IT Security in der Praxis

33 % der Unternehmen in Deutschland sind von Cybersicherheitsvorfällen betroffen

In Zeiten von Cloud, Containering, Big Data und Digitalisierung bleibt IT-Sicherheit für viele ein brandaktuelles Thema. Unternehmen werden immer öfter neuen Cyber-Risiken ausgesetzt. Laut einer Cyber-Sicherheitsumfrage (1) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) waren im Jahr 2018 ca. 33 % der Unternehmen und Institutionen verschiedener Größen in Deutschland von Cybersicherheitsvorfällen betroffen – Tendenz weiter steigend. In jedem zweiten Fall waren die Angriffe erfolgreich und haben dem Angreifer Zugang zu IT-Systemen ermöglicht. Dadurch konnten Funktionsweisen beeinflusst und Internetauftritte manipuliert werden. Als häufigste Folge der Cyberangriffe waren Betriebsausfälle oder -störungen zu verzeichnen. Und das kann schnell teuer werden.

„Je schneller, desto besser"

Patrick Ben Koetter, eine Koryphäe auf seinem Gebiet, erklärte anhand zahlreicher Beispiele, warum die IT-Sicherheit auf keinen Fall vernachlässigt werden sollte. Wann ist der beste Zeitraum für ein Unternehmen sich das Thema auf die Agenda zu schreiben und mit einem IT-Auditor zu sprechen? „Je schneller, desto besser", rät Patrick, denn die Folgen der Cyberangriffe zu beseitigen ist meistens viel teurer als rechtzeitiges Einführen und Beachten einer soliden IT-Sicherheit von Anfang an. Im Anschluss stellte Patrick die „sichere Email" in Unternehmen anhand von DANE vor. DNS-based Authentication of Named Entities (DANE) ist ein Netzwerkprotokoll zur Absicherung des Datenverkehrs. Durch die Verbreitung der Transportwegverschlüsselung SSL/TLS können die verwendeten Zertifikate nicht unbemerkt ausgewechselt werden und dadurch wird die Sicherheit beim verschlüsselten Transport von Emails und beim Zugriff auf Webseiten erhöht.

Wie weit darf die IT-Security gehen und welche ethischen Grundwerte sollten bei der Schaffung von Cybersecurity eine Rolle spielen? IT-Sicherheit ist ein Prozess und es ist wichtig angemessen auf einen Fall zu reagieren. Was passiert im Falle von CEO-Fraud? Das waren einige wichtige Punkte der Diskussion. Mit realistischen Beispielen wurde auf Folgen und Risiken hingewiesen.
IT-Security ist eine Haltung, ein ganzheitlicher Ansatz und auf keinen Fall allein eine Aufgabe der IT-Abteilung.
Um IT-Sicherheit effektiv zu verbessern muss umgedacht werden. Auch Anwender sollten in die Pflicht genommen werden, denn die Erkenntnis, dass IT-Sicherheit einen immer größeren Stellenwert in der modernen Geschäftswelt einnimmt, muss sich unternehmensweit durchsetzen. Jedem sollte klar sein, dass es für ein Unternehmen große Verluste bedeutet, wenn durch Malware Geschäftsgeheimnisse gestohlen werden oder Betriebsausfälle drohen. IT-Security braucht Zusammenarbeit aber auch kontinuierliches Bewusstsein für potenzielle Risiken. Monitoring spielt hier eine ebenso wichtige Rolle und sollte nicht außer Acht gelassen werden – ebenso wie die Berücksichtigung von Sicherheitsmechanismen bei der Implementierung von Lösungen. Kontrolle schafft Sicherheit, damit die Angriffsfläche so gering wie möglich gehalten werden kann.

Was können Unternehmen proaktiv für ihre Sicherheit tun?

Neben der technischen Absicherung, ist die methodische Herangehensweise und eine umfassende Dokumentation wichtig. Die Einführung eines Information Security Management System (ISMS) unterstützt nicht nur bei Auditierungen nach ISO 27001 oder IT-Grundschutz, sondern hilft Unternehmen geeignete technisch-organisatorische Maßnahmen zu finden, um Sicherheit im Unternehmen herzustellen. Beginnend mit einer Einführung in die Methodik und der Rechte- und Rollenkonzepte, bis hin zu den Gefährdungen sowie entsprechenden Maßnahmen (wie Notfallvorsorge) und Hilfsmitteln für die Umsetzung anhand von zahlreichen Beispielen, bieten IT-Grundschutz-Kataloge solide Leitlinien für Datensicherheit.

becon *unterstützt Sie ganzheitlich rund um Themen der Informationssicherheit. Von der technischen Absicherung bis hin zur umfassenden Schwachstellenanalyse, dem Aufbau eines ISMS auf Basis von i-doit und der Auditvorbereitung mit zertifizierten Experten. Sprechen Sie uns an oder nutzen Sie unseren Callback-Service. Wir unterstützen Sie gern.*

(1) https://bit.ly/2Mc8ANC

Kontakt:

becon GmbH
Hauptstraße 8b
82008 Unterhaching

T.: +49 89 608668-0
info@becon.de

www.becon.de
www.OpenCelium.io