Digitale Gewalt

Cyberstalking erkennen.
Beweise sichern.
Sicherheit zurückgewinnen.



11/2026

Praxisleitfaden für Betroffene, Angehörige und ihr Umfeld

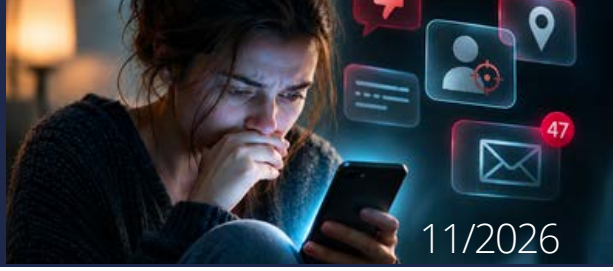
Sie sind nicht allein.
Digitale Gewalt, Cyberstalking und unbefugte Zugriffe auf Konten oder Geräte können sehr belastend sein. Dieser Leitfaden unterstützt Sie dabei, die Situation einzuordnen, Ihre persönliche und digitale Sicherheit zu verbessern sowie Beweise zu sichern.

Sofort-Checkliste

- ○ Bei akuter Gefahr: 110 wählen
- ○ Eine Vertrauensperson informieren (am besten eine Beratungsstelle)
- ○ Vorfälle mit Datum und Uhrzeit dokumentieren
- ○ Screenshots, Nachrichten und E-Mails sichern
- ○ Wichtiges E-Mail-Konto über ein sicheres Gerät absichern
- ○ Passwörter ändern und Zwei-Faktor-Authentisierung aktivieren
- ○ Standortfreigaben und verknüpfte Geräte prüfen
- ○ Bank und Mobilfunkanbieter bei Verdacht informieren
- ○ Beratungsstelle, Polizei oder Rechtsberatung kontaktieren

SYSTAG GmbH · Gutenbergstr. 47, 72555 Metzingen · 07123 - 9202-333 · cybersecurity@systag.com

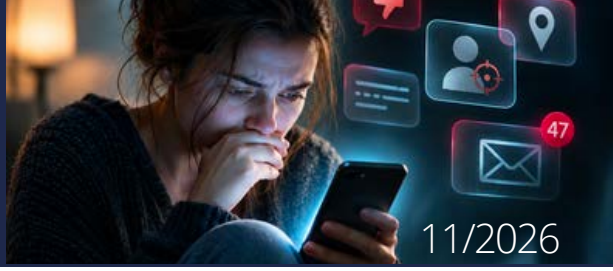
Inhalt



11/2026

Budget	3
Sofortmaßnahmen bei akuter Gefahr	3
Digitale Vorfälle dokumentieren und Beweise sichern	4
Sichere Kommunikationswege einrichten	4
E-Mail-Konten und Passwörter	5
Smartphones, Tablets und Computer	5
Standortfreigaben, Tracker und vernetzte Geräte	5
Router, WLAN und Smart-Home-Systeme	6
Mobilfunkvertrag, SIM-Karte und eSIM	6
Bankkonten und Zahlungsdienste	7
Soziale Netzwerke, Messenger und Online-Profile	7
Fake-Profile und unerwünschte Inhalte	7
Beratungsstellen und weitere Hilfsangebote	8
Disclaimer, Rechtliche Einordnung	9

SYSTAG GmbH · Gutenbergstr. 47, 72555 Metzingen · 07123 - 9202-333 · cybersecurity@systag.com



Bei akuter Gefahr

Wenn Sie sich bedroht fühlen, Gewalt befürchten oder vermuten, dass jemand Zugang zu Ihrer Wohnung oder Ihren Geräten hat:

1. Wählen Sie im Notfall die 110.
2. Bringen Sie sich an einen sicheren Ort.
3. Informieren Sie eine Person Ihres Vertrauens.
4. Treffen Sie die betreffende Person nicht allein, wenn Sie sich dabei unsicher fühlen.
5. Vermeiden Sie direkte Konfrontationen, wenn diese die Situation verschärfen könnten.

Cyberstalking kann strafbar sein. § 238 Strafgesetzbuch regelt die Strafbarkeit von Nachstellung, wenn eine Person wiederholt und unbefugt verfolgt, überwacht oder in ihrer Lebensgestaltung erheblich beeinträchtigt wird.

DIE WICHTIGSTEN SCHRITTE IM ÜBERBLICK

Persönliche Sicherheit priorisieren
Technische Maßnahmen sind wichtig, aber ersetzen keine persönliche Sicherheitsplanung. Wenn Sie sich bedroht fühlen, holen Sie frühzeitig Unterstützung – etwa bei der Polizei, Beratungsstellen, einer Rechtsberatung oder vertrauten Personen.

Beweise sichern – bevor Sie etwas löschen
Sichern Sie auffällige Nachrichten, E-Mails, Screenshots, Anruflisten, Bilder, Beiträge und Konto-Benachrichtigungen, bevor Sie Accounts bereinigen oder Geräte zurücksetzen. Die Polizei empfiehlt, digitale Beweise möglichst frühzeitig zu sichern und zur Anzeigenerstattung mitzubringen. Falls dies zu belastend ist, kann eine Vertrauensperson die Sicherung übernehmen.

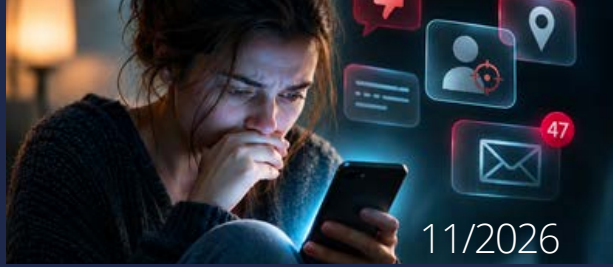
Wichtig: Setzen Sie ein möglicherweise betroffenes Smartphone oder einen Computer nicht vorschnell zurück. Dabei können wichtige Beweise verloren gehen. Holen Sie bei einem konkreten Verdacht fachliche Unterstützung ein.

Einen sicheren Kommunikationsweg schaffen
Wenn Sie vermuten, dass Ihr Smartphone, Computer oder E-Mail-Konto betroffen sein könnte:

- Nutzen Sie für wichtige Änderungen ein vertrauenswürdiges Gerät.
- Richten Sie bei Bedarf eine neue E-Mail-Adresse für sensible Kommunikation ein.
- Teilen Sie diese Adresse nur mit wenigen, vertrauenswürdigen Personen und Stellen.
- Melden Sie sich auf möglicherweise kompromittierten Geräten nicht in neu eingerichtete oder besonders wichtige Konten ein.

SYSTAG GmbH · Gutenbergstr. 47, 72555 Metzingen · 07123 - 9202-333 · cybersecurity@systag.com

Vorfälle dokumentieren und Konten absichern



11/2026

VORFÄLLE DOKUMENTIEREN

Ein Vorfallsprotokoll schafft Übersicht und kann bei einer Anzeige, rechtlicher Beratung oder technischer Untersuchung helfen. Notieren Sie zu jedem Vorfall:

Datum und Uhrzeit – z. B. 14.09.2026, 22:43 Uhr
Was ist passiert? – z. B. unbekannte Anmeldung im E-Mail-Konto
Wo ist es passiert? – z. B. Messenger, Social Media, Online-Banking, Wohnung
Welche Beweise gibt es? – z. B. Screenshot, E-Mail, Konto-Benachrichtigung
Wer könnte etwas beobachtet haben? – z. B. Nachbarin, Freund, Kollegin
Welche Folgen hatte es? – z. B. Passwort geändert, Konto gesperrt, Termin abgesagt

Zusätzlich sinnvoll:

- Screenshots mit sichtbarem Absender, Datum, Uhrzeit und Internetadresse sichern;
- E-Mails im Original aufbewahren;
- Chatverläufe exportieren, wenn die Plattform dies ermöglicht;
- Links zu Profilen, Beiträgen oder Fake-Accounts dokumentieren;
- Kopien der Beweise sicher speichern, beispielsweise auf einem verschlüsselten Datenträger oder bei einer Vertrauensperson.

KONTEN ABSICHERN – DIE RICHTIGE REIHENFOLGE

Das E-Mail-Konto ist besonders wichtig: Darüber lassen sich häufig Passwörter zurücksetzen und Sicherheitsinformationen anderer Dienste empfangen. Gehen Sie daher idealerweise in dieser Reihenfolge vor:

1. Primäres E-Mail-Konto
2. Passwortmanager
3. Apple-, Google- oder Microsoft-Konto
4. Bankkonten und Zahlungsdienste
5. Messenger und soziale Netzwerke
6. Cloud-Speicher
7. Online-Shops, Buchungsportale und Kundenkonten
8. Mobilfunkanbieter, Versicherungen und Behördenportale

Für jedes wichtige Konto gilt:

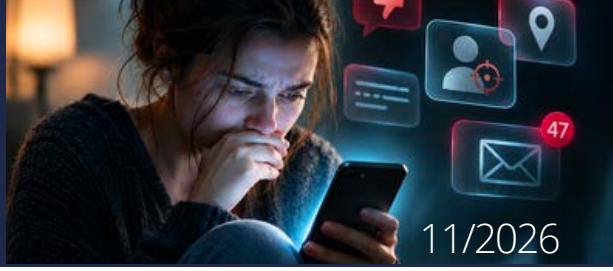
- Ist das Passwort lang, individuell und nur für dieses Konto verwendet?
- Ist Zwei-Faktor-Authentisierung aktiviert?
- Sind Wiederherstellungs-E-Mail-Adresse und Telefonnummer korrekt?
- Sind unbekannte Geräte oder aktive Sitzungen angemeldet?
- Gibt es unbekannte Drittanbieter-Apps oder App-Passwörter?
- Wurden Kontaktdaten, Lieferadressen oder Zahlungsdaten verändert?
- Gibt es automatische Weiterleitungen oder Freigaben?

Tipp: Verwenden Sie für jedes Konto ein eigenes Passwort. Ein Passwortmanager kann dabei helfen, lange und individuelle Kennwörter sicher zu verwalten.

SYSTAG.COM

SYSTAG GmbH · Gutenbergstr. 47, 72555 Metzingen · 07123 - 9202-333 · cybersecurity@systag.com

E-Mail, Geräte und Standortfreigaben prüfen



11/2026

E-MAIL-KONTO PRÜFEN UND ABSICHERN

Ändern Sie das Passwort eines möglicherweise betroffenen E-Mail-Kontos nur über ein vertrauenswürdiges Gerät (am besten ein Gerät von Freunden oder Neugerät) .

Prüfen Sie insbesondere:

- automatische Weiterleitungen;
- E-Mail-Regeln und Filter;
- hinterlegte Wiederherstellungsdaten;
- angemeldete Geräte und aktive Sitzungen;
- unbekannte App-Passwörter;
- Anwendungen von Drittanbietern mit Zugriff auf Ihr Postfach;
- Sicherheitsmeldungen zu Logins oder Passwortänderungen.

Melden Sie unbekannte Geräte und Sitzungen ab. Ändern Sie **danach** das Passwort und aktivieren Sie Zwei-Faktor-Authentisierung.

SMARTPHONE, TABLET UND COMPUTER ABSICHERN

Cyberstalking kann über unbefugte Kontozugriffe, Standortfreigaben, verknüpfte Geräte, Fernzugriffe oder unerwünschte Software erfolgen. Das BSI weist darauf hin, dass dabei unter anderem sogenannte Stalkerware auf mobilen Geräten eingesetzt werden kann.

Prüfen Sie auf allen Geräten:

- Ist das Betriebssystem aktuell?
- Sind alle Apps auf dem neuesten Stand?
- Ist der Geräte-PIN, Sperrcode oder das Anmeldekennwort sicher?
- Sind unbekannte Fingerabdrücke, Gesichtsdaten oder Benutzerkonten hinterlegt?
- Gibt es unbekannte Apps, Profile oder Geräteverwaltungen?
- Welche Apps dürfen auf Standort, Kamera, Mikrofon, Kontakte und Fotos zugreifen?
- Welche Geräte sind mit Ihrem Konto oder Ihrem Smartphone verknüpft?
- Sind Standortfreigaben aktiv?

Bei einem begründeten Verdacht auf unerwünschte Software kann ein Zurücksetzen auf Werkseinstellungen sinnvoll sein. Dies sollte jedoch erst nach einer möglichen Beweissicherung und einer individuellen Einschätzung erfolgen. Das BSI nennt einen Werksreset mit anschließender Neuinstallation von Apps als mögliche Maßnahme nach einem Sicherheitsvorfall.

STANDORTFREIGABEN, TRACKER UND VERNETZTE GERÄTE PRÜFEN

Überprüfen Sie, ob Ihr Standort mit anderen Personen geteilt wird. Dies kann unter anderem über folgende Dienste erfolgen:

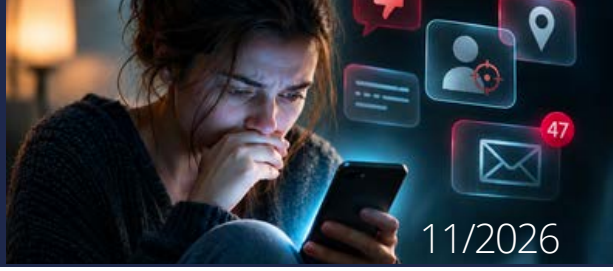
- Apple „Wo ist?“
- Google Maps
- Messenger-Dienste
- Fitness- und Gesundheits-Apps
- Familien- und Kalender-Apps
- Smartwatches
- Fahrzeuge und Fahrzeug-Apps
- Bluetooth-Tracker, beispielsweise AirTags oder vergleichbare Produkte

Prüfen Sie, ob unbekannte Tracker in Taschen, Fahrzeugen oder persönlichen Gegenständen auftauchen. Viele moderne Smartphones informieren über fremde Tracker, die sich über längere Zeit mit Ihnen bewegen.

SYSTAG.COM

SYSTAG GmbH · Gutenbergstr. 47, 72555 Metzingen · 07123 - 9202-333 · cybersecurity@systag.com

Router, WLAN, Smart Home & Mobilfunk



11/2026

ROUTER, WLAN UND SMART HOME ABSICHERN

Wenn eine andere Person Zugang zu Ihrer Wohnung, Ihrem Router oder Smart-Home-System hatte, sollten Sie auch diese Systeme überprüfen.

Router und WLAN

- Ändern Sie das Administrator-Passwort des Routers.
- Ändern Sie das WLAN-Passwort.
- Prüfen Sie das Gäste-WLAN.
- Deaktivieren Sie WPS.
- Installieren Sie aktuelle Firmware-Updates.
- Prüfen Sie Fernzugriffe, VPN-Verbindungen und Portfreigaben.
- Kontrollieren Sie die Liste bekannter Geräte und entfernen Sie unbekannte Geräte.
- Beziehen Sie WLAN-Repeater, Powerline-Adapter und Mesh-Systeme ein.

Ein versteckter WLAN-Name bietet keinen wirksamen zusätzlichen Schutz. Wichtig sind ein starkes Passwort, aktuelle Verschlüsselung und ein sicher konfigurierter Router.

Smart Home und digitale Zutrittssysteme

Prüfen Sie insbesondere:

- smarte Türschlösser und Zugangscodes;
- Fingerabdrücke oder andere biometrische Zugänge;
- Video-Türklingeln und Überwachungskameras;
- Alarmanlagen;
- Sprachassistenten;
- Licht-, Heizungs- und Garagensteuerungen;
- gemeinsame Haushalts- oder Familienzugänge.

Entziehen Sie nicht mehr benötigte Berechtigungen und ändern Sie Zugangscodes. Wenn Zugriff auf Wohnungsschlüssel möglich war, kann der Austausch von Schlössern sinnvoll sein.

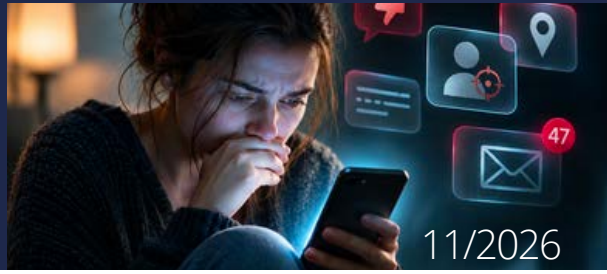
MOBILFUNKVERTRAG, SIM-KARTE UND ESIM PRÜFEN

Der Mobilfunkvertrag ist wichtig für SMS-Codes, Passwort-Wiederherstellungen und Freigaben beim Online-Banking. Wenden Sie sich bei einem Verdacht an Ihren Mobilfunkanbieter und prüfen Sie:

- hinterlegte Vertrags- und Kontaktdaten;
- Kundenkennwort oder Service-PIN;
- registrierte SIM-Karten und eSIMs;
- Ersatz-SIM-Karten;
- Optionen für Rufnummernmitnahme;
- Drittanbietersperren;
- ungewöhnliche Vertragsänderungen.

SYSTAG GmbH · Gutenbergstr. 47, 72555 Metzingen · 07123 - 9202-333 · cybersecurity@systag.com

Bank, Profile und was Sie vermeiden sollten



11/2026

BANKKONTEN UND ZAHLUNGSDIENSTE ABSICHERN

Informieren Sie Ihre Bank oder Ihren Zahlungsdienstleister unverzüglich, wenn ein unbefugter Zugriff möglich ist.

Teilen Sie mit:

- Es besteht ein IT-Sicherheitsvorfall oder ein entsprechender Verdacht.
- Eine andere Person könnte Zugriff auf Geräte, Daten oder Zugangsdaten gehabt haben
- Sie bitten um Prüfung und Absicherung Ihrer Konten.

Prüfen Sie:

- letzte Umsätze und offene Aufträge;
- hinterlegte Telefonnummern und E-Mail-Adressen;
- registrierte Geräte für TAN- oder Freigabe-Apps;
- gespeicherte Zahlungsarten bei Online-Shops;
- hinterlegte Lieferadressen;
- Bankvollmachten und andere Berechtigungen.

Wichtig: Eine **Bankvollmacht** bleibt bestehen, bis sie ausdrücklich widerrufen wird. Eine Passwortänderung allein reicht dafür nicht aus.

SOZIALE NETZWERKE, MESSENGER ONLINE-PROFILE und APPS

Prüfen Sie bei Messenger-Diensten, sozialen Netzwerken, Dating-Plattformen und Online-Marktplätzen:

- angemeldete Geräte und aktive Sitzungen;
- verknüpfte E-Mail-Adressen und Telefonnummern;
- Zwei-Faktor-Authentisierung;
- Privatsphäre- und Sichtbarkeitseinstellungen (setzen Sie Profile auf privat, prüfen Ihre Freundeslisten und Gruppenmitgliedschaften)
- Standortfreigaben; nicht nur bei Apps sondern auch Dienste wie Apcoa-Flow (wo gehen die Emails hin)
- unbekannte Drittanbieter-Apps;
- Apps fürs Auto - man kann darüber nicht nur die Klima einschalten sondern auch den Standort tracken
- unbekannte Nachrichten, Beiträge oder Werbeanzeigen;
- gefälschte Profile mit Ihrem Namen oder Ihren Bildern.

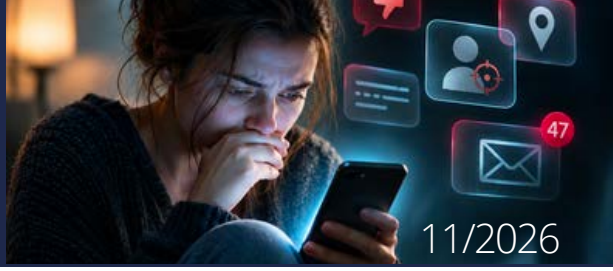
Melden Sie Fake-Profile und rechtswidrige Inhalte direkt bei der jeweiligen Plattform. Dokumentieren Sie vorher die Internetadresse, Screenshots sowie Datum und Uhrzeit.

WAS SIE MÖGLICHST VERMEIDEN SOLLTEN

- Öffnen Sie keine unerwarteten Links oder Dateianhänge.
- Geben Sie keine Passwörter oder Sicherheitscodes weiter.
- Löschen Sie mögliche Beweise nicht vorschnell.
- Verwenden Sie Passwörter nicht mehrfach.
- Konfrontieren Sie eine verdächtigte Person nicht, wenn Sie eine Eskalation befürchten.
- Installieren Sie keine unbekannten „Sicherheits-“ oder „Überwachungs-Apps“.
- Melden Sie sich auf möglicherweise kompromittierten Geräten nicht in besonders wichtige Konten ein.

SYSTAG GmbH · Gutenbergstr. 47, 72555 Metzingen · 07123 - 9202-333 · cybersecurity@systag.com

Hilfe und Beratung



11/2026

HateAid – Hilfe bei digitaler Gewalt
Beratung bei Hass im Netz und digitaler Gewalt, einschließlich Unterstützung bei der Einschätzung rechtlicher Handlungsmöglichkeiten.
030 252 088 38 · Mo. 10–13 Uhr, Do. 15–18 Uhr
Onlinehilfe und Betroffenenberatung: HateAid

WEISSER RING – Opferhilfe und Beratung
Unterstützung für Betroffene von Straftaten, darunter Cyberstalking. Kostenlose und anonyme Beratung.
116 006 · täglich 7–22 Uhr
WEISSER RING e. V.

Hilfetelefon Gewalt gegen Frauen – Hilfe bei Stalking und Gewalt

Kostenlose, anonyme und mehrsprachige Beratung für betroffene Frauen, auch bei Cyberstalking.
116 016 · rund um die Uhr
Onlineberatung per Chat und E-Mail: onlineberatung.hilfetelefon.de

Nummer gegen Kummer – Kinder- und Jugendtelefon
Anonyme und kostenlose Beratung bei Cybermobbing, Belästigung, Bedrohungen und anderen Sorgen.
116 111 Mo.–Sa. 14–20 Uhr
Onlineberatung per Mail und Chat: Nummer gegen Kummer

JUUUPORT – Hilfe bei Problemen im Netz
Kostenlose und vertrauliche Onlineberatung durch speziell geschulte Jugendliche, beispielsweise bei Cybermobbing, Sextortion und sexueller Belästigung im Internet.
Zur Onlineberatung: juuuport.de

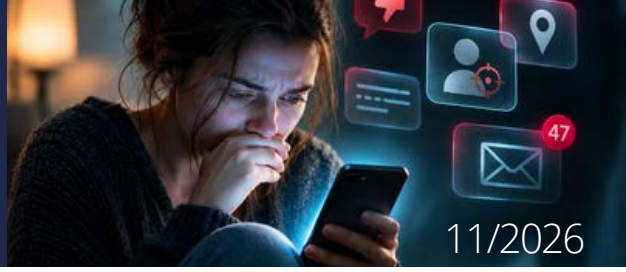
JugendNotmail – Psychosoziale Onlineberatung
Vertrauliche und kostenlose Beratung für Kinder und Jugendliche bei Gewalt, Mobbing, Ängsten und psychischen Belastungen.
Zur Onlineberatung: https://jugendnotmail.de/

Bei akuter Bedrohung: Polizei unter 110 verständigen. Beratungsstellen ersetzen keine polizeiliche Soforthilfe. Sie können sich außerdem an eine Polizeidienststelle wenden und Anzeige erstatten. Die Polizeiliche Kriminalprävention informiert über Stalking, Cyberstalking, Beweissicherung und Schutzmöglichkeiten.

Weitere Unterstützung
- Fachberatungsstellen gegen Stalking und Gewalt in Ihrer Region
- Rechtsanwältinnen und Rechtsanwälte, beispielsweise mit Schwerpunkt Strafrecht, Familienrecht oder Opfervertretung
- IT-Forensik und IT-Sicherheitsberatung bei konkreten technischen Verdachtsmomenten

SYSTAG GmbH · Gutenbergstr. 47, 72555 Metzingen · 07123 - 9202-333 · cybersecurity@systag.com

Hilfe und Beratung



11/2026

WEITERE UNTERSTÜTZUNG

- Fachberatungsstellen gegen Stalking und Gewalt in Ihrer Region
- Rechtsanwältinnen und Rechtsanwälte, beispielsweise mit Schwerpunkt Strafrecht, Familienrecht oder Opfervertretung
- IT-Forensik und IT-Sicherheitsberatung bei konkreten technischen Verdachtsmomenten

SCHLUSSWORT

Digitale Gewalt und Cyberstalking können das Sicherheitsgefühl nachhaltig beeinträchtigen. Sie müssen die Situation nicht allein bewältigen.
Sichern Sie Beweise, holen Sie Unterstützung und gehen Sie technische Maßnahmen Schritt für Schritt an. Technische Schutzmaßnahmen können Risiken deutlich reduzieren, ersetzen jedoch keine persönliche Sicherheitsplanung, psychosoziale Beratung oder rechtliche Unterstützung.

Hinweis: Dieser Leitfaden bietet allgemeine Informationen und ersetzt keine individuelle Rechtsberatung, psychologische Beratung, polizeiliche Gefährdungseinschätzung oder IT-forensische Untersuchung.

Fehlt etwas in unserem Leitfaden?

Haben wir etwas übersehen? Fehlen wichtige Informationen oder hilfreiche Anlaufstellen? Dann schreiben Sie mir gerne direkt eine E-Mail an linda.weidenbacher@systag.com! Ich freue mich über Ihre Hinweise und Anregungen, damit wir den Leitfaden gemeinsam noch hilfreicher gestalten können.

Herausgeber: SYSTAG GmbH, Gutenbergstraße 47, 72555 Metzingen
Telefon: +49 7123 9202-0 · E-Mail: cybersecurity@systag.com · Web: www.systag.com

Stand: November 2026

Senden Sie uns eine vertrauliche Email.