Cybersecurity

Unsere Leistungen für Ihre IT-Sicherheit

it.conex GmbH

Herrenbühlstraße 9
78658 Zimmern ob Rottweil

Sedanstraße 5
72764 Reutlingen

Inhalt

Ihre IT-Security als Haus

Türen/Fenster = Firewall/Antivirenprogramme

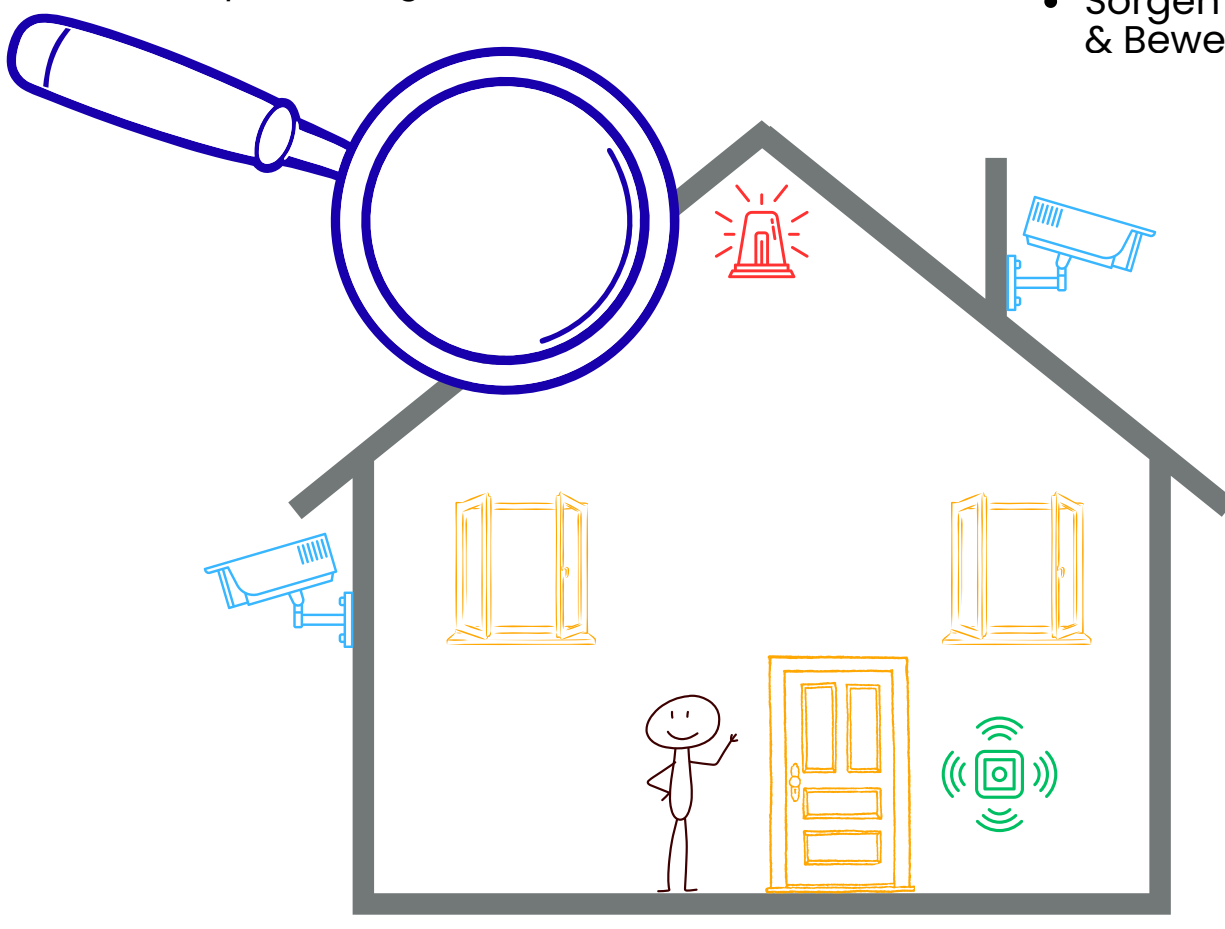
- Schützen vor unbefugtem Zutritt
- Mindestmaß an Sicherheit für Ihr Haus
- Kein Vollständiger Schutz vor Einbrechern/Betrügern

Expertenprüfung = Penetrationtesting

- Türen, Fenster, Alarmanlagen werden von Experten getestet
- Schwachstellen werden aufgedeckt und behoben
- Ausführlicher Bericht zur Optimierung

Überwachungskameras = SIEM (Security Information & Event Management)

- Zeichnen alle Aktivitäten auf
- Sorgen für Nachverfolgbarkeit & Beweise bei Einbruch



Alarmanlage = EDR/XDR

- Warnt bei verdächtigen Aktivitäten
- 24/7 Überwachung
- Automatisierte Sicherheitsreaktion durch XDR-Systeme

Mitbewohner sensibilisieren = Awareness-/ Phishingkampagnen

- Betrüger klingen an der Tür, wollen Zugang
- Öffnen Sie nicht jedem die Tür
- Vorsicht bei falschen Handwerkern, Paketboten, Behördern

Elektronischer Zugangschip = Passwortmanager

- Nur berechtige Personen haben Zugriff
- Jeder “Schlüssel” ist einzigartig
- Kein Schlüsselbund, nur zugangschips

Vorstellung

Wir sind Experten rund um Digitalisierung, Automatisierung, Prozessoptimierung und IT-Sicherheit. Wir möchten Unternehmen dabei unterstützen, den nächsten Schritt zu gehen – strategisch, digital & nachhaltig. Technische Herausforderungen verstehen wir nicht nur, sondern finden auch maßgeschneiderte, einfach umsetzbare Lösungen.

Unsere Branche verändert sich ständig, und die Bedeutung von Technologie wächst täglich. Wir sind stolz darauf, diesen Wandel aktiv mitzugestalten und neue Lösungen für unsere Kunden zu finden – immer mit der Devise: IT einfach einfach.

Dietmar Lang
Geschäftsführer

Einführung

Die Relevanz von Cybersecurity

Die Digitalisierung ist für Unternehmen längst kein optionaler Schritt mehr, sondern ein entscheidender Faktor für ihre Wettbewerbsfähigkeit. Gleichzeitig entstehen durch digitale Prozesse und automatisierte Systeme neue Angriffsflächen für Cyberkriminelle. Gerade in der deutschen Industrie zeigt sich, dass die Sicherheitsstrategien mit der technologischen Entwicklung oft nicht Schritt halten – zu abstrakt erscheinen die Risiken, zu unsichtbar die Benefits von Investitionen in Cybersicherheit.

Als IT-Dienstleister mit Fokus auf Digitalisierung und Automatisierung wissen wir: Fortschritt und Sicherheit schließen sich nicht aus – im Gegenteil. Nur wer beides zusammendenkt, kann nachhaltige, zukunftsfähige Strukturen schaffen. Dieses Whitepaper zeigt auf, warum Cybersecurity heute essenziell ist – und wie Unternehmen zielgerichtet und wirksam investieren können, um ihre digitale Transformation abzusichern.

Menschlicher Faktor als größte Schwachstelle

Während das technische Eindringen in gut abgesicherte Netzwerke für Angreifer mit erheblichem Aufwand verbunden ist, sind sie bei einem anderen Ansatz oft schneller am Ziel: dem Menschen. Mitarbeitende werden gezielt über gefälschte Portale oder manipulierte E-Mails kontaktiert – mit dem Ziel, an Zugangsdaten zu gelangen oder Schadsoftware einzuschleusen. Phishing und Ransomware zählen dabei zu den häufigsten und folgenschwersten Angriffsmethoden.
Die Auswirkungen sind gravierend: finanzielle Schäden in dreistelliger Milliardenhöhe, Datenverlust und ein oft irreparabler Reputationsschaden. Umso wichtiger ist es, Cybersecurity nicht nur technisch, sondern auch organisatorisch und kulturell zu verankern – durch Sensibilisierung, klare Prozesse und moderne Sicherheitslösungen.

Beispiele aus der Realität

29. Januar 2025 | 22:43 Uhr

Cyberangriff treibt Maxx Hotel in Aalen in die Insolvenz

Die Betreibergesellschaft des Vier-Sterne-Hotels Maxx in Aalen hat Insolvenz angemeldet. Wesentlicher Auslöser für die finanzielle Schieflage der Scoop Aalen Hotelbetriebs GmbH war ein Cyberangriff auf das Hotel, welches erst im Sommer 2022 eröffnet wurde.

Auch Balingen und Meßkirch betroffen

Nach Cyberangriff: Bizerba baut rund 450 Stellen ab

Stand: 30.1.2024, 17:46 Uhr

RECYCLING UND ENTSORGUNG

Cyberangriff drängt Familienunternehmen in die Insolvenz

Bei der deutschen Recyclingfirma Eu-Rec ist es finanziell zuletzt nicht gut gelaufen. Nach einer Cyberattacke folgt nun ein Insolvenzverfahren.

in Pocket speichern | merken

25. April 2025, 9:20 Uhr, Marc Stöckel

Business Email Compromise als Wirtschaftsrisiko: Schon zu Mitte dieses Monats warnte die Polizei in Bayern vor einem verstärkten Aufkommen von Business Email Compromise (**#BEC**) vor allem auch im Mittelstand vor Ort - kurze Zeit später gab es nun einen weiteren Vorfall mit einer der bislang höchsten Schadenssummen.

Der Fall unterscheidet sich nach gegenwärtigem Informationsstand in seiner Durchführung nicht wesentlich von den Fällen zuvor: Ein beauftragter Unternehmer, der durch Cyberkriminelle zuvor kompromittiert wurde, verschickte falsche Rechnungen, die durch das wirtschaftlich geschädigte Opfer gezahlt wurden - diesmal waren es 100.000 EUR:

"Nach deren Angaben erstattete der Mann am Freitag Anzeige. Demnach beauftragte er eine Firma mit der Renovierung der Fassade eines seiner Gebäude in München. Später erhielt er von dieser mehrere Rechnungen in Höhe von insgesamt über 100.000 Euro und bezahlte diese auch.

Im Nachhinein stellte sich heraus, dass die beauftragte Firma aus dem Raum Neufahrn bei Freising Opfer eines Hackerangriffs geworden war und ein unbekannter Täter falsche Rechnungen an den Rottaler ausgestellt hatte."

Beispiele aus der Realität

Um zu verdeutlichen, wie massiv ein Cyberangriff ein Unternehmen treffen kann, zeigen wir hier den Fall eines mittelständischen Betriebs, der 2023 Opfer einer Ransomware-Attacke wurde. „Wir haben Euch gehackt – alle weiteren Informationen im Darknet“, stand auf Ausdrucken, die morgens auf jedem Drucker lagen.
Kurz darauf war nichts mehr funktionsfähig: Server, Rechner, Produktion – alles stand still. Die Folgen: Millionenverluste, Personalabbau von über 100 auf nur noch acht Mitarbeitende, Verkauf der Betriebsimmobilie. Der Angriff brachte das Unternehmen an den Rand der Insolvenz – ein eindrückliches Beispiel dafür, dass Cyberangriffe zur existenziellen Bedrohung geworden sind.

Beispiele aus der Realität

Ich habe das bereits selbst vor kurzem bei Kunden erlebt, was vorallem auch dafür gesorgt hat, dass jeder im Adressbuch noch eine schädliche E-Mail erhalten hat. Das trifft auch Anwälte und Steuerberater, die sensible Daten über diesen Weg versenden.

BEC-Angriffe umgehen klassische Schutzmechanismen – gerade bei Microsoft 365. Wer denkt, „wir haben ja Microsoft Defender for office", hat oft nur eine vermeintliche Sicherheit. Schade, dass das noch immer so ist und solche Dinge erst passieren müssen.

IT- und Informationssicherheit ist Chefsache - die Geschäftsleitung muss sichergestellen, dass das Unternehmen über die notwendigen Systeme, Maßnahmen sowie qualifizierte Mitarbeiter mit adäquatem Know-how verfügt.

Das erinnert mich an den Fall von KNP in UK. Hier musste ein 158 Jahre altes Unternehmen wegen eines Ransomwareangriffs schließen. Das sind leider die Fälle, von denen man hofft, dass sie einen nicht selbst treffen.

Eine Firma, bei der ich Geschäftsführer war, wurde gehackt. Es waren die schlimmsten zwei Jahre meines Lebens. Ja, es hat zwei Jahre gedauert, bis alles abgeschlossen war. Nach dem Hackerangriff und der Wiederherstellung der Daten kamen die Klagen von Kunden und Personen, deren Daten im Darknet aufgetaucht sind.
Die Zusammenarbeit mit der Kripo NRW war wirklich super, die haben uns sehr geholfen, ebenso die Ministerien.
Ich wünsche viel Glück!!!!! 🍀

IT ist reine Führungsverantwortung

IT-Sicherheit betrifft das ganze Unternehmen – nicht nur die IT-Abteilung

Ein Cyberangriff ist längst kein rein technisches Problem mehr. Ob Phishing, Ransomware oder Datenlecks – die Auswirkungen betreffen alle Geschäftsbereiche.

Cybersecurity ist damit ein zentrales Führungsthema und sollte entsprechend strategisch betrachtet werden. Die Folgen eines erfolgreichen Angriffs reichen weit über IT-Systeme hinaus:

- Finanzieller Schaden: Betriebsunterbrechungen, Datenverluste, Erpressungszahlungen und die teils enormen Wiederherstellungskosten können das Budget massiv belasten.
- Rechtliche Risiken: Verstöße gegen Datenschutzgesetze (z. B. DSGVO), die NIS-2-Richtlinie oder das Lieferkettengesetz können zu Geldbußen oder sogar Haftstrafen führen.
- Vertrauensverlust bei Kunden und Partnern: Sicherheitsvorfälle schädigen das Image eines Unternehmens nachhaltig – insbesondere bei sensiblen oder geschäftskritischen Daten.
- Existenzgefährdung: In besonders schweren Fällen kann ein Angriff sogar zur Insolvenz führen – gerade bei kleinen und mittleren Unternehmen ist das Risiko hoch.

Cybersicherheit ist deshalb keine reine IT-Aufgabe, sondern eine unternehmensweite Verantwortung – und ein wesentlicher Bestandteil moderner Unternehmensführung.

Unser Security Portfolio

Fundament Ihrer IT-Sicherheit

für jedes Unternehmen unverzichtbar

Richtet sich an alle KMU's, unabhängig von Branche und Größe, mit dem Ziel die häufigsten Sicherheitslücken zu schließen und ein Fundament Ihrer Cybersicherheit zu bilden.

Leistungsübersicht

- **Firewall & Antivirus**: Einrichtung bzw. Absicherung vorhandener Systeme
- **Patch-Management**: Automatisierte Software- und Systemupdates
- **Backup-Lösungen**: Implementierung und Überprüfung funktionierender Datensicherungen, Backup-Wiederherstellungstests: Prüfung der Datenintegrität
- **Mehr-Faktor-Authentifizierung (MFA)**: Einführung sicherer Zugangsverfahren
- **Passwortmanagement**: Sichere Passwortrichtlinien & Passwortmanager
- **Grundlagenschulung für Mitarbeitende**: Awareness zu Phishing, Social Engineering & sicherem Verhalten → Phishing-Simulationen: Realistische Angriffstests zur Schulung

Unser Security Portfolio

Erweiterter Schutz

proaktive Sicherheitsüberwachung rund um die Uhr

Richtet sich an alle KMU’s mit sensiblen Daten, digitalisierten Prozessen oder Compliance-Anforderungen, um Risiken frühzeitig zu erkennen, bevor Schäden entstehen.

Leistungsübersicht

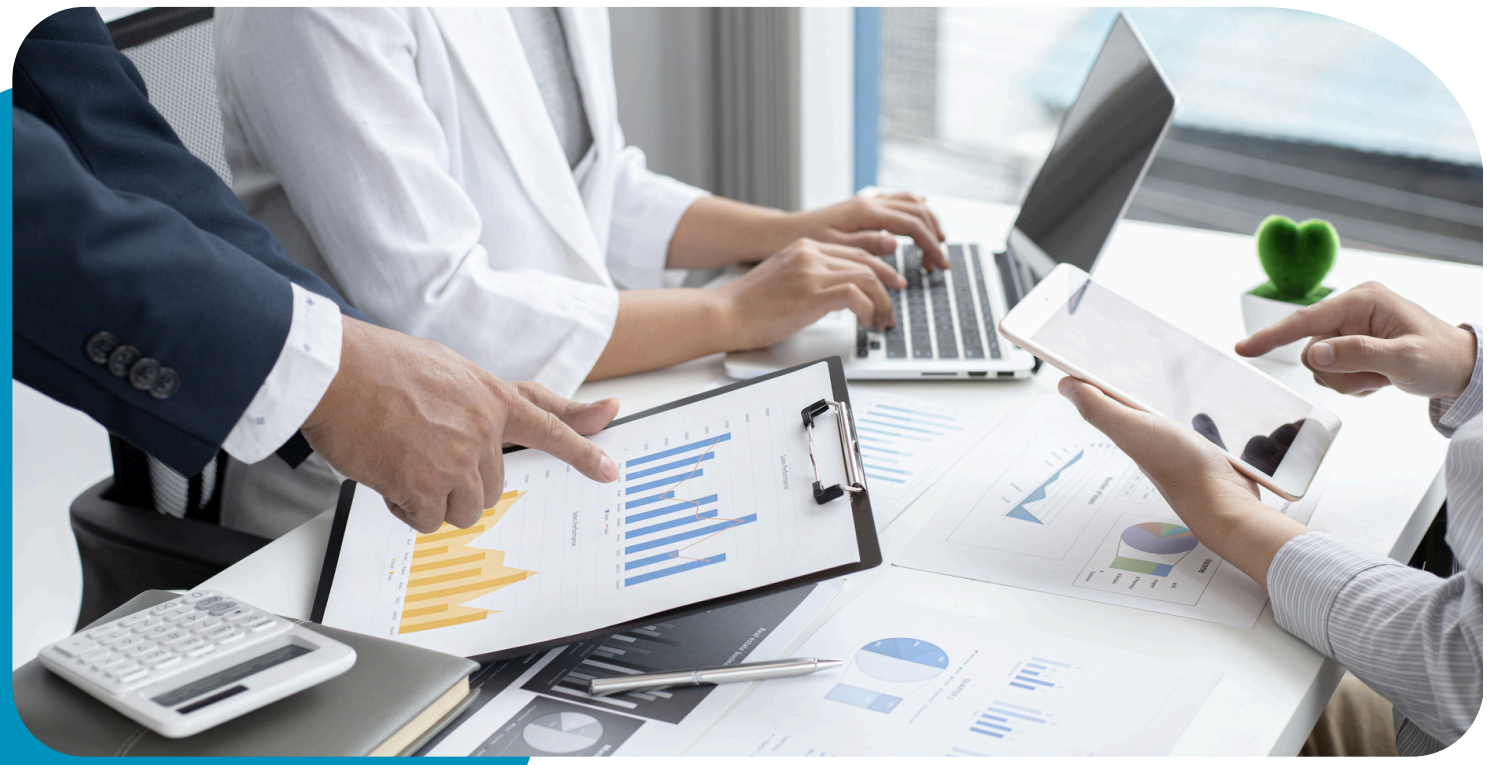
- **Alle Leistungen aus Stufe 1**
- **24/7 Monitoring & Schwachstellen-Scanning**: Permanente Überwachung & Alarmierung
- **IT-Forensik & Ereignisrekonstruktion**: Analyse verdächtiger Aktivitäten
- **Asset-Management**: Strukturierte Verwaltung von Geräten, Servern, Software
- **Active Directory-Sicherheitsanalyse**: Überprüfung auf Fehlkonfigurationen & Angriffsvektoren

Individueller IT-Sicherheitsschutz

Modulare Sicherheitsprojekte für Unternehmen mit spezifischen Anforderungen

Diese Dienstleistungen können unabhängig von den Sicherheitsstufen Basic und BasicPlus gebucht werden. Für maximale Wirksamkeit wird jedoch ein bestehendes Sicherheitsfundament empfohlen.

Unsere Preisangaben für individuelle IT-Sicherheitsmaßnahmen verstehen sich als einmalige Investition – ohne laufende Gebühren oder versteckte Folgekosten.



Individueller IT-Sicherheitsschutz

Penetration Tests

Ziel: Identifikation realer Schwachstellen durch kontrollierte, praxisnahe Angriffe

Leistungsumfang:

- Infrastruktur-Tests;
  - Umfassende Prüfung der kompletten Netzwerkinfrastruktur
  - Angriffe auf kritische Systeme wie Active Directory-Server
- Webanwendungs-Tests:
  - OWASP Top 10 Schwachstellenprüfung für Webanwendungen
  - Sicherheitsanalyse von Webservern und APIS
- Individuelle Anwendungstests
  - Gezielte Prüfung geschäftskritischer Anwendungen
  - Analyse von Cloud-Services und SaaS-Lösungen
  - Tests von internen Business-Applikationen

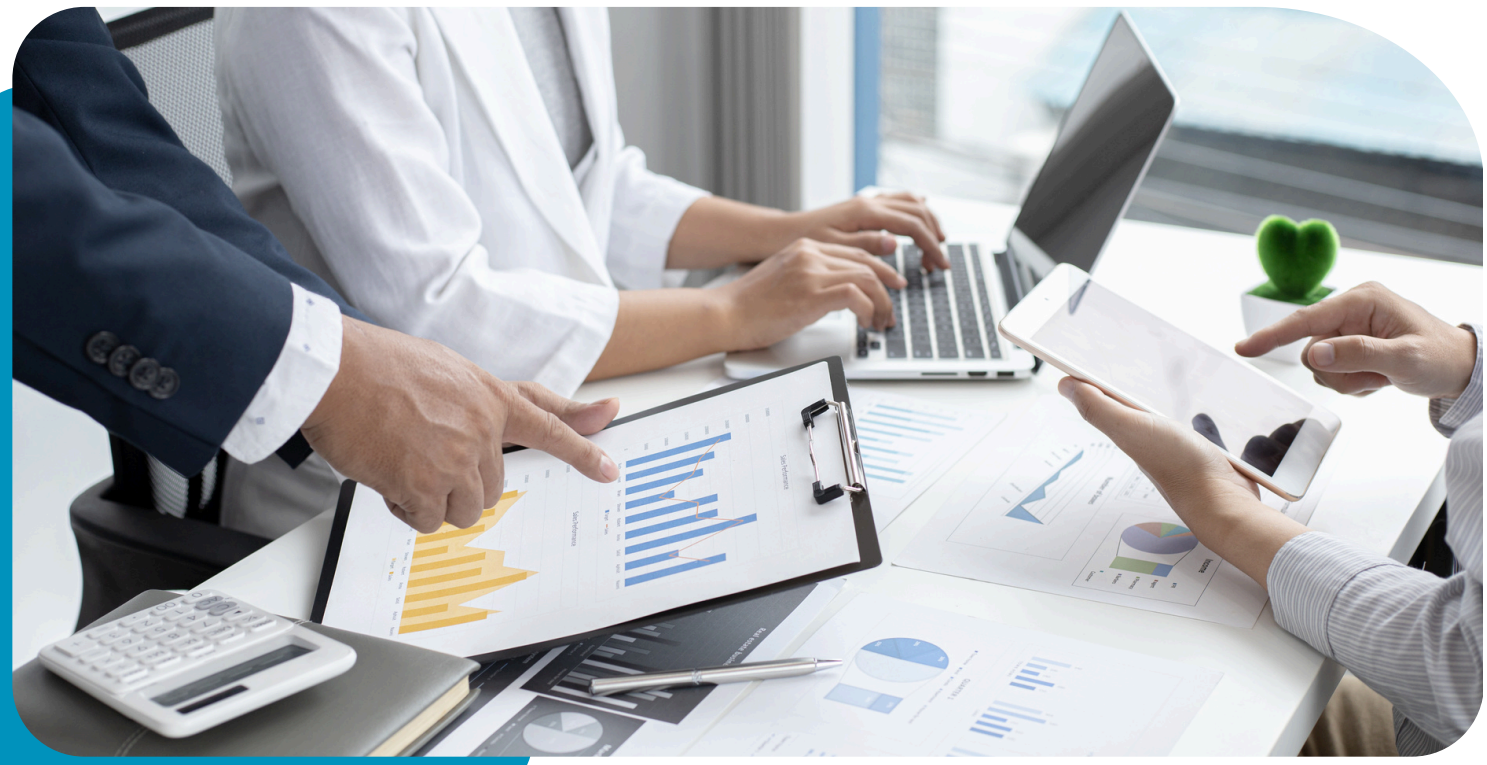
Individueller IT-Sicherheitsschutz

FTAPI

Ziel: Absicherung öffentlich erreichbarer Werbedienste gegen die wichtigsten Schwachstellen (OWASP Top 10)

Leistungsumfang:

- Prüfung auf SQL Injection, XSS, Authentifizierungsfehler, Session Hijacking, etc.
- Tests von Front-End und Back-End (API, Login, Rollen)
- Manuelle und automatische Prüfmethoden
- Empfehlung zur Härtung und sichere Konfiguration



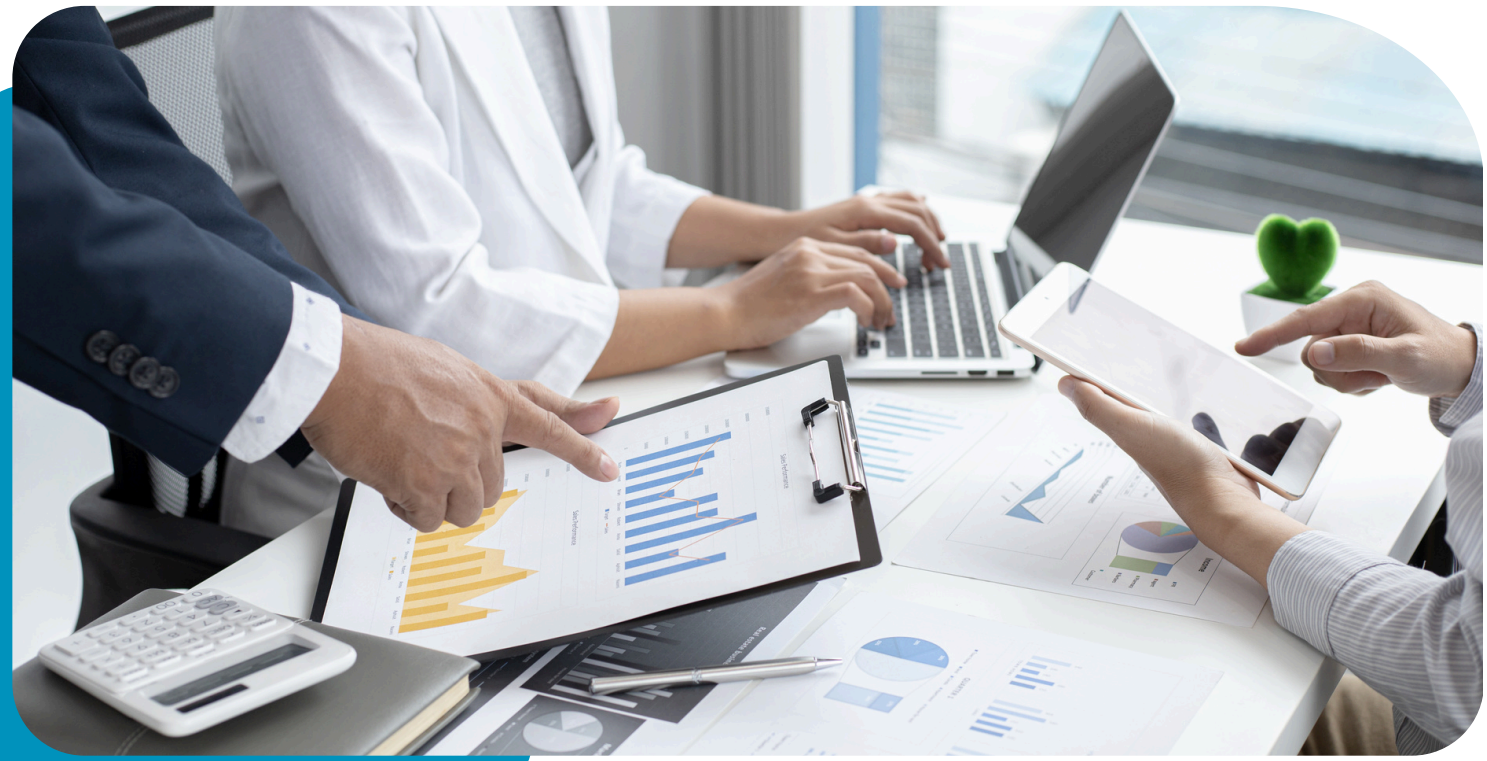
Individueller IT-Sicherheitsschutz

terraXaler

Ziel: Absicherung öffentlich erreichbarer Werbedienste gegen die wichtigsten Schwachstellen (OWASP Top 10)

Leistungsumfang:

- Prüfung auf SQL Injection, XSS, Authentifizierungsfehler, Session Hijacking, etc.
- Tests von Front-End und Back-End (API, Login, Rollen)
- Manuelle und automatische Prüfmethoden
- Empfehlung zur Härtung und sichere Konfiguration



Individueller IT-Sicherheitsschutz

ISO/ IEC 27001 Audit-Vorbereitung & Gap-Analyse

Ziel: Prüfung und Vorbereitung auf eine ISO 27001 Zertifizierung – praxisorientiert und verständlich

Leistungsumfang:

- Ermittlung des IST-Zustands (Gap-Analyse)
- Aufbau eines maßgeschneiderten ISMS-Rahmens
- Unterstützung bei Risikoanalysen & Mapnahmenplanung
- Dokumentationscheck (Richtlinien, Rollen, Prozesse)
- Vorbereitung auf interne/ externe Audits

Individueller IT-Sicherheitsschutz

NIS2 Readiness Audit

Ziel: Prüfung und Vorbereitung auf die Anforderungen der NIS2-Richtlinie für betroffene Unternehmen

Leistungsumfang:

- Identifikation der NIS2-Pflichten für das Unternehmen
- Bewertung technischer und organisatorischer Maßnahmen
- Erstellung eines Maßnahmenplan zur Umsetzung
- Reporting für Management & Aufsichtsbehörden

Unser Projektablauf

1. Kontaktaufnahme
2. Gemeinsame Zielsetzung
3. On-Boarding
4. Anwendungsbereich festlegen
5. Projektdurchführung
6. Präsentation mit Rückblick

Ihr Ansprechpartner

Bei Fragen oder weiteren Informationen steht Ihnen unser Spezialist zur Verfügung:

Samil Gencaslan ist unser Experte für Cybersicherheit – mit einem scharfen Blick für Schwachstellen und einem klaren Fokus auf pragmatische, wirksame Schutzmaßnahmen.

Als erfahrener Cybersecurity Consultant vereint er tiefgehendes technisches Know-how mit einem ganzheitlichen Verständnis für unternehmerische Risiken. Ob Netzwerksicherheit, Schwachstellenanalysen oder Awareness-Trainings – unser Experte entwickelt maßgeschneiderte Sicherheitskonzepte, die weit über Standardlösungen hinausgehen.

Sein Anspruch: Sicherheitsstrategien, die nicht nur auf dem Papier funktionieren, sondern in der Praxis schützen – skalierbar, zukunftsfähig und realistisch umsetzbar. Dabei steht stets der Mensch im Mittelpunkt: Technik und Sensibilisierung müssen Hand in Hand gehen.

Mit seiner Expertise ist er zentraler Bestandteil unseres Cybersecurity-Portfolios – und unterstützt Unternehmen dabei, IT-Sicherheit als strategischen Erfolgsfaktor zu begreifen.

Samil Gencaslan
Cybersecurity Consultant

E-Mail: s.gencaslan@itconex.de
Telefon: 0741 320 710 35

Kontakt

Samil Gencaslan
s.gencaslan@itconex.de
0741 320 710 35

Dietmar Lang
d.lang@itconex.de
0741 320 710 21

Adresse
Herrenbühlstraße 9
78658 Zimmern ob Rottweil

Sedanstraße 5
72764 Reutlingen