Ihr Service für Information und Technologie

AN IHREM UNTERNEHMEN
IST DIE NSA
NICHT INTERESSIERT?

GLÜCK GEHABT!

Wirtschaftsspionage durch Geheimdienste oder andere Unternehmen kann aber alle treffen.

Wie sicher ist IHRE Unternehmenskommunikation?

Vertrauen ist gut, Schutzmaßnahmen sind besser

Die aktuellen Enthüllungen sorgen für große Empörung und Unruhe. Viele Unternehmen sind von den Abhörtätigkeiten der Geheimdienste und deren Umfang überrascht, jedoch sind die Risiken und Bedrohungen für Firmen nicht neu. Dabei müssen Unternehmen weniger Angst vor Geheimdiensten als vor Kriminellen oder Mitbewerbern haben, die internes Wissen für eigene wirtschaftliche Interessen und Wettbewerbsvorteile missbrauchen wollen.

Wirtschaftsspionage ist seit Jahren eine konkrete Bedrohung. Die erforderlichen Schutzmaßnahmen sind bekannt und geeignete Lösungen am Markt verfügbar.

Hundertprozentige Sicherheit kann nicht erreicht werden, wer aber nichts unternimmt, läuft nicht nur Gefahr, ausspioniert zu werden, sondern riskiert die Offenlegung seiner geschäftskritischen Unternehmensgeheimnisse. Punktuelle Einzelmaßnahmen zeigen aber keinerlei Wirkung! Security muss ganzheitlich betrachtet, längst fällige Maßnahmen müssen konsequent umgesetzt werden.

Absolut unverzichtbare Maßnahmen

Der Grundschutz

- Die Aufklärung der Mitarbeiter und das Schaffen eines Sicherheitsbewusstseins in Form von unternehmensweiten Informationskampagnen
- Bewusste Kommunikation und Datenaskese, d. h. Verzicht auf überflüssige Kommunikation und Internet-Services
- Wollen Sie Ihr Unternehmen jedoch wirksam schützen, reicht das bei weitem nicht aus, sondern es müssen zusätzliche Maßnahmen ergriffen werden.

Notwendige Maßnahmen

Erhöhte Schutzstufe

- **Nutzung von Verschlüsselungsverfahren**
  - Geschützte E-Mail-Kommunikation ohne technische Belastung der Anwender
  - Einsatz von VPNs für Kommunikation mit Geschäftspartnern und verbundenen Standorten
  - Umsetzung einer durchgängigen Ende-zu-Ende-Verschlüsselung
  - Verschlüsselung von Cloud-Inhalten bzw. Verzicht auf Online-Speicherung insbesondere im Ausland
- **Vertrauenswürdige Hard- und Software**
  - Einsatz von Lösungen deutscher Hersteller, die unserer strengen Gesetzgebung unterliegen und kontrolliert werden; Der BND hat keinen gesetzlichen Auftrag zur Wirtschaftsspionage
- **Vertrauenswürdige Dienstleister**
  - Zusammenarbeit mit deutschen Unternehmen, bei denen sich auch die Daten in Deutschland befinden
  - Nutzen Sie keine ausländischen Cloud-Services; E-Mail- und Cloud-Provider, die in Deutschland ansässig sind, unterliegen deutschem Datenschutzrecht
- **Technisch gestützte Datenaskese**
- **Technische Infrastrukturmaßnahmen**
  - DMZ- und Hochsicherheitsnetzkonzepte (inkl. Firewalls, IPS usw.) mit entsprechendem Logging/Alerting
  - Starke Authentisierung (2-Faktor-Authentisierung) und sichere Remote-Zugänge (z. B. SSL-VPNs)
  - Monitoring des aktuellen Sicherheitsstands mittels Schwachstellenscannern
  - Aktuelles Asset- und Patch-/Update-Management
  - Data Loss/Leakage Prevention (DLP) – Schutz vor Weitergabe sensibler Daten

Empfohlene Maßnahmen

Höchste Schutzstufe

Der **wirksamste Schutz** gegen Bedrohungen ist ein im Unternehmen etabliertes Managementsystem für Informationssicherheit. Damit können die drei Grundpfeiler der Informationssicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – dauerhaft aufrechterhalten werden.

Durch die Einführung und den Betrieb eines Informationssicherheits-Managementsystems (ISMS) werden alle wesentlichen Maßnahmen der zugrunde liegenden Schutzstufen abgedeckt. Zu empfehlen ist dabei die Einführung eines ISMS nach ISO/IEC 27000.

Mit dem international anerkannten Standard können Organisationen aller Branchen ihr Informationssicherheits-Managementsystem (ISMS), also ihre Prozesse und Maßnahmen zur Gewährleistung der Informationssicherheit, nach ISO/IEC 27001 zertifizieren lassen. So können Sie sicher sein, dass sämtliche notwendigen Maßnahmen und Aktivitäten zur Gewährleistung der Informationssicherheit in Ihrem Unternehmen professionell umgesetzt sind.

Unsere Empfehlung

Sicherheit gibt es nicht von der Stange. Sicherheitslösungen sind maßgeschneidert.

Wir unterstützen Sie gerne bei der Konzeption und Umsetzung der für Ihr Unternehmen und Ihre Anforderungen erforderlichen Sicherheitsmaßnahmen. Sprechen Sie uns an!

Ihr Service für Information und Technologie

Ihre Vorteile

- Aufbau eines ganzheitlichen, optimal an Ihren Geschäftsprozessen orientierten Sicherheitsmanagements
- Risiken werden sichtbar und minimiert
- Herstellerneutrale Beratung für eine optimale Gesamtlösung
- Einsatz modernster Sicherheitsmethoden und -technologien für höchstmöglichen Schutz

Warum IS4IT?

Der Geschäftsbereich Security der IS4IT ist seit Jahren erfolgreich am Markt etabliert. Wir unterstützen Sie umfassend auf Basis unserer langjährigen Erfahrungen und umfangreichen Kenntnisse. Wir erarbeiten individuell auf Ihre Anforderungen zugeschnittene Lösungen, die nicht nur zuverlässig sind, sondern auch einen deutlichen Mehrwert bieten und dazu kostengünstig zu betreiben sind. Gerne übernehmen wir auch den Support und Betrieb Ihrer Umgebung und bieten hierzu flexible Managed-Service-Konzepte.

Unser oberstes Ziel ist die angemessene Sicherung Ihrer Unternehmenswerte.

IS4IT und unsere Mitarbeiter verfügen über ein breites Know-how-Portfolio, das durch zahlreiche produkt- und herstellerunabhängige Zertifizierungen untermauert wird. Namhafte Kunden aller Branchen setzen auf unsere Expertise.

- ISO 27000
- ITIL
- Certified Information Security Auditor nach ISACA
- Certified Information Security Manager nach ISACA
- Berufsverband der EDV-Revisoren
- CISSP – Certified Information System Security Professional nach ISC2

IS4IT sorgt für Sicherheit – Vertrauen auch Sie auf uns als Sicherheitspartner!

Grünwalder Weg 28 b 82041 Oberhaching Telefon: +49 89 6389848-0 Telefax: +49 89 6389848-9 info@is4it.de www.is4it.de