Bayerisches Staatsministerium der Justiz

CYBERCRIME

Hilfe für betroffene Unternehmen

www.justiz.bayern.de

Impressum

Herausgeber
Bayerisches Staatsministerium der Justiz
Referat für Öffentlichkeitsarbeit
Prielmayerstraße 7, 80335 München

Bilder
shutterstock.com

Gestaltung und Corporate Design
Atelier Hauer + Dörfler GmbH, Berlin

Druck
Offsetdruckerei Gebr. Betz, Weichs

Stand
Januar 2025

Auf eine geschlechterspezifische Differenzierung wurde aus Gründen der leichteren Lesbarkeit verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Bayerisches Staatsministerium der Justiz

CYBERCRIME

Hilfe für betroffene Unternehmen

VORWORT

Daten sind der zentrale Rohstoff in der digitalen Welt. Dabei geht es um personenbezogene Daten, aber auch um klassische Betriebsgeheimnisse. Cyberangriffe sind daher eine ganz reale Gefahr für viele Unternehmen. Einen wesentlichen Beitrag zur Verhinderung von Cyberangriffen können und müssen die Unternehmen selbst leisten, indem sie ein modernes IT-Sicherheitssystem und -management aufbauen und in die Schulung der Mitarbeiter und Mitarbeiterinnen im Bereich Cybersicherheit investieren.

Um den Herausforderungen auch auf staatlicher Seite wirksam begegnen zu können, hat Bayern bei Polizei, Verfassungsschutz und Justiz spezialisierte Einheiten gegründet. Bei der bayerischen Justiz steht als vertraulicher Ansprechpartner für Unternehmen jeder Größe - neben den örtlichen Staatsanwaltschaften - die Zentralstelle Cybercrime Bayern bei der Generalstaatsanwaltschaft Bamberg, kurz ZCB, zur Verfügung.

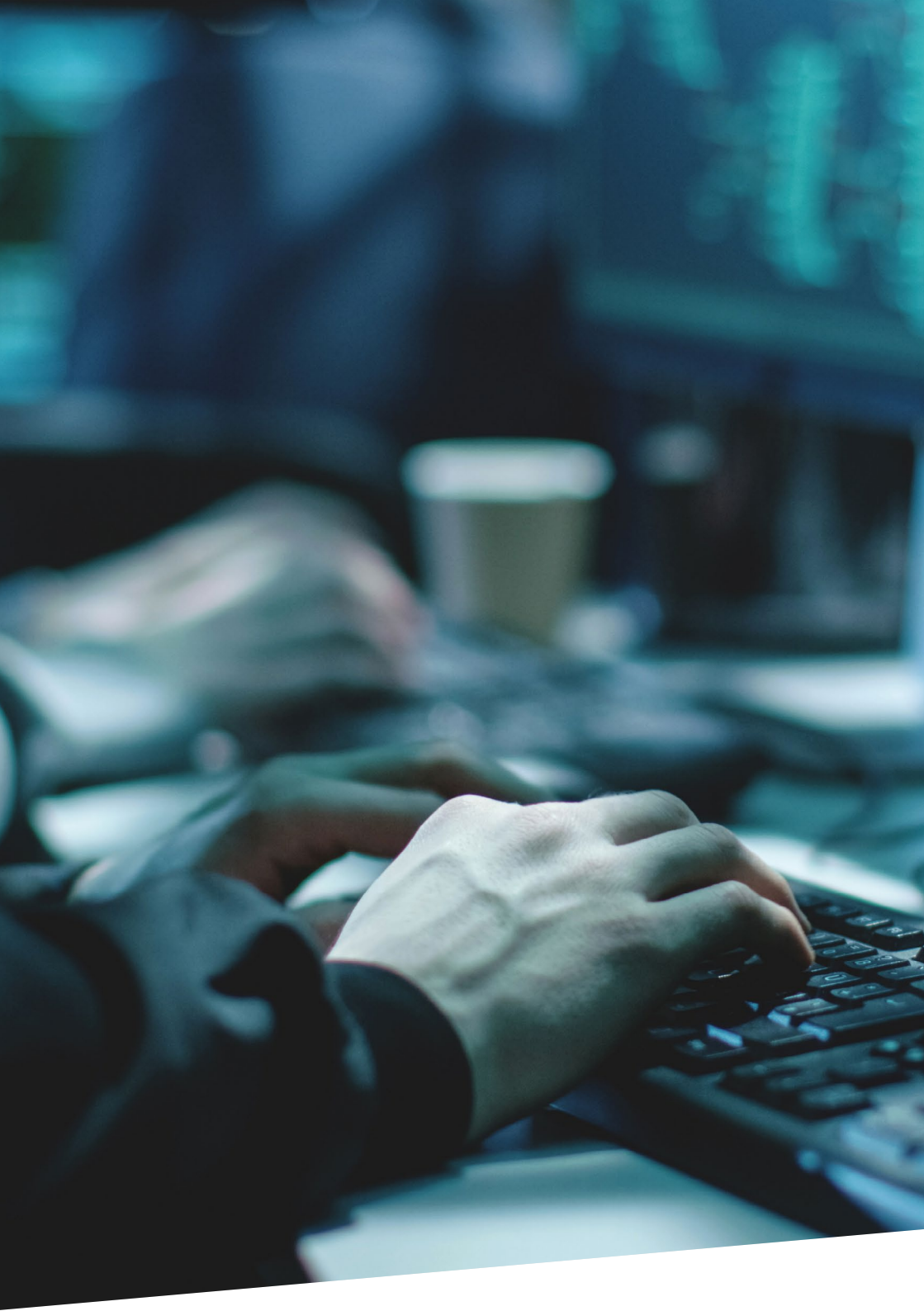
Die ZCB ist bayernweit zuständig für die Bearbeitung besonders herausgehobener Ermittlungsverfahren im Bereich der Cyberkriminalität. Sie ermittelt z.B. bei Hackerangriffen auf Industriesteuerungssysteme, bei kriminellen Zugriffen auf Kundendaten oder bei Erpressungsversuchen nach illegaler Verschlüsselung von Firmensoftware. Darüber hinaus fallen auch Angriffe auf kritische Infrastrukturen in ihre Zuständigkeit. Gemeinsam mit den IT-Experten klären unsere international bestens vernetzten Staatsanwälte Cyberdelikte auf. Speziell für Angriffe u.a. auf Unternehmen besteht bei der ZCB die Taskforce „Cyberangriffe auf Unternehmen und Einrichtungen".

Die ZCB ist bei der Ermittlung der Täter darauf angewiesen, dass die Unternehmen eng und vertrauensvoll mit der Justiz zusammenarbeiten – und zwar so früh wie möglich. Denn die ZCB kann besonders in den frühen Stadien einer Tat effektiver helfen, den Schaden zu begrenzen und die Täter zur Verantwortung zu ziehen.

Durch konsequente Strafverfolgung wollen wir nicht nur eine abschreckende Wirkung auf die Täter erzielen. Wichtig ist mir auch das Signal an Sie, sehr geehrte bayerischen Unternehmerinnen und Unternehmer: Mittlere und kleine Unternehmen sind das Rückgrat der bayerischen Wirtschaft. Bei Angriffen auf unsere Unternehmen und unseren wirtschaftlichen Wohlstand gibt es zahlreiche Möglichkeiten der Unterstützung durch die ZCB und die Polizei. Die Staatsregierung bittet Sie, diese Möglichkeiten zu nutzen.

München, im Januar 2025

Georg Eisenreich, MdL
Staatsminister der Justiz



INHALT

Cybercrime – Hilfe für betroffene Unternehmen

Viele Aufgaben des alltäglichen Lebens, aber auch im Firmenumfeld, verlagern sich ins Internet oder werden automatisiert durch die elektronische Datenverarbeitung erledigt. Auch für kleinere und mittlere Unternehmen (KMU) ergeben sich hierdurch neue Geschäftsfelder und Einsparungspotentiale. Leider werden die damit verbundenen Risiken oft nicht wahrgenommen oder falsch bewertet. Als Rückgrat der bayerischen Wirtschaft werden gerade leistungsfähige KMU häufig Opfer von Cybercrime. Denn auch die Täter denken profitorientiert. IT-Systeme sind lukrativ für Angreifer, da mit wenig Risiko und geringem Aufwand hohe Gewinne erzielt werden können.

Das Internet darf kein rechtsfreier Raum sein.

Um sich und andere zu schützen, ist es wichtig, Cyberkriminalität konsequent zu verfolgen. Denn das Internet darf kein rechtsfreier Raum sein. Unterstützen Sie Staatsanwaltschaften und Polizei durch eine frühzeitige Strafanzeige. Denn so können wichtige Beweismittel und flüchtige Spuren im Netz zuverlässig gesichert werden. Nur die Ermittlung und Verurteilung der Täter zu empfindlichen Strafen können die zunehmende Computerkriminalität eindämmen.

1. MIT WELCHEN TYPISCHEN CYBERANGRIFFEN MUSS ICH RECHNEN?

Wenn Ihre IT-Strukturen verletzlich sind, können Straftäter diese Schwachstellen ausnutzen, um Sie zu betrügen, zu erpressen oder Ihre Daten oder die Ihrer Kunden zu Geld machen.

Straftaten im Netz:

Schadprogramme (Ransomware):
Den Tätern gelingt es, Schadsoftware auf den Rechnern des Opfers zu installieren. Zum Teil geschieht dies durch das Öffnen von E-Mails mit bösartigen Computerprogrammen im Anhang. Aber auch Angriffe auf technische Schwachstellen, Sicherheitslücken oder über Drittsoftware (sog. Supply-Chain-Angriffe) werden immer häufiger. Die Programme verbreiten sich im gesamten Firmennetz, stehlen Daten und beginnen danach, alle Daten zu verschlüsseln. Dann wird das Unternehmen erpresst: Die Entschlüsselung ermöglichen die Täter nur nach Zahlung eines hohen Betrags in Kryptowährung (meist in Bitcoins).

Haben Sie ein aktuelles funktionsfähiges Backup, das nicht über das Netzwerk erreichbar ist?

Es handelt sich um den Straftatbestand der gewerbsmäßigen Erpressung (§ 253 Abs. 1 und 4 StGB). Die Tat wird mit Freiheitsstrafe von 1 bis 15 Jahren geahndet. Auch wenn es nicht zu Zahlungen kommt: Bereits der Versuch ist strafbar.

Computersabotage:
Das Ziel ist, die Systeme zum Zusammenbruch zu bringen oder zu beschädigen. Beispiel „DDoS-Angriff" (Distributed Denial of Service): Dabei werden Server durch eine große Anzahl an Anfragen aus dem Netz lahmgelegt. Das Unternehmen ist dann für Dritte (Kunden/Geschäftspartner) nicht mehr erreichbar.

Wie wichtig ist es für Ihr Unternehmen, dass Ihre Kunden und Mitarbeiter aus dem Internet auf Ihre Website zugreifen?
Ist Ihr Server ausreichend gehärtet?

§

Computersabotage (§ 303b StGB) wird mit Geldstrafe oder Freiheitsstrafe geahndet, die – abhängig vom konkreten Fall – bis zu 10 Jahre betragen kann.

CEO Fraud:
Der Angriff erfolgt nicht auf die Systeme, sondern zielt auf Ihre Mitarbeiter. Meist sollen diese dazu gebracht werden, Überweisungen auf die Konten der Täter vorzunehmen. Nicht signierte E-Mails sind leicht zu fälschen! Ein geschickter Täter kann so mit einer scheinbar echten E-Mail der Firmenleitung die Buchhaltung zur Zahlung hoher Geldsummen in „einer höchst geheimen Angelegenheit" veranlassen. Mithilfe künstlicher Intelligenz können die Täter die Kontaktaufnahme noch glaubhafter gestalten. Glauben Ihre Mitarbeiter einer Mail, nur weil sie den Absender (vermeintlich) kennen?

§

Solches Vorgehen ist gewerbsmäßiger Betrug (§ 263 Abs. 1 und 3 S. 2 Nr. 1 StGB). Die Täter müssen mit Freiheitsstrafen von 6 Monaten bis zu 10 Jahren rechnen.

Phishing:
Die Täter verleiten Ihre Mitarbeiter dazu, sich auf gefälschten Internetseiten bekannter Portale anzumelden und erhalten hierdurch Zugang zu Ihren Passwörtern. Neben dem daraus resultierenden Zugriff auf sensible Daten können dann von diesen kompromittierten E-Mail-Accounts gezielt weitere Phishing-Mails an deren Kontakte versendet werden.

§

Bereits das Versenden der E-Mail kann als Fälschung beweiserheblicher Daten (§ 269 StGB), Vorbereiten des Ausspähens von Daten (§ 202c StGB) oder nach dem Markengesetz strafbar sein. Gelangen die Täter an Daten und nutzen diese in der Folge, kommen weitere Straftatbestände in Betracht.

Hacking:
Hierbei werden gezielt Schwachstellen ausgenutzt, um unbefugten Zugriff zu erhalten. Die Täter leiten in großem Umfang (sensible) Daten wie Kundendaten, Bankzugangs- oder Kreditkartendaten und Passwörter aus. Diese Daten werden später zur Erpressung genutzt, an Dritte verkauft oder schlicht zur Schädigung des Unternehmens öffentlich zugänglich gemacht. Der Zugang zu den Systemen erfolgt meist wie bei der Ransomware oder über die „Schwachstelle" Mensch.

§

Das Ausleiten der Daten ist als Ausspähen von Daten (§ 202a StGB) oder Abfangen von Daten (§ 202b StGB) strafbar. Abhängig von der weiteren Nutzung der Daten kommen zusätzliche Straftatbestände in Betracht.

Spionageattacken:
Insbesondere Unternehmen, die im Bereich der Forschung und Entwicklung tätig sind, können Opfer gezielter Ausforschung durch Konkurrenzunternehmen oder auch durch fremde Staaten werden.

§

Neben Datendelikten (§§ 202a bis d StGB) ist auch eine Strafbarkeit nach dem Außenwirtschaftsgesetz, dem Bundesdatenschutzgesetz oder dem Geschäftsgeheimnis-Schutzgesetz denkbar.

Rechnungsfälschung/Manipulation der elektronischen Kommunikation:
Die Täter fangen E-Mails ab, manipulieren diese und leiten sie dann an den Empfänger weiter (sog. „Man in the middle-Angriff"). Insbesondere werden dabei häufig in Rechnungsanhängen die IBAN-Nummern geändert.

§

Es handelt sich um gewerbsmäßigen Betrug (§ 263 Abs. 1 und 3 S. 2 Nr. 1 StGB). Die Täter müssen mit Freiheitsstrafen von 6 Monaten bis zu 10 Jahren rechnen.

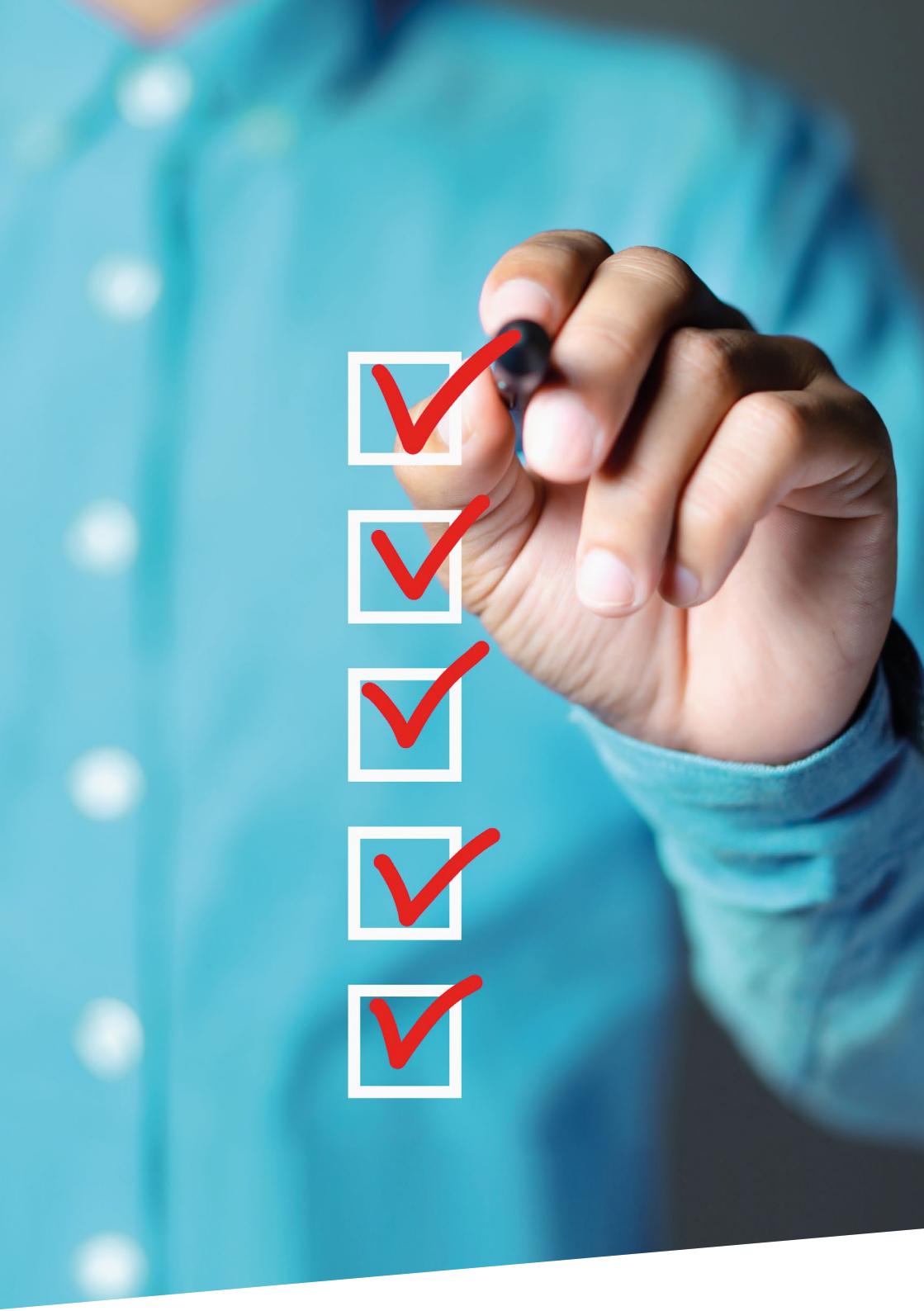
Insiderangriffe:
Mitarbeiter mit Zugang zu den elektronischen Systemen missbrauchen den Zugang, um u. a. Schadsoftware aufzuspielen oder Daten auszuleiten. Mögliche Täter sind auch ehemalige Mitarbeiter, deren Zugang nicht gesperrt wurde.

2. WARUM BETRIFFT DAS MEIN UNTERNEHMEN?

Jedes Unternehmen kann Ziel sein.

Jedes Unternehmen ist potenzielles Ziel der Cyberkriminalität. Während große Unternehmen meist sehr gut geschützt sind, ist für die Täter der erforderliche Aufwand im Bereich der KMU oft geringer.

Dies dürfte ein Grund dafür sein, dass mittelständische Unternehmen am stärksten von Cyberattacken betroffen sind. Für Mittelständler kann eine Cyberattacke dabei insbesondere im Hinblick auf die erheblichen Kosten für Produktionsausfälle, den Verlust von Geschäftsgeheimnissen oder die Kosten für eine Wiederherstellung von Daten **existenzgefährdend** sein.



3. WIE KANN ICH MEIN UNTERNEHMEN DAVOR SCHÜTZEN (CHECKLISTE)?

Absolute Sicherheit lässt sich nicht erreichen. Mit relativ einfachen Maßnahmen kann man aber ein hohes Maß an Schutz erzielen.

3.1 Organisatorisches

? **Notfallplan „Was passiert, wenn…?":** Welche Konsequenzen ein Angriff hat, sollte man abschätzen, bevor es dazu kommt. Insbesondere sollten Kommunikationswege gesichert sein, wenn E-Mail-Server und/oder Telefonanlagen ausfallen. Welche Systeme sind miteinander verbunden? Welche Systeme arbeiten unabhängig voneinander? Gibt es kritische Systeme, die besonders geschützt sind oder werden sollten?

? Gibt es eine **Erste-Hilfe-Liste** mit zu kontaktierenden Ansprechpartnern (Softwareunternehmen, Servicepartner, Polizei, Zentralstelle Cybercrime Bayern, Bayerisches Landesamt für Datenschutzaufsicht etc.)? Ist die Liste auch offline verfügbar?

? Gibt es eine vollständige Liste aller Rechner, einschließlich Testrechner und Testumgebungen?

3.2 Technisches

✓ Werden regelmäßig **Backups** der eigenen Systeme durchgeführt? Wie und wo werden diese gesichert? Backups mit Netzwerkanbindung können leicht verschlüsselt oder infiziert werden. Bestehen Möglichkeiten, sich auf einen Betrieb ohne IT vorzubereiten?

✓ Sind die Systeme durch aktuelle **Virenscanner** geschützt? Besteht eine funktionierende Firewall? Ist sichergestellt, dass die Schutzsysteme von Dritten oder Mitarbeitern nicht ausgeschaltet werden können? Nehmen Sie Warnmeldungen der Antivirensoftware bitte ernst und gehen Sie den Ursachen sorgfältig nach.

✓ Werden regelmäßige **Systemupdates** durchgeführt? Sind die Systeme auf aktuellem Stand? Haben Ihre IT-Verantwortlichen ausreichend Zeit, sich über aktuelle Gefahren zu informieren und Vorkehrungen zu treffen?

✓ Sind die eigenen sensiblen **Daten besonders gesichert oder verschlüsselt?** Wichtige Daten und Kundendaten sollten nicht auf Systemen gespeichert werden, die direkten Zugang zum Internet haben. Sind sensible Bereiche durch Zwei-Faktor-Authentifizierung geschützt?

✓ Sind die **Zugänge aus dem Internet (VPN)** gesichert? Wer hat darauf Zugriff?

✓ Vergessen Sie bitte auch nicht das **„Internet der Dinge"**. Auch Router, Überwachungsanlagen, Messstellen und Telefonanlagen werden häufig Ziel von Angriffen.

3.3 Mitarbeiter

✓ **Sensibilisieren Sie Ihre Mitarbeiter!** Mitarbeiter, die die Gefahren im Netz kennen, sind der beste Schutz eines Unternehmens gegen Cybercrime. Finden regelmäßige Mitarbeiterschulungen statt?

✓ Wurden die **Zugriffsrechte für Mitarbeiter** und zugangsberechtigte Dritte **begrenzt?** Gibt es eindeutige Anweisungen zum Umgang mit **externen Datenträgern?** Werden Berechtigungen ehemaligen Mitarbeitern/Servicepartnern entzogen?

4. WIE UND WO KANN ICH EINEN ANGRIFF ANZEIGEN?

4.1 Was habe ich im Fall eines Angriffs zu beachten?

Wenn Sie Opfer eines Cybercrime-Angriffs geworden sind, müssen Sie bitte schnell, aber auch besonnen handeln.

› Unterbrechen Sie die Netzwerkverbindung laufender Systeme, schalten Sie ausgeschaltete Rechner nicht ein, isolieren Sie Ihre Backups und vermeiden Sie eine Anmeldung mit Administratorrechten.

› Organisieren Sie in Abstimmung mit den Ermittlungsbehörden die **forensische Sicherung**. Isolieren und sichern Sie die Beweismittel, löschen Sie diese nicht. Lassen Sie alle Maßnahmen dokumentieren. Setzen Sie die Systeme mit Hilfe sauberer Backups komplett neu auf. Leisten Sie keine Zahlungen an die Täter, ohne zuvor mit den Ermittlungsbehörden gesprochen zu haben.

4.2 Was habe ich bei der Erstattung der Strafanzeige zu beachten?

4.2.1 Bei wem kann ich Strafanzeige erstatten?

Informieren Sie möglichst schnell die Polizei. Bei größeren Angriffen oder erheblichen Folgen können Sie sich auch unmittelbar an die **Zentralstelle Cybercrime Bayern** wenden. Die Anschrift finden Sie am Ende der Broschüre. Nutzen Sie dabei nicht das infizierte System für die Kontaktaufnahme.

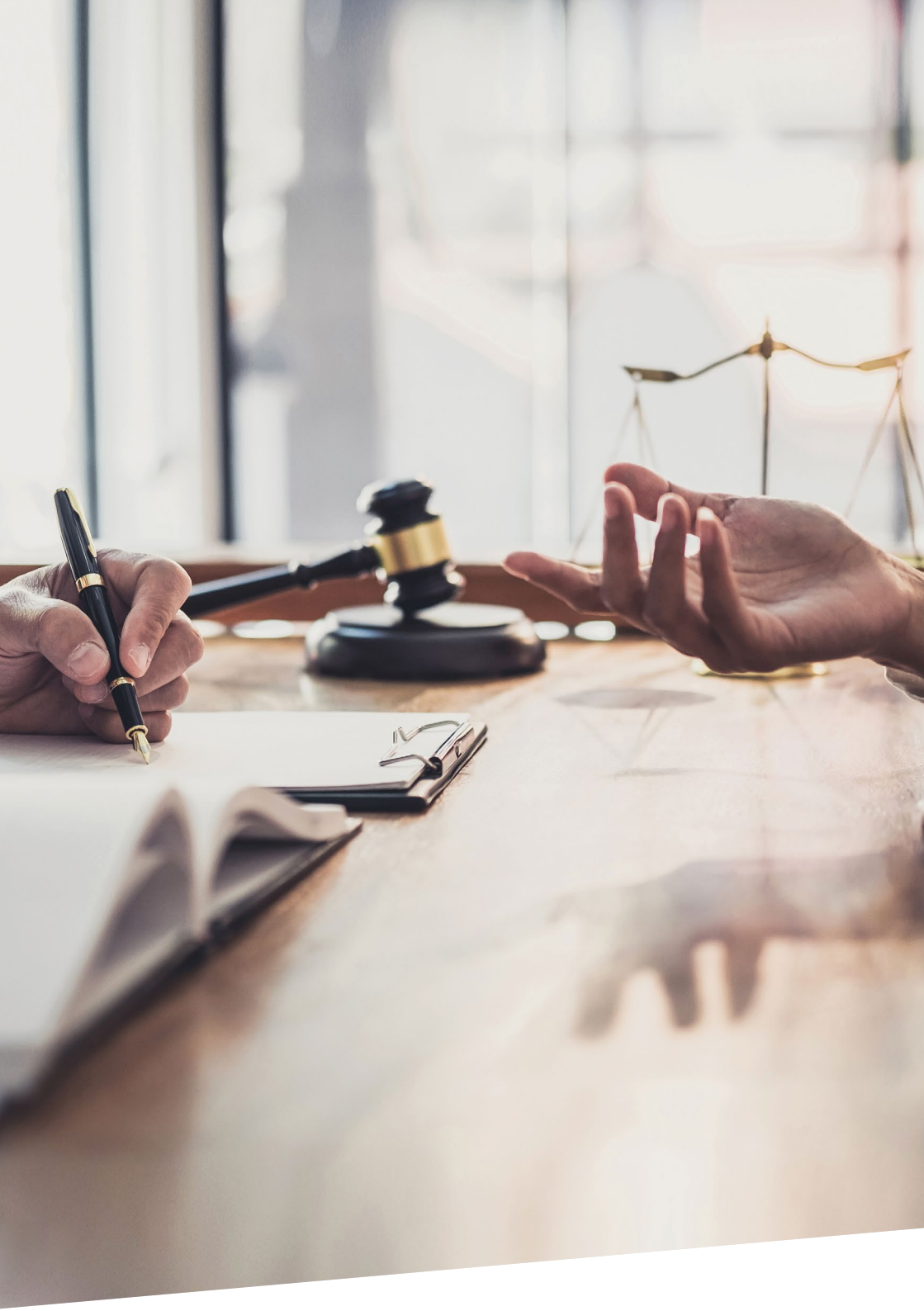
4.2.2 Wie kann ich Strafanzeige erstatten?

Grundsätzlich ist es ausreichend, Polizei oder Staatsanwaltschaft über den Angriff in Kenntnis zu setzen. Dies kann ohne jede Form auch mündlich, telefonisch oder per E-Mail geschehen. Die Beteiligung eines Rechtsanwalts ist nicht erforderlich.

4.2.3 Was sollte ich in der Anzeige mitteilen?

Wichtig ist es zunächst, dass die Ermittlungsbehörden schnell Kenntnis von der Straftat erhalten. In der Anzeige sollten Sie den Sachverhalt grob schildern und in jedem Fall Ihre eigene Erreichbarkeit angeben. Die Experten von Polizei und Staatsanwaltschaft haben in allen Deliktsbereichen große Erfahrung und wissen genau, welche Daten für die Ermittlung des Täters von Bedeutung sind. Was für die Strafverfolgung benötigt wird, hängt von der Art des Angriffs ab. Insbesondere folgende Überlegungen können dabei eine Rolle spielen:

- Wie gelangten die Täter in das System? (z. B. E-Mail-Anhang, USB-Stick, Fernwartungszugang, Software-Schwachstelle)
- Ist die ursprüngliche Schadsoftware noch vorhanden?
- Ist die E-Mail noch vorhanden?
- Wer kann wozu Auskunft erteilen?
- Wie hoch schätzen Sie den Schaden?
- Stehen Log-Dateien zur Verfügung?
- Wurden Daten durch das Unternehmen bereits verändert? Wenn ja, welche und wie?



5. WAS PASSIERT NACH EINER STRAFANZEIGE?

Staatsanwaltschaft und Polizei ermitteln die genauen Umstände der Tat. Internationale Abkommen ermöglichen häufig auch ein Vorgehen gegen ausländische Täter. Wenn die Täter identifiziert wurden und diesen eine Strafbarkeit nach Beurteilung der Staatsanwaltschaft nachgewiesen werden kann, erhebt die Staatsanwaltschaft Anklage. In der öffentlichen Hauptverhandlung werden dann Beweise erhoben. Zum Schutz von Geschäfts- und Betriebsgeheimnissen kann die Öffentlichkeit zum Teil von der Verhandlung ausgeschlossen werden.

Die Staatsanwaltschaft ist in jeder Phase des Verfahrens angehalten, die Belastungen des Geschädigten möglichst gering zu halten und seine Interessen zu wahren. Insbesondere ist es in fast allen Fällen möglich, die für die Ermittlungen erforderlichen Daten mit nur geringen Einschränkungen des Geschäftsbetriebs Ihres Unternehmens zu erheben. Eine nach Ermittlung des Täters durchzuführende Hauptverhandlung vor Gericht ist zwar grundsätzlich öffentlich, im Ermittlungsverfahren wird die Staatsanwaltschaft aber immer bemüht sein, Ihre Interessen zu berücksichtigen.

5.1 Welche Vorteile hat eine Strafanzeige

Warum eine Strafanzeige?

- Der Vorfall wird neutral dokumentiert.
- Die Zusammenarbeit mit den Ermittlungsbehörden kann das Vertrauen Ihrer Kunden in Ihre Kompetenz in Krisensituationen stärken.
- Die Erfahrungen von Polizei und Staatsanwaltschaft aus vergleichbaren Fällen können für Sie bei der Schadensminimierung, der Öffentlichkeitsarbeit und der Entwicklung zukünftiger Sicherungskonzepte hilfreich sein.
- Die Staatsanwaltschaft hat Ermittlungsmöglichkeiten, die Privatpersonen nicht zustehen. Eine Täterermittlung ohne die Staatsanwaltschaft ist weitgehend aussichtslos.
- Sie werden im Rahmen des Strafverfahrens beteiligt und haben u. a. ein Akteneinsichtsrecht.
- In geeigneten Fällen kann die Staatsanwaltschaft gerichtliche Maßnahmen zur Vermögenssicherung, wie das „Einfrieren" der Täterkonten, veranlassen und nach einer Verurteilung die eingezogenen Mittel an Sie als Geschädigten auskehren. Im Fall der Täterermittlung können Sie außerdem leichter Schadensersatzansprüche geltend machen.
- Durch die Anzeige entstehen Ihnen keine direkten Kosten.
- Nur eine Verurteilung des Täters kann dazu beitragen, dass dieser keine weiteren Straftaten mehr begeht und Nachahmer abgeschreckt werden!

5.2 Wen kann/sollte ich noch einschalten?

Wichtig: Bei einer Verletzung des Schutzes personenbezogener Daten nach Art. 33 DSGVO muss das Bayerische Landesamt für Datenschutzaufsicht **(BayLDA)** *informiert werden. Dieses kann Sie auch bei der Frage unterstützen, ob zudem eine Meldung an Ihre Kunden nach Art. 34 DSGVO erforderlich ist. Die Strafanzeige ist kein Ersatz für die Meldung nach Art. 33 DSGVO an das BayLDA.*

- Bei komplexeren Rechtsfragen, insbesondere beim Verlust von Kundendaten, bietet es sich an, einen **Rechtsanwalt** zur Unterstützung in allen rechtlichen Belangen zu konsultieren.
- Qualifizierte Dienstleister bei Cyberangriffen können beim Bundesamt für Sicherheit in der Informationstechnik (BSI) angefragt werden.
- Wenn Sie kritische Infrastrukturen betreiben (etwa Hersteller von Medizinprodukten, regionale Stromanbieter, größere Verkehrsunternehmen), müssen Sie in bestimmten Fällen Cyberangriffe an das BSI melden (§ 8b Abs. 4 BSIG).
- Sollten Sie gegen Cyberangriffe versichert sein, prüfen Sie bitte Ihre Vertragsunterlagen umgehend darauf, welche Obliegenheiten und Verpflichtungen Sie im Schadensfall haben und verständigen Sie das Versicherungsunternehmen.

6. AN WEN KANN ICH MICH WENDEN?

Generalstaatsanwaltschaft Bamberg
Zentralstelle Cybercrime Bayern (ZCB)
Wörthstr. 7, 96052 Bamberg
Telefon: 0951 833-1451
Telefax: 0951 833-1442
E-Mail: cybercrime@gensta-ba.bayern.de

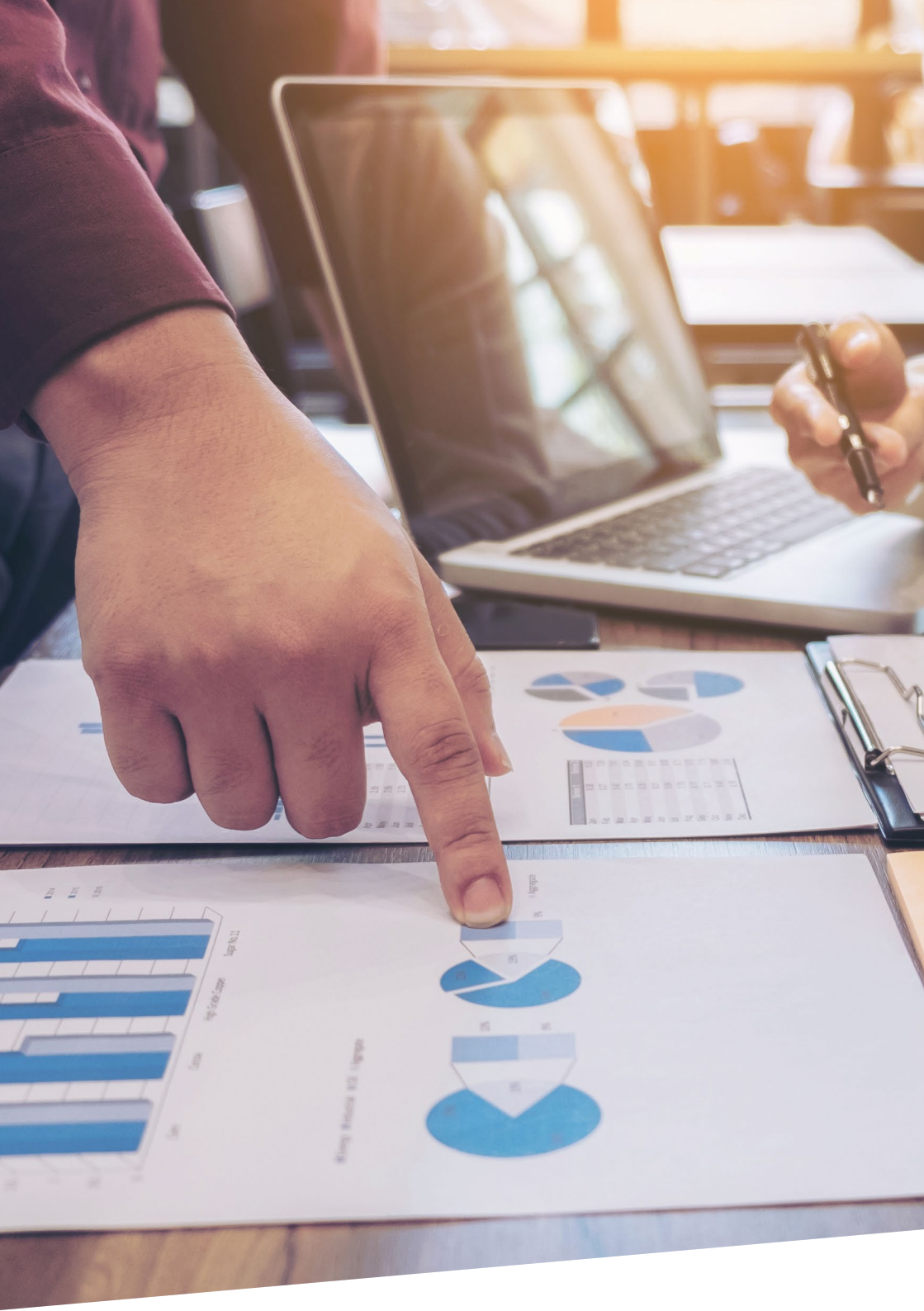
Die bei der Generalstaatsanwaltschaft Bamberg errichtete ZCB ist bayernweit zuständig für die Bearbeitung herausgehobener Ermittlungsverfahren im Bereich der Cyberkriminalität. Die technisch und ermittlungstaktisch geschulten Spezialstaatsanwältinnen und -staatsanwälte ermitteln mit IT-Forensikerinnen und -Forensikern sowie in Zusammenarbeit mit den Spezialisten der bayerischen Polizei oder des Bundeskriminalamts und mit internationalen Partnern z. B. bei Angriffen auf bedeutende Wirtschaftszweige und öffentliche Einrichtungen oder bei Verfahren aus dem Bereich der organisierten Cyberkriminalität. Die ZCB ermittelt auch dann, wenn bei Verfahren der Allgemeinkriminalität ein hoher Ermittlungsaufwand im Bereich der Computer- und Informationstechnik abzuarbeiten ist. Zum 1. Oktober 2022 wurde bei der ZCB eine Taskforce „Cyberangriffe auf Unternehmen und Einrichtungen" eingerichtet. Die Leitung der Taskforce ist zugleich persönliche Ansprechstelle speziell für Unternehmen. Die Taskforce ist u.a. zuständig für Ermittlungsverfahren wegen Cyberangriffen auf Unternehmen, Einrichtungen und Behörden und wegen anderer technischer Angriffe unter Einsatz von Schadsoftware.

Zentrale Ansprechstelle Cybercrime der Polizei Bayern (ZAC)
Maillingerstr. 15, 80636 München
Telefon: 089 1212-3300
E-Mail: zac@polizei.bayern.de

Die ZAC ist als zentraler Ansprechpartner bei der Bayerischen Polizei für alle bayerischen Unternehmen, Behörden, Verbände und sonstigen Institutionen angesiedelt. Als kompetenter Partner ist die ZAC nicht nur „Ersthelfer" und Berater für von Cyberkriminalität betroffene Stellen, sondern berät interessierte Stellen auch präventiv.

Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)
Promenade 18, 91522 Ansbach
Postfach 1349, 91504 Ansbach
Telefon: 0981 180093-0
Telefax: 0981 180093-800
E-Mail: poststelle@lda.bayern.de

Das BayLDA überwacht die Einhaltung des Datenschutzrechts im nicht-öffentlichen Bereich in Bayern, d. h. in den privaten Wirtschaftsunternehmen, bei den freiberuflich Tätigen, in Vereinen und Verbänden sowie im Internet. Auf die Einhaltung der datenschutzrechtlichen Vorschriften bei den Verantwortlichen und Auftragsverarbeitern hat insbesondere der betriebliche Datenschutzbeauftragte selbst hinzuwirken. Das BayLDA steht hierbei zur Unterstützung und Beratung der Datenschutzbeauftragten zur Verfügung, aber auch zur Kontrolle von Datenverarbeitungsverfahren bei Verantwortlichen.



www.justiz.bayern.de

BROSCHÜREN UND INFORMATIONSMATERIAL

Das Bayerische Staatsministerium der Justiz gibt eine Reihe von Broschüren und Informationsmaterialien heraus.

Folgende Themenbereiche stehen Ihnen zur Verfügung:

- Karriere bei der bayerischen Justiz
- Vorsorge und Betreuung
- Ehrenamt in der bayerischen Justiz
- Ehe und Familie
- Recht im Alltag
- Vor Gericht

www.justiz.bayern.de/service/broschueren/

Schauen Sie mal rein!

Außerdem können Sie die Broschüren über das zentrale Broschürenportal der Bayerischen Staatsregierung anschauen, herunterladen und in Papierform kostenlos bestellen.

www.bestellen.bayern.de

WOLLEN SIE MEHR ÜBER DIE ARBEIT DER BAYERISCHEN STAATSREGIERUNG ERFAHREN?

BAYERN | DIREKT ist Ihr direkter Draht zur Bayerischen Staatsregierung. Unter Telefon 089 12 22 20 oder per E-Mail unter direkt@bayern.de erhalten Sie Informationsmaterial und Broschüren, Auskunft zu aktuellen Themen und Internetquellen sowie Hinweise zu Behörden, zuständigen Stellen und Ansprechpartnern bei der Bayerischen Staatsregierung.

Die Servicestelle kann keine Rechtsberatung in Einzelfällen geben!

BAYERN | DIREKT
www.bayern.de Tel. 089 12 22 20

Justiz ist für die Menschen da.