

# Grundlagen der IT-Sicherheit für KMU: Organisatorische IT-Sicherheit

Ein Merkblatt der Industrie- und Handelskammer Hannover

Technische Sicherheitsmaßnahmen allein reichen nicht aus. Obschon hier in den letzten Jahren verstärkt Anstrengungen unternommen wurden, haben viele Unternehmen die organisatorische Ebene der IT-Sicherheit vernachlässigt. Welchen Nutzen stiften etwa Passwörter, wenn nicht durch Anweisungen innerhalb der Organisation sichergestellt ist, wie damit sicher umzugehen ist? Solche oder vergleichbare Umstände führen zu erheblichen Schwachstellen und Angriffspunkten im Unternehmen, nicht zuletzt vor dem Hintergrund, dass ein Großteil der IT-Sicherheitsrisiken aus dem (Fehl-) Verhalten der eigenen Mitarbeiter resultiert.

Grundlegende Voraussetzung für mehr Sicherheit im Unternehmen ist jedoch, dass IT-Sicherheit von der Unternehmensleitung als strategische Aufgabe wahr- und angenommen wird. Dieser hohe Stellenwert ist zudem seitens der Geschäftsleitung im gesamten Unternehmen zu kommunizieren.

Das vorliegende Merkblatt in Form einer Kurzanleitung nebst Kurz-Checklisten soll einige wichtige Schritte auf dem Weg zu mehr IT-Sicherheit im Unternehmen skizzieren und verschiedene Anhaltspunkte und Anstöße für die betriebliche Umsetzung geben. Weitere Hinweise zum tieferen Einstieg in die Materie befinden sich am Ende des Merkblatts.

## 1. Festlegung eines IT-Sicherheitsverantwortlichen

Verantwortlichkeiten und Zuständigkeiten müssen auch für den Bereich IT klar geregelt sein. Durch die Unternehmensleitung sollte ein Verantwortlicher für die IT-Sicherheit festgelegt werden, der als direkter Ansprechpartner für die Mitarbeiter bei auftretenden Sicherheitsproblemen fungiert und in dieser Funktion auch einen Zugang zur Unternehmensleitung hat. Dies gilt umso mehr, sofern der Betrieb über keine eigene EDV-Abteilung verfügt. Aufgrund natürlicher Fehlzeiten (Urlaub, Krankheit etc.) muss auch hier für eine Vertretungsregelung gesorgt werden. Der bzw. die IT-Sicherheitsverantwortliche/n muss/müssen bei allen Mitarbeitern als Ansprechpartner bekannt gemacht werden. Großunternehmen sowie große mittelständische Unternehmen sollten über ein umfassendes IT-Sicherheitsmanagement verfügen.

→ Hat Ihr Unternehmen einen Ansprechpartner für IT-Sicherheitsfragen und einen entsprechenden Vertreter?

→ [Deutschland sicher im Netz e. V.: IT-Sicherheitsmanagement für Ihr Unternehmen](https://www.sicher-im-netz.de/unternehmen/174.aspx)  
<https://www.sicher-im-netz.de/unternehmen/174.aspx>

## 2. Erstellung eines Notfallplans

Stromausfall, die versehentliche Löschung ganzer Datenbestände, eine Infizierung des Netzwerks mit Viren, Computerwürmern oder Trojanern oder ein Angriff auf die Unternehmens-Website – ein betrieblicher Notfallplan für die wichtigsten denkbaren Szenarien im Bereich der IT-Sicherheit sollte auf jeden Fall vorhanden sein um größeren Schäden vorzubeugen. Darin sind die Verantwortlichen innerhalb und außerhalb des Betriebes für den jeweiligen Notfall mit aktuellen Kontaktdaten aufzuführen. Gerade wenn die IT-Betreuung auf einen oder mehrere Dienstleister – ggf. sogar mit Service-Level-Agreements für Notfälle – ausgelagert ist, sollte ein aktueller Notfallplan vorhanden und allen bekannt sein. Im Schadensfall sollte jeder Mitarbeiter wissen, was zu tun ist und sofort reagieren können.

→ Haben Sie in Ihrem Betrieb einen aktuellen Notfallplan?

→ Deutschland sicher im Netz e. V.: Notfall-Flyer  
<https://www.sicher-im-netz.de/unternehmen/185.aspx>

→ Deutschland sicher im Netz e. V.: Leitfaden Sicher im Netz (S. 74 ff.)  
<https://www.sicher-im-netz.de/unternehmen/110.aspx>

## 3. Sicherheitsrichtlinien für Mitarbeiter

Oft unterschätzt gilt jedoch das Fehlverhalten der eigenen Mitarbeiter also eines der größten Risiken für die eingesetzte IT. Eine unternehmensweite und verbindliche IT-Sicherheitsrichtlinie (häufig auch als „IT Security Policy“ oder „IT-Sicherheitsleitlinie“ bezeichnet) sorgt für Abhilfe. Sie enthält Vorgaben für die Mitarbeiter, wie sie IT und Internet sicher nutzen können. Darin ist etwa festzulegen, was die Mitarbeiter bei der Nutzung des Internet zu beachten haben, wie korrekt mit Passwörtern und Zugangsdaten umzugehen ist etc. Die Sicherheitsrichtlinie ist an aktuelle Entwicklungen, z. B. in Bezug auf die fortschreitende Nutzung mobiler Endgeräte (Smartphones, PDA), regelmäßig anzupassen bzw. zu ergänzen.

→ Hat Ihr Unternehmen eine für alle Mitarbeiter transparente, aktuelle Sicherheitsrichtlinie?

→ BSI: IT-Sicherheitsleitlinie  
[https://www.bsi.bund.de/cln\\_156/ContentBSI/grundschutz/webkurs/gskurs/seiten/s2400.htm.html](https://www.bsi.bund.de/cln_156/ContentBSI/grundschutz/webkurs/gskurs/seiten/s2400.htm.html)

→ BITKOM e. V.: Leitfaden Email und Internet im Unternehmen  
[http://www.bitkom.org/de/publikationen/38337\\_33696.aspx](http://www.bitkom.org/de/publikationen/38337_33696.aspx)

#### 4. Mitarbeiter schulen

Dem Verhalten der Mitarbeiter als Schnittstelle zwischen der vom Unternehmen eingesetzten IT und den Risiken im Internet kommt eine herausragende Rolle zu. Der sichere Umgang mit den IT-Systemen innerhalb der Organisation setzt daher eine ausreichende Einführung und Schulung der Mitarbeiter voraus. Dazu gehören Technik und Programmfunktionen ebenso wie ein sicherheitsorientierter Umgang mit Unternehmensdaten und IT-Systemen.

Diese Schulungen und Sicherheitssensibilisierungen sind regelmäßig zu wiederholen, um das Sicherheitsbewusstsein im Betrieb auf einem hohen Niveau fortlaufend zu gewährleisten. Die Beschäftigten sind zudem über aktuelle Bedrohungen im Internet rechtzeitig zu unterrichten.

→ Wann haben Ihre Mitarbeiter die letzte Schulung zur IT-Sicherheit erhalten?

→ Initiative Deutschland sicher im Netz e. V.: Checkliste für Mitarbeiter  
<https://www.sicher-im-netz.de/unternehmen/174.aspx>

#### 5. Datensicherung

Eine aktive Datensicherung (Back-up) ist für Unternehmen unabdingbar. Ein auch nur temporärer Verlust wichtiger Unternehmensdaten (z. B. von Forschungsdaten) kann zu gravierenden Einschränkungen für den Betrieb und damit zu erheblichen wirtschaftlichen Schäden führen. Ein – wenngleich eher unwahrscheinlicher – vollständiger Datenverlust kann gar die Existenz des Unternehmens ernsthaft bedrohen.

Wichtig ist also eine regelmäßige Datensicherung im Unternehmen. Dafür gibt es verschiedene technische Systeme und auch die Regelmäßigkeit der Sicherung kann je nach Bedeutung der jeweiligen Daten unterschiedlich festgelegt werden. Wichtige Unternehmensdaten sollten als regelmäßig aktualisierte Sicherungskopie zusätzlich auch außerhalb des Unternehmen eingelagert werden, um im Katastrophenfall (Beispiel: Brand) das Risiko des vollständigen Datenverlustes zu streuen. Zudem sollte unbedingt regelmäßig getestet werden, ob die gesicherten Daten auch jederzeit wieder erfolgreich eingespielt werden können (sog. Rücksicherung/Restore).

→ Existiert in Ihrem Unternehmen ein Datensicherungskonzept?

→ Netzwerk Elektronischer Geschäftsverkehr (NEG): Wie sichere ich meine Daten - 10 Tipps zur Datensicherung  
<http://www.ec-net.de/EC-Net/Navigation/Bibliothek/publikationen,did=353348.html>

## 6. Richtiges Löschen von Daten

Werden Daten nicht mehr benötigt, wenn beispielsweise die gesetzlichen Aufbewahrungsfristen enden oder wenn die Hardware, auf der die Daten vorgehalten werden, ersetzt wird, sind diese weiterhin vor unbefugter Kenntnisnahme durch Dritte zu schützen. Oftmals befinden sich auf ausrangierten Festplatten noch sensible Unternehmensdaten wie interne Zahlen, Kundeninformationen oder andere Zugangsdaten. Vielen Nutzern ist nicht bewusst, dass ein einfaches Löschen dieser Daten in keinem Fall ausreicht, da die Daten mit relativ geringem Aufwand von Dritten wiederhergestellt werden können. Es ist daher auf spezielle Soft- oder Hardwarelösungen zurückzugreifen, um derartige Datenbestände endgültig unbrauchbar zu machen. So sorgt etwa professionelle Datenlöschungssoftware oder die thermische Zerstörung von Datenträgern für den gewünschten Effekt.

→ Wie geht Ihr Unternehmen mit nicht mehr benötigten Datenbeständen um?

→ BITKOM e. V.: Leitfaden zum sicheren Datenlöschen  
[http://www.bitkom.org/de/publikationen/38337\\_52528.aspx](http://www.bitkom.org/de/publikationen/38337_52528.aspx)

→ Netzwerk Elektronischer Geschäftsverkehr (NEG): Sicherheitstipp Sicheres Speichern und Löschen Ihrer Daten  
<http://www.ec-net.de/EC-Net/Navigation/Bibliothek/publikationen,did=352962.html>

## 7. Dokumentation

Für den Krisenfall ist eine aktuelle Dokumentation des betrieblichen IT-Systems eine hilfreiche und notwendige Grundlage, um ohne größere Zeitverluste die Problemlösung in Angriff zu nehmen. In die Dokumentation gehören ein aktuelles Inventar der eingesetzten Hard- und Software, die Konfiguration der wichtigsten Systeme und die Servicenummern der wichtigsten IT-Lieferanten und IT-Dienstleister inklusive vertraglicher Vereinbarungen, soweit diese etwa in Form von Service-Level-Agreements abgeschlossen wurden.

→ Verfügt Ihr Unternehmen über eine aktuelle Dokumentation?

## 8. Aktualität gewährleisten

Durch den Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) für das zweite Quartal 2010 wird deutlich, dass immer neue Schadprogramme mit hohem Gefährdungsgrad hinzukommen, die die bestehenden Antivirenprogramme an ihre Grenze stoßen lassen. Im Lagebericht wird ferner darauf verwiesen, dass auch neue Technologien, wie etwa der Microblogging-Dienst Twitter, durchaus für Angriffe missbraucht werden können.

Daher sind sämtliche erforderliche Sicherheitsvorkehrungen zu ergreifen, d. h. neue Sicherheits-Updates sind zeitnah in das IT-System einzuspielen, Virenschutzprogramme ständig zu aktualisieren und auch die eingesetzte Hardware ist regelmäßig einer Wartung zu unterziehen. Die fortlaufende Aktualisierung ist ein Muss und wird häufig durch automatische Update-Funktionen in der Software unterstützt.

Die organisatorischen Sicherheitsmaßnahmen und Vorgaben sind zudem in regelmäßigen Abständen auf ihre Einhaltung und Wirksamkeit hin zu überprüfen und ggf. anzupassen. Dazu gehört zunächst eine interne Prüfung der Aktualität der eingesetzten IT-Systeme, der Einhaltung der Vorgaben seitens der Mitarbeiter, beispielsweise beim Zugangsschutz am Arbeitsplatz und bei der Internetnutzung, sowie die Aktualität der Notfallpläne und Dokumentationen. Eine weitere, aber aufwändigere Methode der Prüfung sind Tests der betrieblichen IT-Sicherheit durch externe Dienstleister, die systematisch nach Schwachstellen suchen und Angriffe von außen beispielsweise über sogenannte Penetrationstests simulieren können.

- Ist Ihr IT-System inklusive der mobilen Arbeitsplätze auf dem neuesten Stand?
- Wann fand die letzte Überprüfung Ihrer IT-Sicherheitsmaßnahmen statt?

→ BSI: Info-Dienst über aktuelle Bedrohungen & Sicherheitsupdates:  
<http://www.buerger-cert.de/>

→ BSI: Lageberichte IT-Sicherheit:  
[https://www.bsi.bund.de/cln\\_165/sid\\_5B11DF213980866741EF952D944B9BFF/ContentBSI/Publikationen/Lageberichte/bsi-lageberichte.html](https://www.bsi.bund.de/cln_165/sid_5B11DF213980866741EF952D944B9BFF/ContentBSI/Publikationen/Lageberichte/bsi-lageberichte.html)

### Weiterführende Literatur

Neben den oben bereits aufgeführten Links liefern insbesondere das Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM e. V.), Berlin, der Verein Deutschland sicher im Netz, Berlin, sowie das Institut für Internet-Sicherheit (if)is, Gelsenkirchen, auf ihren Websites weitere Informationen zum Thema in Form von Checklisten, Leitfäden und Broschüren:

- Bundesamt für Sicherheit in der Informationstechnik (BSI): Leitfaden Informationssicherheit  
[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschatz/Leitfaden/GS-Leitfaden\\_pdf.pdf?\\_\\_blob=publicationFile](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschatz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile)
- Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM e. V.): Leitfaden Sicherheit für Systeme und Netze in Unternehmen  
[http://www.bitkom.org/de/publikationen/38337\\_38229.aspx](http://www.bitkom.org/de/publikationen/38337_38229.aspx)

- Deutschland sicher im Netz e. V.“: Leitfaden Sicher im Netz  
<https://www.sicher-im-netz.de/unternehmen/110.aspx>
- Institut für Internet-Sicherheit if(is): Überblick IT-Sicherheitsthemen:  
<http://www.internet-sicherheit.de/service/>

### **Hinweis**

Dieses Merkblatt soll – als Service Ihrer Industrie- und Handelskammer Hannover – nur erste Hinweise geben und erhebt keinen Anspruch auf Vollständigkeit. Obwohl es mit größtmöglicher Sorgfalt erstellt wurde, kann eine Haftung für die inhaltliche Richtigkeit nicht übernommen werden.

Stand: Oktober 2010

### **Autor**

Dr. Elmar Weißnicht  
Abteilung Kommunikation  
Tel. (0511) 3107-358  
Fax (0511) 3107-450  
E-Mail: [weissnicht@hannover.ihk.de](mailto:weissnicht@hannover.ihk.de)

Industrie- und Handelskammer Hannover  
Schiffgraben 49  
30175 Hannover  
[www.hannover.ihk.de](http://www.hannover.ihk.de)