Kritische Erfolgsfaktoren für ein
Computer Emergency Response Team (CERT)
am Beispiel CERT-Niedersachsen

D i p l o m a r b e i t

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

vorgelegt von:
Stefan Hoyer

[redacted]

Erstprüfer: Prof. Dr. Michael H. Breitner

Hannover, den 22.02.2006

Inhaltsverzeichnis

Seite

1 Einleitung

1.1 Problemstellung

In den vergangenen Jahren ist durch das Internet die Vernetzung von Rechnern schneller vorangeschritten, als die Globalisierung insgesamt. Über das weltweite Datennetz werden immer mehr Transaktionen und Geschäfte abgewickelt. Im Grunde hat jedes Unternehmen und jede öffentliche Verwaltung heutzutage schützenswerte Informationen und IT-Infrastrukturen. Doch trotz der vielfach eingesetzten IT-Sicherheitsmaßnahmen werden permanent neue Schwachstellen in Betriebssystemen und Programmen entdeckt oder z. B. Viren und Trojaner in Umlauf gebracht. Heutzutage werden Sicherheitslücken zunehmend schneller und auch vermehrt für kriminelle Machenschaften (z. B. Sabotage, Industriespionage, Datendiebstahl) ausgenutzt und verursachen somit immer beträchtlichere Schäden.[1] Neben den bekannten sind es oftmals die unbemerkt und nach neuen Mustern ablaufenden Einbruchsversuche bzw. erfolgreichen Einbrüche in ein IT-System, die einen immensen Wertschaden und Imageverlust für betroffene Organisationen bedeuten können. Durch eine verstärkte Automatisierung von Angriffen ist die Anzahl der gemeldeten Vorfälle in den letzten Jahren so gewaltig angestiegen, dass das CERT Coordination Center mittlerweile auf deren Veröffentlichung verzichtet (Abbildung 1 auf Seite 2).[2] Die Nachfrage nach Fachkräften auf diesem Gebiet ist somit eindeutig vorhanden. Nicht umsonst werden seit dem Aufbau des ersten Computer Emergency Response Teams (CERT) 1988 weltweit immer neue Kompetenzteams errichtet, die im Grunde ein gemeinsames Ziel verfolgen: das Internet sicherer zu machen und die betreuten Anwender und ihre IT-Systeme in diesem Zusammenhang vor Bedrohungen unterschiedlicher Art zu bewahren.[3]

Doch trotz eines großen Bedarfes an sachkundigen Kapazitäten, und nicht zuletzt aus ökonomischen Überlegungen heraus, stellt sich irgendwann die Frage, *was erfolgreiche von weniger erfolgreichen Computer-Notfallteams unterschei-*

---

[1] Vgl. Stoffel [2004, S. 486f.].
[2] Vgl. CERT Coordination Center [2006c]. Über eine viel höhere Dunkelziffer von nicht gemeldeten Vorfällen kann nur spekuliert werden.
[3] Einen Überblick über spezielle Bedrohungen bietet z. B. Eckert [2004, S. 32ff.].

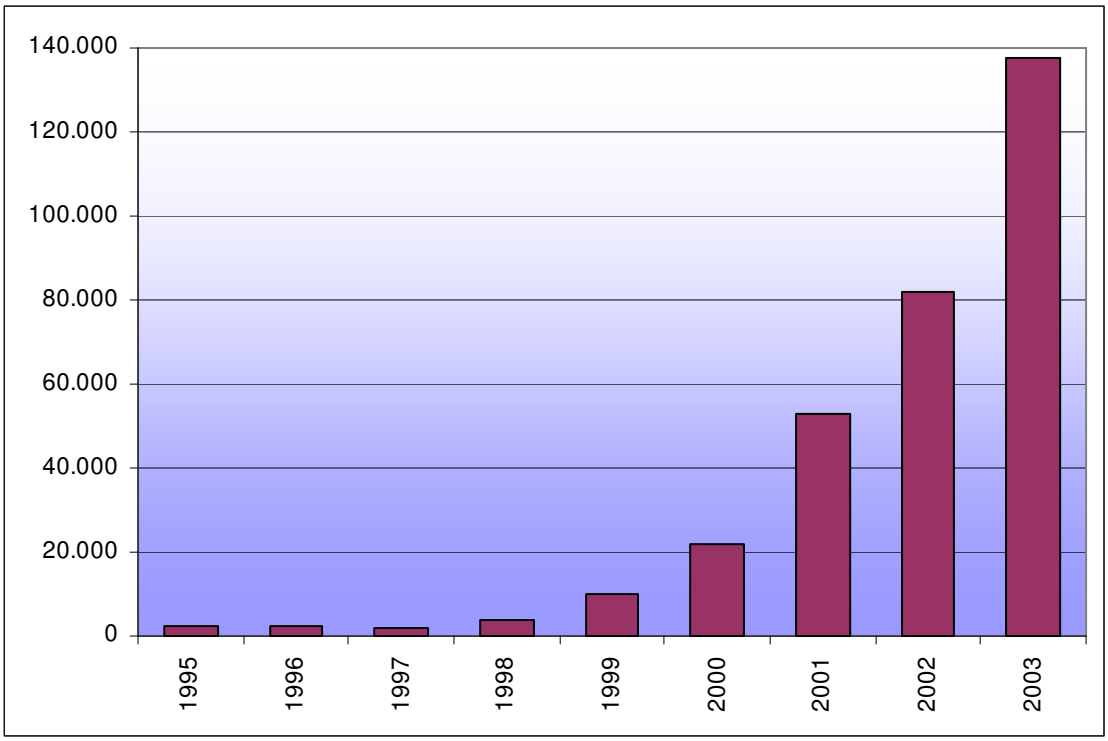

Abbildung 1: Gemeldete Vorfälle an das CERT Coordination Center (1995 - 2003)
Quelle: Eigene Darstellung in Anlehnung an CERT Coordination Center [2006c].

det und wie deren Erfolg für andere operationalisiert werden kann. Als Ausgangspunkt für diese Arbeit wird deshalb von der These ausgegangen, *dass ein Computer-Notfallteam nur erfolgreich sein kann, wenn bestimmte Erfolgsfaktoren, die bei dem Aufbau und dem Betrieb eines CERTs existieren, rechtzeitig erkannt und beachtet werden.*[4]

Aus dem Thema der Arbeit und der angeführten These lassen sich zusammenfassend diverse Fragestellungen ableiten. Prinzipiell muss in einem ersten Schritt geklärt werden, *aus welchen grundlegenden Merkmalen ein Computer-Notfallteam besteht, welche Aufgaben es wahrnimmt und welche Organisationsmodelle generell zum Einsatz kommen können.* In einem zweiten Schritt ist zu ermitteln, *wie der geschichtliche Hintergrund aussieht und welche bedeutenden Organisationen in diesem Umfeld bestehen.* Ein Kernziel dieser Arbeit besteht nun darin *herauszuarbeiten und zu überprüfen, welche Faktoren für den Erfolg oder den Misserfolg ein CERTs entscheidend sein können.* Ansetzend an diesen Ergebnissen soll abschließend den Fragen nachgegangen werden, *wie das Vorhaben in Niedersachsen zum Aufbau eines eigenen Computer-Notfall-*

[4] Vgl. Killcrece u. a. [2003a, S. 35], Pattloch/Kossakowski [2001, S. 28ff.], Smith [1995, S. 35].

teams momentan aussieht, wie es insgesamt zu beurteilen ist und welche Empfehlungen sich für dessen Gestaltungen ableiten lassen.

1.2 Methodik zur Gewinnung der Ergebnisse

Für die Grundlagen dieser Arbeit wurden zahlreiche Quellen gesichtet und bearbeitet. Die Erkenntnisse und Hypothesen bezüglich der potenziellen Erfolgsfaktoren von Computer-Notfallteams basieren auf einer systematischen Auswertung verfügbarer Literaturquellen. Alle relevanten Quellen wurden auf Erfolgsaussagen hin durchsucht, welche in der Folge zu Oberbegriffen zusammengefasst wurden. Die Informationen über das CERT-Niedersachsen stammen überwiegend aus projektinternen Papieren.

Zur Überprüfung und Würdigung der aus der Literatur extrahierten potenziellen Erfolgsfaktoren wurde eine empirische Untersuchung in begrenztem Umfang durchgeführt. Zu Anfang war diese als Telefoninterview angedacht, musste dann jedoch aufgrund von Sicherheitsbedenken auf Seiten der Teilnehmer in schriftlicher Form durchgeführt werden. Dazu wurde ein fünfseitiger Fragebogen entwickelt und zur Beantwortung an Vertreter verschiedener Computer-Notfallteams in ganz Deutschland versendet.

1.3 Aufbau der Arbeit

Die vorliegende Arbeit gliedert sich in insgesamt sieben Kapitel. Eine Einführung in das Thema und die Darstellung der zugrunde liegenden Fragestellungen erfolgt in Kapitel 1. In Kapitel 2 werden zunächst notwendige theoretische Grundlagen erläutert, die zum Verständnis dieser Arbeit notwenig sind. Dazu gehören sowohl die Aspekte der IT-Sicherheit als auch grundlegende Begrifflichkeiten zu Computer Emergency Response Teams (CERT). Direkt im Anschluss daran gibt Kapitel 3 einen Überblick über die geschichtliche Entwicklung des Incident Handlings und stellt wichtige Organisationen aus diesem Bereich dar. Damit sollen sowohl ein Verständnis für die Bedeutung und die Wichtigkeit von Computer-Notfallteams geschaffen als auch Kooperationsmöglichkeiten aufgezeigt werden.

Unter Verwendung dieser Grundlagen befasst sich das vierte Kapitel intensiv mit möglichen Erfolgsfaktoren von CERTs. Anhand einer systematischen Aus-

wertung verfügbarer Literatur werden zunächst Sachverhalte gesammelt und daraus Hypothesen abgeleitet. Diese Annahmen sind zugleich Ausgangspunkt für die Entwicklung eines Fragebogens zu deren empirischer Überprüfung. Nach einer kurzen Erläuterung zum Aufbau der empirischen Untersuchung werden in Kapitel 5 die Ergebnisse ausgewertet und Erkenntnisse in Bezug auf potenzielle Erfolgsfaktoren von Computer-Notfallteams formuliert. Diese Erkenntnisse werden schließlich in Kapitel 6 auf das CERT des Landes Niedersachsen angewendet. Dazu werden einleitend die Rahmenbedingungen in Niedersachsen analysiert und darauf aufbauend Gestaltungsempfehlungen für das niedersächsische Computer-Notfallteam ausarbeitet. Abschließend reflektiert Kapitel 7 noch einmal kurz die gewonnenen Ergebnisse dieser Arbeit.

2 Allgemeine Grundlagen zu Computer Emergency Response Teams (CERT)

2.1 Anforderungen an IT-Sicherheit als Arbeitsgrundlage eines CERTs

2.1.1 Begriff der IT-Sicherheit und deren Eigenschaften

Der Begriff der IT-Sicherheit wird nicht immer einheitlich verwendet und je nach Spezialisierung z. B. auch als Informationssicherheit, Netzwerksicherheit oder Datensicherheit bezeichnet.[5] Im Grundsatz drücken alle diese Begriffsbestimmungen aus, dass ein Objekt vor Beeinträchtigungen geschützt wird und im Rahmen normaler Parameter funktioniert.[6] Etwas detaillierter formuliert dies z. B. Krampert, der IT-Sicherheit definiert, als „(…) das Vorhanden sein von Integrität, Verbindlichkeit, Verfügbarkeit und Vertraulichkeit in einem geplanten Ausmaß.“[7] In der Literatur finden sich verschiedene dieser qualitativen Eigenschaften, die mitunter als „Ziele“[8], „Aspekte“[9] oder auch „Gefahren“[10] der IT-Sicherheit bezeichnet werden. Dierstein bezeichnet diese Eigenschaften dage-

---

[5] Vgl. Hoppe/Prieß [2003, S. 22ff.].
[6] Vgl. Stahlknecht/Hasenkamp [2005, S. 479], Aebi [2004, S. 4], Königshofen [2002, S. 653].
[7] Krampert [2003, S. 20].
[8] Vgl. z. B. Eckert [2004, S. 6], BITKOM [2003], Rannenberg u. a. [1999, S. 19].
[9] Vgl. z. B. Hoppe/Prieß [2003, S. 14], Schumann [2003, S. 98], Hansen/Neumann [2001, S. 174].
[10] Vgl. z. B. Stahlknecht/Hasenkamp [2005, S. 480], Königshofen [2002, S. 653].

6.4 Zwischenfazit

Zu Beginn dieses Kapitels wurden Rahmenbedingungen dargestellt, bestehend aus der Situation Niedersachsens und den aus dem Projektauftrag und den vorliegenden Zwischenergebnissen hervorgehenden Informationen. Im Rahmen der Möglichkeiten wurde eine darauf folgende vorsichtige Bewertung der Erfolgsaussichten eines CERT-Niedersachsen vorgenommen. Der Kern dieses Kapitels bestand jedoch darin, die kritischen Erfolgsfaktoren eines Computer-Notfallteams auf Grundlage der vorangegangenen Ausführungen auf Niedersachsen zu beziehen und konkrete Gestaltungsempfehlungen abzuleiten.

Es ist deutlich zu erkennen, dass Niedersachsen auf dem richtigen Weg ist. Die Notwendigkeit von Maßnahmen zur Verbesserung der IT-Sicherheit und deren Aspekte im Einzelnen wurden schon lange erkannt. Der Grundstein für weitere Komponenten in der IT-Sicherheitsorganisation des Landes Niedersachsen ist u. a. durch den geplanten Aufbau eines Computer-Notfallteams gelegt worden. Insgesamt bleibt jedoch abzuwarten, wie die wirkliche Ausgestaltung der Folgeprojekte aussieht und der tatsächliche Erfolg des gesamten Vorhabens in diesem Zusammenhang letztendlich ausgeprägt ist. Es ist durchaus denkbar, dass später auch andere Lösungen realisiert werden, als im Rahmen des Vorprojektes oder dieser Arbeit in Betracht gezogen wurden.

7 Fazit

Als Ausgangspunkt für die Betrachtung von Computer-Notfallteams wurden zu Beginn der Arbeit (Kapitel 2) zunächst die Aspekte der IT-Sicherheit erläutert. Diese umfassen sowohl eine technische (Vertraulichkeit, Integrität, Verfügbarkeit) als auch eine nicht-technische Sicht (Zurechenbarkeit, Verbindlichkeit, Authentizität). Im weiteren Verlauf des zweiten Kapitels wurden dann wichtige Rahmenbedingungen dargestellt, die kennzeichnend für ein CERT sind (z. B. Mission Statement, Constituency, Autorität). Die Dienstleistungen eines Computer-Notfallteams lassen sich generell in Reaktion (z. B. Vorfallsbearbeitung), Prävention (z. B. regelmäßige Empfehlungen) und Nachhaltigkeit (z. B. Schulungen) unterteilen. Zur Erbringung dieser Leistungen gibt es verschiedene grundlegende Organisationsmodelle (z. B. dezentrales CERT, zentrales CERT,

kombiniertes CERT), die sich jeweils in bestimmten Bereichen bevorzugt einsetzen lassen.

Zur Ergänzung der Grundlagen, und zu einem besseren Verständnis von Computer-Notfallteams, wurde in Kapitel 3 zu Anfang kurz deren historische Entwicklung anhand der Gründung des CERT Coordination Centers beschrieben. Sowohl auf internationaler als auch nationaler Ebene entwickelten sich daraus einige wichtige Organisationen (z. B. FIRST, TF-CSIRT, CERT-Verbund) und Teams (z. B. DFN-CERT, CERT-Bund), die besonders für eine informelle Zusammenarbeit von Bedeutung sein können.

Ein wesentlicher Schwerpunkt dieser Arbeit bestand in der Ermittlung potenzieller Erfolgsfaktoren für ein Computer-Notfallteam (Kapitel 4), da in der Literatur bisher keine dementsprechenden Ausarbeitungen verfügbar sind. Aufgegliedert nach dem Aufbau und dem Betrieb eines CERTs wurden anschauliche Hinweise und Textstellen aus den verfügbaren Quellen zu möglichen Faktoren zusammengefasst. Das Ergebnis bestand aus insgesamt zehn theoretischen Erfolgsfaktoren, davon konnten fünf sowohl zum Aufbau als auch zum Betrieb zugeordnet werden (Unterstützung durch das Management, Unterstützung durch andere CERTs, Ressourcenverfügbarkeit und -einsatz, Verfügbarkeit qualifizierter Mitarbeiter, gutes Verhältnis zur Constituency). Für den Aufbau wurden zwei spezifische Faktoren als relevant identifiziert (Verfügbarkeit von Informationen, Einhaltung zeitlicher Vorgaben), für den Betrieb konnten drei weitere unterschieden werden (Dienstleistungsangebot, Dokumentation, Informationspolitik).

Darauf aufbauend konnte anhand einer empirischen Befragung (Kapitel 5) gezeigt werden, dass alle vorgestellten Faktoren im Kern als bedeutsam für ein Computer-Notfallteam angesehen werden und auf dessen Erfolg einwirken können. Aus den Ergebnissen ließen sich zudem zahlreiche stützende und ergänzende Aussagen für einzelne Erfolgsfaktoren gewinnen. Dabei ergab sich auch, dass z. B. die Dauer des CERT-Aufbaus weniger eine Rolle spielt, als die Einhaltung kommunizierter Zeitvorgaben. Den Antworten der Befragten konnte auch entnommen werden, dass z. B. das Vorhandensein einer sicheren Kom-

munikationsinfrastruktur für die Zusammenarbeit mit anderen CERTs notwendig ist.

Bevor die herausgearbeiteten Erfolgsfaktoren schließlich auf das CERT-Niedersachsen angewendet werden konnten, wurde zunächst die derzeitige Situation hinsichtlich der IT-Sicherheitsorganisation in Niedersachsen skizziert (Kapitel 6). Demnach verfügt das Land aufgrund des Ressortprinzips über eine bisher uneinheitliche Ausstattung an IT-Ressourcen und wenig übergreifende IT-Sicherheitsprävention. Diese Umstände wurden erkannt und sollen im Rahmen der strategischen Neuausrichtung des IT-Einsatzes behoben werden. Die konkreten Anforderungen an ein mögliches CERT-Niedersachsen konnten durch den Projektauftrag und den Zwischenbericht deutlich gemacht werden. Durch die Verteilung der Aufgaben auf vorhandenes Fachpersonal sollen z. B. Neueinstellungen weitgehend vermieden und Ressourcen eingespart werden. Dazu ist vorgesehen, dass bestehende Sicherheitsteams die Rolle eines „virtuellen“ dezentralen CERTs übernehmen, das von einer zentralen Koordinierungsstelle angeleitet und überwacht wird. Dabei wird im Rahmen der Möglichkeiten u. a. auch das Outsourcing verschiedener Leistungen an externe Anbieter angestrebt.

Im Rahmen einer kurz gefassten Bewertung wurden einige mögliche Kritikpunkte herausgestellt, wobei besonders auf die Unentbehrlichkeit eines politischen Rückhalts als Bedingung für weitere Planungen hinzuweisen ist. Alles in allem ist das zielgerichtete Vorgehen des Landes Niedersachsen als positiv zu sehen und das spätere Gelingen kann daher nicht als abschlägig beurteilt werden. Darauf bauen auch die vorgenommenen Gestaltungsempfehlungen, die unter der Bedingung formuliert wurden, dass das niedersächsische Computer-Notfallteam de facto aufgebaut wird und zum Einsatz kommt. Wiederum nach dem Aufbau und dem Betrieb eines CERT gegliedert, wurden die einzelnen Faktoren auf die konkrete Situation in Niedersachsen herunter gebrochen und mit nahe liegenden Erwägungen abgeschlossen. Dazu gehören z. B. die Empfehlungen, während der Aufbauphase weiterhin mit dem DFN-CERT zusammenzuarbeiten und beim späteren Betrieb auch die mögliche Überbelastung von Teammitgliedern nicht zu übersehen.

Wie letztendlich der Aufbau des CERT-Niedersachsen tatsächlich vollzogen wird und ob dieser und der spätere Betrieb von Erfolg gekrönt sein werden, ist zu diesem Zeitpunkt nicht absehbar. Derzeit stehen die erforderlichen Entscheidungen für die Ausgestaltung und die Umsetzung des bisherigen Konzeptes aus, die Notwendigkeit und der Bedarf sind dagegen schon deutlich vorhanden. Daher bleibt es abzuwarten, wie u. a. die politischen Entscheidungen dazu ausfallen werden und ob diese dem endgültigen Gelingen nicht entgegenstehen. Zur Verbesserung der niedersächsischen IT-Sicherheitsorganisation insgesamt lässt es jedoch hoffen, dass am Ende der veranschlagten drei Jahre alle geplanten Maßnahmen erfolgreich umgesetzt werden konnten und ein einsatzfähiges Computer-Notfallteam daraus entstanden ist.