



KÖNIG & HAUSWIRTH OEG
EDV CONSULTING und LÖSUNGEN
A- 2340 Mödling, Beethoven G. 36

Gute Beratung wird verstanden

Sehr geehrte Damen und Herrn!

Wüssten Sie gern, ob die in **Ihrem Unternehmen** angewandten Maßnahmen zur **Sicherheit** der Informationstechnik noch **ausreichen**?

Wenn Sie sicher sein wollen, dass Sie nichts übersehen haben und dass die in Ihrer Organisation umgesetzten **Sicherheitsmaßnahmen zusammenpassen**, dann sollten Sie sich mit dem IT-Grundschutz beschäftigen.

Insgesamt passieren immer mehr Störfälle der IT. Obwohl es zunehmend schwerer wird, die Verursacher dafür herauszufinden, werden immer mehr Sicherheitsverstöße festgestellt, die von **unautorisierten Benutzern** verursacht wurden – zunehmend auch von **eigenen Mitarbeitern**. Das meist unbewusst.

Die gefährlichsten Angriffe gehen von Schadprogrammen mit Computer-Viren oder Würmern aus. Der allein durch Computer-Viren verursachte wirtschaftliche Schaden ergibt jährlich einen dreistelligen Millionen-Betrag – mit steigender Tendenz. Bedrohlich sind für die Unternehmen die massenweise eingehenden E-Mails, Spam, die zusätzlich auch über mobile Geräte und über Instant Messaging in die Unternehmen eindringen. Zudem gefährden Web-Attacken von Hackern die **Unternehmensrechner** und die auf ihnen gespeicherten Informationen. Die Angriffe auf die IT von Unternehmen verursachen zunehmend **Datenverluste** und durchschnittlich in jedem zwölften Störfall einen Totalausfall des Netzes und aller Dienste. Zunehmende Angriffe zielen mit neuen Phishing-Techniken und ferngesteuerten Computernetzen, Botnets, auf den **Diebstahl von Daten** und Passwörtern in Unternehmen. Meist folgt dem Diebstahl vertraulicher Informationen ein **finanzieller Verlust** für das Unternehmen. Wenn es sich dabei um Wirtschaftsspionage handelt, liegen die Schäden in einer Größenordnung von **mehreren Milliarden Euro** pro Jahr.

Der nachfolgende **Fragebogen** soll Ihnen und Ihren Mitarbeitern einen Überblick über mögliche **Sicherheitslücken und -gefahren** in Ihrem Unternehmen verschaffen und diese aufdecken. Sie können diesen Fragebogen auch von allen Ihren Mitarbeitern getrennt ausfüllen lassen. Somit haben Sie einen noch besseren Überblick und zwar aus verschiedenster Sichtweise!

Gerne helfen wir Ihnen bei der Auswertung der Fragebögen, der Analyse, der Planung und der Umsetzung von zielführenden Maßnahmen, die Sicherheit und Zuverlässigkeit in Ihrem Unternehmen zu erhöhen.

Tipp: Senden Sie uns Ihren ausgefüllten Fragebogen, wir helfen Ihnen!

(Via Fax an die Nummer +43(0)2236 89364001 oder via Email an office@qotec.com)



Seite 1 von 6

Telefon:	0810 700 009	UID:	ATU52837104	Kontonr.:	705.814
Fax:	+43(0)2236-89364001	Firmenbuchnr.:	213589 b	BLZ:	32250
E-Mail:	office@qotec.com	Landesgericht	Wiener Neustadt	IBAN:	AT463225000000705814
Internet:	www.qotec.com	Bank:	RAIKA-Guntramsdorf	BIC:	RLNWATWWGTD



Unternehmen:
Anschrift:
PLZ und Ort:
Name:
Email:
Telefon:
Datum:

KÖNIG & HAUSWIRTH OEG
EDV CONSULTING und LÖSUNGEN
A- 2340 Mödling, Beethoven G. 36

IT Fragebogen

Bitte füllen Sie den nachfolgenden Fragebogen in Ruhe und richtig aus! Ihre Antworten helfen die Sicherheit und Zuverlässigkeit im Umgang mit der IT zu erhöhen bzw. auf einem hohen Level zu halten. Fragen, die auf Sie bzw. auf Ihr Unternehmen nicht zutreffen, überspringen Sie bitte.

Kategorie „Allgemein & Infrastruktur“:

Gibt es einen IT-Beauftragten?

JA NEIN WEISS ICH NICHT

Gibt es geeignete Vertretungsregelungen für Verantwortliche und sind die Vertreter mit ihren Aufgaben vertraut?

JA NEIN WEISS ICH NICHT

Gibt es Checklisten, was beim Eintritt neuer Mitarbeiter und beim Austritt von Mitarbeitern zu beachten ist (Berechtigungen, Schlüssel, Unterweisung etc.)?

JA NEIN WEISS ICH NICHT

Gibt es eine Dokumentation des gesamten IT-Systems?

JA NEIN WEISS ICH NICHT

Wissen Sie, wo sich der nächste Handfeuerlöscher befindet?

JA NEIN WEISS ICH NICHT

Überprüfen Sie regelmäßig, ob die Fenster (falls sich diese öffnen lassen) bei Verlassen der Räume verschlossen sind?

JA NEIN WEISS ICH NICHT

Schließen Sie bei Verlassen Ihres Büros die Tür ab, um den Zugriff auf darin befindliche Unterlagen und IT-Einrichtungen für Unbefugte zu verhindern?

JA NEIN WEISS ICH NICHT



Ist die Kabelführung in Ihrem Büro so, dass die Kabel nicht stören und Sie nicht darüber stolpern können?
 JA NEIN WEISS ICH NICHT

Haben die Kabel ausreichend Spielraum, so dass sie genügend Zugentlastung in den Steckern haben?
 JA NEIN WEISS ICH NICHT

Haben Ihre Geräte einen entsprechenden Abstand zu den Heizkörpern?
 JA NEIN WEISS ICH NICHT

Werden Geräte wie Server, Switches und Router in einem verschließbaren Schrank oder einem eigenen Raum verwahrt?
 JA NEIN WEISS ICH NICHT

Haben nur befugte Personen Zutritt zu Ihren Geräten?
 JA NEIN WEISS ICH NICHT

Besteht ein angemessener Schutz der IT-Systeme gegen Feuer, Überhitzung, Wasserschäden, Überspannung und Stromausfall?
 JA NEIN WEISS ICH NICHT

Kategorie „IT Organisation“:

Gibt es für die eingesetzten Datenträger ein Bestandsverzeichnis?
 JA NEIN WEISS ICH NICHT

Sind die Datenträger gekennzeichnet?
 JA NEIN WEISS ICH NICHT

Werden die Datenträger sachgerecht und vor unbefugtem Zugriff geschützt aufbewahrt?
 JA NEIN WEISS ICH NICHT

Werden Vollständigkeitskontrollen des Datenträgerbestandes vorgenommen?
 JA NEIN WEISS ICH NICHT

Werden von Dritten erhaltene Datenträger auf Computer-Viren überprüft?
 JA NEIN WEISS ICH NICHT

Ist Ihr Computer, und der Ihrer Mitarbeiter frei von Software die Sie selbst besorgt haben? (Spiele, lustige Bildschirmschoner, ...)
 JA NEIN WEISS ICH NICHT



Achten Sie darauf, Fremde (Besucher, Handwerker, Wartungs- und Reinigungspersonal) nicht unbeaufsichtigt zu lassen?

JA NEIN WEISS ICH NICHT

Kategorie „Passwort Handhabung“:

Haben Sie ein Netzwerk-Passwort?

JA NEIN WEISS ICH NICHT

Haben Sie bei Ihrem Computer oder Notebook ein BIOS Passwort definiert?

JA NEIN WEISS ICH NICHT

Ist auf Ihrem Rechner ein Bildschirmschoner mit integriertem Passwortschutz installiert?

JA NEIN WEISS ICH NICHT

Sind Ihre Passwörter nur Ihnen bekannt?

JA NEIN WEISS ICH NICHT

Enthalten Ihre Passwörter Begriffe aus Ihrem Umfeld? (Automarke, Hobby, etc.)?

JA NEIN WEISS ICH NICHT

Verwenden Sie bei der Bildung Ihrer Passwörter Sonderzeichen oder Zahlen?

JA NEIN WEISS ICH NICHT

Bieten Programme und Anwendungen Sicherheitsmechanismen wie Passwortschutz oder Verschlüsselung?
Sind die Sicherheitsmechanismen aktiviert?

JA NEIN WEISS ICH NICHT

Wurden voreingestellte oder leere Passwörter geändert? (z.B. Router, Firewall, ...)?

JA NEIN WEISS ICH NICHT

Wurden voreingestellte oder leere Passwörter geändert? (z.B. Router, Firewall, ...)?

JA NEIN WEISS ICH NICHT

Werden vertrauliche Daten und besonders gefährdete Systeme wie Notebooks ausreichend durch Verschlüsselung oder andere Maßnahmen geschützt?

JA NEIN WEISS ICH NICHT

Sind die wichtigsten Passwörter für Notfälle sicher hinterlegt?

JA NEIN WEISS ICH NICHT

Kategorie „Virenschutz“:

Werden flächendeckend Viren-Schutzprogramme eingesetzt?

JA NEIN WEISS ICH NICHT

Werden die Viren-Schutzprogramme regelmäßig, am besten täglich aktualisiert?

JA NEIN WEISS ICH NICHT

Wird die Aktualität des Virenschutzes ständig kontrolliert?

JA NEIN WEISS ICH NICHT

Besteht ein mehrstufiger Virenschutz (Arbeitsplatz, Server, Außenverbindungen, Notebooks, PDA)?

JA NEIN WEISS ICH NICHT

Werden ein- und ausgehende Emails auf Viren überprüft?

JA NEIN WEISS ICH NICHT

Sind Ihre Mitarbeiter gesondert über den umsichtigen und sachgerechten Umgang mit E-Mails und Internetbrowsern informiert worden?

JA NEIN WEISS ICH NICHT

Existieren Vorkehrungen zur Reduzierung ungewünschter E-Mails (SPAM)?

JA NEIN WEISS ICH NICHT

Kategorie „Datensicherung“:

Führen Sie eine tägliche, automatische Datensicherung durch?

JA NEIN WEISS ICH NICHT

Wird das Ergebnis der Datensicherung täglich von Ihnen oder einer Vertrauensperson überprüft?

JA NEIN WEISS ICH NICHT

Werden die aktuell benutzen Sicherungsmedien sofort nach Abschluss der Datensicherung lokal sicher z.B. in einem Safe aufbewahrt?

JA NEIN WEISS ICH NICHT

Werden die nicht aktuell benötigten Sicherungsdatenträger außerhalb Ihres Gebäudes, z.B. in einem Bankschließfach aufbewahrt?

JA NEIN WEISS ICH NICHT

Wird in regelmäßigen Abständen versucht, die Datensicherungen wiederherzustellen?

JA NEIN WEISS ICH NICHT

Speichern Sie und Ihre Mitarbeiter Ihre Daten auf einem Laufwerk, das automatisch gesichert wird?
JA NEIN WEISS ICH NICHT

Sichern Sie die Konfiguration Ihrer Server oder Workstation mit einem Image Programm?
JA NEIN WEISS ICH NICHT

Kategorie „Firewall & Netzwerk“:

Gibt es eine Firewall?
JA NEIN WEISS ICH NICHT

Ist sichergestellt, dass alle Außenverbindungen des Netzwerkes wirklich über eine Firewall abgesichert sind (auch ISDN-Karten, Modems in PC-Systemen)?
JA NEIN WEISS ICH NICHT

Werden sichere Verschlüsselungstechnologien für Remotezugänge (Einwahl in das Netzwerk von außen) eingesetzt?
JA NEIN WEISS ICH NICHT

Nutzen Sie Sicherheitstechniken zur Verschlüsselung und Absicherung des Funknetzwerkes wie WEP, WPA, IPsec, etc.?
JA NEIN WEISS ICH NICHT

Nutzen Sie ein Netzwerkmonitoring?
JA NEIN WEISS ICH NICHT

Ist geregelt, auf welche Datenbestände jeder Mitarbeiter zugreifen darf? Gibt es sinnvolle Beschränkungen?
JA NEIN WEISS ICH NICHT

Danke für Ihre Zeit! Der Fragebogen ist nun zu Ende.