

Blickpunkt:KMU Verlag GmbH
4052 Basel
061/ 205 34 24
www.blickpunktkm.ch

Medienart: Print
Medientyp: Fachpresse
Auflage: 13'500
Erscheinungsweise: 6x jährlich

Themen-Nr.: 663.26
Abo-Nr.: 663026
Seite: 36
Fläche: 43'144 mm²

SWISS SECURITY DAY

«Speziell Schweizer KMU stellen interessante Ausspähungsziele dar!»

Am 10. März 2010 findet der Swiss Security Day statt. Zum mittlerweile fünften Mal will dieser Aktionstag Privatpersonen und KMU für das Thema Computersicherheit sensibilisieren. Im Interview mit Blickpunkt:KMU erklärt Wolfgang Sidler, Präsident des veranstaltenden Vereins InfoSurance, welche Themen in diesem Jahr im Fokus stehen – und worauf gerade KMU besonders achten sollten.

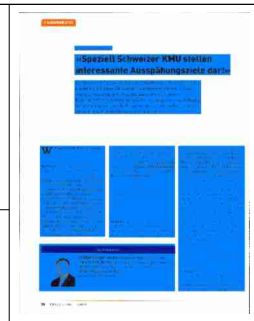
Wo liegen für KMU Ihrer Erfahrung nach die grössten Gefahren im Bereich der IT-Sicherheit?

W. Sidler: Der Umgang mit dem Thema Wirtschaftsspionage und mit vertraulichen Firmendaten ist verbesserungsfähig. So werden Notebooks mit zum Teil sensiblen Firmendaten gestohlen oder gehen verloren. Ich empfehle, die Festplatte des Notebooks komplett zu verschlüsseln. Weiter sollte der Zugriff auf Daten je nach Funktion und Hierarchie der Mitarbeiter geregelt werden. E-Mails mit vertraulichen Inhalten sind zu verschlüsseln, ebenso Wireless-Netzwerke mit WPA oder WPA 2. Neben technischen kann aber auch mit organisatorischen Massnahmen die IT-Sicherheit erhöht werden. Diese kosten in der Regel nichts, bedingen aber eine konsequente Handhabung und Orientierung innerhalb des Betriebs. Denn häufig verursachen die Mitarbeiter zusätzliche IT-Kosten, indem sie sogenannte Freeware auf ihre Geschäftscomputer laden, was teure Virenangriffe, Programmabstürze und im schlimmsten Fall einen Totalausfall der IT zur Folge haben kann.

Man hört immer häufiger von Attacken, die gezielt auf ein bestimmtes Unternehmen verübt werden – im Gegensatz zu den eher wahllosen Angriffen, die

früher beispielsweise durch Phishing-Mails stattfanden. Gilt dieser Trend nur für die ganz grossen Unternehmen, oder müssen auch KMU vermehrt mit solchen Angriffen rechnen?

W. Sidler: Speziell unsere Schweizer KMU stellen wegen ihrer innovativen Forschungs- und Entwicklungsvorhaben und ihres Know-hows häufig interessante Ausspähungsziele dar. Besonders beliebt sind auch Messen, wie beispielsweise die CeBIT in Hannover. Hier sind Spione gezielt am Werk und greifen offen auf Informationen zu, die nicht selten in Joint Ventures münden. Dabei bedienen sich die Spione der Social Engineering Methode, um an die sensiblen Informationen zu kommen. Social Engineering ist ein Weg, um unberechtigten Zugang zu Informationen oder IT-Systemen durch «Aushorchen» zu erlangen. Dabei werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Meistens merkt das ausspionierte Unternehmen nichts – bis von seinem Produkt eine sehr gute Kopie auf dem Markt erscheint. Heute ist es für einen Angreifer leichter, mit Hilfe der Social Engineering Methode an Informationen zu kommen, als ihre Firewall hacken zu lassen. Internet-Kriminalität ist eine wachsende Branche, welche sich professionell organisiert hat.



Blickpunkt:KMU Verlag GmbH
4052 Basel
061/ 205 34 24
www.blickpunktkm.ch


Medienart: Print
Medientyp: Fachpresse
Auflage: 13'500
Erscheinungsweise: 6x jährlich

Themen-Nr.: 663.26
Abo-Nr.: 663026
Seite: 36
Fläche: 43'144 mm²

Gibt es KMU, die beispielsweise aufgrund Ihrer Infrastruktur oder Ihrer Branche besonders gefährdet sind?

W. Sidler: Speziell sind jene Unternehmen gefährdet, welche sehr vertrauliche Dokumente bearbeiten und speichern. Zum Beispiel Rechtsanwälte, Ärzte oder Treuhänder. Die Infrastruktur einer Firma mit

IM INTERVIEW



Wolfgang Sidler, Informationssicherheits-Spezialist, freier Coach, Berater und Autor, ist Präsident des Vereins InfoSurance sowie Gründer und Inhaber der Sidler Information Security GmbH.
www.sidler-security.ch

komplexen Maschinen ist ebenso abhängig von der Sicherheit, jedoch ist hier die Verfügbarkeit wichtiger als die Vertraulichkeit. Denn ein Ausfall einer komplexen Industriemaschine hat einen Produktionsausfall oder eine Lieferverzögerung zur Folge. Je nach Unternehmen ist also die Vertraulichkeit oder die Verfügbarkeit wichtiger zu werten. Sie als Unternehmer entscheiden, welche Werte Sie in Ihrem Betrieb mit welchen Sicherheitsmassnahmen schützen möchten. Auch Sie entscheiden, was Ihnen dieser Schutz «ert ist.

Wo liegt der Fokus des diesjährigen Swiss Security Day?

W. Sidler: Der Schwerpunkt des diesjährigen SwissSecurityDay steht unter dem Motto «Augen auf!». Wir möchten die Schweizer Bevölkerung auf die Gefahren im Internet aufmerksam machen. Es gelten generell unsere fünf Schritte für eine bessere Computer-Sicherheit: Sichern, Schützen, Überwachen, Vorbeugen, Aufpassen. Mehr dazu finden Sie auf der Website www.swisssecurityday.ch.

Welches sind die wichtigsten Aktionen am 10. März? Sind einige davon speziell auf KMU ausgerichtet?

W. Sidler: Da wir im Besonderen alle Gruppen der Schweizer Bevölkerung ansprechen, ist auch das KMU davon betroffen. Denn der grösste Teil der Bevölkerung arbeitet für ein Schweizer KMU. So unterstützen wir indirekt auch die KMU. Auf www.infosurance.ch bieten wir kostenlos unser erweitertes 10-Punkte Programm für eine bessere Sicherheit in einem KMU und weitere interessante Merkblätter zum Download an.

Herr Sidler, herzlichen Dank für das Gespräch. tw ♦

SWISS SECURITY DAY

Alle Informationen zum Swiss Security Day, Daten und Orte für Schulungen sowie Checklisten zum Herunterladen finden Sie auf www.swisssecurityday.ch