UIMC: Ob Bundestag oder Wirtschaftsunternehmen ? Reicht ein Update der IT-Sicherheitstechnik aus?

UIMC: Ob Bundestag oder Wirtschaftsunternehmen - Reicht ein Update der IT-Sicherheitstechnik aus?

Aktuell wird das IT-System des Bundestags komplett neu aufgesetzt, um nach dem Hackerangriff die Sicherheitstechnik zu aktualisieren. Hierdurch soll der Stand der Sicherheit maßgeblich verbessert werden. Dr. Jörn Voßbein, mehrfach bestellter IT-Sicherheitsbeauftragter, weist aber darauf hin, dass dies nur ein Baustein zur Verbesserung der Sicherheit ist; vielmehr muss auch der Benutzer in die Überlegungen und Maßnahmen viel stärker einbezogen werden.
Nicht erst seit den Enthüllungen rund um die NSA oder dem Angriff auf das Netzwerk des Bundestages ist vielen (nicht nur großen) Unternehmen bewusst, dass sie sich um die Sicherheit der IT-Systeme und ihrer vertraulichen Daten kümmern müssen. Hierzu werden den IT-Abteilungen entsprechende Budgets für die Anschaffung und den Betrieb von Sicherheitssystemen zur Verfügung gestellt.
Doch wenn über IT-Sicherheit, Informationssicherheit oder auch über Datenschutz gesprochen wird, liegt der Hauptaugenmerk oftmals auf den Aktivitäten der IT-Abteilung. Es werden Firewalls, Virenscanner, Intrusion Detection Systeme oder Verschlüsselungsprogramme angeschafft und eingesetzt, so dass die IT-Systeme dadurch "gehärtet" werden. Dass es trotzdem immer wieder zu Virenbefall, Spionagefällen oder anderen Vorfällen kommt, ist aber insbesondere auch in einem Faktor begründet: dem Menschen bzw. dem User.
Trotz der technischen Aufrüstung müssen immer wieder Sicherheitsvorfälle registriert werden, wodurch z. T. hochvertrauliche Informationen nach Außen dringen, Systeme "lahmgelegt" oder Compliance-/Datenschutz-Probleme bekannt werden. Vertrauensverlust, Vertraulichkeitsverlust bei Betriebsgeheimnissen wie Produktionsverfahren oder Preiskalkulationen oder die Nicht-Verfügbarkeit von Systemen oder Daten: Durch solche Vorfälle ist die Wettbewerbsfähigkeit des Unternehmens gefährdet.
Doch woran liegt dies, wo doch soviel in die Sicherheit investiert wird? Grund hierfür sind nicht ausschließlich Hacker. So zeigen diverse Sicherheitsstudien, dass über zwei Drittel der Sicherheitsvorfälle im Unternehmen durch die eigenen Mitarbeiter verschuldet werden. Dabei handelt es sich oftmals nicht um bewusste oder mutwillige Verstöße. Vielmehr sind sie vielmehr die Konsequenz aus Unwissenheit oder fehlender Sensibilität der Mitarbeiter.
Die Erfahrungen der UIMC zeigen dabei, dass viele Mitarbeiter die Sicherheitsmaßnahmen umgehen, entweder weil sie sie nicht verstehen, den Sinn nicht erkennen oder von ihnen gar nicht erst wissen. Auch wiegen sich viele Mitarbeiter aufgrund der ausgefeilten Sicherheitstechnik in "falscher" Sicherheit, schließlich "kümmert sich ja eine ganze Abteilung um die IT-Sicherheit". Soziale Netzwerke, private Smartphones oder Cloud-Speicher-Dienste reißen indes weitere Löcher in die Sicherheitsarchitektur.
Doch sollte hierbei der User nicht als Täter oder "Feindbild" gesehen werden. Vielmehr sollte man ihn als Teil der Sicherheitsarchitektur sehen und auch diesen Bereich - analog zu den technischen Sicherheitsmaßnahmen - "härten".
Beginnen sollte man nach einer kurzen Risikoanalyse zunächst mit verbindlichen Regelungen, um Transparenz und einen Rahmen zu schaffen, in dem sich die Mitarbeiter sicher bewegen können. Danach sollten praxisorientierte Schulungen und Sensibilisierungsmaßnahmen gestartet werden. So muss der Mitarbeiter nicht nur auf die Richtlinien verpflichtet, sondern auch über die Gefahren informiert und auf die Notwendigkeit der Maßnahmen hingewiesen werden. Denkbar sind persönliche Schulungen, E-Learning-Plattformen und/oder Informationsmaterialien wie interne Newsletter, Blogs oder Flyer. Solche Maßnahmen sollten aber nicht als einmaliges Projekt, sondern vielmehr als ein kontinuierlicher Prozess verstanden werden, in dem laufend auch aktuelle Themen aufgegriffen werden.

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_=595641" 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.