

Kriterien zur Auswahl eines IT-Sicherheitsexperten:

Grundsätzlich muss beachtet werden, dass sich IT-Sicherheit in verschiedene Bereiche untergliedert, unter anderem in:

- IT-Security: dies betrifft unter anderem den Schutz vor gezielten Angriffen, z.B.: Hackangriffen, Industriespionage, Datendiebstahl, Vandalismus, etc.(Endpoint Security, Perimeter Security, ergo Anti-Malware, Firewall, IDS, Scans, etc.)
- IT-Safety: betrifft den Schutz vor höherer Gewalt, technischem Gebrechen, menschlichem Versagen, usw. (Backup und Recovery, Redundanz und Skalierbarkeit etc.)
- IT-Forensik: betrifft die Rekonstruktion, Rettung und Auswertung von Daten nach einem Sicherheits-Zwischenfall im strafrechtlichen (z.B. gerichtliche Anordnung) oder persönlichen Interesse.

Ein IT-Sicherheitsexperte der beispielsweise Erfahrung darin hat, Hochverfügbarkeitslösungen und redundante Netzwerke aufzubauen, muss nicht gleichzeitig Erfahrung in der forensisch korrekten Beweissicherung von Rechnern, welche einem Angriff ausgesetzt waren, haben. Darum ist es sehr wichtig, gezielt nach spezialisierten IT-Experten in dem jeweils für das Unternehmen relevanten Bereich zu suchen.

Vor Vertragsabschluss sollten zudem Gespräche mit dem IT-Sicherheitsexperten bezüglich der eigenen Branche, der konkreten Anforderungen des Unternehmens, sowie der sicherheitsrelevanten Richtlinien (z.B. Informationssicherheitspolitik) geführt werden.

Weitere wesentliche Kriterien sind:

- Vorlage und Prüfung von **einschlägigen Kundenreferenzen** sowie **Projekterfahrung** für die gesuchte Dienstleistung
- **Überprüfung der Verantwortlichkeiten des IT-Sicherheitsunternehmens** z.B. Abschluss einer Haftpflichtversicherung speziell bei der Durchführung von Penetrationstests
- Forderung nach vollständiger und umfangreicher **Dokumentation** sämtlicher Maßnahmen
- Anwendung von **Geheimhaltungsverpflichtungen** (§ 15 DSGVO 2000)
- Nachweis von **Qualifikationen**
 - Zertifikate im IT-Bereich (Prüfung von Personenzertifizierungen z.B. ISO-27001, ITIL, CISSP, etc., vgl. http://de.wikipedia.org/wiki/Liste_der_IT-Zertifikate)
 - laufende Weiterbildung
 - einschlägige technische Ausbildung der Mitarbeiter/Unternehmensleitung

Beispiele für technische Ausbildungen:

- Masterstudium Netzwerke und Sicherheit, Johannes Kepler Universität
<http://nws.fim.uni-linz.ac.at/>

- Masterstudium Sichere Informationssysteme, FH Hagenberg
<http://www.fh-ooe.at/?id=2305>

- Masterstudium Information Security, FH St. Pölten
<http://www.fhstp.ac.at/studienangebot/master/is/information-security>

- Masterstudium IT Security, FH Campus Wien
http://www.fh-campus-wien.ac.at/forschung_entwicklung/kompetenzzentrum_fuer_it_security/master_studium_it_security/

- Masterstudium Informationsmanagement und Computersicherheit, FH Technikum Wien
http://www.technikum-wien.at/studium/master/informationsmanagement_und_computersicherheit/

- Studium der Informatik mit Spezialisierung auf IT-Sicherheit