

ALLGEMEINE RECHTSFRAGEN - R84

Stand: September 2017

Ihr Ansprechpartner
Ass. Thomas Teschner
E-Mail
thomas.teschner@saarland.ihk.de
Tel.
(0681) 9520-200
Fax
(0681) 9520-690

Wirtschaftskriminalität

Kein Unternehmen ist vor Spionage oder Datendiebstahl mehr gefeit. Und Industrie 4.0 bietet eine noch größere Angriffsfläche. Den Schaden, der pro Jahr zuletzt in Deutschland entstand, beziffert der Bitkom fast auf die Höhe des Staatshaushalts des Freistaats Bayern. Mehr als die Hälfte der Unternehmen (53 Prozent) in Deutschland sind einer Studie des Digitalverbands Bitkom zufolge in den vergangenen zwei Jahren Opfer von Sabotage, Spionage und Datendiebstahl geworden. Dabei sei ein geschätzter Schaden von rund 55 Milliarden Euro pro Jahr entstanden.

Studie: <https://www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutz-in-der-digitalen-Welt.html>

Die Angreifer kommen der Studie zufolge zum überwiegenden Teil aus dem Kreis der aktuellen oder ehemaligen Mitarbeiter des Unternehmens, 62 Prozent der Betroffenen haben demnach die Täter in diesem Umfeld identifiziert. Die Unternehmen sollten sich nicht allein auf eine IT-Firewall verlassen, sondern benötigen auch eine humane Firewall. Dazu gehört eine Unternehmenskultur, die dazu beiträgt, dass Informationsabflüsse durch Mitarbeiter soweit wie möglich reduziert würden. Mit 41 Prozent folgen darauf als Angreifer Wettbewerber, Kunden, Lieferanten oder Dienstleister. Von Hobby-Hackern wurden 21 Prozent getroffen, lediglich 7 Prozent der Attacken stammten aus der organisierten Kriminalität. Auf ausländische Nachrichtendienste entfielen 3 Prozent der Fälle.

Allerdings schaltet nicht einmal jedes dritte betroffene Unternehmen staatliche Stellen nach einem entsprechenden Vorfall ein. Von den Unternehmen, die das überhaupt getan haben, wendete sich ein Großteil an die Polizei, 57 Prozent informierten die Staatsanwaltschaft. An die Datenschutz-Aufsicht oder an das Bundesamt für Sicherheit in der Informationstechnik, das sich als erste Anlaufstelle für solche Vorfälle versteht, wandten sich lediglich jeweils 15 Prozent der Unternehmen. Es ist jedoch von großer Bedeutung, entsprechende Informationen zu teilen. Nur wenn Unternehmen Angriffe melden, können die Sicherheitsbehörden ein realitätsnahes Lagebild erstellen und Abwehrstrategien entwickeln.

Die zuständigen Stellen im **Saarland** sind:

1. **Landespolizeipräsidium Saarland**
Dezernat LPP222 Cybercrime
Hellwigstr. 8-10
66121 Saarbrücken
Tel. 0681 962-0
E-Mail: lpp222@polizei.slpol.de
2. **Landesamt für Verfassungsschutz**
Postfach 10 20 63
66020 Saarbrücken
Tel. 0681 3038-0
E-Mail: info@lfv.saarland.de
3. **Unabhängiges Datenschutzzentrum Saarland**
Fritz-Dobisch-Str. 12
66111 Saarbrücken
Tel. 0681 94781-0
E-Mail: poststelle@datenschutz.saarland.de

Die zuständigen Stellen im **Bundesgebiet** sind:

1. **Bundeskriminalamt**
65173 Wiesbaden
Tel. 0611 55-0
E-Mail: poststelle@bka.de-mail.de (Diese E-Mail-Adresse ist ausschließlich für Inhaber eines DE-Mail-Kontos nutzbar.)
Homepage: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Wirtschaftskriminalitaet/wirtschaftskriminalitaet_node.html
2. **Bundesamt für Verfassungsschutz**
Merianstraße 100
50765 Köln
Tel. 0221 792-0
E-Mail: bfvinfo@verfassungsschutz.de
Homepage: <https://www.verfassungsschutz.de/de/arbeitsfelder/af-spionage-und-proliferationsabwehr>
3. **Bundesamt für Sicherheit und Informationstechnologie**
Postfach 200363
53133 Bonn
Tel. 0228 999582-0
E-Mail: bsi@bsi.bund.de
Homepage: <https://www.bsi.bund.de>

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