STW Sicherheitsleitfaden (Version 2024.06)

STW Datentechnik GmbH & Co. KG
Pestalozzistraße 2–4
36132 Eiterfeld

T: 06672.86919-0 | F: 06672.86919-50
M: vertrieb@stw-datentechnik.de
stw-datentechnik.de

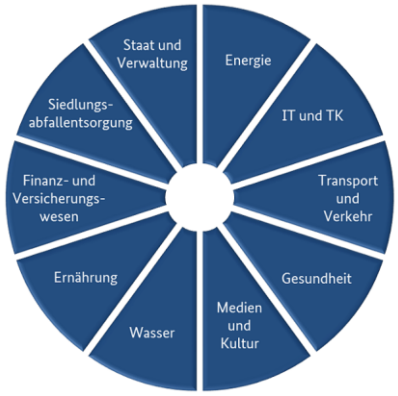
Durch die wachsende Komplexität der IT-Strukturen und die Tatsache, dass immer mehr Cyberangriffe auf Unternehmen durchgeführt werden, sind IT-Sicherheitsmaßnahmen regelmäßig zu prüfen und bei Bedarf entsprechend anzupassen.

Da jedes Unternehmen eine betriebliche Organisationspflicht hat möchten wir Sie deshalb informieren und Sie dafür sensibilisieren.

Bundesamt für Sicherheit in der Informationstechnik

Umfassende Informationen bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI). Sie sollten sich hier auch entsprechend informieren: BSI - Bundesamt für Sicherheit in der Informationstechnik

Anforderungen an kritische Infrastrukturen (KRITIS)



Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

BSI - Allgemeine Informationen zu KRITIS (bund.de)

Wir als STW Datentechnik sehen es als unsere Pflicht an Sie entsprechend zu informieren und besprechen gerne mit Ihnen Möglichkeiten der Vorkehrung. Es sei aber immer wieder gesagt, dass niemand 100% Schutz bieten kann. Weiterhin muss jedes Unternehmen eine Abwägung bzgl. der Kosten machen.

Laut Umfragen geht der aktuelle Trend dazu, dass Unternehmen sich nicht mehr die Frage stellen ob, sondern wann man Opfer einer Cyberattacke wird. In welchem Umfang auch immer. Das Unternehmen, welches sich vorbereitet hat (Präventiv-Maßnahmen getroffen hat) ist dann besser vorbereitet.

Nachfolgend stellen wir Ihnen Präventiv-Maßnahmen vor. Maßnahmen die mit 👍 gekennzeichnet sind sehen wir als sehr wichtig an. Alle anderen Maßnahmen haben ebenfalls Ihre Daseinsberechtigung. Jedes Unternehmen muss dies für sich bewerten. Wir helfen gerne.

STW Datentechnik GmbH & Co. KG
Pestalozzistraße 2–4
36132 Eiterfeld

T: 06672.86919-0 | F: 06672.86919-50
M: vertrieb@stw-datentechnik.de
stw-datentechnik.de

Stellen Sie sich bitte folgendes Szenario vor

**Wir möchten keine Angst machen, sondern möchten Sie nur sensibilisieren.
Wir hoffen das nichts von dem hier Beschriebenen eintritt!**

Sie und Ihre Mitarbeiter kommen morgens ins Unternehmen und müssen feststellen, dass keine Anmeldung mehr an den IT-Systemen möglich ist.

Sie werden dann umgehend die IT-Abteilung oder der IT-Dienstleister anrufen.

Meist gibt es dann auch schnell die Meldung - Cyber Attacke und eine entsprechende Lösegeldforderung.

Die IT-Abteilung/IT-Dienstleister muss dann auch erkennen, dass viele oder gar alle Systeme betroffen sind.

Sehr häufig übernehmen die Angreifer das sog. Windows Domain Netzwerk und verschaffen sich dann die notwendigen administrativen Berechtigungen.

Ab diesem Zeitpunkt handeln die Hacker wie ein eigener Administrator!

Es werden meist als erstes große Datenmengen aus dem Netzwerk gestohlen und dann tritt die Verschlüsselung der Daten auf der Infrastruktur ein.

Sollte auch der Zugang zum Backupsystem gelingen, wird versucht die Backups zu löschen. Dies erfolgt oft auch direkt über die Backupsoftware und auf allen angeschlossenen Datensicherungsmedien, wie NAS-System, USB-Festplatten usw.

Somit sind die erstellten Backups unbrauchbar bzw. nicht mehr existent.

Jetzt ist überlegtes und zielgerichtetes Handeln wichtig damit auch die rechtlichen Schritte und Fristen von Meldungen usw. eingehalten werden.

Je nach Umfang müssen das BSI und andere Stellen informiert werden. Wenn man eine Cyber-Versicherung abgeschlossen hat, so ist dies oft die erste sichere Anlaufstelle da dort die Experten den weiteren Ablauf mit Ihnen koordinieren.

Nicht selten müssen Forensiker eingeschaltet werden und die Systeme dürfen nicht mehr „angefasst" werden. Eine Freigabe dauert nicht selten mehrere Tage bis Wochen.

Liegt ein Offline-Backup vor, so ist hier auch zu prüfen, ob nicht die Schadsoftware bereits in älteren Backupsätzen enthalten ist. Diese Prüfung ist sehr zeitaufwändig und oft bleibt auch hier ein Restrisiko.

Eine Rücksicherung des Backups ist dann erstmal nicht auf den befallen Systemen möglich.

Jetzt stellt sich die Frage: Wie lange kann das Unternehmen ohne IT-Systeme auskommen? Da die Antwort meist im Bereich von wenigen Tagen liegt muss ein Notfallsystem aufgebaut werden.

Nur wenn es im Vorfeld einen getesteten Notfallplan gibt, hat man eine Chance hier erfolgreich zu sein.

Läuft die Firma im Notfallbetrieb, so muss nach Freigabe auch wieder der Normalbetrieb erfolgen und die Systeme aktualisiert und zurückgespielt werden.

STW Datentechnik GmbH & Co. KG
Pestalozzistraße 2–4
36132 Eiterfeld

T: 06672.86919-0 | F: 06672.86919-50
M: vertrieb@stw-datentechnik.de
stw-datentechnik.de

BASIS Schutz eines jeden Unternehmen
Überwachung, Patchverwaltung, Virenschutz und Kennwortrichtlinien

STW-Monitoring Überwachung	Hier managen wir Ihre Serversysteme und Arbeitsplätze. Wir erkennen Hardwareausfälle und weitere Systemstörungen.
STW-Monitoring MS-Patchverwaltung	In diesem Baustein führen wir regelmäßige Patchprüfungen durch und installieren entsprechend die von Microsoft zur Verfügung gestellten Sicherheitsupdates.
STW-Monitoring **Dritt-Anbieter-Patchverwaltung**	Zentrale Verwaltung der Patches, Updates von Drittanbieter Software und Steuerung der Installation. Erweitertes Software-Management ist ein integriertes Patch-Management-System von **Drittanbietern**, mit dem Sie alle von Ihnen verwalteten Geräte mit den neuesten Funktionen und Sicherheitspatches für über 100 Softwareanbieter auf dem neuesten Stand halten können. Da immer mehr Applikationen von Sicherheitslücken betroffen sind empfehlen wir diesen Baustein sehr.
STW-Monitoring Virenschutz Erweiterung	Die Virenschutzrichtlinien sollten über dem Standard liegen. Hier können wir den Virenschutz um folgende Funktionen erweitern: **Verhaltensschutz:** Blockiert gefährliche Programme und Anwendungen auf Ihrem Gerät. **CyberCapture:** Sendet verdächtige Dateien zur Analyse an das Virenlabor.
Kennwortrichtlinie	Einführung und Umsetzung einer komplexeren Kennwortrichtlinie. Durch die Aktivierung und Umsetzung einer unternehmensweiten Kennwortrichtlinie, kann man der Tatsache entgegenwirken, dass zu schwache oder alte Passwörter von Angreifern ausgenutzt werden.
Multifaktor-Authentifizierung (MFA)	Durch die Aktivierung einer Multifaktor-Authentifizierung wird zusätzlich zu den bekannten Sicherheitsmerkmalen (Benutzername und Kennwort) noch ein weiterer Faktor benötigt, um sich gegenüber der Anwendung zu authentifizieren. Dies ist in der Regel eine am Smartphone installierte App, welche einen für eine begrenzte Zeit gültigen Zugangscode generiert. Erst nachdem Benutzername, Passwort und der temporäre Code erfolgreich übermittelt wurden, wird der Zugriff gestattet. So wirkt man der Tatsache entgegen, dass ein Angreifer den Benutzername und das dazugehörige Passwort ermittelt hat. Er müsste dann zusätzlich noch den Code haben, was den Zugriff auf das Smartphone voraussetzen würde. Der Code kann auch über ein Hardwaretoken (spezielle USB-Sticks) generiert werden. Dies ist sehr wichtig bei Cloud-Diensten wie Microsoft 365 aber auch anderen wichtigen Verbindungen zum Unternehmensnetzwerk wie VPN-Zugänge, Einkaufsportale etc.

STW Datentechnik GmbH & Co. KG
Pestalozzistraße 2–4
36132 Eiterfeld

T: 06672.86919-0 | F: 06672.86919-50
M: vertrieb@stw-datentechnik.de
stw-datentechnik.de

Regelmäßige IT-CHECKs sind einzuplanen

damit der einmal eingerichtete Schutz auch Bestand hat und Anpassungen im Laufe der Zeit berücksichtig werden!

Regelmäßige IT-CHECKs	
Firewall CHECK	Wir empfehlen die Firewall Funktionen regelmäßig zu prüfen. Hier ist besonders die Prüfung von verschlüsselten Verbindungen (DPI-SSL) zu aktivieren. Auch sollten die Firewall Regeln kritisch geprüft werden und nur die notwendigsten Ports freigegeben werden. Nicht genutzte Regeln sollten gelöscht werden. Der Aufbau von VPN-Verbindungen sind nur mittels einem zusätzlichen Faktor neben Benutzername und Passwort (MFA) erlaubt.
Dienste CHECK	Keine Dienste mit User Anmeldung durchführen! Alle Dienste auf den Systemen müssen geprüft werden. Es sollten keine Systemdienste unter einer Benutzeranmeldung laufen. Hier sind sog. Service Accounts anzulegen.
Rechte CHECK	Berechtigung von Anwender prüfen und einschränken! Anwender sollten nur die notwendigen Berechtigungen in den Systemen erhalten. Sie sollten z.B. keine lokalen Adminrechte auf Ihren Arbeitsplätzen haben. Im Falle eines Angriffs übernehmen die Hacker so das Konto des Anwenders und haben damit erhöhte Rechte.
eMail CHECK	Überprüfung der aktuellen Sicherheitstechniken. Sender- und Empfängerreputation. Störungen in der Kommunikation zwischen Absender und Empfänger vermeiden. Deshalb werden DNS Einträge geprüft, erweitert oder entfernt.
Domain CHECK	Überprüfung der Microsoft Domaine (AD) auf aktuelle Authentifizierungstechniken. Deaktivierung veralteter Techniken und Verschlüsselungsmechanismen. Weiterhin auch Prüfung von veralteten Benutzerkonten, Computerkonten und Freigaben. Aber auch sind Anwendungen zu prüfen, die an der Windows Domaine angebunden sind und Daten auslesen.

STW Datentechnik GmbH & Co. KG
Pestalozzistraße 2–4
36132 Eiterfeld

T: 06672.86919-0 | F: 06672.86919-50
M: vertrieb@stw-datentechnik.de
stw-datentechnik.de

Sicherheit Trainings für Ihre Mitarbeiter

Allein kann die IT den Kampf gegen Cybercrime nicht gewinnen. Machen Sie alle Mitarbeitenden mit den Awareness Trainings und Phishing-Simulationen fit!

Ob Phishing, Smishing oder Business E-Mail Compromise – Cybercrime nutzt viele Wege, um Mitarbeitende hinters Licht zu führen.

Die Gefahr wird von vielen Unternehmen jedoch unterschätzt. Oder anders ausgedrückt: Die IT wird sich schon darum kümmern.

Doch sichere Passwörter zu nutzen, MFA zu aktivieren und gefährliche Anhänge in Mails zu melden, geht alle etwas an.

Security Awareness Trainings	Mit spannenden Online-Kursen und regelmäßigen Phishing-Simulationen stärken Sie die Sicherheitskultur in Ihrem Unternehmen.
Phishing-Simulation (Kampagne)	Testen Sie im echten Arbeitsalltag, wie Ihre Mitarbeitenden auf gefährliche Mails und Phishing-Versuche reagieren. Wir senden vorgetäuschte Phishing-Mails direkt in die Postfächer Ihres Teams. Sie erhalten einen nachvollziehbaren Bericht mit Kennzahlen, wie oft potenziell gefährliche Anhänge geöffnet oder Daten herausgegeben wurden. So wird das Sicherheitsbewusstsein messbar.
Online-Trainings und Unterweisungen	Die Kurse stellen Sie Ihren Mitarbeitenden bequem über unser Learning Management System zur Verfügung. Alle User greifen direkt über den Browser darauf zu und starten ihr erstes E-Learning nach dem Einloggen mit nur zwei Klicks. Sie benötigen in Ihrem Unternehmen nur eine Plattform auf dem Sie sowohl Security Awareness Trainings als auch betriebliche Unterweisungen einfach online durchführen. Ihr Team muss sich an nur eine neue Plattform gewöhnen und Sie nur ein System administrieren. Ein Gewinn für alle.

STW Datentechnik GmbH & Co. KG
Pestalozzistraße 2–4
36132 Eiterfeld

T: 06672.86919-0 | F: 06672.86919-50
M: vertrieb@stw-datentechnik.de
stw-datentechnik.de

Datenorganisation und Datensicherung

Analyse der Daten bis zum Notfall Sicherungskonzept

Nur wer die Daten kennt kann diese organisieren.

Daten CHECK	Es ist wichtig seine Daten zu kennen. In einem Workshop ermitteln wir mit Ihnen die wichtigsten, unternehmenskritischsten Daten (Kronjuwelen Ihres Unternehmens). Dies ist die Basis für eine konkrete Empfehlung zur Datensicherung, die auch im Notfall greift.
Datensicherung mit Offline-Auslagerung und regelmäßigem Rücksicherungstesten	Das Datensicherungskonzept muss auf Ihre Anforderungen abgestimmt sein (Daten CHECK). Hier ist zu bestimmen wie lang, welche Datensicherungen aufbewahrt werden sollen/müssen. Hier kommt auch neben Datensicherung die Archivierungsdauer zum Tragen und muss besprochen und geklärt werden! Daraus ergeben sich die Anforderungen an das Backupkonzept. Neben der Sicherung auf NAS-Systemen empfehlen wir eine Auslagerung der Sicherungen in die Cloud. Hier werden die Datensicherungen verschlüsselt abgelegt und mit einem Überschreibschutz versehen. Die Offline-Sicherung sollte zudem lokal zur Verfügung stehen. Hier empfehlen wir LTO-Bandlaufwerke. Die Bänder sind dann regelmäßig zu wechseln und an einem sicheren Ort aufzubewahren. LTO-Bänder haben eine sehr hohe Aufbewahrungsdauer von über 10 Jahren. Zudem gibt es auch Bänder, die nur einmal beschrieben werden können.

STW Datentechnik GmbH & Co. KG
Pestalozzistraße 2–4
36132 Eiterfeld

T: 06672.86919-0 | F: 06672.86919-50
M: vertrieb@stw-datentechnik.de
stw-datentechnik.de

IT Sicherheitszentrum (XDR/SOC)

Prävention, Erkennung, Untersuchung und Abwehr

Erweitert die Standard-Reaktionszeiten von STW (8-17 Uhr an Wochentagen) bis zu 24*7/24 h und bietet weitere Ergänzungen!

Extended Detection and Response (XDR)	XDR vereint Prävention, Erkennung, Untersuchung und Abwehr und bietet so Sichtbarkeit, Analysen, Warnungen und automatisierte Reaktionen – alles mit dem Ziel, die Datensicherheit zu optimieren und Bedrohungen abzuwehren/zu erkennen. Alle Sicherheitsfunktionen wie: • eMail Security • Endpoint Security • Server Security • Netzwerk Security • Cloud Security sind hier als Baustein zu buchen. Das SOC-Team schaut auf alles und handelt aktiv bei Auffälligkeiten bis hin zur automatischen Isolation von betroffenen Systemen. Erweitert die Standard-Reaktionszeiten von STW (8-17 Uhr an Wochentagen) bis zu 24*7/24h.

STW Datentechnik GmbH & Co. KG
Pestalozzistraße 2–4
36132 Eiterfeld

T: 06672.86919-0 | F: 06672.86919-50
M: vertrieb@stw-datentechnik.de
stw-datentechnik.de

Dokumentation und Notfall-Konzept

Um für eine anstehende Notfallwiederherstellung gewappnet zu sein, ist vor allem eines unabdingbar: eine saubere, lückenlose und aktuelle Dokumentation der IT-Ressourcen.

Notfallplan / Dokumentation **regelmäßige Überprüfung** **(Audit und Training)** 	Um für eine anstehende Notfallwiederherstellung gewappnet zu sein, ist vor allem eines unabdingbar: eine saubere, lückenlose und aktuelle Dokumentation der IT-Ressourcen. Eine wichtige Rolle spielen hier nicht nur die Daten über Systeme, sondern vor allem auch deren Anwender, verantwortliche Mitarbeitende, Kontaktdaten u. v. m. Eine standardisierte IT-Dokumentation sorgt im Falle eines IT-Desasters dafür, dass unmittelbar reagiert werden kann. Ein IT-Notfallhandbuch bündelt genau diese Informationen und stellt sie zentral zur Verfügung. Es bietet u. a. einen Handlungsleitfaden für den Ernstfall und kritische Situationen, enthält praktische Ansätze für Lösungen und regelt detailliert die Verantwortlichkeiten für jeden einzelnen Prozess. Dies kann im Ernstfall wichtige Zeit einsparen und größeren Schaden verhindern. **Ausdruck sämtlicher Dokumentationen und Anleitungen** Die gesamte Dokumentationen, Notfallbeschreibungen, Prozessbeschreibungen müssen ausgedruckt vorliegen. Selbst Daten, die man meist gar nicht für wesentlich erkennt sind im Notfall sehr wichtig. Diese sollten in ausgedruckter Form vorliegen. Beispiele sind Adresslisten mit Ansprechpartnern, Zugangsdaten, Kennwortliste… Regelmäßige Überprüfung sind in einem Audit durchzuführen und der Ernstfall ist zu trainieren.
Notfall Umgebung	Wie lange können Sie ohne die IT auskommen? Durch einen Cyber-Angriff kann es sein, dass Teile oder die gesamte IT-Umgebung für mehrere Tage bis Wochen nicht genutzt werden können da die Systeme durch Forensiker untersucht werden müssen. Während dieser Zeit darf die Umgebung nicht verändert werden. Dies hat den Hintergrund, dass man in der Regel immer erst versuchen wird, das Einfallstor zu ermitteln, damit das spätere System nicht wieder über diesen Weg angegriffen werden kann. Kann man evtl. eine Notfall Umgebung aktivieren damit die wichtigsten Systeme und einige Mitarbeiter arbeiten können? In einem Workshop erarbeiten wir mit Ihnen gemeinsam einen Vorschlag und prüfen die realistische Umsetzung.

STW Datentechnik GmbH & Co. KG
Pestalozzistraße 2–4
36132 Eiterfeld

T: 06672.86919-0 | F: 06672.86919-50
M: vertrieb@stw-datentechnik.de
stw-datentechnik.de

Leistungen von externen Dienstleistern	
CYBER Versicherung 	Cyber-Versicherungen decken Schäden ab. Sie klären Verdachtsfälle und bieten eine Schadenshotline damit im Schadensfall schnell und rechtssicher gehandelt werden kann. Der Cyber-Versicherer unterstützt das Notfallmanagement und liefert wichtige Maßnahmen und Empfehlungen.
IT-Sicherheits-Basis-Check	Effektiver Überblick zu Ihrem aktuellen Cyber-Sicherheitsniveau (ca. 2 Stunden) • Unabhängige Überprüfung durch Cyber-Sicherheits-Expertinnen und -Experten • Audit speziell geeignet für kleinere und mittelgroße Unternehmen/Organisationen • Bereitstellung priorisierter Handlungsempfehlungen in einem detaillierten Bericht
Deep Scan	Einmalige technische Überprüfung der aus dem Internet erreichbaren Infrastruktur auf Schwachstellen (externer Schwachstellenscan) und der Exponierung der Kundendaten in bekannten Datenlecks im Dark Web • Ergebnisbericht mit Handlungsempfehlungen zur Behebung gefundener Schwachstellen und umfangreicher Risiko-Bewertung • Inklusive einem Re-Scan, d.h., auf Wunsch findet eine erneute Überprüfung statt, um die Behebung der Schwachstellen zu verifizieren – ohne zusätzliche Kosten!
IT-Sicherheitsprüfungen	Detaillierte und unabhängige Bestimmung Ihres aktuellen Cyber-Sicherheitsniveaus durch Cyber-Sicherheits-Expertinnen und -Experten (ca. 6 Stunden) • Berücksichtigung der Vorgaben internationaler Standards • Audit speziell geeignet für mittelgroße und große Unternehmen/Organisationen • Bereitstellung priorisierter Handlungsempfehlungen in einem detaillierten Bericht
Dokumentenanalyse	Überprüfung vorhandener Sicherheitsdokumentation auf Vollständigkeit inklusive Verbesserungsvorschlägen in den Dokumentenkategorien (Auszug): • Organigramm der Sicherheitsorganisation • Leitlinie der Informationssicherheit • Themenspezifische Richtlinien der Informationssicherheit • Asset Register (Auszug) • Prozessdokumentation/Verfahrensanweisungen, z.B. Change-Management, Patch Management • Datenschutz-Handbuch und Datenschutzrichtlinie • Notfallhandbuch und Notfallpläne • Risikomanagement-Dokumentation (Risiko-Register) • Organigramm Krisenstab
IT-Schwachstellenscans – Interner Schwachstellenscan	Prüfung der internen, nicht aus dem Internet erreichbaren IP-Adressen (max. 250) • Unkomplizierte Installation und Konfiguration der technischen Parameter auf der Managed Vulnerability Scanning Plattform (MVSP)

STW Datentechnik GmbH & Co. KG
Pestalozzistraße 2–4
36132 Eiterfeld
T: 06672.86919-0 | F: 06672.86919-50
M: vertrieb@stw-datentechnik.de
stw-datentechnik.de

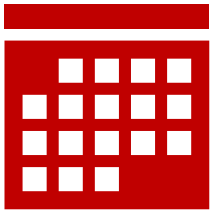
	Voll automatisierter Schwachstellenscan i.d.R. in der drei Phasen: • Identifikation der zu den angegebenen IP-Adressen gehörenden Systeme • Erkennung der auf diesen Systemen installierten Dienste • Ermittlung möglicher Schwachstellen und IT-Lücken dieser Dienste
Penetrationstests	Simulierte Hackerangriffe zum Testen bestehender Sicherheitsmechanismen, z.B.: • Identifikation ausnutzbarer Schwachstellen in der IT-Infrastruktur • Test der IT-Infrastruktur auf Sicherheitslücken • Prüfung der Wirksamkeit bestehender Schutzmaßnahmen • Abstimmungsgespräch zwischen Pentester und Kunden zur Definition von Scope und Umfang des geplanten Penetrationstests • Detaillierter Bericht mit Handlungsempfehlungen und ggf. Abschlussbesprechung • Varianten: Externer und interner Penetrationstest
Aufbau von Managementsystemen und regulatorische Beratung	Holistische Beratung durch eine ganzheitliche Betrachtung und Gestaltung einer individuellen Cyber-Sicherheitskonzeption • Einführung und Weiterentwicklung von Managementsystemen (ISMS, BCMS) im Einklang mit ISO 27001 bzw. ISO 22301 • Systematische Identifizierung, Implementierung und Überwachung erforderlicher Prozesse unter Berücksichtigung unternehmens- und branchenspezifischen Vorgaben, wie z. B. NIS2 • Richtlinien-/Gesetzeskonform bis zur Zertifizierungsreife • Stärkung der Cyber-Sicherheit dank Planbarkeit • Konkrete Ansprechpartner für alle Fragen rund um Informations-/Cyber-Sicherheit
Externe Informationssicherheitsbeauftragte (externe ISB)	Sicherstellung des für Unternehmen geeigneten Informationssicherheitsniveaus • Maßgeschneiderte und ortsunabhängige Beratung mit hoher fachlicher Expertise • Flexibilität in Zeit und Umfang • Konkrete Ansprechpartner für alle Fragen rund um Informations-/Cyber-Sicherheit

STW Datentechnik GmbH & Co. KG
Pestalozzistraße 2–4
36132 Eiterfeld

T: 06672.86919-0 | F: 06672.86919-50
M: vertrieb@stw-datentechnik.de
stw-datentechnik.de

Individuelle Beratung

Bitte Termin vereinbaren!



Wir stehen Ihnen gerne zur technischen Beratung und individuellen Abstimmung zur Verfügung. Wir führen aber keinerlei Rechtsberatung durch.

Machen Sie gerne Terminvorschläge. Bitte planen Sie für ein Erstgespräch 2 Stunden ein.

Senden Sie uns eine eMail an helpdesk@stw-datentechnik.de damit wir ein Beratungstermin vereinbaren können.

Ihr Team der

STW Datentechnik GmbH & Co. KG
Pestalozzistr. 2-4
36132 Eiterfeld

helpdesk@stw-datentechnik.de
06672-86919-0
www.stw-datentechnik.de