UIMCommunic@tion
praxisnah.gut.informiert.

08/2023
Ausgabe für Deutschland

IT-Sicherheit in KMU stärken

Kleine Maßnahmen sorgen für frische Impulse und legen Fundament für Sicherheit

Die Cyber-Sicherheit ist für Unternehmen von größter Bedeutung. Die Zeiten sind turbulent und anspruchsvoll zugleich. Tatsächlich ist das Risiko in kleinen und mittleren Unternehmen (KMU) von einem Cyber-Vorfall betroffen zu werden nicht geringer als bei größeren Unternehmen. Auch wenn Hackerangriffe in ihrer Art und Durchführung stark variieren, lassen sich die Ziele und Motive der Cyberkriminellen eingrenzen. Ein begehrtes Ziel sind natürlich Daten, aber auch Systeme und Geräte liegen im Interesse der Hacker, letztlich mit dem Ziel daraus finanziellen Profit zu schlagen. Doch man kann es den Cyberkriminellen schwerer machen. „Das ist in vielen Unternehmen – gerade im Mittelstand – leichter gesagt als getan“, erklärt UIMC-Geschäftsführer Dr. Jörn Voßbein, der dabei auf seine in vielen Jahren erworbenen Erfahrungswerte zurückgreift. Problem Nummer eins ist, dass die Ressourcen für die IT-Sicherheit in KMU oftmals begrenzt sind. Die UIMC geht in einer fünfteiligen Reihe auf verschiedene Themen der Informationssicherheit ein. Heute startet sie mit Teil 1.

Zwei Fragen sollte sich jedes Unternehmen stellen, egal welche Größe es hat:

„Wer ist in meinem Unternehmen für das Thema Cybersicherheit verantwortlich?“ Die richtige Antwort in jedem Unternehmen: Die Geschäftsleitung. Aber das ist auch nur die halbe Wahrheit. Eindeutig ist, dass sich Cyber-Sicherheit nicht zum wegdelegieren eignet. Konkret: Es muss bei der Unternehmensleitung ein Bewusstsein für das Thema vorhanden sein; andernfalls muss dies geschaffen werden. Denn wer hier nachlässig ist, indem er das Thema nicht ernst nimmt und zu geringe Ressourcen bereitstellt, der gefährdet die Geschäftsgrundlagen und im schlimmsten Fall die Existenz des Unternehmens. Eine Hackerattacke kann weit mehr als nur das Image des Unternehmens gefährden. Auch wochenlange Produktionsausfälle mit allen damit verbundenen Konsequenzen sind möglich.

Die nächsten Teile dieser Reihe
beschäftigen sich mit folgenden Themen:

2. Fünf Handlungsfelder, die die Sicherheit verbessern
3. Gefahren durch Admins, Dienstreisen und Home Office
4. Informationssicherheit durch „menschliche“ Firewall verbessern
5. Lohnt ein Versicherungsschutz?

Neben dem Bewusstsein in der Unternehmensleitung müssen aber natürlich auch klare Zuständigkeiten für den Betrieb der IT-Systeme und die IT-Sicherheit festgelegt werden und den Zuständigen die notwendige Zeit eingeräumt werden. Auch: Wer ist wann zu beteiligen? Welche Handlungsempfehlungen sind anzuwenden?

Eine weitere Fragestellung lautet für jedes Unternehmen: „Wie gut kennen Sie Ihre IT-Systeme?“ Um sich zielgerichtet vor Cyberkriminellen schützen zu können, ist eine Inventarisierung der im Unternehmen verwendeten Hard- und Software, der bestehenden Datensätze und Verarbeitungsprozesse notwendige Voraussetzung. Dazu gehört auch eine Auflistung aller Zugriffsrechte sowie der IT-Verbindungen mit der Außenwelt. Es muss klar sein, was zu schützen ist. Die im Unternehmen verwendeten und verarbeiteten Daten sollten klassifiziert werden, um das

Fortsetzung auf der Rückseite

UIMC vor Ort:

Cybersecurity Day, 20.10.2023 in Saarbrücken
9. imh Jahrestagung Datenschutz, 24./25.10.2023 in Mauerbach bei Wien
DIGITAL FUTUREcongress, 08.11.2023 in Bochum

Sprechen Sie uns an; zum Teil haben wir vergünstigte Eintrittskarten.

UIMC Dr. Vossbein GmbH & Co KG, Otto-Hausmann-Ring 113, 42115 Wuppertal
Tel.: +49-202-946 7726 200, Fax: - 19, E-Mail: consultants@uimc.de, Internet: www.UIMC.de

Schutzniveau zielgerichtet anzupassen. Welche Daten sind unverzichtbar und bedürfen eines maximalen Schutzes? Welche Daten besitzen eventuell ein nicht ganz so hohes Schutzinteresse? Diese Fragen sind aus 2 Gründen wichtig: Kritische Daten und Systeme sind angemessen zu schützen; bei weniger wichtigen Daten/Systemen sollten nicht unnötig ressourcenverbrauchende Maßnahmen ergriffen werden.

„Die Beantwortung dieser Fragen bringt wichtige Impulse für die Sicherheit des eigenen Unternehmens. Sie bilden die Grundlagen für eigene zielgerichtete Anstrengungen in diesem Bereich und bieten den Einstieg in eine pragmatische Sicherheits-Organisation bzw. ein praktikables Informationssicherheits-Managementsystem“, unterstreicht UIMC-Geschäftsführer Dr. Jörn Voßbein.

Wussten Sie schon?

Im eCollege finden Sie unter FAQ den Bereich „FAQ und Wissenswertes“. Hierin haben wir viele nützliche Informationen hinterlegt, wie zum Beispiel:

- Typische Fragen aus unserem Beratungsgeschäft
- Praxishilfen wie bspw.
  - Ablauf eines Outsourcing-Prozesses
  - Umgang mit Cookies
  - Einführung neuer IT-Systeme
- Vorträge (Präsentation und zum Teil Videos)
- Tipps und Tricks im Datenschutz für Fachbereiche sowie
- weitere nützliche Informationen und ein Glossar.

Dies ist kostenfrei für alle User unserer E-Learning-Plattform: http://faq.uimcollege.de

Sie haben noch keinen eCollege-Zugang?
Dann kommen Sie gerne auf uns zu!

Neues Schweizer Datenschutzgesetz ab 01.09.2023

Im September 2020 hatte der Gesetzgebungsprozess in der Schweiz (endlich) einen Abschluss gefunden: Das Parlament stimmte der Revision des Schweizer Datenschutzgesetzes zu, welches nun in Kraft tritt.

Mehr unter www.uimc.ch

Spruch des Monats: September

Man könnte auch sagen „Wer nicht wagt, der nicht gewinnt“. Doch dies kann in vielen Bereichen durchaus große Konsequenzen haben. Daher ist es sehr wichtig zu wissen, welche Risiken bestehen.

Was diese Redewendung bedeutet, was es übertragen auf Ihr Unternehmen heißt und welches „Goodie“ wir diesen Monat für Sie vorbereitet haben, finden Sie unter unter

www.uimc.de/kalendersprueche

Aktuelles im Online-Formular-Center

Um über Neuerungen zeitnah informiert zu werden, können Sie unser News-Forum abonnieren und erhalten daraufhin eine E-Mail, sofern Sie einen personalisierten Account haben.

www.uimcollege.de