Bild: Archiv

Ein IT-Sicherheitskonzept ist nicht in einem Tag erstellt.

Das IT-Sicherheits-konzept

Die Rahmenbedingungen für eine sichere IT-Umgebung bilden die IT-Strategie und darauf aufbauend ein IT-Sicherheitskonzept. In vielen Firmen verfügen über eine Strategie, jedoch das ebenso wichtige Sicherheitspapier fehlt. Dieser Beitrag zeigt, wie Sie ein IT-Sicherheitskonzept planen und damit auch die Grundlagen für ein ISMS erstellen.

Das IT-Sicherheitskonzept beschreibt die notwendigen Massnahmen zur Realisierung und Aufrechterhaltung des für das Unternehmen definierten Sicherheitsniveaus. Wichtig ist, dass das IT-Sicherheitskonzept alle Stufen anspricht: die Geschäftsführung ist ebenso angesprochen, wie die IT-Leitung und alle Mitarbeitenden.

Damit das IT-Sicherheitskonzept erstellt werden kann, müssen vier Fragen beantwortet werden:

1. Was will ich schützen?
2. Wogegen soll ich mich schützen?
3. Wie kann ich diesen Schutz erzielen?
4. Ob und wie will ich mir diesen Schutz leisten?

Schutzbedarf

Die erste Frage gilt dem Schutzbedarf. Was will ich schützen? Die drei Anforderungen Vertraulichkeit, Integrität und Verfügbarkeit helfen, diese Frage zu beantworten. Die Vertraulichkeit regelt den Zugriff auf die Informationen. Die Integrität stellt sicher, dass Daten nicht unerkannt beziehungsweise unbemerkt verändert werden können. Die Verfügbarkeit gibt an, welche Prozesse, Abläufe, Systeme, Netzwerkverbindungen und Personen für welche Situation zur Verfügung stehen müssen. Drei Beispiele dazu:

Cockpit eines Flugzeuges

Im Cockpit ist es von zentraler Bedeutung, dass die Instrumente immer verfügbar sind und die Angaben auf den Anzeigen korrekt, also verbindlich sind. Die Daten sind jedoch nur minimal vertraulich. Aus diesem Grund werden die wichtigsten Anzeigen in einem Flugzeug in doppelter oder gar dreifacher Ausführung angebracht. Auch wenn ein Instrument ausfällt, kann immer noch an die flugrelevante Information gelangt werden.

Online-Bank

Bei einer Online-Bank ist dem Kunden wichtig, dass die Vertraulichkeit jederzeit gewährleistet ist. Nur ich darf meine Daten sehen. Unvorstellbar, wenn diese Angaben in die Hände Dritter gelangen oder die Informationen abgefangen werden. Die Verfügbarkeit ist aus Sicht des Images einer Bank ebenfalls wichtig. Das Vertrauen in eine Bank schwindet, wenn die Kunden während mehreren Tagen nicht mehr an die Konten gelangen. Die Verbindlichkeit folgt an dritter Stelle. Niemand hätte Freude, wenn der Kontostand plötzlich nicht mehr korrekt ist.

Kasse eines Parkhauses

Bei einer Kasse ist die Integrität wichtig. Es freut sich niemand, wen nach korrekter Bezahlung das Parkhaus doch nicht verlassen kann und die Barriere unten bleibt. Sollte die Kasse einmal nicht verfügbar sein, steht auch die Schranke offen. Es stört in der Regel auch nicht, wenn der Hintermann den zu bezahlenden Betrag mitlesen kann (Vertraulichkeit).

Wogegen muss ich mich schützen?

Ein Unternehmen muss wissen, welche Gefährdungen vorhanden sind und ab welchem Punkt ein Schaden bedrohlich wird. Hier gilt es, verschiedene Szenarien und die Folgen abzuschätzen. Dies können zum Beispiel Stromausfall, Wassereinbruch, Mitarbeiterausfall, Systemabsturz, Viren, Hacker, Sabotage, usw. sein. Die Grundschutzkataloge des deutschen BSI (Bundesamt für Sicherheit in der Informationstechnik) bietet einen umfassenden Katalog an Bedrohungen.

Massnahmenauswahl

Aus dem Schutzbedarf und der begleitenden Risikoanalyse werden Massnahmen abgeleitet. Welche Massnahmen sind möglich? Damit auch verbunden, welche Gefährdungen kann eine einzelne Massnahme abdecken. Hat diese allenfalls Einfluss auf andere Gefährdungen oder Massnahmen? Welche Bereiche werden tangiert? Je nachdem, welche Bereiche abgedeckt werden, sind mehr Personen (ev. sogar externe) involviert oder es müssen verschiedene Prozesse angepasst werden. Eine zentrale Frage ist auch der Nutzen. Was bringt es mir, wenn ich eine Massnahme umsetze? Habe ich anschliessend die Ressourcen, diese Massnahme aufrechtzuerhalten. Als ein Stichwort ein Intrusion Detection Systeme. Die Flut an Daten wird hier oft unterschätzt und die Kontrolle dieser wird nur unregelmässig durchgeführt. Wenn diese jedoch nicht ausgewertet werden, ist das System nutzlos.

Sobald Massnahmen für die einzelnen Bereiche definiert wurden, gilt es diese zusammenzufassen und Synergien zu finden.

Wirtschaftlichkeit

Schlussendlich dreht sich alles um den finanziellen Aufwand. Kann und will ich mir diesen Schutz leisten? Hier scheitern viele Projekte. Doch es ist wichtig, anzuschauen, welchen Schaden eine Gefährdung anrichten kann. Tei-

len Sie die Auswirkungen in Kategorien von niedriger bis mittleren Schaden, hoher Schaden und sehr hoher Schaden ein. Dort wo der Schaden am grössten wird, sollten die ersten Massnahmen umgesetzt werden.

Es stellen sich nun die Fragen nach den Restrisiken. Was bleibt übrig, wenn ich eine Massnahme umgesetzt habe? Wie hoch ist die Eintrittswahrscheinlichkeit für die restlichen Gefährdungen? Allenfalls müssen weitere Massnahmen geplant und umgesetzt werden.

Vorgehen

Mit den Antworten auf diese vier Fragen kann das weitere Vorgehen definiert werden. Die Resultate sind zu bewerten und detailliert auszuarbeiten. Damit verbunden sind die Kosten. Erfahrungsgemäss wird zuerst der materielle Aufwand angeschaut und die zeitliche Belastung eher vernachlässigt. Dies ist aber ebenso einzuplanen. Mit der Auswahl der Massnahmen kann auch die Reihenfolge definiert werden. Welche Massnahmen sind zeitkritisch? Welche Massnahmen lassen sich auch später noch realisieren? Hier lohnt es sich, einen detaillierten Ablauf zu erstellen. Was sich zusammenlegen lässt, sollte auch gleichzeitig umgesetzt werden.

Wichtig bei der Umsetzung ist auch die Definition der Verantwortlichkeiten. Wer trägt die Verantwortung für eine Massnahme? Nur wer sich verpflichtet fühlt, wird auch das Zepter in der Hand nehmen.

Gleichzeitig mit der Umsetzung sind die begleitenden Massnahmen anzugehen. Die Schulung und Sensibilisierung von Mitarbeitern sind ebenso wichtig. Die Mitarbeiter müssen genug früh auf die Umstellungen vorbereitet werden, um einen möglichen Widerstand vorzubeugen.

Kontrolle

Mit der Planung und Umsetzung von Massnahmen ist das IT-Sicherheitskonzept nicht abgeschlossen. Eine regelmässige Kontrolle ist notwendig, um Abweichungen und veränderte Bedingungen zu erkennen und Anpassungen zu treffen. Auch hier gilt es Verantwortlichkeiten und Rechte festzuhalten, damit dies in periodischen Abständen passiert. Sollte es zu Änderungen kommen, ist das Management miteinzubeziehen und Entscheide zu treffen. Denken Sie auch hier daran, frühzeitig alle Mitarbeiter über die veränderten Situationen zu orientieren

Fazit

Ein IT-Sicherheitskonzept ist nicht in einem Tag erstellt. Die Vorbereitungsarbeiten nehmen viel Zeit in Anspruch. Doch dieser Aufwand lohnt sich, um die Informationssicherheit nachhaltig zu erhöhen. Massnahmen, die sich auf kritische Systeme auswirken, sollten anschliessend im ersten Schritt umgesetzt werden. Halten Sie fest, wer die Verantwortung für die Umsetzung und Kontrolle von Massnahmen trägt. Während und nach der Umsetzung gilt es, diese Massnahmen zu kontrollieren, sei dies durch externe oder interne Stellen.

Denken Sie immer daran, nur was bekannt ist, wird auch gelebt. Kleinigkeiten könnten ein Projekt scheitern lassen. Daher schulen und sensibilisieren Sie alle Stufen, von der Geschäftsleitung bis zum Mitarbeiter. So wird auch Ihr Konzept zum Erfolg.

.

INFOS | KONTAKT

goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch