Niedersächsisches Ministerium
für Inneres und Sport

Kritische Erfolgsfaktoren für ein Computer Emergency Response Team (CERT)

am Beispiel CERT-Niedersachsen

Niedersächsisches Ministerium für Inneres und Sport
- Zentrales IT-Management der Landesverwaltung -
Lavesallee 6
30169 Hannover
Tel. (0511) 120-3027
eMail: ZIM@mi.niedersachsen.de

Dieses Dokument wurde erstellt von

Dipl.-Ök. Stefan Hoyer

in Zusammenarbeit mit dem Niedersächsischen Ministeriums für Inneres und Sport
als Fortschreibung und Zusammenfassung der Ergebnisse seiner gleichnamigen Diplomarbeit,
begleitend zum Projekt CERT Niedersachsen,
im Rahmen der Entwicklung eines ganzheitlichen und ressortübergreifenden Konzeptes für Informationssicherheit in der Niedersächsischen Landesverwaltung.

Projektleitung: Zentrales IT-Management der Landesverwaltung, Herr Dipl.-Ing. (FH) Claus Irion

Kontakt:
Dipl.-Ök. Stefan Hoyer
eMail: hoyer.stefan@nexgo.de
Tel.: 0174 / 2515000

1. Auflage September 2006, 60 Exemplare

Druck und Bindung:
Landesvermessung + Geobasisinformation Niedersachsen (LGN)

Stand: 30. Juni 2006

Inhaltsverzeichnis

Seite

Management Summary

Ein Computer-Notfallteam oder auch Computer Emergency Response Team (CERT) trägt mit seiner Expertise zum Thema IT-Sicherheit maßgeblich dazu bei, dass möglichen Angriffen auf IT-Infrastrukturen bereits im Vorfeld wirksam begegnet werden kann. Auch nach einem IT-Sicherheitsvorfall ist ein CERT bei der Wiederaufnahme des Regelbetriebs und der Ermittlung der Verursacher eine nahezu unverzichtbare Unterstützung. Dieser Bericht erläutert zunächst die notwendigen Grundlagen zum Verständnis eines CERTs und befasst sich danach intensiv mit der Fragestellung, anhand welcher Faktoren der Erfolg eines Computer-Notfallteams festgemacht werden kann und welche Punkte sowohl bei dessen Aufbau als auch dessen Betrieb beachtet werden sollten. Für den Aufbau können als besonders wichtige Faktoren z. B. die Unterstützung durch das Management, die CERT-Mitarbeiter, das Verhältnis zur betreuten Zielgruppe oder auch die Einhaltung zeitlicher Vorgaben genannt werden. Während der Betriebsphase eines Computer-Notfallteams sind z. B. besonders ein zielgerichtetes Dienstleistungsangebot, der Austausch von Informationen mit anderen CERTs und die Verfügbarkeit sicherer Kommunikationstechnologien von großer Bedeutung. Der Bericht schließt mit konkreten Gestaltungsempfehlungen für ein CERT-Niedersachsen, welche sich aus den kritischen Erfolgsfaktoren ableiten lassen. Dazu gehört z. B. vor allem die eindeutige Entscheidung der politischen Entscheidungsträger für ein Computer-Notfallteam und auch die langfristige Unterstützung des zuständigen IT-Managements (CIO bzw. CISO).

1 Einleitung

In den vergangenen Jahren ist die Vernetzung von Rechnern durch das Internet schneller vorangeschritten, als die Globalisierung insgesamt. Über das weltweite Datennetz werden zunehmend 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 und/oder terroristische Machenschaften (z. B. Sabotage, Industriespionage, Datendiebstahl) ausgenutzt und verursachen somit immer gezielter beträchtliche Schäden. Die Komplexität der Angriffswerkzeuge nimmt weiter zu, wohingegen die Angreifer selbst immer weniger Wissen benötigen, um „erfolgreich“ zu sein. 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 (Abb. 1). 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.

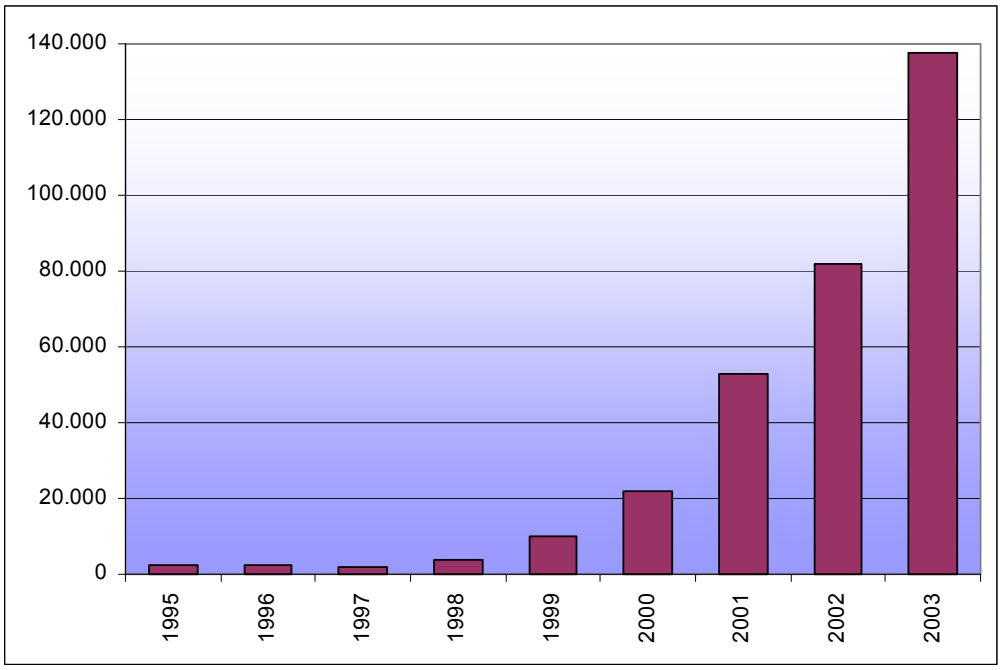

Abb. 1: Gemeldete Vorfälle an das CERT Coordination Center (1995 - 2003)

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 unterscheidet 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 er-

kannt und beachtet werden. Ein Kernziel dieser Arbeit besteht darin aufzuzeigen, welche Faktoren für den Erfolg oder den Misserfolg eines CERTs entscheidend sein können. Anhand dieser Ergebnisse soll beleuchtet werden, wie das Vorhaben in Niedersachsen zum Aufbau eines eigenen Computer-Notfallteams momentan aussieht, wie es insgesamt zu beurteilen ist und welche Empfehlungen sich für dessen Gestaltungen ableiten lassen.

2 Grundlagen zu Computer Emergency Response Teams (CERT)

2.1 Grundlegende Begriffe eines CERTs

2.1.1 Grundgerüst eines CERTs und zugehörige Begriffe

In der verfügbaren Literatur ist keine allgemein anerkannte Definition eines Computer-Notfallteams zu finden. Dies mag vor allem daran liegen, dass es sich zumeist um die Dokumentation einer praktischen Anwendung handelt und nicht um eine rein wissenschaftliche Forschung. Zudem werden in der überwiegend englischsprachigen Literatur verschiedene Begriffe synonym verwendet, wobei sehr häufig von „CERT“ (Computer Emergency Response Team), „CSIRT“ (Computer Security Incident Response Team) oder „IRT“ (Incident Response Team) gesprochen wird. Im deutschen Sprachraum wird häufig der Ausdruck „Computer-Notfallteam“ verwendet. Die Bezeichnung „CERT“ ist dagegen ein vom CERT Coordination Center geschütztes Markenzeichen, wird jedoch mit dessen Erlaubnis im Namen vieler Teams geführt und kann daher auch als gängige Bezeichnung verwendet werden. Die Vielfalt der Begriffe zeigt, dass sich ein Computer-Notfallteam durch etwas anderes als nur seinen Namen definieren muss.

Ein Computer-Notfallteam kann zunächst beschrieben werden als eine „(…) service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity.“[1] Etwas genauer lässt es sich definieren als „(…) capability or team that provides services and support to a defined constituency for preventing, handling and responding to computer security incidents.“[2] Zu den Hauptaufgaben eines Computer-Notfallteams gehört es daher, einer Zielgruppe bei der Bewältigung von Sicherheitsvorfällen zu helfen, deren Auswirkungen zu reduzieren und zukünftige Ereignisse zu verhindern. Damit sich eine Organisation jedoch als CERT bezeichnen kann, muss diese wenigstens eine Incident Handling Dienstleistung (Vorfallsbearbeitung) anbieten. Daraus geht hervor, dass die Dienste eines Computer-Notfallteams überwiegend reaktiver Natur sind. Daneben kann und sollte das Team auch verschiedene präventive Dienstleistungen oder Unterstützung im Sicherheitsqualitätsmanagement anbieten.

Jedes Computer-Notfallteam ist anders, verfolgt eigene Ziele und hat seine Besonderheiten, was nicht zuletzt aus den unterschiedlichen Begriffsverwendungen und den jeweiligen Aufgaben folgt. Gemeinsam haben sie jedoch alle ein Grundgerüst (Basic Framework), das aus vier wichtigen Elementen besteht:

- Mission Statement bzw. Auftragserklärung (was tut das CERT?),
- Constituency bzw. Zielgruppe (für wen?),
- Einbindung in die Organisation (in welchem Umfeld?) und
- Beziehung zu anderen Teams (mit wem arbeitet es zusammen?).

Die kurze und prägnante Erklärung des Auftrages in Form eines Mission Statements ist unbedingt notwendig, da es die grundlegenden Absichten und den eigentlichen Zweck des Computer-Notfallteams beschreibt. Klare und realistische Ziele definieren Umfang und Grenzen der Arbeit sowie die zu betreuende Zielgruppe. Das Mission Statement liefert somit ein Grundverständnis der Arbeitsweise und der Prioritäten des Teams und sollte daher sowohl öffentlich bekannt gemacht (z. B. durch Veröffentlichung im Internet) als auch vom leitenden Management unterstützt werden.

[1] Killcrece u. a. [2003b, S. 11].
[2] Alberts u. a. [2004, S. 2].

Eine Constituency ist „(…) der Kreis der Individuen, Organisationen oder Gruppen (…), auf den die Dienstleistungen (…) ausgerichtet [sind].“[3] Dieser Begriff lässt sich im Deutschen am ehesten mit Zielgruppe übersetzen. Dessen formelle und eindeutige Festlegung erfolgt anhand verschiedener Merkmale (z. B. Zugehörigkeit zu einer Organisation oder geografischen Region) und kann dabei durch die Auflistung von Domänennamen unterstützt werden. Je nach Art und Umfang der Constituency kann dies sehr leicht oder sogar unmöglich sein.

Die grundlegende Beziehung zur Constituency und darüber hinaus auch die Art der angebotenen Dienstleistungen werden davon beeinflusst, in wieweit das Computer-Notfallteam ermächtigt ist, eigenständig über Sicherheitsmaßnahmen zu entscheiden. Diese Befugnisse (Authority) lassen sich konkretisieren als „(…) the control that the CSIRT has over its own actions and the actions of its constituents related to computer security and incident handling activities.“[4]

Der Umfang der Befugnisse kann in drei Stufen differenziert werden: volle, eingeschränkte und keine Autorität (Tab. 1 auf S. 12). Hat ein Computer-Notfallteam umfassende Befugnisse, kann es ohne Rücksprache mit der Constituency alle notwendigen Maßnahmen ergreifen. Sind die Befugnisse dagegen eingeschränkt, sind die Klienten an den Entscheidungen über vorzunehmende Maßnahmen beteiligt. Das CERT unterstützt dann die Klienten direkt bei der Umsetzung. Wenn ein Team indessen keine Befugnisse hat, kann es einzig Empfehlungen aussprechen und nur als Berater für die Constituency auftreten.

Tab. 1: Mögliche Befugnisse eines Computer-Notfallteams

Level of Authority	CSIRT/Constituency Relationship
Full	The members of the CSIRT have the authority to undertake any necessary actions on behalf of their constituency.
Shared	The members of the CSIRT provide direct support to their constituents and share in the decision-making process.
None	The members of the CSIRT have no authority over their constituents and can act only as advocates or advisors.

Unabhängig von den Befugnissen des Teams wird die Constituency aufgetretene Sicherheitsvorfälle jedoch nur dann melden, wenn sie Vertrauen in die Kompetenzen und Fähigkeiten des Teams hat. Das Vertrauen und den Respekt der betreuten Zielgruppe zu gewinnen ist daher eine der Hauptaufgaben eines Computer-Notfallteams, da es ansonsten nicht effektiv arbeiten kann.

Zudem ist es wichtig, zwischen einer formell festgelegten und einer informellen Constituency zu unterscheiden. Die informelle Constituency entsteht, wenn das Team erfolgreich ist und über die Grenzen seiner Zielgruppe hinaus Vertrauen aufbaut. Dies ist insofern bedeutsam, als dass die Dienstleistungen eines Computer-Notfallteams in erster Linie für die festgelegte Zielgruppe erbracht werden. Öffentlich zugängliche Informationen können dagegen auch von einer unbestimmten Anzahl von Interessenten genutzt werden, auf die das CERT keinen direkten Einfluss hat.

[3] Kossakowski [2000, S. 13].
[4] Killcrece u. a. [2003a, S. 37].

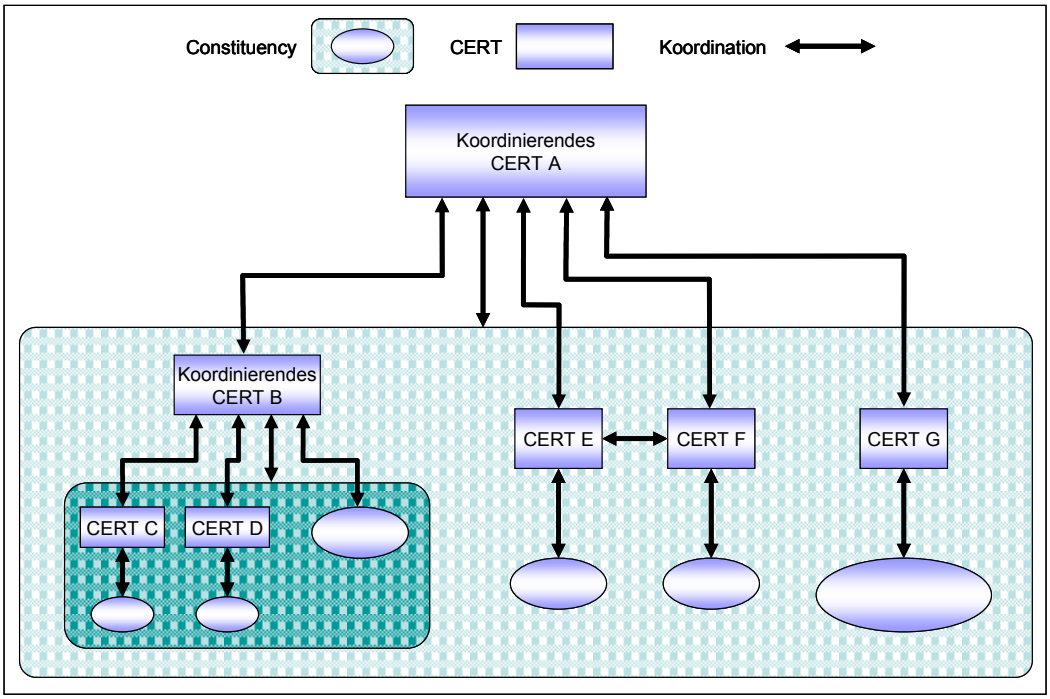

Abb. 2: Koordinationsbeziehungen zwischen Computer-Notfallteams

Zur Erfüllung ihrer Aufgaben müssen Computer-Notfallteams mit anderen Teams kooperieren und ihre Aktionen koordinieren. Zu diesem Zweck existieren vorwiegend informelle und freiwillige gleichrangige Koordinationsbeziehungen zwischen den heute bestehenden CERTs (Abb. 2). Dazu kann grob unterschieden werden zwischen Computer-Notfallteams, die national oder international eine koordinierende Rolle zwischen verschiedenen Teams übernehmen und solchen, die nur Dienstleistungen für eine festgelegte Constituency erbringen und gegebenenfalls untereinander koordiniert vorgehen.

Eng verbunden mit dem Mission Statement und zu einem Teil abhängig von der betreuten Constituency, ist die Einbindung in die Organisation bzw. das Umfeld des Computer-Notfallteams. Möglich ist z. B. eine Implementierung als eigenständige Abteilung oder eine Ansiedlung in bestehenden IT-, Sicherheits- oder Revisionsabteilungen. Die Inanspruchnahme von Dienstleistungen eines externen CERTs ist gleichermaßen denkbar. Zudem sollte ein Computer-Notfallteam in die Geschäftsstruktur der betreffenden Organisation und auch in ein eventuell bestehendes Risikomanagement eingebunden werden. Es gibt jedoch keine durchweg gebräuchliche oder standardisierte Form der Einbindung in eine Organisation.

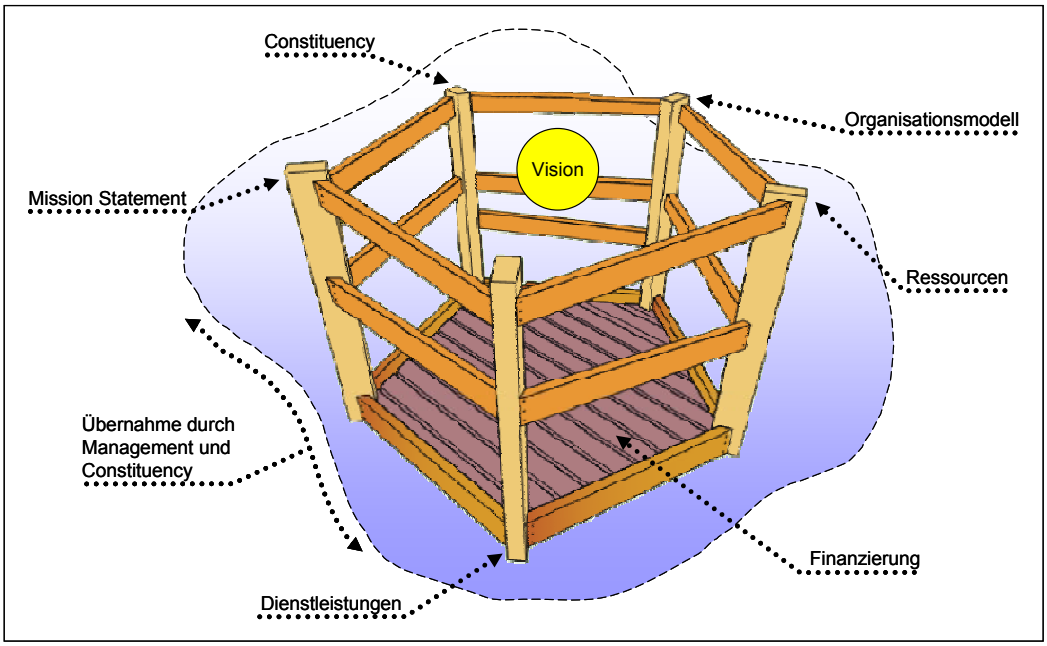

Abb. 3: Umfassendes Konzept für Computer-Notfallteams [5]

In Verbindung mit den angebotenen Dienstleistungen, dem Organisationsmodell des Teams, den benötigten Ressourcen und der langfristigen Finanzierung, lässt sich aus dem Grundgerüst ein umfassendes Bild (Vision) bezüglich der wesentlichsten Komponenten eines Computer-Notfallteams entwickeln (Abb. 3). Wie Informationen über diese Punkte bereitgestellt werden sollten, können z. B. RFC 2350 entnommen werden. Dort werden Anforderungen und Erwartungen an ein CERT in Form einer „Best Current Practice“ präsentiert.

2.1.2 Typische Dienstleistungen eines CERTs

Es gibt eine Reihe von Aufgaben, die von einem Computer-Notfallteam wahrgenommen werden können. Von einem Team müssen jedoch nicht alle erdenklichen Dienstleistungen angeboten werden. Diese sollten sorgfältig ausgewählt werden und sowohl den Auftrag als auch die Constituency eines CERTs sinnvoll unterstützen, da dessen Erfolg wesentlich von der Qualität der angebotenen Dienstleistungen beeinflusst wird. Die Dienste eines Computer-Notfallteams lassen sich drei Kategorien zuordnen: Reaktion, Prävention und Sicherheitsqualitätsmanagement (Abb. 4 auf S. 15).

Reaktive Dienstleistungen zeichnen sich dadurch aus, dass sie durch ein Ereignis (z. B. Anfrage eines Kunden) bzw. einen konkreten Sicherheitsvorfall ausgelöst werden. Mit ihnen wird ein geeignetes Entgegenwirken angestrebt, um verfügbaren Mitteln die Entstehung größerer Schäden sowie das Auftreten ähnlicher Vorfälle zu verhindern. Als Aufgabenfelder können, neben der Warnungsmeldung an die Constituency und der Bearbeitung von IT-Sicherheitsvorfällen (Incident), die folgenden zwei konkretisiert werden. Wenn z. B. bei einem System die Möglichkeit zur Umgehung der Sicherheitsmaßnahmen besteht und dies von Angreifern ausgenutzt werden kann, wird dies als Schwachstelle bzw. Sicherheitslücke (Vulnerability) bezeichnet. Häufig stützen sich Angreifer dabei auf den Einsatz von Angriffswerkzeugen (Artifacts[6]), um sich z. B. unrechtmäßig Zugang zu den betroffenen Systemen zu verschaffen.

[5] Quelle: Carnegie Mellon University [2002], Übersetzung des Originals
[6] Andere verwendete Bezeichnungen sind z. B. „Critter“ oder auch „Malicious Code“.

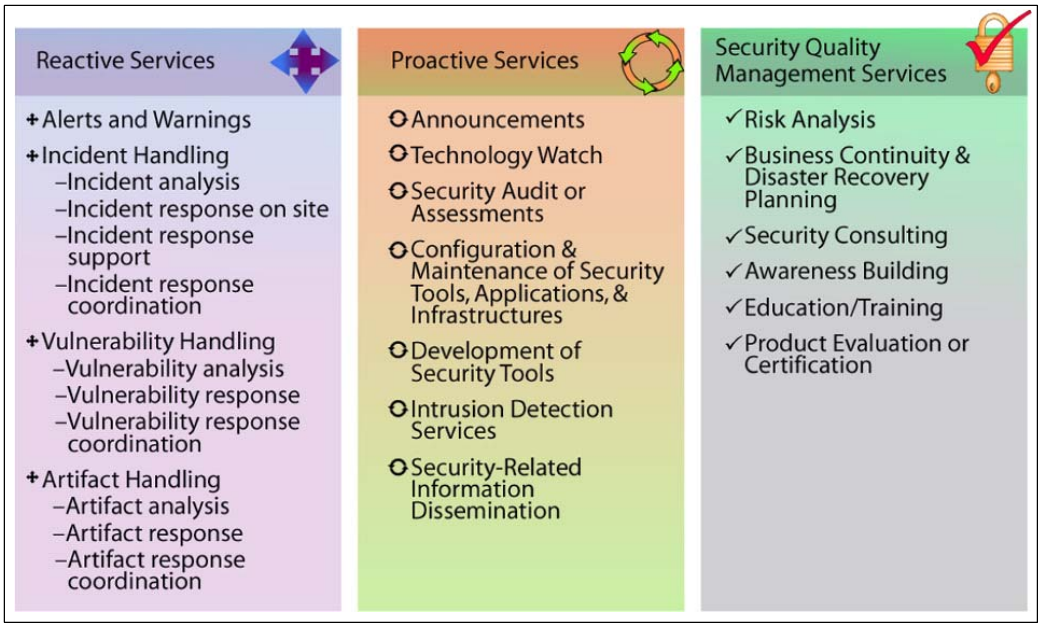

Abb. 4: Typische Dienstleistungen von Computer-Notfallteams

Ein Computer-Notfallteam bietet seiner Constituency reaktive Hilfe durch die technische Analyse und Sicherung möglicher Beweismittel (Analysis) sowie der Unterstützung bei der Reaktion (Response, Response on Site) auf Vorfälle, Schwachstellen oder Angriffswerkzeuge. Zudem kann es die Bemühungen anderer beteiligter Parteien koordinieren (Response Coordination). Dazu gehören auch die Bearbeitung von Anfragen zu Sicherheitsvorfällen (Requests) sowie die Verifizierung von Informationen auf ihre Echtheit (Clearinghouse). Alle reaktiven Dienstleistungen können zu den Kernaufgaben eines Computer-Notfallteams gezählt werden.

Durch das Angebot präventiver (proaktiver) Dienstleistungen soll bereits das Auftreten zukünftiger Probleme und Vorfälle vermieden und folglich deren negative Auswirkungen reduziert werden. Erreicht wird dies u. a. durch eine Verbesserung der Sicherheitsprozesse und der frühzeitigen Warnung der Constituency vor Eintreten eines Vorfalles. Dies wiederum erfolgt durch eine regelmäßige Verteilung sicherheitsrelevanter Empfehlungen (Announcements), die vor allem auf den Ergebnissen anderer Dienstleistungen beruhen. Dazu gehört z. B. die fundierte Sammlung und Analyse von technologiebezogenen Informationen (Technology Watch), die Analyse und Überprüfung von Kundensystemen auf Verwundbarkeiten (Security Audit) bzw. deren Umgebung (Neighbourhood Watch) oder auch die frühzeitige Erkennung von Angriffen oder Missbrauch (Intrusion Detection). Durch Konfigurations- und Wartungshilfen für sicherheitsbezogene Programme (Security Tools) kann die Constituency ebenso unterstützt werden, wie durch die Entwicklung speziell zugeschnittener Sicherheitsprogramme (Tools Development). Mittlerweile wird auch die Prävention von Sicherheitsvorfällen als den Hauptaufgaben von Computer-Notfallteams zugehörig angesehen.

Die Nachhaltigkeit der Sicherheit soll durch Dienstleistungen im Bereich Sicherheitsqualitätsmanagement (Security Quality Management) erreicht werden. Diese präventiv geprägten Aufgaben sind nicht allein kennzeichnend für ein Computer-Notfallteam, da sie auch von anderen Abteilungen unabhängig von der Vorfallsbearbeitung erbracht werden können. Das CERT übernimmt hier vorwiegend eine Steuerungsfunktion, damit die Expertise aller Beteiligten eingebracht werden kann und alle die für sie notwendigen Informationen erhalten. Diese Dienstleistungen sind zwar nicht als Kernaufgaben anzusehen, können allerdings für ein bestehendes Risikomanagement von Nutzen sein und somit vorbeugend wirken.

Das CERT kann seine Kunden bei einer realistischen Analyse ihrer Sicherheitsrisiken (Risk Analysis) oder bei der Gestaltung und Überprüfung von Plänen zur Wiederaufnahme ihrer Geschäfte nach einem Ernstfall (Business Continuity Planning) unterstützen. Aufgrund seiner Expertise kann das Team auch umfassende Sicherheitsberatungen (Security Consulting) oder Aus- und Weiterbildungen (Training) für sicherheitsverantwortliches Personal anbieten. Dadurch und mit Hilfe weiterer Sensibilisierungsmaßnahmen wird bei der Constituency u. a. auch ein Bewusstsein für die Notwendigkeit von Sicherheitsmaßnahmen sowie eine Resonanz bezüglich der Aufgaben und Fähigkeiten des Computer-Notfallteams erzeugt (Awareness Building).

Für die letztlich angebotenen Dienstleistungen bedarf es des Verständnisses, dass einige von ihnen aufeinander aufbauen bzw. voneinander abhängig sind und somit verschiedene Voraussetzungen für deren Erbringung bestehen. Auch müssen nicht alle Dienstleistungen eines Computer-Notfallteams zwingend in Eigenregie übernommen werden („Make or Buy“). Handelt es sich nicht um rein unternehmensspezifische Problemstellungen, kann ein Teil der Dienste durch Outsourcing an kostengünstigere externe Anbieter abgegeben werden.

2.1.3 CERT-Organisationsmodelle

Das Organisationsmodell bzw. die Organisationsstruktur eines Computer-Notfallteams beschreibt dessen grundlegenden organisatorischen Aufbau und umfasst dabei sowohl den physikalischen Standort als auch die Stellung innerhalb der Organisation oder Constituency. Der organisatorische Aufbau selbst hängt mit den spezifischen Anforderungen zusammen, die sich u. a. aus Mission Statement, formeller Constituency und anzubietenden Dienstleistungen ergeben. Da jedes Team spezifisch auf die Gegebenheiten seines Umfeldes abgestimmt werden muss, ist eine Verallgemeinerung möglicher Teamtypen aufgrund des Situationsbezuges angebotener Dienstleistungen schwierig. Ein Computer-Notfallteam kann folgenden Kategorien zugeordnet werden: Sicherheitsteam einer Organisation (Ad hoc Team), zentral und/oder dezentral in einer Organisation eingebundenes CERT sowie national bzw. übernational koordinierendes CERT.

Sicherheitsteam
Ein Sicherheitsteam ist an sich kein vollwertiges CERT-Modell, da die Verantwortungen für die Vorfallsbearbeitung nicht formell festgelegt wurden. Für ein effizientes Management von auftretenden IT-Sicherheitsvorfällen bestehen also keine wirklichen Strukturen. Bei ihrem Auftreten werden alle Vorfälle ad hoc gehandhabt und isoliert von anderen Vorgängen bearbeitet. Ein solches Team besteht aus einer oder mehreren Personen und umfasst dabei vorwiegend Administratoren und verfügbares IT-Personal. Der Fokus eines Sicherheitsteams liegt auf der Absicherung von in der Organisation verwendeten Systemen und Netzwerken sowie dem Entdecken von Unregelmäßigkeiten im Betrieb. In einer Organisation kann es auch mehrere Sicherheitsteams geben, die jeweils einen Bereich betreuen. Die von einem Vorfall betroffenen Systeme sollen schnellstmöglich wiederhergestellt und nutzbar gemacht werden. Zu finden ist ein Sicherheitsteam in Organisationen, wo eine sicherheitsbezogene System-Administration benötigt wird. Dazu zählen üblicherweise Unternehmen, öffentliche Verwaltungen und Wissenschaftseinrichtungen (z. B. das Sicherheitsteam des RRZN). Das Sicherheitsteam hat keine Autorität gegenüber seiner Constituency und arbeitet nur in einem sehr begrenzten lokalen Umfeld. Im Bezug auf die Vorfallsbearbeitung bietet dieses Modell keine wirklichen Stärken. Allerdings verursacht es auch keine zusätzlichen Kosten, da Personal und Ausstattung bereits vorhanden sind.

Dezentrales CERT
Das dezentrale bzw. (intern) verteilte CERT ist ein formal festgelegtes Computer-Notfallteam, welches die Verantwortung für die Bearbeitung von IT-Sicherheitsvorfällen hat. Die Mitglieder dieses Teams wurden aufgrund ihrer Erfahrung mit bestimmten Systemen oder Techniken ausgewählt und bleiben weiter an ihrem ursprünglichen Arbeitsplatz einge-

setzt. Da die CERT-Mitglieder über verschiedene Abteilungen und Unternehmensstandorte verstreut sind, bilden sie ein „virtuelles“ Team. Neben den Aufgaben in ihrer Abteilung übernehmen sie zusätzlich die Rolle eines Mitgliedes im Computer-Notfallteam. Daraus ergibt sich allerdings auch eine Doppelbelastung für die Mitglieder des Teams, da diese einen Teil ihrer Arbeitszeit an das CERT abgeben. Bei der Bearbeitung eines IT-Sicherheitsvorfalls kommt den Incident Handling Aufgaben eine höhere Priorität zuteil und diese müssen der täglichen Routine vorgezogen werden. Zwingend notwendig ist jedoch die Koordination des Teams durch einen zentral angeordneten CERT-Manager, der zugleich das Team nach außen hin vertritt und als Ansprechpartner mit anderen Stellen (z. B. externe CERTs) fungiert. Darüber hinaus werden durch das zentrale CERT-Büro Meldungen und Berichte aufbereitet bzw. bezüglich ihrer Relevanz gefiltert und allen Mitgliedern zugänglich gemacht.

Der Vorteil einer dezentralen Einheit liegt vor allem darin, dass sie durch die in der Organisation verstreuten Mitglieder ein breites Wissen über die verwendeten Systeme und die betrieblichen Abläufe hat und in vielen/allen Abteilungen präsent sein kann. Allerdings können sich auch Probleme ergeben, wenn z. B. das Team aus Mitarbeitern unterschiedlicher Abteilungen und Standorte „zusammengewürfelt“ wurde oder sich die Verantwortlichkeiten der Teammitglieder überschneiden. Insgesamt kann dieses Modell bevorzugt in großen und über mehrere Standorte verteilten Organisationen (z. B. Regierungsorganisationen oder multinationale Konzerne) eingesetzt werden. In kleineren Organisationen ist der Einsatz einer dezentralen Einheit dagegen nicht geeignet. Die konkrete Ausgestaltung der Strukturierung des Teams hängt von verschiedenen Faktoren ab, z. B. Größe der zu betreuenden Organisation, Standortanzahl, Anzahl unterstützter Systeme und Plattformen. So ist es einerseits denkbar, dass bestimmte Dienstleistungen von einzelnen Mitgliedern oder Abteilungen erbracht werden. Andererseits besteht auch die Möglichkeit, dass die Mitglieder einer Region (z. B. Firmenstandort in Deutschland) alle Aufgaben übernehmen.

Zentrales CERT
Bei dem zentralen CERT handelt es sich ebenfalls um ein formal festgelegtes Computer-Notfallteam mit der eindeutigen Verantwortung für die Bearbeitung von IT-Sicherheitsvorfällen. Im Gegensatz zu einem dezentralen CERT werden bei diesem Modell jedoch alle Mitarbeiter und Ressourcen an einem zentralen physischen Standort zu einer spezialisierten Einheit zusammengefasst. Die Mitglieder des Teams wurden auch hier aufgrund ihrer Expertise ausgewählt, unterstehen jedoch keinen anderen Abteilungen und können somit ihre volle Arbeitszeit dem CERT widmen. Zusätzlich gibt es die Möglichkeit, ein solches Kernteam durch die Hinzunahme von Teilzeitkräften zu verstärken oder ein partielles Outsourcing der Dienstleistungen vorzunehmen. Hier ist ebenfalls ein CERT-Manager notwendig, der das Team repräsentiert und die Arbeit des Computer-Notfallteams koordiniert.

Von der Constituency, den anzubietenden Dienstleistungen und der Anzahl der Vorfälle in der Organisation hängt letztlich die Größe der zentralen Einheit ab. Eine Stärke dieses Modells gegenüber dem einfachen Sicherheitsteam und dem dezentralen CERT liegt darin, dass den Teammitgliedern die volle Arbeitszeit zur Verfügung steht und somit mehr Möglichkeiten zur präventiven Vorfallsbearbeitung bestehen. Gleichzeitig dient es als zentrale Anlaufstelle für alle Angelegenheiten bezüglich der IT-Sicherheit. Allerdings besteht hier auch die Gefahr, dass das CERT aufgrund seiner zentralen Anordnung möglicherweise keinen Einblick in die Abläufe der verschiedenen Abteilungen hat. Somit verfügt ein zentrales CERT nicht über dasselbe breite Organisationswissen (z. B. Abläufe und Prozesse in anderen Bereichen), wie ein dezentrales CERT, was zwangsläufig zu einer Trennung zwischen Vorfallsbearbeitung und anderen betrieblichen Vorgängen führt. Daher muss das Team besonders gut mit anderen Stellen in der Organisation zusammenarbeiten können.

Besonders geeignet für dieses Modell sind Organisationen, in denen alle IT-Aufgaben durch eine zentrale Abteilung erledigt werden können (z. B. kleinere Unternehmen oder Hersteller).

Es ist jedoch auch möglich, diese Art von CERT in einer größeren Organisation mit mehreren Standorten und einer breiteren Constituency aufzubauen (z. B. Regierungsorganisationen mit mehreren Abteilungen oder große Bildungsinstitutionen).

Kombiniertes CERT
Dieses Organisationsmodell ist eine Kombination aus den beiden zuvor beschriebenen Modellen. Es vereint die Strukturen eines zentral angeordneten CERTs, dessen Mitglieder in Vollzeit zur Verfügung stehen und bietet zugleich die Möglichkeiten einer dezentralen Einheit, da auch hier Teammitglieder über die Organisation verteilt sind und einen Teil ihrer Arbeitszeit an das Team abgeben. Die zentrale Koordinierungsstelle sammelt relevante Informationen aus diversen Quellen, bearbeitet und verbreitet sie schließlich in der Organisation. Dadurch ist es vor allem geeignet, höherwertige Analysen vorzunehmen und Strategien zur Umsetzung zu empfehlen. Die dezentralen Mitglieder liefern die notwendige Expertise aus ihrem jeweiligen Verantwortungsbereich, sodass das kombinierte CERT über eine breite Wissensbasis in Bezug auf organisationsinterne Abläufe verfügen kann.
Auch hier ist die Existenz eines zentralen CERT-Managers erforderlich, um die Aktivitäten des gesamten Computer-Notfallteams zu koordinieren. Allerdings müssen nun zwei Systeme gemanagt werden, was eine höhere Belastung für den CERT-Manager bedeutet. Insgesamt besteht bei einer nicht ausreichenden Verzahnung der beiden Systeme die Gefahr, dass es zu einer Isolierung der zentralisierten Einheit kommen kann. Dies ist vergleichbar mit den Schwächen eines zentralisierten CERTs.

Die Stärke dieses Modell liegt darin, dass nun ein zentrales Spezialistenteam über ein verteiltes Expertennetzwerk verfügt, so in vielen Betriebsbereichen präsent sein kann und ein breites Wissen über betriebliche Abläufe ermöglicht wird. Dadurch wird der Einsatz von verfügbaren Mitarbeitern an strategischen Positionen in der Organisation maximiert und es kommt zwangsläufig zum Kontakt zwischen CERT und Constituency. Der Einsatz eines kombinierten CERTs eignet sich somit vorwiegend in sehr großen verteilten Organisationen oder Constituencies.

Koordinierendes CERT
Die Anstrengungen eines koordinierenden CERTs (Koordinierungszentrum) richten sich voll und ganz auf die Abstimmung von Aktivitäten zwischen verschiedenen Parteien, um die Vorfallsbearbeitung insgesamt zu erleichtern. Die Koordination kann sich auf verschiedene Ebenen beschränken, z. B. Grenzen eines Landes (national) bzw. Kontinentes (übernational) oder Zugehörigkeit zu einem Verbund. Die formale Constituency eines koordinierenden CERTs besteht somit aus vielen verteilten und unabhängigen Einheiten (z. B. andere CERTs bzw. Sicherheitsteams und deren Constituencies).

Das koordinierende CERT unterscheidet sich dabei grundlegend von den anderen Modellen, obwohl es teilweise identische Komponenten enthält bzw. Dienstleistungen anbietet. So ist es z. B. meist als dezentrales Team organisiert, obwohl es einen zentralen Standort hat und von einem zentralen CERT-Manager geleitet wird. Dienstleistungen zur Wiederherstellung nach einem Vorfall bietet ein solches Team allerdings nicht an. Eine der Hauptschwächen dieses Modells besteht darin, dass das Team möglicherweise kein einsatzfähiges Wissen vorweisen kann und Schwierigkeiten bei der Erreichung aller Einheiten in seiner Constituency auftreten. Daher ist hier die Akzeptanz durch die Constituency besonders wichtig, um eine Vertrauensstellung aufzubauen. Im Gegensatz zu den anderen Organisationsmodellen bietet das koordinierende CERT jedoch ein besonderes Maß an Neutralität, da es unter anderem für ein stabiles Kernteam von Incident Handling Experten an einem zentralen Standort sorgt.

3 Wichtige bestehende CERT-Organisationen

3.1 Geschichtliche Entwicklung des Incident Handlings

Die Auswirkungen des ersten Internet-Wurms im Jahre 1988 werden häufig als Auslöser für die Gründung des ersten CERT angeführt. Demnach setzte der Student Robert Tappan Morris Jr., Sohn eines damaligen Kryptografie- und Sicherheitsexperten der NSA, am zweiten November 1988 seinen selbst programmierten Wurm frei. Innerhalb von nur wenigen Stunden wurden über 6.000 Systeme des ARPANETs (ca. 10 % des gesamten Netzwerks) infiziert und für mehrere Tage lahm gelegt. Ein Wurm ist ein schädliches Programm, welches sich besonders durch die Ausnutzung von Systemschwachstellen über das Internet verbreitet und selbst reproduziert.

Als direkte Folge dieses Vorfalls gründete die Defense Advanced Research Project Agency (DARPA) schließlich im November 1988 das erste Computer Emergency Response Team. Die Leitung und Verantwortung für das „CERT Coordination Center“ gab sie dafür an das staatlich geförderte Software Engineering Institute (SEI) der amerikanischen Carnegie Mellon University ab. Seit diesem Zeitpunkt dient dieses CERT als zentrale Anlaufstelle für ein koordiniertes Vorgehen bei Internet- und Netzwerknotfällen. Es unterstützt dabei sowohl bei der technischen Bewältigung und Analyse von Sicherheitsvorfällen als auch bei der Erkennung von Angriffsmustern. Dazu arbeitet es mit anderen Computer-Notfallteams und IT-Sicherheitsexperten weltweit zusammen und dient dabei vor allem auch als Vorbild für den Aufbau neuer Teams. Das schnelle Wachstum des Internets und der durch intensive Nutzung bedingte Bedarf an kompetenter Hilfe bei Sicherheitsvorfällen führen global zu einer fortwährend steigenden Anzahl an operierenden CERTs.

Nachfolgend wird ein kurzer Überblick über einige der wichtigsten Organisationen auf internationaler Ebene und in Deutschland gegeben. International sind dies z. B. das „Forum of Incident Response and Security Teams” (FIRST) oder das Asia Pacific Computer Emergency Response Team (APCERT) beispielhaft für ein übernational koordinierendes CERT. In Deutschland gibt es neben den Computer-Notfallteams des Deutschen Forschungsnetzes (DFN-CERT) und der Bundesbehörden (CERT-Bund) weitere Teams auf Landes- oder Organisationsebene.

3.2 Incident Handling auf internationaler Ebene

3.2.1 Forum of Incident Response and Security Teams (FIRST)

Innerhalb der ersten zwei Jahre nach dem Aufbau des CERT Coordination Centers stießen neu gegründete Teams auf Koordinationsprobleme, die sich auf Sprachbarrieren, verschiedenen Zeitzonen und unterschiedlichen internationalen Standards zurückführen ließen. Vor diesem Hintergrund wurde schließlich das „Forum of Incident Response and Security Teams” ins Leben gerufen, um die Kommunikation zwischen seinen Mitgliedern grundlegend zu verbessern und zu einem kooperativen Wissensaustausch beizutragen.

Seit seiner Gründung im November 1990 verzeichnet FIRST[7] eine stetig steigende Anzahl an registrierten Mitgliedern aus verschiedenen Kontinenten, Sektoren und Organisationen. Um aufgenommen zu werden, müssen sich die Anwärterteams ein bestehendes FIRST-Mitglied als Sponsor suchen. Diese Regelung gewährleistet die tatsächliche Existenz des neuen Mitgliedes und seiner Vertrauenswürdigkeit. Von großer Bedeutung ist, dass jedes registrierte Computer-Notfallteam als Repräsentant seiner Constituency auftritt und gleichermaßen die Verantwortung für sie trägt. Innerhalb des Forums sind alle Mitglieder einander

[7] http://www.first.org

gleichgestellt d. h., es gibt keine hierarchischen Strukturen. Die Größe einzelner CERTs spielt ebenfalls keine bedeutende Rolle, sodass auch kleinere Teams bestehen können. Die jährliche Gebühr für eine volle FIRST-Mitgliedschaft belief sich 2005 auf 1.100 US-Dollar.

Jährlich organisiert und veranstaltet das Forum öffentlich zugängliche Konferenzen und für Mitglieder vorbehaltene technische Workshops. Dort können sich vor allem Mitglieder intensiv mit dem Incident Handling auseinander setzen und Möglichkeiten zum Austausch von persönlichen Erfahrungen wahrnehmen. Dienstleistungen, die sich z. B. mit der Koordination von Vorfallsbearbeitungen befassen, bietet FIRST dagegen seinen Mitgliedern nicht. Eine FIRST-Mitgliedschaft bietet vielseitige Kontakte zu anderen Teams sowie umfangreiche Möglichkeiten der Kooperation. Dadurch kann vor allem die Reaktionsfähigkeit auf Vorfälle verbessert und die Qualität der angebotenen Dienstleistungen gesteigert werden.

3.2.2 Asian Pacific CERT (APCERT)

Ein weiteres Beispiel für die länderübergreifende Koordination von Computer-Notfallteams ist das Asia Pacific Computer Emergency Response Team (APCERT[8]), dessen erklärtes Ziel in der Förderung der internationalen Zusammenarbeit bei IT-Sicherheitsproblemen liegt. Im Gegensatz zum FIRST wird hier jedoch auch eine übernationale Koordination von Incident Handling Aktivitäten angestrebt. Gegenwärtig besteht der in 2003 gegründete Verbund aus 17 Mitgliedern, die über 13 Länder der asiatischen Pazifikregion verteilt sind (z. B. Australien, China und Japan).
Grundsätzlich kann jedes CERT aus der asiatischen Pazifikregion dem APCERT beitreten. Das APCERT bietet interessierten Computer-Notfallteams der betreuten Region dazu eine Mitgliedschaft in zwei Akkreditierungsstufen an. Zunächst muss jedes Team die Kriterien einer allgemeinen Mitgliedschaft erfüllen, bevor es als volles Mitglied aufgenommen werden kann. Der Unterschied zwischen diesen beiden Stufen besteht in der Berechtigung, für den Lenkungsausschuss zu kandidieren sowie eine Stimme bei dessen Wahl abzugeben. Diese Rechte stehen nur einem Vollmitglied zur Verfügung. Alle Gründungsmitglieder sind zugleich auch volle Mitglieder.

Zur Verbesserung der Kooperation und zum Austausch von Informationen und Erfahrungen veranstaltet das APCERT überdies jährliche Konferenzen. Die Teilnahme steht dabei sowohl Mitgliedern als auch IT-Sicherheitsorganen weltweit offen.

3.2.3 Task Force CSIRT (TF-CSIRT)

Die Task Force CSIRT (TF-CSIRT) ist eine von derzeit sieben Arbeitsgruppen der Trans-European Network and Education Networking Association (TERENA). TERENA wurde im Oktober 1994 durch die Zusammenführung von zwei europäischen Wissenschaftsnetzwerken geschaffen. Das Ziel dieses Zusammenschlusses liegt darin „(…) to promote and participate in the development of a high quality international information and telecommunications infrastructure for the benefit of research and education.“[9]

Die TERENA Task Forces sind freiwillige Arbeitsgruppen und bestehen aus Vertretern verschiedener Organisationen. Eine Mitarbeit steht dabei generell jedem offen, der einen nutzbringenden Beitrag leisten kann. Dieser kann sowohl durch Expertenwissen als auch Ressourcen jeglicher Art erfolgen. Seit 1999 dient die TF-CSIRT den europäischen Computer-Notfallteams als Forum zum Erfahrungsaustausch und fördert deren Kooperation. Dazu gehört sowohl die Unterstützung neuer CERTs bei ihrem Aufbau und der Ausbildung ihrer Mitarbeit als auch die Einführung von neuen Standards oder Diensten für die Computer-

[8] http://www.apcert.org
[9] http://www.terena.nl/about/mission.html

Notfallteams in Europa. Eine Errungenschaft dieser Arbeitsgruppe ist z. B. der Trusted Introducer, welcher im nachfolgenden Abschnitt näher beschrieben wird.

Insgesamt sollte von einem CERT eine Zusammenarbeit mit der TF-CSIRT in Erwägung gezogen werden. Besonders für Teams, die ihre Zielgruppe international repräsentieren, ist eine Teilnahme an der Task Force CSIRT interessant.

3.2.4 Trusted Introducer (TI)

Seit dem ersten September 2000 verwaltet der Trusted Introducer (TI) im Auftrag von TERENA ein Verzeichnis bekannter europäischer Computer-Notfallteams. Von Seiten der europäischen Teams bestand ein großes Interesse an dieser Dienstleistung. Anhand laufend aktualisierter Informationen bietet der Trusted Introducer den CERTs abseits formeller Strukturen die Möglichkeit, untereinander ein Netzwerk des Vertrauens („Web of Trust“) aufbauen. „The TI accreditation service is meant to do just that: facilitate trust by formally accrediting CSIRTs that are ready to take that step.“[10]

Die Akkreditierung eines CERTs erfolgt nach einem festgelegten dreistufigen Prozess. Um als „Level 0“ bzw. „gelistet“ in das Verzeichnis aufgenommen zu werden, genügt ein Antrag an den Trusted Introducer, über den dann alle akkreditierten Teams entscheiden können. Erst danach gilt ein Team als „bekannt“ und wird von den anderen auch als Computer-Notfallteam anerkannt. Der eigentliche Akkreditierungsprozess beginnt mit einer ausdrücklichen Einladung durch den Trusted Introducer. Ein CERT wird dann zunächst als „Accreditation Candidate“ (Level 1) geführt und muss innerhalb vorgegebener Fristen obligatorischen Anforderungen genügen. Dazu gehört u. a. auch die Entrichtung einer einmaligen Gebühr von derzeit 900 Euro. Um schließlich als „Level 2“ eingestuft zu werden, müssen weitere verbindliche Kriterien in einem festgelegten Zeitrahmen erfüllt werden. Dazu gehört auch die Verpflichtung, ein bestimmtes Maß an Informationen zu übermitteln, z. B. eine Beschreibung der angebotenen Dienstleistungen nach RFC 2350 oder eine Änderung der Constituency. Je nach Dringlichkeit sind diese Daten in einem Zeitraum von zwei Wochen bis spätestens vier Monaten zu aktualisieren und durch den TI zu verifizieren. Andernfalls läuft die Einstufung als „Level 2“ nach einer Frist von zwei Monaten aus und das Team wird zurückgestuft auf „Level 0“. Die jährliche Pflichtgebühr für akkreditierte Teams beträgt gegenwärtig 1.056 Euro.

Die Dienstleistungen des Trusted Introducer bestehen darin, akkreditierten Teams den Zugang zu einem geschlossenen Servicebereich zu ermöglichen, der z. B. Zugriff auf erweiterte Informationen und Mailinglisten bietet. Zusätzlich bietet der TI allen Interessierten auf einer frei zugänglichen Internetseite ein zentrales Kontaktverzeichnis gelisteter und akkreditierter CERTs sowie Informationen über sich selbst und den Aufnahmeprozess.

Trotz der Anforderungen des umfangreichen Akkreditierungsprozesses sollten sich alle europäischen Teams beim Trusted Introducer eintragen lassen (Level 0). Eine Einstufung als Level 2 empfiehlt sich besonders dann, wenn die Qualität und Zuverlässigkeit extern angebotener Dienstleistungen signalisiert werden soll und viele Kontakte mit anderen Teams zu erwarten sind.

3.3 Incident Handling in Deutschland

3.3.1 CERT der Hochschulen und Wissenschaftseinrichtungen (DFN-CERT)

Das Deutsche Forschungsnetz (DFN) hat sich bereits frühzeitig zum Ziel gesetzt, eine sichere Kommunikation für Forschung und Lehre zu gewährleisten. Dazu wurde im Januar 1993

[10] http://www.trusted-introducer.nl/about_ti/services.html

das DFN-CERT[11] ins Leben gerufen, das mittlerweile rechtlich selbstständig ist und seit Anfang 2004 als DFN-CERT Services GmbH seine Dienste anbietet. Seit seiner Gründung ist das DFN-CERT Mitglied im FIRST und kooperiert darüber hinaus aktiv mit weiteren Verbänden und Computer-Notfallteams.

Die erklärte Constituency des DFN-CERTs sind alle Hochschulen und Wissenschaftseinrichtungen in Deutschland, die Mitglied im DFN sind. Ihnen soll es als zentrale Anlaufstelle für alle sicherheitsbezogenen Probleme mit Computern und Netzwerken dienen. Darüber hinaus vertritt das Team das DFN gegenüber internationalen Computer-Notfallteams. Zu den wesentlichsten Dienstleistungen gehören zum einen die Verbreitung von Hinweisen und Warnmeldungen über Mailinglisten und die eigene Internetseite. Zum anderen bietet das DFN-CERT fachkundige Unterstützung bei der Umsetzung von Präventionsmaßnahmen und bei der Reaktion auf IT-Sicherheitsvorfälle (z. B. durch Analysen und technischen Hilfestellungen).
Aufgrund der langjährigen Erfahrungen und fachlichen Kompetenzen kann die Unterstützung durch das DFN-CERT als Berater und Kooperationspartner für den Aufbau eines neuen Teams durchaus von Vorteil sein.

3.3.2 CERT der Bundesbehörden (CERT-Bund)

Das Computer-Notfallteam für Bundesbehören (CERT-Bund[12]) ging im September 2001 aus dem seit 1995 bestehenden BSI-CERT hervor. Es hat sich dabei als zentrale Anlaufstelle für Behörden auf Bundesebene (formelle Constituency) in Bezug auf IT-Sicherheitsvorfälle jeder Art neu ausgerichtet. Bei dem Vorhandensein von ausreichenden Ressourcen bearbeitet es außerdem Anfragen aus dem privaten Bereich. Das CERT-Bund bietet dazu sowohl einen Bereitschaftsdienst von 24 Stunden am Tag als auch ein Lagezentrum für den Einsatz bei besonders schwerwiegenden Vorfällen.

Zur Wahrnehmung der Aufgaben umfasst das Dienstleistungsspektrum des Teams diverse präventive und reaktive Maßnahmen, wie z. B. Veröffentlichung von Handlungsempfehlungen über Mailinglisten und die eigene Internetseite, Durchführung von Workshops und Trainings für den Ernstfall oder Unterstützung durch den Betrieb einer Notfall-Hotline.

Aufgrund der engen Definition der formellen Constituency und der insgesamt begrenzten Kapazitäten ist hier nicht mit einer umfassenden Betreuung zu rechnen. Das CERT-Bund fördert allerdings die kooperative Zusammenarbeit im Rahmen von Verbänden und Arbeitsgruppen, sodass dort auf eine Unterstützung hingearbeitet werden kann.

3.3.3 Bundesländer-CERTs

Mittlerweile formieren sich neben dem CERT-Bund auch Computer-Notfallteams auf der Ebene der einzelnen Bundesländer, um deren jeweilige Verwaltungsbehörden koordiniert und kompetent bei Vorfällen zu betreuen. Nach aktuellem Stand verfügen darüber bereits Bayern (Bayern-CERT), Nordrhein-Westfalen (CERT-NRW) und Baden-Württemberg (CERT Baden-Württemberg). Das Land Niedersachsen befasst sich derzeit mit dem Aufbau eines eigenen Teams und ist auch Gegenstand dieser Arbeit.

Die CERTs der Bundesländer sollen dabei nicht nur die Landesbehörden und zugehörige Einrichtungen in Bezug auf IT und Daten schützen, sondern auch als kompetenter Ansprechpartner für alle sicherheitsbezogenen Anfragen von außen dienen. Die konkrete Einbindung des Computer-Notfallteams ist jedoch von Bundesland zu Bundesland verschieden. Das Bayern-CERT ist z. B. organisatorisch beim zentralen IT-Dienstleister aufgehängt. Die

[11] http://www.dfn-cert.de
[12] http://www.bsi.de/certbund/

Aufsicht hat jedoch der CISO im Bayerischen Staatsministerium des Innern. In Nordrhein-Westfalen ist das Team im Landesamt für Datenverarbeitung und Statistik angesiedelt und befindet sich dort in einem Referat unterhalb der Linie im Geschäftsbereich „Informationstechnik", Fachbereich „Netzdienste, IT-Service". Über das CERT in Baden-Württemberg dagegen ist bisher nach außen hin nur wenig bekannt. Gemäß einem Papier des Innenministeriums bündelt das Land aktuell bestehende Incident Handling Aktivitäten in einem landeseigenen CERT und entwickelt diese weiter.

3.3.4 Unternehmens-CERTs und kommerzielle Dienstleister

Die Wichtigkeit einer aktiven Handhabung von IT-Sicherheitsvorfällen haben einige Unternehmen bereits frühzeitig erkannt. Nur so können beachtliche Schäden vermindert bzw. verhindert werden, die sich sowohl finanziell als auch in einem Imageverlust auswirken können. Besonders größere Unternehmen verfügen heute bereits über interne Kompetenzen zur Bewältigung von IT-Sicherheitsvorfällen. Teils aus der Notwendigkeit bedingt durch konkrete Vorfälle heraus, teils aus Vorausschau werden seit geraumer Zeit eigene Computer-Notfallteams aufgebaut.

Diese kooperieren zwar in unterschiedlichem Ausmaß mit anderen Teams oder Verbänden, halten sich gegenüber der Öffentlichkeit ansonsten aber eher bedeckt. Nach außen präsente Unternehmens-CERTs sind z. B. das S-CERT der Sparkassenorganisationen oder das dCERT von T-Systems. Diese verfügen über eigene Internetseiten und treten u. a. auch durch die Veröffentlichung von sachbezogenen Artikeln in Erscheinung. Teilweise sind diese internen Unternehmens-CERTs jedoch gänzlich von der Außenwelt abgeschirmt, z. B. das CERT-VW der Volkswagen AG oder das Siemens-CERT der Siemens AG. Bis auf Einträge im Verzeichnis des Trusted Introducer sind für Außenstehende keine Informationen zu bekommen, da u. a. auch keine öffentliche Internetseite angeboten wird. Für Unternehmen gilt es hier vor allem zu bedenken, einen vernünftigen Mittelweg zwischen der Kooperation mit anderen und der Absicherung sensibler Bereiche und Geschäftsinterna zu finden.

Neben unternehmensinternen Teams gibt es mittlerweile auch einige kommerzielle CERT-Dienstleister am Markt. Diese bieten diverse Beratungsleistungen und Unterstützung bei Vorfällen durch zum Teil branchenspezifische Betreuung an. Hierzu zählen z. B. die Mcert Deutsche Gesellschaft für IT-Sicherheit mbH, die PRESECURE Consulting GmbH, die CERTCOM AG (CERTCOM) oder die Global Network Security GmbH (GNS-CERT).

Besonders interessant ist das Mcert, da es sich zum Ziel gesetzt hat, vornehmlich kleine und mittelständische Unternehmen kostengünstig mit sicherheitsrelevanten Empfehlungen und Warnungen zu versorgen und so zu einer Vorbeugung beizutragen. Dabei handelt sich um eine öffentlich-private Zusammenarbeit zwischen dem Bundesinnenministerium, dem Bundesministerium für Wirtschaft und Arbeit sowie einer Vielzahl namhafter Unternehmen und Sponsoren aus der Industrie.

3.3.5 Verbund deutscher CERTs (CERT-Verbund)

Primär allen deutschen Computer-Notfallteams steht auf nationaler Ebene die Mitwirkung im Rahmen des CERT-Verbundes[13] offen. Die Initiative wurde auf Betreiben von CERT-Bund, DFN-CERT und einigen Unternehmens-CERTs im August 2002 gegründet und hat zum Ziel, die Zusammenarbeit deutscher Teams zu fördern. Die freiwillige Teilnahme ist ohne Kosten verbunden und basiert auf festgelegten Leitlinien, welche z. B. die Vertraulichkeit und den Erfahrungsaustausch regeln („Code of Conduct").

[13] http://www.cert-verbund.de

Im Rahmen des CERT-Verbundes werden von den Mitgliedern verschiedene Projekte bearbeitet, die sich z. B. mit einem nationalen Frühwarnsystem (CarmentiS) oder der Standardisierung von Sicherheitsmeldungen in Deutschland befassen (Deutsches Advisory Format). Neben der Mitwirkung am Aufbau wichtiger Infrastrukturen bestehen zudem vielfältige Möglichkeiten zum Knüpfen von neuen Kontakten und zum Austausch wertvoller Erfahrungen.

Aktuell zählen alle größeren deutschen Computer-Notfallteams (z. B. DFN-CERT, CERT-Bund, S-CERT) sowie alle bisher bestehenden Bundesländer-CERTs zu den Mitgliedern. Neben weiteren Unternehmens-CERTs sind auch einige kommerzielle Dienstleister vertreten. Besonders für neue CERTs ist eine Mitarbeit im Rahmen des CERT-Verbundes empfehlenswert, da es vor allem in Deutschland keine vergleichbaren Kooperationen gibt. Besondere Anforderungen oder Kosten sind nicht ersichtlich.

4 Kritische Erfolgsfaktoren für Aufbau und Betrieb eines CERTs

4.1 Begriff des Erfolgsfaktors und seine Charakteristiken

Die Definition des Begriffs „Erfolgsfaktor“ bedingt vorab prinzipiell eine Klärung dessen, was unter Erfolg verstanden wird. Erfolg kann als positives Resultat bewusst eingesetzter Handlungen angesehen werden und bedeutet z. B., dass ein Unternehmen langfristig auf einem Markt überleben kann. Auf den Erfolg eines Computer-Notfallteams kann dies insofern übertragen werden, als dass dessen Aufbau zu einem einsatzfähigen Team führt, welches langfristig in Betrieb ist und geplante Maßnahmen mit einem insgesamt positiven Ergebnis umsetzen kann. Der Erfolg kann z. B. daran überprüft werden, inwieweit den Zielen des Mission Statements entsprochen wird.

Der Begriff des Erfolgsfaktors beruht im Wesentlichen auf den Ausführungen von R. D. Daniel [1961]. Demnach gibt es für einzelne Branchen bzw. Organisationen trotz zahlreicher Einflussgrößen nur eine beschränkte Anzahl Faktoren, die sowohl für den Erfolg als auch den Misserfolg ausschlaggebend sind. Erfolgsfaktoren lassen sich somit bündig umschreiben als diejenigen Faktoren, die direkt den Unternehmenserfolg oder -misserfolg beeinflussen. Dabei geht es vor allem um die Identifikation dieser zentralen Faktoren, die den Unternehmenserfolg langfristig beeinflussen. Umfassendere Definitionen gehen darüber hinaus und beinhalten zudem weitere Elemente, wie z. B. die prinzipielle Beeinflussbarkeit der Faktoren durch das Unternehmen und dessen Manager. Diese Faktoren werden dann auch als kritische Erfolgsfaktoren (KEF) bezeichnet. Für den Begriff des „kritischen Erfolgsfaktors“ existieren verschiedene gleichbedeutende Umschreibungen, z. B. Einflussgröße, Schlüsselfaktor oder auch strategischer Erfolgsfaktor (SEF). Im englischen Sprachraum wird vielfach nur von einem „Critical Success Factor“ (CSF) gesprochen.

Die Verantwortung für den Unternehmenserfolg liegt bei der Unternehmensführung. Demzufolge hat gerade sie die Pflicht zur Ermittlung kritischer Erfolgsfaktoren, mit deren Hilfe auch Schwächen in Geschäftsprozessen der Unternehmung identifiziert werden können. Ein wirklicher Erfolg lässt sich insgesamt nur dann erzielen, wenn durch die richtige Ausgestaltung der kritischen Erfolgsfaktoren ein Wettbewerbsvorteil aufgebaut werden kann. Es ist zudem darauf hinzuweisen, dass verfügbare Instrumente erst dann zu Erfolgsfaktoren werden, wenn nachgewiesen werden kann, dass mit ihrer Hilfe bessere Entscheidungen getroffen werden als ohne. Sonst verursacht deren Einsatz nur einen unnötigen Verzehr wichtiger und knapper Ressourcen. Kritiker bemängeln allerdings auch, dass einmal ermittelte Erfolgsfaktoren durch Bekanntmachung ihre Wirksamkeit verlieren würden, da sie kopiert werden könnten. In diesem Zusammenhang muss jedoch immer auch beachtet werden, dass Erfolgsfaktoren branchen- bzw. situationsspezifisch sein können (z. B. können die für ein Kreditinstitut ermittelten Erfolgsfaktoren nicht einfach auf eine Werbeagentur übertragen werden). Ein wirklicher Nutzenvorteil für eine Organisation kann also nur dann entstehen, wenn Wettbewerber diese nicht auch zeitgleich erkannt haben. Ist ein Erfolgsfaktor dagegen allgemein bekannt und bestehen keine Zweifel an der Gültigkeit, kann dessen Anwendung eher als „Best Practice“ vorausgesetzt werden.

4.2 Potenzielle Erfolgsfaktoren für den Aufbau eines CERTs

Zu den Erfolgsfaktoren eines Computer-Notfallteams ist bisher keine spezifische Literatur verfügbar. Daher wurden zur Ermittlung potenzieller Erfolgsfaktoren besonders solche Literaturquellen analysiert, die sich mit dem Aufbau und/oder dem Betrieb eines solchen Teams befassen und zum Teil als „Best Practice“ vorgeschlagen werden. Insgesamt wurden knapp zwanzig Quellen nach Erfolgsaussagen durchsucht. Alle relevanten Textstellen wurden gesammelt und übersetzt, sofern es zum eindeutigen Verständnis nötig war. Anhand der Bil-

dung von Oberbegriffen wurden die Aussagen aus der Literatur zunächst verdichtet und dann nach Möglichkeit in die Bereiche „Aufbau eines CERTs“ bzw. „Betrieb eines CERTs“ eingeordnet. Diese Unterscheidung wurde vorgenommen, da der Aufbau eines Teams direkte Auswirkungen auf den späteren Erfolg haben kann. Die Reihenfolge der Präsentation stellt keinerlei Wertung hinsichtlich der Wichtigkeit einzelner Faktoren dar. Gleichermaßen kann die Auflistung aufgrund eines starken Situations- und Organisationsbezuges von Erfolgsfaktoren nicht als erschöpfend oder vollständig betrachtet werden.

Der Aufbau eines Computer-Notfallteams erfolgt üblicherweise im Rahmen des bekannten Projektmanagements. Folglich kann davon ausgegangen werden, dass hier auch die kritischen Erfolgsfaktoren des Projektmanagements (z. B. Definition der Projektziele, Einbindung der Betroffenen, Erfahrungen des Projektleiters) gelten. Sie sind jedoch zum einen nicht kennzeichnend für ein CERT und zum anderen hat die Literatur auf diesem Feld umfangreiche Forschung betrieben. Da diese hier nicht noch einmal zusammengefasst werden sollen, wird zur Vereinfachung für den weiteren Verlauf dieser Arbeit die folgende Annahme getroffen und nicht weiter verfolgt: *Generell haben für den Aufbau eines Computer-Notfallteams die Erfolgsfaktoren des Projektmanagements ihre Gültigkeit.*

4.2.1 Unterstützung durch das Management

In der Literatur gibt es deutliche Hinweise darauf, dass sich der Aufbau eines Teams ohne das Einverständnis des verantwortlichen Managements als schwierig und problematisch gestalten kann. „(…) without management approval and support, creating an effective incident response capability can be extremely difficult and problematic.”[14] Dies wird durch Aussagen dahingehend spezifiziert, dass ein Computer-Notfallteam ohne Managementunterstützung nicht die notwendigen Ressourcen erhalten wird, um erfolgreich sein zu können. „Without management support it will be very difficult for the CSIRT to obtain the funding, staffing, and resources to be a success.”[15] Dazu zählt auch, dass das Management z. B. die Autorität von unternehmensintern operierenden Teams gewährleistet. „Otherwise, the team will lose credibility in the organization and will not be successful.”[16]

Daher lässt sich folgende Hypothese formulieren: *Der erfolgreiche Aufbau eines Computer-Notfallteams erfordert die frühzeitige und langfristige Unterstützung des zuständigen Managements, welches auch die Beschaffung benötigter Ressourcen sicherstellt.*

4.2.2 Unterstützung durch andere Teams

Auf den Erfolg kann es auch Auswirkungen haben, ob sich das im Aufbau befindliche CERT direkt die Unterstützung durch bestehende Teams sichert. „One of the most beneficial steps a newly forming team can take is to seek opportunities to meet other teams. (...) their experience might be especially valuable to your success in planning and implementing your team.”[17]

Der Aufbau eines neuen Teams kann durch den Zugriff auf Erfahrungsberichte oder bewährte Vorgehensweisen erleichtert werden. “Because the task of forming and operating a CSIRT is fraught with pitfalls that can result in the demise of a team, (…) supporting information and guidance would be imperative for success.”[18] Dies beinhaltet vor allem die Verwendung von „Best Practices“, um einen reibungslosen Aufbau sicherzustellen. „Having access to such resources can help a new CSIRT in its planning and implementation, providing opportunities to

[14] CERT Coordination Center [2002b].
[15] CERT Coordination Center [2002a].
[16] Killcrece u. a. [2003a, S. 38].
[17] Killcrece u. a. [2003a, S. 9f.].
[18] West-Brown u. a. [2003, S. xi].

leverage other work that has been successfully implemented as a best practice in parts of the CSIRT community."[19]

Daraus folgt unmittelbar: *Der erfolgreiche Aufbau eines Computer-Notfallteams erfordert die Unterstützung durch erfahrene und sachkundige Teams.*

4.2.3 Verfügbarkeit und sinnvoller Einsatz von Ressourcen

Die Verfügbarkeit von Ressourcen ist entscheidend für den Erfolg eines Teams, z. B. genügend qualifizierte Arbeitskräfte und benötigte Technologien. „These issues (…) are not all exclusive to an incident handling service, but they are critical to its success."[20] Aus einem vorangegangenen Abschnitt geht hervor, dass das Management in der Verantwortung steht, die notwendigen Ressourcen zu beschaffen. „Getting it right the first time will remove the need to expend precious resources on fixing a problem (…)."[21] Mit Hilfe einer sorgfältigen Aufbauplanung können daher frühzeitige Fehler vermieden und wertvolle Ressourcen eingespart werden. Dazu gehört auch die Sicherstellung der Finanzierung, da dies neben dem Mangel an qualifizierten Mitarbeitern zu den größten Herausforderungen gehört, denen sich ein CERT gegenübersieht. „One of the biggest problems faced by CSIRTs is the ability to obtain and maintain funding."[22] Erfahrungsberichten zufolge kann eine ungesicherte Finanzierung z. B. dazu führen, dass ein Team nicht das erforderliche Personal anwerben und halten kann.

Damit kann Folgendes als potenzieller Erfolgsfaktor festgehalten werden: *Der erfolgreiche Aufbau eines Computer-Notfallteams erfordert die Verfügbarkeit und den sinnvollen Einsatz benötigter Ressourcen (Humankapital, Technologie, Finanzen usw.).*

4.2.4 Mitarbeiter als Faktor zum Erfolg

Die sorgfältige Auswahl eines Mitarbeiters ist für ein Computer-Notfallteam sehr wichtig, da „(…) the success of the team could be undermined if that team member exhibits behaviours that undermined the trust of the constituency in the team."[23] Daher müssen die Mitarbeiter grundsätzlich mehr Fähigkeiten vorweisen können, als nur fachgerechte Erfahrungen aus dem Bereich der IT-Sicherheit. Denn „(…) the image that its staff members project through the way they conduct themselves, and the quality of service they provide, are paramount to the CSIRT's success."[24]

Zudem besteht am Markt ein genereller Mangel an geschultem Personal, da es unter anderem auch immer noch keinen qualifizierten Ausbildungsgang in diesem Bereich gibt. Daher kosten das Training und die Ausbildung des Personals sowie die Einarbeitung „eingekaufter" Mitarbeiter wertvolle Zeit und gerade die ist in der Aufbauphase nur begrenzt verfügbar.

Aus den vorangegangenen Ausführungen kann die folgende Annahme getroffen werden: *Der erfolgreiche Aufbau eines Computer-Notfallteams erfordert qualifizierte und erfahrene Mitarbeiter.*

4.2.5 Verhältnis zur Constituency

Der Beziehung zwischen Computer-Notfallteam und Constituency wird in zahlreichen Quellen eine hohe Bedeutung beigemessen. Akzeptiert die Constituency das CERT nicht oder

[19] Killcrece u. a. [2003b, S. 128].
[20] West-Brown u. a. [2003, S. 7].
[21] Smith [1995, S. 35].
[22] Killcrece u. a. [2003b, S. 55].
[23] Smith [1995, S. 18].
[24] West-Brown u. a. [2003, S. 4f.].

kann seine Dienste nicht wertschätzen, wird sie keine Vorfallsmeldungen vornehmen. Damit würde dem Team insgesamt seine Arbeitsgrundlage entzogen. “The key to success here is to establish an environment where individuals want to report suspicious activity.”[25] Somit hängt der Erfolg eines CERTs vor allem von dem Vertrauen ab, welches die Constituency in die Kompetenzen des Teams setzt. In deutlicherer Form bedeutet dies: „A team will live or die by its credibility – if the constituency stops trusting in the CSIRT then it will be next to impossible for it to succeed.”[26]

Um Akzeptanz und Vertrauen aufbauen zu können, wird vor allem Zeit benötigt. Daher wirkt sich ein möglichst frühzeitiger Kontakt positiv auf das beiderseitige Verhältnis aus. „To be a successful and effective team, a CSIRT must stay in contact with its constituency. This is always easier if the team is relatively near to the constituency from the start.“[27] Dazu ist es vorab wichtig, die Bedürfnisse der Constituency zu verstehen. Missverständnisse und Anfangsprobleme können zudem durch eine klare und offene Verständigung verringert werden. Daher kann die Beziehung zur Constituency als weiterer Erfolgsfaktor vermutet werden: *Der erfolgreiche Aufbau eines Computer-Notfallteams erfordert die Akzeptanz durch die Constituency, welche durch einen frühzeitigen und engen Kontakt erzeugt wird.*

4.2.6 Beschaffung von Informationen

Bei der Planung und Einführung eines neuen CERTs können zahlreiche Fehler gemacht werden. Die ausreichende Versorgung mit relevanten Informationen wirkt sich dabei nicht unwesentlich auf den Erfolg aus. Aus diesem Grund gehört das Sammeln relevanter Informationen zu den Grundvoraussetzungen für einen erfolgreichen Aufbau. Umfangreiche Informationen werden z. B. benötigt, um einerseits das Dienstleistungsangebot an den Bedürfnissen der Constituency auszurichten und andererseits daraus die notwendigen Qualifikationen der Mitarbeiter abzuleiten. Dazu gehören können z. B. auch rechtliche Erfordernisse, die sich aus der Gestaltung einer juristischen Person ergeben. Aus diesem Grunde ist die Beschaffung unterstützender Informationen unbedingt notwendig, um den Aufbau eines Teams erfolgreich gestalten zu können. Diese können z. B. auch aus der Verwendung von Dokumentationen oder „Best Practices“ gewonnen werden. „Having access to such resources can help a new CSIRT in its planning and implementation, providing opportunities to leverage other work that has been successfully implemented as a best practice in parts of the CSIRT community.“[28]

Folgende Hypothese lässt sich unmittelbar daraus ableiten: *Der erfolgreiche Aufbau eines Computer-Notfallteams erfordert die Identifikation und Sammlung relevanter Informationen, besonders unter Verwendung der Erfahrungen („Best Practice“) funktionierender Teams.*

4.2.7 Einhaltung zeitlicher Vorgaben

Der Aufbau eines Computer-Notfallteams erfolgt in der Regel als Projekt, also als zeitlich begrenztes Vorhaben. In diesem Zusammenhang gibt es eine Vielzahl von Umständen, die die zeitliche Planung negativ beeinflussen können. Zeitliche Verzögerungen können z. B. aus der Gestaltung des rechtlichen Rahmenkonstruktes (Rechtsform) entstehen, die sich dann insgesamt auf den Aufbau auswirken. Gleichermaßen stellt die Beschaffung und die Ausbildung qualifizierten Personals ein Problem für die zeitliche Planung dar. Ein knappes Zeitfenster zeigt sich spätestens bei Aufnahme der Dienstleistungen, wenn Vorgaben und Vorgehensweisen nicht ausreichend definiert wurden. Auch das Vertrauen der Constituency in das Team wird durch Verzögerungen negativ beeinflusst, da es mit mangelnden Kompeten-

[25] Killcrece u. a. [2003a, S. 36].
[26] Killcrece [2004, S. 19].
[27] Killcrece u. a. [2003b, S. 23].
[28] Killcrece u. a. [2003b, S. 128].

zen gleichgesetzt wird. Zusätzlich ist zu bedenken, dass der effektive Nutzen eines CERTs erst nach einer längeren Betriebsdauer ermittelt werden kann. Um also eine valide Erfolgsaussage für das zuständige Management oder das Team selbst treffen zu können, muss an dieser Stelle besonders der Zeitfaktor berücksichtigt werden.

Daher kann Folgendes vermutet werden: *Der erfolgreiche Aufbau eines Computer-Notfallteams erfordert die Einhaltung zeitlicher Vorgaben und berücksichtigt auch mögliche Verzögerungen.*

4.3 Potenzielle Erfolgsfaktoren für den Betrieb eines CERTs

4.3.1 Unterstützung durch das Management

Wie auch während der Aufbauphase ist es danach eine wichtige Herausforderung für ein Computer-Notfallteam, seinen Betrieb langfristig durch die Unterstützung des Managements sicherzustellen. „Without this continued support the CSIRT's long-term success may be in jeopardy.“[29] Dies bedeutet zunächst, dass das Management vor allem für eine ausreichende Versorgung mit notwendigen Ressourcen (Mitarbeiter, Technologie, Finanzen, usw.) sorgen muss, „(…) or the CSIRT will not be successful and their constituents will not report incidents to them.“[30] Für das Gelingen des CERTs ist die Mitwirkung durch das Management somit unentbehrlich. Ein grundlegendes Verständnis für die Wichtigkeit und die Funktionen eines Teams hilft den verantwortlichen Entscheidungsträgern, sowohl die Ziele als auch die im Grundgerüst festgelegten Funktionen zu unterstützen. Das Management muss z. B. die Autorität des CERTs genehmigen und sich dafür einsetzen, da es ansonsten an Glaubwürdigkeit bei seiner Constituency verlieren wird.

Im Ergebnis führt dies zu folgender Annahme: *Erfolgreiche Computer-Notfallteams werden langfristig durch das zuständige Management unterstützt, welches auch die Beschaffung benötigter Ressourcen sicherstellt.*

4.3.2 Unterstützung durch andere Teams

Die Unterstützung durch andere CERTs kann während des Betriebes in unterschiedlicher Weise erfolgen. Besonders im Rahmen von Verbandsmitgliedschaften (z. B. FIRST, TF-CSIRT) steht allen Computer-Notfallteams die Möglichkeit offen, aktiv am Austausch von Erfahrungen und der Entwicklung von „Best Practices“ beizutragen.

Im Übrigen haben sie weiterhin die Möglichkeit, sich die Unterstützung eines Teams im Rahmen einer direkten Kooperation zu sichern. Durch ein koordiniertes Vorgehen bei Vorfällen können z. B. Synergien genutzt und deren Bearbeitung insgesamt effizienter gestaltet werden. Folglich ist die Zusammenarbeit und Koordination mit anderen Teams überaus wichtig, um den Erfolg eines CERTs zu sichern.

Daraus lässt sich eine nahe liegende Vermutung ableiten: *Erfolgreiche Computer-Notfallteams kooperieren bei ihrer Arbeit mit anderen Teams (Erfahrungsaustausch, Zusammenarbeit, Koordination).*

4.3.3 Verfügbarkeit und sinnvoller Einsatz von Ressourcen

Die bei Computer-Notfallteams vielfach vorherrschende knappe Ressourcensituation setzt dessen Wirksamkeit Grenzen. So werden z. B. wichtige Ressourcen bereits im Vorfeld durch eine fundierte Ausbildung von Mitarbeitern verbraucht, ohne die jedoch eine effektive Arbeit nicht möglich ist. Durch die Knappheit von Ressourcen wird immer eine besondere Form der

[29] CERT Coordination Center [2002b].
[30] CERT Coordination Center [2002c, S. 10].

Arbeitsbelastung erzeugt, die im Ergebnis zu kurzfristigen Resultaten führt. Die Teams müssen insgesamt härter arbeiten und haben weniger Zeit, sich auf eine Verbesserung ihrer Fähigkeiten zu konzentrieren. Um jedoch schnell Resultate vorweisen zu können, werden in der Folge daher oftmals vorübergehende Lösungen beschlossen. Langfristig führt dies jedoch zu erheblichen Problemen, da einige Fähigkeiten nur unzureichend ausgebildet werden können.

Um eine wirksame Arbeit des Teams überhaupt erst zu ermöglichen, müssen besonders während einer Phase hoher Belastung ausreichend Kapazitäten vorhanden sein. Die Sicherstellung des erfolgreichen Betriebs erfordert somit die Verfügbarkeit erforderlicher Mittel und zugleich auch eine flexible Anpassung an veränderte Bedürfnisse. Dies kann zum Teil auch durch die Umverteilung anderweitig eingesparter Ressourcen erreicht werden. Für den Erfolg entscheidend sind sowohl die technische Ausstattung als auch die Verfügbarkeit an Humankapital. Außerdem bedarf es auch hier, vergleichbar mit anderen Geschäftsbereichen einer Unternehmung, einer gesicherten Finanzierung.

Die diesbezügliche Hypothese lautet daher folgendermaßen: *Erfolgreiche Computer-Notfallteams verfügen über eine langfristig gesicherte Finanzierung und über ausreichende Ressourcen (Humankapital, Technologie usw.), welche sinnvoll eingesetzt werden.*

4.3.4 Mitarbeiter als Faktor zum Erfolg

Die Mitarbeiter sind die Schnittstelle zwischen Computer-Notfallteam und Constituency. Unzureichend ausgebildete Mitarbeiter gefährden die Qualität und Verfügbarkeit von Dienstleistungen und beeinflussen dementsprechend auch den Ruf und das Erscheinungsbild des CERTs in negativer Weise. „(…) ultimately the success of the team could be undermined if that team member exhibits behaviours that undermined the trust of the constituency in the team.“[31] Für den erfolgreichen Betrieb eines Computer-Notfallteams können daher dessen Mitarbeiter als ein weiterer wichtiger Faktor angesehen werden. Erfahrene Mitarbeiter sind am Markt jedoch schwer zu rekrutieren, weil geeignetes Fachpersonal knapp ist. Dies rührt teilweise auch daher, dass es bisher keine etablierte methodische Ausbildung zum „Incident Handler“ gibt. Besonders wichtig ist daher eine gute „on the job“-Einarbeitung neuer Mitarbeiter, die ein signifikantes Maß an Ressourcen beanspruchen kann.

Gleichermaßen müssen Maßnahmen getroffen werden, um qualifiziertes Personal im Team halten zu können. Daher kann auch die Ausgestaltung des Teamumfeldes sowohl auf die Rekrutierung als auch die Sicherung hoch qualifizierten Personals einen großen Einfluss ausüben. Werden die Beiträge aller Mitglieder berücksichtigt und gefördert, festigt dies den Zusammenhalt innerhalb des Teams und bindet die Mitarbeiter stärker an das CERT. In Teams mit einer ungesicherten Finanzierung kann zudem notwendiges Personal nur schwer gehalten werden.

Als Schlussfolgerung kann somit festgehalten werden: *Erfolgreiche Computer-Notfallteams beschäftigen hoch qualifizierte und von der Constituency als kompetent angesehene Mitarbeiter.*

4.3.5 Verhältnis zur Constituency

Für den Betrieb eines Computer-Notfallteams ist ein enges Verhältnis zur Constituency von kritischer Bedeutung, da ohne die Akzeptanz und das Vertrauen der Constituency dem CERT keine Vorfälle gemeldet werden. „A team will live or die by its credibility – if the constituency stops trusting in the CSIRT then it will be next to impossible for it to succeed.“[32] Eine vertrauensvolle Beziehung muss langfristig aufgebaut und fortlaufend gepflegt werden.

[31] Smith [1995, S. 18].
[32] Killcrece [2004, S. 19].

Ein Anzeichen für den Erfolg eines Teams kann die Entstehung einer informellen Constituency kann. Allerdings können dadurch auch weitere Probleme erwachsen, da insgesamt von einer steigenden Arbeitsbelastung ausgegangen werden kann.

Grundsätzlich müssen der Constituency die Kompetenzen des Teams deutlich gemacht werden. Vor allem wird es immer wieder seinen Nutzen und seine Notwendigkeit unter Beweis stellen müssen. Fehlverhalten von Seiten der Mitarbeiter, eine mangelnde Dienstleistungsqualität und zeitliche Verzögerungen können zu Unzufriedenheit und Zweifeln bei der Constituency führen. „This directly reflects on the perceived competence and level of trust of a team by its constituency.“[33] Dadurch kann insgesamt das Vertrauensverhältnis negativ beeinträchtigt werden.

„Erfahrungen mit anderen CERTs haben gezeigt, dass die Ausrichtung auf die Zielgruppe entscheidend für den Erfolg und die Akzeptanz der Dienstleistung ist.“[34] Dies bedeutet, dass die Bedürfnisse und Ziele der Constituency in besonderem Maße zu berücksichtigen sind und sowohl die organisatorischen Strukturen als auch die angebotenen Dienstleistungen darauf zugeschnitten werden müssen. Als wichtig wird auch angesehen, dass das CERT geeignete Schnittstellen zur Constituency schafft. Dies kann weitere Ressourcen beanspruchen.

Folglich lautet die Annahme hier: *Erfolgreiche Computer-Notfallteams haben das Vertrauen ihrer Constituency erworben, welche auftretende Vorfällen meldet.*

4.3.6 Angebot an Dienstleistungen

Die Bedürfnisse der Constituency sind ausschlaggebend für die Ausrichtung des Dienstleistungsangebotes eines Computer-Notfallteams. Mittlerweile wird daneben auch die Ansicht vertreten, dass sowohl reaktive als auch präventive Maßnahmen gleichermaßen im Dienstleistungsportfolio vertreten sein sollten. Im Hinblick auf die Erreichung eines allgemeinen Sicherheitsbewusstseins kommt der Schulung der Constituency eine besondere präventive Bedeutung zu. Gelingt dies, wirkt es sich insgesamt positiv auf die Arbeitsbelastung des CERTs aus, da die Vorfälle in Anzahl und Schwere reduziert werden.

„The continuity of consistent and reliable services is essential to the successful operation of a CSIRT.“[35] Zum einen werden die Verfügbarkeit und die Qualität der Dienstleistungen direkt durch die Mitarbeiter beeinflusst. Zum anderen kann ein kontinuierliches Dienstleistungsangebot nur durch eine langfristig gesicherte Finanzierung erbracht werden. Die Beanspruchung von Ressourcen, u. a. durch entstehende Implementierungskosten gewünschter Dienstleistungen, sollte daher nicht unbeachtet bleiben.

Ein weiterer Aspekt für die Gestaltung des Dienstleistungsangebots sind die vielfältigen Abhängigkeiten zwischen den verschiedenen Tätigkeiten, da einige Aufgaben z. B. die Ergebnisse vorangegangener Dienstleistungen weiterverarbeiten. Das Verständnis um diese Verkettungen erhöht die Chancen für den erfolgreichen Aufbau neuer Dienstleistungen und kann dazu beitragen, Kosten zu senken. Diese Zusammenhänge können durch eine umfassende Definition und gründliche Dokumentation der Dienstleistungen sichtbar gemacht und Betriebsprobleme weitgehend vermieden werden.

[33] West-Brown u. a. [2003, S. 151].
[34] Pattloch/Kossakowski [2001, S. 31].
[35] West-Brown u. a. [2003, S. 151].

Somit ist für den Betrieb eines CERTs folgende Hypothese ableitbar: *Erfolgreiche Computer-Notfallteams Notfallteams kennen die Verbindungen zwischen einzelnen Dienstleistungen und richten ihr Dienstleistungsangebot nach den spezifischen Bedürfnissen ihrer Constituency, welches sowohl präventive als auch reaktive Dienste beinhaltet.*

4.3.7 Dokumentation von Vorgehensweisen und Richtlinien

„Documenting policies and procedures is one of the most important activities a CSIRT must undertake to be successful over the long term.“[36] Ansonsten kann z. B. die Kontinuität der Dienstleistungen nicht gewährleistet werden, da Mitarbeiter ohne eine Handlungsanleitung zwangsweise eigene Vorgehensweisen entwickeln und nach eigenen Regeln handeln. Weiterhin müssen der Constituency klare Anweisungen an die Hand gegeben werden, wie sie das CERT zu kontaktieren und wie Vorfallsmeldungen zu erstatten sind.

Zu einer umfassenden Dokumentation kann auch das Sammeln von Daten über gemeldete Vorfälle und spezifische Aktivitäten des Teams gezählt werden. Mit der Analyse dieser Statistiken können sowohl dem verantwortlichen Management als auch der Constituency die Leistungen und die Entwicklungen des Teams verdeutlicht werden. Zusätzlich können daraus Erfolgsaussagen abgeleitet werden.

Aus diesem Grunde lässt sich als Vermutung festhalten: *Erfolgreiche Computer-Notfallteams dokumentieren ihre Richtlinien und Vorgehensweisen, welche auch die angebotenen Dienstleistungen mit einbeziehen.*

4.3.8 Gestaltung einer unterstützenden Informationspolitik

„For a team to be able to operate at all, it must disclose information. However if disclosure is conducted inappropriately, this routine activity can result in the team’s demise.“[37] Ein vertrauensvoller Umgang mit Informationen ist also unbedingt erforderlich. Gelingt einem Team der angemessene Umgang mit Informationen nicht, ist mit einem Vertrauensverlust in der Constituency zu rechnen. Um Kontrolle über die notwendigen Informationsflüsse zu behalten, muss ein Computer-Notfallteam folglich auch über klar definierte Richtlinien in Form einer Informationspolitik verfügen. „It is important to define an information disclosure policy for the realm of incident response and beyond.“[38]

Der Erfolg eines Teams kann auch davon abhängen, dass für eine Aufrechterhaltung wichtiger Kommunikationsverbindungen mit anderen CERTs gesorgt wird. Nicht nur das Vertrauen der Constituency ist wichtig, sondern auch das der CERT-Gemeinschaft. Somit muss eine Informationspolitik auch die Verwendung sicherer Kommunikationswege und –mittel vorsehen (z. B. digital signierte und/oder verschlüsselte Emails).

Diese Ausführungen bewirken schließlich folgende letzte Hypothese: *Erfolgreiche Computer-Notfallteams verfügen über eine Informationspolitik, welche den vertrauensvollen Umgang mit Informationen regelt.*

4.4 Zwischenfazit

Aus der ausgewerteten Literatur geht deutlich hervor, dass der Erfolg sowohl beim Aufbau als auch beim Betrieb eines CERTs verschiedenen Einflüssen ausgesetzt ist. Durch die Aufstellung von Hypothesen wurden diverse mögliche Erfolgfaktoren identifiziert. Die Ergebnisse

[36] Killcrece u. a. [2003b, S. 106].
[37] West-Brown u. a. [2003, S. 132].
[38] West-Brown u. a. [2003, S. 144].

werden durch Abb. 5 auf S. 33 grafisch zusammengefasst. Demnach wirken fünf Faktoren gleichermaßen, mit nur marginal abweichenden Aspekten, auf den Aufbau und den Betrieb eines Computer-Notfallteams ein:

- Unterstützung durch das Management
- Unterstützung durch andere CERTs
- Ressourcenverfügbarkeit und –einsatz
- Verfügbarkeit und Qualifikation der Mitarbeiter
- Akzeptanz durch die Constituency

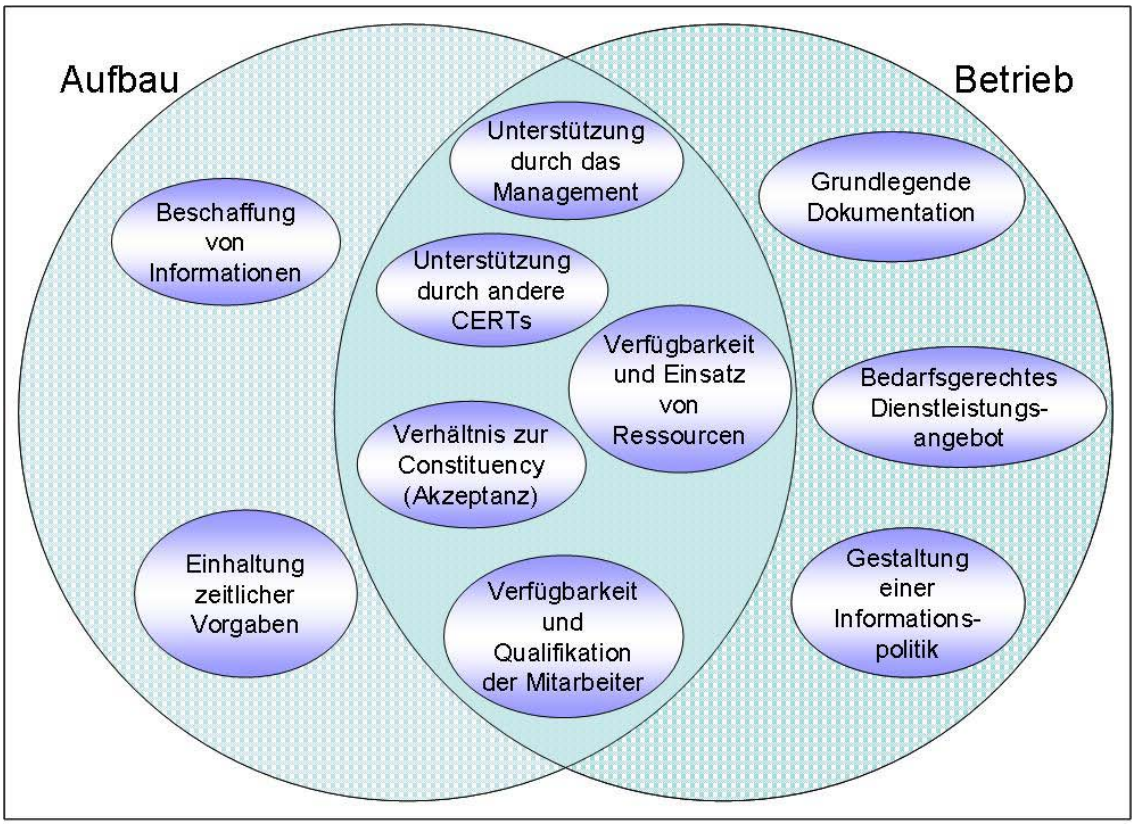

Abb. 5: Kritische Erfolgsfaktoren für Aufbau und Betrieb eines CERTs [39]

Als kennzeichnend für den Aufbau eines Teams wurden zwei Faktoren ermittelt:

- Verfügbarkeit von Informationen
- Einhaltung zeitlicher Vorgaben

Zudem konnten weitere Faktoren unterschieden werden, die allein Einfluss auf den Betrieb eines CERTs haben:

- Bedarfsgerechtes Dienstleistungsangebot
- Grundlegende Dokumentation
- Vorhandensein einer Informationspolitik

[39] Quelle: Projekt „CERT Niedersachsen“ [2005]; Dr. K.-P. Kossakowski

5 Empirische Überprüfung der Erfolgsfaktoren eines CERTs

Im Folgenden wird zunächst kurz auf das Design des Fragebogens eingegangen, um schließlich eine Auswertung der Ergebnisse vornehmen zu können. Ein voller Abdruck des Fragebogens und der Ergebnisse ist zusätzlich im Anhang zu finden.

5.1 Design des Fragebogens

5.1.1 Inhaltlicher Aufbau des Fragebogens

Der verwendete Fragebogen wurde im Zusammenhang mit der Extraktion potenzieller Erfolgsfaktoren aus der verfügbaren Literatur konzipiert. Besonders wichtig war es, die Anzahl der Fragen möglichst gering zu halten und dabei trotzdem qualitativ vertretbare Ergebnisse zu erzielen. Der Fragebogen besteht aus insgesamt 27 Fragestellungen, die in sieben thematische Segmente (Blöcke A bis G) unterteilt wurden.

Der einleitende Block A dient als „Eisbrecher“, um den Einstieg in den Fragebogen zu erleichtern. Er enthält vier einfache Fragen zum Erfahrungsstand des Befragten (Fragen 1 bis 4). Block B stellt daran anschließend vier grundlegende Fragen zum Aufbau des CERTs, bei dem der Befragte tätig wurde. Mit diesen Fragen wird beabsichtigt, etwas über die Dauer und Gründe für den Aufbau sowie die Schwierigkeiten währenddessen zu erfahren. Analog zu Block B soll der dritte Block (Fragen 9 bis 21) möglichst viele Informationen über den aktuellen CERT-Betrieb liefern. Im Zentrum steht dabei die Ermittlung von Rahmenbedingungen der jeweils befragten Teams (Mission Statement, Constituency, Befugnisse, Organisation des Teams, Kooperation mit anderen, Finanzierung). Zudem wird explizit nach Schwierigkeiten bei dem Betrieb der CERTs gefragt. Die Fragenblöcke D und F befassen sich vornehmlich mit Einflüssen, die sich positiv oder negativ auf den Erfolg beim Aufbau bzw. Betrieb eines Computer-Notfallteams auswirken (Hindernisse und Erfolgsfaktoren). Schließlich werden die Teilnehmer in den Blöcken E und G mit einer Reihe von Aussagen konfrontiert, deren Relevanz bezüglich der Wirkung auf den Erfolg eines CERT zu bewerten ist. Diese entstammen den Hypothesen aus Kapitel 4 und stellen das eigentliche Ziel der Befragung dar. Die Gestaltung der Aussagen wird im Anschluss an das Fragebogendesign dargestellt. Die Fragen dieser vier letzten Blöcke bauen stark auf die persönlichen Erfahrungen jedes Befragten und hängen somit besonders von deren Antwortbereitschaft ab.

5.1.2 Formaler Aufbau des Fragebogens

Zu Beginn der Arbeit erschien eine telefonische Befragung von CERT-Experten als einfach und kostengünstig durchzuführen. Computer-Notfallteams operieren jedoch in hochsensiblen Sicherheitsbereichen von Organisationen. Bei einer ersten Kontaktaufnahme zu potenziellen Teilnehmern stellte sich daher schnell heraus, dass die Bereitschaft einiger CERTs zur Teilnahme an telefonischen Interviews aufgrund ihrer zum Teil restriktiven Informationspolitiken nicht sehr hoch sein würde. Auch die Entwicklung einer Online-Umfrage konnte trotz diverser Vorteile aufgrund des begrenzten Zeitraumes nicht in Betracht gezogen werden.[40] Bei der Erstellung eines Online-Fragebogens hätte es zeitintensive Vorarbeiten und Tests zur Gewährleistung aller Aspekte der IT-Sicherheit benötigt. Um die Bedenken gegenüber einer Befragung abzuschwächen, fiel schließlich die Entscheidung für einen schriftlichen Fragebogen. Dieser wurde zusammen mit einem frankierten Rückumschlag verschickt, um eine möglichst hohe Rücklaufquote zu erhalten. Zusätzlich wurden alle Teilnehmer per Email an die Abgabefrist erinnert.

[40] Vorteile können u. a. sein: die Zielgruppe ist leichter erreichbar, es entstehen weniger Kosten, die Ergebnisse liegen sofort in elektronischer Form vor.

Der Fragebogen wurde ursprünglich als Leitfaden für ein Interview mit einer Dauer von etwa fünfzehn Minuten konzipiert. Der Fragebogen besteht daher sowohl aus geschlossenen (Vorgabe von Antwortmöglichkeiten, z. B. Frage 12) als auch offenen Fragen (freie Antwortmöglichkeit, z. B. Frage 7), die an einigen Stellen (Fragen 4, 5 und 19) auch Mehrfachnennungen zulassen. Um möglichst profunde Angaben zu erhalten, wird bei einzelnen Fragen auch eine Mischform angewendet (vorformulierte Antworten mit der Möglichkeit zur freien Antwort, z. B. Frage 19). Die Überprüfung möglicher Erfolgsfaktoren erfolgt schließlich anhand einer Auflistung formulierter Aussagen (Block E und G), die von den Befragten mittels einer vierfachen Skala von „sehr relevant" („++") bis „nicht relevant" („--") hinsichtlich deren Wichtigkeit bewertet werden können.

5.1.3 Ableitung der zu bewertenden Aussagen

In Kapitel 4 wurden mögliche Erfolgsfaktoren für den Aufbau und den Betrieb eines Computer-Notfallteams identifiziert. Dabei zeigte sich, dass einige davon während beider Phasen Einfluss auf den Erfolg haben können, jedoch mit teilweise verschiedenen Gesichtspunkten. Um die Möglichkeit offen zu halten, diese Unterschiede in der Befragung genauer evaluieren zu können, wurden aus den Erfolgsfaktorhypothesen etwas differenziertere Aussagen zur Bewertung abgeleitet. Zudem sollten die Teilnehmer nicht durch klar formulierte Erfolgsfaktoren bei der Beantwortung der Frageblöcke D und F beeinflusst werden. Aufgrund der angenommenen gegenseitigen Wirkungsbeziehungen zwischen den Faktoren können einige Aussagen verschiedenen Erfolgsfaktoren zugeordnet werden (z. B. betrifft die Forderung nach der Versorgung mit notwendigen Ressourcen durch das Management sowohl den Faktor „Ressourcen" als auch „Management"). Die nachfolgende Tabelle zeigt in Bezug auf den Aufbau eines Computer-Notfallteams, zu welchen Erfolgsfaktoren sich die jeweiligen Aussagen zuordnen lassen.

Tab. 2: Aussagen zum erfolgreichen Aufbau eines CERTs

Erfolgsfaktor	Aussage(n)
Unterstützung durch das Management	• Das Management muss die Unterstützung langfristig zusichern. • Notwendige Ressourcen (Personal, Technologie, Finanzen usw.) müssen vom Management ausreichend zur Verfügung gestellt werden.
Unterstützung durch andere Teams	• Die Unterstützung durch erfahrene CERTs muss sichergestellt werden (z. B. direkte Hilfe beim Aufbau, Nutzung von Best Practices).
Ressourcenverfügbarkeit und -einsatz	• Notwendige Ressourcen (Personal, Technologie, Finanzen usw.) müssen vom Management ausreichend zur Verfügung gestellt werden. • Der Aufbau eines neuen Teams muss gut koordiniert werden. Fehler bei der Einführung eines neuen Teams verbrauchen später notwendige Ressourcen.
Verfügbarkeit und Qualifikation der Mitarbeiter	• Es müssen genügend qualifizierte Mitarbeiter vorhanden sein. • Eine fundierte Ausbildung neuer Mitarbeiter muss vor Betriebsaufnahme erfolgen.
Akzeptanz durch die Constituency	• Bereits während der Einführung muss ein vertrauensvolles Verhältnis zur Constituency aufgebaut werden. • Frühzeitig muss ein enger Kontakt zur Constituency (Kundenkreis) hergestellt und aufrechterhalten werden.
Verfügbarkeit von Informationen	• Alle relevanten und benötigten Informationen für Planung und Einführung müssen früh beschafft und zur Verfügung gestellt werden. • Es muss Klarheit herrschen über die anzubietenden Dienstleistungen und benötigten Vorgehensweisen.
Einhaltung zeitlicher Vorgaben	• Beim Aufbau müssen zeitliche Verzögerungen, bedingt durch verschiedene Faktoren (z. B. erfahrenes Personal nicht verfügbar), eingeplant werden. • Der Aufbau eines neuen Teams muss schnell erfolgen.

Zur Bewertung standen auch die formulierten Anforderungen aus der nächsten Tabelle, deren Fokus auf dem Betrieb eines CERTs liegt. Sie zeigt, aus welchen Erfolgsfaktoren die jeweiligen Aussagen hervorgehen.

Tab. 3: Aussagen zum erfolgreichen Betrieb eines CERTs

Erfolgsfaktor	Aussage(n)
Unterstützung durch das Management	• Das Management muss seine Unterstützung langfristig zusichern (z. B. Zusicherung der Befugnisse). • Notwendige Ressourcen (Personal, Technologie, Finanzen usw.) müssen vom Management ausreichend zur Verfügung gestellt werden.
Kooperation mit anderen Teams	• Die Unterstützung durch andere CERTs muss sichergestellt werden (z. B. Nutzung von Best Practices). • Die eigene Arbeit muss mit anderen Teams abgestimmt werden.
Ressourcenverfügbarkeit und -einsatz	• Notwendige Ressourcen (Personal, Technologie, Finanzen usw.) müssen vom Management ausreichend zur Verfügung gestellt werden.
Verfügbarkeit und Qualifikation der Mitarbeiter	• Erfahrene und qualifizierte Mitarbeiter müssen vorhanden sein. • Die Mitarbeiter beeinflussen das Erscheinungsbild des Teams und müssen sich jederzeit kompetent und angemessen verhalten.
Akzeptanz durch die Constituency	• Das Vertrauen der Constituency muss langfristig erworben werden. • Bei der Constituency muss ein allgemeines Bewusstsein für Sicherheit und die Arbeit des Teams geschaffen werden.
Bedarfsgerechtes Dienstleistungsangebot	• Das Dienstleistungsangebot muss sich an den spezifischen Bedürfnissen der Constituency ausrichten. • Die Dienstleistungen müssen reaktive/präventive Aufgaben umfassen. • Die Verbindungen zwischen verschiedenen Dienstleistungen müssen bekannt sein.
Grundlegende Dokumentation	• Vorgehensweisen und Dienstleistungen müssen dokumentiert werden. • Der Constituency müssen klare Richtlinien zur Berichterstattung gegeben werden. • Zur Messung des Erfolgs und zur Planung zukünftiger Vorgehensweisen müssen Daten gesammelt und analysiert werden (z. B. von bearbeiteten Vorfällen).
Vorhandensein einer Informationspolitik	• Der Informationsfluss zwischen allen Beteiligten muss durch eine umfassende Informationspolitik geregelt ablaufen.

Im Fragebogen selbst wurden die Aussagen in ungeordneter Reihenfolge präsentiert. Die Teilnehmer sollten so vor ähnlichen aufeinander folgenden Formulierungen bewahrt und damit eine unterschiedslose Einheitsbewertung verhindert werden.

5.2 Auswertung der Ergebnisse

Nachdem eine erste Kontaktaufnahme zu den Teilnehmern via Email hergestellt wurde, wurden die Fragebögen schließlich in der 49. Kalenderwoche 2005 mit der Post versendet. Von den insgesamt 13 ausgesandten Fragebögen kamen sieben im Januar 2006 zurück und konnten für eine Auswertung verwendet werden. Eine Übersichtstabelle der Ergebnisse befindet sich zudem im Anhang.

Als Einstieg in den Fragebogen wurde sowohl nach der aktuell ausgeübten Funktion als auch nach der Dauer der Arbeit mit Computer-Notfallteams gefragt. Demnach üben alle Teilnehmer eine Leitungsfunktion in ihrem jeweiligen Team aus und verfügen über Berufserfahrungen zwischen zwei und dreizehn Jahren. Im Mittel arbeiten die Befragten seit fünf Jahren im CERT-Betrieb. Dies ist nicht verwunderlich, denn ein Blick auf das ebenfalls ermittelte Datum der CERT-Inbetriebnahme zeigt, dass fast alle befragten Teams innerhalb der letzten fünf Jahre aufgebaut wurden. Hinsichtlich des Aufbaus von Computer-Notfallteams können

die Teilnehmer ebenfalls Erfahrungen aufweisen. Jeder von ihnen war an mindestens einem Projekt beteiligt, der Höchstwert lag bei zehn betreuten Projekten. Ein Projekt beanspruchte dabei im Durchschnitt 10,5 Monate, das Spektrum der Antworten reicht von drei bis achtzehn Monaten.

5.2.1 Erkenntnisse und Folgerungen für den Aufbau eines CERTs

Im Folgenden werden nun die Ergebnisse zum Aufbau eines Computer-Notfallteams nach den jeweiligen Erfolgsfaktoren geordnet dargestellt. Direkt im Anschluss an jeden Faktor wird kurz erläutert, ob der Faktor durch die Befragung bestätigt werden konnte bzw. welche Bedeutung ihm aus den Ergebnissen zukommt. Alle Aussagen zum Aufbau eines CERTs können in Tab. 2 auf S. 35 nachgelesen werden.

Faktor: Unterstützung durch das Management
Im Fragebogen wurde dieser Faktor mit Hilfe von zwei differenzierten Aussagen abgefragt. Eine langfristige Unterstützung durch das Management bewerteten 86 % der Befragten mit „sehr relevant“, weitere 14 % hielten diese für „relevant“. Bei einer Rangbildung der Aussagen hinsichtlich deren Wichtigkeit für den Erfolg beim CERT-Aufbau belegt diese Aussage den obersten Rang. Die Anforderung, dass die notwenigen Ressourcen vom zuständigen Management ausreichend zu Verfügung gestellt werden müssten, bewerteten alle Fachleute mit mindestens „relevant“. Zudem finden sich unter den Antworten auf die direkten Fragen nach möglichen Hindernissen und Faktoren weitere Angaben, welche die Wirksamkeit des Erfolgsfaktors stützen. Als mögliche Hindernisse wurden z. B. „Fehlende Management-Zustimmung“ und „Fehlendes Commitment der Mutter-Organisation“ aufgezählt. Als zum Erfolg beitragende Faktoren wurden dagegen „Management Support“ und „Klares Commitment des Vorstandes“ genannt. Damit wird „Unterstützung durch das Management“ als kritischer Erfolgsfaktor bestätigt.

Faktor: Unterstützung durch andere CERTs
Dieser Faktor stand mit einer konkreten Aussage zur Bewertung, welche von nur 29 % als „wenig relevant“ beurteilt wird. Der größere Anteil von 72 % verteilt sich mit 57 % auf „relevant“ und 29 % auf „sehr relevant“. Unter den frei formulierten Antworten findet sich dazu einzig der Hinweis, dass „Unterstützung der beteiligten Parteien und Partner“ notwendig sei. Der Erfolgsfaktor „Unterstützung durch andere Teams“ wird zwar nicht durch persönliche Erfahrungen der Befragten belegt, kann jedoch aufgrund der Bewertung auch nicht entkräftet werden.

Faktor: Verfügbarkeit und sinnvoller Einsatz von Ressourcen
Die Teilnehmer konnten zwei Aussagen zu diesem Faktor bewerten. Alle Fachleute waren sich einig, dass eine ausreichende Versorgung mit Ressourcen (Personal, Technologie, Finanzen usw.) durch das zuständige Management als mindestens „relevant“ einzustufen ist. Die Einsparung von Ressourcen durch einen gut koordinierten Aufbau eines Teams hielt eine Mehrheit von 57 % für „relevant“ und weitere 29 % für „sehr relevant“. Insgesamt liegen diese beiden Aussagen in der Bewertung an vierter und fünfter Stelle. Aus den Erfahrungsberichten der Befragten geht auch hervor, dass zu bewältigende Schwierigkeiten in der „Finanzierung“ und der „Ausstattung mit Ressourcen (Budget, Personal)“ liegen. Nicht verwunderlich ist daher, dass als weitere Hindernisse auch „Finanzierung einer angemessenen Dienstleistung“, „zu wenig Ressourcen“ und „Ressourcenbeschaffung in Zeiten der Kostensparprogramme“ genannt werden. Als einen der wichtigsten Faktoren sehen die Teilnehmer aus diesem Grund auch eine „ausreichende Ausstattung an Personal und Technik“ an. Im Ergebnis führt dies zur Legitimität des Erfolgsfaktors „Verfügbarkeit und sinnvoller Einsatz von Ressourcen“.

Faktor: Verfügbarkeit und Qualifikation der Mitarbeiter
Eine sehr hohe Bedeutung wurde dem Personal zugemessen. Die Anforderung, dass genügend qualifizierte Mitarbeiter zur Verfügung stehen müssten, bewerteten 71 % mit „sehr relevant“ und die restlichen 29 % mit „relevant“. Diese Aussage belegt damit neben zwei weiteren den zweiten Rang. Auch dass eine fundierte Ausbildung neuer Mitarbeiter vor Betriebsaufnahme eines CERTs erfolgten müsste, stuften sechs von sieben Teilnehmern als „relevant“ ein. Nur ein Experte sah diesen Punkt als „wenig relevant“ an. Sehr konkret waren auch die Angaben zu möglichen Schwierigkeiten und Hindernissen. So wurde z. B. ein „Mangel an Personal mit entsprechender Fachkompetenz“ ebenso genannt, wie „wechselndes Personal“. Aus diesem Grund finden sich auch bei den Erfolg verursachenden Faktoren sehr eindeutige Aussagen, z. B. wurde neben der zweimaligen Nennung von „Personal“ als Einflussgröße zusätzlich auch eine „breite Fachkompetenz der Mitarbeiter“ aufgeführt. Damit kann als weiterer Erfolgsfaktor beim CERT-Aufbau die „Verfügbarkeit und Qualifikation der Mitarbeiter“ bestätigt werden.

Faktor: Akzeptanz durch die Constituency
Das Verhältnis zwischen Computer-Notfallteam und Constituency wurde von allen potenziellen Erfolgsfaktoren mit am höchsten gewertet. Bereits während der Einführung eines Teams ein vertrauensvolles Verhältnis zur Constituency aufzubauen, wurde von 57 % als „sehr relevant“ und von den übrigen 43 % als „relevant“ angesehen. Höher bewertet wurde die Anforderung, dass frühzeitig ein enger Kontakt zur Constituency hergestellt und aufrechterhalten werden müsse. Diese Aussage wurde von 71 % mit „sehr relevant“ bewertet und nimmt einen zweiten Rang ein. Dies wird auch durch verschiedene Angaben getragen, dass z. B. „Akzeptanz bei der Constituency“ zur Erfolgsmessung genutzt wird oder „fehlende Akzeptanz bei den verantwortlichen Administratoren“ als großes Hindernis beim CERT-Aufbau angesehen wird. Verständlicherweise wird daher auch die „persönliche Nähe zum Kunden“ als wichtiger Punkt zum Gelingen angesehen. Alles in allem stellt das Verhältnis zur Constituency, insbesondere deren Akzeptanz, einen der wichtigeren Erfolgsfaktoren dar.

Faktor: Verfügbarkeit von Informationen
Im Rahmen dieses Faktors wurden die teilnehmenden Experten gebeten, die Wichtigkeit der frühzeitigen Beschaffung von relevanten Informationen zu bewerten. Diese Aussage wurde von über zwei Dritteln als „relevant“ angesehen. Knapp ein Drittel jedoch stufte diese sogar als „wenig relevant“ ein. Aussagekräftiger sind dagegen die Bewertungen der zweiten Anforderung. Demnach sehen 86 % das Vorliegen von Klarheit über Dienstleistungen und Vorgehensweisen als „sehr relevant“ an. Nur ein Befragter äußerte sich hier mit „wenig relevant“. Den Erfahrungen der Teilnehmer zufolge, führt die unzureichende „Definition von Dienstleistungen“ zu Schwierigkeiten und bringt zeitliche Verzögerungen mit sich. Daher werden „unklare Aufgaben“ sowohl als Hindernis als auch wichtiger Faktor im Sinne von „Festlegung der Aufgaben“ genannt. Die „Verfügbarkeit von Informationen“ ist somit auch als ein Erfolgsfaktor für die Einführung von neuen Computer-Notfallteams zu bejahen.

Faktor: Einhaltung zeitlicher Vorgaben
Als letzter Faktor in der Aufbauphase sollte die Einhaltung zeitlicher Vorgaben beurteilt werden. Dass insgesamt mit zeitlichen Verzögerungen zu rechnen ist, sahen 86 % der Befragten als „relevant“ an. Sehr deutlich wurde jedoch gegen einen schnellen Aufbau neuer Teams Stellung bezogen. Dies sahen mehr als zwei Drittel als „wenig relevant“ an. Diese beiden Aussagen belegen von ihrer Wichtigkeit her die hinteren Ränge. Somit spielt die Dauer des Aufbaus weniger eine Rolle, als dass dieser im Rahmen von zeitlichen Vorgaben erreicht werden kann. Bestätigt wird dies zum einen durch Erfahrungsberichte der Teilnehmer, wonach ein erfolgreicher Aufbau z. B. durch Meilensteine des Aufbauprojektes und die Einhaltung des Starttermins evaluiert werden kann. Zum anderen werden als wichtige Einflussgrößen weiterhin eine „gute Projektplanung“ sowie „Starttermin festlegen und einhalten“ genannt. Die „Einhaltung zeitlicher Vorgaben“ als Erfolgsfaktor ist als solches nicht abzulehnen.

Den Ergebnissen zufolge spielt die Dauer des Aufbaus in diesem Zusammenhang jedoch keine bedeutende Rolle.

5.2.2 Erkenntnisse und Folgerungen für den Betrieb eines CERTs

In diesem Abschnitt werden die Ergebnisse aus den Frageblöcken F und G zusammengefasst. Dort sollten mögliche Erfolgsbarrieren genannt und Aussagen in Hinsicht auf den erfolgreichen Betrieb eines Computer-Notfallteams bewertet werden. Die genauen Wortlaute sämtlicher Aussagen zum Betrieb können in Tab. 3 auf S. 36 nachgelesen werden.

Faktor: Unterstützung durch das Management
Hinsichtlich des Aufbaus eines Teams waren das Ergebnis der ersten Anforderung sehr deutlich und führte zum ersten Rang unter allen Aussagen. In Bezug auf den Betrieb eines CERTs wurde hier eindeutig anders geurteilt. Demnach sehen die langfristige Unterstützung durch das Management nur noch 43 % als „sehr relevant", weitere 43 % immerhin noch als „relevant" an. Nicht zuletzt, weil 14 % der Teilnehmer dies als „wenig relevant" einstuften, landete diese Aussage nun auf Rang 5. Die Anforderung, dass das Management für die notwendigen Ressourcen zu sorgen habe, wurde dagegen vergleichbar mit der Aufbauphase bewertet. Alle Teilnehmer halten dies für mindestens „relevant", drei von ihnen sogar für „sehr relevant". Aus den genannten Hindernissen geht hervor, dass ein Teil der Unterstützung sogar kontraproduktiv sein kann. Dort wird der Punkt „Management mischt sich ein" als mögliche Schwierigkeit für einen erfolgreichen CERT-Betrieb angeführt. Eine produktive Beziehung zur Führungsebene schließt dies jedoch nicht aus, da z. B. „direktes Reporting an Vorstand oder Geschäftsleitung" für wichtig gehalten wird. Insgesamt besitzt der Erfolgsfaktor „Unterstützung durch das Management" auch hier seine Gültigkeit, wenn auch nicht mit der gleichen Bedeutsamkeit wie beim Aufbau.

Faktor: Unterstützung durch andere CERTs
Eine unterstützende Zusammenarbeit mit anderen Computer-Notfallteams und die Nutzung von „Best Practices" sieht eine Mehrheit von 86 % als mindestens „relevant" an. Nur 14 % stimmten mit „wenig relevant" dagegen. Dass die eigene Arbeit darüber hinaus mit anderen Teams koordiniert und abgestimmt werden muss, weisen jedoch 43 % der Befragten als „wenig relevant" zurück. Die Unterstützung beschränkt sich damit vornehmlich auf eine informelle Zusammenarbeit. Jedes der befragten CERTs gab an, Mitglied in mindestens zwei Verbänden oder freiwilligen Arbeitsgruppen zu sein (z. B. CERT-Verbund, FIRST oder TF-CSIRT). Weiterhin wird genannt, dass z. B. zur erfolgreichen Kooperation bei der Verarbeitung von Meldungen standardisierte Schnittstellen zu anderen Teams vorhanden sein müssen, da sonst keine automatisierte Verarbeitung von Meldungen vorgenommen werden kann. Der zugehörigen Hypothese aus Kapitel 4 entsprechend, liegt der Schwerpunkt dieses Erfolgsfaktors auf der Zusammenarbeit und dem Austausch von Erfahrungen. Dies wird auch durch die Ergebnisse der Befragung bestätigt, weshalb seine Wirksamkeit nicht abgelehnt werden kann.

Faktor: Verfügbarkeit und sinnvoller Einsatz von Ressourcen
An dieser Stelle stand nur eine Aussage zur Bewertung. Als mindestens „relevant" für den erfolgreichen Betrieb sahen 100 % der befragten CERT-Leiter eine ausreichende Versorgung mit Ressourcen durch das Management an. Die Mehrheit bewertete hier mit „relevant". Im Vergleich mit der Wichtigkeit anderer Aussagen liegt diese auf dem dritten Rang. Auf die Frage nach erlebten Schwierigkeiten wurden sogar eindeutig „Ressourcen (monetäre Ausstattung)" als Problem identifiziert. Ein weiterer Punkt, der auch als Hindernis betrachtet wird, ist die Ausstattung mit „zu wenig Personal". Insgesamt kann auch hier die Gültigkeit des Erfolgsfaktors „Verfügbarkeit und sinnvoller Einsatz von Ressourcen" nicht widerlegt werden. Von seiner Anwendbarkeit ist daher auszugehen.

Faktor: Verfügbarkeit und Qualifikation der Mitarbeiter
Die Teilnehmer wurden auch hinsichtlich der Bedeutung von Humankapital bei dem Betrieb eines CERTs befragt. Demnach halten 71 % das Vorhandensein von erfahrenen und qualifizierten Mitarbeitern für „sehr relevant“, weitere 29 % für „relevant“. Im Ganzen ein deutliches Ergebnis, wodurch diese Aussage auch auf den ersten Rang platziert wird. Etwas geringer, aber dennoch nicht unbedeutend, wurde ein kompetentes und angemessenes Auftreten der Mitarbeiter einschätzt. Immerhin halten dies die Befragten zu je 43 % für „sehr relevant“ bzw. „relevant“ und nur 14 % für unbedeutender. Getragen werden diese Bewertungen durch Erfahrungen der Teilnehmer, wonach z. B. „fehlendes qualifiziertes Personal“ und ein „Personalweggang und Aufwuchs“ als Schwierigkeiten erlebt wurden. Als Hindernis wird daher angesehen, wenn „zu wenig Personal“ vorhanden ist. Demzufolge ist eine „ausreichende Personalausstattung“ ebenso wichtig für einen erfolgreichen Betrieb, wie z. B. „qualifizierte und motivierte Mitarbeiter“ zu haben, die über eine „breite Fachkompetenz“ verfügen. Als Quintessenz kann daraus abgeleitet werden, dass der Faktor „Verfügbarkeit und Qualifikation der Mitarbeiter“ von großer Wichtigkeit für den Erfolg ist.

Faktor: Akzeptanz durch die Constituency
Der Constituency eines Computer-Notfallteams kommt auch während des Betriebs eine besondere Bedeutung zu. So stuften 71 % die Anforderung, das Vertrauen der Constituency langfristig erwerben zu müssen, als „sehr relevant“ ein. Die restlichen 29 % sahen dies als „relevant“ an. Damit belegt auch diese Aussage in der Bewertung einen ersten Rang. Weiterhin wird auch die Schaffung eines Bewusstseins für Sicherheit und die Arbeit des CERTs bei der Constituency sehr deutlich befürwortet. Zu je 43 % beurteilen die Befragten dies mit „sehr relevant“ und „relevant“. Zudem gaben einige Teams an, ihren Erfolg über Zufriedenheitsmessungen und Feedback von der Constituency zu evaluieren. In diesem Zusammenhang wurde auch das Stichwort „Akzeptanz“ eingebracht. Als aktuelle Schwierigkeiten werden „Vermittlungsprobleme zur Notwendigkeit von CERT-Dienstleistungen in der Constituency“ angegeben. Weiterhin wurden „fehlender Kontakt zur Constituency“, „schlechte Vermittlung der Arbeit an die Constituency“ und „CERT wird falsch verstanden“ als mögliche Hindernisse genannt. Dies deckt sich damit, dass für den Erfolg ein „gutes Standing in der Constituency“ und eine „Sensibilisierung des Kunden“ als wichtig angesehen werden. Nicht zuletzt aus diesen Angaben lässt sich schlussfolgern, dass das Verhältnis zur Constituency ein bedeutsamer Erfolgsfaktor ist.

Faktor: Bedarfsgerechtes Dienstleistungsangebot
Um zu ermitteln, welche Beachtung der Ausgestaltung des Dienstleistungsangebotes entgegengebracht wird, wurden drei unterschiedliche Aussagen formuliert. Als „sehr relevant“ ordneten 57 % der Teilnehmer ein, dass sich das Dienstleistungsangebot an den spezifischen Bedürfnissen der Constituency ausrichten sollte. Weitere 29 % werteten hier mit „relevant“. Damit rangiert diese Aussage im Vergleich mit den anderen an dritter Stelle. Auch die Anforderung, das Dienstleistungsangebot müsse sowohl reaktive als auch präventive Aufgaben beinhalten, sahen je ein Drittel als „sehr relevant“ oder zumindest „relevant“ an. Das Verständnis um die Verbindung zwischen einzelnen Dienstleistungen wird insgesamt von 71 % als „relevant“ angesehen. Damit wird dies zwar nicht unwichtig, hat aber im Vergleich mit anderen Anforderungen auch keine zu hohe Bedeutung. Eine mögliche Hürde für einen erfolgreichen CERT-Betrieb ist ein „fehlender Dienstleistungsgedanke“. Bestätigt wird dies durch Schwierigkeiten, von denen im Rahmen der Befragung berichtet wurde. Demnach stellt die „Anpassung an neue Herausforderungen“ ein aktuelles Problem dar. Das Dienstleistungsangebot muss also ständig auf die Bedürfnisse der Constituency hin überprüft und angeglichen werden. Ein wichtiger Punkt ist damit ein „regelmäßiges Anpassen der Dienste an die Bedürfnisse“. Dem Dienstleistungsangebot eines Computer-Notfallteams sollte als Erfolgsfaktor Beachtung geschenkt werden.

Faktor: Dokumentation von Vorgehensweisen und Richtlinien
Weniger bedeutsam wurde alles in allem die Dokumentation von Vorgehensweisen und Richtlinien eingestuft. Zunächst beurteilen 86 % der Befragten eine grundlegende Dokumentation als „relevant“. Dies beinhaltet aber nicht das Sammeln und Analysieren von Vorfallsdaten zur Planung zukünftiger Vorgehensweisen. Diese Aussage wurde zu 57 % als „wenig relevant“ angesehen und belegt insgesamt den letzten Rang von allen Aussagen. Dass der Constituency klare Anweisungen zur Berichterstattung an die Hand gegeben werden müssen, wurde in den Auswirkungen auf den Erfolg zwar von über zwei Dritteln als mindestens „relevant“ bewertet, dennoch hielt dies auch knapp ein Drittel für „wenig relevant“. Mit dem drittletzten Rang belegt diese Aussage ebenfalls einen der hintersten Plätze. Einige Teams verwenden zwar gesammelte Daten zur Erfolgsmessung, wie z. B. die Anzahl der erfolgreich behandelten Vorfälle. Doch damit kann Erfolg nicht erzeugt, sondern nur belegt werden. Folglich umfasst der Erfolgsfaktor „Dokumentation von Vorgehensweisen und Richtlinien“ nicht die Aspekte „Sammeln von Daten“ und „Richtlinien zur Berichterstattung“. Seine Gültigkeit beschränkt sich damit auf die Zusammenstellung von Handlungsanweisungen und Regelungen.

Faktor: Vorhandensein einer Informationspolitik
Abschließend wurden die Teilnehmer auch hinsichtlich der Ausgestaltung einer Informationspolitik befragt. Als mindestens „relevant“ sahen 86 % einen durch eine umfassende Informationspolitik geregelten Informationsfluss an. Nur 14 % hielten dies für „wenig relevant“. Als wichtige Punkte für den erfolgreichen Betrieb eines CERT wurden eine „offene Kommunikation“ und „Kommunikationsstrukturen müssen stehen“ aufgezählt. Dies kann ein Hinweis dafür sein, dass die Ausgestaltung einer Informationspolitik besonders auf das Vorhandensein von sicheren Kommunikationskanälen hinarbeiten sollte. Insbesondere bei Kooperationen müssen vertrauensvoll und ungehindert Informationen ausgetauscht werden können. Der Erfolgsfaktor „Vorhandensein einer Informationspolitik“ ist daher besonders unter diesen Gesichtspunkten zu betrachten.

5.3 Zwischenfazit

Obwohl im Rahmen der Befragung alle vorgestellten Erfolgsfaktoren in ihrer Gültigkeit bestätigt wurden, konnten an einigen Stellen leicht verschobene Schwerpunkte ausgemacht werden, auf die besonders geachtet werden sollte:

- Bei der Einführung eines neuen CERTs spielt den Ergebnissen zufolge die Dauer des Aufbaus eine unbedeutende Rolle.
- In der Betriebsphase ist zudem eher von einer Zusammenarbeit zwischen den Teams als nur der Unterstützung durch andere auszugehen.
- Die Dokumentation umfasst vornehmlich die Erfassung von Vorgehensweisen und Regelungen, nicht jedoch das Sammeln von Daten oder ähnlichem.
- Aus der Befragung ging auch hervor, dass der Erfolgsfaktor „Vorhandensein einer Informationspolitik“ besonders im Hinblick auf sichere Kommunikationstechniken gesehen werden muss.

Die Deutlichkeit der Befragungsergebnisse ist nicht von der Hand zu weisen, da sie die Hypothesen hinsichtlich potenzieller Erfolgsfaktoren bei Aufbau und Betrieb eines CERTs stützen. Trotzdem soll an dieser Stelle ausdrücklich darauf hingewiesen werden, dass nur wenige Teams in Deutschland befragt werden konnten. Daher führt die geringe Teilnehmerzahl dazu, dass die Ergebnisse nicht statistisch repräsentativ sind. Es zeigt jedoch insgesamt, dass der richtige Weg eingeschlagen wurde, welcher als Fundament für weitere Forschungsarbeit dienen kann.

6 CERT des Landes Niedersachsen

6.1 Rahmenbedingungen in Niedersachsen als Voraussetzung für Aufbau und Betrieb eines CERTs

6.1.1 Lage der Organisationsstruktur für IT-Sicherheit in Niedersachsen

Das Bundesinnenministerium stellte 2005 den „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ (NPSI) vor. Dieser verfolgt im Wesentlichen drei Kernziele: angemessene Absicherung von IT-Infrastrukturen (**Prävention**), wirkungsvolle Behandlung von IT-Sicherheitsvorfällen (**Reaktion**) und die Stärkung deutscher Kompetenzen in der Hinsicht auf IT-Sicherheit (**Nachhaltigkeit**). Darin wird bei der Reaktion auf Vorfälle vor allem auch eine Zusammenarbeit von Bund und Ländern auf verschiedenen Ebenen und das Vorhandensein zweckmäßiger Schnittstellen für ein umfassendes Krisenmanagement gefordert.

Die aktuelle Situation in der niedersächsischen Landesverwaltung lässt sich im Hinblick auf eine Organisationsstruktur für IT-Sicherheit wie folgt beschreiben. In Niedersachsen gilt, wie in jedem anderen Bundesland und bei der Bundesverwaltung auch, das „Ressortprinzip“. Dieses bedeutet, dass alle Ressorts die Verantwortung für den eigenen Geschäftsbereich tragen und eigene Entscheidungen treffen können. Geführt hat dieses in der Vergangenheit zu heterogenen Strukturen bei der IT-Organisation und der IT-Landschaft. Eine durchgängige Organisationsstruktur für IT-Sicherheit ist bisher nur bei der Polizei vorhanden. Diese verfügt auch über ein eigenständiges Sicherheitsteam. Einen hauptamtlichen IT-Sicherheitsbeauftragten gibt es in Niedersachsen bisher nur bei der Polizei sowie beim zentralen IT-Dienstleister des Landes, dem Informatikzentrum Niedersachsen (izn). Letzterer ist auf Ebene einer Stabstelle bei der Geschäftsleitung des izn angesiedelt.

Insgesamt verfügt die Landesverwaltung bisher also nicht über eine etablierte und durchgängige Organisationsstruktur für IT-Sicherheit. Es fehlt ein (ressortübergreifendes) IT-Notfall- oder IT-Krisenmanagement. Deshalb findet derzeit bei IT-Vorfällen keine ressortübergreifende und zentral koordinierte Prävention hinsichtlich IT-Sicherheit statt. Entsprechendes gilt bei der Reaktion auf IT-Sicherheitsvorfälle. Eine zentrale Koordination von IT-Vorfällen innerhalb eines Geschäftsbereiches ist nur bei der Polizei vorhanden. Unter anderem für diesen Zweck verfügt das Polizeiamt für Technik und Beschaffung über ein zentrales IT-Sicherheitsmanagement. Ziel dieses IT-Sicherheitsmanagements ist es, die polizeieigenen Geschäftsprozesse vor IT-Sicherheitsvorfällen angemessen zu schützen, auf IT-Notfälle vorbereitet zu sein sowie bei Vorfällen geplant und zielgerichtet vorzugehen.

Mit Ausnahme der Polizei finden in anderen Behörden der Landesverwaltung bisher kaum Sensibilisierungs- oder Weiterbildungsmaßnahmen für Führungskräfte und Mitarbeiter zum Thema IT-Sicherheit statt. Keine Stelle in der Landesverwaltung kann eine verifizierbare Aussage über die aktuelle Gefährdung der IT-unterstützten Geschäftsprozesse oder aktuelle IT-Sicherheitslücken bei eingesetzten IT treffen. Das stets vorhandene Restrisiko bei der Anwendung von IT in den Geschäftsprozessen ist in den meisten Fällen unbekannt. Es stehen global weder verifizierbare Informationen über bereits aufgetretene IT-Sicherheitsvorfälle noch über eingetretene Schäden oder die Wirtschaftlichkeit der eingesetzten Ressourcen für IT-Sicherheit zur Verfügung. Keine autorisierte Stelle in der Landesverwaltung verfügt über einen Gesamtstatus zur IT-Sicherheitslage im eigenen Bereich, oder bei den Partnern außerhalb der Landesverwaltung (andere Verwaltungen, Geschäftspartner).

Obige Ausführungen gelten, wie schon erwähnt, im Wesentlichen nicht für den Bereich der niedersächsischen Polizei. Aufgrund von Vorgaben des Bundes ist die Polizei seit einigen Jahren dabei ein IT-Sicherheitsmanagement aufzubauen, die erforderlichen organisatori-

schen Strukturen und Abläufe zu schaffen sowie ihre IT-unterstützten Geschäftsprozesse durch zwei andere Länderpolizeien auditieren zu lassen. Dabei wurden bereits beachtliche Erfolge erzielt. Dennoch fehlt auch hier die erforderliche Verbindung zu den anderen Ressorts und dem Informatikzentrum Niedersachsen, denn ein Sicherheitsvorfall kennt meist keine Verwaltungsgrenzen.

Die niedersächsische Landesverwaltung ist seit Ende 2005 dabei, ihren IT-Einsatz strategisch neu auszurichten und strebt sowohl eine Zentralisierung der IT-Ressourcen als auch eine Standardisierung benötigter Hard- und Software an. Ziel des IT-Landeskonzeptes ist es, den IT-Einsatz wirtschaftlicher und effizienter zu gestalten. Im zehnten Leitsatz des IT-Landeskonzeptes wird auf die Wichtigkeit der Informationssicherheit für die Geschäftsprozesse eingegangen. Es wird klar gestellt, dass trotz Zentralisierung von Teilen der IT (einschließlich Personal) die Gesamtverantwortung für Informationssicherheit in den Ressorts, also bei den „Eigentümern“ der Geschäftsprozesse verbleibt. Im vierten Quartal 2004 bzw. ersten Quartal 2005 hat das Zentrale IT-Management der Landesverwaltung, unter Mitwirkung aller Ressorts sowie weiterer Dienststellen, strategische Ziele und Prinzipien für Informationssicherheit definiert und diese in einem Entwurf für eine „IT-Sicherheitsleitlinie“ festgehalten (Abb. 6). Dieser erste Entwurf wurde im zweiten Quartal 2006 an die Ziele des zwischenzeitlich verabschiedeten IT-Landeskonzeptes angepasst sowie mit den Aussagen des NPSI und den im Januar 2006 veröffentlichten neuen BSI-Standards 100-1 (Managementsysteme für Informationssicherheit) und 100-2 (IT-Grundschutzvorgehensweise) synchronisiert. Dieses kommt äußerlich in der neuen Bezeichnung „Leitlinie für Informationssicherheit in der Landesverwaltung“ zum Ausdruck. Die Umsetzung der mit Absicht recht allgemein gehaltenen Leitlinie wird durch daraus abgeleiteten Sicherheitsrichtlinien sach- und zielgruppenorientiert weiter konkretisiert. Die Richtlinien machen ressortübergreifende Vorgaben, in welchem Rahmen eine Umsetzung der strategischen Ziele und Prinzipien für Informationssicherheit vorzunehmen ist.

Die taktischen Vorgaben für die Umsetzung von Maßnahmen finden sich wieder in folgenden Dokumenten:

- „Richtlinie für Informationssicherheit in der Landesverwaltung“ (RL IS)
- „Richtlinie für die Organisationsstruktur für Informationssicherheit“ (RL IS Orga)
- „Richtlinie für die Dokumentation für Informationssicherheit“ (RL IS Doku)

Die tatsächliche Umsetzung der Ziele der Leitlinie und der Vorgaben aus den Richtlinien erfolgt schließlich auf operativer Ebene in den einzelnen Ressorts sowie dem Informatikzentrum Niedersachsen. Zu unterscheiden ist dabei die Umsetzung von Maßnahmen in den Geschäftsprozessen der Behörden aufgrund von Fachkonzepten sowie deren technische Realisierung beim izn mittels technischer Konzepte für die IT-unterstützten Geschäftsprozesse. Dabei wird sich die Landesverwaltung zukünftig ressortübergreifend allgemeiner Standards (BSI, ISO) und „Best Practices“ bedienen. Bezüglich der effizienten Organisation des IT-Betriebes in einzelnen Ressorts sowie beim Informatikzentrum Niedersachsen wird bereits jetzt schon auf die Vorgehensweisen des IT Service-Managements (ITSM) nach der IT Infrastructure Library (ITIL) zurückgegriffen.

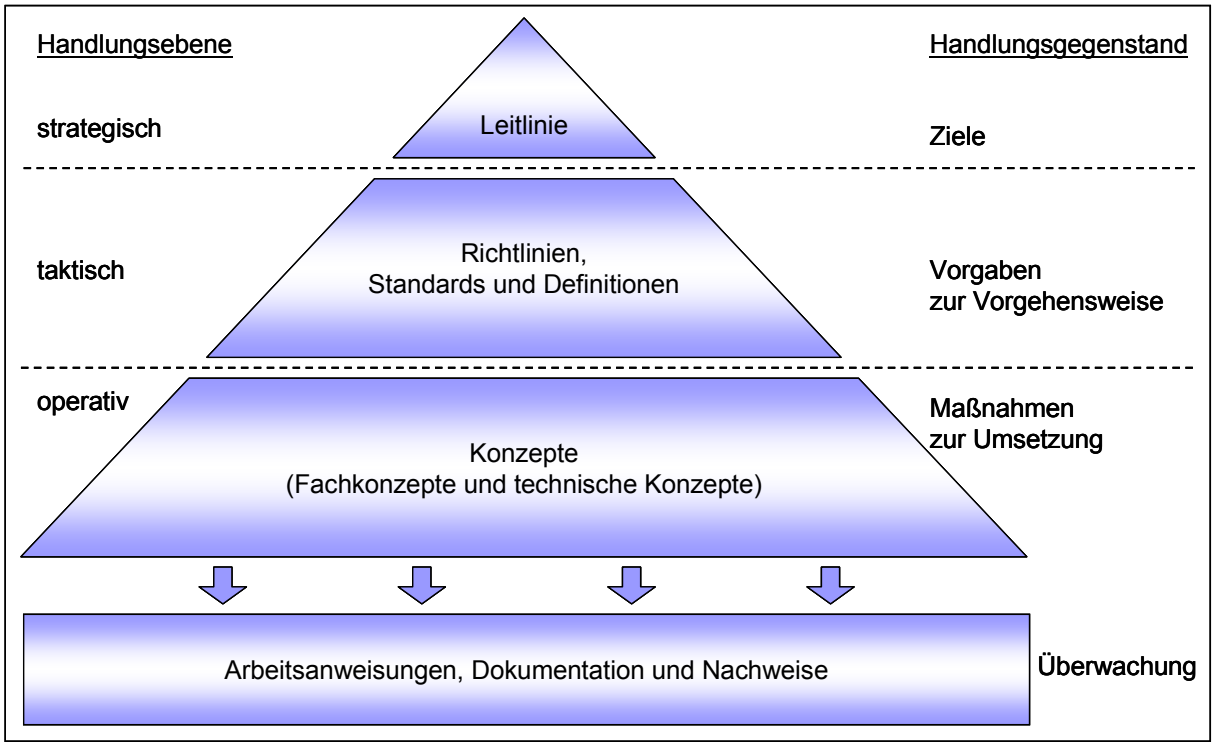

Abb. 6: Organisation von IT-Sicherheitsdokumenten in Niedersachsen [41]

Im Rahmen der strategischen Neuausrichtung der IT in der niedersächsischen Landesverwaltung wird auch die Struktur des IT-Managements weiter optimiert. Bisher wurden IT-bezogene Querschnittsthemen beim Zentralen IT-Management (ZIM) im Ministerium für Inneres und Sport unter starkem Einfluss der Ressorts (Ressorthoheit) koordiniert. Im Januar 2006 wurde ein IT-Bevollmächtigter in Form eines CIO („Chief Information Officer“) bestellt. Dieser kann als „oberster Stratege“ für Informationsverarbeitung angesehen werden und verfügt zur Wahrnehmung seiner Aufgaben über ein entsprechendes politisches Mandat (z. B. Festlegung der IT-Strategie, IT-Controlling oder Mitsprache beim IT-Budget). Die einzelnen Ressorts werden weiterhin die Verantwortung für die eigenen ressortspezifischen Fachverfahren tragen.

Bisher bestehen die Leitlinie sowie die Richtlinien für Informationssicherheit in der niedersächsischen Landesverwaltung nur im Entwurf. Ein Kabinettsbeschluss zu deren verbindlichen Einführung ist für Ende 2006 geplant. Bei den bisher im Entwurf vorliegenden oder noch in Bearbeitung befindlichen Dokumenten zur Informationssicherheit handelt es sich momentan also nur um Visionen und Arbeitsergebnisse aus verschiedenen Projekten des zentralen IT-Managements.

Die Leitlinie geht aus dem Projekt „IT-Sicherheit in der Landesverwaltung“ (ITS Land) hervor, welches hauptsächlich im vierten Quartal 2004 unter Beteiligung aller Ressorts stattfand und im ersten Quartal 2005 abgeschlossen wurde. Die bisher nicht in Kraft gesetzte Leitlinie wurde im zweiten Quartal 2006 aufgrund geänderter Rahmenbedingungen fortgeschrieben. Im Februar 2005 startete das Projekt „IT-Sicherheit in der niedersächsischen Justiz“ (ITS Justiz). Bei diesem Projekt, unter Federführung des zentralen IT-Managements der Landesverwaltung, wurde im ersten Schritt für die Justiz eine ressortspezifische IT-Sicherheitsrichtlinie entwickelt. Dieses Dokument wurde in einem zweiten Schritt erfolgreich durch Konsolidierung und Abstraktion in eine ressortübergreifende Sicherheitsrichtlinie für das Land transformiert. Im gleichen Projekt wurde die erste Fassung einer Organisationsrichtlinie entwickelt,

[41] Quelle: Projekte „CERT Niedersachsen“ und „ITS Doku“ [2005/2006]; Dipl.-Ing. (FH) Claus Irion

welche die Organisationsstruktur für IT-Sicherheit aus Ressortsicht sowie Verantwortlichkeiten und Rollen für IT-Sicherheit in der Landesverwaltung beschreibt. Dieses Dokument befindet sich derzeit in der Fertigstellung. Aus dem im Abschluss befindlichen Projekt „ITS Justiz“ wurde schließlich die Konzipierung eines CERT-Niedersachsen (CERT NDS) als eigenständiges Projekt ausgegliedert, da dieses Thema bei Projektbeginn noch nicht erkannt war und den Projektrahmen gesprengt hätte. Das Projekt „CERT-Niedersachsen“ (CERT NDS) ist Gegenstand der weiteren Betrachtungen.

6.1.2 CERT-Projekt zur Bedarfsermittlung (Projektauftrag)

Im September 2005 startete planmäßig das Projekt „CERT Niedersachsen“ unter Federführung des Zentralen IT-Managements. Das Projektteam setzte sich aus Vertretern der Polizei, der Steuerverwaltung, der Agrarverwaltung, der Universität Hannover und des Informatikzentrum Niedersachsen zusammen. Verstärkt wurde das Team durch die Fachkompetenz des DFN-CERT.

Aus dem Projektauftrag zum „CERT-Niedersachsen“ vom September 2005 geht hervor, dass das Projektziel zunächst in einer Bedarfsermittlung lag. Es sollte vorab untersucht werden, wie die Notwendigkeit und die Erfordernis eines landeseigenen Computer-Notfallteams einzuschätzen ist. In diesem Rahmen sah der Auftrag auch eine Klärung der Nutzungsmöglichkeiten im Hinblick auf ein Angebot interner und externer CERT-Dienstleistungen vor. Dieses sollte besonders unter Berücksichtigung einer zukünftigen landesweiten Organisationsstruktur für IT-Sicherheit untersucht werden.

Das Projekt gliederte sich in zwei Phasen. Die erste Phase begann im September 2005 und endete im Januar 2006 mit einem Zwischenbericht. Schwerpunkt der ersten Phase war die grundlegende Klärung, ob das Land Niedersachsen überhaupt ein eigenes Computer-Notfallteam benötigt, welche Kernfunktionen es haben und welchen Zielgruppen es zur Verfügung gestellt werden könnte. Damit einhergehend wurde auch erarbeitet, welches CERT-Organisationsmodell sich grundsätzlich zur Umsetzung anbietet. Dieses ist besonders wichtig zur Ermittlung des erforderlichen Ressourcenbedarfes. Mit den Arbeiten der zweiten Phase wurde im Anschluss an den Zwischenbericht begonnen, nachdem die Frage nach der Notwendigkeit und der Umsetzbarkeit eines CERT-Niedersachsen positiv beschieden wurde. Das Projekt „CERT Niedersachsen“ endete im Juni 2006 mit einem Abschlussbericht.

6.1.3 Abschlussbericht des CERT-Projektes

Die Arbeitsergebnisse der ersten Projektphase werden in Abschlussbericht zusammengefasst. Dieser beschreibt ein grobes Konzept für das zukünftige CERT-Niedersachsen und folgt dabei den Ausführungen zum Grundgerüst eines Computer-Notfallteams. Für den gesamten Aufbau bis zur Betriebsbereitschaft wird mit einem zeitlichen Umfang von mindestens drei Jahren gerechnet. Im Folgenden werden kurz die Ergebnisse präsentiert, welche für den weiteren Fortgang dieser Arbeit relevant und besonders für die abschließenden Empfehlungen von Bedeutung sind.

Constituency

Aus dem Bericht geht hervor, dass die Constituency des CERT-Niedersachsen in drei Klassen zu unterteilen ist. Am wichtigsten für das Team ist die primäre Constituency, der die gesamte niedersächsische Landesverwaltung zugeordnet wird. Das spätere Dienstleistungsangebot des Computer-Notfallteams wird sich in erster Linie an den Bedürfnissen dieser Gruppe auszurichten haben. Ebenfalls von großer Bedeutung sind die für die IT-Infrastruktur des Landes wichtigen IT-Dienstleister (z. B. Rechenzentren). Diese werden somit gleichfalls zu den „Hauptkunden“ gezählt. Zweitrangig sind dagegen alle nur indirekt betroffenen Verwaltungen, z. B. die einzelnen Kommunen des Landes, Behörden anderer Bundesländer oder des Bundes. Aufgrund unmittelbarer Abhängigkeiten im Zusammenhang mit Schnittstellen

und technischen Aspekten ist eine übergreifende Zusammenarbeit unumgänglich. Dies trifft auch auf andere, vor allem in Deutschland operierende Computer-Notfallteams zu. An dritter Stelle stehen schließlich alle weiteren Organisationen und Nutzer, die z. B. durch die Teilnahme an elektronischen Verwaltungsverfahren (eGovernment) mit der IT des Landes in Berührung kommen. In Notfällen stellt das CERT-Niedersachsen auch für diese einen Ansprechpartner dar und muss auf Anfragen aus dieser Gruppe vorbereitet sein.

Organisationsmodell (Betriebsmodell)
Für das niedersächsische Computer-Notfallteam wird im Bericht ein kombiniertes Team (vgl. dazu S. 16f.) empfohlen. Aufgrund der Eigenständigkeit der einzelnen Ressorts sowie der sehr unterschiedlichen (kritischen) Geschäftsprozesse kann ein CERT-Niedersachsen nicht allein durch ein zentrales Team betreut werden. Darüber hinaus erschwert die Größe der Landesverwaltung und deren geographische Verteilung auf viele Behördenstandorte eine flächendeckende Vor-Ort-Betreuung. Diese würde sich unnötig kostenintensiv gestalten und wäre auch wirtschaftlich kaum zu rechtfertigen. Aus diesem Grund ist eine Integration bestehender Sicherheitsteams in den einzelnen Ressorts zur dezentralen Erbringung von CERT-Dienstleistungen in Verbindung mit der Koordination durch zentral angeordnete CERT-Komponenten vorgesehen (vgl. dazu auch Abb. 7 auf S. 47).

Dienstleistungen
Die anzubietenden Dienstleistungen werden im Rahmen der Voruntersuchung in drei Kategorien unterteilt. So fallen zunächst zentrale Basisdienstleistungen an, die vorwiegend dem Aufbau von Organisationsstrukturen dienen und Kontakte zur Constituency herstellen sollen. Dazu zählt z. B. die Bekanntmachung des CERTs gegenüber der Constituency durch Veranstaltungen und Rundschreiben, der Aufbau einer technischen Infrastruktur zur Gewährleistung einer sicheren Kommunikation, die Einführung eines sicheren Vorfallsberarbeitungssystems und eines internen Expertenverzeichnisses. Diese Gruppe von Dienstleistungen wird ohne Beteiligung externer Dienstleister erbracht, stellt insgesamt jedoch nur einen Teil der mindestens erforderlichen Aufgaben eines Computer-Notfallteams dar. Gemäß den Ausführungen des Abschlussberichtes fallen weitere darauf aufbauende Dienstleistungen an. Diese werden als erweiterte Basisleistungen bezeichnet und umfassen vor allem reaktiv geprägte Maßnahmen zur Bewältigung von IT-Sicherheitsvorfällen. Die erweiterten Basisleistungen können teilweise durch Outsourcing an externe Dienstleister sichergestellt werden und enthalten z. B. die frühzeitige Warnung und Alarmierung bei Gefährdungen, die direkte Unterstützung und Reaktion auf Vorfälle, die Bearbeitung von sicherheitsbezogenen Anfragen, die Identifikation von Schwachstellen sowie gleichermaßen Weiterbildungsmaßnahmen zum Thema Vorfallsbearbeitung. Folglich sind Aufgaben aller drei Dienstleistungskategorien (Reaktion, Prävention, Nachhaltigkeit) enthalten. Darauf bauen schließlich verschiedene individuelle Zusatzleistungen auf, die für ein minimales CERT als nicht erforderlich angesehen und daher auch nicht näher im Abschlussbericht erläutert werden. Diese können später je nach Bedarf modular in das Dienstleistungsangebot eingepasst werden.

Finanzierung
Zur Finanzierung werden die angebotenen Dienstleistungen danach unterschieden, ob sie sich an die Gemeinschaft der Constituency richten (Basisleistungen) oder direkt für einzelne Kunden erbracht werden (individuelle Zusatzleistungen). Kann eine Leistung nicht zu einem alleinigen Nutznießer zugeordnet werden, wird eine genaue Abrechnung schwierig. Daher wird im Bericht eine zentrale Finanzierung für die Basisleistungen vorgeschlagen, die von der Netzzugehörigkeit der Benutzer abhängen soll. Die Zusatzleistungen lassen sich dem jeweiligen Kunden unmittelbar zuordnen und werden demnach gesondert in Rechnung gestellt.

Des Weiteren listet der Abschlussbericht einige Punkte auf, die schon vorab als mögliche Kostenquellen identifiziert werden können. Dies sind z. B. Personalkosten für zentrale und

dezentrale CERT-Mitarbeiter, Infrastrukturkosten zum Aufbau und Erhalt des Teams oder Kosten für den Einsatz externer CERT-Dienstleister. Dazu zählen jedoch auch Aufwendungen zur Erstellung eines Informationsportals in Landesintranet bzw. Internet, Aus- und Weiterbildungskosten zur Qualifizierung der Mitarbeiter und Kosten im Rahmen der Teilnahme an Veranstaltungen des CERT-Verbundes. Der genaue Umfang der Kosten steht jedoch erst nach einer genaueren Planung fest, weshalb der Bericht an dieser Stelle keine Zahlen nennen kann.

Autorität

Der Bericht macht keine konkrete Aussage darüber, in welchem Umfang die Befugnisse des Computer-Notfallteams ausgestaltet werden sollen. So geht daraus hervor, dass zunächst vor allem die Leistungen des Teams von großer Bedeutung sind. Je erfolgreicher es ist, desto mehr Kompetenzen wird die Constituency hier erkennen und die Empfehlungen des CERTs akzeptieren und umsetzen. Es wird allerdings auch deutlich gemacht, dass eine gewisse Autorität und Entscheidungsbefugnis zur Erreichung höherer Sicherheitsziele erforderlich sein wird. Die genaue Ausgestaltung der CERT-Autorität ist von den politischen Entscheidungsträgern aufgrund ihrer Gesamtverantwortung für das Risikomanagement abhängig zu machen und wird im Folgenden nicht weiter erläutert.

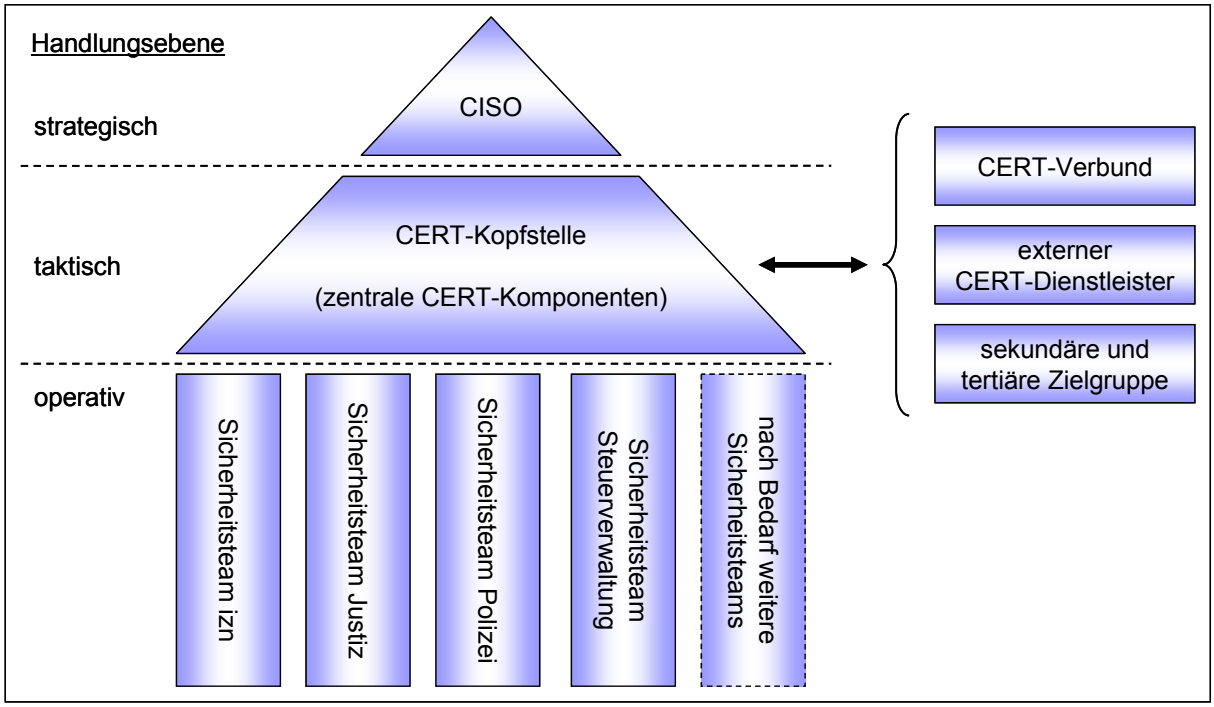

Abb. 7: Organisationsstruktur des CERT Niedersachsen (Rollen) [42]

Aus Abb. 7 geht die Empfehlung des Projektberichtes hervor, das Computer-Notfallteam organisatorisch direkt einem CISO (Chief Information Security Officer) zu unterstellen, solange dieser nicht vorhanden ist, soll der „IT-Bevollmächtigte“ (CIO) trotz Rollenkonflikt diese Rolle mit übernehmen. Folglich wird daher dessen konkrete Unterstützung von essenzieller Bedeutung für das Team sein. Auf taktischer Ebene übernimmt die CERT-Kopfstelle als zentraler Ansprechpartner und Repräsentant des Teams auch die Aufgabe, den Kontakt mit der Außenwelt zu halten (z. B. CERT-Verbund, externe Dienstleister, Geschäftspartner). Hier ist der Einsatz eines qualifizierten und belastbaren CERT-Managers bzw. Teamleiters von großer Wichtigkeit. Dieser hat den Einsatz der dezentral angeordneten CERT-Mitglieder zu koordinieren, welche im Rahmen bisher bestehender Sicherheitsteams einzelner Ressorts ope-

[42] Quelle: Projekt „CERT Niedersachsen“ [2006]; Dr. K.-P. Kossakowski, Dipl.-Ing. (FH) Claus Irion

rativ weiterhin vor Ort tätig werden. Dies zeigt auch Abb. 8 auf S. 48. Auf strategischer Ebene steht der CISO in Verbindung mit der Pressestelle (PR) und stimmt die Sicherheitsstrategie des Landes mit den IT-Verantwortlichen der einzelnen Ressorts im Koordinierungsausschuss IT (KA-IT) ab. In diesem Ausschuss ist auch der Landesbeauftragte für den Datenschutz (LfD) vertreten. Es findet auf strategisch/taktischer Ebene eine Abstimmung zwischen dem CISO und dem IT-Sicherheitsmanagement Team (IT-SiMa Team) statt. Der CISO leitet diesen Abstimmungskreis, welchem primär die obersten IT-Sicherheitsbeauftragten der Ressorts und ein Vertreter des LfD angehören.

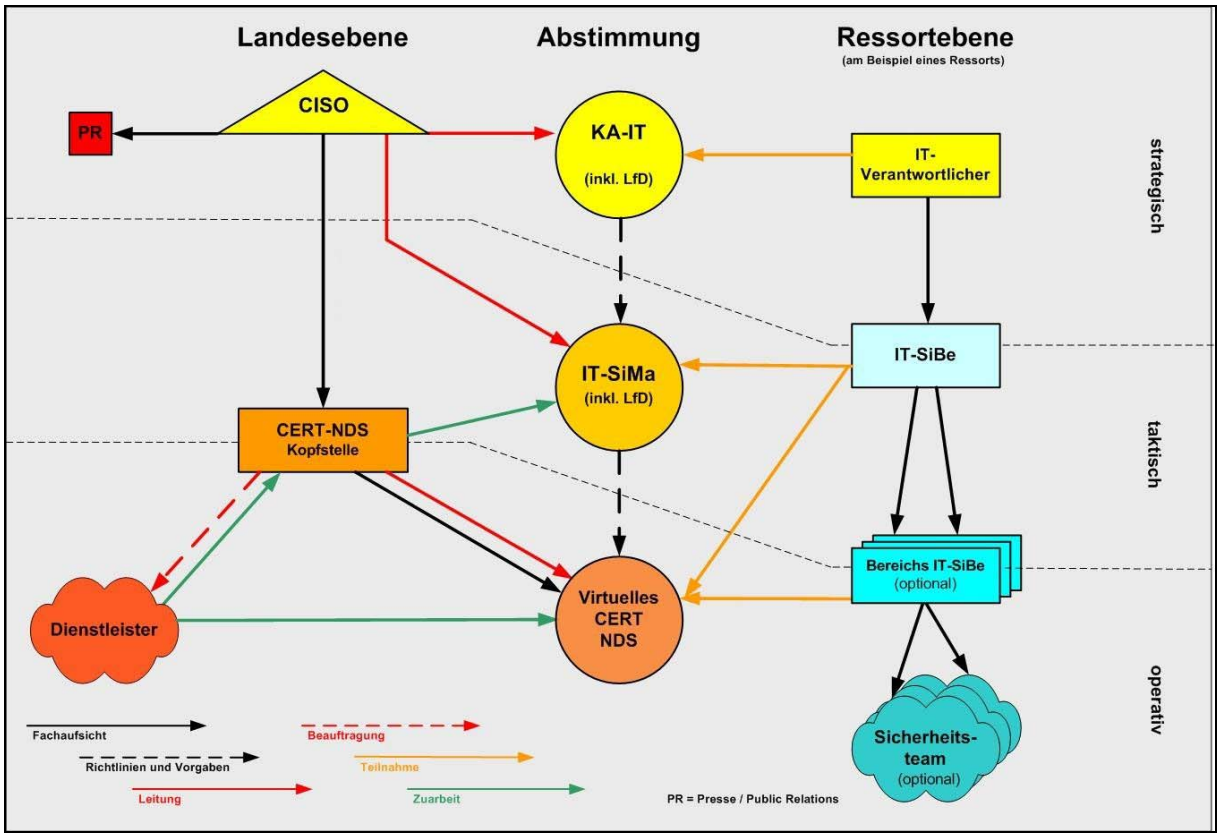

Abb. 8: Detaillierte Organisationsstruktur eines CERT Niedersachsen (Rollen) [43]

Operativ untersteht das virtuelle CERT der CERT-Kopfstelle, die bei Bedarf externe CERT-Dienstleister zur Unterstützung (Fachexpertise, Arbeitsspitzen) beauftragen kann. Dem virtuellen CERT-Niedersachsen (CERT-NDS) gehören (wenn vorhanden) sowohl die IT-Sicherheitsbeauftragten der einzelnen Bereiche der Ressorts als auch bestehende Sicherheitsteams an. Diese Sicherheitsteams verbleiben in ihren jeweiligen Bereichen und sind vertraut mit den angewendeten Systemen und Fachverfahren (vgl. „Werksfeuerwehr“).

6.2 Kritische Bewertung der Erfolgschancen des CERT-Niedersachsen

Im Folgenden wird vorweg eine differenzierte Betrachtung einiger möglicher Kritikpunkte und Erfolgsaussichten zum CERT-Niedersachsen gegeben, bevor im Anschluss daran die Erfolgsfaktoren auf die Situation in Niedersachsen herunter gebrochen und daraus Gestaltungsempfehlungen abgeleitet werden. Wie schon im vorigen Abschnitt mehrfach angedeutet wurde, sind bisher keine bindenden Entscheidungen über die dargestellten Kernpunkte gefällt worden. Da die konkrete inhaltliche Ausgestaltung des CERT-Niedersachsen zudem erst

[43] Quelle: Projekt „CERT Niedersachsen“ [2006]; Dr. K.-P. Kossakowski, Dipl.-Ing. (FH) Claus Irion

in den nächsten drei Jahren vorgenommen wird, können in diesem frühen Stadium keine verbindlichen Aussagen formuliert werden.

Ein Computer-Notfallteam ist als operativer Bestandteil einer durchgängigen Organisationsstruktur für IT-Sicherheit anzusehen. In diesem Zusammenhang kann argumentiert werden, dass jeder hierbei getätigte Aufwand gerechtfertigt ist, solange ihm ein akzeptabler Nutzen gegenübersteht. Aufgrund des immer stärkeren Einsatzes von Informationstechnologien in den Geschäftsprozessen und einer zunehmenden Bedrohung durch Sicherheitslücken und Angreifer besteht gerade bei kritischen Geschäftsprozessen der Bedarf an einem hohen IT-Sicherheitsniveau. IT-Sicherheit kann niemals vollständig gewährleistet werden und ist deshalb als fortlaufender Prozess zur Anpassung und Verbesserung von organisatorischen und technischen Sicherheitsmaßnahmen zu sehen. Dieses beinhaltet daher auch die Konzentration von Fachkompetenzen in Form einer respektierten Gruppe von Spezialisten mit dem erforderlichen Kenntnissen zu den kritischen Geschäftsprozessen (vertraulich bis geheim), zur Bewältigung von eingetretenen IT-Sicherheitsvorfällen (Schadensminimierung) oder zur frühzeitigen Erkennung möglicher Bedrohungen (Schadensabwehr). Nur so können effektiv Schäden begrenzt oder gar vollständig verhindert werden. Dazu müsste ein CERT insgesamt, wie vorgesehen, in die vorhandenen Strukturen und Prozesse der niedersächsischen Landesverwaltung, insbesondere der Organisationsstruktur für IT-Sicherheit, integriert werden und sollte nach Möglichkeit auf bestehende Einrichtungen zurückgreifen können. Der Erfolg hängt daher besonders von den Ergebnissen des Folgeprojektes ab, sofern es zur Realisierung kommt. Zu diesem Zeitpunkt ist noch nicht bekannt, ob und wie die (politische) Entscheidung für den Aufbau eines CERTs ausfallen wird. Grundsätzlich wäre ein Beschluss zu Gunsten des Computer-Notfallteams jedoch als positiv zu bewerten.

Zwischen einem kommerziellen oder unternehmensinternen CERT und einem Computer-Notfallteam für eine öffentliche Verwaltung gibt es Unterschiede. Aufgrund des in den Behörden vorherrschenden Ressortprinzips hängt die Entscheidungsbildung in einer öffentlichen Verwaltung häufig von verschiedenen Stellen ab und kann daher bis zu einem endgültigen Ergebnis mehr Zeit beanspruchen, als dies z. B. ökonomisch sinnvoll ist. Abgesehen von wirtschaftlichen Gesichtspunkten oder der Erfordernis eines Computer-Notfallteams sind die politische Rückendeckung und die deutliche Entscheidung für ein CERT-Niedersachsen unabdingbar. Dies ist aber auch kritisch zu sehen, da der Aufbau des Teams letztendlich von politischen Gemeinschaftsentscheidungen abhängig gemacht wird und somit einer Vielzahl von Hindernissen oder Störfaktoren ausgesetzt sein kann. So könnte vor allem unter Kostengesichtspunkten mit einer engen Haushaltslage in Niedersachsen und dem Sparkurs der Landesregierung gegen ein CERT argumentiert werden. Durch die Bündelung bestehender Kompetenzen für IT-Sicherheit und der Nutzung von Synergieeffekten sollen insgesamt Ressourcen eingespart werden. Es ist jedoch kaum abschätzbar, ob sich z. B. die Betriebskosten des geplanten Computer-Notfallteams allein mit diesen Einsparungen begleichen lassen. Gerade im Anfangsstadium wird ein Outsourcing möglicher Dienstleistungen beabsichtigt, welches zumindest vorübergehend Mehrkosten mit sich bringen wird und besonders in Zeiten mit angespannter Haushaltslage auf keine Befürwortung stoßen könnte. Solange die Notwendigkeit und der langfristige, wirtschaftliche Nutzen eines CERTs durch Schadensabwehr den Zielgruppen nicht vermittelt werden kann sowie keine politische Rückendeckung vorhanden ist, ist ein Scheitern des gesamten Vorhabens CERT-Niedersachsen vorprogrammiert.

Entscheidungen zur Aufstellung eines CERT wurden bereits in anderen Bundesländern (z. B. Bayern oder Nordrhein-Westfalen) herbeigeführt, wo die Teams mit Erfolg aufgebaut werden konnten. Hier könnte sich besonders ein Blick auf das bayerische CERT anbieten, welches aufgrund seiner organisatorischen Anbindung an das dortige Staatsministerium für Inneres dem Konzept aus Niedersachsen recht ähnlich ist.

Neben den Entscheidungen auf politischer Ebene ist auch das spätere Verhalten einer Constituency nur schwer berechenbar und könnte ebenfalls als problematisch angesehen werden. Das Vertrauen und die Akzeptanz durch die Constituency sind zweifelsfrei unerlässlich für die Arbeit eines Computer-Notfallteams. Selbst wenn sich die Landesverwaltung für ein CERT entscheidet, bedeutet dies nicht gleichzeitig die Unterstützung durch die betreute Zielgruppe. Die primäre Constituency besteht jedoch gänzlich aus Teilen der Landesverwaltung und könnte letztendlich durch Anordnung von oben zur Kooperation angetrieben werden. Der geplante Aufbau als dezentrales „virtuelles“ Team erleichtert sicherlich die Integration des CERTs in die alltäglichen Abläufe (Geschäftsprozesse, IT-Betrieb) und bewirkt eine „fühlbare“ Nähe zur Constituency auf beiden Seiten.

Trotz vorstellbarer Hindernisse bietet das niedersächsische CERT-Konzept zum aktuellen Zeitpunkt und mit den bislang vorliegenden Informationen insgesamt chancenreiche Aussichten. Unter der Voraussetzung, dass wirklich eine (politische) Entscheidung zugunsten des Aufbaus getätigt wird, sind keine unlösbaren Schwierigkeiten oder schwerwiegenden Schranken für das niedersächsische Computer-Notfallteam zu erkennen. Dass der Weg bis zu einem akzeptablen Gesamtergebnis mühsam werden kann und mit einem hohen Arbeitsaufkommen sowie Kräfte zehrenden Anstrengungen zusammenhängt, ist nicht auszuschließen.

6.3 Erkenntnisse und Gestaltungsempfehlungen für das CERT-Niedersachsen

Der tatsächliche Aufbau, die Pilotierung und der sukzessive Übergang des CERT in den Wirkbetrieb soll im Rahmen eines dreiphasigen Projektes innerhalb von drei Jahren erfolgen. Dabei überlappen sich die Phasen teilweise. Alle nachfolgenden Empfehlungen werden daher unter der Prämisse formuliert, dass sich die Landesverwaltung tatsächlich für den Aufbau eines CERT-Niedersachsen ausspricht und dieses nach den Inhalten des Projektberichtes realisiert.

6.3.1 Empfehlungen für einen erfolgreichen Aufbau

Im Folgenden werden zu jedem Erfolgsfaktor richtungweisende Überlegungen und Erkenntnisse zusammengetragen und dann jeweils mit einer Empfehlung abgeschlossen.

Faktor: Unterstützung durch das Management
Die Unterstützung durch das verantwortliche „Management“ sicherzustellen umfasst in einem CERT für eine öffentliche Verwaltung andere Aspekte, als dies bei einem kommerziellen CERT-Dienstleister oder einem unternehmensinternen CERT der Fall ist. Da in einer öffentlichen Verwaltung viele verschiedene Stellen an der Entscheidungsbildung beteiligt sind, steht die Erzeugung einer generellen politischen Rückendeckung für das Computer-Notfallteam an vorderster Stelle. Die Verwaltung als solches muss von dessen Notwendigkeit und dessen langfristigem Nutzen überzeugt sein, da sie u. a. für die benötigten Ressourcen durch Veranschlagung der Mittel im Haushalt sorgen muss. Nicht zuletzt hängt jedoch auch die Ausgestaltung der CERT-Autorität von politischen Entscheidungen ab, was ein grundlegendes Verständnis für die Arbeitsweise des Teams voraussetzt. Aus dem Abschlussbericht geht hervor, dass die direkte Verantwortung für das CERT-Niedersachsen dem CIO in Ermangelung der Rolle eines CISO übertragen werden soll. Deshalb sollte auch der CIO im Rahmen seiner Zuständigkeit für die IT-Strategie des Landes ein Verständnis für die Arbeit des Teams entwickeln und seine Unterstützung sichtbar machen. Ein deutliches Commitment für das CERT hat insbesondere einen Einfluss auf die Wahrnehmung der Constituency. Dies kann sich positiv auf deren Akzeptanz auswirken und letztendlich das Vertrauen in die Kompetenzen des Computer-Notfallteams stärken.

Aus den Erkenntnissen kann als Handlungsempfehlung formuliert werden: *Die politischen Entscheidungsträger der Landesverwaltung sollten sich ausdrücklich für ein CERT-Niedersachsen aussprechen und dessen langfristige Unterstützung garantieren.*

Faktor: Unterstützung durch andere CERTs
Im Rahmen des Vorprojektes hat sich das Land Niedersachsen bereits Unterstützung durch ein bestehendes CERT eingeholt und infolgedessen als Berater den Geschäftsführer des DFN-CERT, Herrn Dr. Kossakowski, verpflichtet. Das DFN-CERT als ältestes Team in Deutschland verfügt über langjährige praktische Erfahrungen („Best Practices“) und kann somit hilfreich zu einem erfolgreichen Aufbau beitragen. Sicherlich wären auch andere bestehende CERTs in der Lage gewesen, qualifizierte Unterstützung zu leisten. Da jedoch angenommen werden kann, dass aufgrund der erfolgreichen Zusammenarbeit im bisherigen Projekt „CERT Niedersachsen“ ein Vertrauensverhältnis zum DFN-CERT aufgebaut wurde, bietet sich auch künftig dessen Einbeziehung an. Zudem verfügt das DFN-CERT durch das Projekt nun über wertvolle Kenntnisse zu den organisatorischen Besonderheiten der öffentlichen Verwaltung. Darüber hinaus könnte sich ein Erfahrungsaustausch mit den CERTs anderer Bundesländer als nützlich erweisen und sollte bei einem Folgeprojekt zum Aufbau eines CERT geprüft werden.

Dies impliziert als Empfehlung: *Bei den Folgeprojekten sollte das DFN-CERT weiterhin in einer beratenden Funktion eingebunden werden.*

Faktor: Verfügbarkeit und sinnvoller Einsatz von Ressourcen
Ein besonderes Augenmerk ist auf die Versorgung mit Ressourcen zu legen, da in Zeiten knapper Haushaltskassen gespart werden muss. Niedersachsen verfolgt hierbei vor allem die Absicht, unnötigen Mehraufwand durch ein effizientes Vorgehen zu vermindern und durch Bündelung von Fachkompetenzen. Die Nutzung von Synergien durch die Einbeziehung bestehender Strukturen (z. B. Sicherheitsteams) zeigt ein verantwortungsvolles Vorgehen. So ist u. a. beabsichtigt, Aufgaben in Rollenkonzepte zusammenzufassen und auf vorhandenes Personal zu verteilen. Ein „virtuelles“ Team könnte auf Neueinstellungen weitgehend verzichten. Wie aus dem Abschlussbericht hervorgeht, kann der Bedarf an finanziellen Mitteln jedoch nicht gänzlich vermieden werden (z. B. Bezug externer Dienstleistungen, Aufbau von Infrastrukturen, Schulungen). Es ist eine ausreichende Versorgung des im Aufbau und später in Betrieb befindlichen CERT mit den erforderlichen Ressourcen sicherzustellen.

Aus den Überlegungen entstammt daher als Gestaltungsempfehlung: *Die benötigten Ressourcen, in diesem Fall finanzielle Mittel, sollten frühzeitig beantragt und in der Haushaltsplanung zur Verfügung gestellt werden. Außerdem sollten auch weiterhin bestehende Strukturen auf Einspareffekte hin untersucht und mögliche Synergien angestrebt werden, ohne jedoch dabei den Aufbau des CERT-Niedersachsen essenziell zu gefährden.*

Faktor: Verfügbarkeit und Qualifikation der Mitarbeiter
Einige Ressorts verfügen bereits über eigene Sicherheitsteams, die dem Computer-Notfallteam als dezentrale Einheiten dienen sollen. Daher kann davon ausgegangen werden, dass in diesem Bereich zunächst ein ausreichender Bestand an sachkundigem Personal vorhanden ist. Für die zentrale Kopfstelle müssen jedoch sehr wahrscheinlich neue Stellen geschaffen werden. Insgesamt ist anzunehmen, dass alle Mitarbeiter durch Trainings auf ihre Rolle als CERT-Mitglied und ihre zukünftigen Aufgaben vorbereitet werden müssen. Da vorgesehen ist, später auch externe Dienstleister einzusetzen, entfällt bei einigen erweiterten Basisleistungen der zeitliche und finanzielle Aufwand geeignete Mitarbeiter zu finden bzw. diese entsprechend zu qualifizieren.

Dies führt im Ergebnis zu folgender Empfehlung: *Alle zugeteilten CERT-Mitglieder sollten sorgfältig ausgewählt, im erforderlichen Umfang geschult und grundlegend auf künftige Aufgaben vorbereitet werden.*

Faktor: Akzeptanz durch die Constituency
Da die Constituency als „Kunde" von wesentlicher Bedeutung für die Ausgestaltung der Dienstleistungen ist, müssen bereits frühzeitig deren Bedürfnisse und Anforderungen an ein Computer-Notfallteam erkannt und berücksichtigt werden. Vorab müssen dazu jedoch das CERT gegenüber der Constituency bekannt gemacht und auch seine zukünftige Rolle verständlich dargestellt werden. Je sorgfältiger dieses erfolgt, desto breiter wird auch die spätere Akzeptanz durch die betroffenen Benutzer sein. Der Abschlussbericht sieht bereits Maßnahmen zur Erschließung der Constituency als Teil der zentralen Basisleistungen vor. Diese sollten jedoch nicht erst während des Pilotbetriebes, sondern schon wesentlich früher durchgeführt werden.

Insgesamt kann daraus als Empfehlung festgestellt werden: *Kontakte zur Constituency sollten bereits vor bzw. während des Aufbaus hergestellt und durch vertrauensbildende Maßnahmen (z.B. Sensibilisierung) gefestigt werden.*

Faktor: Verfügbarkeit von Informationen
Die Einführung eines neuen Computer-Notfallteams ist vielschichtig und kommt kaum ohne die effiziente Nutzung vorhandener Informationen aus. Daher lässt sich das CERT-Niedersachsen bei seinem Aufbau entscheidend durch ein bestehendes Computer-Notfallteam unterstützen. So kann z. B. das hinzugezogene DFN-CERT grundlegendes Wissen zur Verfügung stellen oder aufgrund eigener Erfahrungswerte frühzeitig auf mögliche Probleme und organisatorische Schwachstellen hinweisen. Zudem gibt es einschlägige Internetseiten, die zahlreiche Anleitungen, technische Dokumentationen und Zusammenstellungen von „Best Practices" zur eigenständigen Verwendung bereitstellen. Hier sei als Beispiel das umfangreiche Informationsangebot auf der Homepage des CERT Coordination Centers aus den USA genannt.[44] Auch über den direkten CERT-Aufbau hinaus werden z. B. Informationen über die Bedürfnisse und die Zufriedenheit der Constituency zu ermitteln sein. Diese könnten in Form einer breit angelegten Befragung der Zielgruppen ermittelt werden.

Als Empfehlung folgt daraus unmittelbar: *Relevante Informationen sollten unter Zuhilfenahme aller vertretbaren und erschwinglichen Optionen gesammelt und ausgewertet werden.*

Faktor: Einhaltung zeitlicher Vorgaben
Aus dem Abschlussbericht geht hervor, dass für den gesamten Aufbau des niedersächsischen Computer-Notfallteams (bis zum Produktivbetrieb) insgesamt drei Jahre veranschlagt werden. Im Rahmen der durchgeführten CERT-Befragung (Kapitel 5) konnte ermittelt werden, dass die Dauer des Aufbaus dabei weniger relevant ist. Eine viel größere Bedeutung kommt dagegen der Einhaltung vorgegebener Fristen zu. Da bereits frühzeitig mit der Bekanntmachung des CERTs begonnen werden sollte, könnte ein gravierender Aufschub des anvisierten Starttermins die Constituency dazu verleiten, dies auf die zukünftige Arbeitsweise des Teams zu übertragen. Die von der Constituency möglicherweise unterstellte „Unfähigkeit" hätte insgesamt negative Auswirkungen auf das Ansehen des Computer-Notfallteams und die entgegenbrachte Akzeptanz. Dem kann nur durch klare Ansagen, eine gute Zeitplanung und eine Termineinhaltung vorgebeugt werden.

Die abschließende Empfehlung für den Aufbau lautet: *Kommunizierte zeitliche Vorgaben bezüglich der Betriebsaufnahme des CERT-Niedersachsen sollten so gut wie möglich eingehalten werden.*

[44] http://www.cert.org

6.3.2 Empfehlungen für einen erfolgreichen Betrieb

Überlappend mit dem Pilotbetrieb ist der sukzessive Übergang in den Wirkbetrieb vorgesehen. Für den Pilotbetrieb werden 24 Monate, für den Übergang in den Wirkbetrieb 18 Monate veranschlagt. Der im Abschlussbericht empfohlene Zeitraum von drei Jahren für Aufbau, Pilotierung und Inbetriebnahme des CERT Niedersachsen wird damit optimal ausgenutzt.

Faktor: Unterstützung durch das Management
Das langfristige Commitment durch die politischen Entscheidungsträger sowie die für einen CERT-Betrieb verantwortlichen Instanzen wurde bereits deutlich als ein wesentliches Erfordernis herausgestellt und korrespondiert eng mit der im vorigen Abschnitt dargestellten Empfehlung. Obgleich der CIO, in Ermangelung eines CISO, die Hauptverantwortung für das Computer-Notfallteam tragen würde, wird dieses auch weiterhin auf die Akzeptanz bei den jeweiligen Zielgruppen angewiesen sein. Besonders die Abhängigkeit vom Landeshaushalt bedingt die Unterstützung und die Fürsprache des Finanzministeriums (Ressourcen), des Innenministeriums (Gefahrenabwehr) sowie des Landesrechnungshofes (Wirtschaftlichkeit und Sparsamkeit). In diesem Rahmen wird das CERT wiederholt seinen Nutzen und seine Vorzüge unter Beweis stellen müssen, um seine Existenz zu begründen und zukünftigen Einsparmaßnahmen der Landesregierung nicht zum Opfer zu fallen.

Abgeleitet aus den vorangegangenen Ausführungen kann folgende Empfehlung festgehalten werden: *Die politischen Instanzen, der CIO und auch die Zielgruppen sollten sich gemeinsam nachdrücklich für Aufbau und Betrieb eines CERT-Niedersachsen einsetzen und seinen Fortbestand langfristig garantieren.*

Faktor: Unterstützung durch andere CERTs
Unter der Unterstützung durch andere Teams ist während des Betriebes vorrangig eine informelle Zusammenarbeit im Rahmen von Interessengemeinschaften und Verbänden zu verstehen. Einige Kooperationsmöglichkeiten wurden ab S. 19 anhand wichtiger CERT-Organisationen dargeboten. Da das CERT-Niedersachsen vorwiegend auf Landesebene tätig wird, kommt ohne Zweifel eine Mitwirkung im Rahmen des CERT-Verbundes in Frage. Daraus ergeben sich zudem zahlreiche Kontaktgelegenheiten zu anderen deutschen Computer-Notfallteams. Insbesondere mit dem CERT-Bund wird es aufgrund der Verflechtungen zwischen Bundes- und Landesverwaltung höchstwahrscheinlich zu Interaktionen kommen. Darüber hinaus könnten sich auch aus einer Mitgliedschaft beim Trusted Introducer, dem Verzeichnis europäischer CERTs, Vorteile ergeben, was konkret zu prüfen wäre. Aus dem Projektbericht geht hervor, dass eine Vollmitgliedschaft als nicht unbedingt erforderlich angesehen wird, eine zumindest teilweise Registrierung jedoch nicht grundsätzlich unbeachtet bleiben sollte. Gleichermaßen in Betracht zu ziehen ist auch eine Teilnahme an internationalen Konferenzen oder Workshops zum Thema Incident Handling, sofern dieses die Fachkompetenzen des CERT-Niedersachsen alles in allem fördern kann.

Die Empfehlung lautet daher an dieser Stelle: *Mitgliedschaften beim CERT-Verbund und Trusted Introducer sollten auf ihren Nutzen hin überprüft werden. Kooperationen mit deutschen Computer-Notfallteams sind auf jeden Fall anzustreben.*

Faktor: Verfügbarkeit und sinnvoller Einsatz von Ressourcen
Langfristig ist nach dem aktuellen Konzept vor allem mit finanziellen Belastungen durch die Verpflichtung externer CERT-Dienstleister zu rechnen. Darüber hinaus können z. B. auch Kosten aus dem Verlust von Humankapital durch altersbedingtes Ausscheiden, Abwerbung oder Kündigung bzw. Versetzung qualifizierter Mitarbeiter antizipiert werden. Diesem kann nur durch Neueinstellungen und der Qualifizierung des verfügbaren Personals entgegengewirkt werden, was zum einen Zeit und zum anderen finanzielle Mittel beansprucht. Gleichermaßen wird das Computer-Notfallteam ein stärkeres Interesse daran haben, mit seiner Aus-

stattung auf dem aktuellsten Stand der Technik zu sein, als dies vielleicht in anderen Bereichen der Fall ist. Deshalb ist auch bei der Aufrechterhaltung benötigter sicherer Infrastrukturen mit Kosten zu rechnen. Ohne eine grundlegende Planung, kontinuierliche Berichtigungen und eine anschließende Kontrolle ist eine verantwortungsbewusste Ressourcenverwendung schlecht zu realisieren.

Dies lässt sich zu nachstehender Empfehlung zusammenfassen: *Ressourcen sollten ausreichend zu Verfügung gestellt werden. Im Hinblick auf die Einsatzfähigkeit des Teams ist deren Verwendung jedoch maßvoll zu gestalten und muss überwacht werden.*

Faktor: Verfügbarkeit und Qualifikation der Mitarbeiter
Wie schon zuvor dargestellt, setzt das bisherige Konzept des niedersächsischen Computer-Notfallteams für die Erbringung der erweiterten Basisleistungen und der individuellen Zusatzleistungen vermehrt auf den Einsatz externer CERT-Dienstleister. Dies hilft vor allem kurzfristig, Versorgungsengpässe zu vermeiden, Personal einzusparen und Ausbildungskosten zu senken. Eine fundierte Ausbildung bestehender Mitarbeiter ist jedoch unausweichlich, da sonst auf lange Sicht keine Kompetenzen aufgebaut und erweitert werden können. Trotz Outsourcing einer bestimmten Anzahl von Dienstleistungen kann das Computer-Notfallteam, bedingt durch steigende Arbeitsbelastung und Personalabgang, im Verlauf feststellen, dass ein zusätzlicher Bedarf an zentral oder dezentral eingesetztem Personal besteht. Dieses beinhaltet auch die zum vorigen Faktor skizzierten Überlegungen zum Humankapital. Es sollte bedacht werden, dass die Mitglieder des „virtuellen“ Teams neben den anfallenden CERT-Aufgaben weiterhin ihre tägliche Arbeit in der jeweiligen Dienststelle zu bewältigen haben (Gefahr des Burn-Out bei andauernder Überbelastung).

Im Ergebnis führt dies zu folgender Empfehlung: *Alle Mitarbeiter sind hinreichend auszubilden und regelmäßig zu schulen. Mögliche Überbelastungen sollten antizipiert und durch passende Maßnahmen kompensiert bzw. umgangen werden.*

Faktor: Akzeptanz durch die Constituency
Die Leistungen des Teams und sein Verhalten tragen einen beachtlichen Teil zur Wahrnehmung der Fachkompetenz durch die Constituency bei. Jedoch sind es letztlich auch die langfristig angelegten vertrauensbildenden Maßnahmen und wiederholten Informationsveranstaltungen, die der Constituency ein grundlegendes Verständnis für die CERT-Aufgaben vermitteln. Da der Aufbau einer guten Beziehung zwischen Computer-Notfallteam und Constituency vor allem Zeit beansprucht, veranschlagt der Abschlussbericht z. B. auch einen Zeitraum von mindestens drei Jahren bis zur vollständigen Betriebsbereitschaft. Obwohl der Fokus des CERT-Niedersachsen auf der primären Zielgruppe liegt, dürfen auch die Bedürfnisse der anderen identifizierten Gruppen nicht vernachlässigt werden. In regelmäßigen Abständen können und sollten daher die Leistungen des Teams an der Zufriedenheit der Constituency überprüft werden.

Daraus lässt sich eine deutliche Empfehlung formulieren: *Das CERT-Niedersachsen sollte der Akzeptanz durch die Constituency besondere Aufmerksamkeit schenken und diese durch entsprechende Maßnahmen fördern.*

Faktor: Bedarfsgerechtes Dienstleistungsangebot
Das bisherige Leistungskonzept des CERT-Niedersachsen sieht sowohl reaktive als auch präventive Dienste vor und ermöglicht obendrein Maßnahmen zur Verbesserung der Nachhaltigkeit der IT-Sicherheit. Im Rahmen des Projektes wurden bereits für als wesentlich erachtete Basisleistungen im Kern grob abgegrenzt und müssen im Folgeprojekt genauer ausdefiniert werden. Dabei kann auch das Bewusstsein um Abhängigkeiten zwischen einzelnen Aufgaben hilfreich sein. Das tatsächliche Dienstleistungsangebot des CERTs hat sich in der Folge schließlich an den betroffenen Benutzern auszurichten. Auf die Bedeutung einer

guten Beziehung zur Constituency und dem grundlegenden Verständnis ihrer Bedürfnisse wurde deutlich im Vorangegangenen hingewiesen. Sowohl der Inhalt als auch der Umfang der einzelnen Leistungen muss der Constituency als Empfänger deutlich kommuniziert und verständlich gemacht werden.

Als Empfehlung kann daher Folgendes zusammengefasst werden: *Auf Grundlage der Ergebnisse des Zwischenberichtes sollte die exakte Nachfrage der Constituency zur Ausgestaltung eines bedarfsgerechten Dienstleistungsangebotes ermittelt werden.*

Faktor: Dokumentation von Vorgehensweisen und Richtlinien
Aus Abb. 6 auf S. 44 geht die organisatorische Struktur hervor, mit der zukünftig die niedersächsische Landesverwaltung sein Vorgehen hinsichtlich Informationssicherheit dokumentiert. Anhand einer zunächst noch abstrakten Leitlinie auf strategischer Ebene führt dies über die Definition von Vorgaben in Richtlinien zu konkreten operativen Konzepten und Handlungsanweisungen. Da nicht nur die Constituency ein klares Verständnis der zur Verfügung stehenden Leistungen benötigt, sondern auch den CERT-Mitgliedern deutliche Arbeitsanweisungen an die Hand gegeben werden müssen, sollten vor allem die Dienstleistungen besonders präzise definiert und beschrieben werden. Nur so kann letztendlich die Kontinuität eines qualifizierten CERT-Angebotes auf hohem Niveau sichergestellt werden. Die CERT-Befragung ergab, dass das Sammeln und Auswerten statistischer Daten zwar für eine Erfolgskontrolle von Bedeutung sein kann und laut Projektbericht auch erfolgen soll. Für den eigentlichen Erfolg ist dies jedoch eher zweitrangig.

Festgehalten werden kann somit die nachstehende Empfehlung: *Mit der Ausgestaltung des Dienstleistungsangebotes sind die einzelnen Leistungen und Prozesse genau zu definieren und verständlich zu beschreiben.*

Faktor: Vorhandensein einer Informationspolitik
Wie in vorweg verdeutlicht wurde, umfasst dieser Faktor vor allem den Aufbau und die Nutzung einer sicheren Kommunikationsinfrastruktur. Damit ist zugleich eine Vorbedingung für den vertrauensvollen Umgang mit sensiblen Informationen (Sicherheitslücken, Vorfälle) gegeben. Eine Informationspolitik regelt im alltäglichen CERT-Betrieb, wem welche Informationen zugänglich zu machen sind und wie tiefgründig die Auskünfte zu spezifischen sicherheitsbezogenen Anfragen sein werden. Dies geht auch aus den Angaben des Projektberichtes hervor, der den Aufbau und den Betrieb einer sicheren Kommunikations- und Informationsinfrastruktur zu den zentralen Basisleistungen des zukünftigen CERT-Niedersachsen zählt.

Für den erfolgreichen Betrieb des Computer-Notfallteams wird abschließend als Empfehlung angeführt: *Vor allem auf technischer Seite sollte das CERT-Niedersachsen für eine vertrauenswürdige und gesicherte Kommunikationsinfrastruktur sorgen.*

6.4 Bewertung

Es ist zu erkennen, dass die niedersächsische Landesverwaltung trotz der schwierigen Haushaltslage dem Thema Informationssicherheit zukünftig mehr Aufmerksamkeit schenken wird. Die Notwendigkeit von Maßnahmen zur Verbesserung der Informationssicherheit und deren Aspekte im Einzelnen wurden erkannt. Der Grundstein für eine operative Komponente in der zukünftigen Organisationsstruktur für IT-Sicherheit der niedersächsischen Landesverwaltung ist u. a. durch die Überlegungen zum Aufbau eines Computer-Notfallteams gelegt worden. Insgesamt bleibt jedoch abzuwarten, wie die Entscheidung zu einem Folgeprojekt ausfällt und dessen konkrete Ausgestaltung aussieht. Die Ausgestaltung des Folgeprojektes wird wesentlichen Einfluss auf den tatsächlichen Erfolg des Gesamtvorhabens haben. Es ist durchaus denkbar, dass später auch andere Lösungen realisiert werden, als im Rahmen des CERT-Projektes oder dieser Arbeit in Betracht gezogen wurden. Ob diese, zumindest aus theoretischer Sicht, dann genauso zielführend sein werden wie die im vorliegenden Projekt mit einem erfahrenen Sicherheitsexperten und unabhängigen CERT-Dienstleister erarbeiteten Projektergebnisse, bleibt abzuwarten.

7 Fazit

Ein wesentlicher Schwerpunkt dieser Arbeit bestand in der Ermittlung potenzieller Erfolgsfaktoren für ein Computer-Notfallteam. 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 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 Kommunikationsinfrastruktur für die Zusammenarbeit mit anderen CERTs unabdingbar ist.

Bevor die herausgearbeiteten Erfolgsfaktoren schließlich auf das CERT-Niedersachsen angewendet werden konnten, wurde zunächst die derzeitige Situation hinsichtlich der Organisationsstruktur für IT-Sicherheit in Niedersachsen skizziert. Demnach verfügt das Land aufgrund des Ressortprinzips über eine bisher uneinheitliche Ausstattung an IT-Ressourcen, wenig übergreifende IT-Sicherheitsprävention sowie keine ressortübergreifend koordinierte Reaktion auf IT-Sicherheitsvorfälle. Diese Umstände wurden erkannt und sollen möglichst im Rahmen der strategischen Neuausrichtung des IT-Einsatzes behoben werden. Die konkreten Anforderungen an ein zukünftiges CERT-Niedersachsen konnten durch den Projektauftrag und den Abschlussbericht 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 von dezentralen CERT-Komponenten übernehmen, die von einer zentralen Kopfstelle angeleitet und überwacht wird. Zusammen ergibt dieses das „virtuelle“ CERT-Niedersachsen. 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 einer politischen Rückendeckung als Bedingung für weitere Planungen hinzuweisen ist. Alles in allem ist das zielgerichtete Vorgehen des Landes 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 erfolgreich 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 Informationssicherheit bei den Geschäftsprozessen der niedersächsischen Landesverwaltung 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.

8 Literaturhinweise

Dieses Dokument ist eine gekürzte Fassung der folgenden Diplomarbeit:

Hoyer [2006]: Kritische Erfolgsfaktoren für ein Computer Emergency Response Team (CERT) am Beispiel CERT-Niedersachsen. Diplomarbeit am Institut für Wirtschaftsinformatik an der Wirtschaftswissenschaftlichen Fakultät der Universität Hannover. Abgegeben am 22.02.2006.

Weitere Quellen:

Alberts u. a. [2004]: Defining Incident Management Processes for CSIRTs: A Work in Progress. http://www.cert.org/archive/pdf/04tr015.pdf

CERT Coordination Center [2002a]: Computer Security Incident Response Team (CSIRT) - Frequently Asked Questions (FAQ). http://www.cert.org/csirts/csirt_faq.html

CERT Coordination Center [2002b]: Creating a Computer Security Incident Response Team - A Process for Getting Started. http://www.cert.org/csirts/Creating-A-CSIRT.html

CERT Coordination Center [2002c]: CSIRT Services. http://www.cert.org/archive/pdf/CSIRT-services-list.pdf

Killcrece [2003]: Security Professionals Workshop - Creating a CSIRT. http://www.educause.edu/ir/library/pdf/SEC0302.pdf

Killcrece [2004]: Steps for Creating National CSIRTs. August 2004. http://www.cert.org/archive/pdf/NationalCSIRTs.pdf

Killcrece u. a. [2003a]: Organizational Models for Computer Incident Response Teams (CSIRTs). http://www.cert.org/archive/pdf/03hb001.pdf

Killcrece u. a. [2003b]: State of the Practice of Computer Incident Response Teams (CSIRTs). http://www.cert.org/archive/pdf/03tr001.pdf

Kossakowski [2000]: Information Technology Incident Response Capabilities. Libri Books on Demand, Hamburg 2000.

Kossakowski [2006]: CERT-Leistungen für Niedersachsen - Abschlussbericht. Niedersächsisches Ministerium für Inneres und Sport (MI). Zentrales IT-Management (ZIM). Projektinterner Zwischenbericht. Stand: 28. Juni 2006.

Irion [2005]: Projektauftrag "CERT Niedersachsen" (CERT-NDS). Niedersächsisches Ministerium für Inneres und Sport (MI). Zentrales IT-Management (ZIM). Stand: 21.09.2005.

Pattloch/Kossakowski [2001]: CERT-Dienstleistungen für kleine und mittlere Unternehmen (KMU). http://www.kossakowski.de/kmucert-gutachten.pdf

Smith [1995]: Forming an Incident Response Team. ftp://ftp.auscert.org.au/pub/auscert/papers/Forming_an_Incident_Response_Team_A4.ps

West-Brown u. a. [2003]: Handbook for Computer Security Incident Response Teams (CSIRTs). 2nd. Ed. http://www.cert.org/archive/pdf/csirt-handbook.pdf

Anhang 1: Fragebogen zu kritischen CERT-Erfolgsfaktoren

Erfolgsfaktoren von
Computer Emergency Response Teams

A. Einige Fragen zu Ihren persönlichen Erfahrungen

1. Wie viele Jahre arbeiten Sie bereits im CERT-Betrieb?

   _____

2. Welche Funktion(en) üben Sie aktuell in Ihrem CERT aus?

   _____

   _____

3. Bei wie vielen CERT Aufbau-Projekten wurden Sie bisher tätig?

   _____

4. Welche Rolle(n) haben Sie dabei ausgeübt? (Mehrfachnennung möglich)

   - ❒ Projektleiter
   - ❒ Projektmitglied
   - ❒ externer Berater
   - ❒ _____

B. Allgemeine Fragen zum Aufbau Ihres CERT

5. Welchen Grund gab es für den Aufbau Ihres CERT? (Mehrfachnennung möglich)

   - ❒ Anforderungen durch Management bzw. Organisation
   - ❒ Konkreter Sicherheitsvorfall
   - ❒ Kein spezieller Grund
   - ❒ _____

     _____

6. Wie viele Monate beanspruchte der Aufbau Ihres CERT?

   _____

7. Wo gab es Schwierigkeiten beim Aufbau Ihres CERT?

   _____

   _____

   _____

8. Wie messen Sie den Erfolg der Aufbauphase?

   _____

   _____

   _____

Erfolgsfaktoren von
Computer Emergency Response Teams

C. Allgemeine Fragen zum Betrieb Ihres CERT

9. Seit wann ist Ihr CERT in Betrieb?

_____

10. Wurde eine Auftragserklärung (Mission Statement) definiert?

- ❒ Ja
- ❒ Nein

11. Wenn Ja, wurde diese öffentlich bekannt gemacht?

- ❒ Ja, kann öffentlich eingesehen werden.
- ❒ Nein, ist nur intern bekannt.

12. Hat Ihr CERT einen festgelegten Kundenkreis (Constituency)?

- ❒ Ja
- ❒ Nein

13. Wenn Ja, wurde dieser öffentlich bekannt gemacht?

- ❒ Ja, kann öffentlich eingesehen werden.
- ❒ Nein, ist nur intern bekannt.

14. Welche Befugnisse (Autorität) hat Ihr CERT gegenüber den Kunden?

- ❒ Keine (kann nur durch Empfehlungen beeinflussen)
- ❒ Eingeschränkte (alle Maßnahmen werden abgesprochen)
- ❒ Volle (kann Maßnahmen ohne Rücksprache durchführen)
- ❒ Hängt von der jeweiligen Dienstleistung ab
- ❒ _____
  _____
  _____

15. Wo ist Ihr CERT in der Organisation angesiedelt?

- ❒ Managementebene (z. B. als Stabstelle)
- ❒ IT-Abteilung
- ❒ Eigenständige Abteilung
- ❒ Eigenständige Organisation (rechtlich selbstständig)
- ❒ _____
  _____
  _____

Erfolgsfaktoren von
Computer Emergency Response Teams

16. Durch welche der folgenden Kategorien wird Ihr CERT am Besten beschrieben?

- ❒ Ad hoc Team (wird zusammengerufen, wenn ein Vorfall auftritt)
- ❒ Intern verteiltes Team (Rollenverteilung innerhalb der Organisation)
- ❒ Intern zentrales Team (es gibt eine zentrale Abteilung)
- ❒ Kombination aus verteiltem und zentralem Team
- ❒ Koordinierendes Team (koordiniert die Arbeit anderer Teams)
- ❒ _____

17. Kooperiert Ihr CERT mit anderen Teams oder Verbänden?

- ❒ Ja
- ❒ Nein

18. Wenn Ja, mit wie vielen?

_____

19. Wie finanziert sich Ihr CERT? (Mehrfachnennung möglich)

- ❒ Das Team wird durch die umgebende Organisation finanziert.
- ❒ Mit Hilfe staatlicher Unterstützung (Bund / Land / Region / Stadt).
- ❒ Jede Dienstleistung ist mit einer Gebühr belegt.
- ❒ _____

20. Wo gab oder wo gibt es aktuell Schwierigkeiten beim Betrieb Ihres CERT?

_____

21. Wie messen Sie den Erfolg der Betriebsphase?

_____

Erfolgsfaktoren von
Computer Emergency Response Teams

D. Fragen zu den Hindernissen und Erfolgsfaktoren beim Aufbau eines neuen CERT

22. Wo liegen nach Ihrer Erfahrung die 2 größten Hindernisse beim Aufbau eines neuen CERT?

a) _____

_____

b) _____

_____

23. Was sind für Sie die 3 wichtigsten Faktoren für den erfolgreichen Aufbau eines neuen CERT?

a) _____

_____

b) _____

_____

c) _____

_____

E. Nehmen Sie nun bitte eine Bewertung der folgenden Aussagen vor!

24. Wie bewerten Sie die nachfolgenden Aussagen hinsichtlich ihrer Wichtigkeit für den Erfolg beim Aufbau eines neuen CERT?

Abstufung: ++ = sehr relevant, + = relevant, - = wenig relevant, -- = nicht relevant	++	+	-	--
Das Management muss die Unterstützung für das Team langfristig zusichern (z. B. Zusicherung der Befugnisse).	❒	❒	❒	❒
Frühzeitig muss ein enger Kontakt zur Constituency (Kundenkreis) hergestellt und aufrechterhalten werden.	❒	❒	❒	❒
Alle relevanten und benötigten Informationen für Planung und Einführung müssen früh beschafft und allen Beteiligten zur Verfügung gestellt werden.	❒	❒	❒	❒
Es müssen genügend qualifizierte Mitarbeiter vorhanden sein.	❒	❒	❒	❒
Notwendige Ressourcen (Personal, Technologie, Finanzen usw.) müssen vom Management ausreichend zur Verfügung gestellt werden.	❒	❒	❒	❒
Eine fundierte Ausbildung neuer Mitarbeiter muss vor Betriebsaufnahme erfolgen.	❒	❒	❒	❒
Es muss Klarheit herrschen über die anzubietenden Dienstleistungen und benötigten Vorgehensweisen.	❒	❒	❒	❒
Bereits während der Einführung muss ein vertrauensvolles Verhältnis zur Constituency aufgebaut werden.	❒	❒	❒	❒
Der Aufbau eines neuen Teams muss schnell erfolgen.	❒	❒	❒	❒
Der Aufbau eines neuen Teams muss gut koordiniert werden. Fehler bei der Einführung eines neuen Teams verbrauchen später notwendige Ressourcen.	❒	❒	❒	❒
Die Unterstützung durch erfahrene CERTs muss sichergestellt werden (z. B. direkte Hilfe beim Aufbau, Nutzung von Best Practices).	❒	❒	❒	❒
Beim Aufbau müssen zeitliche Verzögerungen, bedingt durch verschiedene Faktoren (z. B. erfahrenes Personal nicht verfügbar), eingeplant werden.	❒	❒	❒	❒

Erfolgsfaktoren von
Computer Emergency Response Teams

F. Fragen zu den Hindernissen und Erfolgsfaktoren beim Betrieb eines CERT

25. Wo liegen nach Ihrer Erfahrung die 2 größten Hindernisse beim Betrieb eines CERT?

a) _____

_____

b) _____

_____

26. Was sind für Sie die 3 wichtigsten Faktoren für den erfolgreichen Betrieb eines CERT?

a) _____

_____

b) _____

_____

c) _____

_____

G. Nehmen Sie nun bitte eine Bewertung der folgenden Aussagen vor!

27. Wie bewerten Sie die nachfolgenden Aussagen hinsichtlich ihrer Wichtigkeit für den Erfolg beim Betrieb eines CERT?

Abstufung: ++ = sehr relevant, + = relevant, - = wenig relevant, -- = nicht relevant	++	+	-	--
Das Management muss seine Unterstützung langfristig zusichern (z. B. Zusicherung der Befugnisse).	❒	❒	❒	❒
Das Dienstleistungsangebot muss reaktive und präventive Aufgaben umfassen.	❒	❒	❒	❒
Der Informationsfluss zwischen allen Beteiligten muss durch eine umfassende Informationspolitik geregelt ablaufen.	❒	❒	❒	❒
Erfahrene und qualifizierte Mitarbeiter müssen ausreichend vorhanden sein.	❒	❒	❒	❒
Bei der Constituency muss ein allgemeines Bewusstsein für Sicherheit und die Arbeit des Teams geschaffen werden.	❒	❒	❒	❒
Das Dienstleistungsangebot muss sich an den spezifischen Bedürfnissen der Constituency ausrichten.	❒	❒	❒	❒
Die Verbindungen zwischen verschiedenen Dienstleistungen müssen bekannt sein.	❒	❒	❒	❒
Zur Messung des Erfolgs und zur Planung zukünftiger Vorgehensweisen müssen Daten gesammelt und analysiert werden (z. B. von bearbeiteten Vorfällen).	❒	❒	❒	❒
Die eigene Arbeit muss mit anderen Teams koordiniert und abgestimmt werden.	❒	❒	❒	❒
Die Mitarbeiter beeinflussen das Erscheinungsbild des Teams und müssen sich jederzeit kompetent und angemessen verhalten.	❒	❒	❒	❒
Vorgehensweisen und Dienstleistungen müssen gut dokumentiert werden.	❒	❒	❒	❒
Die Unterstützung durch andere CERTs muss sichergestellt werden (z. B. Nutzung von Best Practices).	❒	❒	❒	❒
Das Vertrauen der Constituency muss langfristig erworben.	❒	❒	❒	❒
Notwendige Ressourcen (Personal, Technologie, Finanzen usw.) müssen vom Management in ausreichender Menge zur Verfügung gestellt werden.	❒	❒	❒	❒
Der Constituency müssen klare Richtlinien zur Berichterstattung gegeben werden.	❒	❒	❒	❒

Anhang 2: Antworten der CERT-Befragung

Fragebogen Antwortübersicht	Angaben aller Bögen, außer Bewertungen
A. Einige Fragen zu Ihren persönlichen Erfahrungen	
1. Wie viele Jahre arbeiten Sie bereits in einem CERT-Betrieb?	- von 2 bis 13 Jahre [2, 3, 3, 3.5, 4, 5, 13] - Mittelwert liegt bei 4.79 Jahren
2. Welche Funktion(en) üben Sie aktuell in Ihrem CERT aus?	- Leiter / Teamleiter / technischer Leiter (7x) - zusätzliche einige: Vorstand / Konzernkoordinator / Advisory-Autor
3. Bei wie vielen CERT Aufbau-Projekten wurden Sie bisher tätig?	- von 1 bis 10 Projekte [1, 1, 1, 2, 2, 5, 10] - Mittelwert liegt bei 3.14 Projekten
4. Welche Rolle(n) haben Sie dabei ausgeübt?	- Projektleiter (4x) - Projektmitglied (3x) - externer Berater (3x)
B. Allgemeine Fragen zum Aufbau Ihres CERT	
5. Welchen Grund gab es für den Aufbau Ihres CERT?	- Anforderungen durch Management bzw. Organisation (4x) - konkreter Sicherheitsvorfall (2x) - öffentl. Bedürfnis an CERT für Mittelstand - kommerzielle Idee
6. Wie viele Monate beanspruchte der Aufbau Ihres CERT?	- von 3 bis 18 Monate [3, 3, 6, 7, 11 ,18 ,18] - Mittelwert liegt bei 9.43 Monaten
7. Wo gab es Schwierigkeiten beim Aufbau Ihres CERT?	- Management musste überzeugt werden, genaue Abgrenzung der Aufgaben - Finanzierung (weil privates Unternehmen), 1 Jahr Vorlaufzeit zur Beschaffung der Finanzen - Regelung, Entscheidungskompetenzen, Organisatorische Zugehörigkeit - wechselndes Personal, keine langfristigen und durchgängigen Verantwortlichkeiten für einen Bereich - Definition der Dienstleistungen, Verzögerungen - Personal, fehlende Information, keine Prozesse, Kontakt mit Zielgruppe, unklare Vorstellungen - Zuständigkeiten und Befugnisse - keine Angabe (1x)
8. Wie messen Sie den Erfolg der Aufbauphase?	- Unternehmen trägt sich - CERT trägt sich selbst - neue Kunden konnten gewonnen werden - bestehende Aufträge wurden verlängert - Ausstattung mit Ressourcen (Budget, Personal) - Akzeptanz innerhalb Konzern - Integration in Linienorganisation - Starttermin wird eingehalten - Messung erfolgte über Meilensteine - guter Kompromiss zwischen PR und "technischen" Anforderungen wird gefunden - Akzeptanz bei der Constituency - Kenntnis der Benutzerschaft des CERT - gar nicht, ist Bauchgefühl - oder - Bereitschaft der Zielgruppe zu reden und zu melden
C. Allgemeine Fragen zum Betrieb Ihres CERT	
9. Seit wann ist Ihr CERT in Betrieb?	- von 1994 bis 2004 [1994, 1999, 2000, 2002, 2003, 2003, 2004]
10. Wurde eine Auftragserklärung (Mission Statement) definiert?	- Ja (6x) - Nein (1x)
11. Wenn Ja, wurde diese öffentlich bekannt gemacht?	- Ja (4x) - Nein (3x)
12. Hat Ihr CERT einen festgelegten Kundenkreis (Constituency)?	- Ja (7x) - Nein (0x)
13. Wenn Ja, wurde dieser öffentlich bekannt gemacht?	- Ja (7x) - Nein (0x)
14. Welche Befugnisse (Autorität) hat Ihr CERT gegenüber den Kunden?	- Keine (4x) - Eingeschränkte (1x) - Volle (1x) - Hängt von der jeweiligen Dienstleistung ab (1x)
15. Wo ist Ihr CERT in der Organisation angesiedelt?	- eigenständige Organisation (3x) - eigenständige Abteilung (1x) - IT-Abteilung (2x) - Managementebene, frei: Stabstelle bei ausführender Einheit (1x)
16. Durch welche der folgenden Kategorien wird Ihr CERT am Besten beschrieben?	- Zentrales Team (5x) - Koordinierendes Team (2x) - Dezentrales Team (2x) - Ad hoc Team (1x)
17. Kooperiert Ihr CERT mit anderen Teams oder Verbänden?	- Ja (7x) - Nein (0x)
18. Wenn Ja, mit wie vielen?	- von 2 bis 12 [2, 3, 3, 3, 5, 12] - Frage wurde mit Angabe der Verbände beantwortet, daher unbrauchbar (undeutlich gestellte Frage)
19. Wie finanziert sich Ihr CERT?	- Das Team wird durch die umgebende Organisation finanziert. (4x) - Jede Dienstleistung ist mit einer Gebühr belegt. (3x) - Mit Hilfe staatlicher Unterstützung. (1x) - frei: Dienstleistungspaket wird zentral für Constituency finanziert (1x) - frei: Sponsoren (1x)
20. Wo gab oder wo gibt es aktuell Schwierigkeiten beim Betrieb Ihres CERT?	- Ressourcen (monetäre Ausstattung) - fehlendes qualifiziertes Personal - Personalweggang und Aufwuchs - zunehmende Belastung durch Vorfälle, Millionen von Angriffen verbieten manuelle Arbeit - Die Personalsituation ist aufgrund des virtuellen Teams oft angespannt - Anpassung an neue Anforderungen - Vermittlungsprobleme zur Notwendigkeit von CERT-Dienstleistungen in der Constituency - Zweifel an Unabhängigkeit wegen Ansiedlung in Organisation - Kontrollierende Maßnahmen - Zwangsabschaltung - Schwierigkeiten beim Aufbau eines Portals zur Vorfallsbearbeitung (Eigenentwicklung, persönl. Controlcenter) - eigentlich keine (1x) - keine Angabe (1x)
21. Wie messen Sie den Erfolg der Betriebsphase?	- Anzahl erfolgreich behandelter Incidents, Zeitspanne Erkennung bis Abwehr von Angriffen etc. - Kundenzufriedenheit (Online-Umfragen), Kundenzahlen, Akzeptanz, Qualität der Dienstleistungen - Alle 6 Monate Feedback der Constituency - Positives Kundenfeedback - Etablierung als interner Dienstleister für Sicherheitsfragen - eigentlich nur über BWL-Kennzahlen, geht nur mit Geschäftszahlen (Bilanz) - Über die Jahre Modelle entwickelt, mit denen man Veränderungen ausmachen kann. Werden dann besprochen.

Seite 1 von 2

Fragebogen Antwortübersicht	Angaben aller Bögen, außer Bewertungen
D. Fragen zu den Hindernissen und Erfolgsfaktoren beim	
22. Wo liegen nach Ihrer Erfahrung die 2 größten Hindernisse beim Aufbau eines neuen CERT?	
a)	- Mangel an Personal mit entsprechender Fachkompetenz - Entscheidungskompetenz und Weisungsbefugnisse - Festlegung der Aufgaben (unklare Aufgaben) - fehlende Ausrichtung an Kundenbedürfnissen / Erkennen der Kundenbedürfnisse - fehlende Akzeptanz bei den verantwortlichen Administratoren - Finanzierung einer angemessenen Dienstleistung - Management muss überzeugt werden (vor allem für finanzielle Mittel & Personal)
b)	- Finanzierung - Ressourcenbeschaffung in Zeiten der Kostensparprogramme - Ausstattung mit genug Know-how um proaktiv reagieren zu können (zuwenig Ressourcen) - fehlendes Commitment der Mutter-Organisation und der Partner - Platzierung und Bekanntmachung in der Organisation - Fehlende Management-Zustimmung - Integration ins gesamte Risikomanagement
23. Was sind für Sie die 3 wichtigsten Faktoren für den erfolgreichen Aufbau eines neuen CERT?	
a)	- (gutes) Personal (3x) - breite Fachkompetenz der Mitarbeiter - Festlegung der Aufgaben - Klares Commitment des Vorstandes bzw. Geschäftsleitung - Unterstützung der beteiligten Parteien / Partner - Vertrieb ist wichtiger Faktor / Key-Account aufbauen, persönliche Nähe zum Kunden (kommerzieller Dienstleister) - Geld
b)	- Ausreichende Ausstattung an Personal und Technik - Know-how-Konzentration muss möglich sein - zielgerichtete Dienstleistungen - gute Projektplanung - Zeit und Geduld
c)	- Finanzierung - definierte und angemessene Kosten - Dienstleistungsgedanke - klar definierte Aufgaben - Vorhandene Securitypolicies im Unternehmen - Starttermin festlegen & einhalten - Management Support und Bekenntnis zur "Feuerwehr" statt "Polizei"
F. Fragen zu den Hindernissen und Erfolgsfaktoren beim	
25. Wo liegen nach Ihrer Erfahrung die 2 größten Hindernisse beim Betrieb eines CERT?	
a)	- Management mischt sich ein - fehlende Entscheidungskompetenz - Zuständigkeiten - fehlender Dienstleistungsgedanke - zu wenig Personal - Personal und Personalburnout - Hotline ggf. überlastet, gleicht sich aber aus, da einige Kunden häufiger anrufen, andere dafür weniger
b)	- fehlende oder unvollständige Prozesse in der IT-Produktion - CERT wird falsch verstanden bzw. versteht sich falsch - fehlender Kontakt zur Constituency - schlechte Vermittlung der Arbeit an die Constituency - mangelnde Sensibilisierung - stetige Finanzierung
26. Was sind für Sie die 3 wichtigsten Faktoren für den erfolgreichen Betrieb eines CERT?	
a)	- Zuständigkeiten festlegen / klare Zuständigkeiten - qualifizierte & motivierte Mitarbeiter - gutes Personal - breite Fachkompetenz der Mitarbeiter - Offene Kommunikation - Hotline (SPOC), Ticketsystem muss funktionieren - Leidensfähigkeit
b)	- Sensibilisierung des Kunden - regelmäßiges Anpassen der Dienste an Bedürfnisse - ausreichende Personalausstattung - Kommunikationsstrukturen müssen funktionieren/stehen - "Standing" in der Zielgruppe - Geduld
c)	- Management-Unterstützung - direktes Reporting an Vorstand / Geschäftsleitung - Transparenz von Kosten und Leistung - Support - Schulung der Mitarbeiter - gutes "Standing" in der Constituency - Schnittstellen zu anderen müssen da sein & passen, autom. Verarbeitung von Meldungen, national vereinheitlicht

Anhang 3: Ergebnisse der Aussagenbewertung

Bewertungsübersicht (KEF sortiert)	Anteil	Anteil	Anteil	Anteil	Anzahl	Wert	#

E. Nehmen Sie nun bitte eine Bewertung der folgenden Aussagen vor! (Aufbau eines CERTs)	sehr relevant (++ = 3)		relevant (+ = 2)		wenig relevant (- = 1)		nicht relevant (-- = 0)		gesamt Angaben	Mittel-wert	Rang
24. *Wie bewerten Sie die nachfolgenden Aussagen hinsichtlich ihrer Wichtigkeit für den Erfolg beim Aufbau eines neuen CERT?*											
1 Das Management muss die Unterstützung für das Team langfristig zusichern (z. B. Zusicherung der Befugnisse).	6	86%	1	14%	0	0%	0	0%	7	2,86	1
13 Die Unterstützung durch erfahrene CERTs muss sichergestellt werden (z. B. direkte Hilfe beim Aufbau, Nutzung von Best Practices).	2	29%	3	43%	2	29%	0	0%	7	2	8
6 Notwendige Ressourcen (Personal, Technologie, Finanzen usw.) müssen vom Management ausreichend zur Verfügung gestellt werden.	3	43%	4	57%	0	0%	0	0%	7	2,43	6
12 Der Aufbau eines neuen Teams muss gut koordiniert werden. Fehler bei der Einführung eines neuen Teams verbrauchen später notwendige Ressourcen.	2	29%	4	57%	1	14%	0	0%	7	2,14	7
4 Es müssen genügend qualifizierte Mitarbeiter vorhanden sein.	5	71%	2	29%	0	0%	0	0%	7	2,71	2
8 Eine fundierte Ausbildung neuer Mitarbeiter muss vor Betriebsaufnahme erfolgen.	0	0%	6	86%	1	14%	0	0%	7	1,86	9
10 Bereits während der Einführung muss ein vertrauensvolles Verhältnis zur Constituency aufgebaut werden.	4	57%	3	43%	0	0%	0	0%	7	2,57	5
2 Frühzeitig muss ein enger Kontakt zur Constituency (Kundenkreis) hergestellt und aufrechterhalten werden.	5	71%	2	29%	0	0%	0	0%	7	2,71	2
3 Alle relevanten und benötigten Informationen für Planung und Einführung müssen früh beschafft und allen Beteiligten zur Verfügung gestellt werden.	0	0%	5	71%	2	29%	0	0%	7	1,71	11
9 Es muss Klarheit herrschen über die anzubietenden Dienstleistungen und benötigten Vorgehensweisen.	6	86%	0	0%	1	14%	0	0%	7	2,71	2
14 Beim Aufbau müssen zeitliche Verzögerungen, bedingt durch verschiedene Faktoren (z. B. erfahrenes Personal nicht verfügbar), eingeplant werden.	0	0%	6	86%	1	14%	0	0%	7	1,86	9
11 Der Aufbau eines neuen Teams muss schnell erfolgen.	0	0%	2	29%	5	71%	0	0%	7	1,29	12

G. Nehmen Sie nun bitte eine Bewertung der folgenden Aussagen vor! (Betrieb eines CERTs)	sehr relevant (++ = 3)		relevant (+ = 2)		wenig relevant (- = 1)		nicht relevant (-- = 0)		gesamt Angaben	Mittel-wert	Rang
27. *Wie bewerten Sie die nachfolgenden Aussagen hinsichtlich ihrer Wichtigkeit für den Erfolg beim Betrieb eines CERT?*											
2 Das Management muss seine Unterstützung langfristig zusichern (z. B. Zusicherung der Befugnisse).	3	43%	3	43%	1	14%	0	0%	7	2,29	5
14 Die Unterstützung durch andere CERTs muss sichergestellt werden (z. B. Nutzung von Best Practices).	1	14%	5	71%	1	14%	0	0%	7	2	9
11 Die eigene Arbeit muss mit anderen Teams koordiniert und abgestimmt werden.	1	14%	3	43%	3	43%	0	0%	7	1,71	14
16 Notwendige Ressourcen (Personal, Technologie, Finanzen usw.) müssen vom Management in ausreichender Menge zur Verfügung gestellt werden.	3	43%	4	57%	0	0%	0	0%	7	2,43	3
5 Erfahrene und qualifizierte Mitarbeiter müssen ausreichend vorhanden sein.	5	71%	2	29%	0	0%	0	0%	7	2,71	1
12 Die Mitarbeiter beeinflussen das Erscheinungsbild des Teams und müssen sich jederzeit kompetent und angemessen verhalten.	3	43%	3	43%	1	14%	0	0%	7	2,29	5
15 Das Vertrauen der Constituency muss langfristig erworben.	5	71%	2	29%	0	0%	0	0%	7	2,71	1
6 Bei der Constituency muss ein allgemeines Bewusstsein für Sicherheit und die Arbeit des Teams geschaffen werden.	3	43%	3	43%	1	14%	0	0%	7	2,29	5
8 Das Dienstleistungsangebot muss sich an den spezifischen Bedürfnissen der Constituency ausrichten.	4	57%	2	29%	1	14%	0	0%	7	2,43	3
3 Das Dienstleistungsangebot muss reaktive und präventive Aufgaben umfassen.	2	33%	2	33%	1	17%	1	17%	6	1,83	13
9 Die Verbindungen zwischen verschiedenen Dienstleistungen müssen bekannt sein.	1	14%	5	71%	1	14%	0	0%	7	2	9
13 Vorgehensweisen und Dienstleistungen müssen gut dokumentiert werden.	1	14%	6	86%	0	0%	0	0%	7	2,14	8
17 Der Constituency müssen klare Richtlinien zur Berichterstattung gegeben werden.	1	14%	4	57%	2	29%	0	0%	7	1,86	12
10 Zur Messung des Erfolgs und zur Planung zukünftiger Vorgehensweisen müssen Daten gesammelt und analysiert werden (z. B. von bearbeiteten Vorfällen).	0	0%	3	43%	4	57%	0	0%	7	1,43	15
4 Der Informationsfluss zwischen allen Beteiligten muss durch eine umfassende Informationspolitik geregelt ablaufen.	1	14%	5	71%	1	14%	0	0%	7	2	9