

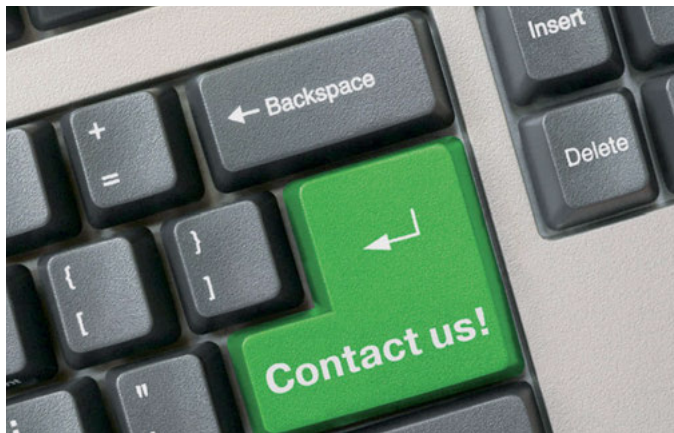
Fazit

Erarbeiten Sie Regeln zum Umgang mit Besuchern und Fremdpersonal, die auf den Bedarf Ihres Unternehmens angepasst sind. Der Erfolg des Besuchermanagements hängt vom Sicherheitsbewusstsein jedes Einzelnen ab.

Nur sensibilisierte Mitarbeiter sind in der Lage, entsprechende Regelungen mitzutragen und im Sinne der Sicherheitskultur des Unternehmens mit Leben zu füllen.

Benennen Sie Verantwortliche, die bei Auffälligkeiten und Verstößen zur Verfügung stehen und entsprechende Maßnahmen einleiten.

Sprechen Sie uns an und vereinbaren Sie einen Termin für ein vertrauliches Sensibilisierungsgespräch



Ihre Ansprechpartner im Wirtschaftsschutz

Landesamt für Verfassungsschutz Hessen
Spionageabwehr / Wirtschaftsschutz
Konrad-Adenauer-Ring 49
65187 Wiesbaden

E-Mail: wirtschaftsschutz@lfv.hessen.de
Tel.: 0611 / 720-600



Gemeinsam. Werte. Schützen.

Dort finden Sie weitere Informationen sowie die Kontaktdaten Ihrer örtlichen Ansprechpartner.



www.wirtschaftsschutz.info

Impressum

Herausgeber: Bundesamt für Verfassungsschutz für den Verfassungsschutzverbund
Bilder: © fhmedien_de - Fotolia.com
© redkoala - Fotolia.com
© Erhan Ergin - Fotolia.com
© Nikolai Sorokin - Fotolia.com
Stand: März 2016

Verfassungsschutz



**Bund
Länder**

Wirtschaftsschutz

**Umgang mit
Besuchern und
Fremdpersonal**

Besuchermanagement

Effektives Besuchermanagement ist für den Know-how-Schutz von elementarer Bedeutung. Es regelt u.a. die Ein- und Ausgangskontrolle, Zutrittsberechtigungen, das Ein- und Ausführen von Gegenständen in den Betrieb und das Führen von Besucherlisten und -ausweisen.

Mangelhaftes oder fehlendes Besuchermanagement ist ein Risiko für die Unternehmenssicherheit.



Risikogruppen

Im Geschäftsleben ist es unumgänglich, unterschiedlichsten Personen Zugang zum Unternehmen zu gewähren. Dazu zählen neben Kunden und Geschäftspartnern auch Zulieferer, Praktikanten, Werksstudenten, Delegationen sowie Dienstleister und weitere Fremdfirmen.

Insbesondere wenn Externe Zugriffe auf Firmennetza haben, ist eine hohe Sensibilität erforderlich. Fremde Nachrichtendienste und Konkurrenten können dies gezielt ausnutzen.

Fallbeispiele

- Unbemerkt fotografiert ein ausländischer Geschäftspartner mittels einer Minikamera Details von Produktionsteilen und Fertigungsanlagen
- Ein Exportdienstleister missbraucht seine Zugänge zum Firmennetzwerk des Auftraggebers, um an sensible Informationen zu gelangen und einen parallelen Vertriebsweg aufzubauen
- Ein Delegationsmitglied entfernt sich unbemerkt von der Gruppe und wird im Bereich der zugriffsbeschränkten Entwicklungsabteilung angetroffen



Empfehlungen

- Klassifizieren und Einrichten zugriffsbeschränkter Bereiche
- Striktes Einhalten von Zutrittsberechtigungen
- Fachkundiges Personal am Empfang
- Registrieren aller Unternehmensfremden (Name, Gesprächspartner, Grund, Zeitpunkt, Betreten und Verlassen)
- Begleiten von Besuchern in sensiblen Bereichen
- Sichtbares Tragen von Mitarbeiter- und Besucher ausweisen
- Schriftliche Anerkennung der Sicherheitsvorschriften
- Optische Sicherheitshinweise
- Für Externe Beschränkung von Zugriffsberechtigungen auf das Firmennetzwerk
- Konsequentes Vorgehen bei Missachtung