfolgung des Angreifers hilfreich sein. Der Vorteil dieser Sicherungskopien liegt darin, dass sie auch verborgene Dateien und Verzeichnisse, 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 umgehend die Polizei informieren, damit diese die Möglichkeit hat, auch Kopien zu forensischen Zwecken anzufertigen (siehe Nr. 5).

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 rele-

vante 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 des Zeitaufwands.
- 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 sowie verdächtiger Dateien und E-Mails 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.

4.3 HINWEISE ZUM INFORMATIONSAUSTAUSCH

Infizierte Systeme sollten grundsätzlich nicht dazu verwendet werden, um sich über einen Angriff oder die Reaktion darüber auszutauschen.

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. 3.3 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, sollten Sie Informationen über den Zwischenfall nach dem Grundsatz *„Kenntnis nur, wenn nötig“* begrenzen.

4.4 EVENTUELLE BENACHRICHTIGUNG VON WEITEREN GESCHÄDIGTEN ODER HERSTELLERN

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 gegebenenfalls weitere Schäden an anderen Systemen verhindern.

4.5 MELDEN VON STRAFTATEN AN STRAFVERFOLGUNGSBEHÖRDEN

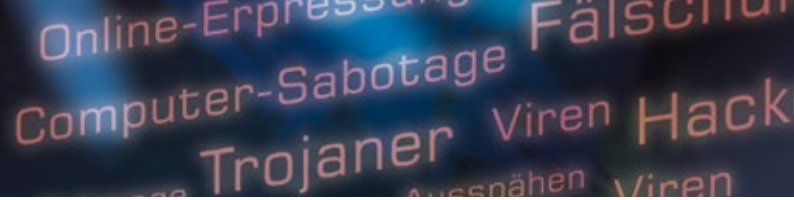
Wenn Sie im Zusammenhang mit einem Vorfall den Verdacht haben, dass dieser eine Straftat darstellen könnte, sollten Sie sich an die dafür festgelegte bzw. vorgeschriebene Vorgehensweise in Ihrer Firma halten und unverzüglich die zuständige Strafverfolgungsbehörde informieren.

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.

4.6 BENACHRICHTIGUNG VON BETROFFENEN UND DER ZUSTÄNDIGEN AUFSICHTSBEHÖRDE

Führen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust oder Veränderung in Ihrem Unternehmen zur (unbefugten) Offenlegung personenbezogener Daten, so hat nach Art. 33 Datenschutzgrundverordnung (DSGVO) immer dann



eine Benachrichtigung an die zuständigen Aufsichtsbehörden[8] zu erfolgen, wenn dies ein Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat. In den Fällen, in denen ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen besteht, sind nach Art. 34 DSGVO überdies die betroffenen Personen zu benachrichtigen.

4.7 MASSNAHMEN ZUR MINIMIERUNG ANHALTENDER SCHÄDEN

Zur Unterbindung anhaltender Schädigungen durch einen aktuellen Angriff auf das Netzwerk sollten beispielsweise Filter zur Abwehr von DDoS-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

[8] Siehe hierzu Art. 55, 56 DSGVO. In der Regel handelt es sich dabei um die Datenschutzbeauftragten in den einzelnen Bundesländern.

könnte, dass seine Attacke entdeckt wurde. Er könnte seine Spuren auf den Systemen löschen oder gar 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 festzulegen, 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.

4.8 VERZICHT AUF EIN EINDRINGEN IN DEN QUELLCOMPUTER BZW. EINE BESCHÄDIGUNG DES QUELL-COMPUTERS

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 und Sie sich selbst strafbar machen.

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.

5 Zusammenarbeit mit der Polizei

5.1 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 bundesweit eingerichteten Zentralen Ansprechstellen Cybercrime für die Wirtschaft (ZAC), zu wenden. Zur Identifizierung der für Sie geeigneten Ansprechpartner wird bereits im Vorfeld konkreter Anlässe eine Verbindungsaufnahme mit Ihrer für Cybercrime zuständigen Ansprechstelle der Polizei empfohlen. Die entsprechenden Kontaktdaten finden Sie am Ende dieser Broschüre.

5.2 ERMITTLUNGEN UND TATORTARBEIT

Die Polizei führt auf Grundlage der Strafprozessordnung 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.

Die Polizei ist sich auch der Interessenlage der Firmen zu dem Aspekt *„Imageschaden“* bewusst. So ist die Polizei grundsätzlich bestrebt, mit nur so vielen Beamten vor Ort zu erscheinen, wie es für die Durchführung der zu treffenden Maßnahmen notwendig ist. Soweit vermeidbar wird auf den Einsatz uniformierter Beamter verzichtet. Abhängig von der Ausgangssituation 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 Maßnahme kann es erforderlich sein, Daten vor Ort auf Firmenrechnern

und -servern zu sichern. Dies geschieht in der Regel durch eine sogenannte Spiegelung der Daten in Zusammenarbeit mit Ihren hauseigenen IT-Verantwortlichen. Dies bedeutet, dass die als grundsätzlich beweisrelevant eingeschätzten Daten der Firma vor Ort auf einen von der Polizei mitgebrachten Datenspeicher kopiert werden. Die Firmencomputer werden also nicht zwingend sichergestellt bzw. beschlagnahmt. Der laufende Betrieb der Firma wird somit im Normalfall nicht weiter beeinträchtigt. Im Anschluss werden die so sichergestellten Daten durch IT-Forensiker der Polizei 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 Person 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 Gegenstände 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, die Maßnahmen erfolgen unter Einbindung von und in enger Abstimmung mit den IT-Sicherheitsverantwortlichen Ihres Unternehmens.

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

5.3 RELEVANZ DER EINBINDUNG DER POLIZEI

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

schreckende Wirkung auf andere potenzielle Nachahmungs- oder Wiederholungstäter entfalten und damit einen wichtigen Beitrag für die Sicherheit im Internet darstellen. Darüber hinaus dienen anonymisierte Erkenntnisse aus Strafverfahren den Sicherheits- und Strafverfolgungsbehörden der Optimierung bestehender und Entwicklung neuer Präventions- und Bekämpfungsstrategien und tragen somit zu einem erhöhten Schutz für alle Nutzer von informationstechnischen Systemen bei. Auch der Gesetzgeber orientiert sich beispielsweise bei der Anpassung des Rechtsrahmens und der Schaffung der Rahmenbedingungen zur Eindämmung und Bekämpfung von Cyberkriminalität vor allem an gesicherten Fallzahlen und der fachlichen Beratung durch die Strafverfolgungsorgane.

Insoweit tragen 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 – mit Sicherheit!

Nützliche Links

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

https://www.bsi.bund.de
https://www.sicher-im-netz.de
https://www.allianz-fuer-cybersicherheit.de
https://www.bitkom.org
http://www.bmwi.de
https://www.asw-bundesverband.de
https://www.dsin-sicherheitscheck.de
https://www.nomoreransom.org

Impressum

Herausgeber
Bundeskriminalamt
Referat SO 41
65173 Wiesbaden
Tel.: 0611/55-15037
E-Mail: zac@cyber.bka.de
Internet: www.bka.de

Stand
Oktober 2019

Druck
Druckerei Ebenhoch,
Niedernhausen

Gestaltung:
Agentur Luh Media,
Niedernhausen

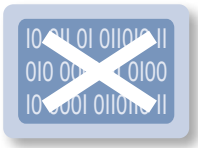
Bildnachweis
Udo Luh, Luh Media

Cybercrime-Straftatbestände

Ausspähen von Daten

Abfangen von Daten

Vorbereiten des Ausspähens und Abfangens von Daten



Datenveränderung

Datenhehlerei

Fälschung beweiserheblicher Daten

Computerbetrug

Computersabotage

www.bka.de