


## Verfassungsschutz warnt vor zunehmender Wirtschaftsspionage

 [http://www.securitymanager.de/magazin/artikel\\_2264\\_wirtschaftsspionage.html](http://www.securitymanager.de/magazin/artikel_2264_wirtschaftsspionage.html)

Wirtschaftsspionage wird zunehmend zu einer wachsenden Herausforderung: Nicht nur die ständig zunehmenden Internet-Angriffe, z. B. aus China, Russland oder anderen Ländern, mit denen Daten, Forschungsmaterial, Innovationen und wissenschaftliche Studien ausgespäht werden, liegen dabei im Fokus der Verfassungsschützer, sondern auch reale Spione – seien es spionierenden Praktikanten oder als Firmenbesucher getarnte Späher aus dem Ausland.

Nach Aussage des NRW-Verfassungsschutzes von Sommer fällt die Bilanz besonders für Unternehmen ernüchternd aus, die der Auffassung sind, dass sie von Spionage verschont blieben. Ohne konkrete Zahlen zu liefern, wurde nach aktuellen Opfer- und Dunkelfeldstudien bereits ein großer Teil aller Firmen ausspioniert, kleine und mittelständische ebenso wie große Konzerne. Der Bereich der IT-Sicherheit spielt eine immer wichtigere Rolle – egal wie groß das Unternehmen ist. Seit Jahren bemühen sich die Verfassungsschützer, Unternehmen für existenzbedrohende Spionageangriffe zu sensibilisieren: Die Gefahr für ein Unternehmen, Opfer von Wirtschaftsspionage zu werden, steigt ständig. Alarmierend sei, dass viele Unternehmen sich gar nicht oder nur unzureichend schützen.

### Wirtschaft wie auch Politik ist von Spionage gleichermaßen betroffen

Nach einer Publikation des Verfassungsschutzes von Ende 2008 zum Thema Spionage ist auch Deutschland „bedeutendes Aufklärungsziel“ für die „Nachrichtendienste einer Reihe von Staaten“ – wegen seiner wichtigen Rolle in EU und NATO, aber auch aufgrund seiner geopolitischen Lage. Eine zunehmende Bedeutung gewinnen auch hier „internetbasierte Angriffe auf Computersysteme“ von Regierungsstellen und Innovationstreibern aus der Wirtschaft.

Der Bundesverfassungsschutz spricht auch vor dem Hintergrund der Enttarnung eines international operierenden Spionagenetzes im Internet von einer Bestätigung der bisherigen Einschätzung: Das sogenannte „Ghostnet“ hatte bei bis zu 30 Prozent der infizierten Rechner „hochrangige Ziele“ wie Regierungsstellen, Außenministerien, Medien und internationale Organisationen im Visier. In Deutschland stehen die Botschaften Zyperns, Indiens und Portugals mit auf der Liste. In weniger als zwei Jahren wurden dabei mindestens 1295 Rechner in 103 Ländern ausgespäht und zahllose Dokumente gestohlen.

### IT-Bedrohungen nicht isoliert betrachten

Die mittlerweile hochspezialisierten Methoden von Computerkriminellen zeigen erneut, wie bedeutsam Vorkehrungen zur Steigerung des Sicherheitsniveaus für ein Unternehmen und Behörden sind – tragen sicherheitstechnische Vorsorgemaßnahmen doch direkt dazu bei, die Wertschöpfung abzusichern. Was jedoch ein effektives Sicherheitsmanagement ausmacht, ist der ganzheitliche Ansatz: Nicht nur die IT-Prozesse selbst, sondern auch infrastrukturelle, personelle und organisatorische Aspekte der gesamten IT-Umgebung müssen berücksichtigt werden.

Welchen Zweck haben beispielsweise Firewalls zur Kontrolle des Netzwerkverkehrs, wenn Praktikanten und Besucher unbedacht Zugang zu verschiedensten Gebäuden und Systemen erhalten? Was nützt ein gesichertes Rechenzentrum, wenn weder Kommunikation, Notebooks noch mobile Wechseldatenträger wie USB-Sticks verschlüsselt sind? Welchen Stellenwert besitzt das Patch-Management, wenn dieses nicht angemessen betreut und somit lückenhaft durchgeführt wird? Hierbei sei an den Conficker-Wurm erinnert, der in der jüngsten Vergangenheit zahlreiche Netzwerke von Kommunen, Krankenhäuser und militärischen Einrichtungen lahmlegte.

Um sich effektiv vor Wirtschaftsspionage zu schützen, muss Informationssicherheit im weiteren Sinne verstanden werden – als ganzheitlicher Prozess. Die Erfahrung zeigt, dass es ohne ein funktionierendes Informationssicherheitsmanagement praktisch nicht möglich ist, ein durchgängiges und angemessenes Sicherheitsniveau zu erzielen und zu erhalten.

"Für ein nachhaltiges Managementsystem für Informationssicherheit (ISMS) empfehlen wir eine Orientierung an international anerkannten Standards, wie beispielsweise der ISO 27001 auf der Basis von BSI IT-Grundschutz", berichtet Vincenzo Abate, Partner der buw consulting GmbH.

### Jedes Unternehmen sollte seine Geschäftsprozesse sicher gestalten

Damit das angestrebte, und den Unternehmensbedürfnissen angemessene Informationssicherheitsniveau erreicht wird, müssen bestehende Schwachstellen in Form eines ganzheitlichen Ansatzes ermittelt und alle erforderlichen Maßnahmen identifiziert werden. Vor allem müssen alle Maßnahmen, die im Sicherheitskonzept vorgesehen sind, auch konsequent anhand eines Realisierungsplans umgesetzt werden.

"Viele unserer Kunden haben mit dem buw-ITK-Security-Check diesen ersten Schritt methodisch eingeleitet: Innerhalb weniger Tage erfolgt eine Analyse der angewandten IT-Sicherheitsmaßnahmen auf Grundlage des international anerkannten Standards ISO/IEC 27001 auf Basis von BSI IT-Grundschutz" erläutert Vincenzo Abate.

Bei der Erstbetrachtung empfiehlt sich grundsätzlich eine Prüfung der kritischen Geschäftsprozesse, um darauf aufbauend den Grundstein für ein strategisches Sicherheitsmanagement zu legen. Oberstes Gebot ist hierbei eine ganzheitliche Methodik, die nicht nur die IT-Prozesse selbst, sondern gleichermaßen infrastrukturelle, personelle und organisatorische

Aspekte in die Analyse einbezieht.

Das Ergebnis der Betrachtung sollte einen schnellen Überblick zum sicherheitstechnischen Status Quo ermöglichen, konkrete Handlungsempfehlungen zur Steigerung des Sicherheitsniveaus liefern und somit auch gegenüber Kunden, Wirtschaftsprüfern, Kreditgebern und Versicherungen als Nachweis gelebter IT-Sicherheit dienen.

*Erschienen: 10/2009*

*Autor: Andreas G. Weyert*



Andreas G. Weyert ist lizenzierter BSI IT-Grundschutz-Auditor und Security Consultant bei der buw consulting.