MEHARI 2007

Handbuch Risikoanalyse

April 2007

Methods Commission

* Mehari ist ein von CLUSIF eingetragenes Warenzeichen

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS
30, rue Pierre Semard, 75009 PARIS, FRANCE
Tel. : +33 153 25 08 80 – Fax : +33 1 53 25 08 88
e-mail : clusif@clusif.asso.fr - Web : http://www.clusif.asso.fr

Inhaltsverzeichnis

Abbildungsverzeichnis

DANKSAGUNG

CLUSIF möchte sich bei den Kommissionsmitgliedern für die Teilnahme an der Erstellung dieses Dokumentes bedanken. Spezieller Dank gilt Christian Fötinger für die vorliegende deutsche Übersetzung des Dokuments.

1. EINLEITUNG

Ein Überblick über die Prinzipien der Risikoanalyse und der Identifikation von Risikosituationen findet sich im Dokument "*MEHARI – Konzepte und Funktionsweise*".

Die Hauptpunkte sind hier angeführt:

- Eine Risikosituation kann durch ihre gegebene Exponiertheit und Auswirkung, ohne Durchführung von Sicherheitsmaßnahmen, charakterisiert werden.
- Gegebene Exponiertheit und Auswirkung kann erhoben werden.
- Um das tatsächliche Risiko zu vermindern, können Sicherheitsmaßnahmen mit erkennbaren risikovermindernden Faktoren angewendet werden.
- Diese risikovermindernden Faktoren können erhoben werden.
- Mit diesen Elementen als Basis ist es möglich, die verbleibende Exponiertheit und Auswirkung, die Charakteristiken des Risikos, zu erheben und dadurch einen Risiko Level Indikator abzuleiten.
- MEHARI stellt Werkzeuge zur Verfügung, um die Analyse und den Evaluierungsprozess zu unterstützen.

Die Analyse einer Risikosituation kann sofort unter Anwendung der generellen Prinzipien und Erklärungen aus dem Dokument "*MEHARI – Konzepte und Funktionsweise*" durchgeführt werden.

Wenn die analysierte Situation mit einem der Szenarien aus der MEHARI Wissensdatenbank übereinstimmt, ist es möglich, die "*Risikoszenarioreferenz*" für eine sofortige Erhebung des Risikolevels heranzuziehen. Dieses Dokument stellt für jedes Szenario spezifische Hinweise auf Risiko minimierende Faktoren zur Verfügung.

In diesem Dokument beschreiben wir, wie die von MEHARI verwendeten Abläufe zur Erhebung der Risikosituationen verwendet werden sollen. Die verwendeten Beispiele werden derart sein, dass die beobachtete Situation mit einem Szenario aus der MEHARI Wissensdatenbank übereinstimmt.

Wir werden auch beschreiben, wie diese automatisierten Abläufe verwendet werden können, um Risikosituationen für eine detaillierte Analyse hervorzuheben.

2. ANALYSE VON RISIKEN UND DIE ANWENDUNG DER AUTOMATISIERTEN ABLÄUFE

2.1. Risikoanalyseprozess

Abbildung 1, zeigt den allgemeinen Risikoanalyseprozess, wie er bereits im Dokument "*MEHARI - Konzepte und Funktionsweise*" beschrieben wurde.

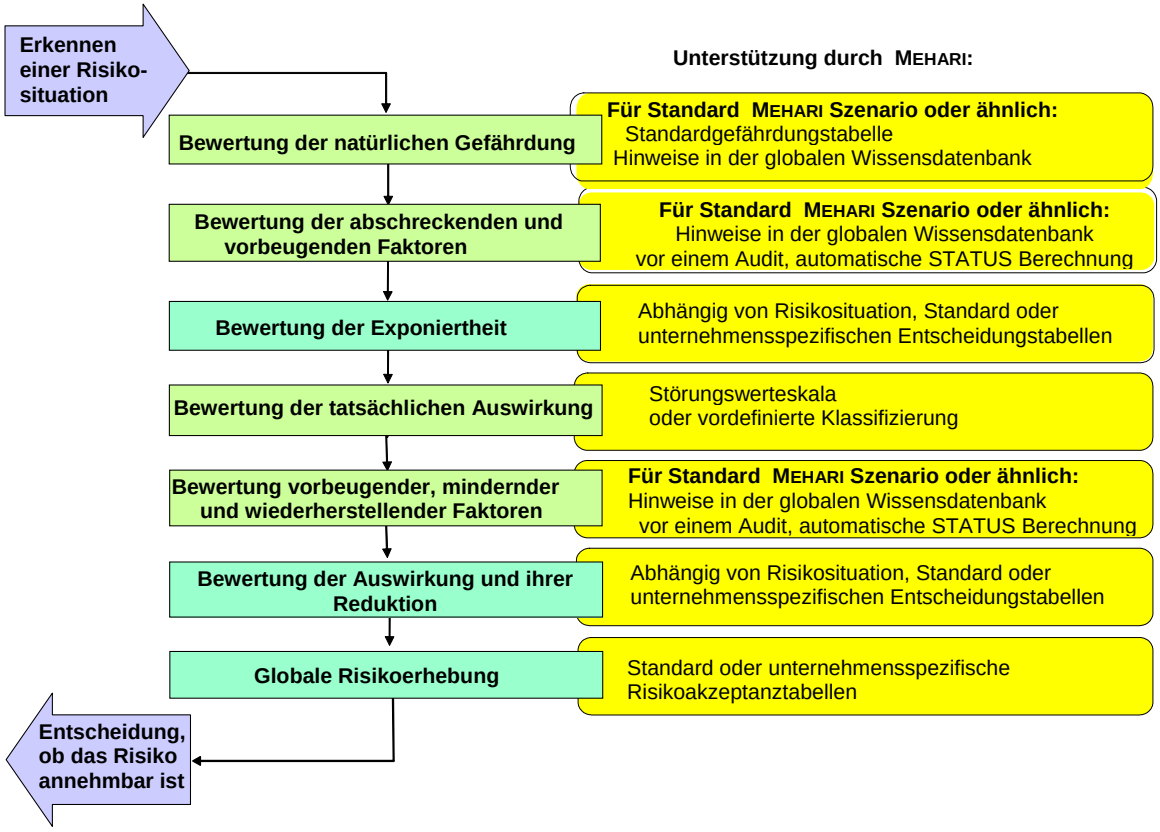

Abbildung 1: Der Risikoanalyseprozess und die Unterstützung durch MEHARI

Daher bietet MEHARI durch die Wissensdatenbank vielfältige Hilfestellungen bei der Risikoanalyse an.

- Unterstützung in der Bewertung der natürlichen Gefährdung
- Automatisierte Abläufe für die Erhebung der risikovermindernden Faktoren (abschreckend, vorbeugend, beschützend, mildernd und wiederherstellend) in Abhängigkeit von der Qualität der organisatorischen Sicherheitsmaßnahmen (Dienste), wenn diese mit einem MEHARI Audit erhoben wurden.
- Eine generische Tabelle über die tatsächliche Auswirkung kann als Ergebnis der Klassifikation oder unter direkter Anwendung einer Wertetabelle (der Störungen) erzeugt werden.
- Automatisierte Abläufe für die Berechnung der aktuellen Exponiertheit und Auswirkung als Funktion von Gefährdung, Auswirkung und risikomildernden Faktoren.

All diese Hilfestellungen stehen automatisch für alle Szenarien der MEHARI Wissensdatenbank zur Verfügung.

2.2. Bewertung der natürlichen Gefährdung

Im Dokument "*MEHARI – Konzepte und Funktionsweise*" haben wir bereits erklärt, dass die natürliche Gefährdung für dasselbe Unternehmen abhängig von zyklischen Erscheinungen variieren kann.

Es trifft allerdings für viele Unternehmen zu, dass eine „normale" oder „Standard" Gefährdung für ein bestimmtes Risiko (d.h. in Abwesenheit jeglicher bestimmter zyklischer Erscheinung) in Übereinstimmung mit allgemeinen Beobachtungen steht und eine erste Bewertung durchgeführt werden kann.

2.2.1 Standard natürliche Gefährdung

Die Szenarien[1] in der MEHARI Wissensdatenbank sind mit einer begrenzten Liste von charakteristischen Ereignissen querverwiesen, für die, egal ob es Unfälle, Fehler oder willentliche Aktionen (bösartig oder nicht) sind, eine erste "Standard" Bewertung der Gefährdung vorgeschlagen wird.

So wird z. B. angenommen, dass die „Standard" Gefährdung für Feuer in einem Unternehmen Level 2 (ziemlich unwahrscheinlich) ist; der Ausfall einer ICT Hardware ist Level 3 (ziemlich wahrscheinlich); und die Fehleingabe während eines Dateneingabeprozesses ist Level 4 (sehr wahrscheinlich).

Eine Liste der Ereignisse und der Standardgefährdung finden Sie im Anhang 1. Wie das Beispiel unten zeigt, bezieht sich jedes Szenario auf einen Ereignistyp:

10.31: Verlust von Dateien, wegen bösartiger Datenträgervernichtung durch Betriebspersonal

TYP-EXPO	EFF-DISS	EFF-PREV
MA010	MAX(MIN(07C02;08E02);08C01)	08A02
EFF-PROT	EFF-PALL	EFF-RECUP
MAX(08C01;08C05)	MAX(MIN(08D05;09D03);09D02)	01D02

Der Gefährdungstyp MA010 findet sich in der Tabelle im Anhang 1 unter: «Willentliche Löschung von Daten oder Diebstahl von Datenträgern" und wird mit einem Standardwert Level 3 (ziemlich wahrscheinlich) bewertet.

2.2.2 Unternehmensspezifische Gefährdung für ein bestimmtes Risiko

Es muss klar gesagt werden, dass die zur Verfügung gestellte Standardbewertung nur als solche zu sehen ist und dass die spezifischen Risikobewertungen der Gefährdungen für das Unternehmen in der Analyse bei weitem bevorzugt werden. Beziehen Sie sich daher für eine derartige Bewertung der Gefährdungsleveldefinitionen auf das Dokument "*MEHARI – Konzepte und Funktionsweise*". Dieses ist im Anhang 2 noch einmal angeführt.

Für ein spezielles Szenario sollten Sie auch im "Risikoszenarien Referenzhandbuch" nachsehen, das spezifische Informationen über die Bewertung der natürlichen Gefährdung enthält.

HINWEIS:

Wenn Risikosituationen systematisch analysiert oder bestimmte Risiken untersucht werden, ist ein Start mit einer Untersuchung aller Ereignisse vorzuziehen und ein übergreifendes Urteil für jede Unternehmensgefährdung zu erstellen.

[1] Die Szenarien in der MEHARI Wissensdatenbank sind nach Familien gruppiert, die ähnliche Konsequenzen haben. In dieser Version gibt es 12 Szenariofamilien.

2.3. Bewertung der tatsächlichen Auswirkung

Die Definition der tatsächlichen Auswirkungen eines Szenarios aus "*MEHARI – Konzepte und Funktionsweise*" ist die Bewertung der Konsequenzen eines aktuell auftretenden Risikoereignisses, unabhängig von jeder Sicherheitsmaßnahme.

Für jedes der Szenarien aus der MEHARI Wissensdatenbank gibt es ein Angriffsziel (einen Vermögenswert, der in dem Szenario zerstört oder beschädigt wird).

Das mögen gestohlene Daten oder Informationen, die Verminderung der Verfügbarkeit von Hardware oder eine Veränderung an Bestandteilen sein. Das wird davon abhängen, ob sich das Szenario auf die Vertraulichkeit, die Verfügbarkeit oder die Integrität eines Vermögenswertes auswirkt. Diese drei Basiskriterien werden von MEHARI standardmäßig abgedeckt.

Die Bewertung der Auswirkung unter solchen Bedingungen bezieht die Bewertung der Kritikalität oder der Schwere des Verlusts der Verfügbarkeit, Vertraulichkeit oder Integrität ein. Dies ist abhängig von der Art des Szenarios und dem darin angesprochenen Vermögenswert.

Der Klassifikationsansatz von MEHARI ermöglicht die Erstellung einer generischen Klassifikationstabelle. Diese Tabelle zeigt die Vermögenswerte, die über den Szenarienkatalog erkannt wurden. Dieser Ansatz ist im Dokument "*MEHARI – Konzepte und Funktionsweise*" und im „*MEHARI - Analyse des Sicherheitsumfeldes und Klassifizierungshandbuch*" beschrieben.

2.3.1 Tabelle der Auswirkungen

Der zur Bewertung der Auswirkung verwendete Ansatz kann sodann zusammengefasst werden. Er beinhaltet das Füllen einer Tabelle mit den Auswirkungen basierend auf einer Tabelle, die im Anhang 3 zur Verfügung gestellt wird. Einen Auszug finden sie hier.

Tatsächliche Auswirkung			
Klassifizierung von Daten, Informationen und Teilen der Infrastruktur	A	I	C
Daten und Informationen			
D01 Dateien oder Applikationsdatenbanken			
D07 Mails und Faxes			
…/…			
IT und Telekom Infrastruktur			
R02 LAN Komponenten und Verkabelung			
S01 Großrechner, Anwendungsserver			

Diese Tabelle wird durch die Übertragung der Höhe der Konsequenzen oder der Auswirkung auf die Verfügbarkeit, Vertraulichkeit oder Integrität für jeden erkannten Vermögenswert vervollständigt. Jedoch werden bestimmte Einträge, z. B. die Vertraulichkeit für Hardwareteile, nicht ausgefüllt.

Der Basisansatz verwendet die Klassifikationstabellen, wie sie im „*MEHARI - Analyse des Sicherheitsumfeldes und Klassifizierungshandbuch*" beschrieben sind.

Im schlimmsten Fall kann dies auch direkt erfolgen, aber der Klassifizierungsansatz aus "*MEHARI – Konzepte und Funktionsweise*", der mit dem obigen Prozess vervollständigt wird, ist unzweifelhaft leichter.

Das allgemeine Prinzip zur Vervollständigung der Tabelle der Auswirkungen ist, den höchsten gefundenen Klassifizierungswert aus dem Klassifizierungsprozess für jeden Typ von Informationen und jedes Kriterium zu kopieren. Details zur Vervollständigung der Tabelle der Auswirkungen mit den Ergebnissen aus dem Klassifizierungsprozess sind in *„MEHARI - Analyse des Sicherheitsumfeldes und Klassifizierungshandbuch“* beschrieben.

Dies erzeugt daher eine Synthese, die verwendet werden kann, um die Auswirkung für jene Szenarien (aus der MEHARI Wissensdatenbank) festzulegen, die eine Auswirkung auf die untersuchten Vermögenswerte haben.

2.3.2 Erweiterung der Tabelle der Auswirkungen

Die Standard MEHARI Tabelle bezieht sich nur auf drei Kriterien: Verfügbarkeit, Vertraulichkeit und Integrität. Es können natürlich auch andere Kriterien verwendet werden. Die Tabelle kann um Kriterien wie Nachvollziehbarkeit, Auditfähigkeit, etc. erweitert werden. Um diese Erweiterung durchzuführen, müssen Szenarien erzeugt (oder bestehende verändert) werden, die diese Kriterien ansprechen. Zusätzlich müssen dazugehörende Bewertungstabellen festgelegt werden.

Mit der Software Risicare[2] können bis zu acht Kriterien berücksichtigt werden.

2.3.3 Bewertung der Auswirkung von Szenarien

Die tatsächliche Auswirkung der einzelnen Szenarien aus der Wissensdatenbank kann einfach bewertet werden. Jedes Szenario hat eine Referenz zu einem Vermögenswert in der Tabelle der Auswirkungen und ein anwendbares Kriterium (A, I oder C – oder möglicherweise andere).

Anders gesagt, jedes Szenario aus der Wissensdatenbank bezieht sich explizit auf einen betroffenen Vermögenswert und auf die Art, wie er betroffen ist (A, I oder C). Auf diese Art und Weise kann die tatsächliche Auswirkung unter Verwendung der Tabelle im Anhang 3 bewertet werden.

2.3.4 Kartographische Aufteilung

Die Standardtabelle, wie sie im Anhang 3 zur Verfügung gestellt wird, zeigt nur eine Zeile für alle Applikationsserver oder Mainframes. Genauso gibt es nur eine Zeile für alle Datenbanken und allgemein nur eine Referenz für jede Art des Vermögenswertes.

Dieser globale Ansatz erlaubt der Risikoanalyse die maximale Sensibilität der betroffenen Vermögenswerte zu berücksichtigen ohne zwischen einzelnen Teilen zu differenzieren oder sie zu benennen. Dies ist eine Vereinfachung, die die zu analysierenden Situationen ohne einer praktischen Konsequenz beschränkt, da bei der Erstellung von Aktionsplänen immer die Möglichkeit besteht, die korrigierenden Maßnahmen nur auf die sensibelsten Vermögenswerte anzuwenden.

Jedenfalls ist es möglich, auf die gleiche Art und Weise, wie Sicherheitsmaßnahmen während eines MEHARI Audit abgewandelt werden, zwischen verschiedenen Variationen von Vermögenswerten zu unterscheiden. Nähere Details finden sie im Auditschema im “*MEHARI – Sicherheitsmaßnahmen Audithandbuch*”.

Diese Erzeugung von Vermögenswertvarianten in der Tabelle der Auswirkungen nennen wir **kartographische Aufteilung**. Sie erlaubt z. B. eine Differenzierung zwischen Servern aus verschiedenen Domänen, Domänen von Datenbanken, Applikationen aus verschiedenen Bereichen, usw. Die Verwendung dieser Aufteilung

[2] Eingetragenes Warenzeichen von BUC S.A.

erlaubt eine gesonderte Behandlung von einem oder mehreren speziellen Aktivitätsbereichen.

Die Software Risicare™ verwendet diese Möglichkeit, um Variationen der Szenarien in Abhängigkeit der erstellten kartographischen Abwandlungen[3] zu erzeugen.

ACHTUNG: Wird diese Option verwendet, kann dies die Aufgabe ernsthaft erschweren, da unvermeidbar mehr Szenarien erzeugt werden.

2.4. Bewertung der risikomindernden Faktoren mittels einem MEHARI Sicherheitsaudit

Die Bewertung der Exponiertheit und die Auswirkung eines Risikos hängen von der Analyse der bestehenden risikomindernden Faktoren und ihrer Qualität ab.

Um die Exponiertheit zu mindern, können abschreckende und vorbeugende Maßnahmen gesetzt werden. Während schützende (eingrenzende), wiederherstellende oder abschwächende (Abwälzung) Maßnahmen die Auswirkung mindern können.

In der Wissensdatenbank stellt MEHARI Bewertungen der Güte der risikomindernden Faktoren zur Verfügung in Abhängigkeit von der Qualität, der zu dem analysierten Szenario gehörenden Sicherheitsmaßnahmen.

Diese automatisierte Bewertung erfolgt in zwei Schritten:

- Durch die Berechnung der Effizienzindikatoren für Sicherheitsmaßnahmen, zu jedem Typ der risikomindernden Faktoren
- Durch die Berechnung der risikomindernden Faktoren selbst

2.4.1 Effizienzindikatoren für Sicherheitsmaßnahmen (Szenario und Risikominderungsmaßnahmen)

MEHARI bestimmt einen Effizienzindikator für jedes Szenario und jede risikomindernde Maßnahme.

Die Effizienz jeder risikomindernden Maßnahme wird mit folgenden Notationen dargestellt:

EFF-DISS	für die Effizienz von *abschreckenden Maßnahmen*
EFF-PREV	für die Effizienz von *vorbeugenden Maßnahmen*
EFF-PROT	für die Effizienz von *schützenden Maßnahmen*
EFF-PALL	für die Effizienz von *abschwächenden Maßnahmen*
EFF-RECUP	für die Effizienz von *wiederherstellenden Maßnahmen*

Diese Indikatoren werden mit Formeln berechnet, die eine Referenz zu der Sicherheitsmaßnahme erstellen.

---

[3] Wenn an Stelle von Risicare die Exceltabellen aus der Wissensdatenbank verwendet werden, muss die Klassifikationstabelle T1 und die Tabelle der Auswirkungen geändert werden (Anhang 3).

Diese Formeln aus der MEHARI Wissensdatenbank beruhen

- entweder direkt auf einer Sicherheitsmaßnahme durch einen Identifikator[4], wenn die Maßnahme die einzige ist, die diese Art von Effekt auf das Szenario hat;
- oder auf einer Formel, die Funktionen enthält: *MIN(arg1 ; arg2 ; …)* oder *MAX(arg1 ; arg2 ; …)*; die Parameter *(arg1 ; arg2, …)* sind Identifikatoren von Sicherheitsmaßnahmen aus der MEHARI Wissensdatenbank.

Daher kann die Formel z.B. folgendes Format haben:

EFF-PALL = 06B01

EFF-PREV = MAX(04B04;MIN(04B01;04B02;04B03))

Die erste Formel besagt, dass die (vorgeschlagene) Effizienz einer abschwächenden Maßnahme eine direkte Funktion der Maßnahme 06B01 ist und nimmt so die Qualitätsebene der Maßnahme als Wert an.

Die zweite Formel besagt, dass die (vorgeschlagene) Effizienz einer vorbeugenden Maßnahme dem größeren Wert zwischen der Qualität der Maßnahme 04B04 und der Funktion, die das Minimum der Maßnahmen 04B01, 04B02 und 04B03 ergibt, gleichzusetzen ist.

HINWEIS:

Die MIN Funktion sagt aus, dass die als Parameter aufgerufenen Maßnahmen komplementär sind. Ist ein Wert niedrig, ist das Ganze niedrig. Ein Beispiel eines solchen Falles ist die Verwaltung von Benutzerkonten und deren Authentifizierung; ist ein Wert schlecht, ist die ganze Zugriffskontrolle schlecht.

Die MAX Funktion zeigt, dass die als Parameter aufgerufenen Maßnahmen Alternativen sind. Ist eine Maßnahme auf einem hohen Niveau, so wird alles auf einem qualitativ hohem Niveau sein. Ein Beispiel dafür ist, abhängig von bestimmten Situationen, der Zugriff auf Daten und die Datenverschlüsselung.

Es kann sein, dass keine der bestehenden Sicherheitsmaßnahmen einen Einfluss auf eine bestimmte Art von Risikominderung für ein bestimmtes Szenario hat.

Als Beispiel zeigt die untere Tabelle den Inhalt der MEHARI Wissensdatenbank für das Szenario 10.31:

10.31: Verlust von Dateien, wegen bösartiger Datenträgervernichtung durch Betriebspersonal

TYP-EXPO	EFF-DISS	EFF-PREV
MA010	MAX(MIN(07C02;08E02);08C01)	08A02
EFF-PROT	EFF-PALL	EFF-RECUP
MAX(08C01 ;08C05)	MAX(MIN(08D05 ;09D03);09D02)	01D02

[4] Der Indikator einer untergeordneten Sicherheitsmaßnahme setzt sich aus einer Domänennummer, einem Buchstaben (der Maßnahme) und einer Nummer der untergeordneten Sicherheitsmaßnahme zusammen (z.B.: 06B01)

2.4.2 "Errechnete" risikomindernde Faktoren

Die oben errechneten Effizienzkoeffizienten *EFF-XXXX* werden auf Basis der Werte der Maßnahmenqualität errechnet, daher gibt es keinen Grund, dass diese bzw. die Effizienzkoeffizienten selbst Ganzzahlen sein müssen. Um die endgültige Berechnung der Exponiertheit und der Auswirkung einfacher zu gestalten, wandelt MEHARI diese, für die Bewertung der risikomindernden Faktoren, in Ganzzahlen um.

In MEHARI, werden risikomindernde Faktoren mit der Notation *STATUS-XXXX* (z. B. *STATUS-DISS* für einen abschreckenden Faktor) gelistet.

Der Wert für den *STATUS* wird durch Auf- oder Abrunden erreicht:

STATUS-XXXX = 1 wenn EFF-XXXX < 1,5

STATUS-XXXX = 2 wenn 1,5 >= EFF-XXXX < 2,5

STATUS-XXXX = 3 wenn 2,5 >= EFF-XXXX < 3,5

STATUS-XXXX = 4 wenn 3,5 >= EFF-XXXX

Wobei *XXXX DISS, PREV, PROT, PALL* oder *RECUP* sein kann.

Hinweis:

Der Wert der Bewertung der Gefährdung wird ebenso mit der Notation *STATUS-EXPO* angezeigt.

Diese risikomindernden Faktoren sind „errechnete" Faktoren. D.h., dass die erhaltenen Werte in einem spezifischen Kontext des Unternehmens oder der Organisation nicht völlig passend sind. Es kann z. B. Situationen geben, in denen Mitarbeiter kaum für abschreckende Maßnahmen empfänglich sind, wo Mitarbeiter Experten sind, wo vorbeugende Maßnahmen nutzlos sind oder Situationen, wo Schutz- oder Milderungsmaßnahmen keinen Effekt auf die reale Auswirkung haben.

MEHARI unterstützt, in dem es errechnete Werte für risikomindernde Faktoren zur Verfügung stellt. Diese Werte sollten jedoch vor der Anwendung überprüft werden.

Ein besonders häufiger Fall sind jene Szenarien, für die angenommen werden kann, dass schützende Maßnahmen die Auswirkung des Szenarios nicht erkennbar mindern (weil z. B. die Erkennung von Betrug oder Enthüllung von Informationen nicht die Bedeutung des Risikos mindert, egal welche Maßnahmen getroffen werden). Solch ein Szenario kann als „nicht entwicklungsfähig" angesehen und derart gekennzeichnet werden[5].

2.4.3 Berechnung der Risikofaktoren

Die Risikofaktoren für ein bestimmtes Szenario sollten vor Anwendung auf ihre Grunddefinitionen überprüft werden (siehe Anhang 4).

[5] In Risicare ist diese Option für Szenarien verfügbar, die anfangs als entwicklungsfähig angenommen werden. Wird diese Option gewählt, wird die Software eine spezielle Bewertungstabelle, ohne Berücksichtigung der Schutzmaßnahmen, verwenden.

2.5. Bewertung von Exponiertheit und Auswirkung

2.5.1 Automatisierte Exponiertheitsbewertung: *STATUS-P*

MEHARI stellt eine automatisierte Exponiertheitsbewertung zur Verfügung, die mit einer Bewertung einerseits der Gefährdung *STATUS-EXPO* und andererseits der Höhe der abschreckenden und vorbeugenden Maßnahmen *STATUS-DISS* und *STATUS-PREV* beginnt.

Durch den Ausdruck des obigen *STATUS* in ganzen Zahlen, bewertet MEHARI die Exponiertheit unter dem Namen *STATUS-P*. Dies wird direkt über Bewertungstabellen aus *STATUS-EXPO, STATUS-DISS* und *STATUS-PREV* abgeleitet

Drei Standardbewertungstabellen werden, abhängig vom Grund für den Unfall oder des Ereignisses, von MEHARI verwendet:

- Naturereignisse oder Unfälle
- menschliche Fehler
- willentliche Taten (bösartig oder nicht)

Diese Standardtabellen können bei Bedarf geändert werden.

Hinweis:

Die Logik hinter diesen Bewertungstabellen ist die Annahme, dass für jede Art der Ursache (Unfall, Fehler oder willentliche Tat), unabhängig von der genauen Beschreibung des Szenarios, demselben Gedankengang gefolgt werden muss. Mit gleich hohen Werten bei der Auswirkung, Abschreckung und Vorbeugung, muss die Exponiertheit zweier Szenarien gleich sein.

2.5.2 Automatisierte Bewertung der Auswirkung: *STATUS-I*

MEHARI stellt ebenso eine automatisierte Bewertung der Auswirkung zur Verfügung, die mit der Auswirkung des Szenarios einerseits und der Höhe der Schutz-, Linderungs- und Wiederherstellungsmaßnahmen andererseits *STATUS-PROT, STATUS-PALL* und *STATUS-RECUP* beginnt.

Die Bewertung wird in zwei Schritten durchgeführt:

- Bewertung eines auswirkungsreduzierenden Indikators: *STATUS-RI*
- Auswirkungsbewertung: *STATUS-I*

2.5.2.1 Bewertung der Auswirkungsmilderung: *STATUS-RI*

MEHARI stellt einleitend eine Bewertung der Auswirkungsmilderung über den als *STATUS-RI* erkennbaren Indikator zur Verfügung. Dieser wird direkt von *STATUS-PROT*, *STATUS-PALL* und *STATUS-RECUP* über Bewertungstabellen abgeleitet. Dieser reduzierende Faktor gibt die Abschwächung der Konsequenzen des Risikos, im Vergleich zu der zuvor bewerteten Auswirkung, an.

MEHARI verwendet, abhängig von der Art der Konsequenz des Szenarios, drei Standardbewertungstabellen, um den *STATUS-RI* zu bewerten:

- Verlust der Verfügbarkeit (A - availability)
- Verlust der Integrität (I – integrity)
- Verlust der Vertraulichkeit (C - confidentiality)

Diese Tabellen berücksichtigen auch, ob das Szenario sich entwickeln kann oder nicht. Diese Charakteristik ist explizit in der MEHARI Wissensdatenbank festgelegt. Zuvor als „entwicklungsfähig“ klassifizierte Szenarien können als „nicht entwicklungsfähig“ bestimmt werden.

Auch diese Standardtabellen können bei Bedarf geändert werden.

Hinweis:

Die Logik hinter diesen Bewertungstabellen ist die Annahme, dass für jede Art der Konsequenz (Verlust der Verfügbarkeit, Integrität oder Vertraulichkeit), unabhängig von der genauen Beschreibung des Szenarios, demselben Gedankengang gefolgt werden muss. Mit gleichen Werten bei den Schutz-, Linderungs- und Wiederherstellungsmaßnahmen, muss auch die Verminderung der Auswirkung für zwei vergleichbare Szenarien gleich sein.

2.5.2.2 Bewertung der Auswirkung: *STATUS-I*

Die verbleibende Auswirkung wird aus der tatsächlichen Auswirkung und dem vermindernden Faktor mit folgender Formel abgeleitet:

I = MIN (tatsächliche Auswirkung; 5 – STATUS-RI)

Dies weist darauf hin, dass *STATUS-RI* einen Effekt für die Festlegung der maximalen Auswirkungshöhe hat:

- Maximale Auswirkungshöhe ist 4, wenn *STATUS-RI* = 1
- Maximale Auswirkungshöhe ist 3, wenn *STATUS-RI* = 2
- Maximale Auswirkungshöhe ist 2, wenn *STATUS-RI* = 3
- Maximale Auswirkungshöhe ist 1, wenn *STATUS-RI* = 4

Die Bewertung des *STATUS-I* kann auch durch folgende Tabelle angezeigt werden:

STATUS-I **Berechnungstabelle**				
STATUS-RI immanente Auswirkung	**1**	**2**	**3**	**4**
4	4	3	2	1
3	3	3	2	1
2	2	2	2	1
1	1	1	1	1

2.5.3 Prinzipien der Bewertungstabellenerstellung

In der Praxis werden Standardtabellen, egal ob für Exponiertheit oder Auswirkung, aufgrund von einer bestimmten Anzahl von Prinzipien erstellt (diese sind im Anhang 5 - Prinzipien für die Erstellung von *STATUS* Bewertungstabellen – beschrieben). Um diese Tabellen zu ändern, sollte mit der Änderung der Prinzipien begonnen und als Ergebnis die Tabellen neu aufgebaut werden.

Die Standardbewertungstabellen sind im Anhang 6 festgehalten.

2.5.4 Bewertung von Exponiertheit und Auswirkung

Wie für die Risikominderungsfaktoren, stellen die auf Basis der Entscheidungstabellen automatisierten Abläufe nur eine Hilfe für die Beurteilung der Indikatorwerte *STATUS* zur Verfügung.

Eine endgültige Beurteilung sollte generell aufgrund der relevanten Beziehung von Exponiertheit *P (Potentiality)* und der Auswirkung *I(Impact)* erfolgen.

2.6. Bewertung der Bedeutung eines Szenarios

Die Bedeutung eines Szenarios wird über die Bewertung der Exponiertheit *P* und der Auswirkung *I*, über eine Risikoakzeptanztabelle, abgeleitet. Dies ist im Dokument "*MEHARI – Konzepte und Funktionsweise*" beschrieben.

2.7. Aufzeigen von Sicherheitsanforderungen

Dieser Schritt wird nur dann verwendet, wenn objektbezogenes Risikomanagement verwendet wird. Er besteht aus der Bewertung zusammengefasster Anforderungen, nachdem die Bedeutung aller Risikosituationen während eines Sicherheitsaudits erkannt wurde.

Dieser Ansatz basiert auf einer Beschreibung der "Maßnahmenanforderung" (siehe Anhang 7).

2.8. Praktischer Hinweis

2.8.1 Der Gedanke hinter dem Risikoanalyseansatz

Wir haben gezeigt, wie die automatisierten Abläufe von MEHARI dazu verwendet werden können, um die Risikolevel zu bewerten.

Es ist wichtig im Hinterkopf zu haben, dass dies ein Bewertungsprozess ist und dass ein Konsens eines Bewertungskomitees verlässlicher ist als automatisierte Abläufe.

2.8.2 Zusammenstellung eines Risikobewertungskomitees

Das Verfahren, das wir beschrieben haben, funktioniert besser, wenn eine repräsentative Arbeitsgruppe oder ein Komitee die Risikobewertung durchführt. Die Zusammenstellung dieser Gruppe ist besonders wichtig und sollte folgende Personen beinhalten:

- Anwender der betroffenen Umgebung. Es sollte ihnen möglich sein, ein Urteil über die Effektivität der Sicherheitsmaßnahmen zu bilden.
- Mitarbeiter der IT, die die Effizienz der verschiedenen Sicherheitsmaßnahmen und wie diese Maßnahmen umgangen oder behindert werden, den anderen Mitgliedern der Gruppe erklären können (Widerstandsfähigkeit und Steuerung/Überwachung).
- Jemand, der die Methode gut kennt und spezifische IT Sicherheitskompetenzen hat.

2.8.3 Anwendung dieses Verfahrens in Verbindung mit einem Sicherheitsaudit

Wir haben bereits erwähnt, dass die automatisierten Abläufe nur als Unterstützung im Bewertungsprozess in Betracht gezogen werden sollten. Es ist jedoch sogar mit einem kompetenten und repräsentativen Komitee möglich, die Qualität der

Sicherheitsmaßnahmen zu hoch zu bewerten – entweder durch ungewollten Optimismus oder aus politischen Gründen.

Ein Sicherheitsaudit kann zusätzlich die Qualität der Vorgehensweise sicherstellen und einen Anhaltspunkt für weitere Fragen bieten.

Die Bewertung von hohen Risiken mittels automatisierter Abläufe kann Schwächen oder Verwundbarkeiten hervorbringen, die in einer direkten Bewertung unbeachtet geblieben wären. Jeder Unterschied zwischen den beiden Ansätzen bedarf einer weiteren Betrachtung.

In diesem Sinne kann eine Bestätigung der direkten Bewertung durch die automatisierten Abläufe als "best practice" angesehen werden.

3. IDENTIFIKATION VON RISIKOSITUATIONEN

Im vorhergehenden Kapitel betrachteten wir die Analyse eines spezifischen Risikos.

Die Identifizierung von zu analysierenden Situationen ist ein einleitender Schritt, für den auch Werkzeuge gebraucht werden.

Es gibt prinzipiell 2 Wege, um Risiken festzustellen:

- Der direkte Ansatz, der die Werteskala der Fehlfunktionen verwendet (siehe "*MEHARI - Konzepte und Funktionsweise*")
- Eine organisierte und systematische Identifikation, die eine automatisierte Bewertung der von MEHARI zur Verfügung gestellten Basisszenarien verwendet.

Dieses Kapitel betrachtet die 2. Möglichkeit.

3.1. Anwendung der Wissensdatenbank für eine systematische Identifizierung

Wir wollen hier die von MEHARI angebotene Unterstützung bei der systematischen Risikosituationserkennung betrachten.

Bei der systematischen Erkennung werden die bereits beschriebene Risikoszenariendatenbank und insbesondere die zuvor beschriebenen automatisierten Abläufe angewendet. Sie basieren auf einer vorangehenden Analyse, deren Ergebnisse in einer Skala der Fehlfunktionen aufscheinen, einer Klassifizierung der Informationssystemwerte und einem Sicherheitsaudit.

Der von MEHARI verwendete Prozess basiert auf einer Szenarienauswahl, die spezifisch für die untersuchte Organisation sind (das ganze Unternehmen, eine operationale Einheit, etc.).

Wie folgendes Bild zeigt, gibt es 2 Hauptschritte:

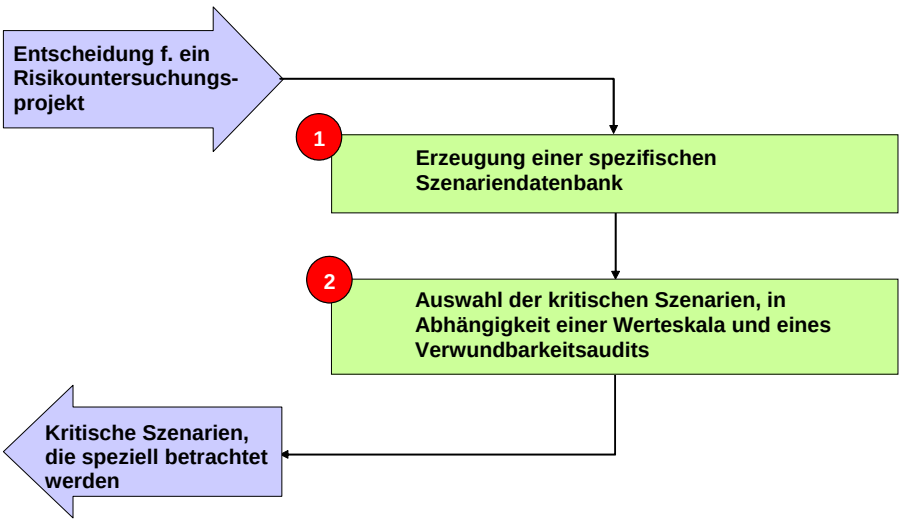

Abbildung 2: Erkennen von Risikosituationen

3.2. Erzeugung einer spezifischen Szenariendatenbank

Eine spezifische Szenariendatenbank kann von den generischen Szenarien, die Teil von der MEHARI Wissensdatenbank sind, abgeleitet werden.

3.2.1 Die generische Risikoszenariendatenbank

Die MEHARI Wissensdatenbank enthält eine Szenarienbasis, die bereits im vorhergehenden Kapitel besprochen wurde.

Es ist ein Szenariensatz, der nach Konsequenzarten zusammengefasst wurde (in dieser Version sind über 170 Szenarien und ihre Variationen nach 12 Familien klassifiziert). Für jedes Szenario gibt es:

- Eine Beschreibung der Konsequenzen des Szenarios
- Eine Beschreibung der Ursache und des Ursprungs des Szenarios
- Die charakteristische Ereignisart, um die Gefährdung zu bewerten
- Die betroffene Art des Vermögenswertes, um die Auswirkung zu bewerten
- Die sinngemäßen Sicherheitsmaßnahmen für das Szenario in Abhängigkeit des erwarteten Ergebnisses (abschreckend, vorbeugend, schützend, mildernd oder heilend)
- Die Formel, die von den automatisierten Abläufen verwendet wird, um die Effizienz der Sicherheitsmaßnahmen zu berechnen.
- Globale Indikatoren der Konsequenzart (A, I oder C für Verfügbarkeit, Integrität oder Vertraulichkeit) der entwicklungsfähigen (oder nicht entwicklungsfähigen) Eigenart des Szenarios und der Ursachenart (A [Accident], E [Error] oder V [Voluntary act] für Unfall, Fehler oder willentliche Tat). Diese Indikatoren werden auch von den automatisierten Abläufen verwendet, um die Exponiertheit und die Verringerung der Auswirkung zu berechnen (für die verwendeten Bewertungstabellen).

Zusätzlich enthält die Wissensdatenbank für jedes Szenario einen Analyseassistenten (genannt der 'globale Ansatz'). Das ist eine Zusammenfassung von angepassten Definitionen für jede Art von Sicherheitsmaßnahmen und Kommentaren zur direkten Erfassung der Effizienz der Sicherheitsmaßnahmen.

3.2.2 Anpassung der Szenarien als Erweiterung der betrachteten Elemente

Wie zuvor beschrieben decken die Szenarien von MEHARI die tatsächlich betrachteten Vermögenswerte (Elemente), da auf Typen bezogen, nur auf einer sehr globalen Ebene ab. Es kann der Wunsch nach einer Differenzierung einzelner Szenarien, abhängig vom involvierten Bestandteil, entstehen.

Insbesondere, wenn eine Klassifizierung für einzelne Gruppen von Servern oder anderen IT-Bestandteilen durchgeführt wurde und spezifische Daten einzelner Applikationsgruppen eine eigene Betrachtungsweise verlangen. Mit anderen Worten, werden genauso viele Szenarien erzeugt, wie Applikationsgruppen bestehen.

Nehmen wir z. B. das generische MEHARI Szenario "Diebstahl von Daten mittels Systemzugriff und Kopieren von Daten durch einen Hacker". Es ist möglich, getrennte Szenarien für die verschiedenen Datenarten (Personaldaten, Verkäufe, usw.) zu erzeugen. Dies bringt mit sich, dass - abgeleitet vom generischen Szenario - spezifische Szenarien für jedes klassifiziertes Element (Vermögenswert) erstellen werden müssen.

Dieser Ansatz ist möglich und wendet das an, was wir zuvor als „Kartographische Aufteilung" bezeichnet haben.

Dies kann zu einer beträchtlichen Anzahl von Szenarien führen, und es sollte vorsichtig damit umgegangen werden, um das Leben nicht unnötig zu verkomplizieren.

In der Praxis besteht der Grundansatz von MEHARI in der Anwendung der generischen Szenarien mit einem nur allgemeinen Vermögenswerttyp, dessen Sensibilität aus der Tabelle der immanenten Auswirkungen genommen wird.

Diese Vereinfachung kann damit gerechtfertigt werden, dass der Grund für die Analyse die Identifizierung jener Risiken ist, die kritisch sind und eine genauere Betrachtung verlangen. So wird festgestellt, welches Szenario das Niveau der Sensibilität der Vermögenswerte festlegt.

3.2.3 Berücksichtigung spezifischer Sicherheitslösungen

Bei der Festlegung, welche Szenarien kritisch sein können, werden die bestehenden Sicherheitslösungen natürlich einen Einfluss haben. Je effizienter diese Lösungen sind, umso weniger kritisch werden die Szenarien sein.

Es ist klar, dass jene Szenarien, für die es z. B. verschiedene Umgebungen oder Systeme gibt, oder genereller, für die es verschiedene Sicherheitslösungen gibt, getrennt behandelt werden müssen. Das ist genau derselbe Ansatz, wie er während einem Audit verwendet wird und *das für das Audit verwendete Schema sollte wiederum für die Auswahl der kritischen Risiken verwendet werden.*

Für eine andere Art der Anwendung des Auditschemas auf die Selektion der kritischen Szenarien ist zu berücksichtigen, dass wir als Basis für die Auswahl das Ergebnis des Sicherheitsaudits verwenden. Wenn es also während des Audits als wichtig angesehen wurde, dass zwischen verschiedenen Instanzen unterschieden werden soll, wird auch im Auswahlprozess zwischen verschiedenen Szenarien (in Abwandlung eines generischen Szenarios) unterschieden werden müssen. So gesehen können verschiedene Sicherheitsanwendungen, die in einem Szenario berücksichtigt sind, getrennt behandelt und bewertet werden.

Es sollte im Hinterkopf behalten werden, dass dies schnell zu einer großen Anzahl an Szenarien führen kann. Ein sehr einfaches Auditschema[6] kann leicht zu einem hohen Multiplikationsfaktor eines generischen Szenarios führen.

3.3. Automatische Bewertung von Szenarien

Die automatischen Abläufe von MEHARI wurden im vorigen Kapitel beschrieben.

Diese Prozeduren verwenden die Ergebnisse eines Sicherheitsaudits (und im speziellen das zur Bildung der Szenarien verwendete Auditschema).

Automatisierte Prozeduren werden verwendet, um den genauen STATUS zu bewerten und abhängig von der gegebenen Exponiertheit und der immanenten Auswirkung jedes Szenarios, die sich ergebende Exponiertheit und die Auswirkung für jedes Szenario zu bestimmen.

Die globale Bedeutung für jedes Szenario und seiner Kritikalität (oder nicht) kann daher aus der Risikoakzeptanztabelle abgeleitet werden.

[6] z.B.: eine Organisationseinheit, 2 Niederlassungen (Zentrale und Zweigstelle), 2 Gebäudearten (IT Technik und Bürogebäude), ein Netzwerk mit einem Netzwerkbetrieb, 2 Systeme (Mainframe und Open Systems) mit einem IT Betrieb, 2 Applikationsarten (1 für den Mainframe und 1 Open Systems) und 2 Entwicklungsarten (Mainframe und Open Systems).

3.4. Auswahl der kritischen Szenarien für die Betrachtung bei einer Risikoanalyse

Beginnend mit der ausgewählten Szenarienbasis und der automatischen Bewertung ihrer Bedeutung ist es einfach, die kritischen Szenarien zu wählen. D. h. jene Szenarien, die bei einer Risikoanalyse betrachtet werden sollten, verwenden den Prozess aus dem vorigen Kapitel.

Szenarien deren Bedeutung über einem bestimmten Level liegen, werden für die Analyse ausgewählt. Normalerweise über dem Wert 3 (bei einer Skala von 1-4).

Hinweis:

Mit der vorher angesprochenen Besonnenheit in Bezug auf die automatische Bewertung empfehlen wir, eine verhältnismäßig strenge Risikoakzeptanztabelle für die automatische Bewertung zu verwenden. Für die Auswahl der kritischen Szenarien kann eine unterschiedliche (strengere) Akzeptanztabelle als in der endgültigen Beurteilung der Bedeutung einer Risikosituation verwendet werden.

Eine verhältnismäßig strenge Tabelle für den Risikowert könnte wie folgt aussehen:

I = 4	3	3	4	4
I = 3	2	3	3	4
I = 2	1	2	3	3
I = 1	1	1	1	3
	P = 1	P = 2	P = 3	P = 4

Wichtig:

Im Allgemeinen empfehlen wir, dass Szenarien mit einem Risikowert von 4 als unternehmensgefährdend (umgehende Aktionen notwendig), jene mit 3 unannehmbar (Sicherheitsinvestitionsplan) und die darunter liegenden als annehmbar zu betrachten sind.

ANHANG 1: STANDARD GEFÄHRDUNGSTABELLE

Bewertung der Exponiertheit / des Ereignisspotentials		sehr unwahr-scheinlich	unwahr-scheinlich	wahr-scheinlich	sehr wahr-scheinlich	Status -Expo
Unfälle						
AC01	Kurzschluss: entweder Kabel oder Komponenten		X			2
AC02	Blitzschlag		X			2
AC03	Feuer: interne Ursache: Papierkorb, Aschenbecher, etc.		X			2
AC04	Beeinträchtigung durch Wasser oder Flüssigkeiten (undichte Leitungen, Verschütten, etc.).		X			2
AC05	Überschwemmung wegen Wasserrohrbruch		X			2
AC06	Überschwemmung wegen ansteigendem Wasserspiegel (Fluss, etc.)		X			2
AC07	Überschwemmung durch Löscharbeiten		X			2
AC08	länger dauernde Stromknappheit wegen externen Gründen		X			2
AC09	Nichterreichbarkeit von Gebäuden (Räumen): Zutritt behördlich verboten (Verschmutzung, Streik, Aufruhr, etc.)		X			2
AC10	Verlust von strategischem Personal		X			2
AC11	Verschiedene Geräteausfälle (Energieversorgung, Klimaanlage, etc.)		X			2
AC12	IT oder Telekommunikationsausfälle		X			2
AC13	Ausfall von IT oder Telekommunikationshardware, die nicht durch Wartung gedeckt ist oder der Wartungspartner nicht verfügbar ist.		X			2
AC14	unlösbarer Software deadlock: Entwickler oder Wartungspartner nicht verfügbar		X			2
AC15	ungewollte Auslastung von Resourcen (CPU, Speicher, Platten, etc.)			X		3
AC16	Datenzerstörung durch Betriebsunfälle			X		3
AC17	Daten oder Kofigurationszerstörung (unbrauchbar) durch einen Virus			X		3
AC18	Verlust von Dateien durch Unfälle in automatisierten Prozessen			X		3
AC19	Verlust von Dateien durch Unfälle wegen Überalterung oder Verschmutzung		X			2
AC20	Verlust von Dateien durch Unfälle wegen Geräteausfällen (disk crash, etc.)		X			2
Böswilligkeit						
MA01	Vandalismus von außen: Projektile oder geworfene Objekte, etc.		X			2
MA02	Vandalismus von innen: authorisierte Personen innerhalb der Räume (Personal, Vertragsnehmer, etc.).		X			2
MA03	Terrorismus: Sabotage, Explosionsstoffe nahe an sensiblen Bereichen	X				1
MA04	Böswillige und wiederholte Auslastung von IT Resourcen durch eine Anwendergruppe		X			2
MA05	Netzwerkbelastung wegen eines Wurms		X			2
MA06	Böswilliges Löschen (dirket oder indirekt) von gespeicherter Software		X			2
MA07	Böswillige Veränderung (direkt oder indirekt) von Programmfunktionen oder Office Programmen (Excel, Access, etc.)			X		3
MA08	fehlerhafte Dateneingabe oder Datenverfälschung			X		3
MA09	beabsichtigter Zugriff auf Daten oder Informationen und Enthüllung von Informationen			X		3
MA10	Entwendung von Dateien oder Diebstahl von Medien			X		3
MA11	Bewusste Löschung (direkt oder indirekt), Diebstahl oder Zerstörung von Programmen oder Datenbereichen (-pools, -containern)			X		3
MA12	Diebstahl von tragbaren PCs außerhalb der Firmengebäude			X		3
MA13	Böswilliges Löschen von Netzwerkkonfigurationen		X			2
MA14	Böswilliges Löschen von System- oder Anwendungskonfigurationen		X			2
MA15	Entwendung von Sourcecode		X			2
MA16	Spionage aus dem Ausland oder der Mafia	X				1
MA17	Diebstahl von IT- oder Netzwerkausstattung, innerhalb der Organisation			X		3
bewusste, nicht böswillige Aktionen						
AV01	Abwesenheit oder Streik von IT Betriebspersonal		X			2
AV02	Abwesenheit oder Rücktritt von strategischem Personal			X		3
AV03	Eindringen in IT Ressourcen durch Dritte mit Unterstützung innerhalb der Organisation oder des Personals			X		3
AV04	Illegale Verwendung von lizenzierter Software oder Produkten			X		3
Fehler						
ER01	Ungewollte Performanceeinbußen wegen Wartungsarbeiten		X			2
ER02	Ungewolltes Löschen von Softwareprogrammen aufgrund eines Unfalls oder menschlichen Versagens			X		3
ER03	Zufällige Veränderung von Daten während Wartungsarbeiten			X		3
ER04	Fehler während der Dateneingabe				X	4
ER05	Fehler im Betriebssystem, Middleware oder Softwarepaket				X	4
ER06	Fehler in Anwendungsprogrammen				X	4
ER07	Während der Änderung von Funktionen oder Makros in einer Tabellenkalkulation eingeschlichene Fehler			X		3

ANHANG 2: DEFINITION DER GEFÄHRDUNGSEBENEN

Risikogefährdung

Ebene 1 : Sehr geringe Gefährdung

Unabhängig von jeder Sicherheitsmaßnahme ist die Möglichkeit, dass ein bestimmtes Szenario eintritt, sehr niedrig und praktisch unerheblich.

Ebene 2 : Geringe Gefährdung

Sogar ohne jegliche Sicherheitsmaßnahmen, ist die Exponiertheit, dass in der Kombination aus Umgebung (Kultur, Mensch, geografisch oder andere) und Kontext (strategisch, Wettbewerb, sozial, …) ein bestimmtes Szenario auftritt, kurz- und mittelfristig sehr niedrig.

Ebene 3 : Mittlere Gefährdung (nicht im Besonderen gefährdet)

Die Umgebung und der Kontext des Unternehmens sind derart, dass wenn nichts zur Vermeidung unternommen wird, das Szenario mehr oder minder kurzfristig eintreten wird.

Ebene 4 : Hohe Gefährdung: (im Besonderen gefährdet)

Die Umgebung und der Kontext des Unternehmens sind derart, dass wenn nichts zur Vermeidung unternommen wird, das Szenario wahrscheinlich kurzfristig eintreten wird.

ANHANG 3: TABELLE DER IMMANENTEN AUSWIRKUNGEN

TABELLE DER IMMANENTEN AUSWIRKUNGEN				
Klassifizierungsebenen von Daten, Informationen, Infrastrukturkomponenten		**A**	**I**	**C**
Daten und Informationen				
D01	Applikationsdateien oder –datenbanken			
D02	Bürodateien und –daten (im Netzwerk)			
D03	Persönliche Dateien (lokal auf dem PC)			
D04	Geschriebene und gedruckte Informationen und Daten, die von Benutzern verwaltet werden sowie persönliche Archive			
D05	Listen und gedruckte Informationen			
D06	Nachrichten, Bildschirmansichten, etc. (Datenausschnitte)			
D07	Mails und Faxe			
D08	Alte ('ererbte') Archive oder anerkannte Dokumente			
D09	Veröffentlichte oder auf internen Webseiten publizierte Daten und Informationen			
D10	Dateien auf PDAs, etc.			
Infrastruktur: Telekommunikation und Systeme				
R01	WAN Equipment und Leitungen (Netzwerksysteme und -software)			
R02	WAN Equipment und Verkabelung (Netzwerksysteme und -software)			
R03	WAN Konfigurationsdaten			
R04	LAN Konfigurationsdaten			
S01	Hauptsysteme, Applikationsserver und ihre Peripheriegeräte, Dateiserver			
S02	Konfigurationsdateien für Hauptsysteme und Server			
S03	Workstations und Benutzerterminals (PC, lokale Drucker, Peripheriegeräte, spezielle Schnittstellen, etc.)			
A01	Applikationssoftware, SW-Pakete und Middleware (ausführbarer Code)			
A02	Source code			
A03	Konfigurationsdateien für Applikationen			
A04	Benutzer- oder Kundensoftware und Anwendungen			
Generelle Infrastruktur				
E01	Benutzerarbeitsplatz und Umgebung			
E02	Geräte für Sprachaustausch (Telefon, etc.)			
Immanente Auswirkungen (Globale Objekt bzw. nicht an ein spezifisches Objekt gebunden)				
Totalausfall oder Zerstörung einer Installation				
I01	Gesamter Serverraum und Telekommunikationseinrichtungen			
Nichtverfügbarkeit von Personen				
P01	Spezialistenteams (geschäftsbezogen)			
P02	IT Betriebsmannschaft			
Nichteinhaltung von Gesetzen und Regelungen				
C01	zum Schutz der Privatsphäre			
C02	für Finanzkontrollen			
C03	zum Schutz von geistigem Eigentum			
C04	zum Schutz der Informationssysteme			
C05	zum Schutz von Menschen, Öffentlichkeit und Umwelt			

ANHANG 4: EBENEN RISIKOMINDERNDER FAKTOREN

Abschreckende Maßnahmen	
Ebene 1:	Der Effekt einer abschreckenden Maßnahme ist gering oder Null. Potentielle Angreifer können davon ausgehen, dass sie kein persönliches Risiko eingehen. Sie gehen davon aus, dass sie nicht erkannt werden oder die Möglichkeit haben, gute Argumente zur Abstreitung der durchgeführten Tat einzubringen oder die Strafe sehr gering sein wird.
Ebene 2:	Der Effekt einer abschreckenden Maßnahme ist mittel. Potentielle Angreifer können davon ausgehen, dass sie kein persönliches Risiko eingehen. In jedem Fall werden resultierende persönliche Vorurteile erträglich sein.
Ebene 3:	Der Effekt einer abschreckenden Maßnahme ist hoch. Potentielle Angreifer können davon ausgehen, dass sie ein hohes Risiko eingehen. Es soll ihnen bewusst sein, dass sie unzweifelhaft erkannt werden und die Strafen ernst sein werden.
Ebene 4:	Der Effekt einer abschreckenden Maßnahme ist sehr hoch. Potentielle Angreifer sollen auf jeden Gedanken zur Durchführung einer Tat verzichten. Sie erkennen, dass sie mit Sicherheit erkannt werden und die sich ergebende Strafe jeden möglichen Vorteil aufhebt.

Vorbeugende Maßnahmen	
Ebene 1:	Der Effekt einer vorbeugenden Maßnahme ist gering oder Null. Jede Person innerhalb der Organisation, in einem Naheverhältnis oder sogar jemand der etwas über sie weiß, kann dieses Szenario, mit begrenzten Mitteln, in Bewegung setzen. Nahezu einfache Umstände können der Grund für dieses Szenario sein (Missbrauch, Fehler, ungünstige Umstände).
Ebene 2:	Der Effekt einer vorbeugenden Maßnahme ist mittel. Ein Professionist kann dieses Szenario ohne spezielle Mittel oder Werkzeugen außerhalb seines Bereiches starten. Seltene natürliche Umstände können dasselbe Ergebnis erzielen.
Ebene 3:	Der Effekt einer vorbeugenden Maßnahme ist hoch. Nur Spezialisten oder Professionisten mit speziellen Tools oder Mitteln oder eine Gruppe von Professionisten mit vereinten Mitteln und Werkzeugen werden erfolgreich sein. Dies ist üblicherweise das Resultat eines Zusammenspiels von seltenen oder außergewöhnlichen Umständen.
Ebene 4:	Der Effekt einer vorbeugenden Maßnahme ist sehr hoch. Nur wenige ausgesuchte Experten mit außergewöhnlichen Möglichkeiten haben Erfolg. Nur das Zusammentreffen sehr seltener und extrem außergewöhnlicher Umstände erzeugt dieses Szenario.

Schutzmaßnahmen oder Eingrenzung

Ebene 1: Die Effekte der Einschränkung der direkten Konsequenzen sind sehr niedrig oder Null.

Entweder kann der Schaden oder seine direkte Konsequenz nicht begrenzt werden, oder er wird einige Zeit nicht entdeckt.

Mögliche Schutzmaßnahmen haben dann nur einen begrenzten Einfluss auf die Höhe der direkten Konsequenzen.

Ebene 2: Die Effekte der Einschränkung und Begrenzung der direkten Konsequenzen sind mittel.

Obwohl der Schaden und seine direkten Konsequenzen beschränkt werden können, ist die Zeit bis zur Entdeckung lang oder die Reaktion ist langsam.

Die angewendeten Schutzmaßnahmen haben einen realen Einfluß auf das Ergebnis, aber die Konsequenzen sind noch immer sehr spürbar.

Ebene 3: Die Effekte der Einschränkung und Begrenzung der direkten Konsequenzen sind hoch.

Das Ereignis wurde rasch entdeckt und eine unmittelbare Reaktion eingeleitet. Die angewendeten Schutzmaßnahmen haben einen realen Einfluß auf die direkte Auswirkung, die aber noch eingeschränkt vorhanden ist und mit der umgegangen werden kann.

Ebene 4: Die Maßnahmen haben einen starken Effekt.

Der Beginn des Szenarios wird in Echtzeit erkannt, bevor noch großer Schaden angerichtet wird, und die Schutzmaßnahmen greifen sofort.

Direkte Konsequenzen von Unfällen, Fehlern oder willentlichen Aktionen werden sofort auf kleine Schäden begrenzt.

Wiederherstellende Maßnahmen

Ebene 1: Die Effekte der Einschränkung der direkten Konsequenzen sind sehr gering oder Null.

Entweder werden nur improvisierte Maßnahmen angewendet, oder es kann angenommen werden, dass die Effekte niedrig sind.

Ebene 2: Die Effekte der Einschränkung der direkten Konsequenzen sind mittel.

Die wiederherstellenden oder entlastenden Maßnahmen wurden weitgehend geplant aber letzte Details fehlen. Es kann angenommen werden, dass entsprechend der mangelnden Details die Effektivität der Maßnahmen fehlt.

Die Zeit zur Wiederaufnahme des Normalbetriebs kann nicht vorhergesagt werden bzw. führt zu keinem fundamentalen Unterschied in der Natur des Schadens.

Ebene 3: Die Effekte der Einschränkung der direkten Konsequenzen sind hoch.

Die wiederherstellenden Maßnahmen wurden nicht bis ins letzte geplant und organisiert, wurden aber getestet und bestätigt.

Die Zeit bis zur Wiederaufnahme des Normalbetriebs ist bekannt oder kann bestimmt werden, und die Maßnahmen reduzieren messbar den Ernst und die indirekten Konsequenzen des Szenarios.

Ebene 4: Die Effekte der Einschränkung der direkten Konsequenzen sind tatsächlich sehr hoch.

Der Normalbetrieb geht ohne merkbare Unterbrechung weiter.

Entschädigende Maßnahmen (Versicherung, etc.)

Ebene 1: Der Effekt von entschädigenden Maßnahmen ist gering oder Null.

Was immer möglicherweise von Versicherungen oder Rechtsklagen entschädigt wird, ist gering im Vergleich zu dem Schaden, der durch die globale Auswirkung des Szenarios und seiner Konsequenzen verursacht wurde.

Ebene 2: Der Effekt von entschädigenden Maßnahmen ist mittel.

Mögliche Entschädigungen sind nicht belanglos, aber die Organisation ist für den größten Teil des verursachten Schadens verantwortlich.

Bei einem großen Störfall ist es nicht sicher, dass der Risikotransfer reicht um das Überleben der Organisation zu sichern.

Ebene 3:	Der Effekt von entschädigenden Maßnahmen ist hoch. Mögliche Entschädigungen reichen aus, um die Auswirkungen zu mindern. In jedem Fall kann weiter gearbeitet werden. Verbleibender Schaden kann sehr ernst sein, erreicht aber nicht die «überlebensbedrohliche» Ebene.
Ebene 4:	Der Effekt von entschädigenden Maßnahmen ist extrem hoch. Wie schlimm das Desaster sein mag, der verbleibende Schaden kann bewältigt werden (Ebene 2).

ANHANG 5: PRINZIPIEN ZUR ERSTELLUNG DER *STATUS* BEWERTUNGSTABELLEN

Die unten beschriebenen Prinzipien sind jene, die verwendet wurden, um die *STATUS-P* und *STATUS-RI* Tabellen zur Konvertierung des *detaillierte*n *STATUS* in einen *globalen* STATUS zu erstellen.

STATUS-P Bewertungstabelle

Die Tabelle basiert auf folgender Begründung:

- Die gegebene Exponiertheit wird durch das intrinsische Potenzial ohne jegliche Sicherheitsmaßnahme definiert. Der Maximalwert von *STATUS-P* ist der von *STATUS-EXPO* (in Abwesenheit jeglicher Maßnahme, d. h. wenn *STATUS-DISS* und *STATUS-PREV* den Wert 1 haben)
- Wenn der Wert von *STATUS-PREV* für Unfälle oder Fehler 3 oder 4 ist, hat *STATUS-P* einen Maximalwert von 2 oder 1.
- Wenn der Wert von *STATUS-PREV* für willentliche Aktionen 4 ist, hat *STATUS-P* einen Maximalwert von 2.
- Wenn der Wert von *STATUS-PREV* für willentliche Aktionen 4 und die Exponiertheit kleiner oder gleich 3 ist, hat *STATUS-P* einen Maximalwert von 1.

STATUS-RI Bewertungstabelle

Die Tabelle basiert auf folgender Begründung:

- Wenn der Wert von *STATUS-RECUP* 3 ist, ist *STATUS-RI* zumindest 2
- Wenn der Wert von *STATUS-RECUP* 4 ist, ist *STATUS-RI* zumindest 3
- Wenn der Wert von *STATUS-PALL*, für verfügbare Szenarien, 3 oder 4 ist, ist *STATUS-RI* zumindest 3 (wenn die Wiederherstellungsplanung ordentlich vorbereitet wurde, kann die sich ergebende Auswirkung nicht ernst sein).
- Ist der Wert von *STATUS-PROT* in einem Integritätsszenario 4, kann alles durch eine schnelle Wiederherstellung vermieden werden und daher richtet sich *STATUS-RI* nach dem Wert von *STATUS-PALL*.
- Ist der Wert von *STATUS-PROT* in einem Integritätsszenario 3 und eine schnelle Wiederherstellung ist möglich (*STATUS-PALL* = 3 oder 4), wird ohne Zweifel das schlimmste verhindert, aber die Situation kann trotzdem ernst bleiben: *STATUS-RI* = 2. Ist jedoch keine schnelle Wiederherstellung möglich (*STATUS-PALL* = 1 oder 2), wurde nichts vermindert und *STATUS-RI* = 1.
- Ist der Wert von *STATUS-PROT* in einem Integritätsszenario 1 oder 2, ist STATUS-RI = 1, außer es gibt eine geplante Maßnahme, die im *STATUS-RECUP* identifiziert wurde (geringer Schutz, keine Wiederherstellungsmaßnahme, weil dies nur aufgesetzte Maßnahmen sind, die keine Auswirkung auf die indirekten Konsequenzen haben und nur die Wiederherstellungsmaßnahmen eine Rolle spielen).

Unter diesen Annahmen wurden die Tabellen der MEHARI Wissensdatenbank erzeugt.

ANHANG 6: STANDARDBEWERTUNGSTABELLEN

Bewertungsraster zu *STATUS-P* für Szenarien:

Jeder Raster korrespondiert mit dem gewählten Wert für die gegebene ('natürliche') Exponiertheit (EXPO)

1. Szenarien basierend auf einem Unfall

	EXPO = 1				EXPO = 2				EXPO = 3				EXPO = 4			
A																
B																
S																
C	1	1	1	1	1	2	2	2	1	3	3	2	1	4	4	2	1
H		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
		V	O	R	B	V	O	R	B	V	O	R	B	V	O	R	B

2. Szenarien basierend auf einem Fehler

	EXPO = 1				EXPO = 2				EXPO = 3				EXPO = 4			
A																
B																
S																
C	1	1	1	1	1	2	2	2	1	3	3	2	1	4	4	2	1
H		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
		V	O	R	B	V	O	R	B	V	O	R	B	V	O	R	B

3. Szenarien basierend auf einer willentlichen Aktion

	EXPO = 1					EXPO = 2					EXPO = 3					EXPO = 4				
A	4	1	1	1	1	4	2	1	1	1	4	3	2	1	1	4	4	3	2	2
B	3	1	1	1	1	3	2	2	1	1	3	3	2	2	1	3	4	3	2	2
S	2	1	1	1	1	2	2	2	2	1	2	3	3	2	1	2	4	4	3	2
C	1	1	1	1	1	1	2	2	2	1	1	3	3	2	1	1	4	4	3	2
H		1	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4
		V	O	R	B		V	O	R	B		V	O	R	B		V	O	R	B

Bewertungsraster für STATUS-RI (Auswirkungsminderung)

1. Szenarien betreffend der Verfügbarkeit (Availability)

	SCHUTZ = 1					SCHUTZ = 2					SCHUTZ = 3					SCHUTZ = 4					SCHUTZ = 0				
V	4	3	3	3	3	4	3	3	3	3	4	3	3	3	3	4	3	3	3	4	4	3	3	3	3
E	3	2	2	3	3	3	2	2	3	3	3	2	3	3	3	3	3	3	3	4	3	2	2	3	3
R	2	1	2	3	3	2	1	2	3	3	2	1	2	3	3	2	2	3	3	4	2	1	2	3	3
S	1	1	2	3	3	1	1	2	3	3	1	1	2	3	3	1	2	3	3	4	1	1	2	3	3
		1	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4
		R	E	C	O	V	R	E	C	O	V	R	E	C	O	V	R	E	C	O	V	R	E	C	O	V

2. Szenarien betreffend der Integrität (Integrity)

	SCHUTZ = 1					SCHUTZ = 2					SCHUTZ = 3					SCHUTZ = 4					SCHUTZ = 0				
V	4	3	3	3	3	4	3	3	3	3	4	3	3	3	3	4	3	3	3	4	4	3	3	3	3
E	3	2	2	2	2	3	2	2	2	2	3	2	2	2	2	3	2	2	3	4	3	2	2	2	2
R	2	1	1	1	1	2	1	1	1	1	2	1	1	2	2	2	1	2	3	4	2	1	1	1	1
S	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	1	1	2	3	4	1	1	1	1	1
		1	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4
		R	E	C	O	V	R	E	C	O	V	R	E	C	O	V	R	E	C	O	V	R	E	C	O	V

3. Szenarien betreffend der Vertraulichkeit (Confidentiality)

	SCHUTZ = 1					SCHUTZ = 2					SCHUTZ = 3					SCHUTZ = 4					SCHUTZ = 0				
V	4	3				4	3				4	3				4	3				4	3				
E	3	2				3	2				3	3				3	3				3	2				
R	2	1				2	2				2	3				2	3				2	1				
S	1	1				1	2				1	3				1	3				1	1				
		1					1					1					1					1				
		R	E	C	O	V	R	E	C	O	V	R	E	C	O	V	R	E	C	O	V	R	E	C	O	V

ANHANG 7: BESTIMMUNG VON SICHERHEITSANFORDERUNGEN

Nachdem der Ernst von Risikosituationen und die Ergebnisse des Sicherheitsaudits (Bewertung der bestehenden Maßnahmen[7]) bewertet wurde, ist es möglich, die Sicherheitsanforderungen in einer Bewertung des konsolidierten Bedarfs auszudrücken und nach ihrer Priorität zu ordnen.

Dieser Ansatz verwendet folgende Beschreibung der "Sicherheitsanforderungen":

Sicherheitsanforderungen

Eine Sicherheitsanforderung gemäß folgender Prinzipien ist für jedes Szenario definiert:

Sicherheitsanforderung für ein Szenario

Eine Sicherheitsmaßnahme kann Einfluss auf den Ernst eines Szenarios haben. **Ist dies der Fall, dann besteht eine Sicherheitsanforderung für die Maßnahmen dieses Szenarios**.

Quantitativ wird diese Anforderung wichtiger sein, da:

- ihr Einfluss (dargestellt durch den *Einflussfaktor*) für dieses Szenario hoch sein wird;
- der Ernst des Szenarios als hoch betrachtet werden kann;
- die bestehende Qualität der Maßnahme niedrig sein wird.

Daher kann bei einer Gegenüberstellung der Maßnahme *i* mit dem Szenario *k* die Sicherheitsanforderung mit folgender Formel berechnet werden:

$$BS_{ik} = e_{ik} . b^{G_k} . (4 - \sigma_i)$$

wobei:

BS_{ik}	=	Anforderung für Maßnahme *i* für Szenario *k*
e_{ik}	=	Koeffizient des Einflusses der Maßnahme *i* für Szenario *k*
b	=	Sensibilitätsparameter
G_k	=	Risikowert (Ernst) des Szenarios *k*
σ_i	=	Qualität der Maßnahme *i*

Der Koeffizient des Einflusses *e*, mit einem Wert zwischen 0 und 16, stellt den Grad des Einflusses der Sicherheitsmaßnahme auf das Szenario dar.

[7] Eine Maßnahme von MEHARI umfasst normalerweise einen größeren Bereich als ein ISO 27001 Kontrollziel.

Dies wird aus dieser von MEHARI zur Bewertung der Effektivität der verschiedenen Maßnahmenarten (abschreckend, vorbeugend, schützend, wiederherstellend oder abwälzend) zu einem Szenario verwendeten Formel abgeleitet.

Dieser Koeffizient wird mit folgender Formel errechnet:

$$e_{ik} = \alpha_{ik} \cdot \beta_{ik}$$

Wenn die Maßnahme nur durch eine Art referenziert wird, wird der Wert von σ_{ik} derart festgelegt:

- Ist die Maßnahme die einzige, die für die betrachtetet Art verwendet wird $\sigma_{ik} = 2$
- Ist die Maßnahme Teil einer Formel *min(serv_A; serv_B)* $\sigma_{ik} = 2$
- Ist die Maßnahme Teil einer Formel *max(serv_A; serv_B)* $\sigma_{ik} = 1$

Im Fall einer komplexen Formel wird nur die direkt auf die Sicherheitsmaßnahme referenzierende Funktion ("min" oder "max.") betrachtet.

Der Wert von σ_{ik} wird durch die Sicherheitsmaßnahme *i* bestimmt:
- ein abschreckender Einfluss auf das Szenario *k*, $\sigma_{ik} = 4$
- ein präventiver Einfluss auf das Szenario *k*, $\sigma_{ik} = 8$
- ein schützender Einfluss auf das Szenario *k*, $\sigma_{ik} = 4$
- ein wiederherstellender Einfluss auf das Szenario *k*, $\sigma_{ik} = 8$
- ein abwälzender Einfluss auf das Szenario *k*, $\sigma_{ik} = 2$

Wenn die Sicherheitsmaßnahme verschiedene Arten verwendet, werden alle Koeffizienten berechnet und der höchste Einflusswert wird verwendet.

Der Sensibilitätsparameter *β*, der zur Verankerung des Ernstes eines Szenarios verwendet wird, hat einen starken Einfluss auf das Endergebnis:

— ein Wert von 2 minimiert den Effekt eines Szenarios

— allgemein wird ein Wert von 8 (12) als gute Wahl angenommen.

Konsolidierung der Sicherheitsanforderungen

Die Konsolidierung der Sicherheitsanforderungen BS_i für die Maßnahme *i* wird mit der einfachen Formel bewertet:

$$BS_i = \sum_K BS_{ik}$$

Die so errechnetet Sicherheitsanforderung BS_i hat mehr Bedeutung, wenn die Maßnahme von mehreren Szenarien verwendet wird, diese ernst sind und die Maßnahme diesen Ernst beeinflussen kann.

Die Wahl zur Verbesserung einer Maßnahme kann jedoch im Gegensatz zur auf einer strategischen Ebene getroffen Auswahl von Maßnahmen der Organisation stehen (Definition in einer Sicherheitspolitik). MEHARI schlägt daher folgenden Ansatz vor:

- Sortiere die Szenarien derart, dass klar die stärksten globalen Anforderungen an die Sicherheitsmaßnahmen gezeigt werden;
- Analysiere, ob diese Sicherheitsmaßnahmen konsistent mit den Direktiven und Empfehlungen der globalen Sicherheitspolitik sind. Jede negative Antwort stellt zwangsläufig die Sicherheitspolitik in Frage.
- Ist eine Antwort positiv, bewerte den revidierten Qualitätslevel jeder Sicherheitsmaßnahme in Hinblick auf die bereits entschiedenen Verbesserungen (hinzufügen oder verändern von Abläufen und/oder Mechanismen);
- Schätze den sich ergebenden Risikowert und die neuen Sicherheitsanforderungen neu ein;
- Beginne von vorne!

Die Software RISICARE[8] enthält Automatismen, die diesem Prozess folgen.

[8] RISICARE ist ein Produkt von BUC S.A.