

Risiko-Kurzanalyse

Die Risiko Kurzanalyse liefert einen schnellen Überblick über die potenziellen Risiken und deren Wahrscheinlichkeit. Kombiniert mit den Angaben zur Signifikanz der Schäden in Bezug auf direkte oder indirekte negative Auswirkungen auf die Geschäftstätigkeit, ergibt sich so eine gute Risikolandkarte. Zur Erstellung dieser Risikolandkarte dient ein fünfteiliger Fragebogen.

Der erste Teil umfasst Fragen zur Schadenswirkung bei Sicherheitsproblemen in den vier Aspekten Vertraulichkeit, Verfügbarkeit, Integrität und Zurechenbarkeit. Daraus ergibt sich eine Verletzbarkeitsmatrix über die gesamte Organisation. Anhand dieser Schadensmatrix werden die möglichen Risiken für die vier Aspekte identifiziert und gewichtet. Dazu dienen die weiteren Fragebogenteile. Aus den Ergebnissen entsteht eine gewichtete Schwachstellenmatrix, aus der sich die erforderlichen Maßnahmen ableiten lassen.

Umfang und Preise

Zur Durchführung einer Risiko Kurzanalyse ist es erforderlich, dass die Geschäftsprozesse zumindest auf der oberen Ebene dokumentiert sind. Das heißt eine Dokumentation der internen Prozesse muss existieren oder im Vorfeld erstellt werden. Falls eine Dokumentation der Geschäftsprozesse erforderlich ist, muss dazu ein dreitägiger Workshop zzgl. Vor- und Nachbereitung durchgeführt werden. An einem solchen Workshop sind Vertreter der verschiedenen Fachbereiche beteiligt. Die Zusammensetzung eines solchen Workshops kann bei kleineren Organisationen aber auch auf ein bis zwei Personen reduziert werden. Der Gesamtaufwand beträgt sieben bis zehn Tage.

Für die Risiko-Kurzanalyse wird je dokumentiertem Prozess ein Fixpreis von 400,- € berechnet.

Kontaktinfo

Bei Interesse an unseren Services nehmen Sie mit uns Kontakt auf:



APIS - Ulrich Moser
Schlossstraße 7
D-78244 Gottmadingen



info@apis-security.com



D +49.7734.935 880
+49.179.915 5418

CH +41.79.311 2051



+49.7734.931 9598



<http://www.apis-security.com>



Ulrich Moser
Diplom-Mathematiker

APIS
Ulrich
Moser



Risiko-Kurzanalyse

Der Umfang, in dem Sicherheitsmassnahmen erforderlich sind, hängt in hohem Maß von dem Gefährdungspotenzial ab, dem eine Organisation ausgesetzt ist. Dieses Gefährdungspotenzial ist von zahlreichen Einflussfaktoren abhängig und kann innerhalb einer Organisation für unterschiedliche Bereiche durchaus verschieden sein. Eine ausreichende Kenntnis der Risiken ist aber die Grundlage für ein sinnvolles und angemessenes Sicherheitskonzept.

Risikoanalyse als Basis einer ganzheitlichen Informationssicherheit

Security Maßnahmen der letzten Jahre waren weitgehend dadurch gekennzeichnet, dass man versucht hat Sicherheitsrisiken durch technische Maßnahmen also IT-Security zu begegnen, ohne sie in den Kontext eines organisationsweiten Sicherheitskonzepts zu stellen. Letztendlich ist IT-Security in vielen Fällen aber den Beweis der Rechtfertigung dieser Investitionen schuldig geblieben. Die Mehrheit der Sicherheitsverstöße ist nach wie vor durch Mitarbeiter bedingt und damit organisatorischen oder betrieblichen Ursprungs. Diesen Problemen kann nur bedingt durch technische Maßnahmen begegnet werden.

Daneben wurden vielfach Maßnahmen eingeführt, die am eigentlichen Problem vorbeigehen, weil die Risiken, die sie bekämpfen möglicherweise im konkreten Fall gar nicht relevant ist, wogegen andere Risiken einfach übersehen wurden.

Eine der Folgen ist auch, dass IT-Security bei den Fachabteilung oft nur als notwendiges Übel oder als Bremser gesehen wird. Eine Risiko-Analyse hilft hier

- i die tatsächlich relevanten Risiken zu erkennen,
- i die Bedeutung und Tragweite der Risiken zu beurteilen,
- i ein umfassenderes Verständnis von Informationssicherheit zu fördern,
- i die richtigen weil die Informationssicherheit fördernden Maßnahmen zu erkennen und umzusetzen.

Was ist ein Risiko?

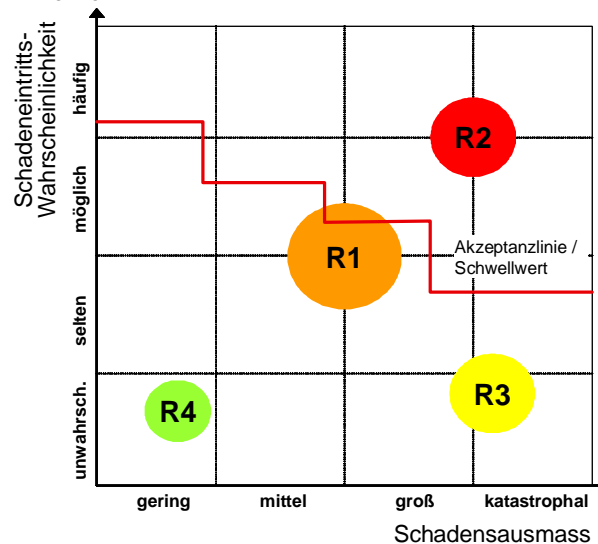
Der Begriff des Risikos ist eher abstrakt. Aus diesem Grund spricht man heute immer häufiger von Schwachstellen und Verletzbarkeit (engl.: vulnerability). Diese Wörter sind für Menschen eher be-greif-lich, da sie körperliche Assoziationen auslösen. Mit diesem Bild im Hintergrund sind also ein Risiko die Möglichkeit, dass ein Ereignis eintritt, das den ordnungsgemäßen Betrieb signifikant stören kann, und gegen das die Organisation nicht oder nur unzureichend geschützt ist. Ein solches Risiko kann von außen einwirken aber auch von innen heraus auftreten. Ein häufiges Beispiel ist der Ausfall einer/eines Mitarbeiterin/s für den kein Stellvertreter existiert.

Risiken erkennen, bewerten und bewältigen

Informationssicherheit soll die

- i Vertraulichkeit
- i Verfügbarkeit
- i Integrität
- i Zurechenbarkeit (Nachweisbarkeit)

von schützenswerten Daten gewährleisten. Risiken sind also Verletzbarkeiten der Informationssicherheit in einem oder mehreren dieser vier Aspekte. zugeordnet. Erstes Ziel einer Risikoanalyse ist es solche Verletzbarkeiten zu erkennen und sie den vier Aspekten zu zuordnen. In eines zweiten Schritt gilt es diese Risiken zu quantifizieren. Man spricht hier auch von einer Business Impact Analyse, also der Bewertung des Schadenspotenzials. Dieses Schadenspotenzial setzt sich zusammen aus der Eintrittswahrscheinlichkeit des entsprechenden Ereignisses, der unmittelbaren Schadenswirkung z.B. Geschäftsausfall und dem Aufwand für die Wiederherstellung des Normalbetriebs und zur Beseitigung des direkten Schadens.



Das Schadenspotenzial kann darüber hinaus auch noch von der Zeit abhängen, die ein Schadensereignis andauert. Aus diesem Grund ist es auch sinnvoll eine Auswertung wie in der nebenstehenden Graphik zu erstellen, die je Risiko diese Abhängigkeit aufzeigt. Die Werte an der vertikalen Achse entsprechen dabei dem erwarteten

Schadensausmaß von 1 für moderat bis 4 für Existenz bedrohend.

Sind die Risiken erkannt müssen im dritten Schritt die erforderlichen Maßnahmen zur Risikobewältigung eingeleitet werden. Hier stehen alle Maßnahmen im Vordergrund die zur Vermeidung von Risiken führen. In zweiter Linie muss versucht werden, die noch vorhandenen Risiken zu vermindern. Schließlich bleiben noch Überwälzung, durch Vertragsklauseln und Versicherungen, und Selbstbehalt. Bei all diesen Maßnahmen muss aber jeweils die Verhältnismäßigkeit geprüft werden. Stehen mehrere Alternativen zur Wahl, sollte zudem darauf geachtet werden, dass im Idealfall die Komplexität verringern aber zumindest nicht erhöht wird.

Die Risiko-Kurzanalyse

Die Risiko Kurzanalyse dient dazu, in kompakter Form und kurzer Zeit die Gefährdungspotenziale einer Organisation zu ermitteln. Die Organisation wird dazu entlang der Geschäftsprozesse daraufhin betrachtet welche Auswirkung Störungen in den einzelnen Prozessen und Prozessschritten auf den laufenden Betrieb haben. Es werden dabei die Schwachstellen gezielt aus geschäftlicher Sicht betrachtet und nicht aus technischer. Das Ziel ist die Verletzbarkeit entlang der verschiedenen Geschäftsprozesse zu erkennen und zu bewerten. Werden in einzelnen Bereichen Problemfälle erkannt, kann in einer weitergehenden Analyse gezielt in diesem Bereich die Gefährdungslage im Detail untersucht werden.

