Von der lästigen Pflichtaufgabe zum echten Mehrwert

Werthaltiges Risikomanagement

Oft verlieren sich Betreiber kritischer Infrastrukturen beim Risikomanagement entweder in endlosen Excelzeilen, oder sie analysieren nur sehr abstrakt Risiken und beschränken sich bei den Sicherheitsmaßnahmen auf eine Compliance-fokussierte Umsetzung einiger Mindestsicherheitsmaßnahmen. Ein derartiges Risikomanagement führt jedoch trotz des wiederkehrenden Aufwands zu kaum einem Mehrwert für den Betreiber. Wie kann man also die Pflichtaufgabe Risikomanagement so gestalten, dass ein wirklicher Nutzen für das Unternehmen entsteht?

Von Dr. Stefan Ransom, TTS Trusted Technologies and Solutions GmbH

Der Gesetzgeber hat festgeschrieben, dass Betreiber kritischer Infrastrukturen angemessene technische und organisatorische Vorkehrungen zur Absicherung der kritischen Dienstleistung nach dem Stand der Technik treffen und diese in regelmäßigen Abständen nachweisen müssen. Eine Kernkomponente ist dabei das Risikomanagement, welches eine angemessene Ausgestaltung der erforderlichen Sicherheitsmaßnahmen sowie deren kontinuierliche Verbesserung garantieren soll.

Vielfach fehlen Unternehmen jedoch Methodik und Werkzeuge für ein wertbringendes Risikomanagement. Weder eine Einbettung in das Unternehmensrisikomanagement nach dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), in dem nur sehr abstrakt das einzelne Risiko „Ausfall der IT“ betrachtet wird, noch Verfahren, bei denen sich die Durchführenden in endlosen Excel-Zeilen verlieren, bilden sinnvolle Ansätze, die im Unternehmensalltag weiterhelfen. Viele Unternehmen fokussieren sich deshalb lediglich auf die Umsetzung von B3S-Maßnahmenkatalogen und der Sicherheitsmaßnahmen aus dem Anhang A der ISO 27001. Allerdings stellen die ISO-27001-Maßnahmen keine Handlungsanweisungen dar, sondern sind lediglich Handlungsempfehlungen. So wird oft versucht, den Aufwand für das Risikomanagement soweit wie möglich zu minimieren, da es im Grunde nur für den Auditor gemacht wird, der im Rahmen der Prüfung dessen Existenz sehen will.

Das Ergebnis ist dann eine Compliance-basierte Sicherheit, die allzu häufig aufgrund fehlender angemessener Ausgestaltung nicht gut zum Unternehmen passt. Auch werden so keine Mehrwerte geliefert, die das Unternehmen im Alltag unterstützen.

Wozu ist Risikomanagement eigentlich da?

Jedes Unternehmen muss zur Erreichung seiner Unternehmensziele Risiken eingehen. Das Risikomanagement soll dabei helfen, die richtigen Entscheidungen, hier aus Sicht der Informationssicherheit, zur Erreichung der Unternehmensziele zu treffen. Es soll Entscheider bei der Bewertung unterstützen, welche Risiken zur optimalen Nutzung bestehender Chancen eingegangen werden können. Weiterhin hilft es dabei, dass nicht akzeptable, hohe Risiken nicht leichtfertig eingegangen werden, sondern nur sehr bewusst. Nicht zuletzt ist es auch die Voraussetzung dafür, dass passgenaue Sicherheit für das Unternehmen etabliert werden kann. Es gilt, sowohl den Betrieb, als auch den digitalen Wandel bestmöglich zu schützen.

Vorteile eines werthaltigen Risikomanagements

Jedes Risikomanagement kann nur so gut sein, wie die Informationsbasis, auf der es operiert. Ein solides und möglichst vollständiges Modell der Informationsverarbeitung im Unternehmen ist dringend angeraten – man kann schließlich schlecht analysieren und bewerten, was man nicht kennt. Ganz nebenbei erreicht das Unternehmen hierbei aber auch eine hohe Transparenz über den aktuellen Zustand seiner Informationsverarbeitung und kann zielgerichtet Optimierungsentscheidungen treffen oder auch lohnende Digitalisierungsprojekte erkennen.

Erfolgsfaktoren für werthaltiges Risikomanagement

_____ solides Modell der Informationsverarbeitung

_____ standardisiertes Vorgehen, das Detailausprägungen zulässt

_____ kontinuierliche Nutzung im Betrieb und in allen Weiterentwicklungsprojekten

_____ gutes Werkzeug, das die Durchführung unterstützt

Ebenfalls profitieren Cyber-Defence-Aktivitäten. Nicht nur können strategisch wichtige Punkte in der IT-Infrastruktur für die Überwachung identifiziert werden, auch im Fall eines Angriffs sorgt eine hohe Transparenz im Idealfall für einen klaren Heimspielvorteil beim Verteidiger.

Gerade in größeren Unternehmen sollte ein unternehmensweit standardisiertes Vorgehen genutzt werden. Nur so können abteilungsübergreifend Ergebnisse gesammelt und verglichen werden, was eine zentrale Steuerung der effizienten Risikobehandlung und das Erzielen von Synergien bei der Umsetzung ermöglicht. Auch kann eine zentrale Sicherheitsabteilung jetzt ihre übergeordnete Position optimal nutzen, um aus zentraler Sicht Risikocluster oder strukturelle Risiken im Unternehmen zu erkennen.

Dabei muss die Risikomethodik aber natürlich so flexibel bleiben, dass individuelle Anforderungs- und Maßnahmenkataloge für bestimmte Bereiche des Unternehmens möglich sind. Insbesondere für die kritischen Dienstleistungen muss die Vermeidung von Versorgungsengpässen im Fokus stehen, und es sind spezielle Vorgaben zum Schutzbedarf und Umgang mit Risiken zu beachten, die nicht nur die wirtschaftlichen Interessen des Betreibers widerspiegeln dürfen.

Nicht für die Schublade

Transparenz über die Informationsverarbeitung und gute Risikomethodik sind aber nur die halbe Miete. Risikomanagement muss gelebt werden, um einen Mehrwert zu erzielen. Eine kontinuierliche Nutzung im Betrieb und konsequente Integration in alle Weiterentwicklungsprojekte sollten sichergestellt werden. Risikoanalysen, die nach der Projektphase beim Betriebsübergang in der Schublade verschwinden und nie wieder angeschaut werden, greifen hier deutlich zu kurz. Vielmehr müssen alle Risiken und risikomindernden Maßnahmen konsequent getrackt werden, damit sie nicht aus den Augen verloren werden.

Mit TTS trax lassen sich anhand der Ausgangs- und Zielrisiken und unter Einbeziehung des Umsetzungsstandes von Maßnahmen die aktuellen Ist-Risiken ermitteln.

Hinzu kommt, dass so auch die aktuelle Ist-Risikosituation ermittelt werden kann. Während viele Risikomethoden nur Ausgangs- und Zielrisiken betrachten, ist für die Leitungsebene eigentlich das aktuelle Ist-Risiko relevant, da dieses auch das jeweilige Haftungsrisiko darstellt. Durch konsequentes Einbeziehen der Umsetzungsstände der Sicherheitsmaßnahmen in die Risikoberechnung kann für die Leitungsebene eine unternehmensweite, immer aktuelle Übersicht der Ist-Risikosituation erstellt werden.

Werthaltige Risikoanalysen sind und bleiben schwierig und aufwendig. Um die Komplexität beherrschbar zu machen, sollten Werkzeuge heutzutage die Durchführung unterstützen, zum Beispiel durch automatisierte Vorbereitung der Risikoanalyse. Bedrohungen zielen häufig auf bestimmte Wertetypen ab, und auch viele Sicherheitsmaßnahmen lassen sich vorab bestimmten Bedrohungen zuordnen. Auf Grundlage einer guten Informationsbasis können Experten zentral Bedrohungs- und Maßnahmenzuordnungen spezifizieren, die dann während der Durchführung der Risikoanalyse als Vorschläge erscheinen und diese deutlich vereinfachen und beschleunigen. Weiterhin kann ein gutes Werkzeug den Nutzer an die Hand nehmen und ihn durch die notwendigen Schritte in der richtigen Reihenfolge geleiten.

Fazit

Die Mehrwerte eines durchdachten Risikomanagements liegen auf der Hand und viele der notwendigen Voraussetzung bringen das Unternehmen auch in anderen Themenbereichen weiter. Und obwohl Risikomanagement nach wie vor mit einem gewissen Aufwand verbunden ist, kann es nun dafür sorgen, dass Entscheidungen auf einer deutlich besseren Wissensbasis getroffen werden, während quasi nebenher die Anforderungen des Gesetzgebers für die angemessen ausgestaltete Absicherung der kritischen Dienstleistung sichergestellt wird.

Mehrwerte

- Darstellung der Ist-Risikosituation (Haftungsrisiken)
- Möglichkeit der Erkennung von Risikoclustern und strukturellen Risiken
- Nachweis der gesetzlichen Anforderungen
- fundierte Entscheidungsbasis
- Transparenz über die Informationsverarbeitung
- Unterstützung der Cyber-Defense-Aktivitäten
- Effizienz durch teilautomatisierte Risikoanalysen