



BRILLSTEIN SECURITY GROUP
www.brillstein-security-group.de
NEWS, Pressemitteilungen



12.11.23

20 Maßnahmen gegen Wirtschafts- und Konkurrenzspionage

1. **Implementierung von Sicherheits- und Verschlüsselungstechnologien:** Schulung von Mitarbeitern im sicheren Umgang mit Kommunikationstechnologien wie Laptops, Smartphones und PDAs. Sicherheitsmaßnahmen sollten die Arbeitsabläufe nicht unnötig behindern.
2. **Zugriffsrechte für sensible Daten:** Zugang zu vertraulichen Dokumenten wie Konstruktionsplänen oder Finanzdaten sollte streng kontrolliert und auf das Nötigste beschränkt werden.
3. **Absicherung von Besprechungsräumen:** Verhinderung von Abhörversuchen durch technische Abschirmungen und bewusstes Management von Informationen in sensiblen Bereichen.
4. **Schutz vor kompromittierenden Emissionen:** Abschirmung von PC-Bildschirmen und -Kabeln gegen Ausspähung.
5. **Überprüfung externer Dienstleister:** Sorgfältige Hintergrundüberprüfungen und Überwachung von Reinigungspersonal, Wachdiensten und Zeitarbeitskräften.
6. **Kontrollierter Zutritt zu Unternehmensbereichen:** Einsatz von Zutrittskontrollsystemen und Videoüberwachung in sensiblen Bereichen.
7. **Mitarbeitersensibilisierung:** Regelmäßige Schulungen und Hintergrundchecks zur Sensibilisierung für Spionagerisiken.

8. **Aufklärung über Informationsweitergabe:** Schulung von Mitarbeitern, um unachtsame Weitergabe von vertraulichen Informationen zu vermeiden.
9. **Schulung zur Erkennung von Spionageversuchen:** Durchführung von Sensibilisierungsseminaren, um Mitarbeiter auf Gefahren aufmerksam zu machen.
10. **Vorsicht bei neuen Mitarbeitern:** Überprüfung von Bewerbern, insbesondere in sensiblen Bereichen, auf mögliche Spionagetätigkeiten.
11. **Überprüfung langjähriger Mitarbeiter:** Auch erfahrene Mitarbeiter sollten regelmäßig auf Integrität und Loyalität überprüft werden.
12. **Klare Kommunikationsrichtlinien am Telefon:** Einrichtung klarer Vorgaben für den Umgang mit vertraulichen Informationen am Telefon.
13. **Vorsicht bei ausländischen Wirtschaftsdelegationen:** Skeptischer Umgang mit Informationen, die bei solchen Treffen ausgetauscht werden.
14. **Abwehr von Abwerbungsversuchen:** Sensibilisierung und Überwachung von Mitarbeitern bei Anzeichen von Abwerbungsversuchen durch Konkurrenten.
15. **Maßnahmen beim Ausscheiden von Mitarbeitern:** Sicherung von sensiblen Informationen und Zugängen bei bevorstehendem Austritt von Mitarbeitern.
16. **Schutzmaßnahmen auf Geschäftsreisen:** Vorsichtiger Umgang mit Laptops und anderen Geräten, insbesondere bei Auslandsreisen.
17. **Verbot von privaten Speichermedien:** Vermeidung des Einsatzes privater Geräte mit Speicherfunktion im Unternehmensnetzwerk.
18. **Effektives Abfallmanagement:** Sichere Vernichtung von sensiblen Dokumenten und Datenträgern.
19. **Etablierung von Sicherheitsrichtlinien:** Entwicklung und Durchsetzung verbindlicher Sicherheitsrichtlinien im Unternehmen.
20. **Vorsicht mit Werbematerial:** Prüfung von Werbematerial auf versteckte Schadsoftware.