

- **Sie haben Fragen?**
- **Sie benötigen weiterführende Informationen?**
- **Sie wünschen einen kostenlosen und unverbindlichen Beratungstermin?**

Dann senden Sie uns Ihren Quickcheck- Fragebogen per Mail oder per Fax ausgefüllt an unsere unten angegebene Adresse zu.

Wir werden uns dann schnellstmöglich für ein persönliches und kostenfreies Beratungsgespräch (ca. 30 Minuten) mit einem Mitgliedsunternehmen bei Ihnen melden.

Die Ergebnisse und den ausgefüllten Fragebogen behandeln wir selbstverständlich vertraulich.

Ein Beratungsgespräch ist auch ohne Zusendung des ausgefüllten Fragebogens möglich.

Ihr Kontakt

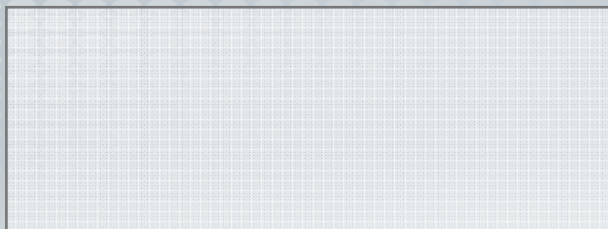
E-Mail: quickcheck@ruhr-networker.de

ruhr networker e.V.
Karolingerstr. 96
45141 Essen

T: +49 (201) 81 27 900

F: +49 (201) 81 27 901

www.quickcheck-it-sicherheit.de



Quickcheck "IT-Sicherheit"

Datenschutz und Datensicherheit bleiben ein wichtiges Thema.

Gerade beim Outsourcing von betrieblichen Prozessen oder dem Zugriff auf externe Anwendungen und Datenspeicher muss ein wirkungsvoller Schutz gewährleistet sein. Für Unternehmen spielt daher die IT-Sicherheit eine immer größere Rolle.

Der ruhr networker e.V. hat hierzu einen Fragebogen "Quickcheck IT-Sicherheit" erstellt. Zu fünf Bereichen werden Fragen gestellt, die mit JA oder NEIN zu beantworten sind. Der Fragebogen ist dabei in weniger als fünf Minuten ausgefüllt.

Bei Unsicherheit oder wenn mindestens eine Frage mit NEIN beantwortet wurde besteht die Möglichkeit eines kostenfreien Beratungstermins (ca. 30 Minuten). Im Rahmen des Gesprächs geben Ihnen unsere Mitgliedsunternehmen wertvolle Expertentipps.

Alles kostenlos – aber nicht umsonst!

1. IT-Sicherheit als Chefsache

JA NEIN

- Ist der Geschäftsführung das Risiko durch eine unzureichende IT-Sicherheit für das eigene Geschäft bekannt?
- Ist das Management von Risiken und Informationssicherheit explizit Bestandteil der Unternehmenspolitik?
- Wird der Geschäftsführung regelmäßig über Risiken und das Sicherheitsniveau direkt berichtet?
- Wurde ein „fachkundiger und zuverlässiger“ Datenschutzbeauftragter gemäß § 4f BDSG bestellt?

2. IT-Sicherheits-Organisation

JA NEIN

- Wurde der Datenbestand im Hinblick auf Sensibilität/Schutzwürdigkeit bzw. Bedeutung analysiert und klassifiziert?
- Existiert ein Datenschutz-Konzept zur Berücksichtigung der gesetzlichen Vorgaben?
- Existiert eine IT-Security-Policy bzw. IT-Sicherheitskonzept?
- Sind eindeutige Verantwortlichkeiten für geschäftskritische Informationen und Verfahren festgelegt?
- Sind Kontrollverfahren etabliert, um interne und externe Prozesse auf Ordnungsmäßigkeit und Einhaltung zu überprüfen?

3. Technische und organisatorische Maßnahme

JA NEIN

- Entsprechen alle Komponenten im Bereich IT dem „State of the Art“?
- Existiert ein Berechtigungskonzept (inkl. der Rechtevergabe), welches sicherstellt, dass jeder Benutzer ausschließlich auf jene Informationen zugreifen kann, die er zwingend für seine Tätigkeiten benutzt?
- Werden unerlaubte Zugriffsversuche auf vertrauliche Daten protokolliert?
- Ist die Vernichtung von Daten und Hardware verbindlich geregelt?
- Werden regelmäßig Backups und Wiederherstellungstests gemacht?

4. Schulung und Richtlinien

JA NEIN

- Ist der Umgang mit der IT und den Daten in Betriebsvereinbarungen bzw. Arbeitsanweisungen geregelt?
- Werden alle Mitarbeiter bei Einstellung sowie regelmäßig zum Thema IT-Sicherheit und Datenschutz sensibilisiert?

5. Compliance/Ordnungsmäßigkeit beim Outsourcing

JA NEIN

- Sind beim Outsourcing die Sicherheitsanforderungen und -verantwortlichkeiten vertraglich festgelegt?
- Werden beim Outsourcing die gesetzlichen Vorgaben des § 11 BDSG stets beachtet?
- Werden Leistungserbringer wie Baumaßnahmen (z. B. in der Nähe des Serverraums) oder Reinigungskräfte im Unternehmen überwacht bzw. gibt es hierzu verbindliche Regeln?