

# Ontologiebasiertes IT Risikomanagement

Andreas Ekelhart<sup>1</sup> · Stefan Fenz<sup>2</sup> · Thomas Neubauer<sup>1</sup>

<sup>1</sup>Secure Business Austria  
ekelhart@securityresearch.ac.at  
neubauer@securityresearch.ac.at

<sup>2</sup>Technische Universität Wien  
fenz@ifs.tuwien.ac.at

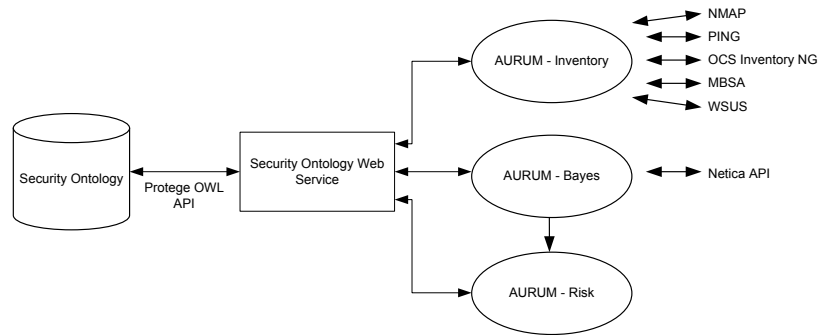
## Zusammenfassung

Informationssicherheitsrisikomanagement (Information Security Risk Management, ISRM) stellt einen effizienten Zugang zur Bewertung, Verringerung und Evaluierung von Informationssicherheitsrisiken dar. Bereits bestehende ISRM-Ansätze sind weitgehend akzeptiert, setzen jedoch sehr detailliertes Informationssicherheitswissen und genaue Kenntnisse des tatsächlichen Unternehmensumfeldes voraus. Die inadäquate Umsetzung von ISRM gefährdet die planmäßige Umsetzung der Unternehmensstrategie und kann zu einer Minderung des Unternehmenswertes führen. Der vorliegende Beitrag präsentiert das AURUM Tool, welches die Schwachstellen bestehender Ansätze adressiert und Entscheidungsträger bei der Auswahl eines effizienten IT-Sicherheitsportfolios unter Berücksichtigung organisationsspezifischer, technischer und wirtschaftlicher Anforderungen unterstützt.

## 1 Einführung

Unternehmen verstärken laufend ihre IT-Sicherheitsinvestitionen. So betragen im Jahr 2005 die weltweiten Einnahmen der Lieferanten von IT-Sicherheitsprodukten und -dienstleistungen \$21.1 Milliarden. Obwohl Unternehmen Sicherheit als eines der wichtigsten Ziele erachten, ist einer Vielzahl von Organisationen nicht bekannt wie hoch ihre Investitionen in Informationssicherheit tatsächlich sind bzw. ob diese Investitionen die gewünschte Wirkung zeigen. ISRM ist für die Gewährleistung langfristiger geschäftlicher Erfolge ausschlaggebend, da es einen effizienten Ansatz zur Verfügung stellt, um Sicherheitsmaßnahmen zu bewerten.

Bereits bestehende ISRM-Ansätze und deren Toolimplementierungen (z.B. CRAMM [Far91], NIST SP 800-30 [SGF02], OCTAVE [ADSW03], EBIOS [DCS04] und kürzlich ISO 27005 [ISO07]) erfordern, insbesondere in der Phase der Risikobewertung und -verminderung, sehr detailliertes Wissen sowohl auf dem Gebiet der IT-Sicherheit als auch bezüglich der tatsächlichen Unternehmensumgebung. Bis zu diesem Zeitpunkt greifen Unternehmen bei der Ausführung von Risikobewertung und -verminderung meistens auf Best-Practice-Guidelines, Informationssicherheitsstandards oder Expertenwissen zurück. Die Verwendung dieser Ansätze ist mit mehreren Problemen verbunden: (1) Best-Practice-Guidelines (z.B. [BSI08] und [DCS04]) stellen ausgezeichnetes Wissen über potentielle Bedrohungen, Schwachstellen und Gegen-



**Abb. 1:** AURUM-Architektur

maßnahmen zur Verfügung. Ein Unternehmen ist jedoch ohne einen Experten in der Regel nicht in der Lage, die komplexen Beziehungen zwischen den IT-Sicherheitskonzepten zu berücksichtigen. Dies resultiert in einem fragmentarischen, das Unternehmen gefährdenden IT-Sicherheitsansatz [Vit86] [BM99] [JHS99] [BW07]; (2) um zu untersuchen, welche konkreten Infrastrukturelemente durch bestimmte Bedrohungen gefährdet sind, müssen Unternehmen manuell das Wissen aus den Best-Practice-Guidelines auf ihre tatsächliche Infrastruktur übertragen [Bas93]; (3) insbesondere Informationssicherheitsstandards wie z.B. ISO 27001 [ISO05] konstatieren nur sehr abstrakte Vorschläge zur Ausführung von Risikoverminderungen, konkrete Gegenmaßnahmen oder mögliche Kombinationen fehlen meistens [BRT07] und (4) die Festlegung von möglichen Bedrohungen basiert meistens auf subjektiven Wahrnehmungen anstatt objektiver Evaluierung [Fro97] [BRT07].

Der in diesem Beitrag vorgestellte AURUM<sup>1</sup> Prototyp wurde entwickelt, um die oben angeführten Probleme zu adressieren. Die theoretischen Grundlagen basieren auf früheren Arbeiten (vgl. [EFKW07, EFGW07, EFNW07, NEF08] bzgl. Sicherheitsontologie und [NS07] bzgl. interaktiver Entscheidungsunterstützung).

## 2 AURUM

Dieser Abschnitt erläutert wie die allgemeinen ISRM-Phasen von AURUM und dessen User Interface unterstützt werden. AURUM wurde entwickelt, um die notwendige Interaktion zwischen Benutzer und System zu minimieren und den Entscheidungsträgern eine intuitive Lösung zur Verfügung zu stellen, die ohne weitreichendes Wissen auf dem Gebiet der Informationssicherheit angewandt werden kann. Allerdings ist AURUM auch in der Lage, professionelle Benutzer auf unterschiedlichen Ebenen mit detaillierten Informationen zu versorgen. Abbildung 1 zeigt die AURUM Architektur.

Die Security Ontology versorgt jedes AURUM-Modul mit detailliertem Informationssicherheitswissen sowie dem spezifischen Sicherheitsstatus des betrachteten Unternehmens. Die Security Ontology ist in der Web Ontology Language (OWL) kodiert [W3C04] und Protege [SCB07] wird zur Modifikation der Ontologie verwendet. Das Security Ontology Webservice agiert als Schnittstelle zwischen den AURUM-Modulen und der Security Ontology. Das AURUM-Modul *Inventory* nutzt Bestände und Netzwerk-Scanning-Lösungen von Dritten, um die Phase der Systemcharakterisierung zu unterstützen. C# und Microsoft .NET Framework

<sup>1</sup> abgeleitet von *AUtomated Risk and Utility Management* (gemäß <http://wordnet.princeton.edu> definieren wir "Utility" als eine Größe, die in jeder entscheidungsbehafteten Situation maximiert werden kann)

3.5 wurden verwendet, um das AURUM-Modul *Bayes* zu implementieren. Es greift auf die Norsys Netica API<sup>2</sup> zurück, um das Bayesianische Netzwerk hinsichtlich der Bestimmung von möglichen Bedrohungen zu generieren und zu modifizieren. Das AURUM-Modul *Risk* ist das zentrale Modul, welches zusammen mit dem Bayes-Modul und dem Security Ontology Webservice die Risikostufe für die zuvor definierten Ressourcen berechnet. Dies geschieht durch Sammeln von Wahrscheinlichkeitswerten aus dem Bayesianischen Netzwerk und deren Multiplikation mit den für die Ressourcen definierten Wichtigkeitswerten, welche in der Ontologie hinterlegt sind.

Abbildung 2 zeigt das Layout der AURUM Arbeitsoberfläche. Der linke Bereich zeigt Informationen zu (a) den Geschäftsprozessen und ihrer Ressourcenabhängigkeit, und (b) den physischen Standorten der Ressourcen im Unternehmen an. Der mittlere Hauptanzeigebereich zeigt dem Entscheidungsträger (a) detaillierte Information über die ausgewählte Ressource, (b) eine graphische Darstellung der ausgewählten Geschäftsprozesse zusammen mit den Ressourcen, die für die Ausführung dieser gewählten Geschäftsprozesse benötigt werden und (c) eine graphische Darstellung der physischen Standorte der Ressourcen. Die im Hauptanzeigebereich zur Verfügung gestellten Informationen hängen von der Auswahl ab, welche der Entscheidungsträger im linken Bereich getroffen hat (dasselbe gilt analog für die Abhängigkeit zwischen mittleren und rechten Bereich). Der rechte Bereich zeigt (a) die Risikostufe für die gewählten Ressourcen, (b) eine Liste der Bedrohungen inkl. deren Wahrscheinlichkeit und (c) implementierte und nicht implementierte Controls und die dazu berechneten Effektivitätskennzahlen an.

## 2.1 Systembeschreibung

AURUM basiert auf einer Security Ontology, die ein höchst ausdifferenziertes Infrastrukturmodell zur Verfügung stellt. Die Basisversion dieser Ontologie bietet dem Benutzer eine umfassende Informationssicherheitswissensbasis. Eine Organisation, die sich dafür entscheidet, die Security Ontology als Basis für das ISRM zu verwenden, muss die Ontologie einmalig mit spezifischen Unternehmensinformationen initialisieren. Diese Phase wird vom AURUM-Modul *Inventory* unterstützt, welches automatisch Software-Daten und Elemente der IT-Infrastruktur erfasst (für eine detaillierte Beschreibung siehe [EFNW07]). Dies ermöglicht es uns, die Effizienz auf der Stufe der Systemcharakterisierung zu steigern, da die Bestandsaufnahme der IT-Strukturelemente ein besonders arbeitsintensiver Schritt ist. AURUM bietet folgende zwei Optionen an, um Informationen bzgl. der Unternehmensressourcen zu erfassen:

- **Prozessmodell:** AURUM verwendet Geschäftsprozessmodelle zur Identifikation von unternehmerischen Risiken. Durch Auswählen eines Prozesses stellt das Tool im mittleren Bereich des User Interfaces eine graphische Repräsentation des Prozesses zur Verfügung. Zusätzlich werden alle für die Ausführung dieses Prozesses benötigten Ressourcen dargestellt. Sobald der Benutzer eine dieser Ressourcen auswählt, zeigt AURUM im rechten Bereich weitere Informationen über Bedrohungen, Schwachstellen, Risikostufen und mögliche Controls an (vgl. Abschnitt 2.2) (vgl. Abbildung 2). Um auch Unternehmen zu unterstützen, die bereits Tools zur Modellierung von Geschäftsprozessen nutzen, werden Importfunktionen (z.B. für Adonis oder ARIS) verwendet.
- **Physisches Modell:** Basierend auf den in der Security Ontology gespeicherten Daten, ermöglicht AURUM die Generierung eines physischen Infrastrukturmodells. Dieses Modell kann genutzt werden, um der Ontologie Ressourcen hinzuzufügen und verschiedene

---

<sup>2</sup> Netica API: [www.norsys.com/netica\\_api.html](http://www.norsys.com/netica_api.html)

Szenarien zu simulieren (z.B. zur Identifikation der optimalen Lage bzgl. einer wertvollen Ressourcen). Der linke Bereich des User Interfaces gibt einen Überblick über die Ressourcen und deren physischen Standorte. Durch Auswahl einer dieser Ressourcen zeigt AURUM eine graphische Repräsentation der Ressourcenstandorte und der angebotenen Geschäftsprozesse an. In Analogie zum Prozessmodell werden durch Auswahl einer Ressource dem Benutzer im rechten Bereich des User Interfaces weitere Informationen zu relevanten Bedrohungen, Risikostufen und möglichen Controls angezeigt (vgl. Abschnitt 2.2) (vgl. Abbildung 2).

## 2.2 Bewertung von Bedrohungen und Schwachstellen

Im Gegensatz zu bestehenden Tools unterstützt AURUM die Entscheidungsträger bei der Beantwortung folgender Fragen: Welche Bedrohungen bestehen für kritische Ressourcen? Welche Bedrohung fungiert als Multiplikator (d.h. welche Bedrohung hat andere Bedrohungen zur Folge)? Welche Schwachstellen müssen von einer Bedrohung ausgenutzt werden, um wirksam zu sein?

Der Bedrohungsbaum (platziert im rechten Bereich des User Interfaces) zeigt die möglichen Gefährdungen für die ausgewählte Ressource, einschließlich eventueller A Priori - Bedrohungswahrscheinlichkeiten und unternehmensspezifischen Angreiferprofilen. Durch Auswählen einer Bedrohungen aus dem dargestellten Baum wird wertvolle Information wie die Beschreibung von Bedrohungen angezeigt. Darüber hinaus werden die betroffenen Sicherheitsattribute (Vertraulichkeit, Integrität und Verfügbarkeit) zur Verfügung gestellt. Zusätzlich kann eine Bedrohung die Konsequenz aus anderen Bedrohungen sein (z.B. unautorisierter physischer Zugriff kann das Resultat einer fehlenden Schlüsselverwaltung sein) und kann selbst wiederum neue Bedrohungen nach sich ziehen (z.B. unautorisierter physischer Zugriff hat die Offenlegung von Daten zur Folge). Hier ist zu bedenken, dass in diesem Schritt dem Risikomanager nur jene Bedrohungen angezeigt werden, die für das Unternehmen und die berücksichtigte Ressource relevant sind. In der Ontologie wurden für jede Bedrohung sehr detailliert Schwachstellen definiert und modelliert. Die Präsentation der Schwachstellen wird durch deren Beschreibung ergänzt. Jeder Schwachstelle ist ein Control zugeteilt, deren Implementierung die Schwachstelle schließt. Um das Verständnis zu erhöhen, wird jedes Control durch eine Beschreibung ergänzt. Durch den Einsatz dieser Funktionen weiss ein Benutzer genau, wie er sein Unternehmen vor spezifischen Bedrohungen schützen kann: Entschärfung von Schwachstellen durch Einsetzen der empfohlenen Controls.

Bis zu diesem Punkt hat der Entscheidungsträger von dem beobachteten System, den potentiellen Bedrohungen und den entsprechenden Schwachstellen, die es den Bedrohungen gestatten, wirksam zu werden, Kenntnis. Bei der Analyse der Controls legt das System fest, welche Controls (entweder technische wie Verschlüsselungsmechanismen oder nicht-technische wie Sicherheitsregeln) bereits etabliert sind, und welche Controls existieren, um die Möglichkeit, dass bestimmte Schwachstellen von einer Bedrohung ausgenutzt werden, zu verringern (z.B. die Bedrohung *unautorisierter physischer Zugriff* nützt die Schwachstelle *keine Kontrolle der Zugangsbedingungen* aus, die durch Installation eines Kontrollpunkts am Eingang, Wachleute oder eine Zugangssystem entschärft werden kann).

Jedes Control beinhaltet eine formelle Beschreibung seiner Implementierung. Die zugrundeliegenden formellen Beschreibungen der Controls können als Regeln in einer konkret modellierten Unternehmensumgebung umgesetzt werden, um zu identifizieren, welche Ressourcen

der Einhaltung unterliegen. Die passenden Ressourcen können mittels des Standort-Modells angezeigt werden (vgl. Abschnitt 2.1). Meistens ist das Wissen, ob ein bestimmtes Control in einem gegebenen Kontext implementiert ist oder nicht, nicht ausreichend. Die wichtigste Information ist, ob das implementierte Control zum Erreichen einer für das beobachtete Ressource akzeptablen Risikostufe geeignet ist oder nicht. Da zur Bestimmung der Risikostufe neben der Wahrscheinlichkeit auch die möglichen Konsequenzen einer Bedrohung gefordert sind, wird jede Ressource aufgrund seiner Bedeutung hinsichtlich der Kriterien Vertraulichkeit, Integrität und Verfügbarkeit bewertet.

## 2.3 Risikobestimmung

Diese Phase umfasst die Bestimmung der Wahrscheinlichkeit, mit der Bedrohungen bestimmte Schwachstellen in einem gegebenen System ausnutzen. Die darauf folgende Analyse der Konsequenzen legt fest, wie die Performance eines Unternehmens beeinflusst wird, falls eine Bedrohung erfolgreich eine bestimmte Schwachstelle ausnützt. Durch die Kombination der Wahrscheinlichkeit einer Bedrohung mit dem Umfang der Konsequenzen kann das Unternehmen die Risikostufe bestimmen und somit die notwendigen Schritte setzen. Im Gegensatz zu anderen Ansätzen (vgl. [SGF02, Sta07]) fokussiert AURUM auf eine automatisierte Unterstützung, wobei die entwickelte Wissensbasis und die darin definierten Beziehungen genutzt werden.

Abbildung 2 zeigt die AURUM-Schnittstelle, die den Risikomanager in der Phase der Risikobestimmung unterstützt. Die exemplarische Bestimmung der Bedrohungseintrittswahrscheinlichkeit wird für das Element *ent:SBACustomerData* durchgeführt und repräsentiert die Kundendaten eines Unternehmens XYZ. Zur Bestimmung der Bedrohungseintrittswahrscheinlichkeit wird basierend auf der Security Ontology ein Bayesianisches Netzwerk generiert. Baumdiagramme werden benutzt, um dieses komplexe Netzwerk in einer verständlichen Form zu visualisieren (siehe den oberen rechten Abschnitt in Abbildung 2). Da *ent:SBACustomerData* ein Datenelement repräsentiert, tritt es drei verschiedenen Risiken gegenüber → Offenlegung von Daten, Datenverlust und Datenmanipulation. Jedes Risiko ist das Produkt einer Bewertung der Wichtigkeit einer Ressource und der Wahrscheinlichkeit der entsprechenden Bedrohung. Die Möglichkeit einer Bedrohung wird anhand der Wahrscheinlichkeit der vorangehenden Bedrohungen, der wahrscheinlichen Ausnutzung der entsprechenden Schwachstellen, der Effektivität der bestehenden Control-Implementierungen, der a priori Bedrohungswahrscheinlichkeit und der Leistungsfähigkeit des Angreifers bestimmt. Da die eingegebenen Werte für bestehende Control-Implementierungen, a priori Wahrscheinlichkeit und die Leistungsfähigkeit des Angreifers von der betrachteten Ressource abhängen, untersucht dieser Abschnitt, wie AURUM die eingegebenen Werte für *ent:SBACustomerData* im Kontext eines drohenden Datenverlustes bestimmt.

Der Ressourcen-Risikobaum in Abbildung 2 zeigt drei verschiedene Typen von Schwachstellen: (1) technisch - kein Virenschanner, (2) physisch - keine Zugangskontrolle und (3) organisatorisch - keine Backup-Strategie.

Um die Möglichkeit zur Ausnutzung der Schwachstelle "kein Virenschanner" zu bestimmen, überprüfen Algorithmen, ob Virenschutzprogramme auf dem Fileserver, auf dem die Kundendaten von XYZ gespeichert sind, installiert sind. Das physische Modell im linken Abschnitt der Benutzeroberfläche zeigt, dass der Virenschanner Ikarus Defender auf dem Fileserver installiert ist. Somit schützt der Virenschanner den Fileserver und die Kundendaten von XYZ vor einem Befall durch bösartige Software und schließt die Sicherheitslücke "kein Virenschanner". Der grüne

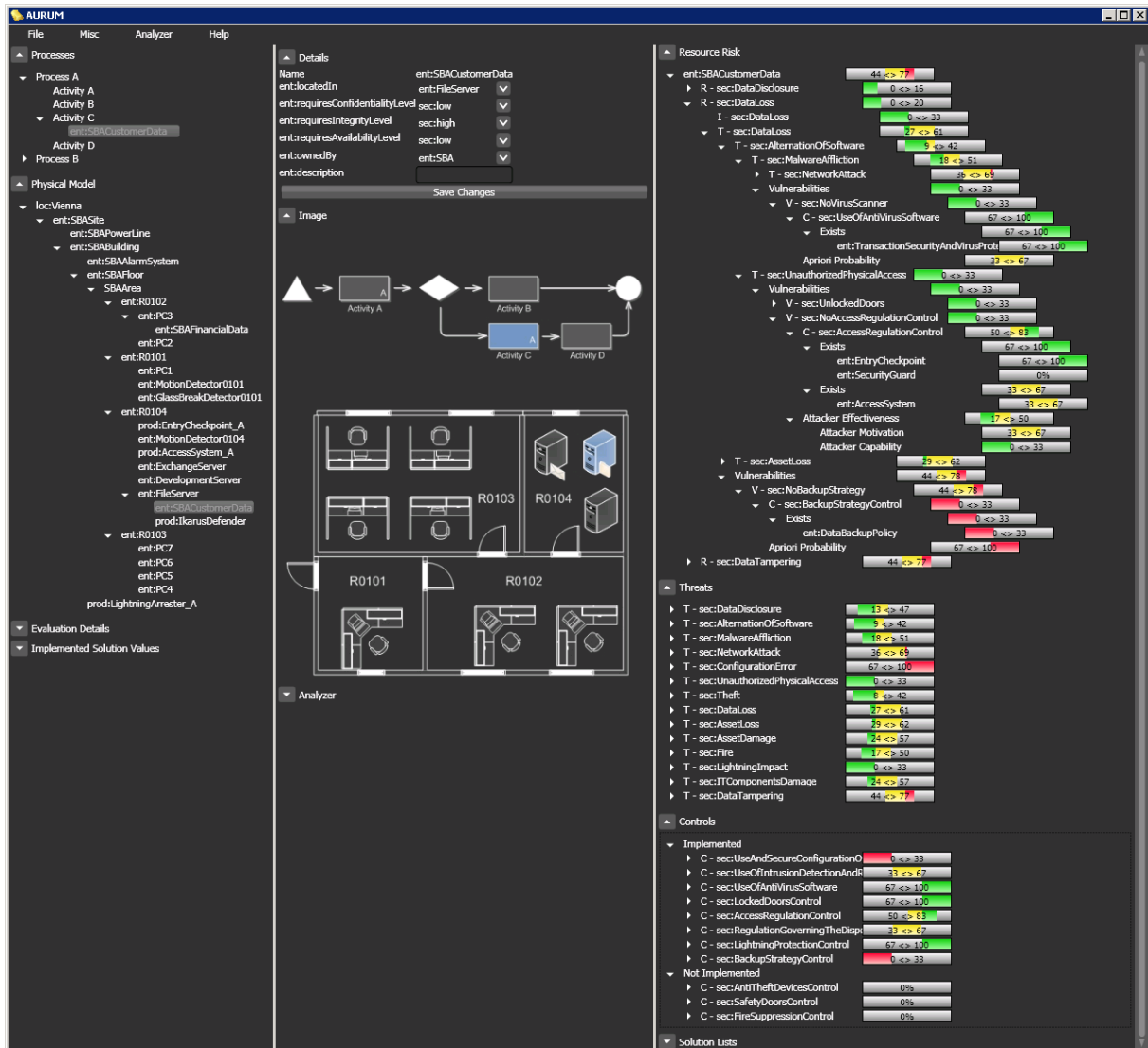


Abb. 2: AURUM-Benutzeroberfläche - Risikobestimmung

Balken der Transaktionssicherheit und des Virenschutz-Knotens zeigt an, dass der Virens Scanner Ikarus Defender effizient arbeitet und die entsprechende Schwachstelle verringert.

Die Wahrscheinlichkeit zur Ausnutzung der Schwachstelle "keine regulierende Zugangskontrolle" wird durch die Wirksamkeit eines Zugangssystems, eines Eingangskontrollpunkts oder Wachmanns und die Leistungsfähigkeit des Angreifers festgelegt. Da die Schwachstelle "keine regulierende Zugangskontrolle" auf der Raumebene (*sec:vulnerabilityOn*) liegt, überprüfen Algorithmen, ob die erforderlichen Controls im Raum *ent:R0104* (der physische Standort des Fileservers) implementiert sind. Wie das physische Modell im linken Bereich der Abbildung 2 zeigt, ist der effiziente *EntryCheckpoint\_A* und das durchschnittlich effiziente *AccessSystem\_A* im Serverraum *ent:R0104* platziert. Da der Angreifer mit einer Leistungsfähigkeit von 17 - 50% und die Controls mit jeweils 33 - 67% und 67 - 100% bewertet sind, wird die Schwachstelle "keine regulierende Zugangskontrollen" auf 0 - 33% Ausnutzungswahrscheinlichkeit verringert.

Die Schwachstelle "keine Backup-Strategie" repräsentiert eine organisatorische Lücke, wodurch die Wahrscheinlichkeit der Ausnutzung anhand einer angemessenen Regelung bestimmt wird. Da die Richtlinien auf der organisatorischen Ebene implementiert werden, kontrollieren logische Algorithmen, ob für das den Fileserver besitzende Unternehmen eine Regelung zum Daten-Backup implementiert ist. XYZ implementierte eine wenig effektive Backup-Regelung, die unter anderem die Daten des Fileservers abdeckt. Aufgrund der hohen a priori Wahrscheinlichkeit eines drohenden Datenverlustes, verringert die wenig effektive Backup-Regelung von XYZ die Ausnutzungswahrscheinlichkeit für die Schwachstelle "keine Backup-Strategie" auf 44 - 78%.

Während der Ressourcen-Risikobaum verständlich die Kalkulation der Bedrohungseintrittswahrscheinlichkeit repräsentiert, könnte er den Benutzer durch die komplexe Darstellung verwirren. Daher zeigt der Überblick über die Bedrohungen im mittleren rechten Abschnitt der Benutzeroberfläche die relevanten Bedrohung und deren Wahrscheinlichkeit. Möchte der Benutzer die Wahrscheinlichkeit einer bestimmten Bedrohung reduzieren, müssen die im unteren rechten Abschnitt gezeigten Controls implementiert werden. Im Fall der XYZ-Kundendaten empfiehlt AURUM für den Fileserver unter anderem die Implementierung einer Anti-Diebstahl-Sicherung sowie einer Sicherheitstür und einer Feuerlöschanlage für den Serverraum.

Aufgrund der Hierarchie der Bedrohungseintrittswahrscheinlichkeiten im Bayesianischen Netzwerk beeinflussen Controls auf verschiedenen Ebenen in unterschiedlicher Intensität die endgültige Bedrohungseintrittswahrscheinlichkeit. AURUM unterstützt den Benutzer mit Richtwerten zu jeder in einem spezifischen Bedrohungskontext erfolgenden Control Implementierung. Für den Fall von Datenverlust wurden von AURUM folgende Werte festgelegt: Richtlinien zum Daten-Backup (0.1666), Regeln bezüglich abgesperrter Türen (0.0763), Zugangssystem (0.0509), Kontrollpunkt beim Eingang oder Sicherheitspersonal (0.0509), Transaktionssicherheit und Virenschutzprogramme (0.0416), Anti-Diebstahl-Sicherungen (0.0277), Überspannungsschutz (0.0138), Sicherheitstür (0.0046) und Feuerlöscher (0.0046). Aufgrund dieser Resultate wird ein Benutzer, um die Kundendaten von XYZ zu schützen, eher solide Backup-Richtlinien implementieren anstatt viel Geld in eine teure Sicherheitstür zu investieren.

Als Beispiel wird folgendes Szenario angenommen: Neben anderen Controls sind die XYZ-Kundendaten durch eine gering wirksame Sicherheitstür und eine wenig effektive Daten-Backup-Regelung geschützt, was hinsichtlich eines Datenverlusts eine Bedrohungseintrittswahrscheinlichkeit von 31 - 64% ergibt. Um die Möglichkeit eines Verlusts wertvoller Kun-

dendaten zu verringern, ist der Risikomanager gezwungen, effektivere Maßnahmen zu implementieren. Die zuvor erwähnten Richtwerte der relevanten Controls haben gezeigt, dass der Risikomanager die Implementierung verlässlicher Richtlinien für Daten-Backup der Investition in eine Sicherheitstüre vorziehen sollte. Die Bestimmung der Bedrohungseintrittswahrscheinlichkeit mit Hilfe der entwickelten Bayesiansischen Netzwerke bestätigt diese Empfehlungen. Werden eine sehr wirksame Sicherheitstür und wenig effektive Richtlinien für Daten-Backup in das Bayesianische Netzwerk eingegeben, sinkt die Wahrscheinlichkeit eines drohenden Datenverlusts um 1% auf 30 - 63%. Werden eine wenig wirksame Sicherheitstür aber hocheffektive Richtlinien für Daten-Backup eingesetzt, verringert sich die Wahrscheinlichkeit eines drohenden Datenverlusts um 15% auf 16 - 49%. Die folgende Kombination bestätigt den geringen Einfluss einer Sicherheitstür auf die Wahrscheinlichkeit eines drohenden Datenverlusts: Wird neben den Richtlinien für Daten-Backup auch die Sicherheitstür als hocheffektiv eingestuft, resultiert dies ebenfalls in einer Bedrohungswahrscheinlichkeit von 16 - 49%.

## 2.4 Evaluierung und Implementierung von Controls

Dieser Schritt umfasst die Identifizierung und Evaluierung von Controls oder deren Kombinationen hinsichtlich des Kosten-Nutzen-Verhältnisses. Daraus resultierend können jene Controls, die geeignet sind, um das Risiko bei möglichst geringen Kosten auf ein akzeptables Niveau zu senken, in den Implementierungsplan aufgenommen werden. An diesem Punkt weiß das Management, welche Risiken für das Unternehmen nicht akzeptabel und folglich welche Maßnahmen zu treffen sind (d.h. in Bezug auf die Controls, welche die identifizierten Risiken verringern oder eliminieren können). Für jede Schwachstelle werden geeignete Controls identifiziert, basierend auf den Best-Practice-Standards. Durch Anbieten dieser Controls werden Entscheidungsträger mit effizienten Gegenmaßnahmen versehen, um die Risikostufe zu senken und somit ihr Unternehmen zu schützen. Da die Controls nur Informationen bezüglich der einzusetzenden Sicherungsmaßnahmen anbieten können (z.B. Feuerlöscher), müssen Instanzen identifiziert werden, die letztendlich in das Unternehmen implementiert werden können. Demzufolge werden potentielle Controls anhand definierter Ressourcen- und Nutzenkategorien evaluiert (z.B. Kosten, Wirksamkeit, Verlässlichkeit), um die unternehmensspezifischen Geschäftsbedürfnisse, übereinstimmend mit ökonomischen Anforderung, präzise anzupeilen. Diese Analyse berücksichtigt Kosten und Nutzen nicht nur in monetärer Hinsicht, sondern inkludiert auch nicht-finanzielle Zielsetzungen. Alle identifizierten potentiellen Controls werden an den gewählten Kriterien und anhand der Daten aus der Security Ontology bewertet. Unter Verwendung der potentiellen Controls und ihrer Bewertungen je Kategorie als Input werden alle Pareto-effizienten Kombinationen von Sicherheitsmaßnahmen bestimmt (d.h. es gibt keine Lösung mit gleich guten oder besseren Werten in allen Zielsetzungen und einem grundsätzlich besseren Wert in zumindest einer Zielsetzung). Alle berücksichtigten Lösungsansätze müssen in Hinsicht auf zwei Beschränkungen durchführbar sein: Das erste Set bezieht sich auf limitierte Ressourcen (z.B. Entwicklungs- oder Erhaltungskosten). Das zweite Set stellt sicher, das bestenfalls ein Maximum – oder zumindest ein Minimum – an Sicherheitsmaßnahmen von den gegebenen Subsets (z.B. von einem bestimmten Typ an Sicherheitsmaßnahmen wie Firewalls) in die realisierbaren Lösungen einbezogen werden.

AURUM stellt eine interaktive Benutzeroberfläche zur Verfügung, die dem Entscheidungsträger Informationen zu einem spezifischen Auswahl-Problem anbietet, während das System sicherstellt, dass die finale Lösung die wirksamste ist. Die Entscheidungsträger lernen über die Konsequenzen ihrer Entscheidungen und bekommen Informationen über den Unterschied (in jeder



Abb. 3: AURUM Auswahl und Evaluierung der Controls

Kategorie) zwischen der bestehenden Lösung und den potentiellen Lösungen.

Wir benutzen eine Prozedur, die von einem effizienten Portfolio ausgeht und dem Entscheidungsträger gestattet, sich im Lösungsraum zu attraktiveren Alternativen iterativ zu "bewegen" bis ein "besseres" Portfolio gefunden wurde. Unser Ansatz basiert auf interaktiven Modifikationen der unteren und oberen Grenzen für eine oder mehrere Zielsetzungen. Die Zielsetzungen werden durch Ressourcen- und Nutzenkategorien repräsentiert und mit Hilfe von Balken in AURUM visualisiert (vgl. den *Analyzer* Abschnitt in Abbildung 3). Zwei bewegliche horizontale Linien mit kleinen Pfeilen auf der einen Seite repräsentieren die unteren und oberen Begrenzungen und sollen dazu dienen, das Set an verbleibenden Lösungen Schritt für Schritt zu beschränken (z.B. indem die Minimalbegrenzung in einer der Zielsetzungen angehoben wird) oder zu erweitern (z.B. indem manche Begrenzungen erneut gelockert werden), entsprechend den Präferenzen des Entscheidungsträgers. In all diesen Fällen bietet das System unmittelbares Feedback über die Folgen solcher Entscheidungen, d.h. die verbleibenden Alternativen, an. Momentan haben wir AURUM folgende Kategorien hinzugefügt: Wirksamkeit, Gewichtung (Einfluss auf die entsprechende Bedrohungseintrittswahrscheinlichkeit), Anschaffungs- und laufende Kosten. Wir führen das Beispiel mit den XYZ-Kundendaten weiter und identifizieren die Bedrohung mit der höchsten Wahrscheinlichkeit, nämlich *T - sec:Datenmanipulation* mit einer Wahrscheinlichkeit von 44 - 77%. Das Management sollte dieser Bedrohung als erstes begegnen, um das Gesamtrisiko zu reduzieren, daher starten wir mit der Kalkulation des bestehenden Sicherheitsportfolios (vgl. Abbildung 3). Für jede Kontroll-Klasse (z.B. *Anti-Viren-Software*) können konkrete Produkte der ontologischen Wissensbasis hinzugefügt werden. Ein Start-Set an Produkten wurde bereits erstellt, kann aber leicht von den Unternehmen, die dieses Tool verwenden, adaptiert und erweitert werden. Der Leser sollte beachten, dass zu Demonstrationszwecken Beispielinstanzen wie *Zugangskontrolle A* und *VerschlusseneTürenRegelung A* hinzugefügt wurden. Das AURUM-Tool findet zu Beginn 150 mögliche Lösungen, indem konkrete Control-Implementierungen kombiniert werden. Im nächsten Schritt setzt der Ent-

scheidungsträger seine vorgegebenen Einschränkungen/Präferenzen ein: In unserem Beispiel gehen wir von beschränkten finanziellen Mittel aus und legen somit die maximalen Anschaffungskosten mit 9.800 und maximalen laufenden Kosten mit 1.000 fest (vergleiche die orangenen "InitialCosts"- und "RunningCosts"-Balken und die oberen roten Linien, die unsere finanziellen Präferenzen anzeigen). Zusätzlich fordern wir zumindest eine durchschnittliche Wirksamkeit des erwägten Portfolios (vergleiche die grünen "Effectiveness"-Balken und die untere rote Linie). Jedes Portfolio wird von einem vertikalen Balken repräsentiert; wie zu sehen ist, bleiben nur 6 Portfolios über, die unsere Anforderungen erfüllen. In Abschnitt 3 wird uns eine Liste an Lösungen zur Verfügung gestellt, die detaillierte Informationen über die verbleibenden Lösungen enthält, einschließlich der exakten Abbildung der Kategoriewerte und der Kandidaten. Zum Beispiel erfordert das ausgewählte Portfolio mit der ID 8332 eine Systemsoftware zur Erkennung von Eindringlingen der Type C, das Antivirenprogramm IkarusDefender, eine Regelung der Type A bezüglich abgeschlossener Türen und einen Zugangskontrollpunkt der Type A. Dieses Portfolio bietet entlang unserer Einschränkungen die größte Wirksamkeit, hat aber höhere Anschaffungs- und laufenden Kosten als andere Lösungen.

In weiteren Iterationen spielt der Entscheidungsträger weiter minimale und maximale Begrenzungen durch, wobei er auf diese Art Erfahrungen bezüglich der Konsequenzen seiner Entscheidungen sammelt. Nach mehreren Zyklen des Einschränkens und Lockerns der Sets von Möglichkeiten wird der Entscheidungsträger schließlich zu einer Lösungsalternative kommen, die einen individuell zufriedenstellenden Kompromiss zwischen den relevanten Zielsetzungen bietet. Man beachte, dass er weder explizite Gewichtungen noch die Form seiner Präferenzfunktion spezifizieren muss oder in irgendeinem Stadium des Verfahrens darzulegen hat, um wie viel die eine Lösung besser ist als eine andere. Stattdessen wird ihm umfangreiche Information zur spezifischen Auswahl zur Verfügung gestellt und das System garantiert, dass die endgültige Lösung die optimale sein wird (d.h. Pareto-effizient), ohne dass eine andere realisierbare Lösung existiert, die von einem objektiven Standpunkt aus "besser" wäre.

### 3 Conclusio

Dieser Beitrag präsentiert das AURUM-Tool, welches sich im Vergleich zu bestehenden Ansätzen durch folgende Eigenschaften auszeichnet: (1) Die ontologische Wissensbasis stellt sicher, dass das Informationssicherheitswissen dem Risikomanager in konsistenter und verständlicher Weise zur Verfügung gestellt wird, (2) das Abbilden von Unternehmensressourcen in unserem ontologischen System garantiert, dass die Ressourcen auf konsistente Art modelliert werden, (3) die Integration bestehender Best-Practice-Guidelines und Informationssicherheitsstandards stellt sicher, dass nur weithin anerkanntes Informationssicherheitswissen für die Identifikation von Bedrohungen/Schwachstellen und Empfehlungen von Controls verwendet wird, (4) die vorgeschlagene Bayesianische Bestimmung von Bedrohungseintrittswahrscheinlichkeit garantiert, dass die Einschätzung der Bedrohungseintrittswahrscheinlichkeit auf einem objektiveren Niveau erfolgt, (6) Controls zur Verminderung des Risikos werden automatisch angeboten, (7) die Verwendung der interaktiven Entscheidungsunterstützung erlaubt Entscheidungsträgern (z.B. dem Risikomanager), verschiedene Szenarien durchzuspielen und so über die Merkmale des zugrunde liegenden Problems Erfahrungen zu sammeln während das System garantiert, dass nur effiziente Lösungen ausgewählt werden können und (8) durch das Abwägen mehrerer Zielsetzungen und der angebotenen Analyse der Unterschiede unterstützen wir Entscheidungsträger dabei, ein besseres "Gefühl" für das Problem, im Sinne von was mit verschiedenen Zielsetzungen zu welchem "Preis" erreicht werden kann, zu bekommen.

## 4 Danksagung

Diese Arbeit wurde vom Bundesministerium für Wirtschaft und Arbeit (BMWA), der Stadt Wien sowie der FIT-IT Forschungsinitiative Trust in IT Systems (Fördervertrag 813701) gefördert und im Rahmen des Kompetenzzentrums Secure Business Austria durchgeführt.

## Literatur

- [ADSW03] Christopher Alberts, Audree Dorofee, James Stevens, and Carol Woody. Introduction to the OCTAVE approach. Technical report, Carnegie Mellon - Software Engineering Institute, Pittsburgh, PA 15213-3890, August 2003.
- [Bas93] Richard Baskerville. Information systems security design methods: Implications for information systems development. *ACM Computing Surveys*, 25(4):375–414, December 1993.
- [BM99] Kakoli Bandyopadhyay and Peter P. Mykytyn. A framework for integrated risk management in information technology. *Management Decision*, 37(5/6):437–444, 1999.
- [BRT07] Wade H. Baker, Loren Paul Rees, and Peter S. Tippet. Necessary measures: metric-driven information security risk assessment and decision making. *Communications of the ACM*, 50(10):101–106, 2007.
- [BSI08] BSI. IT Grundschutz Catalogues, 2008.
- [BW07] Wade H. Baker and Linda Wallace. Is information security under control?: Investigating quality in information security management. *IEEE Security and Privacy*, 5(1):36–44, 2007.
- [DCS04] DCSSI. Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) - Section 2 - Approach. General Secretariat of National Defence Central Information Systems Security Division (DCSSI), February 2004.
- [EFGW07] Andreas Ekelhart, Stefan Fenz, Gernot Goluch, and Edgar Weippl. Ontological mapping of common criteria's security assurance requirements. In Hein Venter, Mariki Eloff, Les Labuschagne, Jan Eloff, and Rossouw von Solms, editors, *New Approaches for Security, Privacy and Trust in Complex Environments, Proceedings of the IFIP TC 11 22nd International Information Security Conference, IFIPSEC2007, May 14-16*, volume 232/2007 of *IFIP International Federation for Information Processing*, pages 85–95, Sandton, South Africa, May 2007. International Federation for Information Processing. 978-0-387-72366-2.
- [EFKW07] Andreas Ekelhart, Stefan Fenz, Markus Klemen, and Edgar R. Weippl. Security ontologies: Improving quantitative risk analysis. In *Proceedings of the 40th Hawaii International Conference on System Sciences, HICSS2007*, pages 156–162, Los Alamitos, CA, USA, January 2007. IEEE Computer Society. 0-7695-2755-8.
- [EFNW07] Andreas Ekelhart, Stefan Fenz, Thomas Neubauer, and Edgar Weippl. Formal threat descriptions for enhancing governmental risk assessment. In Tomasz Janowski and Theresa A. Pardo, editors, *Proceedings of the First International Conference on Theory and Practice of Electronic Governance*, volume 232 of *ACM Interna-*

- tional Conference Proceeding Series*, pages 40–43, New York, NY, USA, January 2007. ACM. 978-1-59593-822-0.
- [Far91] Bill Farquhar. One approach to risk assessment. *Computers and Security*, 10(10):21–23, February 1991.
- [Fro97] Steve Frosdick. The techniques of risk analysis are insufficient in themselves. *Disaster Prevention and Management*, 6(3):165–177, 1997.
- [ISO05] ISO/IEC. ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements, 2005.
- [ISO07] ISO/IEC. ISO/IEC 27005:2007, Information technology - Security techniques - Information security risk management, November 2007.
- [JHS99] Changduk Jung, Ingoo Han, and Bomil Suh. Risk analysis for electronic commerce using case-based reasoning. *International Journal of Intelligent Systems in Accounting, Finance & Management*, 8:61–73, 1999.
- [NEF08] Thomas Neubauer, Andreas Ekelhart, and Stefan Fenz. Interactive selection of iso 27001 controls under multiple objectives. In *Proceedings of the Ifip Tc 11 23rd International Information Security Conference, IFIPSec 2008*, volume 278/2008, pages 477–492, Boston, July 2008. Springer.
- [NS07] Thomas Neubauer and Christian Stummer. Extending business process management to determine efficient it investments. In *Proceedings of the 2007 ACM symposium on Applied computing*, pages 1250–1256, 2007.
- [SCB07] Stanford Center for Biomedical Informatics Research SCBIR. The protege ontology editor and knowledge acquisition system, 2007.
- [SGF02] Gary Stoneburner, Alice Goguen, and Alexis Feringa. Risk management guide for information technology systems. NIST Special Publication 800-30, National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8930, July 2002.
- [Sta07] Manfred Stallinger. *IT-Governance im Kontext Risikomanagement*. PhD thesis, Johannes Kepler Universität Linz, 2007.
- [Vit86] Michael R. Vitale. The growing risks of information systems success. *MIS Quarterly*, 10(4):327–334, December 1986.
- [W3C04] W3C. OWL - web ontology language. <http://www.w3.org/TR/owl-features/>, February 2004.