IT-Sicherheit für Geschäftsprozesse im Finanzsektor

Steffi Rudel[1] · Torsten Bollen[2]

[1]Universität der Bundeswehr München
steffi.rudel@unibw.de

[2]Wincor Nixdorf
Torsten.Bollen@dieboldnixdorf.com

Zusammenfassung

Im vorliegenden Beitrag wird die Kurzfassung einer Fallstudie zur IT-Sicherheit in Kritischen Infrastrukturen beschrieben. Die Fallstudie stellt die Managementlösung PREVENT vor, die im Rahmen eines Forschungsprojektes im Förderschwerpunkt "IT-Sicherheit für Kritische Infrastrukturen" ITS|KRITIS des BMBF entwickelt wird. Die Managementlösung PREVENT stellt Banken Dashboards zur Verfügung, um durch nutzergerechte Aufbereitung eines Lagebildes bei der Risikoeinschätzung zu unterstützen. Dieses Lagebild erlaubt ein effektives und effizientes Risikomanagement für systemkritische Geschäftsprozesse. Die vollständige Fallstudie ist in der Quelle [LDR+18] veröffentlicht sowie unter www.itskritis.de kostenfrei verfügbar.

1 IT-Sicherheit im Bankwesen

Die vorliegende Fallstudie entstand in dem Forschungsprojekt PREVENT des Förderschwerpunktes „IT-Sicherheit für Kritische Infrastrukturen" des Bundesministeriums für Bildung und Forschung (BMBF). Die Fallstudie beschreibt ein IT-Sicherheitsmanagementsystem der nächsten Generation für die als kritisch eingestuften Prozesse einer Bank: die Managementlösung PREVENT.

Für Banken ist seit Basel II das Risikomanagement von Finanztransaktionen ein wichtiges Thema. Diese Finanzrisiken werden vorrangig vom Basler Ausschuss für Bankenaufsicht in Zusammenhang mit der Eigenkapitalquote der Banken gesehen. Zunehmend treten heute jedoch die operativen Risiken in den Vordergrund. Dies sind Risiken, die sich aus Geschäftsprozessen, Menschen und Systemen, sowie deren Interaktion miteinander ergeben. Dieser Umstand findet entsprechende Beachtung u.a. in den Katalogen des IT Grundschutzes vom Bundesamt für Sicherheit in der Informationstechnik (BSI).

2 Einordnung als Kritische Infrastruktur

Kritische Infrastrukturen (KRITIS) werden vom BSI grundsätzlich in verschiedene Sektoren untergliedert. Die Fallstudie mit den beteiligten Playern siedelt sich in dem Sektor Finanz- und Versicherungswesen an [BuSI16].

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 232-235.

Ausschlaggebend für die Einordnung als KRITIS ist die kritische Versorgungsdienstleistung. Die Abwicklung des Zahlungsverkehrs ist eine kritische Dienstleistung sowohl für Privatpersonen (Erhalt des Gehalts, Bezahlen von Rechnungen, Miete, etc.) als auch für Unternehmen. Sie hat damit eine sektorübergreifende Bedeutung und ist daher die wesentliche kritische Versorgungsdienstleistung des Finanzdienstleistungssektors [BuSI16].

Der Finanzsektor stellt unter den KRITIS eine Besonderheit dar, da hier die „Finanzmittel – im Gegensatz zu anderen Wirtschaftsbereichen – nicht nur die Rahmenbedingung für das Wirtschaften, sondern den Geschäftsgegenstand selbst darstellen" [BuSI16]. Als weitere Besonderheit sind in Bankenrechenzentren sowohl die Geschäftsprozesse als auch die Infrastruktur kritisch, da ausschließlich mit Daten und nicht mit physischen Waren gehandelt wird.

3 Managementlösung PREVENT

3.1 Hintergrund und Rahmenbedingungen

In Banken sind per Gesetz grundsätzlich die Vorstände für das Risikomanagement verantwortlich und haftbar zu machen. Aus diesem Grund soll dieser Managementebene mit der Managementlösung PREVENT ein Dashboard auf Basis eines Lagebildes (Compliance Status) zur Verfügung gestellt werden. Dieses soll helfen, Risiken in Echtzeit konkret einschätzen und bewerten zu können und anschließend geeignete Maßnahmen einleiten zu können.

3.2 Abhängigkeit zwischen Prozessen und Anwendungen

Grundsätzlich lassen sich die Prozesse und Anwendungen in einem Finanzunternehmen auf verschiedenen Ebenen betrachten. Die folgende Abbildung 1 visualisiert diese Ebenen.

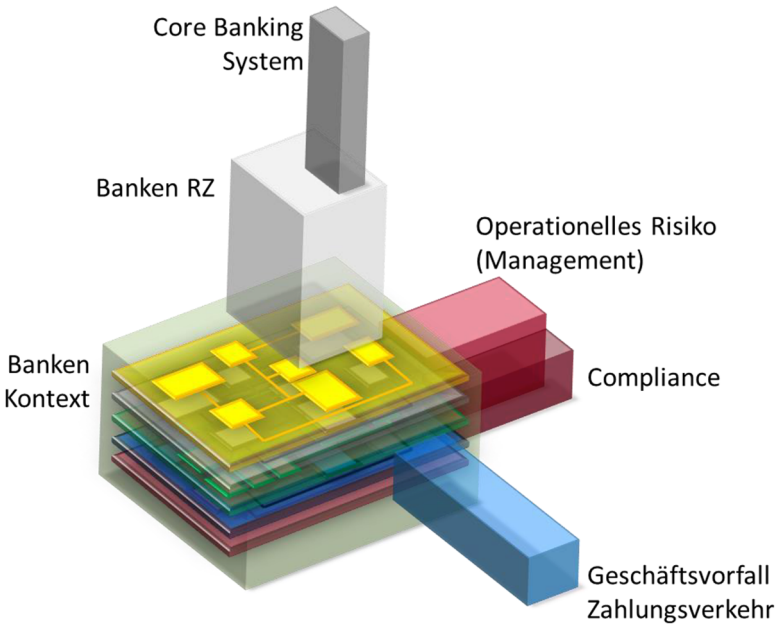

Abb. 1: Ebenen eines Finanzunternehmens

Tritt nun ein Vorfall auf einer der Ebenen auf, so darf dieser nicht isoliert auf dieser Ebene betrachtet werden. Vielmehr ist es wichtig, hier die Zusammenhänge zu erfassen. Denn um der

Managementebene ein aussagekräftiges Lagebild zur Verfügung zu stellen zu können, müssen die Risiken über alle Ebenen aggregiert werden.

Die folgende Abbildung 2 visualisiert daher den Zusammenhang zwischen den Ebenen und welche Auswirkungen ein Vorfall auf der Netzwerkebene auf die anderen Ebenen haben kann.

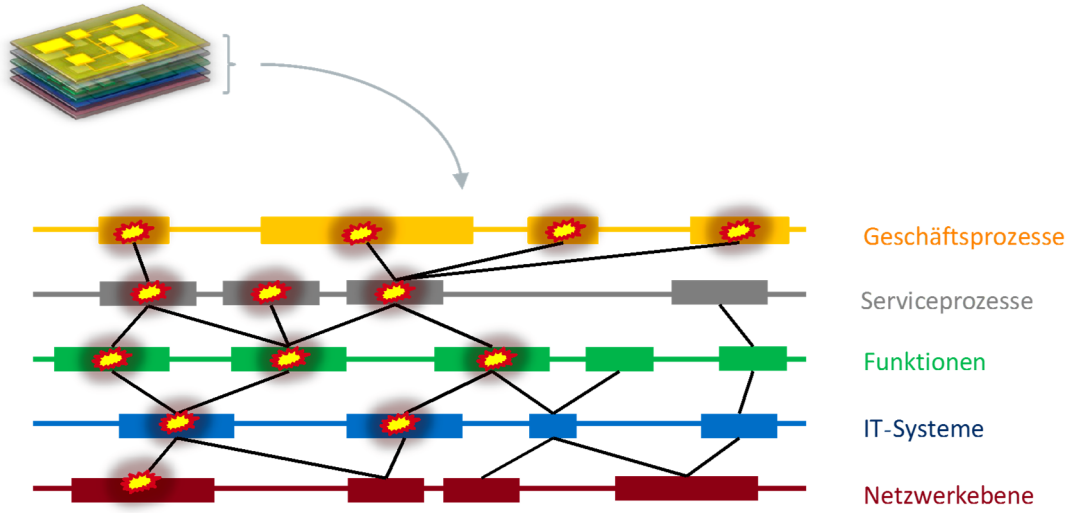

Abb. 2: Wechselwirkungen zwischen den Ebenen

3.3 Gemeinsames Lagebild zur Risikobeurteilung

Mit Hilfe der Managementlösung PREVENT sollen den Verantwortlichen fundierte Gründe für oder gegen eine Maßnahme zur Entscheidungsunterstützung an die Hand gegeben werden. Wirkungsketten sollen erkannt und potentielle Aggregationen von Risiken offengelegt werden.

Um dies umzusetzen, unterstützt die Managementlösung PREVENT bei

- der Modellierung von Businessprozessen,
- der Analyse von Betriebsprozessen und
- der Analyse der unterstützenden Infrastruktur auf Funktions-, Software und Netzwerk sowie Hardwareebene.

Dabei arbeitet PREVENT mit einer aus unterschiedlichen Quellen zusammengeführten Datenbasis. Die liefernden Quellen sind u.a: Log-Files, Zutrittskontrollsysteme oder eingesetzte SIEM-Systeme. Aus der sich ergebenden Datenbasis werden verschiedene Sichten bedarfsgerecht erzeugt. Als Herausforderungen sind hier die Big-Data-Analyse sowie das Erzeugen anwendungsgerechter Sichten zu meistern. Dadurch ist sichergestellt, dass jeder Nutzer die für sich nötige Sicht auf das Lagebild erhält.

So sollen Bedrohungspotentiale besser und schneller erkannt und im Lagebild abgebildet werden können, welches die Basis für proaktive Handlungsanweisungen geben kann.

Die folgende Abbildung 3 zeigt die implementierte Managementlösung PREVENT.

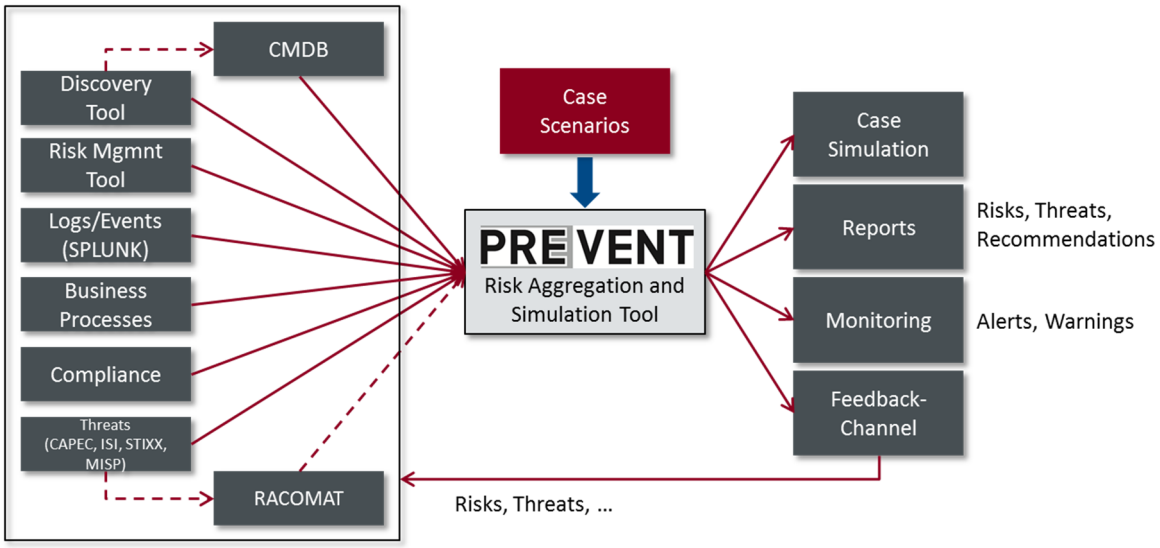

Abb. 3: Implementierte Managementlösung PREVENT

4 Resümee

Die IT-Sicherheit ist im Finanzsektor ein wichtiges Thema. Dies trifft insbesondere auf systemrelevante Bereiche wie die Bankenrechenzentren zu.

Ziel der Managementlösung PREVENT ist die gezielte Information (Dashboarding) unterschiedlicher Nutzergruppen im Unternehmen. So soll der Vorstand genauso über die aktuelle Lage informiert werden wie ein Administrator. Die Managementlösung PREVENT erlaubt neue Risikobewertungen von Aspekten und Zusammenhängen, die bisher nicht betrachtet wurden. Damit löst sie alte, oft heterogene Risikomanagementlandschaften bei den Banken ab.

Danksagung

Wir danken dem Bundesministerium für Bildung und Forschung (BMBF) für die Möglichkeit der Forschung im Rahmen des Projektes VeSiKi, Förderkennzeichen 16KIS0213K, und des Projektes PREVENT, Förderkennzeichen 16KIS0182K.

Literatur

[BuBu09] Bundesamt für Sicherheit in der Informationstechnik; Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2009): Sektoren- und Brancheneinteilung Kritischer Infrastrukturen. Online verfügbar unter http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sektoren_node.html, zuletzt geprüft am 25.04.2018.

[BuSI16] Bundesamt für Sicherheit in der Informationstechnik: P107 Finanz- und Versicherungswesen – Analyse Kritischer Infrastrukturen in Deutschland (2016).

[LDR+18] U. Lechner, S. Dännart, A. Rieb, S. Rudel: CASE KRITIS – Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen, Logos (2018).