IT-Security-Beratung für kleine & mittelständische Unternehmen

**3 verdächtige Anzeichen, dass dein Unternehmen bald gehackt wird**

… und was du jetzt tun solltest, um finanziellen Schaden und juristische Konsequenzen von deinem Unternehmen abzuwenden.

[KOSTENLOSES BERATUNGSGESPRÄCH VEREINBAREN]

**Was du über Hacker wissen solltest …**

Sie warten nicht auf dich.

Oder darauf, dass du deine IT-Security auf Vordermann gebracht hast.

Stell dir einen typischen Arbeitstag vor.

Ein Tag, wie jeder andere, an dem du einfach nur deinen Kernaufgaben nachgehst.

Du kommst gerade aus einem Kundentermin, als du einen Anruf bekommst, der ein inneres Erdbeben in dir auslöst:

***„Chef, wir wurden gehackt.“***

Obwohl dir das Ausmaß des Angriffs im ersten Moment noch gar nicht bewusst ist, überkommt dich ein mulmiges Gefühl, denn:

Dein Unternehmen hat ein großes, wenn nicht sogar **existenzbedrohendes Problem.**

Nach und nach wird dir klar: Im Worst Case hast du auf produktions- oder dienstleistungsrelevante Daten ab sofort keinen Zugriff mehr.

Das macht dich erpressbar und zwingt dich höchstwahrscheinlich zur Bezahlung von hohen Lösegeldforderungen.

Und: Dir stehen möglicherweise sogar juristische Konsequenzen ins Haus, wenn auf diesem Weg sensible Kundendaten an Dritte gelangen. Denn das kann aus datenschutztechnischer Sicht sehr problematisch sein.

Leider nehmen es viele Unternehmen mit der Cybersicherheit nicht so genau – und stehen im Ernstfall vor einem Scherbenhaufen.

Ein solches Szenario ist jedoch vermeidbar – vorausgesetzt du befolgst ein paar elementare Grundregeln zur Risikoreduktion …

**Achtung: Diese 3 Todsünden, machen dein Unternehmen zu einem leichten Opfer von Hackern**

**Todsünde #1: Software mit Sicherheitslücken**

Ist deine Software veraltet oder unpassend konfiguriert, lädst du Täter förmlich dazu ein, in deine Systeme einzudringen.

**Todsünde #2: Vergessene Systeme & Dateien**

Bei 95% unserer Kunden finden wir solche „Karteileichen“ – also Systeme, Tools und Daten, die eigentlich gar nicht mehr da sein dürften, aber unbeabsichtigt nicht entfernt wurden. So etwas ist ein gefundenes Fressen für Hacker, um auf Cloud-Passwörter oder Kundendaten zuzugreifen.

**Todsünde #3: Fehlende Awareness bei den Mitarbeitern**

Schwache Passwörter, unbedachtes Öffnen von Phishing-Mails oder versehentliches Überspielen von Schadsoftware über liegengelassene USB-Sticks. In mindestens 50% der Fälle sorgt eine fehlende Sensibilität seitens der Mitarbeitern dafür, dass Hacker in Systeme eindringen und Schaden anrichten können.

Kannst du alle drei genannten Szenarien in deinem Unternehmen garantiert ausschließen?

Falls nein, ist das ein guter Grund, deine IT-Security einmal gründlich unter die Lupe zu nehmen.

[IT-SICHERHEIT ÜBERPRÜFEN]

**Die gute Nachricht: Du kannst über Hacker lachen, wenn du die richtigen Maßnahmen ergreifst**

Das, was Kidnapping und Banküberfälle früher waren, sind Hacker-Angriffe heute:

Eine gefährliche Bedrohung für viele Menschen und Unternehmen, mit sehr guten Erfolgsaussichten für Kriminelle.

**Laut einer repräsentativen Umfrage von Statista fielen rund 46 Prozent aller Unternehmen in Deutschland schon einmal einer Cyber-Attacke zum Opfer.**

Ebenfalls interessant: Nur jeder fünfte Fall von Cyberkriminalität kann aufgeklärt werden.

Deshalb sagen wir ganz klar:

Prävention ist das beste Heilmittel gegen Hackerangriffe.

Mit einer **professionellen Schwachstellenanalyse** (auch Vulnerability Assessment genannt) bereiten wir dein Unternehmen und deine Mitarbeiter effektiv auf den Ernstfall vor – und schaffen die Voraussetzungen dafür, dass Hacker in eurer IT-Infrastruktur keinen Schaden anrichten können.

Im Klartext: Wir decken mögliche Schlupflöcher **mit bewährten Methoden** auf. Außerdem zeigen wir dir, wo du am besten nachrüsten solltest, um Hackern das Leben möglichst schwer zu machen.

All das passiert nicht mit einer automatischen Software, sondern manuell von Profihand.

Nach Umsetzung der Schutzmaßnahmen profitierst du von einer **bombensicheren IT-Security** und kannst im Fall einer Cyberattacke ganz entspannt sein, denn:

Der Hacker wird sich die Zähne an eurem Sicherheitsnetz ausbeißen.

Und sollten er es doch schaffen einzudringen, trifft er auf vielfach verschlüsselte Daten, mit denen er am Ende nichts anfangen kann.

Ein schlechter Tag für den Hacker.

Aber ein guter Tag für dich.

[JETZT KOSTENLOSEN TERMIN AUSSUCHEN]

**Ablauf der Schwachstellenanalyse – so bringen wir dein Unternehmen in sicheres Fahrwasser:**

**Schritt 1: Terminvereinbarung & Strategiegespräch**

Wähle unten einen Termin für einen gemeinsamen Call. In diesem kostenlosen Strategiegespräch geben wir dir erste wertvolle Impulse, um die IT-Sicherheit deines Unternehmens zu erhöhen. Ausgehend von der Situation deines Unternehmens prüfen wir, ob eine Schwachstellenanalyse Sinn macht.

**Schritt 2: IT-Security-Konzept & Angebot**

Wir erstellen ein individuelles Security-Konzept inkl. Fixpreis-Angebot, welches wir dir in einem zweiten Call präsentieren.

**Schritt 3: BAFA-Förderantrag**

Was viele Geschäftsführer nicht wissen: Maßnahmen zur Verbesserung der IT-Security sind förderbar. Deshalb kümmern wir uns nach der Annahme des Angebots um den BAFA-Förderantrag – was deine Kosten bei einer Zusage um bis zu 80% reduzieren kann.

**Schritt 4: Vertragsschluss**

Nach Abschluss des Förderantrags schließen wir einen schriftlichen Vertrag zur Durchführung der Schwachstellenanalyse.

**Schritt 5: Schwachstellenanalyse & Präsentation**

Wir vereinbaren einen fixen Termin, an dem wir die Schwachstellenanalyse in deinem Unternehmen durchführen. Der gesamte Vorgang dauert rund eine Woche. Im Anschluss präsentieren wir das Ergebnis vor Ort in deinen Räumlichkeiten.

**Schritt 6: Umsetzung & finaler Test (optional)**

Nach Abschluss der Schwachstellenanalyse liegt dir eine exakte Auswertung inkl. Handlungsplan zum Schutz vor Datenverlust und zur Verbesserung der IT-Sicherheit deiner Firma vor. Bei Bedarf vermitteln wir dich an einen Partner unseres Netzwerkes, der sich um die Umsetzung der empfohlenen IT-Security-Maßnahmen kümmert. Auf Wunsch führen wir gerne einen finalen Test durch, der zeigt, ob die Maßnahmen erfolgreich waren.

Du willst ab sofort die volle Kontrolle über deine sensiblen Daten erlangen und dich vor finanziellen Schäden durch Hacking-Angriffe absichern? Dann vereinbare jetzt deinen kostenlosen Beratungstermin mit einem erfahrenen IT-Security-Consultant.

[JA, ICH WILL EINE KOSTENLOSE ERSTBERATUNG]

**IT-Security-Beratung – dein Ansprechpartner**

* Bernhard Furtmayr – IT-Security-Berater
* DEKRA-zertifizierter IT-Sachverständiger
* DEKRA-zertifizierter Cyber Security Analyst
* Über 10 Jahre Erfahrung im Bereich IT-Beratung & IT-Security
* Selbstständiger IT-Dienstleister seit 2018
* Begleitete bereits über 20 Unternehmen auf dem Weg zu einer sicheren IT-Infrastruktur

*„Egal ob früher in der Sicherheitskontrolle am Flughafen oder heute als IT-Security-Spezialist: Menschen und Unternehmen Sicherheit zu geben, ist seit über 10 Jahren meine Mission.“*

**In der Schwachstellenanalyse zeigen wir dir:**

* Wie du eine bombensichere IT-Security auf die Beine stellst, welche die Produktivität und Leistungsfähigkeit deines Unternehmens langfristig schützt.
* Wie du Hackern von vornherein keine Chance lässt und dein Unternehmen so vor einem großen finanziellen Schaden bewahrst.
* Wie du dein Unternehmen und dich selbst gegen schwere juristische Konsequenzen in Folge von Hackerangriffen mit Datenraub absicherst.
* Wie du das Thema IT-Security ohne übermäßigen Aufwand und mit maximaler Effizienz in dein Unternehmen und eure Prozesse integrierst.

**Außerdem bekommst du:**

* Absolute Klarheit über den aktuellen Zustand und mögliche Schwachstellen deiner IT
* 100-prozentige Kontrolle über alle sensiblen Daten in deinem Unternehmen
* Einen klaren Handlungsplan, der auch in der Praxis umsetzbar ist – und zwar ohne die Produktivität in deinem Unternehmen einzuschränken
* Eine perfekte Basis um Hackern langfristig zu signalisieren, dass in deinem Unternehmen nichts zu holen ist
* Wertvolle Zeit, die du nicht in das Beheben von möglichen Schäden als Folge von Hackerangriffen investieren musst
* Das beruhigende Gefühl, gegen Hackerangriffe jederzeit gut gewappnet zu sein.
* Das Schlüsselelement, um den Status deines Unternehmens als vertrauenswürdigen Partner für Kunden und Geschäftspartner zu untermauern.
* Erfahrene Experten für eine hochwertige IT-Security-Beratung, die sich nicht nur um eine umfassende Schwachstellenanalyse, sondern auch um die Förderung selbiger kümmern.

**Für wen ist eine individuelle IT-Schwachstellenanalyse das richtige?**

* Praktisch veranlagte Unternehmer, welche die Handlungsfähigkeit, Produktivität und Ressourcen ihres Unternehmens schützen möchten
* Sicherheitsbewusste Unternehmer, die finanziellen Schaden um jeden Preis vom Unternehmen abwenden wollen
* Aufmerksame Unternehmer, die jederzeit die volle Kontrolle über ihre Daten und maximale Klarheit über den Zustand ihrer IT-Security haben möchten
* Verantwortungsbewusste Unternehmer, die ihren eigenen Ruf schützen und das Vertrauen ihrer Kunden nicht enttäuschen wollen
* Lösungsorientierte Unternehmer, die schon einmal gehackt worden sind und vermeiden möchten, das so etwas noch einmal passiert

[BERATUNG ZUR IT-SECURITY BUCHEN]

**IT-Security-Beratung – das sagen unsere Kunden über uns**

*„Dank der Hilfe von Herrn Furtmayr konnten wir den Hackerangriff auf unser System in der Tierarztpraxis schnell bewältigen! Wir hätten dieses sonst über eine Woche nicht benutzen können! Wir werden bei solchen Problem immer wieder gerne zu Herrn Furtmayr kommen.“*

Dr.med.vet Küster – Kleintierpraxis – https://www.tierarztpraxis-kuester.de/

*„Planung und Umsetzung der Netzwerkinfrastruktur durch Verkabelung und W-LAN, des Multicell DECT Systems und der verschiedenen Endgeräte. Hierbei wurde ein besonderes Augenmerk auf die Sicherheit des Systems gelegt, um den hohen Ansprüchen gerecht zu werden.“*

Landratsamt München – https://www.landkreis-muenchen.de/

*„Wir gaben bei Herrn Furtmayr einen Firewall-Test unseres HA-Clusters im Datacenter in Auftrag. Der Hintergrund war die unabhängige Überprüfung unserer Systeme. Herr Furtmayr führte die Tests ohne unser Wissen von Datum und Ablauf durch, so wie es für einen unabhängigen Test sein soll. Der Angriffsversuch wurde von unseren Systemen erkannt, gemeldet und umgehend von Herrn Furtmayr aufgeklärt. Das Ergebnis war verblüffend und am Ende wurde uns ein umfassender Prüfbericht inkl. Handlungsempfehlungen übergeben. Alles in allem eine angenehme und sehr zufriedenstellende Zusammenarbeit. Wir würden Herrn Furtmayr und sein Prüf- und Berichtskonzept jederzeit weiter empfehlen. Geprüft wurde eine Kombination eines OPNsense HA-Cluster mit vorgeschalteten NETSCOUT Arbor DDoS and Cyber Threat Protection System.“*

Dennis Prior – IT Engineering & Automation – https://www.dennisprior.de/

[BERATUNG ZUR IT-SICHERHEIT BUCHEN]

**„Betrifft uns das überhaupt? Es werden doch hauptsächlich große Unternehmen gehackt, oder?“**

Alleine in Deutschland werden jedes Jahr tausende von Unternehmen gehackt. Dabei ist die komplette Bandbreite vertreten, vom kleinen 2-Mann-Betrieb bis zum Konzern.

Egal ob Onlineshop, Krankenhaus oder Industrie:

**Hacker schlagen dort zu, wo sich ihnen eine Möglichkeit bietet!**

Und das sind oftmals kleine oder mittelständische Unternehmen, die das Thema IT-Security bislang eher stiefmütterlich behandelt haben.

Deshalb ist eine IT-Security-Beratung inkl. Schwachstellenanalyse so wichtig: Sie deckt die Erfolgschancen von Hackern auf und zeigt dir, wo du ansetzen musst, um deine Daten und Systeme zu schützen.

[KOSTENLOSEN BERATUNGSTERMIN VEREINBAREN]

**Blicke Hacker-Angriffen entspannt entgegen**

Es gibt den falschen und den richtigen Weg, mit dem Thema IT-Security umzugehen:

**Option a)** Du tust das, was dir eigentlich gar nicht ähnlich sieht, sprich: Du lässt auf gut Glück erstmal alles so weiterlaufen wie bisher. In der Hoffnung, dass nichts schiefgeht – und immer mit der Sorge im Hinterkopf, was im schlimmsten Fall passieren könnte.

**Option b)** Du machst Nägel mit Köpfen und stellst deine IT-Security auf den Prüfstand. So findest du heraus, wie sicher oder unsicher das Netzwerk deines Unternehmens tatsächlich ist. Und du bekommst einen klaren Handlungsplan für eine wasserdichte IT-Security an die Hand.

Das Resultat: Nach Umsetzung der Schritte kannst du wieder ruhig schlafen, denn:

* All deine sensiblen Daten sind vor Hacker-Angriffen geschützt
* Du bist nicht mehr erpressbar
* Dein Unternehmen ist vor finanziellen Schäden und juristischen Konsequenzen geschützt

Das ist das, was du willst?

Dann wähle im Kalender einen freien Termin für ein kostenloses Erstgespräch zur IT-Sicherheitsberatung aus. Darin zeigen wir dir, was eine sichere IT-Infrastruktur ausmacht und überprüfen gemeinsam, ob eine individuelle IT-Schwachstellenanalyse für dein Unternehmen Sinn macht.

[TERMIN FÜR IT-SECURITY-CONSULTING ANFRAGEN]

**IT-Security-Beratung – häufig gestellte Fragen**

**Was ist eine IT-Schwachstellenanalyse?**

Eine Schwachstellenanalyse ist eine Form der IT-Security-Beratung, welche mögliche Sicherheitslücken in der IT-Infrastruktur von Unternehmen zuverlässig offenlegt und geeignete Maßnahmen zur Behebung vorschlägt. So kann das Risiko auf einen finanziellen und juristischen Schaden durch Hackerangriffe auf einfache Art und Weise reduziert werden.

**IT-Security-Consulting: Wie lange dauert eine Schwachstellenanalyse?**

Der gesamte Vorgang inkl. Analyse von IT-Schwachstellen, Auswertung und Präsentation der Ergebnisse dauert ca. eine Woche.

**Wie viel Zeit muss ich selbst dafür aufbringen?**

Zum Start der Schwachstellenanalyse benötigen wir ca. eine Stunde deiner Zeit, in der wir einen von mir zugesandten Rechner mit eurem Firmennetzwerk verbinden. Für das weitere Vorgehen benötigen wir keine weitere Unterstützung von dir.

**Welche Voraussetzungen muss mein Unternehmen für eine professionelle IT-Schwachstellenanalyse mitbringen?**

Du solltest bereit sein, dich auf neue Impulse und Ideen einzulassen und in der Lage sein, das durch die IT-Security-Beratung neu erlangte Sicherheitsbewusstsein an deine Mitarbeiter weiterzugeben.

**Was kostet die IT-Security-Beratung?**

Das Erstberatungsgespräch ist zu 100% kostenlos. Solltest du dich anschließend für eine Zusammenarbeit entscheiden, unterbreiten wir dir ein individuelles Angebot. Die Kosten für eine professionelle Schwachstellenanalyse liegen je nach Komplexität deiner IT-Infrastruktur bei 1.500,- € bis 3.000,- €.

**Ist eine IT-Security-Beratung förderbar?**

Du hast gute Chancen auf eine Übernahme von 50 – 80% der Kosten. Maßnahmen zur Verbesserung der IT-Security sind durch die BAFA (Bundesamt für Wirtschaft und Ausfuhrkontrolle) förderfähig, wobei die Obergrenze bei 1.700,- € liegt. Als Cyber Security Dienstleister kümmern wir uns um Antragsstellung und Abwicklung.

**Bekomme ich ein Zertifikat?**

Auf Wunsch stellen wir dir als kostenlosen Service gerne ein Zertifikat aus, das du in deinem Empfangsbereich aufhängen oder in deine Website einbinden kannst. Es belegt, dass dein Unternehmen Maßnahmen für mehr digitale Sicherheit durchführt und den Schutz von vertraulichen Daten ernst nimmt.