Das Unternehmen muss Risiken identifizieren und die Eintrittswahrscheinlichkeit sowie die Auswirkungen beurteilen.

GELDVERSCHWENDUNG ODER MEHRWERT?

RISIKOABSCHÄTZUNG VON CYBERBEDROHUNGEN

von Andreas Wisler

Jeden Tag lässt sich von Angriffen und Schwachstellen lesen. Die Folgen für ein Unternehmen sind oft nicht abschätzbar. Soll durch ein Software-Update die Lücke geschlossen und dabei die Gefahr eingegangen werden, dass ein System nicht mehr läuft oder soll ein Unternehmen das Risiko eines Angriffs in Kauf nehmen?

Ein Ausfall oder gar Datenverlust kann gravierende Folgen für das gesamte Unternehmen bis hin zur Insolvenz haben. Menschen und Maschinen sind auf die ständig verfügbaren Informationen angewiesen. Daher gilt es, die IT-Umgebung zu schützen, sei dies vor Angriffen, Ausfällen, Datenmanipulation oder Fehlhandlungen. Die Risikoanalyse zeigt auf, wie es um die eigene IT-Sicherheit steht. Dabei genügt es nicht, nur die technischen Mittel einer Firma zu prüfen. Wichtig sind auch die Organisation und das technische sowie sicherheitsrelevante Wissen.

DAS VIER-LINIEN-MODELL

Das Four-Lines-of-Defense-Model (zu Deutsch das Modell der vier Verteidigungslinien) ist ein Modell zum systematischen Erfassen von Risiken, die in einem Unternehmen auftreten können. Diese müssen frühzeitig erfasst, identifiziert, analysiert, bewertet und mit wirtschaftlich angepassten Massnahmen angegangen werden. Das Modell fördert auch die Verbesserung der Kommunikation innerhalb der Organisation wie auch die Identifikation einzelner Personen, mit dem Ziel eines effektiven Risikomanagements. Die vier (Verteidigungs-) Linien umfassen:

1. Linie: Diese umfasst die Kontrollen im Alltagsgeschäft durch Mitarbeitende und Führungspersonen und stellt Verhaltensgrundsätze wie Reglemente und Weisungen auf.
2. Linie: Diese Linie beinhaltet die Informationspolitik sowie Reglemente und Weisungen. Zentral sind das Risikomanagement, das interne Kontrollsystem (IKS) und die Datenschutz-Funktion durch einen betrieblichen Datenschutzbeauftragten (bDSB) sowie die IT-Security-Funktion durch einen Chief Information Security Officer (CISO). Die Berichterstattung mit jährlichem Risk- und Massnahmenreport erfolgt an den Verwaltungsrat. Die zweite Linie umfasst ausserdem ein Business Continuity Management, regelmässige Schulungen und Übungen und die Strategiekontrolle.
3. Linie: In dieser Linie führt das Unternehmen regelmässige, interne Audits durch. Audits beziehungsweise Zertifizierungen sind beispielsweise die ISO 27001.

4. Linie: Diese beinhaltet die externe Revision und die Berichterstattung an die Aufsicht.

RISIKEN BEURTEILEN UND IDENTIFIZIEREN

Damit dieses Linienmodell funktioniert, gilt es, einen Risikobeurteilungsprozess zu etablieren. Dabei sollte die Informationssicherheit keine Insellösung darstellen, sondern das gesamte Unternehmen umfassen. Für die Durchführung einer Risikoanalyse definiert das Unternehmen in einem ersten Schritt die Kriterien, dazu gehören beispielsweise folgende Fragen: wer, wie, wann, Art der Dokumentation. Es ist wichtig, dass bei einer erneuten Durchführung der Risikobewertung konsistente und vergleichbare Ergebnisse erzielt werden.

Um eine gute Aussage erhalten zu können, identifiziert das Unternehmen in einem ersten Schritt die vorhandenen Prozesse: Was wird in diesen gemacht? Welche Daten werden verarbeitet? Welche Kritikalität haben diese Prozesse? Welche Personen sind involviert? Welche (technischen) Systeme werden genutzt? Somit gibt es bereits Prozesse und Werte. Im Englischen wird das Wort Asset dazu verwendet, was etwas genauer sagt, um was es geht. Es sind nicht nur Server und Laptops gemeint, sondern auch Papier-Unterlagen, Wissen und Patente. Die identifizierten Werte werden einem Besitzer (Owner) zugewiesen und die Vertraulichkeits-, Integritäts- und Verfügbarkeitsanforderungen bestimmt.

Im zweiten Schritt gilt es, mögliche Bedrohungen zu identifizieren. Ein Risiko tritt dann ein, wenn eine Bedrohung und eine Schwachstelle aufeinandertreffen. Wenn zum Beispiel eine Schwachstelle in einer Software vorhanden ist, ist dies zwar ärgerlich, aber noch kein Grund, in Panik zu verfallen. Sobald aber ein Programm oder schon nur eine Anleitung – ein sogenanntes Proof of Concept – zur Ausnutzung der Schwachstelle vorhanden ist, existiert eine reale Gefahr.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein tolles Werkzeug für alle möglichen Bedrohungen erarbeitet. Die Grundschutzkataloge[1] listen in sechs Kategorien über 700 Gefährdungen auf. Das BSI arbeitet ohne Schwachstellen und weist die Bedrohungen direkt den Werten zu, sogenannte Werte-Bausteine. Wer unsicher ist, welche Bedrohungen für einen Wert existieren, geht zum entsprechenden Baustein und im ersten Teil werden alle passenden Bedrohungen aufgelistet. So kann der eigene Aufwand massiv reduziert werden. Hinweis: Das BSI überarbeitet gerade die Grundschutzkataloge und spricht neu vom Grundschutzkompendium. Die nächste Erweiterung ist auf Anfang 2019 geplant.

RISIKOBEWERTUNG

Nun gilt es, das Risiko zu bewerten, wie wahrscheinlich eine Bedrohung wirklich eintritt. Dazu hat sich etabliert, die Eintrittswahrscheinlichkeit und die Auswirkungen einzeln zu bestimmen. Es spielt keine Rolle, ob ein Unternehmen dazu drei, vier, fünf oder gar mehr Stufen verwendet. Es muss aber genau definieren, was die Stufen bedeuten. Die Norm fordert, dass vergleichbare Resultate bei regelmässigen Risikoanalysen entstehen. Eine Möglichkeit ist ein dreistufiges Modell: gering, mittel, hoch mit den jeweiligen Werten null, eins und zwei. In einem nächsten Schritt bringt das Unternehmen die Werte in einen Zusammenhang. Beim Addieren der beiden Werte aus Eintrittswahrscheinlichkeit und Auswirkungen entstehen als Ergebnis Werte von null bis vier. Nun gilt es, Kriterien zur Behandlung dieser Risiken zu bestimmen. Folgende Definition könnte eine Möglichkeit sein: Die Werte null, eins und zwei sind akzeptable Risiken (Grün), während die Werte drei und vier inakzeptable Risiken sind (Rot). Inakzeptable Risiken muss ein Unternehmen behandeln. Sollte jedoch die Auswirkung oder die Wahrscheinlichkeit «Hoch», das heisst Wert 2, sein, entscheidet die Geschäftsleitung, ob das Risiko behandelt werden muss oder nicht (Orange).

Jedem identifizierten Risiko muss zwingend ein Risikoeigentümer zugewiesen werden. Dies kann die gleiche Person / Rolle sein wie der dazugehörige Wert, muss es aber nicht. Die definierte Person / Rolle muss nun das Risiko bearbeiten oder bewusst akzeptieren. Je nach Ergebnis gilt es, die Massnahmen zur Behandlung der Risiken zu priorisieren. Wichtig ist es, diesen Prozess sauber zu dokumentieren. Eine gute Möglichkeit ist es, die erkannten Risiken in einem Ticketing-Tool zu führen. So sind diese immer sichtbar, und jeder Behandlungsschritt lässt sich nachvollziehbar dokumentieren. Zudem kann das Unternehmen auf eine einfache Art und Weise Reminder zur Neubewertung hinterlegen.

BEWÄLTIGUNG DER RISIKEN

Nun gilt es, die möglichen Optionen zur Risikobehandlung zu bestimmen. Klassisch sind dies: Risiken vermeiden, vermindern, überwälzen oder bewusst akzeptieren. Im nächsten Schritt werden alle Massnahmen zur Bewältigung des Risikos ergriffen. Hier können wiederum die Grundschutzkataloge des BSI eine wertvolle Quelle sein; über 1 600 Massnahmen in den sechs Kategorien Infrastruktur, Organisation, Personal, Hard- und Software, Kommunikation und Notfallvorsorge sind darin enthalten. Idealerweise startet das Unternehmen bei den Bausteinen, dort wird kurz erklärt, was dies für ein Baustein ist, welche Gefährdungen existieren und welche Massnahmen das Unternehmen ergreifen kann.

Anhand dieser Massnahmen lässt sich ein Plan zur Informationssicherheitsrisikobehandlung erstellen. Dieser Plan behandelt die erkannten Risiken. Sinnvollerweise gibt er an, was durch wen bis wann umgesetzt wird. Gleichzeitig wird das Restrisiko bewertet, also wie sich das Risiko verändert, wenn das Unternehmen die Massnahme komplett, teilweise oder nicht umsetzt. Als letzter Schritt genehmigt der Risikoeigentümer in Zusammenarbeit mit dem Asset-Inhaber den aus vorherigem Punkt erstellten Plan. Es genügt nicht, pauschal durch die Geschäftsleitung das Risiko und den Risikoplan zu akzeptieren, sondern alle involvierten Personen müssen ihre Zusage dazu geben. Mit diesen Schritten kann ein Unternehmen ein umfassendes Risikomanagement aufbauen. Die IT-Sicherheit erhöht sich nachhaltig durch die Umsetzung der Massnahmen, die auf das identifizierte Risiko angepasst sind. ■

ANMERKUNG
1) www.bsi.de/gshb

ANDREAS WISLER

ist Inhaber und Senior Security Auditor bei der goSecurity GmbH.

www.gosecurity.ch