Bild: Archiv

Gefahren müssen durch Massnahmen auf ein akzeptables Niveau reduziert werden.

Der Security Kreislauf

Informationssicherheit ist keine einmalige Angelegenheit. Alle wissen dies, doch das Tagesgeschäft verhindert regelmässig das konsequente Umsetzen der notwendigen Schritte. Dieser Artikel soll aufzeigen, 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.

Das Vorgehen orientiert sich nach dem folgenden Kreislauf (Bild 1):

Vorbereitung – Plan

Jedes Unternehmen verfolgt Ziele. Im Bereich der Informationssicherheit könnten 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 auch zu erreichen beziehungsweise nicht zu gefährden, müssen mögliche Risiken identifiziert werden. Diese Risiken können von Extern 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 Eintretenswahrscheinlichkeit, wie auch die Auswirkungen betrachtet. Hier empfiehlt es sich, eine Matrix mit einer geraden Anzahl Feldern zu definieren, beispielsweise 4x4 (Bild 2). Für die Auswirkungen könnten folgende Abstufungen beigezogen werden:

Auswirkung vernachlässigbar

Die Schadensauswirkungen sind gering und können vernachlässigt werden.

- Der finanzielle Schaden ist irrelevant (CHF 0 bis 5000).
- Der Imageverlust ist gering (gelegentliche Beschwerden).
- Preisgabe wenig sensibler Daten.
- Geringe interne Unkosten, ausserhalb nicht bemerkbar.
- Netzwerk und Systeme fallen maximal zwei Tage aus.

Auswirkung begrenzt

Die Schadensauswirkungen sind begrenzt und überschaubar.

- Der finanzielle Schaden ist tragbar (CHF 5001 bis 50’000).
- 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.

Auswirkung beträchtlich

Die Schadensauswirkungen können beträchtlich sein.

- Der finanzielle Schaden ist spürbar (CHF 50’001 bis 100’000).
- Der Imageverlust ist gross (schwere Kritik in den Medien).
- Ernsthafte negative Auswirkungen möglich.
- Erhebliche Kosten sind zur Behebung notwendig.
- Netzwerk und Systeme fallen maximal eine Woche aus.

Bild 1: Tätigkeiten-Kreislauf.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

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

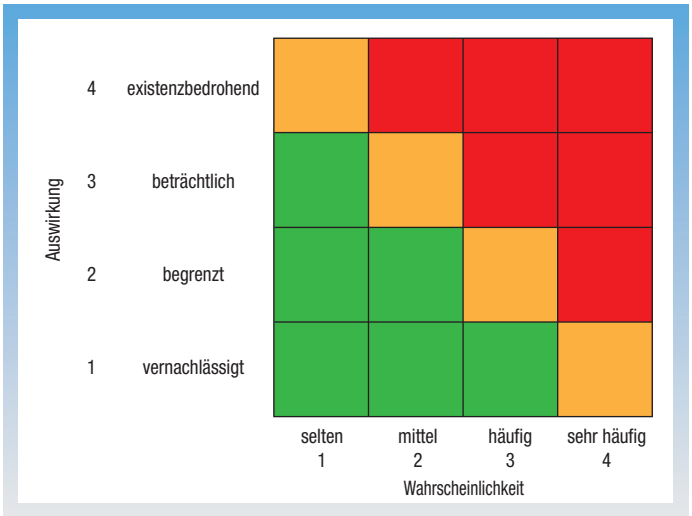

Bild 2: Einschätzung der Auswirkungen.

Auswirkung existenzbedrohend

Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmass erreichen.

- Der finanzielle Schaden bedroht die Existenz (> CHF 100'001).
- 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.

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

- Kategorie gering (grün)
  Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmassnahmen bieten einen ausreichenden Schutz. Das Risiko wird akzeptiert, jedoch die Gefährdung beobachtet.
- Kategorie 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.
- Kategorie hoch (rot)
  Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmassnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.

Umsetzung von Massnahmen – Do

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. Im Internet kann das PDF noch heruntergeladen werden. Auf über 5000 Seiten werden diverse Gefahren und Massnahmen erläutert.

Kontrolle ist besser – Check

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 Penetration-Tests, das heisst ein simulierter Hacker-Angriff oder Sicherheitsprüfungen, das heisst eine Kontrolle möglicher Schwachstellen von Systemen, Netzwerken und Verbindungen durchgeführt werden. Die Resultate ermöglichen, neue Risiken zu erkennen, wie auch der Neubewertung bestehender Risiken. Damit die Kontrollen bewertet werden können, sollten KPIs (Key Performance Indicator), 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.

Das Rad dreht weiter – Act

Bei den Kontrollen, vor allem auch bei Audits, fallen Dinge auf, die verbessert werden können. Gerade 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: System-Ausfall, Fehlmanipulation
- Massnahmen: Backup-System, Monitoring
- Kontrolle: wurde das Backup vollständig durchgeführt? Wöchentlicher Durchführungsrhythmus
- KPI: Anzahl Backups, 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 ihre 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 auch genügt, werden Kriterien (KPIs) definiert. Die Auswertung ermöglicht damit 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.