Der Mensch hebelt als Layer 8 teure Sicherheitssoftware aus

Der Mensch hebelt als Layer 8 teure Sicherheitssoftware aus

In vielen Unternehmen werden zum Teil hohe Summen für durchaus erforderliche Sicherheitssoftware investiert. Nichtsdestotrotz müssen immer wieder Sicherheitsvorfälle registriert werden, wodurch z. T. hochvertrauliche Informationen nach Außen dringen, was wiederum auch die Wettbewerbsfähigkeit gefährdet.
Neben den öffentlich sehr stark wahrgenommenen Hacking-Attacken werden unzählige Vorfälle in den Unternehmen verzeichnet, die weniger durch Kriminelle als vielmehr durch die eigenen Mitarbeiter verschuldet sind. So zeigte beispielsweise die neueste KES-Sicherheitsstudie, dass über 70 % der Sicherheitsvorfälle im Unternehmen durch die eigenen Mitarbeiter verschuldet werden. Die weitaus meisten sind jedoch keine bewussten oder mutwilligen Verstöße, sondern vielmehr Konsequenzen aus Unwissenheit oder fehlender Sensibilität.
Dies legt die Vermutung nahe, dass die Mitarbeiter - also die Nutzer, die in Technikerkreisen auch scherzhaft "Layer 8" genannt werden - im Rahmen der Sicherheitspolitik im Unternehmen vergessen werden.
Die Erfahrungen der UIMC decken sich hierbei mit den Ergebnissen der besagten KES-Studie, dass viele Mitarbeiter die Sicherheitsmaßnahmen umgehen, entweder weil sie sie nicht verstehen oder weil sie die Erfordernis einer bestimmten Maßnahme nicht erkennen. Hinzu kommt, dass sich viele Unternehmen durch die Sicherheitssoftware und -produkte in "falscher" Sicherheit wiegen. Hinzu kommt eine modernere Form der Gefahr: Die Mitarbeiter nutzen soziale Netzwerke und geben dadurch entweder Unternehmensinterna direkt preis, indem sie geheime Informationen auf Fotos von Arbeitsplätzen einsehbar machen, oder geben in "Plauderlaune" andere Interna indirekt einem relativ großen Empfängerkreis "versehentlich" bekannt.
Dies zeigt, dass nicht nur die Layer 1 bis 7 des OSI-Modells durch die IT-Abteilung "gehärtet" werden sollten, sondern auch die achte Schicht selbst. Dies kann einerseits durch klare Vorgaben im Rahmen eines Informationssicherheits-Managementsystems erreicht werden. Andererseits zeigt die Erfahrung der UIMC, dass ohne entsprechende Schulung und Sensibilisierung sowohl technische als auch organisatorische Sicherheitsmaßnahmen weit weniger effektiv sind. So muss der Mitarbeiter über Gefahren informiert, auf die Notwendigkeit von Maßnahmen hingewiesen und allgemein eine Aufmerksamkeit für das Thema Informationssicherheit geschaffen werden.
Dabei sollte eine solche Schulungsmaßnahme kein einmaliges Projekt darstellen, sondern vielmehr ein kontinuierlicher Prozess sein, in dem laufend auch aktuelle Themen aufgegriffen werden. Hierzu eignen sich insbesondere E-Learningplattformen, auf die einerseits dezentral zugegriffen werden und auf denen andererseits Inhalte kontinuierlich aktualisiert werden können, ohne großen Organisationsaufwand zu erzeugen. Innerhalb der Kurse können neben (rechtlichen) Grundlagen insbesondere praktische Themen diskutiert und Tipps zur Einhaltung gegeben werden. Die Möglichkeit, durch Tests das erlernte Wissen zu überprüfen, kann die Mitarbeiter zusätzlich motivieren.
Auch wenn der Frage, ob Sicherheitssoftware ohne Betrachtung von Layer 8 nutzlos ist, sicherlich nicht kommentarlos zugestimmt werden kann, so wird die Effektivität solcher Maßnahmen durch die Kompetenz und die Sensibilisierung der Mitarbeiter maßgeblich bestimmt.

Pressekontakt
UIMC Dr. Voßbein GmbH
 Co. KG
Dr. Jörn Voßbein
Nützenberger Straße 119
42115 Wuppertal
Tel.: 0202 / 265 74 - 0
Fax: 0202 / 265 74 - 19
E-Mail: consultants@uimc.de
Internet: www.uimc.de
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=528113" width="1" height="1">

Pressekontakt

UIMC

42115 Wuppertal

consultants@uimc.de

Firmenkontakt

UIMC

42115 Wuppertal

consultants@uimc.de

Die UIMC DR. VOSSBEIN GmbH & Co KG, gegründet 1997, hat die damals seit über 10 Jahren laufenden Beratungsgeschäfte der Partner und Gesellschafter Dr. Reinhard Voßbein, Professor für Wirtschaftsinformatik und Dr. Jörn Voßbein in einer Beratungsgesellschaft vereint. Seit 1999 ist Dr. Heiko Haaz, der schwerpunktmäßig den Datenschutz betreut, als dritter Partner zur UIMC gestoßen.Kerngebiete ihrer Arbeit sind die IT-Sicherheit und der Datenschutz. Sie kann beachtliche Referenzen von Institutionen aus einer Vielzahl von Wirtschaftszweigen sowie Behörden aufweisen und hat eine umfangreiche Projekt- und Betreuungserfahrung, auch international. Felder, auf denen ihre Erfahrungen branchenführend sind.Ihr Leistungsspektrum/Produktprogramm unterscheidet sich von dem anderer Beratungsunternehmen: Sie setzt ein toolgestütztes Analyse- und Konzeptionierungssystem mit einer wissensbasierten Expertensystem-Komponente in Form einer Shell ein, das ständig ausgebaut und ergänzt wird. Dieses ermöglicht die rationelle und kostengünstige Analyse betriebswirtschaftlicher sowie IT-sicherheits- und datenschutzspezifischer Kern- und Teilgebiete sowie die Berichterstattung und Konzeptionserstellung, womit Rationalisierungs- und Effizienzvorteile für ihre Kunden generiert werden. Im Verlaufe der Zeit wurden eine Vielzahl von individuellen Füllungen für diese Shell erarbeitet und in diese eingebracht. Firmenindividuelle Füllungen sind konzeptionell vorgesehen und auf der Basis der Struktur des Tools komplikationslos zu realisieren.Sie führt Workshops, Schulungen sowie Fortbildungsmaßnahmen auf den Sektoren IT-Sicherheit und Datenschutz mit ihrer Marke UIMCollege auch als Inhouse-Veranstaltungen durch.