Der Security-Kreislauf

Informationssicherheit ist keine einmalige Angelegenheit. Alle wissen dies, doch das Tagesgeschäft verhindert regelmäßig die konsequente Umsetzung der notwendigen Schritte. Der Beitrag zeigt, wie der PDCA-Zyklus im Bereich der Informationssicherheit nachhaltig und ohne großen zusätzlichen Aufwand umgesetzt werden kann. Die Tätigkeiten sollen in den gewohnten Tagesablauf integriert werden und keine zusätzlichen Ressourcen binden.

Um Gefahren im Bereich der Informationssicherheit durch Maßnahmen auf ein akzeptables Niveau zu reduzieren, orientiert sich das Vorgehen an einem Kreislauf, *Bild 1*.

Vorbereitung

Jedes Unternehmen verfolgt Ziele. Im Zusammenhang mit Informationssicherheit können dies beispielsweise folgende sein:

- Das Unternehmen hält die Datenschutzrichtlinien und -bestimmungen ein.
- Die auf das Unternehmen zutreffenden Gesetze und vertraglichen Anforderungen sind bekannt und werden eingehalten.
- Es werden Vorkehrungen zur Reduktion von Schäden durch potenzielle Vorfälle umgesetzt, überwacht und erweitert, falls notwendig.
- Mitarbeitende kennen die Cyber-Gefahren und können entsprechend reagieren.
- Die IT betreibt die Server und Systeme gemäß Best Practices, installiert Updates zeitnah, führt Datensicherungen durch und überprüft die Sicherheit regelmäßig.

Um die Ziele zu erreichen beziehungsweise nicht zu gefährden, müssen mögliche Risiken identifiziert werden. Diese Risiken können von außen auf das Unternehmen einwirken, aber auch in den eigenen Reihen auftreten. Idealerweise werden diese in einem Workshop erarbeitet, zusammengetragen und anschließend bewertet. Bei der Bewertung werden die Eintrittswahrscheinlichkeit wie auch die Auswirkungen betrachtet. Hier empfiehlt es sich, eine Matrix mit einer geraden Anzahl von Feldern zu definieren, beispielsweise 4 × 4, *Bild 2*. Für die Auswirkungen können Abstufungen herangezogen werden.

Vernachlässigbare und begrenzte Auswirkung

Die Schadensauswirkungen sind gering und können vernachlässigt werden:

- Der finanzielle Schaden ist irrelevant (0 bis etwa 4.500 Euro)
- Der Imageverlust ist gering (gelegentliche Beschwerden)
- Preisgabe wenig sensibler Daten
- Geringe interne Kosten, außerhalb nicht bemerkbar
- Netzwerk und Systeme fallen maximal zwei Tage aus.

Die Schadensauswirkungen sind begrenzt und überschaubar:

- Der finanzielle Schaden ist tragbar (etwa 4.500 bis 45.000 Euro)
- Der Imageverlust ist bemerkbar (gelegentliche Kritik in den Medien)
- Kurzzeitige negative Auswirkungen sind möglich
- Kosten spürbar, von außen sichtbar
- Netzwerk und Systeme fallen maximal vier Tage aus.

Beträchtliche und existenzbedrohende Auswirkung

Die Schadensauswirkungen können beträchtlich sein:

- Der finanzielle Schaden ist spürbar (etwa 45.000 bis 90.000 Euro)
- Der Imageverlust ist groß (harte Kritik in den Medien)
- Ernsthafte negative Auswirkungen möglich
- Erhebliche Kosten sind zur Behebung notwendig
- Netzwerk und Systeme fallen maximal eine Woche aus.

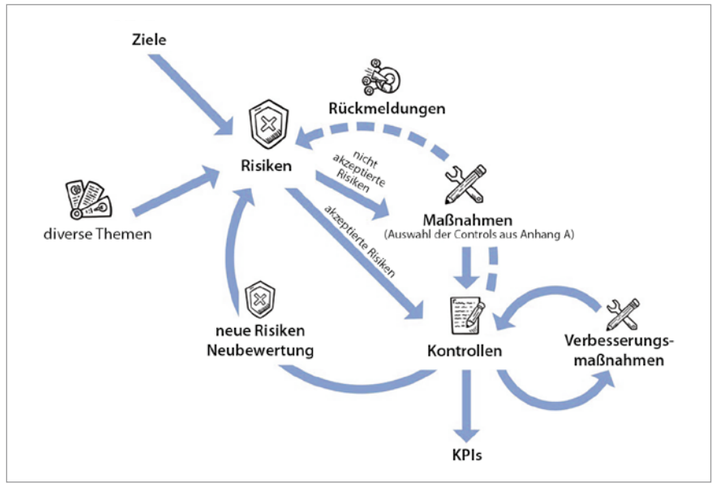

Bild 1 > Kreislauf der Tätigkeiten (© GoSecurity)

Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen:

- Der finanzielle Schaden bedroht die Existenz (mehr als 90.000 Euro)
- Es ist mit bleibendem Schaden zu rechnen
- Verlust von Leben/schwere Rufschädigung
- Erhebliche Störung des Betriebs, es besteht die Gefahr der Insolvenz
- Netzwerk und Systeme fallen mehr als eine Woche aus.

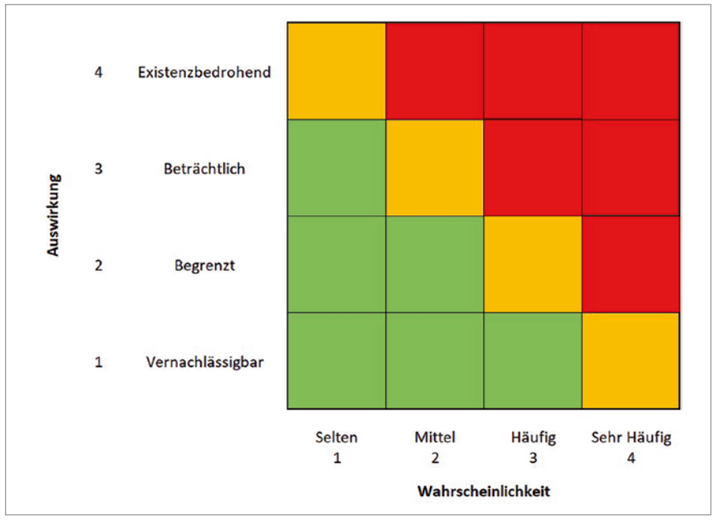

Bild 2 > Einschätzung der Auswirkungen (© Andreas Wisler)

Eintrittswahrscheinlichkeit eines Risikos

Nach Einschätzung der Auswirkungen ist es notwendig, die Eintrittswahrscheinlichkeit eines solchen Risikos festzustellen, zum Beispiel die Wahrscheinlichkeit, dass eine Bedrohung die Schwachstelle des betreffenden Werts ausnutzen könnte:

- Wahrscheinlichkeit selten: Ereignis tritt weniger als alle fünf Jahre einmal ein.
- Wahrscheinlichkeit mittel: Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
- Wahrscheinlichkeit häufig: Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
- Wahrscheinlichkeit sehr häufig: Ereignis tritt mehrmals im Monat ein.

Die Risiken werden in die Matrix übertragen. Dabei gelten folgende Bewertungen:

- Gering (Grün): Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz. Das Risiko wird akzeptiert, jedoch die Gefährdung beobachtet.
- Mittel (Orange): Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus. Die Geschäftsleitung entscheidet, ob Maßnahmen umgesetzt werden oder ob das Risiko akzeptiert wird.
- Hoch (Rot): Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.

Umsetzung von Maßnahmen

Bei den roten Risiken wie auch bei den nicht akzeptierten orangen Risiken werden Maßnahmen zur Reduktion des Risikos geplant. Dies können Maßnahmen aus dem Anhang A der ISO-Norm 27001 sein oder aus dem Grundschutz-Kompendium des BSI. Die ISO-Norm adressiert 114 umzusetzende Maßnahmen. Das BSI hat seine Maßnahmen in zehn übergeordnete Bausteine unterteilt. Im Detail wird beschrieben, was zu tun ist. Das Kompendium ist aus den ehemaligen Grundschutz-Katalogen entstanden. Das PDF kann noch online heruntergeladen werden. Auf über 5000 Seiten werden diverse Gefahren und Maßnahmen erläutert.

Aus den Maßnahmen, aber auch aus akzeptierten Risiken, werden Kontrollen abgeleitet. In definierten Abständen wird überprüft, ob die Maßnahmen korrekt umgesetzt wurden und das erwünschte Resultat ermöglichen. Ergänzend können Penetrationtests – ein simulierter Hacker-Angriff oder Sicherheitsprüfungen, das heißt eine Kontrolle möglicher Schwachstellen von Systemen, Netzwerken und Verbindungen – durchgeführt werden. Die Resultate ermöglichen das Erkennen neuer Risiken und auch die Neubewertung bestehender Risiken. Damit die Kontrollen bewertet werden können, sollten KPIs (Key Performance Indicators), eine Art Leistungskennzahl, abgeleitet werden. Sind die Resultate im grünen Bereich, ist alles in Ordnung. Sollten aber orange oder rote Ergebnisse erzielt werden, ist Handlungsbedarf notwendig. Die Maßnahme funktioniert noch nicht korrekt und muss korrigiert werden.

Bei den Kontrollen, vor allem auch bei Audits, fallen Dinge auf, die verbessert werden können. Vor allem auch von externen Spezialisten werden neue Ideen und Möglichkeiten vorgeschlagen. Diese sollten notiert, geprüft und falls passend umgesetzt werden.

Das nachfolgende Beispiel zeigt die Zusammenhänge auf:

- Ziel: kein Datenverlust durch Systemausfälle
- Risiken: Systemausfall, Fehlmanipulation
- Maßnahmen: Back-up-System, Monitoring
- Kontrolle: Wurde das Back-up vollständig durchgeführt? Wöchentlicher Durchführungsrhythmus
- KPI: Anzahl Back-ups, die fehlgeschlagen sind (monatlich gemessen), Grün: 0, Orange: 1, Rot: > 1

Fazit

Durch ein systematisches Vorgehen kann die Informationssicherheit stetig verbessert werden. Jedes Unternehmen möchte seine Prozesse und Dienstleistungen zeitnah und sicher betreiben. Diesem Ziel stehen Risiken im Wege, die bewertet und behandelt werden müssen. Gefahren werden durch Maßnahmen auf ein akzeptables Niveau reduziert. Die stetige Kontrolle gewährleistet, dass die getroffenen Schritte auch den gewünschten Effekt erzielen. Damit entschieden werden kann, ob eine Kontrolle genügt, werden Kriterien (KPIs) definiert. Die Auswertung ermöglicht Rückmeldungen auf die Risiken und verbessert so das gesamte System. Mit diesem systematischen Vorgehen kann das Unternehmen auch in Zukunft sicher agieren und zeitnah auf veränderte Risiken mit passenden Maßnahmen reagieren. //

Autor

Andreas Wisler ist Security-Experte und Speaker.