Studie: IT-Sicherheit am Mittleren Niederrhein 2019

© stockpics / Adobe Stock

Ziele der Studie

Das Ziel dieser Studie ist es, die IT-Sicherheit der kleinen und mittleren Unternehmen (KMU) im IHK-Bezirk Mittlerer Niederrhein systematisch zu erfassen und zu bewerten. Dabei stehen der Umsetzungsstand, der Bedarf und weitere Einflussgrößen der IT-Sicherheit im Vordergrund der Untersuchung. Die Auswertung unserer Untersuchung soll es den Entscheidern in den Unternehmen ermöglichen, ihr eigenes IT-Sicherheitsniveau mit anderen Unternehmen zu vergleichen. Außerdem sollen sie dazu angeregt werden, die Bedeutung der untersuchten Sicherheitsmaßnahmen für ihr Unternehmen zu bewerten, um möglicherweise passende Maßnahmen in ihrem Unternehmen umsetzen zu können.

Ergebnisse

Unsere IT-Sicherheitsstudie gibt Ihnen Einblicke in den aktuellen IT-Sicherheitsstand von KMU am Mittleren Niederrhein. Die Ergebnisse sind in die folgenden Kategorien unterteilt:

- Strukturdaten,
- Infrastruktur,
- Sicherheitskonzept,
- IT-Sicherheitsbeauftragter,
- Verschlüsselung,
- Mobilgeräte,
- Mitarbeitersensibilisierung,
- Datensicherung,
- Notfallbehandlung und
- Datenschutz.

Hier können Sie sich die gesamte Studie mit allen Ergebnissen als PDF herunterladen.

Kernaussagen der Studie

Die Ergebnisse der Befragung zeigen, dass sich Unternehmen am Mittleren Niederrhein der Notwendigkeit von IT-Sicherheitsmaßnahmen bewusst sind. Ebenso bewusst sind sie sich

der steigenden Bedrohung und Zunahme der Risiken durch IT-Sicherheitsvorfälle. Deshalb besitzt die Informationssicherheit vielfach einen hohen bis sehr hohen Stellenwert für KMU.

Kernaussagen– grafisch aufbereitet für den schnellen Überblick– liefert Ihnen unsere Grafik zur Studie.

Verfügbarkeit und Funktionalität von IT-Systemen und Daten sind gesichert – andere Bereiche werden dagegen vernachlässigt

Unternehmen in der Region sind in einigen Bereichen, beispielsweise bei der Datensicherung, dem Datenschutz und der Infrastruktur, bereits gut aufgestellt und haben viele Maßnahmen umgesetzt. Die umgesetzten Sicherheitsmaßnahmen schützen häufig die Verfügbarkeit und Funktionalität von IT-Systemen und Daten. Allerdings sollten sich Unternehmen nicht nur auf die reine Verfügbarkeit ihrer Systeme konzentrieren, sondern auch Aspekte wie Integrität, Vertraulichkeit und Authentizität nicht vernachlässigen. Diese und andere Bereichen bieten ungenutzte Potenzialeund tragen zu einer Verbesserung des IT-Sicherheitsniveaus bei.

Vor allem kleine Unternehmen haben Probleme bei der Einführung und Etablierung von Schutzmaßnahmen

Die genauere Betrachtung der bereits etablierten IT-Sicherheitsmaßnahmen zeigt eine nicht unerhebliche Diskrepanz zwischen unterschiedlich großen Unternehmen auf. Auch wenn das keine regionale Besonderheit, sondern auch überregional zu beobachten ist, verdeutlicht diese Diskrepanz die Probleme, die gerade kleine Unternehmen bei der Einführung und Etablierungentsprechender Schutzmaßnahmen haben. Die Erhebung zeigt, dass die größten Hemmnisse bei der Verbesserung des IT-Sicherheitsniveaus

- ein zu großes und undurchsichtiges Angebot,
- zu hohe Investitionskosten und
- ein mangelndes Sicherheitsbewusstsein der Mitarbeiter

sind.

Unternehmen brauchen mehr Informationen und Standards und müssen ihre Mitarbeiter für das Thema sensibilisieren

Unternehmen sollten nicht nur wie bisher für das Thema IT- und Informationssicherheit sensibilisiert, sondern auch über aktuelle Vorgehensweisen und Standards wie den BSI-Grundschutz oder die ISO27000er-Reihe informiert werden. So können ihnen die Risiken, der Nutzen und konkrete Kosten näher gebracht werden. Die Unternehmen können sie dann in ein Verhältnis setzen und die Etablierung entsprechender Schutzmaßnahmen wirtschaftlich betrachten.

Die Unternehmen selbst sollten dazu bereit sein, in ihre Mitarbeiter zu investieren und sie für Themen der IT- und Informationssicherheit zu sensibilisieren. Insbesondere große und mittlere KMU gaben an, dass die Mitarbeiter die Hauptursache möglicher IT-Problemesind und deren Schulung die sinnvollste Maßnahme zur Verbesserung des IT-Sicherheitsniveausist. Maßnahmen für eine solche Sensibilisierung können zum Beispiel Informationsveranstaltungenund Schulungsangebote externer Anbieter sowie frei zugängliche Informationendurch Quellen wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) sein.

Fazit

Fest steht: Es gibt einen Unterschied zwischen dem IT-Sicherheitsniveau kleiner und mittlerer Unternehmen. Das war zu erwarten. Denn vor allem kleine Betriebe haben oft nicht das nötige Fachwissen und Geld, um sich intensiv mit dem Thema IT und Informationssicherheit zu beschäftigen. Dennoch sollten sich Unternehmen über aktuelle Themen und Neuigkeiten aus diesem Bereich informieren, um sich entsprechendschützen zu können. Wenn Mitarbeiter mit sensiblen Firmendaten arbeiten, sollten sie entsprechend für die Sicherheit dieser Daten geschult werden.

Unternehmen sollten dasThema IT-Sicherheit zielgerichtet angehen, um so relevante und essenzielle Sicherheitsmaßnahmen bestimmen zu können. Wenn der Einsatz von IT-Sicherheitsmaßnahmen konzeptionellangegangen, geplant und kontrolliert wird und Mitarbeiter entsprechend geschult und sensibilisiertwerden, können Unternehmen ihr IT-Sicherheitsniveau auch mit überschaubaren Kostenverbessern und IT-Sicherheitsvorfällen vorbeugen. Da Unternehmen ihre Angestellten als eineder Hauptursachen möglicher IT-Probleme sehen, sollte der Fokus auf deren Sensibilisierunggelegt werden, um so eine nachhaltige IT-Sicherheitskultur etablieren zu können.

Downloads

- Auswertung ITS-Umfrage
- Poster IHK-Studie mit QR-Codes

Ansprechpartner

Tanja Neumann
Telefon: +49 2161 241-140
Telefax: +49 2151 635-44140
E-Mail: neumann@mittlerer-niederrhein.ihk.de
Bismarckstraße 109
41061 Mönchengladbach

Dokument-Infos

Webcode: 21279
Ausdrucksdatum: 16.09.2019