UIMC: IT-Sicherheit beginnt beim Mitarbeiter

19.09.2018, 16:02 | IT, New Media & Software

Pressemitteilung von: *UIMC Dr. Voßbein GmbH & Co KG*

UIMC: Stets gut beraten

Ein digitaler Einbruch ist heute für viele Unternehmen mindestens so schwerwiegend wie ein herkömmlicher mit Dietrich und Brecheisen – wenn nicht sogar noch schlimmer. Er kann dazu führen, dass strengvertrauliche Daten in die falschen Hände geraten oder wichtige Daten nicht mehr zugänglich sind; aber auch der Imageschaden kann verheerend sein. Wer liest schon gerne über einen Geschäftspartner oder sein eigenes Unternehmen, dass sensible Kundendaten verlorengegangen oder sogar in kriminelle Hände gelangt sind. Kurz: Ein Hackerangriff kann das Renommee oder sogar die Existenz eines Unternehmens gefährden. Weil sich viele Unternehmer und Geschäftsführungen dieser Gefahr bewusst sind, wird seit Jahren viel in die digitale Sicherheit investiert. Milliarden Euro fließen in Firewalls, Virenscanner, Intrusion Detection Systeme oder Verschlüsselungsprogramme. Zeigen die eingesetzten Ressourcen den gewünschten Erfolg? „Zweifel sind angebracht, ob tatsächlich richtig und zielgerichtet investiert wird“, gibt sich IT-Sicherheitsfachmann Dr. Jörn Voßbein nachdenklich. Tatsächlich lassen Berichte über Sicherheitslücken nicht nach.

Diverse Sicherheitsstudien zeigen mit regelmäßiger Konstanz, 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 häufig die Konsequenz aus Unwissenheit oder fehlender Sensibilität der Mitarbeiter.

Beispiel 1: Ransomware. Vielen Mitarbeitern ist nicht bewusst, was sie mit einem unbedachten Anklicken eines Anhangs einer Mail anrichten. Zumal viele Mitarbeiter unter Stress stehen und die Mails mit schädlichen Inhalten häufig „gut gemacht“ sind. Auch wiegen sich viele Mitarbeiter aufgrund der ausgefeilten Sicherheitstechnik im Unternehmen in

„falscher“ Sicherheit, schließlich „kümmert sich ja eine ganze Abteilung um die IT-Sicherheit“.

Beispiel 2: Passwörter. In der heutigen digitalen Welt müssen sich die Nutzer zunehmend mehr Passwörter merken. Dies führt dazu, dass Passworte „synchronisiert“ werden, indem ein Nutzer für mehrere Dienste – ob privat oder dienstlich – das gleiche Passwort nutzt. Wenn, wie jüngst bei dem Chatportal knuddels.de geschehen, die Zugangsdaten durch Hacker entwendet werden, kann dies auch dazu führen, dass Unternehmenssysteme angegriffen werden, wenn der Nutzer beispielsweise eine dienstliche Mail-Adresse hinterlegt hat. Sie dient dem Hacker als Indiz dafür, wo der Nutzer ggf. das gleiche Passwort zum Zugang zu Systemen nutzt.

Dazu passt, dass die Erfahrungen der UIMC zeigen, dass viele Mitarbeiter die Sicherheitsmaßnahmen umgehen, entweder weil sie sie nicht verstehen, den Sinn nicht erkennen oder von ihnen gar nicht erst wissen. 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“. „Sensibilisieren, sensibilisieren und nochmals sensibilisieren für die IT-Sicherheit“, empfiehlt Dr. Voßbein eine langfristige und nachhaltige Konzeption zur Mitarbeiterschulung. „Der Datenschutz mit hohen gesetzlichen Anforderungen durch die Datenschutz-Grundverordnung wird hierdurch ebenfalls verbessert.“

Damit eine solche Schulungsmaßnahme kein einmaliges Projekt darstellt, sollte ein kontinuierlicher Prozess geschaffen weden, in dem laufend aktuelle Themen aufgegriffen werden. Hierzu eignen sich insbesondere E-Learning-Plattformen, auf die einerseits dezentral zugegriffen und auf denen andererseits Inhalte 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.

„Die Mitarbeiter sollten nicht nur auf Richtlinien verpflichtet werden, sondern auch über die Gefahren informiert und auf die Notwendigkeit der Maßnahmen hingewiesen werden“, schlägt Dr. Voßbein vor, um einen hohen Wirkungsgrad für die IT-Sicherheit des Unternehmens zu erreichen.

Portrait

Die UIMC ist eine gesellschaftergeführte mittelständische Unternehmensberatung mit den Kerngebieten Datenschutz und Informationssicherheit; im Datenschutz gehören wir zu den marktführenden Beraterhäusern. Wir bieten als Vollsortimenter sämtliche Unterstützungsmöglichkeiten der Analyse, Beratung, Umsetzung und Schulung/Sensibilisierung bis hin zum Komplett-Outsourcing des Beauftragten an.
Das Schwesterunternehmen UIMCert ist als sachverständige Prüfstelle für die Norm ISO/IEC 27001 von der DAkkS akkreditiert.

News-ID: 1019044 • Views: 625 (Stand: 07.08.2026)

Link zur Pressemitteilung: