



ANDREAS WISLER, GESCHÄFTSLEITER VON GO OUT PRODUCTION

«Industriespionage auch in der Schweiz»

Die Werte der Industriespionage, begünstigt durch mangelnde IT-Sicherheit, haben in der Schweiz erschreckend zugenommen.

Foto: Bilderbox.de

Am 7. März fand zum siebten Mal der SwissSecurityDay, der nationale Tag der Computer-Sicherheit, statt. Ziel war es, die Bevölkerung für den sicheren Umgang etwa beim E-Banking und in Sozialen Netzwerken zu sensibilisieren. Im Interview zeigt Andreas Wisler die Handlungsmöglichkeiten von Unternehmen diesbezüglich auf.

INTERVIEW MARTINA DALLA VECCHIA

Andreas Wisler, in den Medien wird fast wöchentlich von den Risiken im Internet und den Angriffen auf Unternehmensnetzwerke berichtet. Braucht es da noch einen SwissSecurityDay?

Andreas Wisler: Die Gefahren und Risiken haben tatsächlich massiv zugenommen. Auch das organisierte Verbrechen hat den Weg ins Internet gefunden. Dabei geraten vor allem die Privatpersonen ins Visier. Daher versucht der SwissSecurityDay auf die Gefahren aufmerksam zu machen und Lösungsmöglichkeiten zu zeigen.

Mit welchen Sicherheitsthemen sollten sich Unternehmen heute beschäftigen? Was sind Ihre Empfehlungen?

Die Bundesstelle MELANI (Melde- und Analysestelle Informationssicherung) zeigt, dass Industriespionage in der Schweiz erschreckende Werte angenommen hat. Daher gilt es, die eigene IT-Umgebung immer auf dem aktuellsten Stand zu halten, die Firewall konsequent zu warten, sich mit einem soliden Backup-Konzept inklusive Notfallplanung auf einen Zwischenfall vorzubereiten und mittels IT-Strategie, IT-Konzept und Weisungen für Mitarbeiterinnen und Mitarbeiter klare «Spielregeln» aufzustellen.

In jedem Unternehmen sollte eine Person für die Sicherheit der Daten und der Infrastruktur verantwortlich sein. Häufig ist dies der Finanzchef oder der IT-Leiter. Sollte man zusätzlich eine externe Firma mit einem Sicherheits-Check beauftragen?

Die heutige IT ist geprägt von Zeit- und Kostendruck. Zudem ändern sich Hard- und Software sowie deren Möglichkeiten sehr schnell. Da ist es möglich, dass nicht alles umgesetzt oder konfiguriert wird, was möglich ist. Ein externer Sicherheits-Check soll einem Unternehmen helfen, Schwachstellen und Möglichkeiten zur Behebung zu kennen.

ZUR PERSON

Andreas Wisler war nach seinem Informationstechnologiestudium als IT-Sicherheitsspezialist bei der Swisscom AG tätig. Diverse Fortbildungen im IT-Sicherheitsbereich, wie z.B. CISSP, legen ein breites Fundament. Seit 1997 ist er Mitglied der Geschäftsleitung der GO OUT Production GmbH, welche sich durch IT-Security Audits, Penetration Tests und Beratungen mit der ganzheitlichen Betrachtung der IT-Sicherheit auseinandersetzt. Er publiziert regelmäßig Fachberichte in KMU- und technischen Zeitschriften und ist Dozent im CAS Information Security & Risk Management.

Welchen Nutzen haben Unternehmen von einem solchen Sicherheits-Check?

In sehr kurzer Zeit und mit wenig eigenem finanziellen sowie zeitlichen Aufwand kann die IT-Sicherheit erhöht werden. Es geht nicht darum, den bösen Finger zu zeigen, sondern die IT-Umgebung ganzheitlich zu untersuchen und zu verbessern. Eine hersteller- und produktenechte Drittmeinung kann hier viele wertvolle Tipps liefern.

Was sind die häufigsten Manko, die Sie bei derartigen Prüfungen vorfinden?

Im organisatorischen Bereich fehlen die verbindlichen Vorgaben an die IT. Was ist der Zweck? Welche Mittel werden verwendet? Wie wird die IT-Sicherheit erhöht? Welche Anforderungen an die Verfügbarkeit stellt das Business an die IT? Was geschieht bei einem Zwischenfall? Wie ist der Umgang mit den IT-Mitteln? Dies sind nur einige Fragen, die geklärt werden müssen. Anhand der Antworten kann die IT die entsprechenden Umsetzungen tätigen. Im technischen Bereich sind es vor allem Systeme, bzw. die darauf installierten Drittapplikationen, die oft nicht aktuell sind. Dies stellt leider eine gravierende Bedrohung für ein Unternehmen dar, wie auch schon namhafte Unternehmen erfahren mussten. Daher gilt auch hier: Die IT-Sicherheit muss stetig kontrolliert und erhöht werden, um nicht Gefahr durch einen Schaden zu nehmen.

DIE AUTORIN

 Prof. Martina Dalla Vecchia ist Dozentin für E-Business und Online-Marketing am Institut für Wirtschaftsinformatik der Fachhochschule Nordwestschweiz (FHNW). www.fhnw.ch/wirtschaft/weiterbildung/cas-information-security-management-cissp; www.swiss-securityday.ch.

**ANALYSIEREN,
OPTIMIEREN,
MANAGEN.**
MIT KYOCERA MDS VERSTECKTE
OUTPUTKOSTEN ERKENNEN
UND DRASTISCH REDUZIEREN.

Mit KYOCERA Managed Document Services (MDS) können Sie Ihre Outputkosten um bis zu 30%* senken. Und für einen maximalen Effekt kombinieren Sie KYOCERA MDS mit unserer höchst langlebigen, zuverlässigen und produktiven TASKalfa 5550ci-Serie.

Source: *All Associates Group

TASKalfa 5550ci

- Bis zu 50 Seiten pro Minute in Farbe und 55 Seiten in s/w
- 2 GB Seitenspeicher und 320 GB Festplatte
- Software-Entwicklungsplattform HyPAS™
- Exzellente Farbqualität
- Standardmässiger Netzwerkdruck und -scan in Farbe

KYOCERA. RECHNEN SIE MIT UNS.

KYOCERA Document Solutions Europe B.V.,
Niederlassung Schweiz – Tel. +41 (0)44 908 49 49 –
www.kyoceradocumentsolutions.ch
KYOCERA Document Solutions Inc. –
www.kyoceradocumentsolutions.com

KYOCERA
Document Solutions