GEKKO

wir lieben IT!

IT-SECURITY CHECK

IHRE IT-SECURITY VON UNABHÄNGIGEN EXPERTEN GEPRÜFT

www.gekko.at

DIE UNSICHTBARE GEFAHR

Digitale Technologien machen wirtschaftliche Prozesse schneller und effizienter und bieten Unternehmen zudem völlig neue Chancen. Mit der neuen Technik werden die Prozesse aber auch komplexer und anfälliger. Unvorhergesehene Ausfälle, Störungen durch unsachgemäße Nutzung oder durch Unwissenheit entstehende Sicherheitslücken können schnell zu einem ernsten Problem führen. Zusätzlich steigt die Anzahl der Cyberkriminellen, die technische Schwachstellen und menschliches Fehlverhalten gezielt ausnützen, drastisch an.

*„12,6 Prozent mehr Anzeigen von **Internetbetrug** im Jahr 2015 als im Jahr davor.“*

Die Arten der Angriffe sind vielfältig und werden auch immer raffinierter: Von Malware, sogenannter Schadsoftware, die Dateien löscht oder verschlüsselt, um den Dateninhaber anschließend zu erpressen, über Phishing-Attacken, um an Kontodaten zu gelangen, bis hin zum Diebstahl von Kundendaten, Patentinformationen und vielem mehr.

*„+ 60,1 Prozent mehr Fälle von betrügerischem **Datenmissbrauch** im Jahr 2015 als im Jahr davor.“*

Die rasante Zunahme und steigende Qualität von Hackerangriffen, Viren, Trojanern und sonstiger Malware machen ein gut durchdachtes IT-Security-Konzept für jedes Unternehmen unerlässlich.

DER MITTELSTAND IM MITTELPUNKT

Wer denkt, von Cyber-Kriminalität seien ausschließlich große Unternehmen betroffen, irrt leider. Angreifer konzentrieren sich vermehrt auf den Mittelstand: Rund zwei Drittel der Cyberattacken sind mittlerweile auf KMU gerichtet.

*„49 Prozent der österreichischen Unternehmen waren bereits Opfer eines **Cyberangriffes.**“*

Gerade für KMU können solche Angriffe existenzbedrohend sein. Laut einer Studie von Kaspersky Lab betragen die durchschnittlichen Folgekosten einer Cyberattacke auf KMU rund 34.000 Euro. Die Hauptursache für wirtschaftliche Schäden sind laut dem Allianz Risk Barometer 2015 Reputationsverluste (61 %), gefolgt von Betriebsunterbrechungen (49 %) und dem Verlust von Kundendaten (45 %). Der Barometer zeigt auch, dass Cyberrisiken die am häufigsten unterschätzten Bedrohungen sind. Auch die meisten österreichischen KMU erkennen IT-Security nicht als strategisch wichtiges Thema. Hier besteht eindeutig Handlungsbedarf, denn Vorsicht ist besser als Nachsicht.

„Mit GEKKO haben wir einen verlässlichen Partner gefunden, der uns bei der Umsetzung unserer Ziele tatkräftig und zeitnah unterstützt.“
Christian Pettauer, CIO

„GEKKO übernimmt Verantwortung, das gibt ein sicheres Gefühl in der Zusammenarbeit.“
Gerhard Zoubek, GF Adamah Biohof

IT-SECURITY CHECK

Cyberkriminelle sind Experten ihres Faches und analysieren genau, wo sie Schwachstellen in der IT Ihres Unternehmens vorfinden. Mit diesem Wissen entdecken sie schnell einen wunden Punkt, an dem sie ihren Angriff starten. Dieser wird oft, wenn überhaupt, erst dann bemerkt, wenn es zu spät ist. Mit unserer IT-Sicherheitsprüfung können Sie den Angreifern jedoch zuvorkommen.

AUSBAUSTUFEN UND UMFANG

Ihre IT-Sicherheitsprüfung bieten wir Ihnen in den zwei Ausbaustufen A (kleiner Sicherheitstest) und B (erweiterter Sicherheitstest) an, welche sich in Umfang und Tiefe unterscheiden. Bei der IT-Sicherheitsprüfung der Ausbaustufe A übernimmt ein Experte, bei der Ausbaustufe B übernehmen zwei Experten die Prüfung Ihrer Systeme. Beide IT-Sicherheitsprüfungen, sowohl Ausbaustufe A und B, nehmen fünf Werktage in Anspruch.

KOSTEN

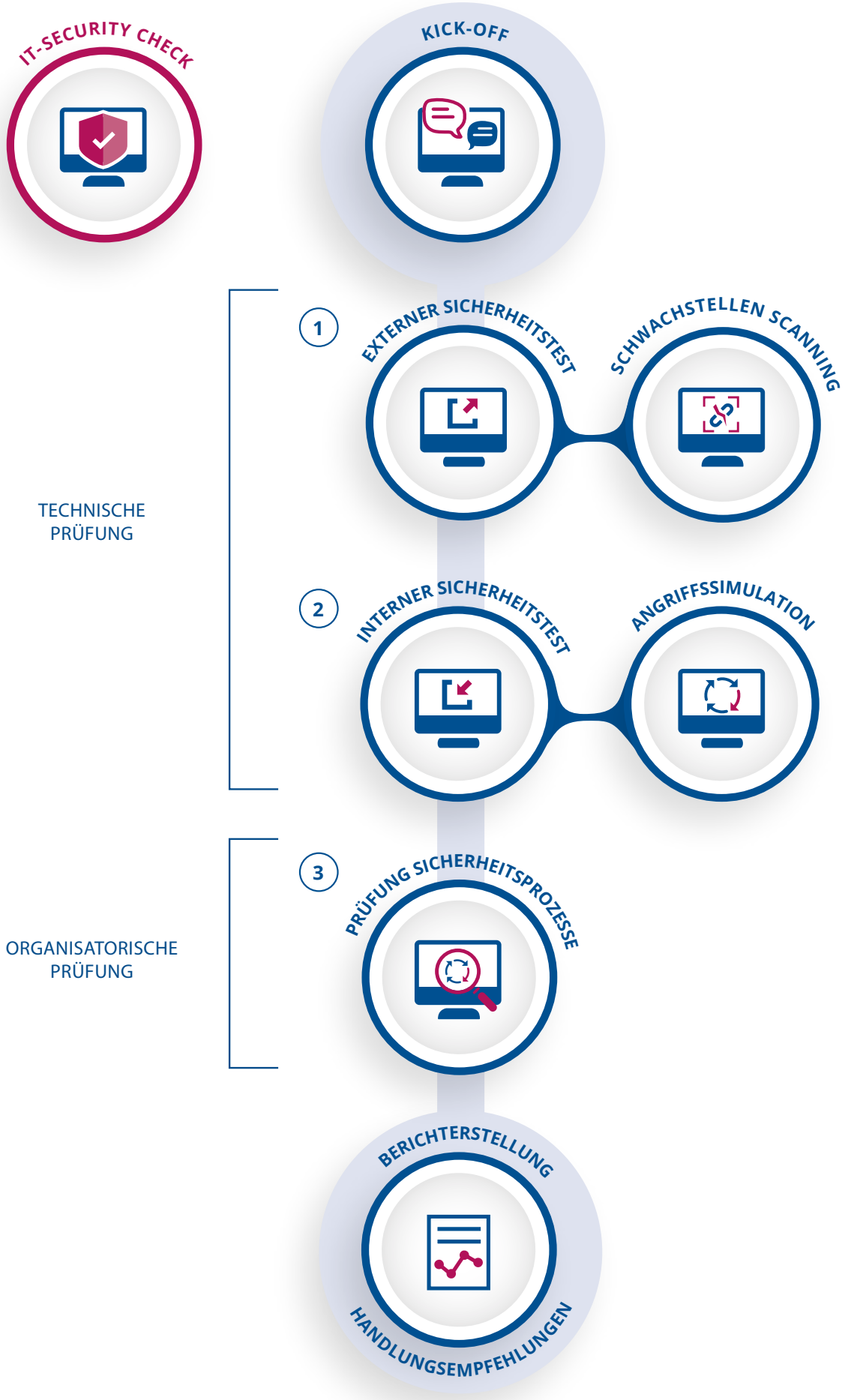
A	Ausbaustufe A – Security Check Basic	6.990,– EUR
B	Ausbaustufe B – Security Check Extended	13.490,– EUR

Reisekosten in Wien und Wien Umgebung sind pauschal inbegriffen. Die Beträge verstehen sich exkl. der Umsatzsteuer in gesetzlicher Höhe.

Gemäß dem Motto „Angriff ist die beste Verteidigung“ simulieren wir gezielte Cyberattacken auf Ihr Unternehmen von außerhalb und innerhalb des Systems und entlarven so Sicherheitslücken, bevor es andere tun.

ENTDECKEN SIE GLEICH AUF DER NÄCHSTEN SEITE WELCHE SCHRITTE UNTERNOMMEN WERDEN.

ABLAUF DES IT-SECURITY CHECK



DIE 3 SCHRITTE IM ÜBERBLICK

	A SECURITY CHECK BASIC	B SECURITY CHECK EXTENDED
KICK OFF		

Gemeinsam bereiten wir Ihren IT-Security Check vor. Es werden die Termine vereinbart, die Verantwortlichkeiten festgelegt, die Kernpunkte erläutert sowie alle notwendige Dokumentationen und Berechtigungen bereitgestellt.

1. EXTERNER SICHERHEITSTEST

Im ersten Schritt erfolgen Angriffsversuche auf das externe, über das Internet erreichbare Netzwerk in Form eines Schwachstellenscans. Wir scannen betroffene Systeme, evaluieren und protokollieren die jeweiligen Versionen, und identifizieren Schwachstellen, die Angreifer leicht ausnutzen könnten.

max. 20 aktive Systeme	✓	✓
Oberflächenüberprüfung einer Webapplikation	✓	✓

2. INTERNER SICHERHEITSTEST

Im zweiten Schritt simulieren wir Angriffsversuche innerhalb des Netzwerks bzw. Systems. Bei dieser Angriffssimulation gehen wir davon aus, dass ein unbefugter Zugriff auf einen Firmencomputer oder auf das Firmennetzwerk hat.
Wir überprüfen Benutzerberechtigungen, Netzwerke und Konfigurationen diverse Programme und Sicherheitseinrichtungen auf Schwachstellen. Gefundene Lücken werden ausgenutzt, um die Auswirkungen aufzuzeigen. Tägliche Statusmeetings und ein Abschlussworkshop informieren über diese Sicherheitslücken.

Sicherheitsprüfung Client	✓	✓
Schwachstellenscan	✗	✓
Prüfung Windows Active Directory	✗	✓
Prüfung 2 Switches/Firewall	✗	✓
Prüfung Security Maßnahmen (A/V, Proxy, NAC, DLP, etc.)	✗	✓
Prüfung WLANs	✗	✓

3. PRÜFUNG SICHERHEITSPROZESSE

Auf Basis der Ergebnisse der Sicherheitstest eruieren wir alle inneren und äußeren Bedrohungen für dasUnternehmen, untersuchen die bestehende Kontrolleinrichtungen und leiten nötige Maßnahmen zur dauerhaften Implementierung eines hohen Sicherheitsniveaus ab. Als Basis dienen die Top 20 der CIS Critical Security Controls (CSC).

PRÜFUNG UMGESETZTER SICHERHEITSPROZESSE UND ANGRIFFSVEKTOREN	✓	✓

BERICHTERSTELLUNG

Die Ergebnisse übermitteln wir Ihnen schriftlich und zeigen auf welche Sicherheitslücken in Ihrem System bestehen, welche Risiken damit einhergehen und wie diese Lücken am besten zu beheben sind. Dieser Endbericht stellt Ihren Sicherheitsstatus dar und gibt Ihnen Handlungsempfehlungen.

Managementpräsentation und Präsentationsunterlagen (inkl. priorisierten Maßnahmen)	✓	✓
Ergebnisworkshop	✗	✓
schriftlicher Endbericht	✓	✓
Detailgrad	limitiert	hoch

WORKSHOP

Viele österreichische Unternehmen sind sich der Gefahren von Cyberkriminalität nicht ausreichend bewusst. Um hier für Aufklärung zu sorgen und den geschäftsführenden Personen Schwachstellen aufzuzeigen, bieten wir in Zusammenarbeit mit unserem Partner eine IT-Risikoanalyse an. Auf diese Weise identifizieren wir die Kernrisiken für Ihre IT-Infrastruktur ohne simulierten Angriff.

1. IDENTIFIKATION VON KERNRISIKEN:
In diesem Workshop erarbeiten Experten zusammen mit der Geschäftsführung, den AbteilungsleiterInnen und Schlüsselpersonen die Kernrisiken und diskutieren die zentralen Systeme und Informationen, die für Ihr Unternehmen besonders kritisch sind. Im Zentrum stehen hier ganz bewusst die Risiken aus Geschäftssicht.

2. BEDROHUNGEN UND MASSNAHMEN:
In diesem Workshop identifizieren wir gemeinsam mit Ihrer IT-Abteilung sowie Sicherheitsverantwortlichen die inneren und äußeren Bedrohungen für das Unternehmen aus IT-Sicht, analysieren bestehende Maßnahmen zur Risikominimierung und leiten Maßnahmen für die Zukunft ab.

3. AKTIONSPLAN:
Abschließend erfolgt die Zusammenführung und Aufbereitung der Ergebnisse der beiden Workshops und die Ableitung von konkreten Maßnahmen und Vorschlägen. Im Rahmen einer Management-Präsentation erläutern wir Ihnen diese Ergebnisse.

KOSTEN

IT-Risikoanalyse – Workshop 4.290,– EUR

Reisekosten in Wien und Wien Umgebung sind pauschal inbegriffen.
Die Beträge verstehen sich exkl. der Umsatzsteuer in gesetzlicher Höhe.

SCHULUNG

Auch wenn alle technischen und organisatorischen Schwachstellen behoben wurden, bleibt noch immer ein wesentliches Sicherheitsrisiko bestehen:
der Mensch selbst.

Die meisten Angreifer zielen auf die Unwissenheit bzw. Gutgläubigkeit von Menschen ab, um diesen wichtige Informationen zu entlocken. Vor allem sogenanntes Spear-Phishing versucht den MitarbeiterInnen mit gezielten Attacken, welche sich durch Personalisierung und einen hohen Grad an Glaubwürdigkeit auszeichnen, Passwörter und Zugangsdaten zu entlocken.

Um auch gegen diese Gefahr gewappnet zu sein, muss der MitarbeiterInnenstab geschult und auf die Bedrohung aufmerksam gemacht werden. Gut informiert können sie Angriffsversuche frühzeitig erkennen und durch kritisches Hinterfragen essentiell zur IT-Security beitragen.

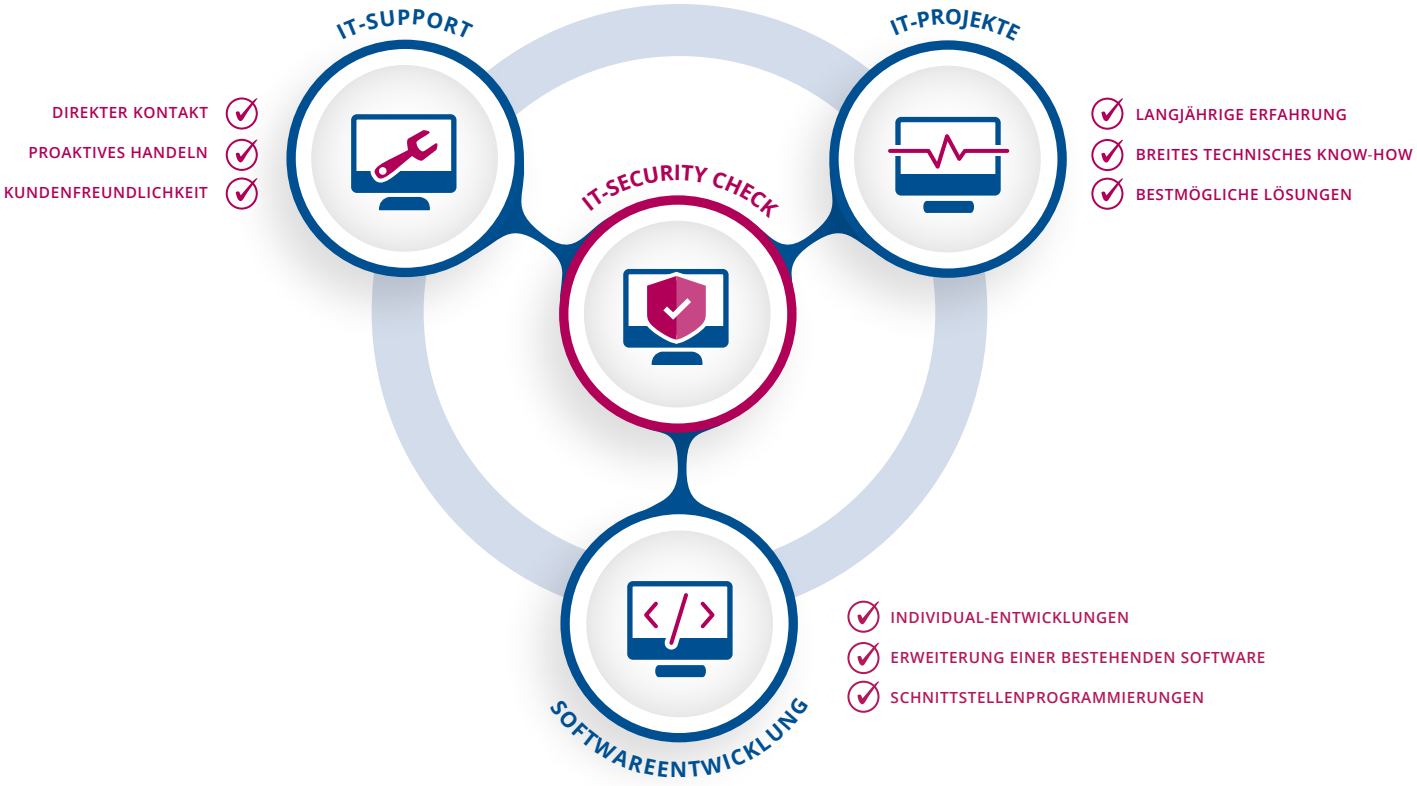
In der Security Awareness-Schulung werden Top Management und MitarbeiterInnen auf Basis des vorhandenen Wissensstands gezielt und individuell auf diese Bedrohungen vorbereitet.

KOSTEN

Security Awareness – Schulung 6.490,– EUR

Reisekosten in Wien und Wien Umgebung sind pauschal inbegriffen.
Die Beträge verstehen sich exkl. der Umsatzsteuer in gesetzlicher Höhe.

IT-SPEZIALIST SEIT 20 JAHREN



Wir von GEKKO sind IT-Dienstleister mit Leidenschaft. Seit nunmehr zwei Jahrzehnten sind wir mit unserem Wissen, unserer Erfahrung und unserem Herzen als IT-Partner für Klein- und Mittelunternehmen im Einsatz.
Jeder unserer Kunden ist einzigartig und erfordert daher auch einen einzigartigen und individuell abgestimmten IT-Service.
Wir bieten IT, die Sie brauchen:

IT-SUPPORT – Bei Problemen, Störausfällen oder als Ansprechperson bei Unsicherheiten:
Unser zertifiziertes Expertenteam ist 365 Tage im Jahr für Sie da.
Wir kümmern uns um Ihre IT, damit Sie sich auf Ihr Kerngeschäft konzentrieren können.

IT-PROJEKTE – Ob kleine, einfache Netzwerkverbindungen oder eine komplexe IT-Infrastruktur:
Wir nehmen jedes Projekt persönlich und zwar von der Konzeption bis zur Umsetzung.

SOFTWAREENTWICKLUNG – Von der Programmierung komplexer Schnittstellen bis hin zu benutzerfreundlichen Ticketing-Systemen:
Individuelle Software-Lösungen sind unsere Spezialität.

IT-SECURITY – Wir nehmen die Sicherheit Ihrer IT ernst.
Um unsere Kunden vor hinterlistigen Angriffen und den Risiken durch Unwissenheit zu schützen, bieten wir für Ihr Unternehmen Risikoanalysen, gezielte IT-Sicherheitsprüfungen und Awareness-Schulungen an. Diese Analysen führen wir in Zusammenarbeit mit einem unabhängigen und renommierten Partner durch, um größtmögliche Qualität und Objektivität gewährleisten zu können.

Johannes Kunschert und Marcus Weixelberger – Inhaber und Geschäftsführer

ÜBER GEKKO – GEKKO wurde 1997 von Marcus Weixelberger und Johannes Kunschert ins Leben gerufen und ist seitdem für Klein- und Mittelunternehmen aus allen Branchen ein inhabergeführter kompetenter Ansprechpartner für alle Themen rund um IT. Über 30 MitarbeiterInnen sorgen dafür, dass sich unsere Kunden auf einen reibungslosen Betrieb ihrer IT-Infrastruktur verlassen können. Als Full-IT-Dienstleister übernehmen wir auch die Einführung, Wartung und Weiterentwicklung von IT-Systemen und IT-Projekten, und bieten maßgeschneiderte Softwarelösungen an. Höchste Kunden- und Mitarbeiterzufriedenheit stehen bei uns immer an erster Stelle.

JETZT KONTAKT AUFNEHMEN UND BERATEN LASSEN!

Thomas Hofstätter – Head of Sales
Mobil: +43 664 8309542
Tel.: +43 1 710 5656
E-Mail: t.hofstaetter@gekko.at

GEKKO

GEKKO IT-SOLUTIONS GMBH
Wiegelestraße 10 | A-1230 Wien

1. PLATZ Wien Kleinbetriebe Austria's Leading Companies 2015 Wirtschaftsblatt

GREAT PLACE TO WORK® Beste Arbeitgeber 2014 Österreich

www.gekko.at