



# 10 Tipps zur Erhöhung der IT-Sicherheit im Unternehmen

Gefördert durch:



aufgrund eines Beschlusses  
des Deutschen Bundestages

Träger des BIEG Hessen



Frankfurt am Main  
Fulda  
Hanau-Gelnhausen-Schlüchtern  
Offenbach am Main



## Am Arbeitsplatz

### **1. Passwörter sind vertraulich und nach Möglichkeit persönlich**

Jeder im Unternehmen hat seine eigenen Zugangsdaten – auf den Rechner oder wenn vorhanden auf das Hausnetz. Diese Daten werden nicht untereinander ausgetauscht. Passwörter werden regelmäßig gewechselt, bei geringen Sicherheitsanforderungen monatlich. Alle Mitarbeiter werden gelegentlich darauf hingewiesen, dass Passwörter Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten und nicht zu kurz sein sollten.

### **2. USB – tut nicht weh?**

USB-Sticks oder andere USB-Geräte sind wirklich praktisch und einfach. Leider überbrücken Sie häufig eigentlich getrennte Sicherheitsbereiche. Wenn der USB-Stick auf einem privaten Rechner ohne Sicherheitsmechanismen wie Antivirenschutz eingesetzt wurde oder bei einer fremden Firma im Einsatz war, kann der Stick schon die gefährlichen Trojaner beinhalten. Als Verantwortlicher können Sie

- die USB-Anschlüsse sperren
- die Mitarbeiter verpflichten, möglicherweise unsichere USB-Geräte an einem dafür vorgesehenen Rechner zu testen.

Sie sollten in jedem Fall für die USB-Problematik sensibilisieren und eine Software auf jedem

Rechner haben, die USB-Geräte überprüfen kann – auch wenn bereits das Einstecken und die damit ausgelöste Selbstinstallation ein Sicherheitsrisiko darstellt.

### **3. Papier weg – oder Raum zu**

Angebote, Kundendaten und sonstige wichtige Papiere sollten nicht in unabgeschlossenen Räumen offen zugänglich sein. Also entweder

- die Papiere in eventuell feuerfeste Schließschränke oder
- die Tür bei Verlassen des Raumes abschließen.

Geschäftskritischer Papierabfall muss geschreddert werden.

### **4. Compliance – Datenschutz, Archivierung und mehr**

Compliance, ein neudeutsches Wort für rechtskonformes Verhalten, umfasst zumeist die datenschutzrechtlichen, steuerarchivierungsrechtlichen IT-Pflichten ebenso wie die unternehmerische Vorsorgepflicht. Investieren Sie die Zeit in ein Überblickseminar!



## Interne Systeme

### **5. Software – nicht unbedingt neu, aber aktualisiert**

Man benötigt nicht unbedingt die neueste Software, um sicher zu arbeiten. Aber alle Betriebssysteme und Anwendungen sollten so automatisch und regelmäßig wie möglich aktualisiert werden.

### **6. Spamfilter erleichtern nicht nur die Arbeit, sie machen sie auch sicherer**

Spam-E-Mails erschweren nicht nur das Erkennen der nützlichen Mails, sie stellen auch zu meist ein Sicherheitsrisiko dar, spähren Passwörter und Kreditkarteninformationen aus und können das Firmennetzwerk oder den Webserver ungewollt in einen böartigen Angreifer verwandeln.

### **7. Nur ein nutzbares Backup ist ein gutes Backup**

Backups, also Sicherungskopien, werden sinnvollerweise möglichst automatisch gemacht. Die Wenigsten testen allerdings, ob sie ihre Sicherungskopien auch wirklich zur Systemwiederherstellung einsetzen können. Auch weiß man erst dann, wie lange denn eine solche Rettungsaktion dauert und was man dabei beachten muss. Backups, deren Nutzbarkeit zur Datenwiederherstellung man nicht getestet hat, bieten maximal eine trügerische Sicherheit. Backups sollten an einem sicheren, aber immer zugängli-

chen Ort (z.B. Bankschließfach) aufbewahrt werden.

## Internet

### **8. Die Geheimhaltungspflicht ausdrücklich auf Social Media ausdehnen**

Im Internet bilden sich immer mehr Gemeinschaften, viele Websites bündeln Personenprofile, immer mehr persönliche Informationen werden im Internet preisgegeben, etwa in Blogs, also in Online-Tagebüchern. Hier brüsten sich Mitarbeiter, dass sie Entwickler in einem High-Tech-Unternehmen seien, oder verschaffen ihrem Ärger über den Chef Luft. Ergänzen Sie die übliche betriebliche Geheimhaltungsvereinbarung ausdrücklich um die sogenannten Social Media und sensibilisieren Sie Ihre Mitarbeiter, dass das Internet nicht vergisst – weder das Lästern über Kunden, Kollegen und Chefs, noch Fotos von Betriebs-feiern oder aus dem Urlaub.

### **9. E-Mail – so sicher wie eine Postkarte**

Unverschlüsselte E-Mails lassen sich relativ leicht mitlesen und gegebenenfalls auch fälschen. Daraus folgt:

- Entweder keine sensiblen Informationen per E-Mail versenden oder
- E-Mails verschlüsseln

## Die Goldene Regel



## 10. Sicherheit muss gelebt werden

IT-Sicherheit sichert ihren Geschäftserfolg und behindert ihn nicht! Wenn Sie dies wirklich verstanden haben, fällt es Ihnen deutlich leichter, selber auf IT-Sicherheit zu achten und auch Ihre Mitarbeiter regelmäßig in abwechslungsreicher, angemessener Form auf wichtige Sicherheitsthemen hinzuweisen.

Weitere Infos: [www.kmu-sicherheit.eu](http://www.kmu-sicherheit.eu)

Stand: Dezember 2009

Autoren:  
Olaf Jüptner  
Torsten Lex  
HA Hessen Agentur GmbH  
[www.hessen-it.de](http://www.hessen-it.de)



### **Für was steht BIEG Hessen?**

BIEG Hessen steht für Beratungs- und Informationszentrum Elektronischer Geschäftsverkehr. Das BIEG Hessen ist eine gemeinsame Einrichtung der Industrie- und Handelskammern Frankfurt am Main, Fulda, Hanau-Gelnhausen-Schlüchtern und Offenbach am Main. Wir sind eines der Kompetenzzentren, die vom Bundesministerium für Wirtschaft und Technologie gefördert werden.

### **Aufgaben des BIEG Hessen**

Das BIEG Hessen hat zur Aufgabe, kleine und mittlere Unternehmen aller Branchen auf dem Weg zu Internet und E-Business neutral zu unterstützen. Wir verstehen uns als Plattform für Anbieter und Nachfrager und wollen dazu beitragen, dass Barrieren abgebaut und Chancen aufgezeigt werden. Das BIEG Hessen ist eine Anlaufstelle für Unternehmer sowie Kommunikator und Koordinator für den elektronischen Geschäftsverkehr.

### **BIEG Hessen**

Börsenplatz 4  
60313 Frankfurt am Main  
Telefon 069 2197-1380  
Telefax 069 2197-1497  
info@bieg-hessen.de

Auf unsere Internetseite [www.bieg-hessen.de](http://www.bieg-hessen.de) finden Sie weitere Leitfäden, Checklisten und Fachartikel zu den Themen Internet und E-Commerce.