

ACTIVE LOSS PREVENTION ALS BASIS FUNDIERTER TECHNOLOGIE-ENTSCHEIDUNGEN

*Identifizieren, quantifizieren und mitigieren von Risiken im
eBusiness-Umfeld*

Im Zeitalter von eCommerce und allgegenwärtiger Webpräsenz stellt die vernetzte Unternehmung keinen Wettbewerbsvorteil mehr dar, sondern ist zur Notwendigkeit geworden. Wettbewerbsvorteile werden jedoch durch die kontinuierliche Bereitstellung der Applikationen oder Services erreicht. Das verändert den Stellenwert, den die IT-Infrastruktur und deren Betrieb in den Unternehmen und bei der Umsatzgenerierung einnimmt. IT-Infrastrukturentscheidungen nehmen damit immer mehr unternehmensstrategischen Charakter an. Gerade in der gegenwärtigen wirtschaftlichen Situation kann es sich das Management nicht mehr leisten, Technologieentscheidungen auf Konsensgrundlage zu fällen. Vielmehr müssen Entscheidungen im IT-Bereich in der gleichen Art und Weise getroffen werden wie “Business Decisions” – auf Grundlage von Kosten und Nutzen und ob sie mit Unternehmenszielen und -strategie übereinstimmen. Die Tage der Technologie um der Technologie Willen sind vorbei!

1 Risiken und Nutzen von Technologie

Ob durch Bereitstellung kritischer Anwendungen, die Unterstützung des Tagesgeschäfts oder dem Hosting von Online-Services – IT-Infrastrukturen sind die leistungsfähigen Komponenten, die Umsatz und Unternehmen vorantreiben. In diesem Zusammenhang ist es von enormer Bedeutung, das zugehörige Risiko der Nichtverfügbarkeit der IT-Services und der damit verbundenen Umsatzverluste, Arbeitsproduktivitätsverluste, Folgekosten, Kundenunzufriedenheit und nicht zuletzt Reputationsschäden zu erkennen. Der Schlüssel zum Geschäftserfolg ist das erfolgreiche Management des Zusammenspiels von Technologien und verbundener finanzieller Risiken.

*“The central question of our age is how to act decisively in the face
of uncertain information.” – Bertrand Russell*

Durch die Analyse von erwartetem Ertrag und innewohnenden Risiken von Technologieinitiativen können eskalierende Infrastrukturbudgets und begrenzte Finanzmittel in Balance gebracht werden, während gleichzeitig diese Technologieinvestitionen mit den Geschäftszielen und Finanzvorgaben abgeglichen werden. Da alle Entscheidungen auf Grundlage begrenzter Informationen gefällt werden, ist

es essentiell, die sich ergebenden Unsicherheiten zu minimieren. Die Auswertung geeigneter Daten, die gerade im Technologiebereich in unübersehbarer Vielfalt vorhanden sind, spielt somit eine herausragende Rolle, um Wissen zu maximieren und intelligente Entscheidungen fällen zu können.

Es ist ein ökonomischer Grundsatz von Initiativen/Projekten bei gegebenem Risikoniveau die erwarteten ROI's zu maximieren. Die Definition eines angemessenen Risikolevels und die Vorgehensweise um den ROI zu maximieren kann folgendermaßen abgefragt werden:

1. Wie deckt die Technologie Geschäftsprozesse und -initiativen ab?
2. Welche finanziellen und Imagerrisiken sind mit den Technologien verknüpft?
3. Wo sind Ansatzpunkte, um die Risiken zu steuern (risk control points)?
4. Wie können die Risiken mitigiert werden, zu welchen Kosten und mit welchen Nutzen?

Aus dem Verständnis dieser Sachverhalte können strategische Entscheidungen über akzeptable Risikolevel und schwierige taktische Entscheidungen über Ressourcenallokationen aufgrund fundierter Informationen gefällt werden. Somit werden Infrastrukturausgaben priorisiert, um Technologien mit Geschäftsinitiativen in Einklang zu bringen sowie gleichzeitig Kosten zu minimieren oder Umsätze zu maximieren. Aber wie werden diese vier Fragen beantwortet?

2 Risk Profiling & Risk Mapping

Damit intelligente Infrastrukturentscheidungen gefällt werden können, muss verstanden werden, wie sich Unternehmensstrategien über Ziele, Vorgaben bis hin zu Geschäftsinitiativen auf Technologien abbilden. Diese Beziehung wird durch die Verfolgung und Aufnahme von diskreten Infrastrukturausfällen und der Analyse deren Auswirkungen auf die Geschäftsumgebung (Business Impact) analysiert und offengelegt.

Aus der Analyse, wie historische technologiebedingte Vorfälle Geschäftskennzahlen beeinflussen (z.B. verlorener Umsatz in Abhängigkeit von der Dauer des Ausfalles und dem durchschnittlichen Umsatz der betroffenen Services und Anwendungen), ergibt sich ein funktionaler Zusammenhang, der die Quantifizierung der Business Impacts ermöglicht. Die Datenbasis für Kennzahlen solcher Gefahrenpotentiale oder Risiken ist in den Datenbanken der Unternehmen vorhanden und muss nur ausgewertet werden. Sind diese Gefahrenpotentiale für jedes Problemfeld verstanden, werden Priorisierungen von Lösungen für technologierelevante Problemgebiete vor dem Hintergrund der Unternehmenszielsetzung ermöglicht.

“[Nature] has established patterns originating in the return of events, but only for the most part.” – Gottfried Leibniz

Die Zukunft mag ungewiss sein, ist aber kein vollständiges Geheimnis. Alle Umgebungen folgen geregelten Verhaltensmustern, die Schlüsse auf die Zukunft erlauben. Netzwerke und Infrastrukturausfälle stellen dabei keine Ausnahme dar. Die heutigen Infrastrukturen sollen robust konstruiert sein, um Geschäftsanwendungen und Services breitzustellen, gleichzeitig aber auch einen Kompromiss zwischen Flexibilität und Handhabbarkeit (Manageability) gewährleisten. In der Praxis ist dies aber eher selten verwirklicht.

Non-linear, complex and tightly coupled systems will always fail. – Charles Perrow

Unvermeidbar ergeben sich mehr oder weniger häufig Infrastrukturausfälle, die die kontinuierliche Bereitstellung der Applikationen oder Services verhindern – aber nicht ohne eine zugrund liegendes Muster zu offenbaren! In diesen historischen Mustern und Strukturen von Verhalten und Ausfall der Infrastrukturen kann das Gefahrenpotential, das Technologierisiko gemessen und verstanden werden. Durch Verwendung von Methoden aus den Bereichen Financial Engineering, Informationstheorie und Statistik kann die Plausibilität finanzieller Verluste aufgrund unerwünschter Ereignisse eingeschätzt werden. Dieses finanzielle Risiko wird als erwarteter täglicher, monatlicher oder jährlicher Verlust modelliert. Er stellt sich als die Wahrscheinlichkeit des Auftretens diskreter Ereignisse multipliziert mit der finanziellen Auswirkung der Ereignisse dar. Durch Sampling (Stichproben) der historischen Problem-Ticket-Datenbanken und log-Files der Unternehmen, und falls angemessen Ergänzung durch Industriedaten, wird das Risikoprofil und das sich ergebende finanzielle Gefahrenpotential erstellt.

Die historischen Daten über Ereignisse, die finanzielle Verluste verursachen, stellen eine Stichprobe dar – sie sind jedoch nicht die vollständige Repräsentation der Wirklichkeit. Erst die Modellierung des gesamten Kontinuums des finanziellen Risikos vom Bedeutungslosen zum Verheerenden (Risk Profiling) ergibt ein umfassendes Bild des finanziellen Gefahrenpotentials aufgrund von Technologieausfällen. Es hindert uns daran, uns im Glauben zu wagen, dass vergangene Erfahrungen alles darstellen was passieren kann. Aufgrund sehr geringer Wahrscheinlichkeiten großverlustiger Ereignisse könnten diese Risiken durch Sampling alleine übersehen werden. Die Modellierung des gesamten Spektrums vermittelt ein umfassendes Verständnis des finanziellen Risikos und erlaubt erst intelligentes Management durch Weitergabe (Versicherung), Vermeidung (Mitigation) oder Akzeptanz (Rücklagen) der Risiken. Die Risikoprofile werden mittels Kurven dargestellt, die das Kontinuum des finanziellen Risikos für eine spezifische Unternehmung aufzeigen (siehe Abbildung 1 auf der nächsten Seite: Annual Risk Exceedance Curve für Security) . Um die bestmöglichen Informationen aus diesen Kurven ableiten zu können, müssen die Risiken vorher strukturiert und technologielevanten Problemgebieten zugeordnet werden(Risk Mapping).

Beginnend mit der Zuordnung individueller Ausfälle zu den darunterliegenden

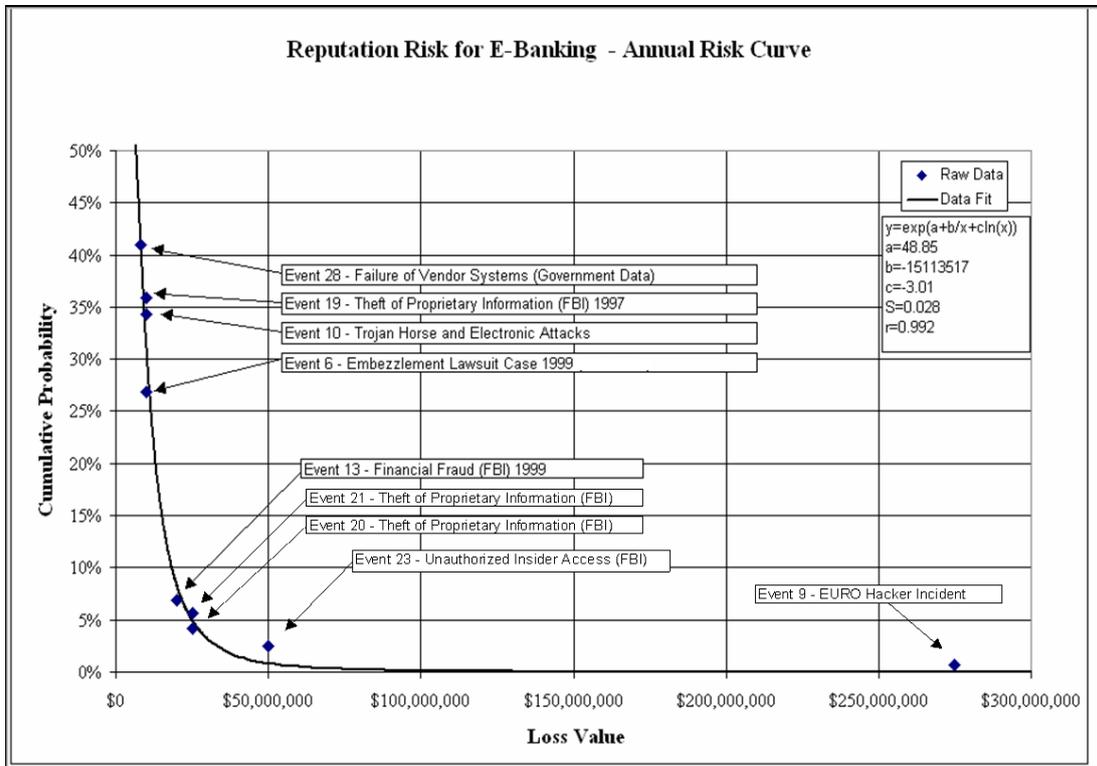


Abbildung 1: Annual Risk Exceedance Curve: Security

Die Risk Exceedance Curve stellt die jährliche Wahrscheinlichkeit dar, dass ein Verluste aufgrund eines diskreten Ausfalles/Vorfalles in der Infrastruktur (in diesem speziellen Fall durch sicherheitsrelevante Vorkommnisse) ein bestimmtes Maß übersteigt. Nimmt man einen bestimmten Verlustwert heraus, stellt die entsprechenden kumulierte Wahrscheinlichkeit die Plausibilität eines finanziellen Verlustes gleich oder höher des gewählten Wertes dar. In diesem Fall gibt es eine 10% Wahrscheinlichkeit das ein Vorfall im Bereich IT-Sicherheit einen Schaden von \$20M oder mehr pro Jahr verursacht.

technologie- oder prozessbezogenen Ursachen (Root Causes) wird für jeden Root Cause Plausibilität und finanzielles Gefährdungspotential aus den Daten der zugeordneten Ausfällen modelliert.

Beispiel: Durch die Einspielung eines fehlerhaften Software-Patch fielen 50% der Geldautomaten einer der größten Banken in Amerika für 6 Stunden aus. Die Ursache für diesen Infrastrukturausfall ist nicht fehlerhafte Technologie sondern deren mangelhaftes Management. Unzureichende Testprozeduren für Changes als Root Cause ordnen sich dann in das Problemfeld Change Management ein.

Daraus ist sofort das Risiko spezifischer Problemfelder, die durch die verschiedenen Root Causes charakterisiert sind, anhand der finanziellen Auswirkungen

erkennbar. In dem man diese taktischen Problemfelder mit den verbundenen Risiken weiter in strategisch-technologierelevante Themen und Managementthemen (z.B. Change Management) verdichtet, ergibt sich eine Risikostruktur für die Technologieumgebung, die detailliert, wie und warum das Unternehmen finanziellen Risiken ausgesetzt ist und wie sich diese Risiken in der Infrastruktur verteilen (siehe Abbildung 2: Event Identification Tree).

Dieses Risk Mapping liefert gleichzeitig direkte Kostenrechtfertigungen für Tech-

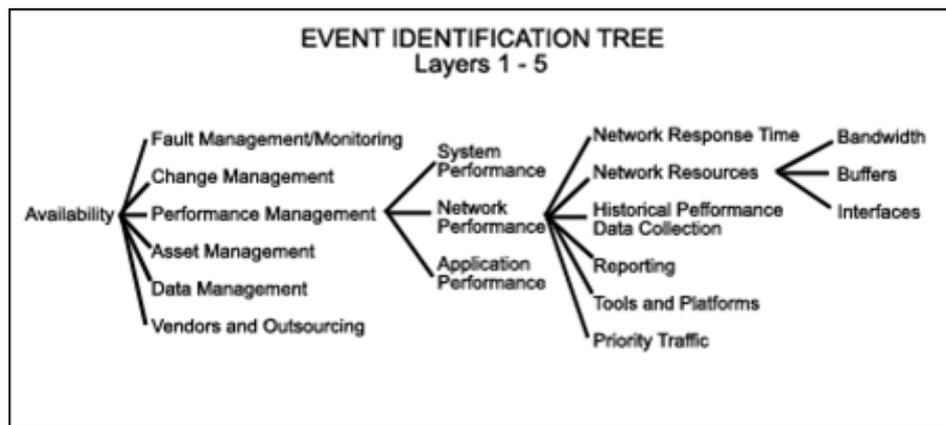


Abbildung 2: Event Identification Tree

Der Event Identification Tree zeigt auf wie Problemfelder in Infrastruktur und Management miteinander gekoppelt sind. Das Diagramm repräsentiert dies exemplarisch auf 5 Ebenen, anfangend mit Managementthemen bis hin zu spezifischen Technologieproblemgebieten. Es wird sowohl eine bottom-up-Betrachtung (Analyse der kundenspezifischen Infrastrukturprobleme) als auch eine top-down-Betrachtung (allgemeine taktische Infrastrukturproblemfelder) durchgeführt.

nologieinitiativen, indem verlorener Umsatz aufgezeigt wird. Dessen Rückgewinnung definiert den Nutzen für diese Initiativen. Durch abzuleitende Mitigationspläne werden Manager in die Lage versetzt effektiv zu planen und zu budgetieren. Durch Identifizierung von Risk Control Points können Auswirkungen auf das derzeitige Risikoprofil eines Unternehmens abgeschätzt werden, woraus sich direkt eine Priorisierung der Initiativen ergibt (siehe Abbildung 3 auf der nächsten Seite: Risikoverteilung).

Risk Mapping ist letzten Endes auch ein direkter Weg, um den Fortschritt von Technologieinitiativen zu messen und kontinuierlich zu verfolgen. Die Erwartungen an solche Initiativen können auf finanzieller Basis gesetzt und dann mittels Risk Profiling und Risk Mapping überprüft werden (siehe Abbildung 4 auf Seite 7: Zusammenfassung).

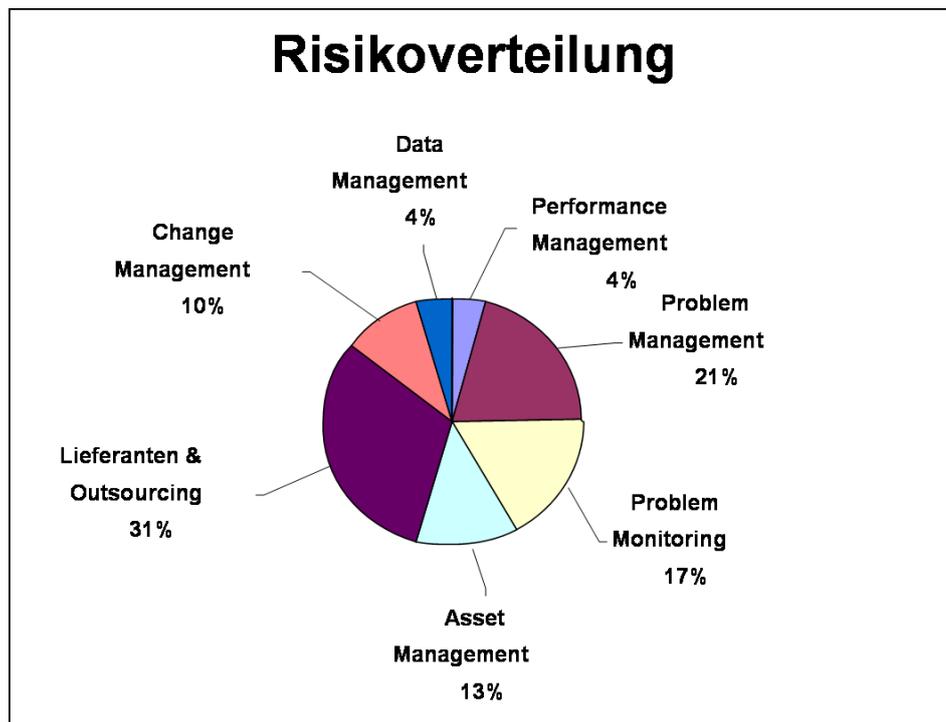


Abbildung 3: Risikoverteilung

Das Kreisdiagramm stellt dar in welchem Ausmaß einzelne Managementproblemfelder zum Gefahrenpotential des Unternehmens beitragen. Dadurch werden Ressourcenallokationen aufgrund von Investitionspriorisierungen vereinfacht.

3 Zusammenfassung

In Zeiten, in denen die Zukunft der Unternehmen immer mehr auf neuen Technologien und IT-Infrastrukturen aufbaut, kann es nicht mehr leichtfertig aufs Spiel gesetzt werden, ob diese Basis auch an den Unternehmenszielen ausgerichtet ist. Risk Profiling und Risk Mapping führen Unternehmen in die Ära aktiver Verlustvermeidung (Active Loss Prevention) und transformieren Bauchentscheidungen über Technologien in informierte, intelligente Entscheidungen. Sobald Unternehmen dringliche Problemfelder im Infrastrukturbereich definieren und priorisieren, Kostenrechtfertigungen (Business Cases) für Technologie-Investitionen erstellen, Erwartungen an Technologieinitiativen festschreiben und den Fortschritt dieser Initiativen messen und verfolgen, sind Technologie-Entscheidungen keine unabschätzbaren, unsicheren Vabanquespiele mehr!

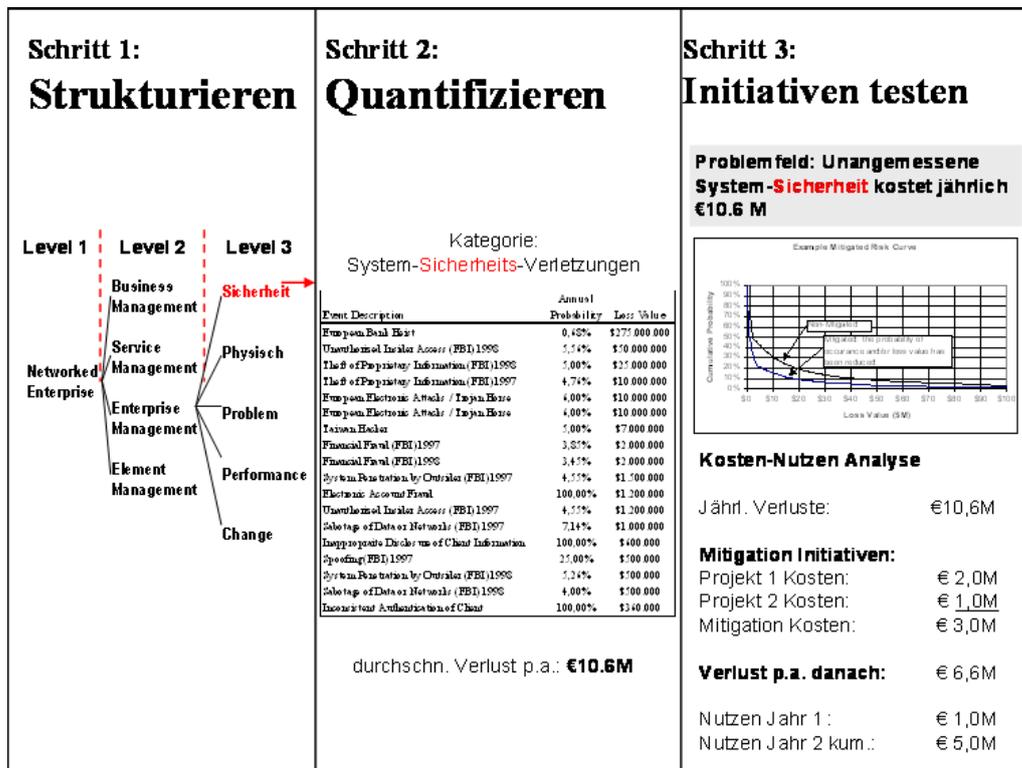


Abbildung 4: Zusammenfassung

Robert Günther hat Volkswirtschaftslehre in Verbindung mit Statistik an der TU Berlin studiert, sowie an einem MBA-Programm an der UBC in Vancouver, Kanada teilgenommen. Vor der Gründung von 4P. hat er bei der IBM Unternehmensberatungsgesellschaft, EDS und Predictive Systems als IT Management Berater mit den Schwerpunkten Prozessmodellierung, IT Kosten-Nutzenrechnung, IT Zentralisierung gearbeitet.