ERNW Newsletter 21 / Februar 2008

Liebe Partner, liebe Kollegen,

willkommen zur 21-ten Ausgabe des ERNW-Newsletters mit dem Thema:

Kurzeinführung in die Risiko-Analyse und Beispiel

Version 1.0 vom 08. Februar 2008

von: Enno Rey, erey@ernw.de

Kurzdarstellung:
Dieser Newsletter beschäftigt sich mit einem der wichtigsten Teilprozesse effektiver Sicherheitsarbeit, der Risiko-Analyse. Nach einer kurzen Einführung wird als Beispiel eine Präsentation aus einem Kundenprojekt referenziert.

INHALTSVERZEICHNIS

1 EINFÜHRUNG

1.1 Der Risiko-Begriff

Es existiert ein dediziertes „Wörterbuch“ der ISO zum Thema (ISO/IEC GUIDE 73:2002), welches den Begriff „Risk“ wie folgt definiert:

“Combination of the probability of an event and its consequence“

Ein Risiko setzt sich danach aus der Eintrittswahrscheinlichkeit eines Ereignisses und der zu erwartenden Auswirkung zusammen. *Beide* Faktoren müssen also bei Anwendung des Risiko-Begriffs nach ISO 73:2002 berücksichtigt werden[1].

1.2 Sinn und Zweck des Risiko-Analyse Prozesses

Risiko-Analyse (kurz: RA) ist ein strukturierter Ansatz (der im Rahmen eines formalisierten Prozesses betrieben werden kann[2]), mit dem Risiken für bestimmte schützenswerte Gegenstände oder Sicherheitsziele untersucht wird. Ziele sind hier unter anderem:

- Die Bewusstmachung von Risiken. Erst durch Risiko-Analyse wird den Beteiligten häufig klar, welche Gefahren die Sicherheit der Gegenstände bedrohen und welche Risiken sich daraus ergeben.
- Die Bewertung von Risiken. Durch Risiko-Analyse werden die Risiken hinsichtlich ihrer Kritikalität für eine Organisation bewertet. Dadurch wird klar, welches Risiko etwa „grösser“ als ein anderes ist.
- Die Priorisierung von Massnahmen. Üblicherweise dient die Risiko-Analyse dazu, bestimmte Sicherungs-Massnahmen anderen vorzuziehen.
- Die Selektion von Lösungen. Generell kann Risiko-Analyse verwendet werden, um eine Entscheidung zu begründen, welche Lösung (aus mehreren möglichen) zur Adressierung eines (Sicherheits-) Problems geeignet ist.
- Die Beantwortung jeder Art von Fragen im Sicherheits-Kontext. Viele Fragen, die sich in der alltäglichen Sicherheits-Praxis ergeben, können mithilfe von Risiko-Analyse effizient (und gleichzeitig in dokumentierter Form) beantwortet werden.

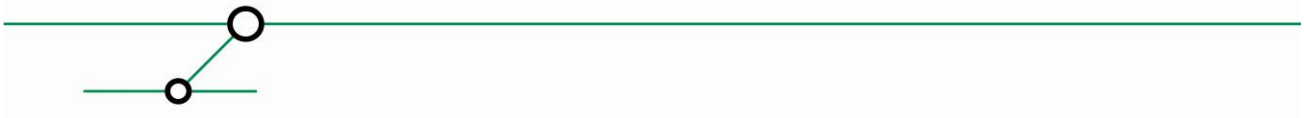
In den Augen vieler Sicherheits-Praktiker bildet Risiko-Analyse daher einen der wichtigsten Teilprozesse effektiver Sicherheitsarbeit. Darüber hinaus fordern verschiedene Standards zur Informations-Sicherheit (etwa ISO 17799/ISO 27001) zwingend die Durchführung regelmässiger Risiko-Analysen. Den wichtigsten Standard zur Risiko-Analyse selbst bildet aktuell der *British Standard* BS 7799-3[3].

---

[1] Dies weicht von einer häufig anzutreffenden, umgangssprachlichen Verwendung ab, bei der der Terminus „Risiko“ verwendet wird, tatsächlich aber eine Bedrohung gemeint ist.

[2] Es sei an dieser Stelle darauf hingewiesen, dass Risiko-Analyse auch ein alltäglicher, permanent praktizierter Vorgang ist. Ein Fussgänger, der eine Strasse überquert (oder dies aufgrund eines nahenden Autos eben unterlässt), hat zuvor eine immanente Risiko-Analyse durchgeführt.

[3] Im Rahmen der Harmonisierung der ISO 27000-Familie wird BS 7799-3 wohl (neben ISO TR 13335-2) im ISO-Standard 27005 aufgehen. Der Zeitpunkt ist jedoch noch unklar.



1.3 Typische Vorgehensweise und Einbindung in einen Prozess

Es wird meist zunächst ein schützenswerter Gegenstand (*Asset*) mit zugehörigen Anforderungen (*Requirements*) und Sicherheitszielen (*Objectives*) definiert. Dann werden mögliche Bedrohungen und Schwachstellen[4] (*Threats & Vulnerabilities*) betrachtet und die resultierenden Risiken (*Risks*) ermittelt. Diese Risiken können dann mithilfe von Massnahmen (*Mitigating Controls*) unterschiedlicher Natur adressiert werden.

2 ANWENDUNG

Wie schon dargestellt, lassen sich diverse Fragestellungen der täglichen Sicherheitsarbeit mithilfe von RA beantworten. Dazu sind Tabellen unterschiedlichen Aufbaus, unterschiedlicher Skalen und Rechenmethodiken notwendig. Betrachtet werden dabei Gegenstände (etwa Systeme, Teilfunktionalitäten, Prozesse oder auch Technologien) und zugehörige Bedrohungen.

Unter der u.g. URL findet sich ein Beispiel aus einem Kundenprojekt. Ziel war hier, bei der Einführung von VoIP mögliche Risiken bewussth zu machen und zu bewerten sowie die Bedrohungen zu identifizieren, die in erster Linie zu adressieren waren. Sollten Sie weitere Fragen zu Risiko-Analyse oder dem Beispiel haben, wenden Sie sich bitte an info@ernw.de.

Die Präsentation ist zu finden unter:

http://www.ernw.de/content/e7/e183/e1088/download1090/voip_risk_analysis_ger.pdf

Mit freundlichen Grüßen,

Enno Rey
Geschäftsführer
ERNW GmbH

ERNW Enno Rey Netzwerke GmbH
Breslauer Str. 28
69124 Heidelberg
Tel. +49 6221 480390
Fax +49 6221 419008
www.ernw.de
info@ernw.de

[4] Eine Schwachstelle ist dabei ein Faktor (z.B. eine nicht-verschlossene Tür), der der Realisierung einer Bedrohung (Diebstahl) Vorschub leistet. Diese werden typischerweise getrennt betrachtet, zumal meist nur auf die Schwachstelle eingewirkt werden kann (durch Massnahmen), nicht aber auf die Bedrohung.