Übungsblatt 2

Aufgabe 5a)

Beschreiben Sie die im dargestellten SeeMe-Modell durch die Nummern (1-5) markierten Relationen textuell.

1. Hier wird der Einfluss des wissenschaftlichen Teils der Informatik auf die Ausbildung von Informatikern in der Praxis dargestellt. Dabei stellen Wissenschaft und Praxis die beiden Haupteilbereiche der Informatik dar, die wiederum Teil der Gesellschaft ist.
2. Aktuelle Forschungsergebnisse aus der gesamten Informatik fließen in die Ausbildung ein.
3. (Praktische) Informatiker entwickeln und beraten ein IuK System. Dieses wird dann später gemeinsam mit dem Anwender innerhalb seiner Einsatzumgebung zum Einsatz gebracht.
4. Die Nutzung eines IuK Systems besteht aus zwei Teilen: Dem erlernen und benutzen. Beide Tätigkeiten beziehen sich auf die Einsatzumgebung, da der Nutzer ihre Funktionen erlernen muss um sie später anzuwenden.
5. Wenn der Nutzer ein IuK System benutzt, kommt er (meistens...) auch zu einem Arbeitsergebnis. z.B. benutze ich gerade mein Office2000 Paket (das auf meiner Win2000 Einsatzumgebung läuft) um diesen Aufgabenzettel zu bearbeiten.

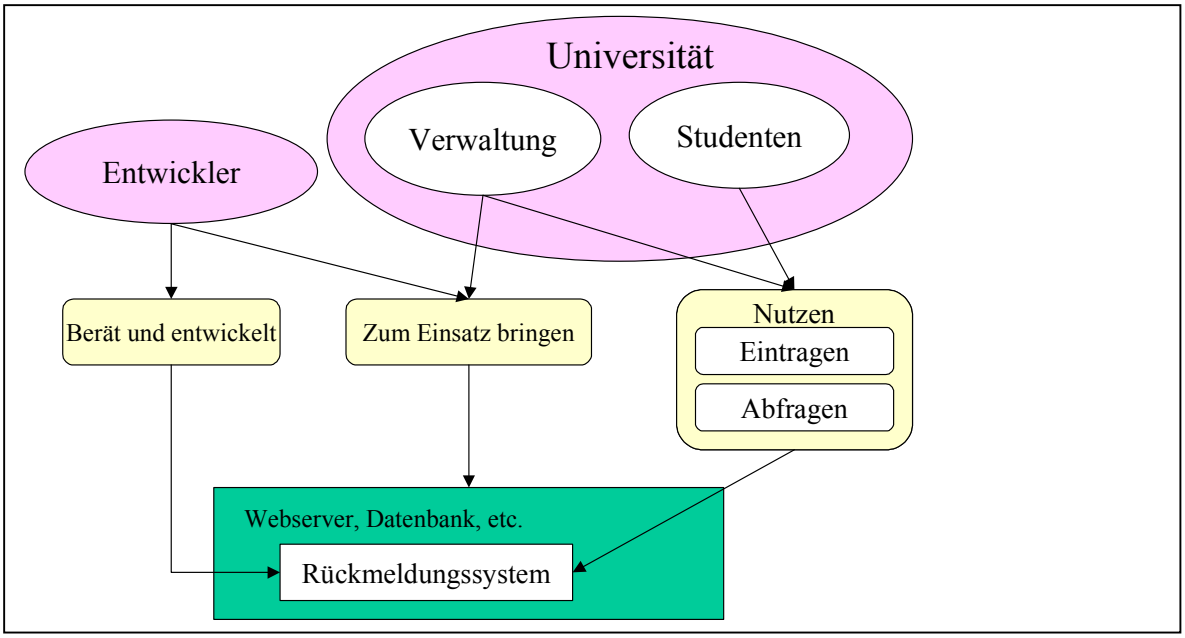
Aufgabe 5b)

Um welche Relationen zwischen den oben dargestellten Rollen lässt sich das Modell erweitern? (Geben Sie 3 weitere Relationen zwischen Rollen an und erläutern Sie dies anhand von Beispielen.)

1. Eine Rückwirkung der Aktivität „zum Einsatz bringen“ auf die Ausbildung von Informatikern, bzw. auf die Forschungsergebnisse. Ohne diese Relation, besteht die Gefahr, dass entweder praxisfremd ausgebildet wird, oder Beobachtungen, die beim Einsatz des Systems entstehen, nicht in die Forschungsergebnisse einfließen.
2. Eine Relation zwischen dem Entscheidungsträger und dem Anwender, der das System letztendlich in Auftrag gibt. Normalerweise wird der bevorstehende Einsatz eines Systems mit z.b. dem Betriebsrat abgesprochen, und er möchte in aller Regel auch über den Fortgang der Einführung Bescheid wissen.
3. Es sollte auch zu einer Absprache zwischen dem Nutzer und Anwender erfolgen. z.B. sollte der Nutzer die Möglichkeit haben, Verbesserungsvorschläge zu machen. Dieser Kanal zwischen Benutzer, Anwender und Entwickler ist besonders wichtig, um z.b. Schulungsbedarf der Nutzer festzustellen, oder das System entsprechend anzupassen.

Aufgabe 6)

Stellen Sie sich vor, dass Sie ein webbasiertes System zur Rückmeldung an der Universität entwickeln sollen. Entwerfen Sie ein SeeMe Modell, das Ihre Vorgehensweise bei der Entwicklung und bei der Einführung des Systems skizziert. Beachten Sie die Vorgehensweise im Kompendium Abschnitt 2.4 und das Modell aus Aufgabe 5. Achten Sie weiterhin darauf, dass Sie nicht die Funktionalität des Systems, sondern dessen Entwicklung modellieren!



Aufgabe 7)

Welches Risiko gehen Institutionen (z.b. Universitäten oder Provider) ein, wenn sie einer großen Anzahl ihrer Mitglieder die Möglichkeit geben, Inhalte in das WWW zu stellen?

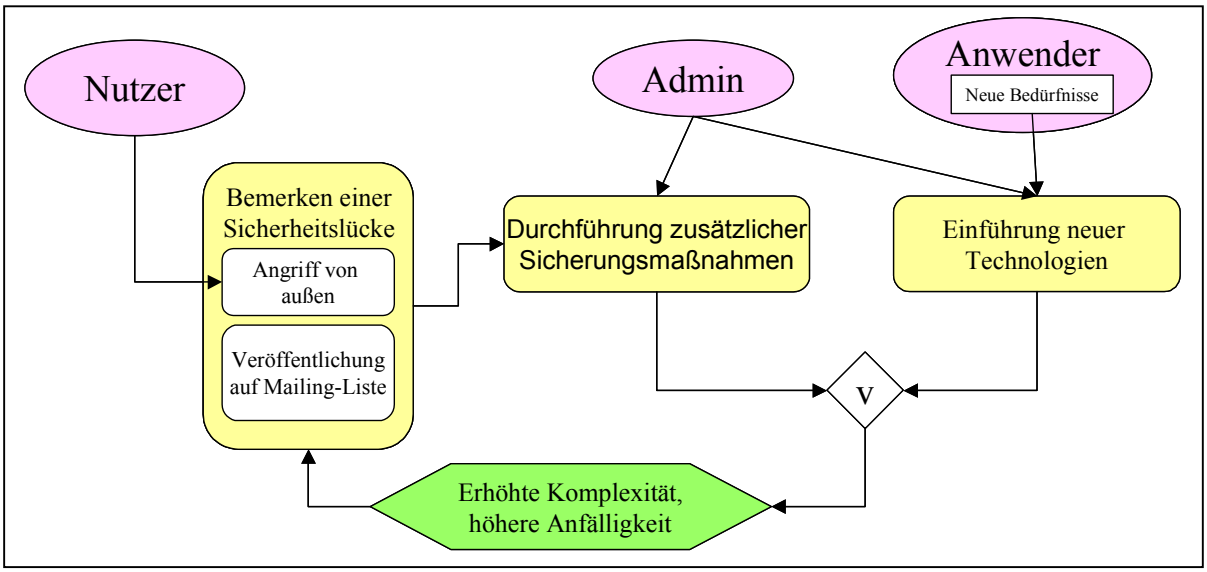
- Eines der Hauptrisiken für den Provider besteht darin, für den Inhalt der Seiten verantwortlich gemacht zu werden. Zum Beispiel besteht das Risiko, dass ein Nutzer Raubkopien anbietet - das entfernen dieser Seiten bedeutet natürlich Arbeits- und Zeitaufwand, und evtl. Schwerwiegende rechtliche Probleme für den Provider.
- Es besteht das Risiko eines Systemausfalls, wobei der Provider u.u. auch für Verdienstausfälle der Nutzer haftbar gemacht werden kann. (durch Online-shops, etc.)
- Wenn wie bei Universitäten üblich, nicht nur WWW Seiten zur Verfügung gestellt werden, sondern auch dial-in Zugänge, shell-accounts u.a. angeboten werden, muss für eine vernünftige Absicherung des Netzes gesorgt werden.

Welche technischen Maßnahmen zur Verminderung der Risiken sind denkbar?

- Keine anonyme Anmeldung, die Identität muss zumindest dem Provider jederzeit bekannt sein. Ansonsten kann es im Ernstfall unmöglich werden, den Verantwortlichen zu finden.

- Das interne Netzwerk muss durch Firewalls, Intrusion-Detection Systeme u.ä. abgesichert werden. Selbst ein interner Angriff von einem der shell-accounts sollte keine schweren Folgen für das restliche Netzwerk haben.
- Missbrauchsszenarien sollten von vornherein geplant werden. z.B. ist dafür zu sorgen, das Adressen wie *abuse@provider*, *webmaster@provider*, usw. eingerichtet werden, um überhaupt für Beschwerden zugänglich zu sein.
- Erfahrene, und gut ausgebildete Administratoren einsetzen.

Stellen Sie die Risikospirale (vgl. Kompendium S. 26ff.) als SeeMe Diagramm dar, in das Sie auch die beteiligten Rollen aufnehmen.



Aufgabe 8)

Die Abgrenzung zwischen Versagen und Missbrauch der Technik erweist sich oftmals als sehr schwierig oder gar unmöglich. Manchmal ist es dennoch notwendig, diesbezüglich eine Entscheidung zu treffen, um die Verantwortung für Schadensfälle zuzuordnen. Sammeln Sie zu den unten stehenden Beispielen Argumente, die für Versagen oder Missbrauch stehen könnten, diskutieren diese und treffen dann eine Entscheidung.

a) *Im Ärger über Überstunden vergisst ein Programmierer eine Grenzwertabfrage, wodurch allen Mitarbeitern in dem ihn beschäftigenden Unternehmen zuviel Gehalt gezahlt wird.*

Hier liegt menschliches Versagen vor. Der Programmierer stand unter Stress, und konnte sich daher nicht auf die Arbeit konzentrieren. Eine Missbrauchsabsicht kann keinem der Beteiligten unterstellt werden.

b) *Die Nutzung eines Mobiltelefons im Flugzeug führt zu Störungen beim Landeanflug.*

Sofern der Fluglinienbetreiber die Nutzung von elektronischen Geräten explizit verbietet, liegt ein Missbrauch vor - so etwas kann aber auch unabsichtlich geschehen.

Andererseits handelt es sich um technisches Versagen, da sich Telefon und Flugzeug gar nicht erst stören dürften - die Hersteller sind zu EMV-Prüfungen verpflichtet, und daher mitverantwortlich.

c) *Jedes mal, wenn Hacker versuchen, in ein System einzudringen, verursacht dies einen Zusammenbruch.*

Hier wird der Missbrauch durch einen technischer Mangel möglich. Je nach Fall kann die Schuld entweder beim Hacker oder Administrator liegen. Wenn das System z.b. nur mit schwachen Passwörtern abgesichert war, kann man dem Admin eine gewisse Fahrlässigkeit unterstellen. Auf jeden Fall sollten bekannte Sicherheitslücken technisch geschlossen werden, um den Missbrauch zu erschweren – Hacker übernehmen hierbei auch eine sinnvolle Rolle, indem sie Sicherheitslücken aufdecken.

d) *Einem kritischen Journalisten gelingt es, in einer Veröffentlichung nachzuweisen, dass er einzelne Einträge aus einer anonymisierten Datei reidentifizieren konnte.*

Hier liegt ein organisatorisches Versagen vor: Es gab z.b. Fälle bei denen schwarze Balken in ein PDF Dokument eingefügt wurden; außerdem bewirkt das löschen einer Datei i.d.R. keine physikalische Löschung der Daten. Da diese Details jedoch kaum ein Büroangestellter kennt, sollten kritische Dokumente nur nach Prüfung durch einen Datenschutzbeauftragten veröffentlicht werden. Auf keinen Fall sollte man den Reporter verantwortlich machen: ohne ihn wäre die Sicherheitslücke überhaupt nicht aufgedeckt worden.

e) *Nach erfolgreichem Abschluss eines Werkvertrages wird einem Programmierer nicht das ihm zustehende Entgelt ausgezahlt. Aufgrund einer Sicherheitslücke gelingt es ihm per Fernwartung, den Fehlbetrag von der Firma auf sein Konto überweisen zu lassen.*

Hier liegt ein Missbrauch vor. Der Programmierer nutz hier sein Insider-Wissen aus, um sich zu bereichern. Ob ihm der Betrag zusteht, hätte ein Gericht entscheiden müssen, nicht er selbst.