Mittelstand 4.0 Kompetenzzentrum Stuttgart #digitalinBW

Sechs Thesen zur IT-Sicherheit in KMU

-Arbeitspapier der AG IT-Sicherheit in der Initiative Mittelstand 4.0-

Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) umfasst die IT-Sicherheit an erster Stelle den Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Da das mittelständische Wirtschaften verstärkt auf Informationen und Prozessen aufbaut, die digital verarbeitet und gesteuert werden, ist die Entwicklung einer adäquaten Sicherheitsstrategie wichtig und notwendig. Unter Federführung des Mittelstand 4.0-Kompetenzzentrums Stuttgart hat die „Arbeitsgruppe IT-Sicherheit" in einem interaktiven Prozess ein gemeinsames Thesenpapier zum Thema „IT-Sicherheit in KMU" entwickelt. Das Thesenpapier nimmt direkte Signale aus dem unternehmerischen Bereich auf und verbindet diese mit den Erfahrungswerten sowie der wissenschaftlichen Expertise der verschiedenen Kompetenzzentren – vor diesem Hintergrund ist das vorliegende Dokument als Impulsgeber für eine vertiefte Diskussion zum Thema „IT-Sicherheit in KMU" gedacht.

1. **IT-Sicherheit darf nicht rein technisch verstanden werden.**

→ Sobald die Aufmerksamkeit der verantwortlichen Akteure ausschließlich auf technischen Aspekten liegt, führt dies zu weniger IT-Sicherheit. Bei der Implementierung von komplexen technischen Lösungen werden oftmals klassische Sicherheitsvorkehrungen (Mitarbeiterschulungen, Maßnahmen zur Sensibilisierung sowie zur Stärkung der Resilienz gegen Social Engineering-basierte Strategien) vernachlässigt. Vor dem Hintergrund des vom Menschen ausgehenden Risikos führt dies dazu, dass die implementierten Maßnahmen in vielen Fällen obsolet sind. Schlimmstenfalls werden aufwendige technische Maßnahmen implementiert, die durch fehlende analoge Ansätze außer Kraft gesetzt werden. Mitarbeiter spielen hierbei eine Schlüsselrolle und müssen deshalb bei der Implementierung von Sicherheitsmaßnahmen eingebunden werden. Nur so kann in einem Unternehmen Verständnis und Akzeptanz für diese Maßnahmen geschaffen werden.

2. **Neben dem Angebot zur Sensibilisierung von Mitarbeitern müssen auch verstärkt Angebote zur Sensibilisierung von Führungskräften entwickelt werden.**

→ Die Implementierung von IT-Sicherheitsmaßnahmen erfordert eine Entscheidung durch das Management. Deshalb ist die IT-Sicherheit in der Regel zu Beginn des Prozesses ein Top-Down-Thema. Aus diesem Grund muss die Unternehmensführung, beispielsweise durch Management-Leitfäden, verstärkt sensibilisiert werden und sich wie bei anderen Risikoabwägungen bewusst mit der Thematik auseinandersetzen.

3. **Das Themenfeld der IT-Sicherheit muss für KMU stärker konkretisiert werden.**

→ In vielen Fällen wird IT-Sicherheit als unübersichtliches Themenfeld wahrgenommen. Dies führt dazu, dass bei KMU die Motivation sinkt, sich mit den damit verbundenen Herausforderungen zu befassen. Vor diesem Hintergrund ist es sinnvoll, die Herausforderungen der IT-Sicherheit anhand maßgeblicher Parameter (Marktsegment, Themenfeld, Digitalisierungsgrad sowie Größe des Unternehmens) zu konkretisieren und aufzuarbeiten.

Mittelstand-Digital

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages

4. **KMU müssen in der Lage sein, eine adäquate Risikoeinschätzung abgeben zu können, um den Nutzen von IT-Sicherheitsmaßnahmen zu bewerten.**

→ Das Risiko allgemeiner Bedrohungslagen gestaltet sich mit Blick auf unternehmensindividuelle IT-Sicherheitsbedarfe sehr unterschiedlich und wird von Unternehmen als unübersichtlich wahrgenommen. KMU müssen in der Lage sein, eine individuelle Risikoanalyse vorzunehmen, um so die eigene Bedrohungslage einschätzen zu können. Nur so können sie mit Blick auf ihr jeweiliges Geschäftsmodell abwägen, ob sich die Implementierung von IT-Sicherheitsmaßnahmen lohnt oder ob sie das Risiko der Nichtimplementierung tragen können.

5. **IT-Sicherheit ist ein „moving target" – deshalb muss die Evaluierung der Sicherheitsstrategie einen regelmäßigen Charakter haben.**

→ Die Herausforderungen im IT-Sicherheitsbereich entwickeln sich in der gleichen Geschwindigkeit weiter wie die eingesetzten Technologien. Die implementierten Maßnahmen zur Gewährleistung von IT-Sicherheit müssen deshalb regelmäßig auf ihre Aktualität sowie ihre Wirksamkeit überprüft werden. Daneben muss IT-Sicherheit von Anfang an bei allen Digitalisierungsprozessen und von allen beteiligten Akteuren mitgedacht werden („Security by Design") – so erhält die IT-Sicherheit mittelfristig mit Blick auf die Digitalisierung einen „enabling character". Um den Professionalisierungsgrad in diesem Bereich zu steigern, ist es aus Kostengründen für KMU sinnvoll, zu evaluieren, ob man den Prozess durch einen vertrauenswürdigen Beratungsdienstleister begleiten lassen möchte. Ein sinnvolles Outsourcing hat den Vorteil, dass das Unternehmen keinen eigenen Sicherheitsexperten einstellen muss, gleichzeitig aber ein adäquates Sicherheitsniveau generieren kann, das regelmäßig geprüft wird.

6. **Um zu verdeutlichen, welche Auswirkungen IT-Sicherheitslücken in KMU haben können, ist es sinnvoll neben „Best Practice Cases" verstärkt auch „Worst Practice Cases" aufzubereiten.**

→ Den meisten KMU ist die Vielzahl der Angriffsvektoren und -szenarien im Bereich des digitalen Wirtschaftens nicht bekannt. Deshalb wäre es sinnvoll, die gängigsten Angriffsarten für KMU aufzuarbeiten und anhand von realen IT-Sicherheitsvorfällen anschaulich darzustellen. In diesem Zusammenhang ist es wichtig, die Bedrohungsszenarien ähnlich wie im zweiten Punkt des Thesenpapiers anhand der entsprechenden Parameter zu konkretisieren und anschließend mögliche Schutzmaßnahmen zu entwickeln. So wird für Unternehmen deutlich, dass präventives Handeln möglich ist und sich dieses mittelfristig gegenüber Schadensbegrenzung auszahlt.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages