Computer Emergency Response Team (CERT): Analyse, Konzept und Umsetzung

Diplomarbeit

zur Erlangung des Grades eines Diplom-Ökonomen der
Wirtschaftswissenschaftlichen Fakultät der Universität Hannover

Vorgelegt von

Marcel Röhl

[redacted]

Erstprüfer: Prof. Dr. Michael H. Breitner

Hannover, den 10.04.2006

Inhaltsverzeichnis

1 Einleitung

1.1 Ausgangspunkt und Motivation

„Deutschland ist auf dem Weg in die Informations- und Wissensgesellschaft im vergangenen Jahr einen großen Schritt vorangekommen.“[1] Mit dieser Feststellung wird im Jahr 2006 die BITKOM-Studie *Daten zur Informationsgesellschaft* eingeleitet.

Information[2] ist in unserer Gesellschaft zu einem bedeutenden Produktionsfaktor geworden. Die Beutung von Informations- und Kommunikationstechnologien nimmt ständig zu. Das Funktionieren unseres gesellschaftlichen und wirtschaftlichen Zusammenlebens wäre ohne diese Technologien undenkbar. Der Bedarf nach Informationsverarbeitungskapazitäten steigt kontinuierlich und die Systeme, die diesen Bedarf befriedigen sollen, werden zunehmend komplexer.[3] Einhergehend mit der immer stärkeren Vernetzung von Informationssystemen[4] nimmt auch die Anzahl der Angriffe weiter zu. Durch die technologische Entwicklung werden Angriffe auf Systeme einer wachsenden Bevölkerungsgruppe immer leichter möglich,[5] wie die folgende Abbildung (Abb. 1) zeigt:

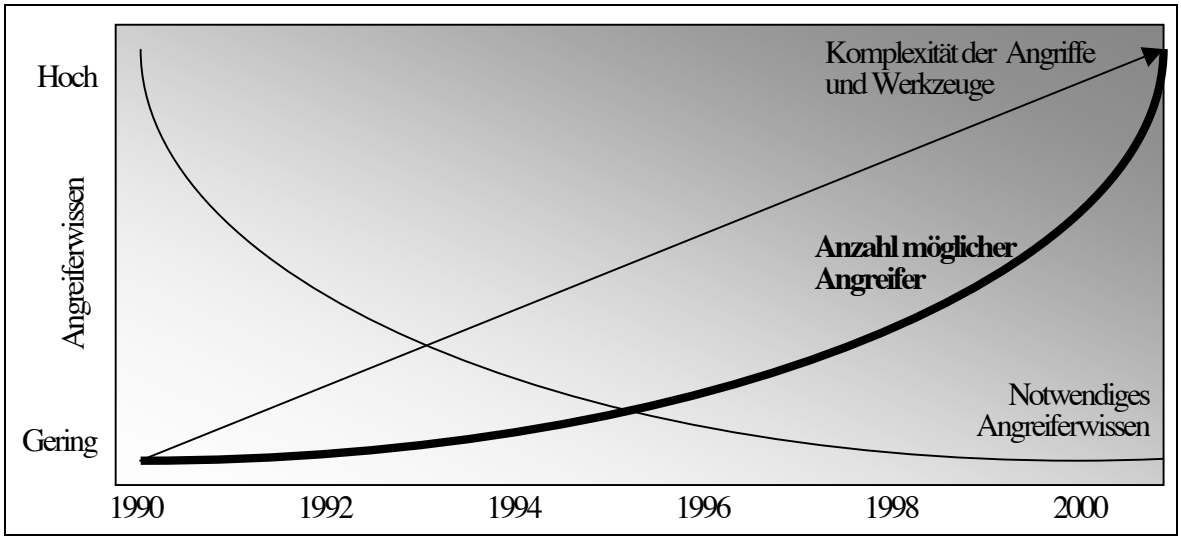

Abbildung 1: Bedrohungssituation

Quelle: Eigene Darstellung in Anlehnung an CERT/CC [2003, S. 18f.].

[1] Vgl. BITKOM [2006, S. 3].
[2] Zu Informationen vgl. Abschn. 2.1.2.
[3] Vgl. u. a. Müller [2003, S. 1]; Sonntag [2005, S. 1f.]; Welsch/Frießem [2005, S. 651f.].
[4] Informationssysteme (IS) umfassen technische Einrichtungen (Computer, Software, Netze) und Menschen (meist in Organisationen), die diese zur optimalen Bereitstellung von Informationen und zur Kommunikation nutzen. Vgl. Breitner [2005, S. 9]; Krcmar [2003, S. 25].
[5] Ein Angreifer braucht heute kein hohes technisches Wissen mehr, sondern kann sich im Internet zahlreiche Angriffstools zeitnah beschaffen.

Die Angriffe und die dabei verwendeten Werkzeuge werden selbst komplexer und zunehmend höher entwickelt. Das Zeitfenster, von der Entdeckung einer Sicherheitslücke bis zu deren Ausnutzung verkleinert sich[6] und Angriffe verbreiten sich weltweit zunehmend schneller über das Internet und weitere angeschlossene Netze, mittlerweile innerhalb von Minuten.[7] Sie können von jedem beliebigem Ort und zu jeder Zeit global ausgeführt werden, jeder Betreiber eines Informationssystems muss jedoch schnellstmöglich lokal reagieren. Es besteht eine asymmetrische Bedrohungsstruktur.[8] Die Anzahl der berichteten Sicherheitsvorfälle nimmt rapide zu (vgl. Abb. 2).

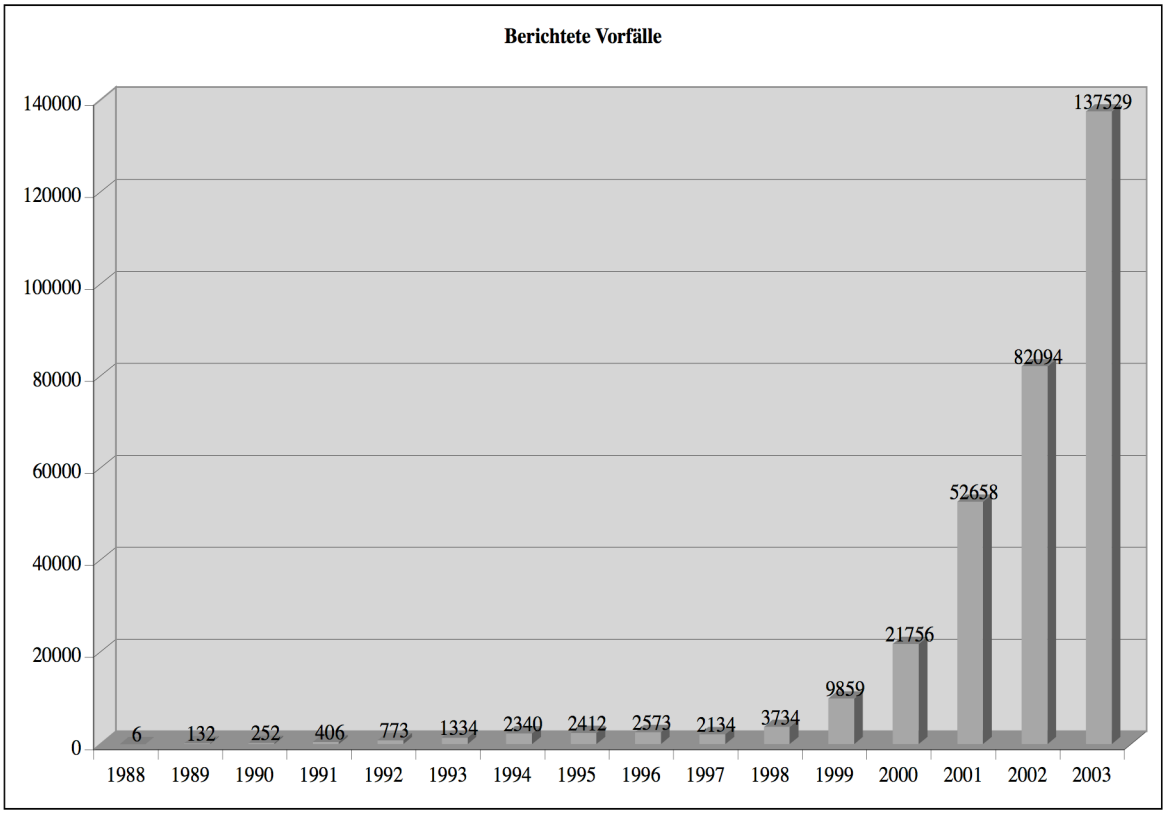

Abbildung 2: Anzahl der berichteten Vorfälle 1988-2003.
Quelle: Eigene Darstellung in Anlehnung an CERT/CC [2006].

[6] Der Wurm „Nimbda“ im Juli 2001 brauchte noch 11 Monate von der Kenntnisnahme der genutzten Sicherheitslücke bis zu seinem Erscheinen. „Blaster“ erschien im August 2003 bereits nach drei Wochen und „Witty“ im März 2004 nach nur einem Tag.
[7] Brauchte der Wurm „Code Red“ im Juli 2001noch Tage, um sich weltweit zu verbreiten, so gelang „Nimbda“ dies innerhalb von Stunden und „Slammer“ im Januar 2003 innerhalb von Minuten.
[8] Vgl. Welsch/Frießem [2005, S. 652].

Diese Umstände können aufgrund der hohen Bedeutung des Funktionierens dieser Systeme für unsere Gesellschaft nicht tatenlos hingenommen werden. Gerade bei den sog. Kritischen Infrastrukturen sind Störungen mit möglicherweise gravierenden Auswirkungen auf große Teile der Gesellschaft verbunden.[9]

Entsprechende Sicherheits- und Abwehrkonzepte sind gefragt, nicht nur auf der rein technischen, sondern vor allem auch auf der organisatorischen Ebene. Schnelles weltweites Reagieren ist von immer größerer Bedeutung. Dazu ist ein zeitnaher und umfassender Informations- und Wissensaustausch notwendig. Zu diesem Zeck wird seit dem ersten sog. Internet-Wurm im Jahr 1988 ein Konzept für die Abwehr von Computer-Notfällen mit entsprechender weltweiter Infrastruktur entwickelt und ständig ausgebaut. Diese Computer-Notfall-Teams (CERT) finden weltweit in unterschiedlichsten Institutionen zunehmend Verbreitung als Antwort auf die heutige und zukünftige Bedrohungslage.

1.2 Problemstellung und Zielsetzung

Im Rahmen dieser Arbeit soll nun der Frage nachgegangen werden, ob Institutionen wie bspw. die Landesverwaltung Niedersachsen, die selbst aktuell im Rahmen eines Projektes Notwendigkeit und mögliche Umsetzungen prüft, ein eigenes CERT benötigen, oder ob sie der Bedrohungslage anders begegnen können, z. B. durch individuelle Schutzkonzepte oder durch die Nutzung der Dienstleistungen eines bestehenden CERTs.

Hierzu ist es von Bedeutung zu analysieren, was ein CERT exakt ausmacht und wie das Konzept dieser Form der Abwehr von IT-Sicherheitsvorfällen gestaltet ist.

Im Falle der eigenständigen Realisierung stellt sich dann die Frage, wie eine optimale organisatorische Umsetzung unter der Berücksichtigung der individuellen Situation anhand des Beispiels der Landesverwaltung Niedersachsen aussehen kann. Ziel der Arbeit ist es, Gestaltungsempfehlungen für eine mögliche Realisierung zu geben.

Hierbei sind die Eingliederung in die bestehenden Strukturen und der Aufbau des Teams an sich von Interesse. Besonders zu berücksichtigen sind bereits bestehende IT-Sicherheitsstrukturen, die Möglichkeiten des Fremdbezuges und die Zusammenarbeit mit anderen CERT-Organisationen.

---

[9] Zu den sog. Kritischen Infrastrukturen in Staat und Gesellschaft zählen Transport/Verkehr, Energie, Gefahrenstoffe, IT/Telekommunikation, Finanz-/Geld-/Versicherungswesen, Versorgung, Behörden/Verwaltung/Justiz und Sonstige (Medien, Großforschung, Kulturgut.). Vgl. BSI [o. A. c, S. 1f.]; Sonntag [2005, S. 37].

1.3 Aufbau der Arbeit

Der Thematik der organisatorischen Umsetzung eines CERT soll sich zuerst in Kapitel 2 mit einer Definition der Informationssicherheit angenähert werden, bevor dann das CERT-Konzept als möglicher Bestandteil dargestellt wird. Dazu werden im ersten Abschnitt die Beweggründe für eine Auseinadersatzung mit dem Thema Informationssicherheit erläutert, bevor die Säulen und danach Grundwerte der Informationssicherheit erläutert werden. Daran anschließend wir das CERT-Konzept dargestellt, beginnend mit Gefährdungspotentialen der Informationssicherheit, die sich in Sicherheitsvorfällen ausprägen können, gefolgt von den Aufgaben von Computer-Notfall-Teams als Antwort darauf.
In Kapitel 3 werden dann im ersten Abschnitt wesentliche Grundlagen der Organisation zum Verständnis dieses Phänomens erläutert, bevor im zweiten Abschnitt die mögliche Einbindung der IT-Aktivitäten in den Organisationsaufbau einer Institution behandelt wird. Um zu ermitteln wie Informationssicherheit organisatorisch umgesetzt werden kann, folgt eine Darstellung des IT-Grundschutzkonzeptes des BSI, in dem neben konkreten Maßnahmen auch Empfehlungen zur Vorgehensweise und zur aufbauorganisatorischen Verankerung von Informationssicherheit gegeben werden. Daran anschließend wird kurz die prozessorientierte ITIL-Vorgehensweise beschrieben, die in allen wesentlichen Prozessen wie auch im Gesamtkonzept den Sicherheitsgedanken mit einschließt. So sollen in diesem Kapitel grundsätzlich denkbare Formen der Organisation eines CERTs ermittelt werden.
Das Kapitel 4 gibt einen Überblick über bestehende CERT-Strukturen und die momentan vorhanden IT-Sicherheitsmaßnahmen der Landesverwaltung Niedersachsen, um einen Ist-Zustand festzustellen. Einleitend wird dazu im ersten Abschnitt die historische Entwicklung des CERT-Konzeptes kurz umrissen, bevor exemplarisch einige bestehende CERTs in Deutschland dargestellt werden, die ihre Existenz kommunizieren und teilweise auch umfangreichere Details offenlegen. Daran anschließend werden die wesentlichen Zusammenschlüsse auf internationaler, nationaler und Europaebene erläutert. Es folgt ein Überblick über die Verwaltungstruktur des Landes Niedersachsen und die bisher eingeleiteten ganzheitlichen Maßnahmen zur IT-Sicherheit.
In Kapitel 5 werden die Ergebnisse einer empirischen Untersuchung im Rahmen dieser Arbeit zusammenfassend dargestellt. Das Ziel dieser Untersuchung war, mehr über organisatorische Realisierungen des CERT-Konzeptes zur erfahren, um dann in Kapitel 6 auf

Basis der gesamten bisher im Gang dieser Arbeit ermittelten Erkenntnisse Gestaltungsempfehlungen, also einen Soll-Zustand, zur praktischen Umsetzung zu entwickeln. Abschließend werden die wesentlichen Ergebnisse dann in Kapitel 7 kurz zusammengefasst.

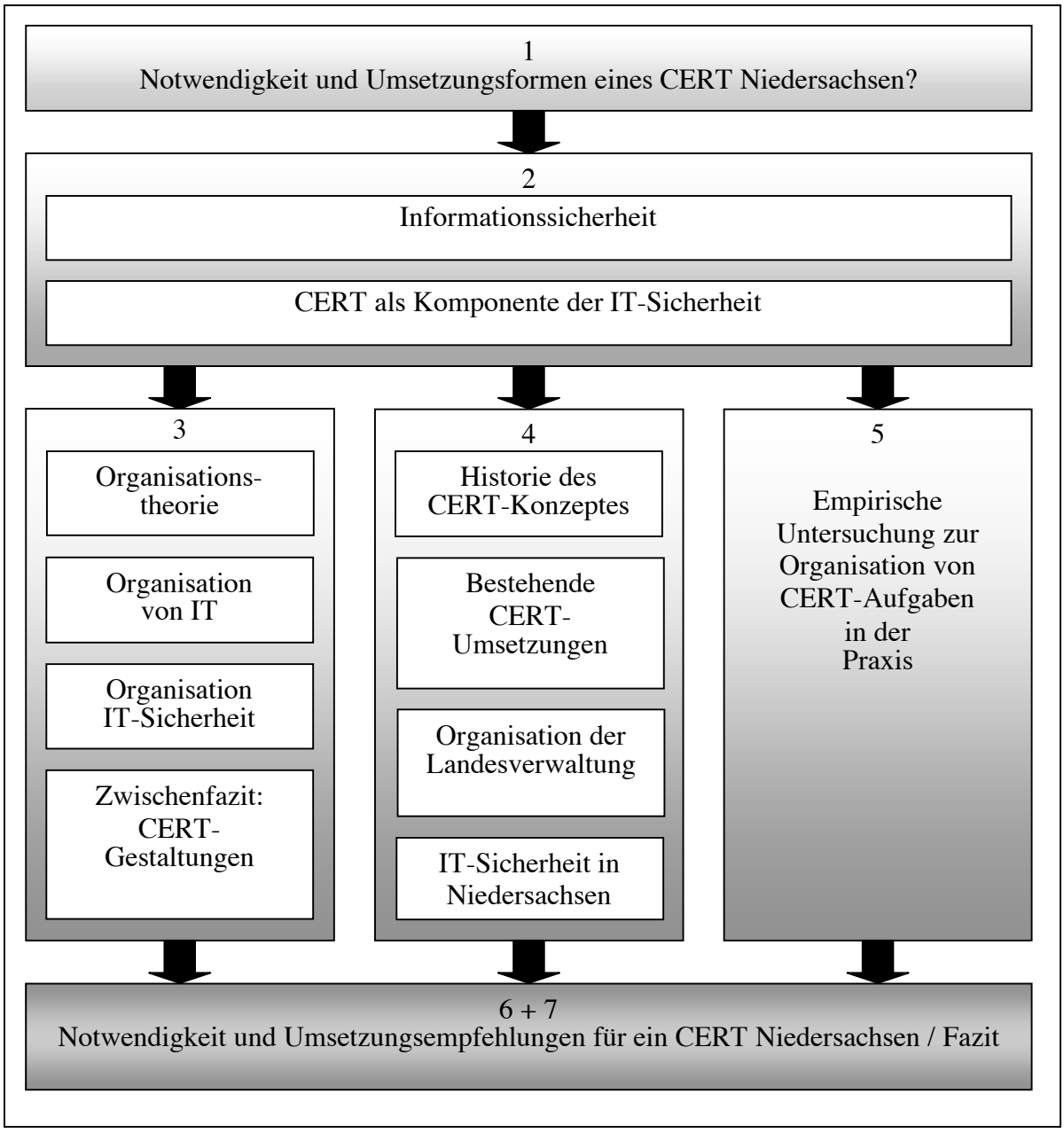

Abbildung 3: Aufbau der Diplomarbeit

7 Fazit: Notwendigkeit, Struktur und Eingliederung eines CERT Niedersachsen

Die Bedeutung der uneingeschränkten Funktionsfähigkeit von Informationssystemen in Unternehmen und öffentlichen Verwaltungen kann nicht oft genug betont werden, besonders im Bereich der sog. Kritischen Infrastrukturen in Staat und Gesellschaft. Zum Schutz der Informationen und IuK-Systeme dieser Institutionen hat sich von den Verneigten Staaten ausgehend weltweit das CERT-Konzept etabliert. Die globale CERT-Infrastruktur wächst beständig: Es werden zunehmend neue Teams gegründet und die Zusammenarbeit, die wesentlicher Bestandteil des Konzeptes ist, nimmt auf bilateraler, nationaler und internationaler Ebene zu.

Der öffentlichen Verwaltung eines Landes wie Niedersachsen kann aufgrund ihrer Bedeutung für die Gesellschaft nur dringend empfohlen werden, der wachsenden und an Komplexität zunehmenden Bedrohungslage durch Implementierung eines eigenen internen CERTs zu begegnen.

Dieses CERT sollte aufgrund der vorhandenen Organisationsstruktur als eine Kombination von verteilten Elementen in den einzelnen Ressorts bzw. Behörden und einem zentralen Koordinationsteam (CERT-CC) an der Spitze umgesetzt werden. Eine Kopfstelle ist zwingend notwendig, da Informationsflüsse und Maßnahmen in der verteilten Struktur koordiniert werden müssen und eine zentrale Wissensbasis notwendig ist. Die dezentralen Aufgaben sollten dabei weitestgehend durch bestehendes Personal in den Ressorts geleistet werden, die weiterhin die Dienstaufsicht über diese Mitarbeiter behalten, was allein aufgrund der Ressorthoheit unumgänglich ist. Auch unter Kostengesichtspunkten erscheint diese Lösung ideal, da nur wenig zusätzliche Personalressourcen benötigt werden. Zudem wird eine optimale Durchdringung der Gesamtorganisation erreicht.

Die Leitung des CERT-CC kann durch den CISO erfolgen oder sollte diesem zumindest direkt unterstellt werden. Nur durch diese Form kann die Anbindung an die politische Führung des Landes erfolgen. Eine rein operativ-technische Verankerung kann nicht empfohlen werden.

Von besonderer Bedeutung durch die empfohlene Umsetzungsform ist die klare Regelung von Kompetenzen, Befugnissen und Schnittstellen des CERT-CC zu anderen Organisationseinheiten. Die Form der Zusammenarbeit sollte zur Verhinderung von Konflikten möglichst

klar geregelt werden und die einzelnen Elemente des CERT optimal miteinander verzahnt werden, die betrifft auch Aufgaben, die von anderen Dienststellen oder durch externe Partner geleistet werden. Die teilweise Aufgabenerfüllung durch vorhandene Organisationseinheiten in der Landesverwaltung (z.B, izn KITS, LKA, CERT Polizei) sollte genau geprüft und möglichst integriert werden, um kosteneffizient arbeiten zu können. Für Krisenfälle, in denen Sicherheitsvorfälle größere Teile der Informationsinfrastruktur bedrohen, müssen vorab unbedingt klare Regelungen getroffen werden, um Schäden zu minimieren und eine Ausweitung zu begrenzen.

Über alle Ebenen der Verwaltung ist die Bildung und Förderung des Sicherheitsbewusstseins dringend anzuraten, da sonst ein Sicherheitsniveau durch das CERT schwer aufzubauen und zu halten ist.

Schon unter Kosten- und Kapazitätsgesichtspunkten sollten Teilleistungen von etablierten Dienstleistern auch extern bezogen werden. Diese können häufig ihre wesentlich höhere Expertise in Teilbereichen durch breite Nutzung kostengünstiger in Dienste umsetzen. Dabei dürfen Kontrolle und Verantwortung aber nicht aus der Hand gegeben werden.

Zum Abschluß soll nochmals die Notwendigkeit der institutionenübergreifenden Zusammenarbeit bekräftigt werden, die erst eine globale Reaktion auf die globale Bedrohung ermöglicht. In den erläuterten Vereinigungen erfolgen aktueller Informations- und Erfahrungsaustausch, wodurch schnellere und bessere Reaktionen ermöglicht und die eigene Wissensbasis erweitert wird.

Es bleibt abzuwarten, in welcher Weise die Landesverwaltung Niedersachsen der Herausforderung zukünftig begegnet. Handlungsbedarf besteht zweifellos.