September 2003

Unterstützung von IT-Sicherheit in Dienstleistungen des E-Government durch Wissensmanagment

Markus Nick
Fraunhofer Institut Experimentelles Software Engineering (IESE)

Björn Snoek
Fraunhofer Institut Experimentelles Software Engineering (IESE), snoek@iese.fhg.de

In: Uhr, Wolfgang, Esswein, Werner & Schoop, Eric (Hg.) 2003. *Wirtschaftsinformatik 2003: Medien - Märkte - Mobilität*, 2 Bde. Heidelberg: Physica-Verlag

ISBN: 3-7908-0111-9 (Band 1)
ISBN: 3-7908-0116-X (Band 2)

Unterstützung von IT-Sicherheit in Dienstleistungen des E-Government durch Wissensmanagement[1]

Markus Nick, Björn Snoek

Fraunhofer Institut Experimentelles Software Engineering (IESE)

Zusammenfassung: Die Gewährleistung der Sicherheit bei E-Government Dienstleistungen ist essentiell für den Erfolg der elektronischen Unterstützung der öffentlichen Verwaltung. Zu diesem Zweck reichen isolierte Sicherheitsbestrebungen nicht aus, sondern es sind vielmehr integrative Konzepte erforderlich. In dem öffentlich geförderten Projekt SKe entwickeln wir einen solchen integrativen Ansatz. Eine Komponente dieses Ansatzes ist eine Wissensmanagement-basierte Lösung zur Unterstützung dynamischer Aspekte der IT-Sicherheit. Diese Komponente - ein intelligenter IT-Sicherheits-Leitstand - unterstützt das IT-Sicherheitspersonal im Alltag durch systematische Aufzeichnung und Bereitstellung von Erfahrungen aus dem täglichen Arbeitsprozess. Die Komponente wird derzeit zusammen mit einem Anwendungspartner entwickelt und ebenso in Projekten mit Industriepartnern verwendet.

Schlüsselworte: E-Government, IT-Sicherheit, Wissensmanagement, Wiederverwendung von Erfahrungswissen, Experience Base, Case-Based Reasoning

1 Einleitung

Die Bedeutung elektronischer Unterstützung für die öffentliche Verwaltung (E-Government) wächst stetig und in vielen Ländern wird dieses Wachstum durch verschiedene Initiativen noch weiter beschleunigt. So gibt es beispielsweise in Deutschland die Initiative BundOnline 2005 [BMI05], deren Ziel die vollständige Online-Verfügbarkeit aller Dienstleistungen des Bundes bis zum Jahr 2005 ist. Weiterhin gibt es E-Government-Initiativen in über 130 deutschen Städten, Gemeinden und Kommunen, welche von Konzeptionen bis hin zu lauffähigen und im Einsatz befindlichen Lösungen reichen [BMWi99][BSI02a]. In den USA wird E-Government gar von der Öffentlichkeit als die nächste amerikanische Revolution

[1] Die vorliegende Arbeit ist Teil des SKe-Projektes [SKe01], dass vom Bundesministerium für Bildung und Forschung (Vertragsnummer 01AK900B) finanziert wird.

eingestuft [CEG02]. Bei all diesen Initiativen hat die Gewährleistung der Sicherheit und der Schutz privater Daten oberste Priorität.

Im Folgenden steht der Begriff *eService* für elektronische Dienstleistungen in der öffentlichen Verwaltung (Regierung, Behörden, etc.) und stellt somit das elektronische Gegenstück zu einer konventionellen Interaktion zwischen den Verwaltungen und deren Kunden dar.

Um die oft erhebliche Menge notwendigen Fachwissens zur Erbringung dieser Leistungen zu bewahren und zur erneuten Verwendung verfügbar zu machen ist Wissensmanagement (WM) ein weiterer wesentlicher Bestandteil in eService- Lösungen.

Um die Sicherheit von eServices zu gewährleisten sind integrierte Sicherheitskonzepte erforderlich, die nicht nur die technische Seite der IT-Sicherheit betrachten sondern auch die rechtlichen Eigenschaften der implementierten administrativen Routinen berücksichtigen [WiBr02]. Bei der Gestaltung sowohl von Sicherheitskonzepten als auch von Wissensmanagementlösungen sind organisatorische, kulturelle und soziale Aspekte zu berücksichtigen [Dist00]. Da der Erfolg eines modernen E- Governments zum größten Teil vom Vertrauen in das Gesamtsystem, aber auch von dessen Benutzbarkeit abhängt sollte das Sicherheitsniveau mit Bedacht gewählt werden, um eine hohe Nutzerakzeptanz zu sichern [OECD01].

Die Forderung nach einer ganzheitlichen Lösung geht einher mit den jüngsten Entwicklungen auf dem Gebiet der IT-Sicherheit, deren Hauptaugenmerk auf die eigentliche Handhabung dieser Sicherheit gerichtet ist. Der IT-Sicherheitsexperte Bruce Schneier beschreibt dies mit den Worten „IT-Sicherheit ist ein Prozess, kein Produkt“ [Schnei00]. Er stellt damit klar, dass es nicht ausreicht, eine Reihe von Produkten zur IT-Sicherheit zu installieren, um die Sicherheit der IT einer Organisation zu gewährleisten. Fallbasiertes Schließen (CBR) [AaPl94] ist sowohl ein Prinzip als auch eine Technologie für Wissensmanagement, welche das Potential zur Verbesserung solcher Prozesse besitzt [Nick+01].

Leider sind heutige IT-Sicherheitskonzepte noch nicht den obigen Anforderungen entsprechend integriert, sondern decken lediglich einzelne Aspekte ab, ohne Beziehungen zu anderen Konzepten aufzuweisen. Es bestehen Lücken bezüglich (a) der Klarheit formaler Schlüssigkeit von Sicherheitskonzepten, (b) der Korrektheit implementierter Sicherheitsmaßen, (c) der kontinuierlichen Überwachung von Messungen und (d) der systematischen Aufzeichnung von Sicherheitsvorfällen und Erfahrungen.

Diese Arbeit ist Teil eines umfassenden Ansatzes, welcher im Rahmen des SKe-Projektes entwickelt wurde. Inhalt des SKe-Projektes ist die Entwicklung eines integrierten Sicherheitskonzeptes, welches Mechanismen zur Wahrung und kontinuierlichen Verbesserung des Sicherheitsniveaus enthält und diese bereits während der täglichen Arbeit anwendet [Rie02][SKe01]. In SKe wird die formale Modellierung der eServices und deren Sicherheitsaspekte zur Identifikation und Prüfung der

für den jeweiligen eService erforderlichen Sicherheitseigenschaften verwendet [RuGü02]. Zusätzlich erlaubt die formale Modellierung richtungsbezogene Simulationen und Analysen von Bedrohungsszenarien. Hierzu ist es erforderlich, explizite Rahmenbedingungen (Voraussetzungen und andere Annahmen) für die Modellierung festzulegen, um die Sicherheitsanforderungen erfüllen zu können. Zur Sicherstellung dieser Rahmenbedingungen sind entsprechende technische und organisatorische Maßnahmen zu treffen. Eine weitere Komponente von SKe ist der elektronische Sicherheitsinspektor (eSI), welcher die kontinuierliche Überwachung der software-technisch messbaren Sicherheitsmaße übernimmt. Die Erfahrungen bezüglich der Reaktion auf Sicherheitsvorfälle (Ereignisse, Einbrüche, Bedrohungen) werden in einer Erfahrungs-basierten Sicherheitsdatenbank (eSDB) zusammengeführt und durch einen intelligenten IT-Sicherheits-Leitstand direkt am Arbeitsplatz bereitgestellt. So wird die sicherheits-relevante Arbeit des IT-Sicherheitspersonals schnell und fortschrittlich unterstützt. Die Resultate von SKe können auch direkt auf eServices außerhalb der öffentlichen Verwaltung übertragen werden, wenngleich dieses Projekt an die speziellen Anforderungen im E-Government angepasst wurde. Beispielsweise arbeiten wir in diesem Projekt mit einem Anwendungspartner zusammen, der als eine Abteilung der öffentlichen Verwaltung für die Finanzangelegenheiten einer deutschen Großstadt verantwortlich ist. Durch dessen Nutzung des Systems im Rahmen einer Fall-Studie erhalten wir wichtige Hinweise und Erkenntnisse aus der täglichen Praxis, die in die Entwicklung des IT-Sicherheits-Leitstandes eingehen.

In dieser Arbeit betrachten wir den IT-Sicherheits-Leitstand und die eSDB. Neben der Entwicklung der eSDB wird ein umfassender Prozess für die nötigen sicherheits- und wissensbasierten Aktivitäten definiert [Alt+01]. Ein integratives Wissensmodell führt schließlich das formale Sicherheitsmodell mit der eSDB zusammen.

Damit IT-Sicherheits-Leitstand und eSDB für unterschiedliche eService-Lösungen geeignet sind müssen sie flexibel und skalierbar bezüglich der organisatorischen Infrastrukturen und der unterschiedlichen Erfahrungsstrukturen sein. Dies führt zu unterschiedlichen Bedürfnissen bezüglich der ‚Intelligenz' des Wissensmanagement-Systems. Weiter ist eine enge Integration in den Arbeitsprozess, wie beispielsweise eine proaktive kontextbezogene Bereitstellung von Wissen [AbMe01], erforderlich. Als Organisationsprinzip für unsere CBR-basierte Wissensmanagement-Lösung nutzen wir das Experience-Factory-Konzept [Bas+94]. Durch die Etablierung einer Feedback-Schleife und deren Unterstützung durch den IT-Sicherheits-Leitstand integrieren wir Aufnahme und Verwendung von Erfahrungen in den täglichen Arbeitsablauf.

Der Nutzen des Wissensmanagements zur Wartung der IT-Sicherheit von eServices ist vielfältig: Wir erwarten durch die Etablierung der Feedback-Schleife zur Erfahrungssammlung und -nutzung ein kontinuierliches Lernen und und damit eine Verbessernung der IT-Sicherheit von eServices. Die eSDB wird eine Reaktionsbeschleunigung und -verbesserung bei Sicherheitsvorfällen und -bedrohungen bewir-

ken, sowie deren Nachvollziehbarkeit verbessern. Zusätzlich bietet die systematische Aufzeichnung von Vorfällen in der eSDB eine solide Basis zur Vorbereitung von Sicherheitsüberprüfungen und -revisionen. Nicht zu vernachlässigen ist schließlich die Tatsache, dass durch die systematische Aufzeichnung von Erfahrungen die Aufrechterhaltung eines gewissen Minimal-Sicherheitsniveaus ermöglicht wird, falls gerade keine IT-Sicherheitsspezialist verfügbar ist (z.B. bei Urlaub, Krankheit oder durch Fluktuation).

Dieses Papier ist im weiteren Verlauf wie folgt strukturiert: Abschnitt 2 beschreibt die Anwendung der WM-Methode DISER [Tau01][AlNi03] zur Identifikation relevanter Szenarien des Erfahrungsmanagement (EM) in der IT-Sicherheit. Dies mündet in die Betrachtung von Erfahrungen bei der Reaktion auf Sicherheitsvorfälle und - als Kernszenario - in einer Erfahrungs-Feedback-Schleife, welche die Aufnahme und Anwendung von Erfahrungen in den täglichen Arbeitsablauf des IT-Sicherheitspersonals integriert. Um diese Feedback-Schleife in die Praxis umzusetzen entwickeln wir einen intelligenten IT-Sicherheits-Leitstand in enger Zusammenarbeit mit unserem Anwendungspartner (Abschnitt 3). Die Planung zur Evaluation des IT-Sicherheits-Leitstandes wird in Abschnitt 4 beschrieben. Die Arbeit schließt mit einer Zusammenfassung und Ausblicken in Abschnitt 5.

2 Wissensmanagement für IT-Sicherheit in E-Government

Zur Spezifikation und Entwicklung der erforderlichen WM-Unterstützung für das IT-Sicherheitspersonal durch die eServices wurde die WM-Methodologie DISER angewandt. Abschnitt 2.1 zeigt einen kurzen Überblick über DISER. In Abschnitt 2.2 werden die Ergebnisse aus der Anwendung verdeutlicht und Abschnitt 2.3 erklärt die Feedback-Schleife, welche den Kern des vorgestellten WM-Systems bildet. Details hierzu sind in den Unterlagen des SKe-Projektes zu finden [Alt+01].

2.1 Die Wissensmanagement-Methodologie DISER

Ziel der ersten Phase von DISER ist es, eine Vision des WM-Systems zu entwickeln, welche mögliche Geschäftsunterstützungen aufzeigt und zugehörige Einbettungen in die Organisation vorschlägt. Der Schwerpunkt liegt daher auf der Beschaffung, Nutzung und Wiederverwendung von Erfahrungswissen. Hierbei sind artverwandte laufende Aktivitäten ebenso zu berücksichtigen, wie bestehende Systeme und Maßnahmen (Abbildung 1: „existierendes Wissen + existierende Infrastrukturen”). Eine Aufgabe der Visions-Generierung ist daher die Analyse existierender WM-Aktivitäten und verwandter Maßnahmen, zur Festlegung des Start-

punktes möglicher WM-bezogener Verbesserungen. Wenn der Auftraggeber bereits Geschäftsziele und Erfolgskriterien festgelegt hat sind diese ebenfalls zu berücksichtigen. Wenn möglich können in der Vision bereits neue EM-Maßnahmen und -Aktivitäten mit vorhandenen verknüpft oder kombiniert werden.

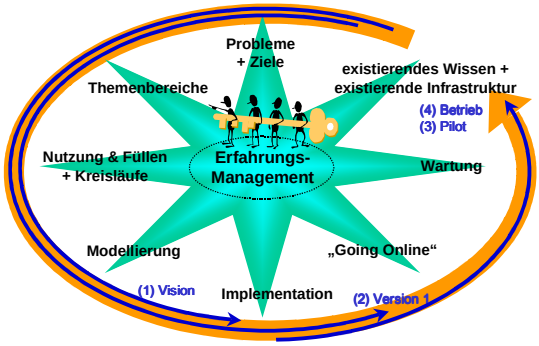

Abbildung 1: Ein Überblick über die Methodologie DISER (=Design and Implementation of Software Engineering Repositories)

Die zweite Phase hat die Aufgabe die zuvor entworfenen Vision des WM-Systems systematisch zu entwickeln und diese in einer ersten Version (Pilot) umzusetzen. Die Vision dient hierbei als Startpunkt für Detailanalysen von Zielen, relevanten Themengebieten, sowie von Aufnahme- & Nutzungs-Szenarien des WM-Systems, welche letztlich die Anforderungen an das WM-System darstellen. Die Nutzungsszenarien beinhalten nun auch Definitionen von Such-Zielen, welche die Informations-Anforderungen aus Sicht der Benutzer in einer deutlich formelleren Art darstellen.

2.2 Die Anwendung von DISER auf das Projekt SKe

Als Resultat der Anwendung von DISER auf die erste Phase von SKe wurden von uns die folgenden Ziele, Themengebiete und Szenarien identifiziert:

Das *Hauptziel* war bereits durch den Forschungsantrag des Projektes gegeben: „Integrierte IT-Sicherheitskonzepte und Mechanismen zur dauerhaften Sicherung und Verbesserung des Sicherheitsniveaus“.

Die wichtigsten *Stakeholder und Benutzer* sind das IT-Sicherheitspersonal. Hierbei unterscheiden wir zwei Rollen: Ein *IT-Sicherheitsspezialist* ist ein Experte in einer speziellen IT-Sicherheitsdomäne. Üblicherweise liegen die Aufgaben, welche er zu bearbeiten hat auch innerhalb dieser Domäne. Ein *IT-Sicherheitsbeauftragter* ist verantwortlich für die Vergabe von Aufgaben an die IT-Sicherheitsspezialisten und die Überwachung der Abarbeitungslisten. In kleinen Unternehmen kann eine Person durchaus beide Rollen gleichzeitig wahrnehmen, wohingegen in größeren Unternehmen etliche IT-Sicherheitsspezialisten erforderlich sind. Weiterhin können

Stakeholder auch noch bei Entwicklern, Systemadministratoren und Benutzern der eServices zu finden sein.

Bezüglich der Themengebiete, welche vom WM der IT-Sicherheit von eServices adressiert werden, müssen wir als erstes zwischen *eService* und *Grundschutz* [BSI02b] unterscheiden:

- eService:
  Die formale Modellierung eines eServices identifiziert sicherheitskritische Ergebnisse in Form der jeweiligen Sicherheitsziele, -anforderungen, -mechanismen und -annahmen. Die Sicherheitsmechanismen und -annahmen sind hierbei entweder als technische oder organisatorische Maßnahmen implementiert oder werden von diesen überwacht.

- Grundschutz:
  Der Grundschutz ist von dem formalen Sicherheitsmodell unabhängig. Einerseits kann der Aufbau des Grundschutzes durch Erfahrungen unterstützt werden, andererseits zeigt das Grundschutz-Handbuch des BSI [BSI02b] in Verbindung mit diesem Aufbau was zu überwachen ist.

Als zweites müssen wir zwischen der *Aufbauphase* und dem *regulären Betrieb* eines eServices unterscheiden:

- Aufbauphase:
  Während der Aufbauphase eines Sicherheitskonzeptes werden die erforderlichen Sicherheitsmaßnahmen identifiziert (z.B. wie oben beschrieben für eService und Grundschutz). Auf einen eService der gerade geplant ist oder sich schon im Aufbau befindet haben die Resultate eines formalen Sicherheitsmodells direkten Einfluss. Für bereits laufende eServices, stellt das formale Sicherheitsmodell eine Bewertungsmöglichkeit bezüglich deren Sicherheit dar.

- Regulärer Betrieb:
  Der reguläre Betrieb behandelt Entscheidungen bezüglich Kontinuität und Dauerhaftigkeit. Dies wird durch die systematische Neuaufnahme und Anwendung von Erfahrungen bei Reaktionen auf Sicherheitsvorfälle, sowie Diagnose und Log-Analyse erreicht. Die systematische Aufnahme von Sicherheitsvorfällen kann zur Identifikation notwendiger Verbesserungen der IT-Sicherheit verwendet werden, woraus sich dann die Möglichkeit ergibt, neue Maßnahmen einzuführen oder bestehende zu verbessern.

Bei der Entwicklung eines *ganzheitlichen Prozesses*, der alle Szenarien berücksichtigt, führen die Ansprüche des regulären Betriebs zu einer Feedback-Schleife für IT-Sicherheitserfahrungen als Kern-Szenario (siehe Abschnitt 2.3). Ebenso resultieren hieraus spezifischere Szenarien, die auf dem IT-Sicherheits-Prozess aus [BSI02b] und den Resultaten der Workshops mit unserem Projektpartner beruhen.

In der zweiten Phase wird von uns gerade eine spezielle Instanz der Vision für unseren Anwendungspartner entwickelt (Abschnitt 3)

2.3 Feedback-Schleife zur dynamischen Überwachung der IT-Sicherheit

Die Feedback-Schleife wird in Abbildung 2 aus Sicht des IT-Sicherheitspersonals dargestellt und bildet mit der systematischen Aufzeichnung und Anwendung von IT-Sicherheits-Erfahrungen den Kern des SKe-Szenarios. Drei weitere Szenarien vervollständigen die Feedback-Schleife [Alt+01].

Wir unterscheiden vier Phasen der Schleife: *Überwachung des Sicherheitsstatus'*, *Diagnose & Entscheidungsunterstützung*, *Reaktion* und *Erfahrungen aufzeichnen & Feedback geben*. Während die Überwachung des Sicherheitsstatus' wegen der Effektivität von Maßnahmen eine kontinuierliche Aufgabe ist werden die anderen drei Phasen durch potentielle Sicherheitsvorfälle ausgelöst und dann sequentiell für jeden dieser Vorfälle durchlaufen.

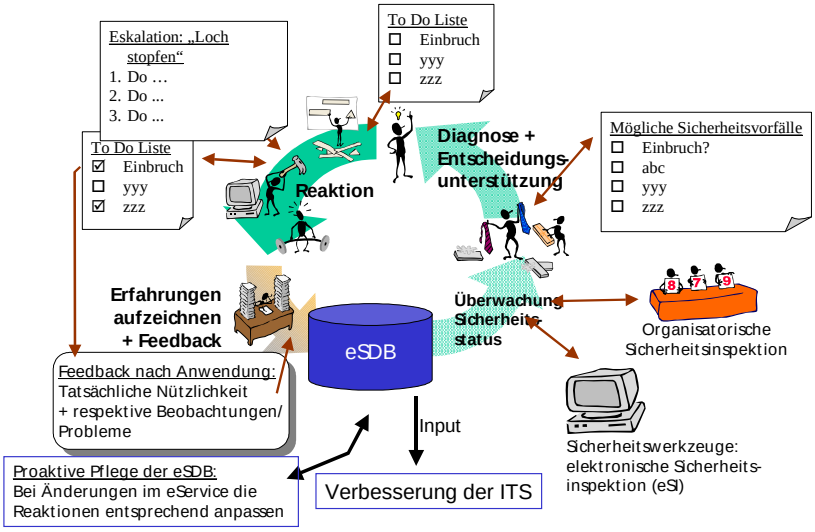

Abbildung 2: Eine in den Arbeitsprozess integrierte Feedback-Schleife für IT-Sicherheitserfahrungen

Die letzten drei Phasen ähneln dem Basis-Zyklus von CBR [AaPl94] auf organisatorischer Ebene [Tau01]. Sie sind weiterhin sehr ähnlich zu CBR-basierten Trouble Ticket Systemen (z.B. [LeDr93]), da sich beide mit der Abarbeitung bestimmter Vorfälle durch die jeweils verantwortlichen Mitarbeiter befassen. Generell ist die Feedback-Schleife tief in den Arbeitsprozess integriert, was ein erfolgreiches Wissensmanagement erst ermöglicht [AbMe01][Web+01].

In der Phase der *Überwachung des Sicherheitsstatus'* meldet der elektronische Sicherheitsinspektor (eSI) software-technisch überprüfbare Zustände mit sogenannten Sensoren. Der organisatorische Sicherheitsinspektor (oSI) liefert Daten und In-

formationen, die aus organisatorischen Maßnahmen resultieren oder aus anderen Gründen nicht software-technisch überwacht werden können. Alle nicht durch eSI oder oSI (z.B. Mitarbeiter) als ‚OK' klassifizierbaren Zustände werden in eine Liste potentieller Sicherheits-Vorfälle aufgenommen.

In der Phase *Diagnose & Entscheidungsunterstützung* wird der Status zunächst auf ‚ungeklärt' gesetzt und es werden mögliche Reaktionen auf Basis der bereits bekannten Erfahrungen vorgeschlagen, woraus eine von dem jeweils verantwortlichen IT-Sicherheit-Mitarbeiter ausgewählt wird. Abhängig von Auswirkung und potentiellem Schaden werden die zu überprüfenden Vorfälle priorisiert und in einer Abarbeitungsliste eingefügt.

Diese Phase weist viele Bezüge zu CBR-basierten Diagnose-Systemen auf, wie sie beispielsweise in Helpdesk-Systemen [Lenz+96][Alt97] und Trouble-Ticket-Systemen [LeDr93] verwendet werden. Im Gegensatz zur Diagnose, die auf strukturiertem CBR basiert (z.B. das CFM-56 Flugzeugtriebwerk-Diagnose-Tool CASSIOPÉE [Lenz+96]), arbeitet der IT-Sicherheits-Leitstand auf schwach strukturiertem Text mit wenigen symbolischen Attributen. Daher sind für unseren Typ von Fällen textuelle CBR-Mechanismen [Lenz+98][Lenz98] (beispielsweise verwendet in der erfolgreichen Dauerlösung SIMATIC von Siemens [Berg+03]) und einige einfache Ähnlichkeitsmodelle für strukturiertes CBR erforderlich. Aufgrund der Tatsache, dass die Fälle unseres Anwendungspartners ein Hauptsymptom besitzen, welches zur Reaktion führt, ist keine besondere Unterstützung für Dialog-orientiertes Retrieval erforderlich, wird aber durch die Wahl einer Retrieval-Komponente (Abschnitt 3.4) wie z.B. dem kommerziellen CBR-Tool orenge der Firma empolis in unserer Lösung (siehe folgender Abschnitt) unterstützt.

In der Phase *Reaktion* werden nun diese Vorfälle vom verantwortlichen Sicherheitspersonal entsprechend ihrer Priorität abgearbeitet. Für den Fall, dass es sich um hochkritische Vorfälle handelt wird weiterhin ein zuvor definierter Eskalationsplan automatisch abgearbeitet, sofern der verantwortliche IT-Sicherheitsmitarbeiter nicht oder nicht schnell genug reagiert oder reagieren kann (z.B. Internetverbindung trennen bei einem Sicherheitsleck an einem Feiertag)

In der Phase *Erfahrungen aufzeichnen & Feedback geben* werden schließlich Erfahrungen über neue oder veränderte Reaktionen auf Sicherheitsvorfälle aufgezeichnet und Feedback in der Form des tatsächlichen Sicherheitsvorfalles in bezug auf Gefährlichkeit, mögliche Auswirkungen und den Erfolg der durchgeführten Reaktionsmaßnahmen durch Angabe eingetretener und verhinderter Schäden gegeben. Dieses Feedback und die neuen Erfahrungen schließen den Kreislauf zur Verbesserung der Diagnose und Entscheidungsunterstützung. Wird ein eService geändert, so ermöglicht die proaktive Wartungsstrategie eine Identifizierung der betroffenen Vorfälle, welche dann entsprechend aktualisiert werden können. Die systematische Aufnahme von Sicherheitsvorfällen hilft bei der Ermittlung von Verbesserungsmöglichkeiten in der IT-Sicherheit und kann daher auch zur Einführung neuer und Verbesserung bestehender Sicherheitsmaßnahmen genutzt werden.

Die Feedback-Schleife ist eine Instanziierung des Standard CBR-Zyklus [AaPl94] auf organisatorischer Ebene [TaAl97][Tau01] und zeigt eine enge Integration in den Arbeitsprozess, der ein Startpunkt für eine erfolgreiches Wissensmanagement [AbMe01] bildet.

3 Ein intelligenter erfahrungsbasierter IT-Sicherheits-Leitstand für eServices

Der IT-Sicherheits-Leitstand stellt eine Realisierung der Kern-Komponente (Feedback-Schleife und weitere verwandte Szenarien) des SKe-Prozesses dar. Die Hauptaufgabe ist die Unterstützung des IT-Sicherheitspersonals bei der täglichen Arbeit.

Um intelligente Unterstützung im täglichen Arbeitsumfeld zu ermöglichen haben wir ein Prozessmodell und eine grafische Benutzerschnittstelle entwickelt, welche die intelligenten Unterstützungen (iSupport) vollständig in den Arbeitsablauf integrieren (Abschnitt 3.1). Das Prozessmodell basiert auf der im letzten Abschnitt beschriebenen Feedback-Schleife. Um Erfahrungen standardisiert ablegen zu können ist eine Schema erforderlich, dass die Art der Wissensaufnahme beschreibt (Abschnitt 3.2). Dieses Schema erlaubt eine Unterscheidung zwischen Standard- und Nicht-Standard-Reaktionen auf Vorfälle. Der Wartungsprozess unterstützt das Zusammenführen von Standard- und verwandten Nicht-Standard-Fällen, wobei die zu verwendende Strategie den jeweiligen Erfordernissen angepasst werden kann (Abschnitt 3.3).Die momentane Implementierung schließlich basiert auf einer Produktlinien-Architektur für Erfahrungsmanagement-Systeme (Abschnitt 3.4).

3.1 Unterstützung des IT-Sicherheitspersonals durch den IT-Sicherheits-Leitstand

Die Beschreibung der Unterstützung des IT-Sicherheitspersonals durch den IT- Sicherheits-Leitstand erfolgt anhand eines Prozessmodells (Abbildung 3), welches die Prozesse mittels Stati (Kästen) und Übergängen (Pfeile) darstellt. Aufbauend auf diesem Prozessmodell entwickelten wir eine grafische Benutzerschnittstelle (GUI) für den IT-Sichereits-Leitstand. Nachfolgend beschreiben wir den Prozess und die jeweiligen Möglichkeiten zur intelligenten Unterstützung innerhalb der verschiedenen Prozessschritte und illustrieren diese anschließend mit Beispielen aus einem Teil der GUI.

Der Benutzer meldet sich zunächst am System an und erhält seine persönliche Oberfläche innerhalb derer er seine Liste offener Vorfälle bearbeiten kann (Abbildung 3: oben Mitte). Ein IT-Sicherheits-Manager hat darüber hinaus Zugriff zu Vorfällen in den Bearbeitungslisten aller Mitarbeiter. Neue Sicherheitsvorfälle

werden vom eSI automatisch gemeldet (z.B. Portscan-Angriff) oder vom oSI vorgegeben, können aber auch manuell vom Benutzer in eine Liste potentieller Vorfälle eingetragen werden.

Sobald ein potentieller Vorfall von einem Benutzer übernommen oder von dem IT-Sicherheits-Manager an einen Benutzer zugewiesen wurde müssen dem Vorfall neben den vorhandenen Auftretens-Charakteristika (z.B. Ursache) weitere Merkmale für die Bearbeitung hinzugefügt werden. Ein iSupport schlägt bereits Kategorien vor, die vom Benutzer angepasst werden können. Durch Knopfdruck bietet der nächste iSupport Prioritätsvorschläge, die auf Basis ähnlicher (bereits priorisierter) Vorfälle im Hintergrund ermittelt wurden.

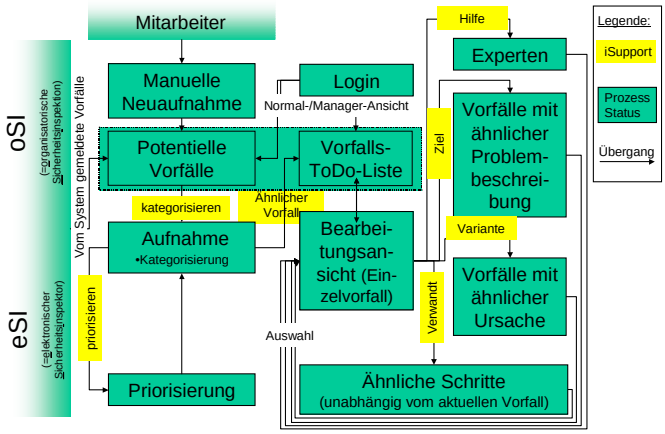

Abbildung 3: Prozesse des IT-Sicherheits-Leitstandes

Bei Aufgaben ohne notwendige Dringlichkeitsreihenfolge können Prioritäten ganz entfallen und bei einer überschaubaren Menge von Arbeitspaketen (5-10 Aufgaben) bedarf es diesbezüglich keiner Werkzeugunterstützung. - Jenseits dieser Grenze ist eine entsprechende Unterstützung jedoch wichtig. Nach unseren Erfahrungen in Projekten sind Prioritätsentscheidungen subjektiv und können meist bereits von einer Person nicht über längere Zeit einheitlich getroffen werden Da sich bei mehreren Personen dieses Problem entsprechend ausweitet ist der iSupport hier von großer Bedeutung. Nach Aufnahme aller neuen Charakteristika stößt der nächste iSupport eine Suche an, welche dem Vorfall den Lösungsweg des ähnlichsten bekannten Vorfalls hinzufügt.

Um den Anforderungen unterschiedlicher Nutzungs-Szenarien für unterschiedliche Umgebungen (verschiedene eServices, Organisationsstrukturen und Erfahrungsstrukturierungen) Rechnung zu tragen wurden verschiedene Varianten zur Präsentation und Modellierung der Reaktionsdarstellung mit unterschiedlichen Funktionalitäten und Formalitätsgraden realisiert. Basierend auf Beispielfällen, welche wir in und aus Diskussionen mit unserem Projektpartner entwickelt haben wurde

strukturierter Text als geeignetste Repräsentation der Reaktionsbeschreibung identifiziert. Varianten dieser Darstellungsgrundlage reichen von einem einfachen Textfeld über strukturierte Reaktionsschritte bis zu entscheidungsbaumartigen Darstellungen. Zur Planung und Ausführung länger laufender Vorfallsbearbeitungen ist eine Repräsentation auf der Basis von Schritten erforderlich. Diese Varianten unterscheiden sich wiederum bezüglich der Unterstützung paralleler Ausführung verschiedener Teilschritte. Weitere Formalisierung ist erforderlich für Schritte, die automatische Ausführung unterstützen. Abbildung 4 zeigt die von unserem Projektpartner gewählte Variante, die parallele Verarbeitung einfacher Schritte durch das IT-Sicherheitspersonal erlaubt.

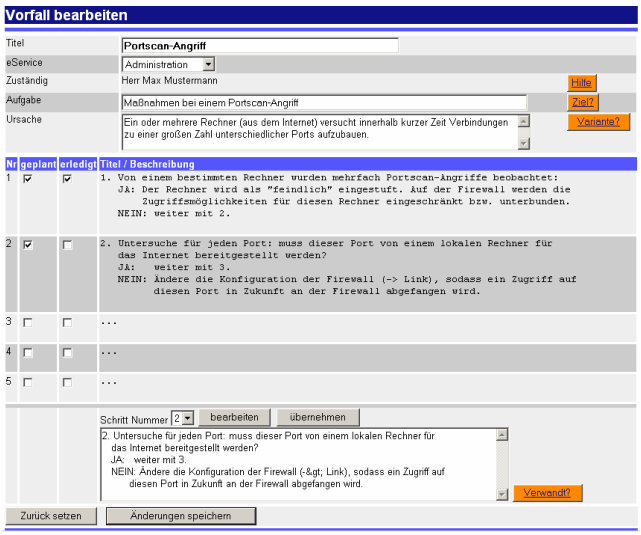

Abbildung 4: Vorfallsbearbeitung in der GUI (iSupport wurde unter anderem auch über die orangen Knöpfe initiiert)

Bei der Vorfallsbearbeitung unterstützen den Mitarbeiter mehrere iSupports, welche unaufdringlich durch einfachen Knopfdruck aktiviert werden können:

- *‚Hilfe'* unterstützt Mitarbeiter, die weitergehende Fragen zu einem Vorfall haben oder aber den Systemantworten nicht ‚so ganz' trauen. Es werden zur Unterstützung auf Basis des aktuellen Vorfalls und seiner Reaktionsbeschreibung ähnliche Vorfälle identifiziert. Dies geschieht durch eine Suche in der Erbahrungsdatenbank, welche eine Liste mit den passenden Vorfällen und Kontaktinformationen zu deren Bearbeitern zurückliefert.
- *‚Ziel'* hilft durch das Auffinden alternativer Reaktionen zur Lösung des Problems. Zu diesem Zweck wird eine Liste von Vorfällen mit ähnlichen Ursachen und Aufgabenstellung generiert.

- *‚Variante'* führt zu einer Suche nach Vorfällen mit alternativen Ursachen für das aktuelle Problem. Dies wird durch einen Vergleich der Aufgabenstellungen erreicht und es resultiert daraus eine Liste von Vorfällen, welche alternative Lösungswege anbieten.
- *‚Verwandt'* hilft dem Mitarbeiter bei dem aktuellen Lösungsschritt der Reaktionsbeschreibung durch das Auffinden von ähnlichen Schritten (im Beispiel aus Abbildung 4 kann zum Schritt 2 so Hilfe zur Firewall-Konfiguration gefunden werden). Dieser iSupport erfordert eine Schritt-Aufteilung der Reaktion in der Vorfalls-Repräsentation.

Der hier beschriebene Prozess verfeinert die Feedback-Schleife unter Berücksichtigung der Benutzerinteraktionen mit dem IT-Sicherheits-Leitstand und zeigt die Integration in den Arbeitsprozess, welcher von der Feedback-Schleife skizziert wird.

3.2 Modellierungsschema der Erfahrungen

Um das in Abschnitt 3.1 beschriebene Prozessmodel geeignet zu unterstützen sind die Vorfälle (oder einfach ‚Fälle') entsprechend dem in Abbildung 5 dargestellten Schema strukturiert. Das Schema wurde so entwickelt, dass es sowohl eine Aggregation der Fälle zwecks einer iSupport-Weiterverarbeitung zulässt (als dynamisches Handbuch zur Sicherheitsvorfallsbearbeitung), als auch Feedback und verschiedene Modelle zur Wartung unterstützt. Darüber hinaus ist die Struktur offen für Erweiterungen, die zusätzliche Funktionalitäten wie z.B. Versionsverwaltungen zulassen.

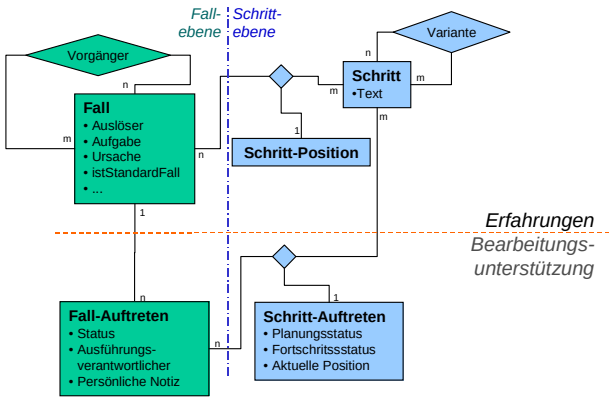

Abbildung 5: Schema für Erfahrungen über IT-Sicherheitsvorfälle und Reaktionen

Das Schema unterscheidet zwischen Standard-Fällen (‚Fall', ‚Schritt- Position', und ‚Schritt') und konkreten Fällen (‚Fall- Auftreten' und ‚Schritt-Auftreten'). Während Standard-Fälle ein vollständiges Vorgehen bei Reaktionen auf bestimmte

Situationen liefern beschreiben konkrete Fälle die Anwendung von Standard-Fällen für einen bestimmten Fall ebenso wie die von Nicht-Standard-Fällen. Die Anwendung eines Standard-Falls kann sich von diesem durch Veränderungen der Reihenfolge von Schritten und ähnlichem unterscheiden. Im Laufe der Zeit werden solche konkreten Fälle zu Standard-Fällen zusammengefügt [Nick+02]. In einem Wartungszyklus werden diese konkreten Fälle benutzt, um die Standard-Fälle zu verbessern, was dann einen Erfahrungs-basierten Verbesserungszyklus für Standard-Fälle erzeugt.

Ein konkreter Fall besteht im Kern aus einem Fall-Auftreten, welches die Attribute seines Auftretens und der aktuellen Bearbeitung an sich bindet. Neben dem Editor (ein verantwortlicher IT-Sicherheitsmitarbeiter) ist dies auch eine Vertretung (z.B. der IT-Sicherheitsbeauftragte), der Auftretenszeitpunkt und ein persönlicher Notiz-Zettel, welcher dem Bearbeiter zur freien Verfügung steht (z.B. für Eigenkontrolle oder Aufgabendelegation) und von niemand anderem einzusehen ist. Dieser kann bei Abschluss des Falles automatisch gelöscht werden. Zusätzlich zum Fallauftreten gehören auch allgemeine Fallseigenschaften (Auslöser, Aufgabe, Titel) zum konkreten Fall, werden aber zur Redundanz-Vermeidung separat verwaltet. Neben diesen allgemeinen Eigenschaften gehört auch eine schrittweise Reaktion zur Lösung der Aufgabe, welche wegen flexibler Bearbeitung, Wartung und zusätzlichen iSupport-Möglichkeiten separat im Datenmodell verwaltet wird. Die Lösungsschritte selbst besitzen textuelle Information und für jede Zugehörigkeit zu einem Fall eine Position (ein Schritt kann in verschiedenen Fällen vorkommen). Zur Planungs- und Bearbeitungsunterstützung besitzt ein Lösungsschritt weiterhin zu jedem konkreten Fall in dem er verwendet wird Statusinformationen und eine Priorität.

3.3 Wartungsprozesse und -strategien

Die Grundlage für den Benutzungsprozess ist mit diesen Vorgaben bereits vollständig beschrieben. Nun ist die Wirkung des Arbeitsprozesses auf die Erfahrungsbasis von Bedeutung. Dies gilt insbesondere für den Wartungs- und Feedback-Prozess .

Da das beschriebene Modell offen und flexibel gestaltet ist kann es für verschiedene Anforderungs-Szenarien eingesetzt werden. Kern der Flexibilisierung ist die Handhabung von Änderungen auf den vorgeschlagenen Vorfällen durch das IT-Sicherheitspersonal. Es kann grundsätzlich zwischen zwei Reaktionen innerhalb der Erfahrungsbasis unterschieden werden:

1. *Konservativ:* Änderungen an einem vorgeschlagenen Fall werden diesem nur als ‚Historie' hinzugefügt, eine Veränderung der Erfahrungsbasis findet nicht statt.

2. *Progressiv:* Jede Änderung an einem vorgeschlagenen Fall führt zur Generierung eines neuen Vorfalls und damit zu einer Erweiterung der Erfahrungsbasis.

Bei sehr sensiblen Vorfällen in bezug auf ihre innere Struktur oder weniger ausgeprägtes Erfahrungswissen des IT-Sicherheitspersonals ist die konservative Variante (1) der progressiven vorzuziehen. Bei diesem Szenario ist eine periodische (oder alternativ getriggerte) Wartung der Erfahrungsbasis durch einen Domänen-Experten erforderlich [Nick+01][Nick+02]. Dieser entscheidet, welche Historien in die Vorfälle einfließen, zu neuen Vorfällen führen oder verworfen werden.

Entgegen dieser Realisierung kann der Wartungsprozess gemäß der Variante 2 ausgelegt werden falls das IT-Sicherheitspersonal selbst aus Experten besteht und ein hohes Maß an Verantwortung mitbringen. Hier ist allerdings immer die Gefahr gegeben, dass durch fehlerhafte Neugenerierungen der Vorfälle die Erfahrungsbasis ‚verwässert'.

Um den Anforderungen der Praxis gerecht zu werden kann eine geschickte Kombination beider Varianten genutzt werden, um die manuellen Arbeiten in den Wartungszyklen zu erleichtert und dennoch ein Verwässern der Erfahrungsbasis zu verhindern.

Hierbei wird die Relevanz von Vorfällen nach der Anzahl Ihrer *unveränderten* Nutzung bewertet. Wird ein vorgeschlagener Vorfall vom IT-Sicherheitsmitarbeiter verändert, so wird aus dem gegebenen Vorfall entweder ein neuer Vorfall generiert, welcher nun eigenständig dem System zur Verfügung steht oder -falls z.B. nur eine syntaktische Korrektur vom Mitarbeiter gewünscht wurde- eine Neugenerierung unterdrückt. Bei Veränderungen kann weiterhin zwischen ‚echten' (z.B. textuellen) Änderungen der einzelnen Lösungsschritte oder aber strukturellen (Lösungsschritte löschen oder verschieben) unterschieden werden. Durch Kombinationen dieser Variantionsvielfalt und entsprechender Reaktion des Systems kann so ein beliebiger Wartungsprozess etabliert werden.

3.4 Architektur

Die Architektur des Systems ist eine Ausprägung der Erfahrungsdatenbank Produktlinienarchitektur INTERESTS[1] des IESE. Abbildung 6 gibt einen Überblick über die Referenz-Architektur der Produktlinie.

[1] INTERESTS = Intelligent Retrieval and Storage System.

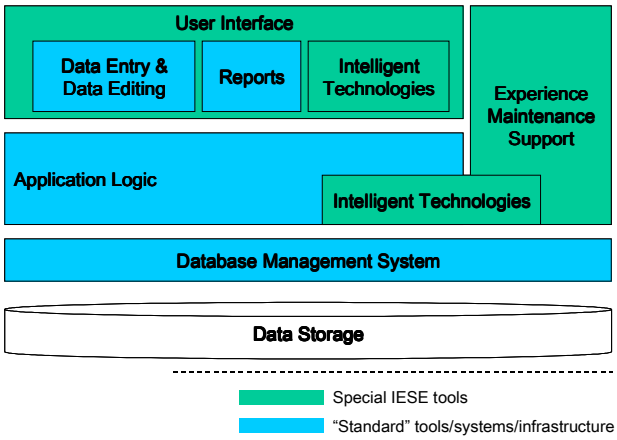

Abbildung 6: INTERESTS Erfahrungsdatenbank Tools der Produktlinienarchitektur

Die Produktlinienarchitektur basiert auf einer stabilen relationalen Datenbank. Über dem Datenbankmanagementsystem liegt die Applikationslogik, sowie die mit intelligenten Technologien angereicherte Benutzerschnittstelle. Skalierbarkeit wird hier im Bezug auf die möglichen Komponenten und das Datenbankschema erreicht. Dieses Schema muss Skalierbarkeit bereits von Anfang an unterstützen damit z.B. eine einfache intelligente Suche später durch eine komplexere ersetzt werden kann. Die Skalierbarkeit beeinflußt sowohl die Funktionalität, als auch den Preis. Beispielsweise kann ein preisgünstiges Commercial-Off-The-Shelf-Tool wie MS-Access als Datenbank leicht durch ein Open-Source-Produkt wie PostgreSQL oder eine anspruchsvolle Oracle-Datenbank ersetzt werden. Als hochentwickelte intelligente Suchmaschine wird das kommerzielle CBR-basierte Tool orenge der Firma empolis als Komponente verwendet [empolis00]. INTERESTS selbst verbindet mittels eigener Routinen alle benötigten Komponenten zu einer Gesamtlösung und liefert mit dem Wissen über Prozesse und Modellierung die notwendige Flexibilität zum Bau einer optimierten Lösung, die sich zu jedem Zeitpunkt anpassen lässt.

Für unseren Anwendungspartner implementieren wir eine kostengünstige Lösung, welche sich auf MS-Access als Datenbankmanagementsystem, J2EE-Technologien (JaverServerPages, JavaBeans, etc.) für die Benutzerschnittstelle und unsere In-house-CBR-Maschine RAISIN[1], die ähnlichkeitsbasiert auf strukturierten Texten arbeitet, stützt. Ein Überblick der GUI ist in Abbildung 4 dargestellt.

[1] RAISIN = RelAtively Intelligent SImilarity eNgine

4 Geplante Evaluation durch Fall-Studien

Die Evaluation erfolgt im allgemeinen in drei Phasen nach [NiFe00] (Abbildung 7). Zunächst wird beim Start der Systembenutzung (Phase 1) unser Standard-Modell zur Messung von Indikatoren der Systemakzeptanz durchgeführt [Nick+01][JeNi02]. Hierbei wird die Systemnutzung (z.B. Anzahl Suchen pro i-Support) mit dem Feedback bezüglich der Nützlichkeit der Erfahrungen (z.B. vorgeschlagene Reaktionen) kombiniert. Diese Kombination von Benutzung und Nützlichkeit erlaubt es schneller ein Bild über die Akzeptanz zu erhalten, als dies mit reiner Benutzungsüberwachung möglich ist. Dies ergibt sich durch die Tatsache, dass die Systemnutzung gerade in der Startphase sehr hoch sein kann, ohne einen besonderen Nutzen zu bringen, weil das System neu ist und jeder ein wenig damit ‚spielt'. Außerdem stellt das Nützlichkeits-Feedback eine sehr gute Möglichkeit dar, die wirklich interessanten und wichtigen Inhalte zu verstehen. Später in Phase 2 werden anwendungsbezogenere Entscheidungen für eine detailliertere Bewertung hinzugefügt. Phase 3 schließlich fokussiert auf den ökonomischen Wert des Systems.

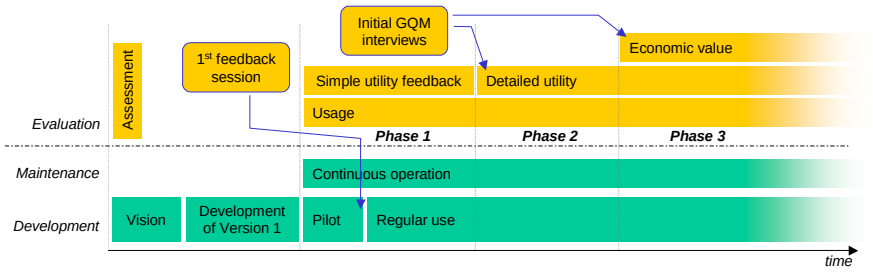

Abbildung 7: Evaluationsphasen verglichen mit Entwicklungs- und Wartungsphasen.

Wir befinden uns derzeit mit dem IT-Sicherheits-Leitstand in Phase 1 und führen daher Messungen der Benutzung sowie Analysen des Feedbacks durch. Die Ergebnisse werden zeigen, wie gut die Feedback-Schleife arbeitet.

5 Zusammenfassung und Ausblick

Wir haben eine angemessene IT-Sicherheit als essentiellen Bestandteil für E- Government-Anwendungen identifiziert. Im Rahmen des SKe-Projektes wurde schrittweise eine umfassende Lösung zur Sicherstellung der IT-Sicherheit von E-Government-Anwendungen entwickelt und getestet. Das Managen von Wissen zur IT-Sicherheit ist ein integraler Teil des SKe-Ansatzes. Wir entwickeln einen sogenannten IT-Sicherheits-Leitstand, welcher speziell zur Unterstützung von E- Government-Internetdiensten geeignet ist und durch die Nutzung von Wissensmana-

gement zur deren Verbesserung beiträgt. Das System unterstützt die systematische Aufzeichnung und Anwendung von Erfahrungen bei Reaktionen auf Sicherheitsvorfälle ebenso wie die Identifikation von Standard-Fällen und die pro- aktive Wartung der dort enthaltenen Reaktionen. Durch die Nutzung von fallbasiertem Schließen [AaPl94] als Prinzip und Technologie ist das System in der Lage intelligente Unterstützung in vielen Bereichen der Vorfallsbehandlung zu bieten, da auf Erfahrungen in ähnlchen, bereits gelösten Vorfällen zurückgegriffen werden kann. Mit dem System haben wir intelligente Unterstützung direkt im Kontext des Arbeitsprozesses integriert [AbMe01] und sowohl ein flexibles Schema, als auch eine skalierbare Architektur geschaffen, die gemeinsam eine einfache Anpassung an verschiedene Erfordernisse unterschiedlicher Einsatzumgebungen (eServices, Organisationsstruktur. etc.) ermöglichen.

Der gegenwärtige Stand der Arbeiten ist der folgende: Basierend auf einer Design-Studie, die reale Beispiele unseres Anwendungspartners verwendet, wurden sowohl Konzept, als auch Benutzerschnittstelle überprüft. Aus den in der Design-Studie enthaltenen Vorschlägen für mögliche Realisierungsformen wurden geeignete Darstellungen sowie relevante, intelligente Unterstützungsformen ausgewählt. Eine erste Version des IT-Sicherheits-Leitstandes wird gerade implementiert und wird noch im ersten Quartal 2003 für Fall-Studien zur Verfügung stehen. Ein Evaluationsplan zum Nachweis der Nützlichkeit wird die Fall-Studien begleiten. Die Erkenntnisse aus SKe werden bereits jetzt in einem Industrieprojekt mit ähnlichen Anforderungen genutzt, in dem wir für die Sicherheitsabteilung eines Unternehmens der Telekommunikationsbranche eine anspruchsvolle Wissensmanagement-Lösung konzipieren.

Entsprechend den Anforderungen und dem erwarteten Nutzen ziehen wir folgenden Schluss: Das Rollenmodell unterstützt Flexibilität bezüglich der Organisationsstruktur. Der IT-Sicherheits-Leitstand kann den unterschiedlichen Bedürfnissen nach intelligenter Unterstützung verschiedener Einsatzumgebungen (intelligente Priorisierung ist z.B. interessant für Umgebungen mit einem großen Aufkommen an Sicherheitsvorfällen) angepasst werden. Wir identifizierten für unseren Anwendungspartner eine einfache Variante der Reaktions-Modellierung, die sowohl Planung von Arbeitsschritten, als auch Ausführungsüberwachung mittels feingranularer Statuskontrolle erlaubt. Für unsere Industriepartner entwickeln wir ein komplexeres Reaktionsmodell, welches zusätzliche Eigenschaften wie z.B. ein Lösungs-Logging (Vergangenheitsbewahrung) mit positiven und negativen Erfahrungen enthält. Das Schema unterstützt verschiedene Wartungsstrategien für die Reaktionen auf Standard-Fälle, welche von konservativen bis zu progressiven Konfigurationen reichen. Dies trägt zum erwarteten Nutzen bezüglich der Nachvollziehbarkeit von Reaktionen auf Standard- und Nicht-Standard-Fälle bei. Weiterhin erlaubt die skalierbare Architektur einen kostengünstigen Start und einen späteren Ausbau der Lösung entsprechend den jeweiligen Anforderungen der Einsatzumgebung. Die Evaluation der ersten Version wird zeigen, ob der IT-Sicherheits-Leitstand die Erfahrungs-Feedback-Schleife in die Praxis umsetzen kann. Der Nutzerkreis unse-

res Anwendungspartners geht von einer effizienteren und effektiveren Problembehandlung durch die eServices aus und warten bereits auf die erste Version des IT-Sicherheits-Leitstandes.

Die nächsten Schritte sind die Fertigstellung der ersten Version und eine Fall-Studie zusammen mit unserem Anwendungspartner, um den praktischen Nutzen des IT-Sicherheits-Leitstandes nachzuweisen. In der zweiten Version fokusieren wir auf die proaktive Wartung der Reaktionsbeschreibungen bei Änderungen von eServices. Aufgrund des positiven Feedbacks unseres Anwendungspartners und der Erfahrungen in anderen Projekten gehen wir von einer Vielzahl an Verbesserungsmöglichkeiten durch die Anwendung von Wissensmanagement für die IT-Sicherheit von eServices im E-Government aus.

Danksagung

Wir bedanken uns beim Bundesministerium für Bildung und Forschung (BMBF) für die Finanzierung des SKe-Projektes (Vertragsnummer 01AK900B). Weiterhin bedanken wir uns bei unseren Kollegen am Fraunhofer IESE, den Projektmitgliedern vom Fraunhofer SIT, der TU Darmstadt und von der Arbeitsgruppe ‚Wissensbasierte Systeme' an der Universität Kaiserslautern für die fruchtbaren Diskussionen und deren Unterstützung.

Literatur

[AaPl94] A. Aamodt and E. Plaza. Case-based reasoning: Foundational issues, methodological variations, and system approaches. *AICom - Artificial Intelligence Communications*, 7(1):39–59, March 1994.

[AbMe01] A. Abecker and G. Mentzas. Active knowledge delivery in semi-structured administrative processes. In *Knowledge Management in Electronic Government (KMGov-2001)*, Siena, Italy, May 2001.

[AlNi03] K.-D. Althoff and M. Nick. *How To Support Experience Management with Evaluation - Foundations, Evaluation Methods, and Examples for Case-Based Reasoning and Experience Factory*. Springer Verlag, 2003. (to appear).

[Alt+01] K.-D. Althoff, S. Beddrich, S. Groß, A. Jedlitschka, H.-O. Klein, D. Möller, M. Nick, P. Ochsenschläger, M. M. Richter, J. Repp, R. Rieke, C. Rudolph, H. Sarbinowski, T. Shafi, M. Schumacher, and A. Stahl. *Gesamtprozess IT-Sicherheit*. Technical Report Projektbericht SKe - AP3, 2001.

[Alt97] K.-D. Althoff. Evaluating case-based reasoning systems: The Inreca case study. Postdoctoral thesis (Habilitationsschrift), University of Kaiserslautern, 1997.

[Bas+94] V. R. Basili, G. Caldiera, and H. D. Rombach. Experience Factory. In John J. Marciniak, editor, *Encyclopedia of Software Engineering*, volume 1, pages 469–476. John Wiley & Sons, 1994.

[Berg+03] R. Bergmann, K.-D. Althoff, S. Breen, M. Göker, M. Manago, R. Traphöner, and S. Wess. *Developing Industrial Case Based Reasoning Applications - The INRECA Methodology*. LNAI. Springer Verlag, 2003. (to appear).

[BMI05] Bundesministerium des Inneren (BMI). Die eGovernment-Initiative BundOnline 2005. http://www.bundonline2005.de/, 2000.

[BMWi99] German Federal Ministry of Economy and Technology (BMWi). The MEDIA@Komm initiative. http://www.mediakomm.net/, 1999.

[Bran+01] M. Brandt, D. Ehrenberg, K.-D. Althoff & M. Nick (2001). *Ein fallbasierter Ansatz für die computergestützte Nutzung von Erfahrungswissen bei der Projektarbeit*. In H. U. Buhl, A. Huther & B. Reitwiesner (Eds.), Information Age Economy, Proc. of 5th Internationale Tagung Wirtschaftsinformatik (WI'01), Heidelberg: Physica, 251-264.

[BSI02a] Bundesamt fuer Sicherheit in der Informatikstechnik (BSI). *E-Government-Handbuch*. October 2002. http://www.bsi.bund.de/.

[BSI02b] Bundesamt fuer Sicherheit in der Informatikstechnik (BSI). *IT-Grundschutz-Handbuch*. October 2002. http://www.bsi.bund.de/.

[CEG02] The Council for Excellence in Goverment. Poll "eGoverment - The Next American Revolution". http://www.excelgov.org/, September 2000.

[Dist00] G. Disterer: *Individuelle und soziale Barrieren beim Aufbau von Wissenssammlungen*. In: Wirtschaftsinformatik 42 6, S.539-546, 2000

[Ehr96] D. Ehrenberg. *Fallbasierte Entscheidungsunterstützung*. In: Wirtschaftsinformatik 38 1, S.7., 1996

[empolis00] empolis GmbH. orenge - empolis knowledge manager. http://www.empolis.com/products/prod_ore.asp, 2000.

[JeNi02] A. Jedlitschka and M. Nick. *Repository validation report*. Technical Report Project ESERNET (IST-2000-28754) - Deliverable D.4.4, Fraunhofer IESE, Kaiserslautern, Germany, 2002.

[LeDr93] L. Lewis and G. Dreo. Extending trouble ticket systems to fault diagnostics. *IEEE Network*, Nov. 1993.

[Lenz+96] M. Lenz, H.-D. Burkhard, P. Pirk, E. Auriol, and M. Manago. CBR for diagnosis and decision support. *AI Communications*, 9(3):138–146, 1996.

[Lenz+98] M. Lenz, A. Hübner, and M. Kunze. Textual CBR. In M. Lenz, H.-D. Burkhard, B. Bartsch-Spörl, and S. Weß, editors, *Case-Based Reasoning Technology — From Foundations to Applications*, LNAI 1400, Berlin, 1998. Springer Verlag.

[Lenz98] M. Lenz. Textual CBR and information retrieval - a comparison. In L. Gierl and M. Lenz, editors, *Proceedings of the Sixth German Workshop on Case-Based Reason-*

ing, volume 7 of *IMIB Series*, Berlin, Germany, Mar. 1998. Institut für Medizinische Informatik und Biometrik, Universität Rostock.

[Nick+01] M. Nick, K.-D. Althoff, and C. Tautz. Systematic maintenance of corporate experience repositories. *Computational Intelligence - Special Issue on Maintaining CBR Systems*, 17(2):364–386, May 2001.

[Nick+02] M. Nick, K.-D. Althoff, and B. Decker T. Avieny. How experience management can benefit from relationships among different types of knowledge. In M. Minor and S. Staab, editors, *Proceedings of the German Workshop on Experience Management (GWEM2002)*, number P-10 in Lecture Notes in Informatics (LNI), Bonn, Germany, March 2002. Gesellschaft für Informatik.

[NiFe00] M. Nick and R. Feldmann. Guidelines for evaluation and improvement of reuse and experience repository systems through measurement programs. In *Third European Conference on Software Measurement (FESMA-AEMES 2000)*, Madrid, Spain, October 2000.

[OECD01] Organization for Economic Development (OECD). Update on official statistics on internet consumer transactions. http://www.oecd.org/pdf/M00027000/ M00027669.pdf, 2001.

[Rie02] R. Rieke. Projects CASENET and SKe - a framework for secure eGovernment. In *Telecities 2002 Winter Conference*, Siena, Italy, December 2002. http://www.comune. siena.it/telecities/program.html.

[RuGü02] C. Rudolph S. Gürgens, P. Ochsenschläger. Role based specification and security analysis of cryptographic protocols using asynchronous product automata. In *DEXA 2002 International Workshop on Trust and Privacy in Digital Business*, pages 473–482. IEEE Press, 2002.

[Schnei00] B. Schneier. *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons, 2000.

[Schol00] C. Scholz: *Personalarbeit im IT-Bereich: Erfolgskritische Aktionsfelder*. In: Wirtschaftsinformatik Sonderheft Oktober , S. 7-8, 2000

[Ske01] SKe - Durchgängige Sicherheitskonzeption mit dynamischen Kontrollmechanismen für eService Prozesse. http://www.ske-projekt.de/, 2001.

[StWe99] M. Stolpmann, S. Wess: *Optimierung der Kundenbeziehungen mit CBRSystemen*. Bonn 1999.

[TaAl97] C. Tautz and K.-D. Althoff. Using case-based reasoning for reusing software knowledge. In D. Leake and E. Plaza, editors, *Proceedings of the Second International Conference on Case-Based Reasoning*. Springer Verlag, 1997.

[Tau01] C. Tautz. *Customizing Software Engineering Experience Management Systems to Organizational Needs*. PhD thesis, University of Kaiserslautern, Germany, 2001.

[Web+01] R. Weber, D. W. Aha, and I. Becerra-Fernandez. Intelligent lessons learned systems. *International Journal of Expert Systems - Research & Applications*, 20(1), 2001.

[WiBr02] M. A. Wimmer and B. v. Bredow. Sicherheitskonzepte fuer e-Government. Technische versus ganzheitliche Ansaetze. *DuD - Datenschutz und Datensicherheit*, (26):536–541, September 2002.