Niedersächsisches Ministerium
für Inneres und Sport

CERT-Leistungen für Niedersachsen

Abschlussbericht

Niedersächsisches Ministerium für Inneres und Sport
- Zentrales IT-Management der Landesverwaltung -
Lavesallee 6
30169 Hannover
Tel. (0511) 120-6357
eMail: ZIM@mi.niedersachsen.de

Dieses Dokument wurde erarbeitet von

Dr. Klaus-Peter Kossakowski, Geschäftsführer der DFN-CERT Services GmbH

im Auftrage des Niedersächsischen Ministeriums für Inneres und Sport,
im Rahmen der Konzipierung eines ganzheitlichen und ressortübergreifenden Landeskonzeptes für Informationssicherheit in der Niedersächsischen Landesverwaltung.

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

Für ihre Mitwirkung bei der Erarbeitung der Inhalte danken wir:

- Ministerium für den ländlichen Raum, Ernährung, Landwirtschaft und Verbraucherschutz, Herrn Uwe Holle
- Niedersächsisches Justizministerium, Herrn Holger Sanio
- Polizeiamt für Technik und Beschaffung Niedersachsen, Herrn Heinz Petersen und Herrn Manfred Burkhardt
- Regionales Rechenzentrum Universität Hannover, Herrn Hergen Harnisch
- Universität Hannover -Institut für Wirtschaftsinformatik- , Herrn Robert Pomes
- Informatikzentrum Niedersachsen, Herrn Torsten Sander
- Oberfinanzdirektion Hannover -Steuerabteilung-, Herrn Harald Sandner

1. Auflage September 2006, 60 Exemplare

Druck und Bindung:
Landesvermessung + Geobasisinformation Niedersachsen (LGN)

Stand: 30. Juni 2006

Inhaltsverzeichnis

Management Summary

Innerhalb des Projektes CERT-Niedersachsen sollte untersucht werden, ob die Schaffung einer CERT-Infrastruktur für die niedersächsische Landesverwaltung - im Weiteren als CERT-Niedersachsen bezeichnet – sinnvoll und notwendig ist. Um diese Frage beantworten zu können, wurden verschiedene Fragestellungen untersucht.

Zusammenfassend kommt die Untersuchung zu dem Ergebnis, das ***der Aufbau eines CERT-Niedersachsen empfohlen wird.*** CERTs - im Deutschen besser bekannt als Computer-Notfallteams - sind eine der wichtigsten Neuerungen im Risiko- und Sicherheits-management. Erst bei einer übergreifenden Koordinierung der Reaktion auf Sicherheitsvorfälle im Umfeld der Nutzung von Informationstechnologie (IT-Sicherheits-vorfälle) für die (kritischen) Geschäftsprozesse der Landesverwaltung durch eine zentrale Stelle ergibt sich die angestrebte Vorwarnfunktion. Durch die damit verbundene Verteilung proaktiver Informationen sollen in Zukunft Sicherheitsvorfälle präventiv verhindert oder eintretende Schäden auf ein Minimum begrenzt werden. Somit kann mit einem CERT-Niedersachsen ein deutlicher Beitrag zur Verbesserung der Informationssicherheit und damit zur Optimierung der Geschäftsprozesse in der Landesverwaltung geleistet werden.

Bei dem Aufbau soll ein komplettes Leistungsangebot berücksichtigt werden, denn nur ***zentrale und erweiterte Basisleistungen zusammen bilden ein CERT.*** Basierend auf den nationalen und internationalen Erfahrungen und Erkenntnissen werden diese benötigt, um durch die zentralen Basisleistungen die Grundlage für eine erfolgreiche Funktion zu gewährleisten. Die erweiterten Basisleistungen ergänzen das Angebot durch konkrete Unterstützung bei Angriffen und Vorfällen.

Für den Aufbau wird ein Zeitraum von drei Jahren empfohlen, so dass die langfristige Kontinuität sichergestellt ist, die für eine erfolgreiche Akzeptanz durch die betreute Zielgruppe entscheidend ist.

Wo es möglich und sinnvoll ist, soll auf den Aufbau zusätzlichen Personals verzichtet werden. Aufgaben, die durch externe Dienstleister mit gleicher Qualität erbracht werden können – vor allem die Erstellung von Sicherheitsinformationen und standardisierten Sicherheitsmeldungen (Advisories) – können durch den ***Zukauf von CERT-Leistungen*** erfüllt werden. Auszunehmen sind hiervon Aufgaben, die zentral in der Verantwortung des Landes bzw. der Ressorts verbleiben müssen (z.B. Risiko- und Notfall-Management). Insbesondere darf keineswegs die Kommunikation und Koordination innerhalb der Landesverwaltung an Externe vergeben werden, da die Verantwortung hierfür nicht delegiert werden kann.

Um die Neutralität und Qualität der CERT-Leistungen sicherzustellen, soll eine fachliche, in die bestehenden Strukturen der Landesverwaltung integrierte, „Organisationsstruktur für IT-Sicherheit“ etabliert werden, in die das CERT- Niedersachsen eingebettet ist. Diese Einbettung soll zudem die Anpassung an die spezifischen Anforderungen der Zielgruppe sowie die Kommunikation in die Zielgruppe hinein unterstützen und die ***Qualität und Neutralität des CERT-Niedersachsen sicherstellen***.

Die Präsenz des CERT-Niedersachsen erlaubt die nationale Einbindung in existierende CERT-Gemeinschaften. Hier ist besonders die enge Zusammenarbeit mit CERTs in Deutschland zu betonen, insbesondere mit DFN-CERT und CERT-BUND, mit denen aufgrund der Vernetzung und Rolle ein direkter Informationsaustausch nötig ist. Damit ***stellt das CERT-Niedersachsen einen gleichberechtigten, vertrauensvollen Partner für andere CERTs in Deutschland dar.***

Auf Basis dieser Aussagen und den in diesem Abschlußbericht vorgelegten Planungsempfehlungen wird des Weiteren empfohlen, Aufbau und Pilotierung das CERT-Niedersachsen weiter voranzutreiben.

1 Einleitung

Innerhalb des Projektes CERT-Niedersachsen sollte zunächst untersucht werden, ob die Schaffung einer CERT-Infrastruktur für die niedersächsische Landesverwaltung - im Weiteren als CERT-Niedersachsen bezeichnet – sinnvoll und notwendig ist. Um diese Frage beantworten zu können, wurden folgende Fragestellungen in diesem Dokument untersucht:

1. Welche CERT-Leistungen sollen im Rahmen eines CERT-Niedersachsen durch welche Komponenten erbracht werden? Worin bestehen die Abweichungen von anderen CERTs und wodurch sind solche Abweichungen begründet?
2. Welche Interaktionen sind zwischen den Komponenten eines CERT-Niedersachsen zu etablieren?
3. Welche Vor- bzw. Nachteile haben verschiedene Betreibermodelle, durch die die Leistungen des CERT-Niedersachsen erbracht werden können?
4. Welche relevanten (Infra)Strukturen gibt es im nationalen und internationalen Bereich? Welche sind für das CERT-Niedersachsen relevant?
5. Wie werden die Interaktionen mit anderen relevanten CERTs bzw. (Infra-) Strukturen gestaltet?

Bedingt durch die strategische Bedeutung des CERT-Niedersachsen richtet sich dieser Abschlußbericht direkt an die Leitungsebene sowie an die Projektgruppe, die zukünftig mit Aufbau und Pilotierung beauftragt wird.

Die Grundlage für die Auseinandersetzung mit der Fragestellung überhaupt leitet sich aus verschiedenen Vorarbeiten ab. Da ist zum Einen das „*IT-Landeskonzept*“ zu nennen, welches mit Kabinettsbeschluss vom 19.04.2005 zur „*Strategischen Neuausrichtung des Einsatzes der IT in der Niedersächsischen Landesverwaltung* (Anlage 2 Beschussvorschlag zur Phase II der Verwaltungsmodernisierung) in Auftrag gegeben wurde. Zum Anderen findet sich aber die Anforderung, flexibel auf Angriffe und Vorfälle reagieren zu können auch im „*Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI)*“ der Bundesregierung vom Juli 2005 (den Innenministern und -senatoren der Länder auf der IMK am 08./09.12.2005 in Karlsruhe vom BMI vorgestellt) wieder, der eine Leitfunktion für die weitere Diskussion des Risiko- und Sicherheitsmanagements gerade im Bereich der öffentlichen Verwaltung haben wird.

Dieser Abschlußbericht ist das Ergebnis einer Arbeitsgruppe, an der Teilnehmer verschiedener Ressorts aktiv beteiligt waren:

- Ministerium für Inneres und Sport -Zentrales IT-Management der Landesverwaltung/IT-Sicherheitsmanagement-
- Ministerium für den ländlichen Raum, Ernährung, Landwirtschaft und Verbraucherschutz -IT-Sicherheitsbeauftragter EU-Zahlstelle-
- Polizeiamt für Technik und Beschaffung -IT-Sicherheitsmanagement Polizei-
- Regionales Rechenzentrum Universität Hannover -IT-Sicherheitsbeauftragter-
- Informatikzentrum Niedersachsen -Kompetenzzentrum IT-Sicherheit-

Im Rahmen von acht Projektworkshops wurde von Oktober 2005 bis März 2006 die sich aus dem Auftrag ergebenden Fragestellungen untersucht. Hierzu wurden vor allem Diskussionen über die einzelnen Fragen genutzt, wobei die Ergebnisse im Nachgang zu den Projektworkshops dokumentiert und letztlich in diesem nunmehr vorgelegten Bericht zusammengefasst wurden.

Dieses Dokument gliedert sich in sieben Kapitel. Im folgenden zweiten Kapitel wird zunächst die Ausgangssituation untersucht, ohne dabei bereits auf das Land Niedersachsen im Besonderen einzugehen. Danach wird das Thema der CERT-Infrastrukturen aufgegriffen und in Hinblick auf die internationalen und nationalen Gremien und Aktivitäten beleuchtet.

Bevor im fünften Kapitel auf das Leistungsspektrum für die Dienstleistungen eines CERT eingegangen wird, werden die zu beachtenden Rahmenvorgaben für ein CERT-Niedersachsen diskutiert. Im vierten Kapitel wird auch die notwendige Integration in die „Organisationsstruktur für IT-Sicherheit“ auf Landesebene betrachtet.

Die Betrachtung möglicher Betriebsmodelle, wobei auch der Ressourceneinsatz sowie die Rollen behandelt werden, bildet den Kern des sechsten Kapitels, an das sich eine Ausarbeitung eines empfohlenen Umsetzungsplans für Aufbau, Pilotierung und Überführung in einen Regelbetrieb anschließt. Den Abschluss des Abschlußberichts bildet ein Kapitel mit einer Zusammenfassung und Aufstellung der Empfehlungen.

Gliederung dieses Dokumentes

Kapitel	***Inhalt***
1.	**Einleitung** beschreibt den Grund dieser Voruntersuchung im Rahmen des Projektes „CERT-Niedersachsen“, definiert die Zielgruppe und spannt den Bogen zu strategischen Zielen der Landes- und Bundesverwaltung.
2.	**Ausgangssituation** betrachtet aus der Historie heraus Sinn und Zweck sowie den Mehrwert des zielgerichteten und koordinierten Umgangs mit Sicherheitsvorfällen.
3.	**CERT-Infrastrukturen im nationalen und internationalen Bereich** gibt einen über die Grenzen Europas hinaus gehenden Überblick über die Entwicklung von CERTs und betrachtet die aktuelle Situation in Deutschland.
4.	**Rahmenvorgaben für ein CERT-Niedersachsen** benennt drei Zielgruppen als Nutznießer, beschreibt die Rolle des CERT innerhalb der noch aufzubauenden „Organisationsstruktur für IT-Sicherheit“ sowie die Erfolgsfaktoren für das Betriebsmodell.
5.	**Leistungen des CERT-Niedersachsen** definiert Basisleistungen und erweiterte Basisleistungen des CERT und gibt Auskunft darüber, wie diese erbracht werden müssen und welche Zielgruppen mit welchem Service-Level versorgt werden sollen. Der Begriff des „Vorfalls“ wird als elementarer Begriff für viele Dienstleistungen definiert.
6.	**Betriebsmodelle für das CERT-Niedersachsen** entwickelt aus den drei traditionellen Betriebsmodellen eine Empfehlung für das CERT der Landesverwaltung. Gibt Auskunft über den Bedarf an Ressourcen, deren Abdeckung und behandelt Rollenkonzepte für die Institutionalisierung der Vorfallsbearbeitung.
7.	**Aufbau, Pilotierung und Betriebsübergang** Es werden die notwendigen Folgeaktivitäten zur Fortsetzung des Aufbaus und der Pilotierung in Art und Umfang beschrieben.
8.	**Zusammenfassung und Empfehlungen** gibt die aus der Projektarbeit gewonnenen Ergebnisse in Form von sechs Empfehlungen zu einem CERT-Niedersachsen wieder.
9.	**Literaturhinweise**

2 Ausgangssituation

Das Auftreten von akuten Sicherheitsproblemen und konkreten Vorfällen hat eine lange Geschichte, die nicht mit dem Internet-Wurm im November 1988 begann. Betrachtet man neben der Existenz von Sicherheitslücken auch die Motivation von Personen und Organisationen, diese zu suchen und sofern vorhanden auszunutzen, findet sich ein Spiegelbild der Gesellschaft mit all ihren Problemen im Netz bzw. den Informationsinfrastrukturen. Dies sollte nicht verwundern - eher erstaunt das "Zwiedenken" vieler Menschen, die einerseits im sozialen Umfeld jede Minute mit der Unsicherheit einer Risikogesellschaft leben und andererseits für die Informationsinfrastrukturen nach absoluter und nicht zu erreichender Sicherheit streben. Das sollte nicht so verstanden werden, dass Sicherheit kein erstrebenswertes Ziel sei. Es ist jedoch nicht entscheidend, das ideelle Ziel zu erreichen, sondern sich ihm möglichst weit anzunähern. Akzeptiert man diese Auffassung, muss zwangsläufig das Auftreten von Angriffen und Vorfällen zugestanden werden. Dann gibt es allerdings keine Entschuldigung mehr dafür, sich nicht dementsprechend darauf vorzubereiten.

In der Praxis haben sich seit dem ersten großen Internet-Vorfall, dem sogenannten Internet-Wurm, im November 1988 Computer-Notfallteams (engl.: CERT, Computer Emergency Response Team - heute wird auch über IRTs, Incident Response Teams, oder CSIRTs, Computer Security Incident Response Teams, gesprochen) als eine wichtige Komponente bei der Bewältigung von Sicherheitsvorfällen herausgebildet. Die steigende Bedeutung solcher Teams zeigt sich auch auf politischer Ebene, so gibt es in Deutschland bereits lange ein CERT (ausschließlich) für die Bundesbehörden, das beim BSI angesiedelt ist, und in anderen Bundesländern (Bayern, Nordrhein-Westfalen, ...) gibt es ähnliche Projekte wie in Niedersachsen. Durch diesen grundlegenden Paradigmenwechsel - weg von der Vorstellung, dass es überflüssig sei sich mit Angriffen und Vorfällen zu beschäftigen, weil ein ausreichendes Maß an Sicherheit erreicht wurde, hin zu der Erkenntnis, auf jeden Fall mit Vorfällen zielgerichtet umzugehen - eröffnen sich neue Möglichkeiten.

Anders als bei den traditionellen Maßnahmen der Rechner- und Netzwerksicherheit werden im Rahmen des CERT-Paradigmas Angriffe und Vorfälle nicht ignoriert, sondern vielmehr in den Fokus gerückt. Damit wird das Wissen über Vorfälle für unterschiedliche Zielgruppen (Projektmanager, IT-Koordinatoren, Risikomanagement, IT-Sicherheitsbeauftragte, „Geschäftspartner“, ...) nutzbar gemacht, um weitere Schäden zu begrenzen oder ganz abzuwehren. Angepasste Verfahren machen Vorfälle erkennbar, verringern mögliche Schäden, erlauben erst effiziente Gegenmaßnahmen und tragen so ebenfalls wirksam zu dem globalen Ziel bei, die Zahl von Angriffen und Vorfällen - und damit Schäden für die Landesverwaltung - zu minimieren. Viele Computernotfallteams bieten folgerichtig vorbeugende Informationen über neue Sicherheitslücken oder Angriffsverfahren an. Dazu kommen häufig auch konkrete Hinweise zur Konfiguration von IT-Systemen und Netzwerken zum Schutz vor Angriffen. Nur dadurch können Vorfälle verhindert werden, bevor sie auftreten können.

Viele Organisationen schätzen die Bedeutung dieser Art der Vorsorge immer noch eher gering ein, treten Vorfälle scheinbar doch nicht sehr häufig auf und stellen meist kein großes Problem dar. Aus dieser Perspektive sind Kosten für die Bereitstellung entsprechender CERT-Leistungen vergeudet oder könnten besser in "absichernde" Maßnahmen investiert werden. Nur eine Erfassung und Analyse tatsächlicher Angriffe und Vorfälle kann hier Antworten geben und ein entsprechendes Bewusstsein schaffen.

Alle bisherigen Computer-Notfallteams zeichnen sich dadurch aus, dass sie für einen mehr oder weniger festgelegten Nutzerkreis - ihre Zielgruppe[1] - tätig sind. Ihre Dienste sind nur ein Teil aller Maßnahmen zur Informationssicherheit dieses betreuten Anwenderkreises. Durch ihre Arbeit soll die Fähigkeit gefördert werden, auf "IT Security Incidents" – IT-Sicherheitsvorfälle – effizient, angemessen und schnell reagieren zu können. Was ein Vorfall ist, wird dabei durch die generellen Vorgaben sowie lokalen Leitlinien und Regelungen festgelegt, wie sie auch für die Landesverwaltung derzeit aufgestellt werden.

[1] Der Fachbegriff hierfür ist im Englischen "Constituency". Im Deutschen findet sich oft dafür der Begriff "Klientel", hier erscheint "Zielgruppe" geeigneter zu sein.

3 CERT-Infrastrukturen im nationalen und internationalen Bereich

Über die Jahre haben sich für Außenstehende nicht immer transparente Gemeinschaften gebildet, die viele existierende CERTs einbinden und informell einen Teil der Aktivitäten koordinieren. Neue CERTs müssen in diese Umgebung eingebettet werden, um ein effektives und effizientes Arbeiten zu ermöglichen. Gegenstand dieses Kapitels ist neben der Darstellung der entstandenen Strukturen auch die Bewertung, welche für das CERT-Niedersachsen relevant sein können.

3.1 FIRST

Seit 1992 gibt es FIRST, das internationale Forum von Sicherheits- und Computer-Notfallteams. FIRST fasst mit seinen derzeit circa 190 Mitgliedern die wichtigsten, international agierenden Teams zusammen, wobei die Mitglieder vor allem aus den USA und Europa stammen, obwohl die Teams in Asien und Südamerika immer weiter zunehmen.

Die Aufnahmeprozedur stellt sicher, dass zwei existierende Mitglieder als Mentoren für ein neu aufzunehmendes Mitglied eintreten. Dies soll gewährleisten, dass es sich tatsächlich um ein reales Team handelt, dem durch die Mentoren wesentliche Konzepte von FIRST vermittelt werden:

- Vertraulichkeit der in FIRST ausgetauschten Informationen.
- Freigabe der Informationen für die Weitergabe bzw. Veröffentlichung durch den Urheber.
- Kooperation bei Anfragen von anderen Mitgliedern, um Angriffen oder Vorfällen nachzugehen.
- Kooperation bei der technischen Analyse neuer Angriffswerkzeuge.

Bei der Aufnahme spielen die Möglichkeiten der einzelnen Teams keine große Rolle, so dass durchaus relativ kleine Teams (z. B. 2 Personen für eine Universität) mit großen Teams (z. B. 50 Personen beim CERT Coordination Center) gleichberechtigt nebeneinander stehen. Zentrale Bedeutung hat die Verantwortung für eine Zielgruppe, die quasi durch das Team vertreten wird. Gleichermaßen sind auch Hersteller als Mitglieder zu finden, die damit als Ansprechpartner für die jeweiligen Produkte zur Verfügung stehen.

Für jeden Interessierten zugänglich sind die jährlichen Konferenzen, die sich speziell dem Thema "Incident Response" annehmen und viele Mitglieder zum Erfahrungsaustausch zusammenführen. Sensitive technische Entwicklungen, die vielleicht noch nicht allgemein bekannt sind, sowie Fallstudien werden allerdings nicht im Programm dieser Konferenzen diskutiert. Hierfür werden technische Workshops (Technical Colloquium genannt) veranstaltet, an denen nur Mitglieder teilnehmen können.

Es findet keine zentrale Koordinierung von Aktionen der Mitglieder bei Vorfällen oder neuen Angriffswerkzeugen statt. Dies bleibt der Initiative von ad hoc Arbeitsgruppen überlassen, die sich aus einem gemeinsamen Interesse heraus zusammenfinden. Für die Organisation von Workshops und Konferenzen sowie die Pflege der internen Mailinglisten und die Betreuung der Mitglieder gibt es eine Sekretariatsfunktion, die von einem Dienstleister bereitgestellt wird.

Bisher gab es keine Bemühungen, eine Standardisierung der CERT-Tätigkeiten oder der Koordinierung voranzutreiben. Dies mag sich in Zukunft ändern, da vor allem neue Mitglieder Unterstützung bei dem Aufbau geeigneter Strukturen und Prozesse benötigen.

Der Mitgliedsbeitrag für FIRST ist z. Z. auf USD 1.100,00 jährlich festgesetzt. Es wird eine Aufnahmegebühr von USD 800,00 erhoben.

Bewertung: Grundsätzlich ist jedem größeren Computer-Notfallteam mit internationalen Aufgaben zu empfehlen, eine FIRST-Mitgliedschaft zu prüfen und anzustreben. Aus der Mitgliedschaft ergeben sich vielfältige Möglichkeiten, die für eine Verbesserung der CERT-Leistung und der Betreuung genutzt werden können. Zu betonen sind hier vor allem die Kontakte zu anderen Teams, durch die die Reaktion auf Angriffe und die Aufklärung von Vorfällen erheblich verbessert werden können.

Für das CERT-Niedersachsen ist eine FIRST-Mitgliedschaft nicht notwendig, einige der Vorteile können auch über die Teilnahme an den jährlichen Konferenzen und die Zusammenarbeit mit FIRST-Mitgliedern erreicht werden.

3.2 TF-CSIRT

Informelle Arbeitsgruppen europäischer Teams haben seit 1993 eine lange Tradition. Zunächst wurden diese Treffen von europäischen Forschungsnetzen getragen, später kamen vor allem FIRST-Mitglieder aus dem kommerziellen Bereich hinzu, heute sind quasi alle Arten von Organisationen und Teams vertreten.

Durch die Task Force CSIRT, kurz TF-CSIRT, unterstützt durch TERENA,[2] werden zweimal pro Jahr jeweils zweitägige Treffen organisiert, die grundsätzlich allen interessierten Teams offen stehen.

Innerhalb der TF-CSIRT wurden verschiedene Dienstleistungen und Anforderungen identifiziert, die einerseits eine Verbesserung der Gesamtsituation bedingen würden und andererseits mit begrenzten Mitteln erfüllt werden können. Allerdings nicht durch eine reine Freiwilligen-Leistung. Hieraus entstand das europäische Verzeichnis bekannter Computer-Notfallteams und der diesem Verzeichnis zugrunde liegende Akkreditierungsprozess des „Trusted Introducer“ (siehe folgender Abschnitt).

Des weiteren wird versucht, innerhalb der TF-CSIRT gemeinsame Probleme zu diskutieren und anzugehen, oder aber Entwicklungen von gemeinsamem Interesse voranzutreiben. Einen großen Raum nimmt der Erfahrungsaustausch ein, wobei einzelne Teams über ihre Erfahrungen mit Dienstleistungen, Angriffen, Hilfsmitteln, etc. berichten.

Es gibt keine Mitgliedschaft im formalen Sinne und daher auch keine Mitgliedsbeiträge.

Bewertung: Für Teammitglieder empfiehlt sich die Teilnahme an den Sitzungen der Task Force CSIRT, wenn das Programm relevante und interessante Vorträge oder Diskussionen enthält. Hier muss dann durch (landes-)interne Veranstaltungen dafür gesorgt werden, dass die Erfahrungen und Erkenntnisse an andere Teammitglieder weitergegeben werden.

3.3 Trusted Introducer

Das Verzeichnis akkreditierter CERTs wird von dem so genannten "Trusted Introducer" im Auftrag von TERENA gepflegt. Das Konzept beruht auf einem Prozess, der die Informationen über alle bekannten (als "Listed" bezeichneten) Teams zusammenführt und definiert, wie sich diese akkreditieren lassen können. Alle Informationen sind über die Web-Site http://www.trusted-introducer.nl öffentlich zugänglich und werden ständig aktualisiert.

Durch eine Akkreditierung kann ein Team erreichen, dass es entsprechend eingestuft wird. Hierzu muss das Team eine definierte Menge von Informationen, z. B. Kontaktadressen, Zielgruppe, Dienste, Erreichbarkeit, grundlegende Arbeitsweisen, liefern und zusichern, diese aktuell zu halten, d. h. Änderungen zu melden. Des Weiteren muss sich das Team verpflichten, die vertrauliche Kommunikation mit anderen Teams zu gewährleisten.

[2] Trans-European Research and Education Networking Association, http://www.terena.nl.

Ein Review Board bestehend aus Repräsentanten der akkreditierten Teams überwacht die Arbeit des Trusted Introducers. Die Bearbeitungsgebühr für den Schritt zum akkreditierten Team wurde auf EURO 900,00 festgelegt, der jährliche Beitrag für akkreditierte Teams auf etwas über EURO 1.000,00.

Bewertung: Grundsätzlich ist jedem europäischem Computer-Notfallteam oder größerem Sicherheitsteam zu empfehlen, sich in das Verzeichnis aufnehmen zu lassen. Insbesondere wenn es sich um extern angebotene Dienstleistungen handelt, deren Qualität demonstriert werden soll und bei denen viele Kontakte mit anderen Teams zu erwarten sind, empfiehlt sich eine Einstufung als akkreditiertes Team. Während eine Akkreditierung für das CERT-Niedersachsen nicht zwingend notwendig scheint, sollte jedoch eine Besonderheit – die Registrierung eines so genannten IRT-Objects beim WHOIS-Dienst des Network Coordination Center (RIPE NCC) – Anlass zu weiteren Überlegungen geben. Durch die Zuordnung von IP-Adressen zu CERTs wird es anderen erheblich erleichtert, Informationen über kompromittierte Systeme oder konkrete Angriffe an die Zuständigen weiterzuleiten.

3.4 Situation in Deutschland

International gibt es Mitte des Jahres 2005 ca. 190 CERTs, die in dem Dachverband FIRST organisiert sind. In Deutschland gibt es mehrere Mitglieder, die folgende Zielgruppen betreuen:

- Das DFN-CERT als Einrichtung des DFN-Vereins[3] betreut den Wissenschaftsbereich, hat aber als "ältestes" Team auch noch eine gewisse Koordinierungsfunktion inne.
- Das BSI betreut mit dem CERT-Bund die Bundesverwaltung. In verschiedenen Bundesländern – z.B. Bayern und Nordrhein-Westfalen - gibt es bereits Landes-CERTs
- Das S-CERT hat eine verteilte Struktur von CERTs und Sicherheitsteams innerhalb der Sparkassen-Finanzgruppe etabliert. Die Commerzbank hat ein internes Team aufgebaut.
- Das SIEMENS-CERT ist international und national für die Unternehmen der SIEMENS Gruppe zuständig. Auch die Telekom hat im Rahmen der Konzernsicherheit ein CERT aufgebaut.
- Weitere Teams sind z. B. interne Teams der Universität Karlsruhe und der secunet Security Networks AG sowie das FSC-CERT für den Hersteller Fujitsu-Siemens.

Ohne eine übergreifende CERT-Infrastruktur gibt es keine Koordinierung bei Vorfällen, die viele einzelne Organisationen gemeinsam betreffen. Dieses wurde bei vielen nicht weit zurück liegenden Viren- und Wurm-Angriffen, aber auch weit reichenden Schwachstellen bei Kommunikations-Protokollen und Infrastrukturkomponenten, offensichtlich.

3.5 CERT-Verbund

Seit etwa 1996 wurden informell Treffen deutscher CERTs durch verschiedene Teams organisiert. Diese dienten vor allem der Verbesserung des Kontakts zu neu etablierten Teams und der Diskussion verschiedener Aspekte, die für Deutschland spezifisch sind. Nachdem Ende der 90er Jahre diese Treffen einschliefen, gab es im Sommer 2002 Diskussionen zwischen CERT-Bund und DFN-CERT, die dann mit anderen Teams im

[3] DFN bezeichnet das Deutsche Forschungsnetz, getragen durch den DFN-Verein, Berlin.

August 2002 die Gründung des deutschen CERT-Verbundes zur Folge hatten (www.cert-verbund.de).

Basierend auf einem besonderen Verhaltenskodex (Code-of-Conduct), der einen Rahmen für die verbindliche Zusammenarbeit bietet bzw. auf einer Vertraulichkeitsvereinbarung[4], werden bestimmte Dienstleistungen angeboten. Dafür wird kein Mitgliedsbeitrag erhoben.

Die Kommunikation wird über verschlüsselte, authentisierte Mailinglisten abgewickelt, jährlich werden zwei Arbeitstreffen organisiert und in Arbeitsgruppen werden bestimmte Inhalte übergreifend erarbeitet, z. B. ein „Deutsches Advisory-Austauschformat (DAF)“, oder aktuelle Themen, wie z. B. „Lagebild“, aufgenommen.

Bewertung: Die Teilnahme am CERT-Verbund ist notwendig, da hierdurch die Wahrnehmung einerseits, aber auch die Kommunikation und Kooperation mit anderen CERTs andererseits, erst ermöglicht wird. Es gibt in Deutschland zum CERT-Verbund keine Alternative, die Teilnahme ist unproblematisch und daher quasi zwingend.

[4] Der gebräuchliche Fachbegriff ist „Non-Disclosure-Agreement“. Ein „NDA“ soll minimal die Vertraulichkeit der sicherheitsrelevanten oder Einrichtungen identifizierenden Informationen schützen, die zwischen Teams ausgetauscht werden.

4 Rahmenvorgaben für ein CERT-Niedersachsen

Die Definition der im Rahmen eines CERT-Niedersachsen zur erbringenden CERT-Leistungen wirft drei Fragen auf: welche Dienstleistungen sollen erbracht werden, für wen sollen diese erbracht werden und wie werden diese finanziert?

Nur durch die Verknüpfung der speziellen Eigenschaften und Anforderungen der Zielgruppe mit der Gesamtmenge an möglichen CERT-Leistungen lässt sich ein spezielles Angebot definieren, das auf die Zielgruppe zugeschnitten ist.

4.1 Zielgruppen eines CERT-Niedersachsen

Zielgruppen für die CERT-Leistungen im Rahmen eines CERT-Niedersachsen sind durch drei Kategorien vorgegeben. Für jede der Kategorien gibt es nicht immer scharf definierte Abgrenzungen, d. h. es gibt Überlappungen. Dennoch ist eine getrennte Priorisierung zielführend, wie bereits anhand der folgenden Aufstellung deutlich wird:

- **Primäre Zielgruppe –** Das Hauptaugenmerk – und damit den Nutzen aus den eingesetzten Ressourcen – liegt auf der niedersächsischen Landesverwaltung. Unabhängig von der jeweiligen Rolle, ob IT-Anwender, Sicherheitsbeauftragter, Service-Desk, CallCenter, Betreiber von Fachverfahren oder IT-Betreiber, muss sich die CERT-Leistung auf diese Zielgruppe ausrichten und deren Anforderungen abdecken. Hinzu kommen die IT-Dienstleister, die eine zentrale Rolle für die IT-Infrastruktur der Landesverwaltung einnehmen, z. B. die Betreiber des Landesdatennetzes, Querschnittsanwendungen, Rechenzentren und Betreiber von Zugängen zu öffentlichen Netzen wie dem Internet.
- **Sekundäre Zielgruppen –** Hier sind die primären und sekundären Netznutzer sowie die Nutzer von Fachverfahren einzuordnen. Dies ist insbesondere auch die mittelbare Landesverwaltung, z. B. die Kommunen. Es gibt direkte technische Abhängigkeiten und Schnittstellen, die eine Koordinierung und Kooperation notwendig machen. Dieses gilt in gleicher Weise für Behörden anderer Bundesländer und des Bundes sowie den für diese agierenden IT-Dienstleister (z. B. TESTA-Netz, CNP/ON Polizei), da auch hier technische Schnittstellen vorliegen und wohl in Zukunft noch weiter ausgebaut werden. Letztendlich sind auch andere CERTs (natürlich vor allem aus Deutschland), die zur erfolgreichen Arbeit beitragen können, hier einzuordnen.
- **Tertiäre Zielgruppen –** Durch die Ausweitung von Geschäftsprozessen im Rahmen von eGovernment erfolgt eine Ausdehnung der IT-Infrastruktur und Fachverfahren der Landesverwaltung auf neue Nutzerkreise (Unternehmen, Bürger). Quasi erfolgt eine fast flächendeckende Ausdehnung der Geschäftsprozesse und damit der IT des Landes auch auf die, die nur indirekt von den eGovernment-Angeboten bzw. Fachverfahren profitieren oder daran teilhaben. Obwohl mit einer geringeren Priorität, ist eine Aufnahme dieser Nutzer in die Betrachtung dennoch notwendig, werden sich doch im konkreten Fall (Notfallsituation) auch aus diesem Kreis Anfragen ergeben. Von diesen Nutzern kann nicht verlangt werden, das diese den organisatorischen (Zuständigkeiten, Verantwortlichkeiten) und technischen Zusammenhängen folgen können, wenn es um Sicherheitsprobleme mit IT-Anwendungen geht.

Die IT-Ausstattung der Zielgruppen sowie die Arten des Zugangs zur IT-Infrastruktur des Landes und zu den Fachverfahren ist aufgrund der aufgezeigten großen Spannweite der Zielgruppen sehr heterogen. Sie reicht von kleinen Einheiten mit nicht vorhandener bzw. minimaler IT-Ausstattung (Einzel-PC) bis zu großen Organisationen mit tausenden von

Endgeräten. Im Gegensatz dazu ist der Bereich der Vernetzung durch das Landesdatennetz als zentrale Kommunikationsplattform der Landesverwaltung mit organisatorisch und technisch zentralisierten Schnittstellen zum TESTA-NETZ, Bundespolizeinetz CNP/ON und ins Internet sehr homogen.

Aus dieser Situation leitet sich auch direkt ab, dass das Bewusstsein für Maßnahmen der IT-Sicherheit im Allgemeinen und für CERT-Leistungen im speziellen sehr unterschiedlich ausgeprägt ist. Insgesamt kaum ausgeprägt ist jedoch die sich aus dem CERT-Konzept ergebende Erkenntnis, dass trotz aller Schutzmaßnahmen Vorfälle auftreten werden, obwohl fast jeder zumindest von Erzählungen anderer mit abschreckenden Beispielen vertraut sein sollte. Folglich gibt es in der Praxis innerhalb des Risikomanagements auch kaum Prozesse, die beschreiben, wie mit solchen Ereignissen umgegangen werden sollte.

Die im Rahmen eines CERT-Niedersachsen zu erbringenden CERT-Leistungen sind nur für die Organisationseinheiten und Nutzer relevant, die über eine IT-Ausstattung verfügen. Je umfangreicher diese Ausstattung und damit Abhängigkeit von IT ist, desto nachhaltiger kann die Unterstützung durch das CERT-Niedersachsen genutzt werden. Für die Nutzung ist darüber hinaus die Identifikation verantwortlichen und vertrauensvollen Personals notwendig, das z. B. sicherheitskritische Informationen und konkrete Maßnahmenvorschläge erhalten soll, die dann vor Ort umgesetzt werden können oder müssen. Dieser letzte Punkt nimmt bereits ein weiteres Ergebnis vorweg, denn die Einbeziehung der für IT-Sicherheit bzw. Informationssicherheit zuständigen Rollen, zumindest in der Landesverwaltung, ist unabdingbar. Hier partizipiert das CERT-Niedersachsen von der Umsetzung des zurzeit in einem parallelen Projekt entwickelten Konzeptes zur „Organisationsstruktur für IT-Sicherheit in der Niedersächsischen Landesverwaltung“ und ist nicht selbst Treiber dieser notwendigen Rahmenbedingung. Um so mehr wird es für den Erfolg des CERT-Niedersachsen auf eine effiziente und nachhaltige Integration in diese Organisationsstruktur ankommen.

4.2 Finanzierung eines CERT-Niedersachsen

Die CERT-Leistungen, die im Weiteren detaillierter betrachtet werden, unterteilen sich in zwei Kategorien:

- **Basisleistungen –** Beim CERT-Niedersachsen handelt es sich um Querschnittsdienste, die zwingend eine 1:n Ausrichtung haben müssen. Alle diese CERT-Leistungen dienen der Solidargemeinschaft und deren Interessen und besitzen daher eine Breitenwirkung, wie sie für Infrastrukturdienste charakteristisch ist.
- **Individuelle Zusatzleistungen –** Alles andere, worauf einzelne Nutzer 1:1 individuell zugreifen möchten.

Die Basisleistungen werden folgerichtig zentral zu finanzieren sein. Hier bietet sich aus jetziger Sicht die Bindung an den Zugang zum Landesdatennetz an. Das Angebot von individuellen CERT-Leistungen, z. B. Vor-Ort-Betreuung, Security Audit, Intrusion Detection, Security Consulting, kann dabei nicht enthalten sein.

Die Einbindung dezentraler Komponenten wird überall dort benötigt, wo IT-Infrastruktur und Fachverfahren vorgehalten, angeboten oder betrieben werden. Der Mehrwert liegt darin, dass bei einer koordinierten, präventiven und reaktiven Vorgehensweise bei Notfällen zusätzliche Aufwände bei den Geschäftsprozessen und im IT-Bereich erst gar nicht entstehen oder die unabdingbar negativen Auswirkungen minimiert werden können. Ein CERT macht sich damit mittel- bis langfristig „bezahlt“.

4.3 Die Rolle innerhalb der Organisationsstruktur für IT-Sicherheit

Bedingt durch die Vorgaben der „Organisationsstruktur für IT-Sicherheit“ ist eine Integration des CERTs in diese unabdingbar.[5] Ohne diese kann keine wirkungsvolle Arbeit erreicht werden. Hierdurch sind auch verschiedene Aspekte, die bei einem CERT vor Beginn der Tätigkeiten festgelegt werden müssen, bereits im Fokus der Verantwortlichen. Dabei ist auch der übergeordnete Aspekt eines übergreifenden Risiko-Managements – losgelöst von der IT – zu betonen, da die IT zwar eine zunehmend wichtige Rolle einnimmt, Krisen aber auch ohne Einwirkungen auf oder von IT auftreten können.

Grundsätzlich ist eine Dreiteilung der Aufgaben (und damit Rollen) vorzusehen, wobei sich dieses Dokument vor allem mit der taktischen und operativen Rolle des CERT-Niedersachsen beschäftigt. Die strategische Ausrichtung und die Verantwortung für die übergreifende Integration – auch innerhalb eines Risiko- und Krisen-Managements – verbleibt beim CISO[6], bzw. da diese Stelle nicht vorhanden ist, beim CIO des Landes.

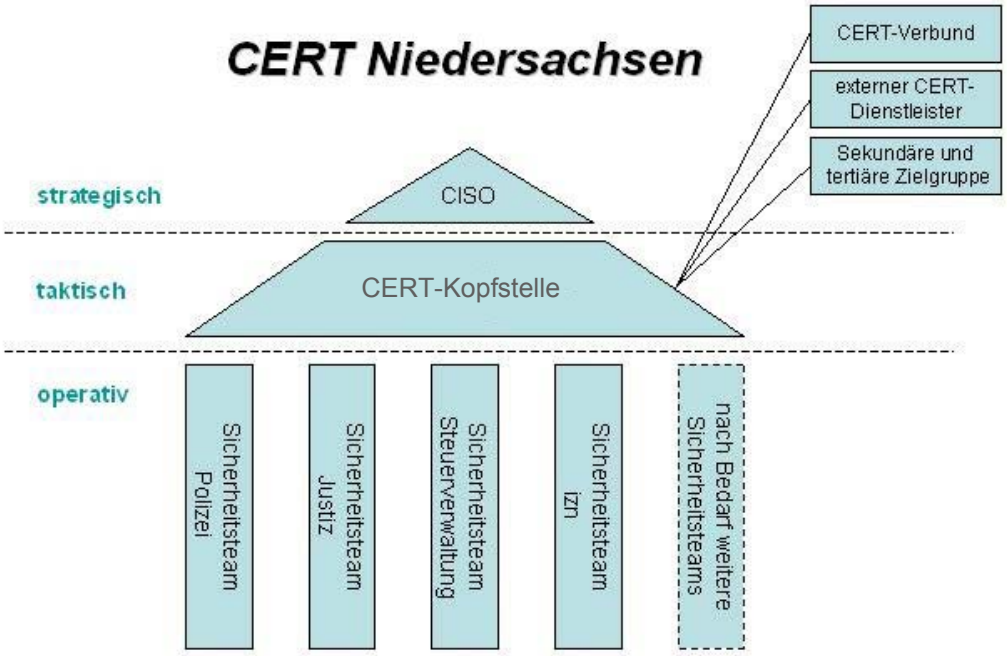

Abbildung 1: Organisationsstruktur des CERT Niedersachsen (Rollen)

[5] Die empfohlene Integration hat auch unabhängig von späteren Änderungen an dem Aufbau oder der Organisation des Landesdatennetzes bestand, da die Verantwortung für alle Sicherheitsvorfälle bzw. das Sicherheitsmanagement insgesamt nicht delegiert werden kann. Also verbleibt diese weiterhin bei den Ressorts bzw. der Landesverwaltung. Nur Leistungen und Versorgung können durch Outsourcing bzw. Outtasking wirtschaftlicher gestaltet werden, Kontrolle, Bewertung und (Risiko-)Management werden weiterhin benötigt.

[6] „Chief Information Security Officer“; Oberste Instanz in einer Organisation, die für den IT-Sicherheitsprozess verantwortlich bzw. für Informationssicherheit zuständig ist.

In Bezug auf das **Berichtswesen** kann fest gehalten werden, das die IT-Sicherheitsbeauftragten und der Landesbeauftragte für den Datenschutz ein starkes Interesse an der CERT-Leistung haben und gleichzeitig am besten beurteilen können, wie gut die Dienstleistung den Erfordernissen entspricht. Daher ist ein Review der CERT-Arbeit durch diesen Kreis vorzusehen. Allerdings wird das CERT allein im Interesse des Landes tätig und ist daher dem CISO (solange dieser nicht benannt ist, entsprechend dem CIO) in Bezug auf Fach- und möglichst auch Dienstaufsicht (wg. Interessenkonflikt Priorisierung der (Personal-)Ressourcen) zu unterstellen.

Bzgl. der **Autorität** ist festzuhalten, dass das CERT zu allererst einmal durch seine Kompetenz und geleistete Arbeit überzeugen muss. Vom Charakter her ist das CERT eher mit einer Feuerwehr zu vergleichen, als mit einer Polizei. Es steht nicht die Ermittlung von Übeltätern im Vordergrund, sondern die Bewältigung technischer Notlagen. Es muss unterstützend, fördernd und beratend tätig sein und eng mit dem Incident Management bezogen auf das momentan in der Landesverwaltung im Aufbau befindliche IT Service Management nach ITIL[7] zusammenarbeiten. Dies wird im Rahmen des weiteren Aufbaus entsprechend zu vereinbaren sein.

Es ist offensichtlich, das ohne eine entsprechende Autorität (z. B. zur Netzabkopplung bei Gefahr im Verzuge, zum Stoppen eines Software-Rollout bei einer nicht zu schließenden Sicherheitslücke, Sperrung unzureichend gesicherter Fachverfahren, ...) bestimmte Sicherheitsziele nicht erreicht werden können. Da jedoch Autorität Verantwortung bedingt, und diese Verantwortung in der jeweiligen Leitungsebene generell sowie bei den IT-Verantwortlichen im jeweiligen Bereich (z.B. Ressorts) verbleibt, ist diese Situation politisch vorgegeben und unabdingbar.

Damit stellt sich das in Abbildung 1 bereits beschriebene Schema eines „virtuellen CERT-Niedersachsen“ im Detail sehr viel unübersichtlicher dar, gibt es doch eine ganze Reihe von Beziehungen, die berücksichtigt werden müssen.

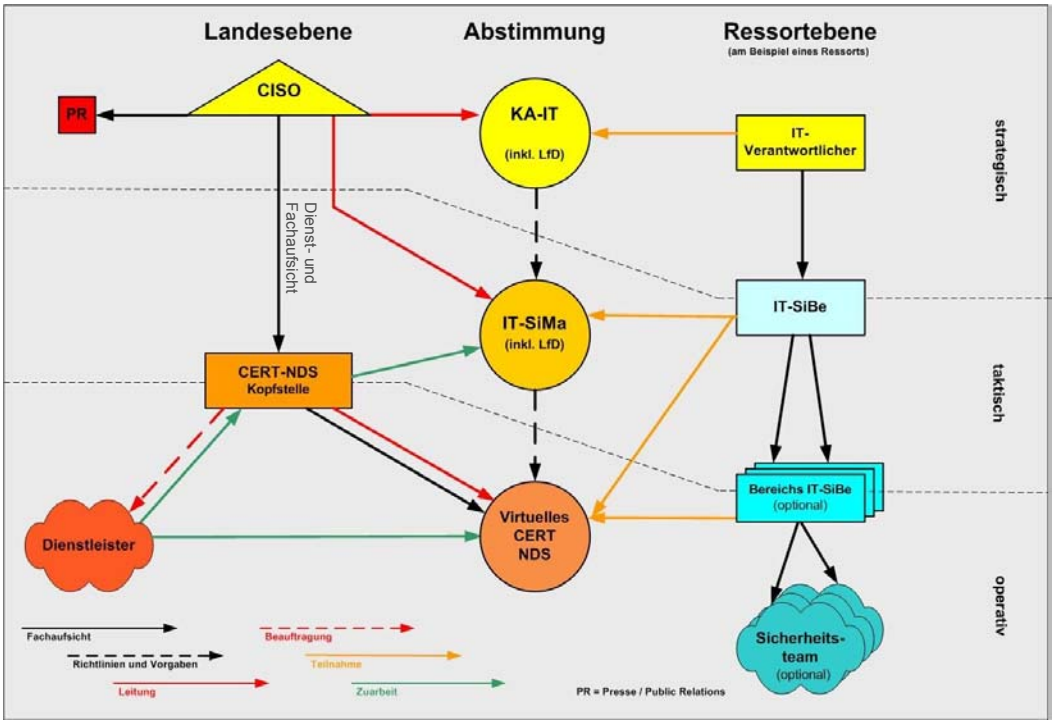

Abbildung 2 : Detaillierte Organisationsstruktur eines CERT Niedersachsen (Rollen)

[7] ITIL (IT Infrastucture Library) ist eine Sammlung von Best Practice Empfehlungen für das IT Service Management des Office of Government Commerce (OGC) der britischen Regierung.

Besonders wichtig ist die unterschiedliche Sichtweise auf die Einstufung „Strategisch“ / „Taktisch“ / „Operativ“, die sich an der Verantwortung der verschiedenen Instanzen festmachen lässt. Während aus Landessicht sich z. B. das CERT-Niedersachsen mit seiner Kopfstelle an der Schnittstelle zwischen taktischen und operativen Geschäft befindet, nimmt es aus Sicht der Ressorts eine rein taktische Rolle ein. Diese Unterschiede führen bei dem Aufbau zu unterschiedlich gestalteten Schnittstellen.

4.4 Erfolgsfaktoren für das auszuwählende Betriebsmodell

Für das Betriebsmodell gibt es eine Reihe von kritischen Erfolgsfaktoren:

- Relativ niedrige Basiskosten für die zentralen Basisleistungen.
- Durch Zukauf von CERT-Leistungen am Markt entfallen der zeitliche und der finanzielle Aufwand für den Aufbau eines entsprechenden Angebots
- Bereits durch die Realisierung der Basisleistungen wird der Zielgruppe eine Hilfe erbracht.

Es wird dabei für die weiteren Planungen, die in Kapitel 7 behandelt werden, von einer Laufzeit von zunächst drei Jahren ausgegangen. Wie die Erfahrung beim Aufbau anderer CERT-Infrastrukturen zeigt, ist dieses ein Zeitraum der mindestens notwendig ist, um die CERT-Leistungen aufzubauen und in der Zielgruppe zu verankern.[8] Ein kürzerer Zeitraum birgt die Gefahr, dass eine Umsetzung in der Zielgruppe nicht erfolgt und somit getätigte Investitionen verloren gehen. Dieser Zeitraum ist im Wesentlichen durch drei Faktoren begründet.

1. Erstens gilt es die (sehr heterogene) Zielgruppe organisatorisch zu erschließen und ihr die Bedeutung der neuen CERT-Infrastruktur zu vermitteln.
2. Zweitens müssen die CERT-Leistungen detailliert formuliert und aufgebaut werden.
3. Und schließlich müssen die neuen CERT-Leistungen so in der Zielgruppe etabliert werden, dass diese in die eigenen Prozesse integriert werden, bzw. dass eigene Ressourcen aufgewendet werden, um konkret mit erhaltenen Informationen sachgerecht umzugehen.

Bevor mit dem Aufbau der eigentlichen CERT-Leistungen begonnen werden kann, sind einige Vorarbeiten erforderlich:

- **Politische Rückendeckung sicherstellen:** Die Rückendeckung und das Mandat für den Aufbau der CERT-Leistungen ist unabdingbar für den Erfolg. Dies muss klar kommunizierbar sein und in der Folge auch kommuniziert werden. Dies beinhaltet eine klare Unterstützung auch in Hinsicht eines angemessen Budgets, dass für die Erbringung der geforderten Leistungen ausreichend ist.
- **Finanzierung sicherstellen:** Es muss das Budget für die Realisierung der Basisleistungen gesichert werden. Dies betrifft alle an der Implementierung Beteiligten, d. h. auch die Ressorts, die Ressourcen für das virtuelle CERT-Team bereitstellen müssen, um damit die Zusammenarbeit zu ermöglichen.

[8] Erfahrungen etablierter Teams haben wiederholt gezeigt, dass von der Bereitstellung einer Meldemöglichkeit von Vorfällen bis zu einer regelmäßigen Nutzung eines CERT ein Zeitraum von ca. neun Monaten vergeht.

- **Zentrale CERT-Kopfstelle festlegen:** Da der zentralen Koordinierung eine bedeutende Rolle im empfohlenen Betriebsmodell zukommt, muss diese Position kompetent und adäquat besetzt werden (Fachkenntnis, Diplomatie, potentielle Akzeptanz in der Zielgruppe). Die Bandbreite der Aufgaben einer zentralen Kopfstelle geht deutlich über die eines klassischen Call-Centers hinaus. Allerdings gibt es teilweise ähnliche Anforderungen, insbesondere unter den Gesichtspunkten Erreichbarkeit und „Single Point of Contact“, so dass eine Zusammenarbeit im Weiteren geprüft werden muss. Zurzeit gibt es keine Organisationseinheit in der Landesverwaltung, in deren Aufgabenbereich die Bereitstellung einer zentralen Kopfstelle eines CERT-Niedersachsen fallen würde.

Nach erfolgreicher Erledigung dieser Vorarbeiten kann mit der Umsetzung des zeitlichen Ablaufplanes und somit mit dem Abschluss der inhaltlichen Ausgestaltung begonnen werden. Konzeption, Spezifikation und Aufbau einzelner Leistungen kann hierzu parallel erfolgen, wie dies auch im Weiteren ausgeführt wird.

4.5 Weitere Aspekte

In Bezug auf die Aufbauorganisation können verschiedene Schlussfolgerungen festgehalten werden, die während der weiteren Umsetzung beachtet werden müssen:

- **Einsatz von einem externen Dienstleister:**

  Um die aufgezeigten Risiken zu vermeiden, müssen externe Dienstleister aufgrund der dort vorhandenen Ressourcen und der bereits aufgebauten Expertise genutzt werden, wenn dieses wirtschaftlich sinnvoll ist. Hierdurch wird auch die Verfügbarkeit der CERT-Leistungen erheblich verbessert. Außerdem können neue CERT-Leistungen rasch integriert werden, aber auch die Ausgliederung nicht mehr benötigter CERT-Leistungen ist möglich.

  Insgesamt werden durch den Einsatz von einem oder mehreren externen Dienstleistern folgende Vorteile erreicht:

  - Eigenes Personal für die ausgelagerten operativen CERT-Leistungen wird nicht benötig.
  - Es wird auf erfahrenes Personal zurückgegriffen.
  - Redundanz wird auf Seiten der Dienstleister sichergestellt.
- **Vorbereitungsphase definieren und klar kommunizieren:**

  Erfahrungen mit anderen CERTs haben gezeigt, dass die Ausrichtung auf die Zielgruppe entscheidend für den Erfolg und die Akzeptanz der Dienstleistung ist. Daher sollen in einer ausreichend dimensionierten Vorbereitungsphase folgende Aufgaben durchgeführt werden:

  - Erschließung der Zielgruppe sowie Überprüfung der Anforderungen nach Initiierung der Diensterbringung.
  - Kontinuierliche Verfeinerung der Dienstleistung mit der Zielgruppe und Definition neuer erweiterter CERT-Leistungen, wo dies notwendig erscheint.
  - Einbeziehung der Schlüsselexpertise für Fachverfahren.

- **Sicherstellung der Neutralität der CERT-Leistung:**

  Bedingt durch die unterschiedlichen Rollen, in die CERT-Mitarbeiter aufgrund ihrer Zugehörigkeit zu einem dezentral aufgestellten virtuellen[9] Team und gleichzeitiger Einbindung in „ihr“ Ressort agieren, kommt der Wahrung der Neutralität eine sehr große Bedeutung bei. Diese muss mit adäquaten Mitteln gewährleistet werden und auch berücksichtigen, dass Konflikte bei den Mitarbeitern auf ein Minimum reduziert werden.

  - Verringerung der Belastung für die Mitarbeiter des virtuellen Teams.
  - Steigerung der Akzeptanz des CERTs insgesamt.

- **Durchführung der CERT-Leistung wird gesichert:**

  Im Sinne der übergeordneten Interessen der Zielgruppe muss die Erbringung der Dienstleistung überwacht werden, um Transparenz, Qualität und eine kontinuierliche Verbesserung sicherzustellen. Adäquate Kontrollmechanismen müssen vereinbart und etabliert werden.

  - Sicherstellung der Neutralität.
  - Sicherstellung des Nutzens des CERTs insgesamt.
  - Möglichkeiten zur Analyse von Schwachstellen und Zielabweichungen.

[9] Mit dem Begriff des “virtuellen” Teams wird ein Team bezeichnet, das in der Organisationsstruktur einen gleichberechtigten Stellenwert zu anderen Teams inne hat, allerdings personell nicht autark ist, sondern (fast) vollständig durch Mitarbeiter anderer Teams besetzt ist.

5 Leistungen des CERT-Niedersachsen

Genauso wie eine zielführende Integration des CERT in die „Organisationsstruktur für IT-Sicherheit“ des Landes gewährleistet sein muss, um seinen Erfolg entfalten zu können, muss dessen Leistungsspektrum passen und den konkreten Bedarf decken. Um dieses zu gewährleisten, wird zunächst ein genereller Überblick über die Einteilung geeigneter CERT-Leistungen gegeben, bevor ein konkreter Vorschlag ausgearbeitet wird.

Ausgehend von der Konkretisierung wird die Frage behandelt, in welchem Maße die identifizierten Nutzergruppen Zugang zu den jeweiligen Dienstleistungen erhalten sollen. In diesem Zusammenhang muss auch ein zentraler Begriff, der des „Vorfalls“, geklärt werden.

5.1 Überblick geeigneter CERT-Leistungen

Als in den 90er Jahren verstärkt CERTs gegründet wurden, entwickelten sich auch die von Ihnen angebotenen CERT-Leistungen. Aufgrund der starken Dynamik in diesem Bereich ist eine vollständige, abschließende Darstellung aller CERT-Leistungen nicht möglich. Trotzdem liegen mittlerweile Klassifikationsschemata vor, z. B. in [Kossakowski 2000]. Dort werden insgesamt 22 CERT-Leistungen definiert, die für CERTs konkret relevant sind und die für die Zusammenstellung eines spezifischen Angebots genutzt werden können. Grundsätzlich können CERT-Leistungen in folgende drei Bereiche unterteilt werden:

- **Reaktive CERT-Leistungen**, die notwendig werden, wenn aktuelle Vorkommnisse oder die Sicherheit betreffend neue Entwicklungen konkrete Maßnahmen erfordern oder eine Unterstützung von Betroffenen notwendig wird
- **Präventive CERT-Leistungen**, die auf die Verbesserung der Sicherheit und der Vermeidung von Vorfällen ausgerichtet sind.
- CERT-Leistungen, die die **Nachhaltigkeit** des Sicherheitsmanagements verbessern, indem Erfahrungen der anderen CERT-Leistungen eingebracht werden.

In der Realität ist jeder CERT-Leistung ein dazugehöriger Dienstprozess zugeordnet, durch den die jeweilige Aufgabe realisiert wird. Die Definition eines Dienstprozesses besitzt dabei ein hohes Abstraktionsniveau, d. h. erst durch die Gestaltung in Subprozesse und die Zuordnung realen Personals und konkreter Verfahren im Rahmen des Aufbaus wird eine angepasste Implementierung möglich. Je nach den zur Verfügung stehenden Möglichkeiten, Ressourcen und Rahmenbedingungen gilt es, effiziente und den Parametern der Anwendungsumgebung möglichst weitgehend angepasste Implementierungen zu identifizieren.

Die Spezifikation eines Dienstangebotes für das CERT-Niedersachsen darf nicht "wissenschaftlich" erfolgen, sondern muss pragmatisch an den tatsächlichen Bedürfnissen der jeweiligen Zielgruppen ausgerichtet sein. Um sich darüber hinaus flexibel auf verschiedene Realisierungskonzepte einstellen zu können, ist es sinnvoll, die Gesamtmenge aller CERT-Leistungen in zentrale Basisleistungen, erweiterte Basisleistungen und individuelle Zusatzleistungen zu unterteilen. Das Zusammenspiel dieser drei Komponenten zeigt die folgende Abbildung.

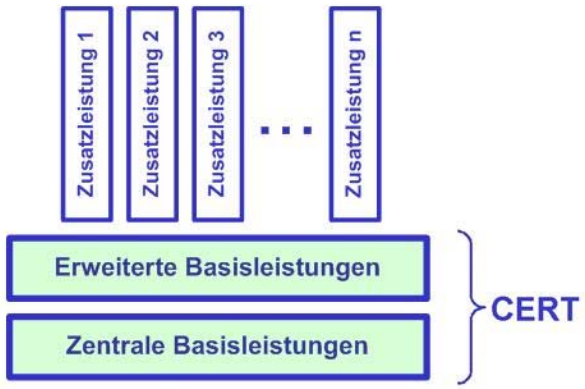

Abbildung 3 : Struktur der Dienstleistungen

Unter **zentralen Basisleistungen** werden alle CERT-Leistungen zusammengefasst, die die notwendige Basis für eine erfolgreiche Etablierung des CERT-Niedersachsen darstellen. Ihre Realisierung ermöglicht es der Zielgruppe, die Sicherheit im eigenen Bereich zu verbessern. Durch die zentralen Basisleistungen alleine wird jedoch noch keine vollständige CERT-Leistung angeboten.

Dies geschieht erst durch die zusätzliche Realisierung der **erweiterten Basisleistungen**. Diese umfassen insbesondere die Unterstützung und Koordinierung bei der Reaktion auf Angriffe und bei der Bewältigung von Vorfällen. Die Gesamtmenge der Basisleistungen (zentrale und erweiterte) stellt somit das (minimale) Angebot eines echten CERTs dar. Je nach Entscheidung der Verantwortlichen können dabei für verschiedene Teilmengen der Zielgruppen unterschiedliche Service-Level definiert werden oder auch der Zugang eingeschränkt oder nur bei Abschluss eines entsprechenden Vertrages gewährt werden.

Darüber hinaus gibt es quasi beliebige individuelle **Zusatzleistungen**, die von einem CERT-Niedersachsen erbracht werden könnten. Welche dieser Zusatzleistungen letztendlich realisiert werden, hängt u. a. von den Anforderungen der Zielgruppe ab und sind damit nicht Gegenstand dieses Konzepts.

Die Zusatzleistungen stellen wünschenswerte Ergänzungen des Basisleistungskatalogs dar. Sie erhöhen den Gesamtnutzen bei den Zielgruppen sukzessiv: je mehr Zusatzleistungen etabliert werden, desto größer ist der Nutzen für die Zielgruppe.

Der Vorteil dieser Vorgehensweise ist in zwei Gesichtspunkten zu sehen, die sich direkt auf das finanzielle Budget auswirken: Zum einen stellt der benötigte Aufwand zur Realisierung der Basisleistungen eine untere Schranke bezüglich der Kosten zum Aufbau eines CERT-Niedersachsen dar: Stehen nur geringere Mittel zur Verfügung, z. B. nur für die zentralen Basisleistungen, so kann der Zielgruppe zwar immer noch eine sinnvolle Hilfestellung zur Verbesserung ihrer Sicherheit angeboten werden, es wird jedoch keine CERT-Leistung im eigentlichen Sinne erbracht. Zum anderen können die nach Aufbau der Basisleistungen zur Verfügung stehenden Ressourcen dynamisch für die Realisierung von Zusatzleistungen verwendet werden, die sich damit in das Gesamtkonzept einpassen. Die Entscheidung, welche Zusatzleistungen realisiert werden sollen, beruht nicht zuletzt auf der Einschätzung der Zielgruppe selbst und den Erfahrungen aus der praktischen Arbeit. Die notwendige Abstimmung innerhalb der Zielgruppe wird wiederum durch die zentralen Basisleistungen,

innerhalb derer die Kommunikation zu der Zielgruppe aufgebaut und gefördert wird, ermöglicht.

Durch diese stufenweise Vorgehensweise gibt es einen Migrationspfad von einem minimalen hin zu einem modular erweiterbaren Angebot.

Eine Darstellung der für das CERT-Niedersachsen zu erbringenden Basis- und Zusatzleistungen wird in den folgenden Abschnitten beschrieben, wobei auch auf weitere Organisationsaspekte eingegangen wird.

Wie oben bereits ausgeführt wurde, sind die Basisleistungen getrennt zu betrachten. Dies wird in den weiteren Abschnitten weiter ausgeführt. Zugleich wird festgelegt, wem die Erfüllung dieser Aufgaben vor allem zuzuordnen sind:

- **Dezentrale Team-Komponenten** – Erbringung vor Ort, innerhalb der Ressorts
- **Zentrale Kopfstelle** – Erbringung muss ressortunabhängig erfolgen, d. h. es werden übergeordnete Aufgaben wahrgenommen
- **Externer CERT-Dienstleister** – Einbindung von Dienstleistern zur Einbringung von Ressourcen und Expertise zu speziellen Fragestellungen sowie zur Einsparung von Kosten. Die Einbindung erfolgt unter Kontrolle der zentralen Kopfstelle[10] (Die Beauftragung von Externen durch Ressorts wird hier nicht betrachtet!)

5.2 Zentrale Basisleistungen

Die zentralen Basisleistungen umfassen insbesondere Aktivitäten, die für die Erschließung der Zielgruppe sowie die Schaffung organisatorischer Strukturen erforderlich sind. Nicht immer sind diese nach außen gerichtet, sondern es handelt sich teilweise um interne Leistungen, die für die Gesamtfunktion notwendig sind. Darüber hinaus wird hierdurch die Bereitstellung eines umfassenden Informationsangebotes sichergestellt und die Basis für die erweiterten Basisleistungen gelegt. Für das CERT-Niedersachsen lassen sich folgende zentrale Basisleistungen (B1-B4) erkennen und weiter unterteilen.

- **B1: Integration des CERT-Niedersachsen in das nationale Umfeld**
  - B1.1 / Zentral: Integration in die nationale CERT-Infrastruktur. Neben der fachlichen und organisatorischen Koordinierung mit nationalen CERTs, beinhaltet dies auch die Teilnahme an die speziellen CERT-Arbeitstreffen mit anderen CERTs aus dem Verwaltungs-, Industrie- und Wirtschaftsbereich.
- **B2: Maßnahmen zur Erschließung der Zielgruppe**
  - B2.1 / Dezentral + Zentral: Zunächst muss das Konzept des CERT-Niedersachsen der Zielgruppe erläutert und bekannt gemacht werden. Dies kann z. B. durch Vorträge oder Rundschreiben erfolgen. Ein Ziel ist es, (insbesondere elektronische) Kommunikationswege zu den Ressorts und verantwortlichen Personen zu etablieren.
  - B2.2 / Dezentral + Zentral: Unter dem Stichwort "Awareness Building" sind Tätigkeiten zu verstehen, die bei der Zielgruppe die (Weiter-) Entwicklung des Bewusstseins für Sicherheitsprobleme allgemein und im Vorfallsbereich im speziellen fördern. Dies muss in enger Abstimmung mit den IT-Sicherheitsbeauftragten erfolgen. Darüber hinaus wird das Verständnis für Arbeiten im Rahmen des CERT-Niedersachsen entwickelt. Zu diesem Zweck ist die Durchführung von Vorträgen und Informationsveranstaltungen erforderlich.

[10] Diese Komponente wird mitunter auch als Kopfstelle bezeichnet.

- o B2.3 / Zentral: Um in direkten Kontakt mit der Zielgruppe zu treten und um die Anforderungen detailliert erarbeiten zu können, sollte einmal pro Jahr eine Informationsveranstaltung durchgeführt werden. Diese ermöglicht es, alle Beteiligten zusammenzubringen und wichtige Fragestellungen ausführlich zu diskutieren.

- **B3: Aufbau und Betrieb einer internen und externen Kommunikations- und Informationsinfrastruktur**
  - o B3.1 / Zentral: Aufbau und Betrieb einer gesicherten technischen Infrastruktur. Als Plattform für die gesamte Kommunikation im Rahmen des CERT-Niedersachsen muss eine technische Basisstruktur geschaffen werden. Dies beinhaltet z. B. den Betrieb von Servern sowie eine Anbindung dieser Systeme an das Landesdatennetz. Gleichzeitig muss diese Infrastruktur so gesichert werden, dass sie möglichen Angriffen, auch aus dem eigenen Bereich heraus, Stand halten kann.
  - o B3.2 / Dezentral + Zentral: : Aufbau und Pflege eines WWW-Angebotes mittels eines Web-Portals. Ein aktuelles, auf die Anforderungen der Zielgruppe zugeschnittenes WWW-Angebot ist ein wichtiger Faktor bei der Realisierung des CERT-Niedersachsen. Dieses Angebot muss neben allgemeinen Informationen auch weiterführende Inhalte enthalten ("Awareness Building"). Als Inhalte sind weiterhin Ankündigungen von Veranstaltungen oder sicherheitsrelevante Kontakte zu Herstellern- und Anbietern von IT sinnvoll. Durch Entwurf eines Logos und einer Tagline können Sichtbarkeit und Einprägsamkeit des CERT-Niedersachsen in der Zielgruppe und – auf eine Untermenge aller Informationen reduziert – in der Öffentlichkeit erhöht werden.
  - o B3.3 / Zentral: Erstellung und Verteilung eines monatlichen Newsletters für die Landesverwaltung im Rahmen des „Awareness Buildings“, der dezentral verteilt wird. Auch hier ist die Zusammenarbeit mit den IT-Sicherheitsbeauftragten unabdingbar. Um die Zielgruppe über aktuelle Entwicklungen im CERT-Umfeld zu informieren, ist die Erstellung und Verteilung eines monatlichen Newsletters sinnvoll.
  - o B3.4 / Dezentral + Zentral: Betrieb einer Kommunikationsinfrastruktur für allgemeine Anfragen. Sobald das CERT-Niedersachsen einen gewissen Bekanntheitsgrad erreicht hat, wird eine Reihe von Anfragen auf diese zukommen. Um damit umzugehen, ist der Aufbau von (zentralen) Telefon-, Fax- und Email-Kontaktmöglichkeiten zu realisieren. Außerdem müssen eingehende Anfragen zeitnah beantwortet werden.

- **B4: Aufbau und Betrieb von CERT-Systemen**
  - o B4.1 / Zentral: Einführung eines CERT-Vorfallsbearbeitungssystems zur verteilten Bearbeitung von Vorfallsinformationen. Auf Basis der Informationen über die Zielgruppe wird eine Datenbank der Ansprechpartner aufgebaut und kontinuierlich gepflegt. Diese kann genutzt werden, um spezifische Informationen direkt an die Betroffenen weiterzuleiten und erlaubt auch die Koordinierung der verteilten Bearbeitung bei Vorfällen.
  - o B4.2 / Dezentral + Zentral: Dokumentation und Statistiken. Die Angabe von Kennzahlen über die erbrachten Leistungen stellt eine wichtige Information über die Entwicklung der Akzeptanz des CERT-Niedersachsen dar. Darüber hinaus ist dies auch eine Möglichkeit zur Darlegung der Aufgabenerfüllung. Allerdings ist die Dokumentation von Einzelfällen viel wichtiger, um so in erheblich detailliertere Art und Weise die gemachten Erfahrungen weiterzugeben.

- o B4.3 / Zentral: Aufbau und Pflege eines internen Expertenverzeichnisses. Durch die Kenntnisse über die Expertise der verschiedenen Mitarbeiter kann die Suche nach einem Experten für einen bestimmten technischen Bereich sehr verkürzt werden. Dies erlaubt vor allem eine effektivere Klärung von Fragen anderer, die ohne die technischen Kenntnisse offen bleiben müssen. Aufgrund der Sensitivität der in diesem Verzeichnis gesammelten Informationen ist der Zugang zu beschränken. In diesem Zusammenhang muss auch die Nutzung einer extern vorhandenen Expertise geregelt werden bzw. über welche Verfahren eine Unterstützung angefordert werden kann.
- o B4.4 / Dezentral + Zentral: Aufbau und aktive Moderation eines Expertenforums für Sicherheitsfragen unter Einbeziehung der IT-Sicherheitsbeauftragten. Zusätzlich zur Beantwortung allgemeiner Anfragen muss ein Forum zur Durchführung sicherheitsrelevanter Diskussionen geschaffen werden. Dies erfolgt sinnvoller Weise durch eine moderierte Mailingliste oder durch ein Web-Angebot, um potentiellen Missbrauch auszuschließen.

5.3 Erweiterte Basisleistungen

Durch die Realisierung der erweiterten Basisleistungen erfolgt eine Erweiterung der zentralen Basisleistungen hin zu einem vollständigen CERT-Dienstleistungspaket. Die folgenden erweiterten CERT-Leistungen (EB1-EB4) sind daher für das CERT-Niedersachsen unbedingt erforderlich. Da sie jedoch auch von den aufgebauten zentralen Basisleistungen abhängen, ist dies bei der Aufbauorganisation zu berücksichtigen.

- **EB1: Sicherheitsbulletins über neue Schwachstellen und Patches, Alarmierung**
  - o EB1.1 / Extern: Durch die Sammlung und Aufbereitung von Informationen über neue Schwachstellen sowie durch Auswertung wichtiger Informationsquellen werden Sicherheitsbulletins erstellt.
  - o EB1.2 / Zentral: Die Zielgruppe sollte dabei die Möglichkeit haben, sich über eine individuell konfigurierbare Schnittstelle die relevanten Informationen regelmäßig und zeitnah zustellen zu lassen.
  - o EB1.3 / Dezentral + Zentral + Extern: Die Sammlung und Auswertung von Informationen erlaubt im Einzelfall die frühzeitige Erkennung von Angriffen oder Gefährdungen mit hohem Bedrohungspotential. Diese Alarme müssen, ähnlich wie Sicherheitsbulletins, verteilt werden.
- **EB2: Unterstützung und Koordinierung bei der Reaktion auf Angriffe und bei der Bewältigung von Vorfällen einschließlich Beweissicherung**
  - o EB2.1 / Dezentral + Zentral: Die Unterstützung beim Umgang mit Angriffen und Vorfällen stellt eine wichtige Dienstleistung dar. Die Erfahrung zeigt, dass viele Angriffe und Vorfälle durch andere Parteien zuerst beobachtet und gemeldet werden. Solche Informationen werden dann an entsprechende Kontakte in den Ressorts weitergeleitet.
  - o EB2.2 / Dezentral + Zentral: Ergänzt werden muss diese Dienstleistung durch die Koordinierung verschiedener Parteien, die von einem Vorfall direkt oder indirekt betroffen sind sowie durch den Informationsaustausch mit anderen CERTs.
  - o EB2.3 / Dezentral: Die dezentral vorliegende besondere Expertise bzgl. der Fachverfahren in den Ressorts erfordert deren Einbindung.

- EB2.4 / Extern: In Einzelfällen kann eine tiefer gehende technische Analyse notwendig werden, in denen eine dezentral und zentral nicht vorhandene Expertise oder eine temporär nicht verfügbare Expertise benötigt werden.
- EB2.5 / Zentral: Vermittlung von internen und externen Kontakten, durch deren Expertise eine konkret durchzuführende Beweissicherung unterstützt werden kann.

- **EB3: Bearbeitung von sicherheitsrelevanten Anfragen, Herstellerkontakte**
  - EB3.1 / Dezentral + Zentral: Die Bearbeitung von sicherheitsrelevanten Anfragen ist eine wichtige Aufgabe. Hierdurch wird zum einen die Verbreitung von Informationen sichergestellt. Zum anderen ergibt sich aus dem Eingang der Fragen eine Art Vorwarnfunktion. Diese erstreckt sich nicht nur auf mögliche Hinweise, die auf Vorfälle hindeuten, sondern auch auf die Interessenslage bei denjenigen, die die Dienstleistung nutzen.
  - EB3.2 / Extern: In Einzelfällen kann eine Beantwortung eine tiefergehende technische Analyse erfordern, die mit den dezentral und zentral verfügbaren Ressourcen oder wegen einer temporär nicht verfügbaren Expertise nicht geleistet werden können.
  - EB3.3 / Dezentral: Identifikation und Dokumentation von Schwachstellen und Problemen mit Produkten der jeweiligen Hersteller sowie die Übernahme der direkten Kommunikation bzgl. der Fachverfahren in den Ressorts.
  - EB3.4 / Zentral: Bündelung der Herstellerkommunikation bei besonders schwerwiegenden Sicherheitsproblemen bzw. ungenügender Reaktionen der betroffenen Hersteller.
- **EB4: Training und Schulung für die Vorfallsbearbeitung**
  - EB4.1 / Zentral + Extern: Zum Verständnis der immer komplexer werdenden Sicherheitslösungen ist eine konkrete Wissensbasis erforderlich. Die Erfahrungen aus der Praxis eines CERTs können zur Verbesserung der fachlichen Kenntnisse genutzt werden, indem genau diese Orientierung vorgenommen wird. Die praktische Auseinandersetzung mit Angriffswerkzeugen, realen Angriffen und nachgestellten Situationen kann die zu fordernde Realitätsnähe herstellen.

Bei den meisten CERT-Leistungen ist eine Definition eines Service-Level nur schwer möglich. Klar ist jedoch, dass die Qualität der CERT-Leistungen angepasst werden muss, wenn die Menge der Anfragen zunimmt und die zur Verfügung stehenden Ressourcen fix sind. Wenn dies nicht geschieht, kann für eine Übergangszeit zwar durch starkes Engagement des Personals die Leistung aufrechterhalten werden, danach allerdings wird eine Fortführung unter den gleichen Bedingungen nicht mehr möglich sein. Dieses könnte, wenn es nicht rechtzeitig erkannt und adressiert wird, den Nutzen des CERT insgesamt und damit die Ziele der IT-Sicherheit bzw. Informationssicherheit gefährden.

5.4 Zugang zu den Dienstleistungen für verschiedene Nutzergruppen

Über die Dienstleistungen eines CERT-Niedersachsen muss weitflächig informiert und kommuniziert werden. Dieses wird dazu führen, dass auch außerhalb der eigentlichen primären und sekundären Zielgruppen (siehe Abschnitt 4.1) die Existenz eines CERT-Niedersachsen bekannt wird.

Insgesamt wird bereits die Existenz – ungeachtet der genauen Inhalte und Informationen, die verfügbar gemacht werden – bestimmte Erwartungshaltungen sowohl bei den

Zielgruppen als auch außerhalb dieser wecken. Hiermit muss von Anfang an sensibel, aber nachdrücklich, umgegangen werden, um negative Auswirkungen auf das CERT bzw. seine öffentliche Wahrnehmung zu vermeiden. Das Hauptaugenmerk muss dabei auf den Zugang zu den Dienstleistungen gerichtet werden, denn wenn etablierte Zugangsbeschränkungen nicht eingehalten werden, führt dies zu zwei Phänomen:

1. Ein „Auffressen“ verfügbarer Ressourcen für nicht übertrage Aufgaben
2. Ein „Gewohnheitsrecht“ über die zusätzlich genutzten Dienstleistungen

In der Vergangenheit ist dieses Phänomen bereits bei anderen Teams zu beobachten gewesen, die sehr viele Schwierigkeiten hatten, im Nachhinein diese Problematik wieder in den Griff zu bekommen.

Um dieses von Anfang an zu vermeiden, muss die Kommunikation der Zielgruppen mit den zugänglichen Dienstleistungen von Anfang an konsistent erfolgen.[11] Insbesondere durch Veranstaltungen generell und alle Maßnahmen zur Bewusstseinsbildung werden Informationen über das CERT-Niedersachsen in die Breite getragen. Dem entsprechend ist hier von Anfang an besonders sorgfältig vorzugehen.

Aus Sicht der Dienstleistung sind einige besonders problematisch in Hinblick auf eine Nutzung durch Personen, die nicht den definierten Zielgruppen zuzuordnen sind. Dies sind prinzipiell alle erweiterten Basisleistungen:

- EB1: Sicherheitsbulletins über neue Schwachstellen und Patches, Alarmierung
- EB2: Unterstützung und Koordinierung bei der Reaktion auf Angriffe und bei der Bewältigung von Vorfällen einschließlich Beweissicherung
- EB3: Bearbeitung von sicherheitsrelevanten Anfragen, Herstellerkontakte
- EB4: Training und Schulung für die Vorfallsbearbeitung

Bzgl. der unterschiedlichen Zielgruppen muss zusätzlich definiert werden, mit welchem Maß diese jeweils bedient werden sollen. Bereits die Einteilung in drei Klassen deutet hier eine Ungleichbehandlung an, die klar die Belange der primären Zielgruppe in den Vordergrund stellt.

Dienstleistung	Primär	Sekundär	Tertiär
EB1: Sicherheitsbulletins	**Ja**	**Ja,** für Netznutzer und Fachverfahren	**Nein,** außer es sind Landesinteressen im Rahmen des eGovernment betroffen
EB2: Reaktion	**Ja**	**Ja,** für Netznutzer und Fachverfahren, sofern das Land Niedersachsen	**Nein,** evtl. Information über EB1

[11] Bei den Mitarbeitern von CERTs kommt es manchmal zu der Fehleinschätzung, dass freie Ressourcen “in der Zwischenzeit” ja sinnvoll anderen von Angriffen Betroffenen zugänglich gemacht werden könnten. Dies steht einer langfristig stabilen Diensterbringung und gezielten Ausrichtung auf die ausgewählten Nutzergruppen im Wege. Die nicht durch Angriffe oder Vorfälle abgerufenen Ressourcen sind in andere Bereiche einzubringen, um dort Verbesserungen zu schaffen und vorbeugend wirken zu können.

		betroffen ist	
EB3: **Anfragen**	**Ja**	**Ja,** für Netznutzer und Fachverfahren, sofern das Land Niedersachsen betroffen ist	**Nein**
EB4: **Training**	**Ja**	**Nein**	**Nein**

5.5 Definition eines Vorfalls aus Landessicht

Ausgangspunkt für die Definition eines Vorfalls ist immer das zugrunde liegende Rahmenwerk, in diesem Fall die „Leitlinie für Informationssicherheit in der niedersächsischen Landesverwaltung“. Dort ist festgehalten:

> *„Diese Leitlinie ist das strategische Basis-Dokument für Informationssicherheit in allen Behörden und Institutionen der niedersächsischen Landesverwaltung für durch Informationstechnologie unterstützte Geschäftsprozesse. Sie ist Grundlage für alle Maßnahmen und Handlungen innerhalb der Geschäftsprozesse und der für diese erforderlichen Informationssicherheit.“* (Kapitel 2, Ziele)
>
> *„Reaktion: Beim Auftreten von Gefährdungen für Informationen in den Geschäftsprozessen ist durch geeignetes, geplantes Vorgehen zu reagieren. Durch rechtzeitige Erkennung der Gefährdungen sowie vorbereitete und geprobte Reaktion auf diese, ist eine negative Beeinträchtigung der Sicherheitsziele in den Geschäftsprozessen zu verhindern bzw. auf ein Minimum zu reduzieren.“*
> (Kapitel 3, Prinzipien)

Für die weitere Betrachtung auch relevant ist, wer als Täter in Betracht kommt. Hierbei müssen auch Innentäter berücksichtigt werden, da diese vielfältige Möglichkeiten haben, die IT-gestützten Geschäftsprozesse negativ zu beeinflussen. Hierbei müssen eben auch bewusste Handlungen berücksichtigt werden, die von Innentätern begehen werden können.

- **Innentäter:**
  - Verstoß gegen Gesetze / Straftaten, die mit Hilfe der IT durchgeführt werden
  - Verstoß gegen Dienstvorschriften
  - Missbrauch / Nicht zweckbestimmte Nutzung von Systemen / Unberechtigte Nutzung von Systemen und IT-Dienstleistungen
  - Bewusste Umgehung von Sicherheitsvorschriften, z. B. unverschlüsseltes Senden von Informationen über das Internet oder an nicht vertrauenswürde Empfänger
  - Andere (fahrlässige) Handlungen, einschließlich solcher aus mangelnder Kenntnis, Unerfahrenheit und solcher aus Überforderung
- **Außentäter:**
  - Verstoß gegen Gesetze / Straftaten, die mit Hilfe der IT durchgeführt werden
  - Fahrlässige oder vorsätzliche Handlungen

Besonders anschaulich kann die Einschätzung, ob ein Vorfall vorliegt, anhand von Beispielen kommuniziert werden. Basierend auf den Diskussionen der Projektarbeit handelt es sich bei den folgenden Ereignissen um Vorfälle, ohne dass die angegebene Reihenfolge selbst bereits eine Bewertung darstellen soll oder der Anspruch erhoben wird, dass die Aufzählung vollständig ist. Für die Praxis ist daher die ständige Aktualisierung einer Liste mit plakativen Beispielen in Form einer Checkliste vorzusehen:

- **Verlust oder Einschränkung der Vertraulichkeit**
  - Diebstahl eines Systems oder Datenträgers
  - Aufzeichnung von auf dem Netzwerk übertragene Daten durch entsprechende Programme
  - Kopieren von internen Daten bzw. Informationen auf Datenträger und Entfernung desselben aus dem Gebäude (bei Innentätern desgleichen, allerdings ohne einen dienstlichen Zweck)
  - Weitergabe von einem Passwort oder anderen Authentisierungstoken
  - Bereitstellung von vertraulichen Daten bzw. Informationen auf öffentlich zugänglichem System / Versenden personenbezogener Daten / Versenden von Geschäftsinformationen
  - Einsehen von Daten, die nicht für den Leser bestimmt sind
- **Verlust der Integrität oder Authentizität**
  - Nutzung einer fremden SignaturCard oder eines fremden Authentisierungstoken
  - Manipulation / Unbefugtes Ändern von Daten
  - Verteilung von Schadsoftware (Viren etc.)
- **Verlust der Verbindlichkeit**
  - Vertragsrelevante Daten werden auf einem System bewusst oder unbewusst manipuliert
  - Informationen werden unter Vortäuschung einer falschen Identität verteilt
  - Übertragene Informationen werden auf dem Weg zwischen Absender und Empfänger geändert
- **Einschränkung oder Verlust der Verfügbarkeit**
  - Ungeplante Ausfälle und nicht durch SLA abgesicherte Ausfälle von sicherheitsrelevanten Systemen oder Kommunikationswegen
  - Systematische Ausfälle / Beeinträchtigungen von technischen Komponenten mit Breitenwirkung (z. B. Festplatten)
- **Angriffe mit weiteren Folgeschäden**
  - „Social Engineering“[12]
  - Angriffe auf die IT von Dritten, insbesondere Geschäftspartnern
  - Feststellung einer neuen / bekannten Sicherheitslücke in Systemen
  - Technische Angriffe auf Systeme / Sabotage / Hacking / Ausnutzung von neuen oder bekannten Sicherheitslücken

[12] Ursprünglich der Versuch eines Hackers, im sozialen Umfeld des Opfers Informationen für Angriffe aufzuspüren. Auch Telefonanrufe als angeblicher Service-Techniker, der für eine Reparatur Details zum Netzwerk braucht. Bei E-Mail-Würmern bedeutet Social Engineering, menschliche Schwächen der Empfänger auszunutzen, um sie zu einer Aktion zu verleiten.

Eine ganze Reihe von Ereignissen können unabhängig von einer straf- oder privatrechtlichen Bewertung als ohne vorrangige Bedeutung für das CERT-Niedersachsen eingestuft werden. Dies bedeutet nicht, dass solche Vorfälle zu ignorieren seien, sondern dass die Verantwortung hierfür über die bereits heute entwickelten Verfahren (Personalverantwortung) wahrgenommen wird. Hierzu zählen unter anderem:

- Persönliche Belästigung eines Kollegen mit Email, sexuelle Belästigungen, Mobbing per Email
- Private Emails bekommen und versenden, private Internetnutzung insgesamt
- Weiterleitung von dienstlichen Emails an eine private Email-Adresse
- Herunterladen von Hackertools, Computer-Spielen, Bildschirmschonern, ...
- Nicht vorhandener Feuerlöscher oder andere nicht eingehaltene Brandschutzmaßnahmen
- Diebstahl von Teilen der PC-Arbeitsplatzausstattung (nur Systemkomponenten ohne Datenträger / Datenspeicher)
- Diebstahl einer Installations-CD für dienstlich beschaffte Software
- Verstoß gegen lizenzrechtliche Bestimmungen bei dienstlich beschaffter Software (zusätzliche Installation auf privatem PC)

Insgesamt müssen diese hier zunächst informell aufgeführten Kategorien in einer übergreifenden, allgemeingültigen Einteilung zusammengeführt werden. Hierbei gibt es zwei grundlegende Dimensionen, die anhand der Einteilung auch die eindeutige Klassifikation erlaubt:

1. **Die Dimension der Kritikalität –** Durch den Unterarbeitskreis IuK der Kommission IuK-Sicherheit des Arbeitskreises II „Innere Sicherheit“ der Ständigen Konferenz der Innenminister und -senatoren der Länder [13] wurde ein Schema zur „Einstufung der Kritikalität von Ereignissen“ (Vorfällen) entwickelt. Das Schema beschreibt den maximal möglichen Schaden, der auf Basis der jeweils aktuell verfügbaren Informationen anzunehmen ist. Es besteht aus drei Kritikalitätsstufen und sollte für das IT-Sicherheitsmanagement der niedersächsischen Landesverwaltung als Ausgangsbasis sinngemäß eingeführt werden. Die Kritikalitätseinschätzung muss im Sinne eines KVP aufgrund neuer Erkenntnisse angepasst werden können.
   - Stufe A (hoch)
   - Stufe B (mittel)
   - Stufe C (niedrig)

   Das entsprechende Kritikalitätsschema der Polizei Niedersachsen ist diesem Dokument als Anlage A beigefügt.
2. **Die Dimension des Ausmaßes –** Abhängig davon, welche Zielgruppen in welchem Ausmaß betroffen sind, stellt das Ausmaß eine weitere Dimension dar. Hierdurch kann Ereignissen Rechnung getragen werden, die zwar von der Kritikalität eher unbedeutend sind, jedoch in der Masse ein ebenso großes Schadenspotential besitzen können. Auch hier muss aufgrund neuer Informationen eine Neubewertung und Einstufung möglich sein.
   Unterschieden werden kann hier anhand der folgenden Klassen:

[13] Vorgestellt auf der 5. Sitzung der „Kommission IuK-Sicherheit“ am 21./22.11.2005 unter TOP 7 (Informations- und Eskalationsprozesse); derzeit bei den Polizeien der Länder in Erprobung

- Landesinfrastruktur (Ressortübergreifende Gesichtspunkte, Verantwortung liegt beim CIO, Betrieb durch das IZN)
- Fachanwendungen (Verantwortung beim Ressort, Betrieb zentralisiert beim IZN bzw. innerhalb eines Ressorts)
- Ressortinfrastruktur (Verantwortung beim Ressort, Betrieb verteilt aufgrund vielfältiger Aspekte und betrieblicher Erfordernisse)
- Lokale Infrastruktur (Verantwortung bei Organisationseinheiten innerhalb der einzelnen Ressorts, Betrieb zentralisiert oder verteilt aufgrund der betrieblichen Erfordernisse)

Bedingt durch die zwei Dimensionen besteht nun die Notwendigkeit, alle Vorfälle, die initial bezüglich dieser beiden Dimensionen eingeschätzt werden müssen, in eine Rangfolge abzubilden. Hierzu werden anhand der folgenden Tabelle die Prioritäten verteilt:

Kritikalität / Ausmaß	Hoch	Mittel	Niedrig
Landesinfrastruktur	**1**	**2**	**3**
Fachanwendungen	**2**	**3**	**4**
Ressortinfrastruktur	**3**	**4**	**5**
Lokale Infrastruktur	**4**	**5**	**6**

Durch die Rangreihenfolge kann nun durch die CERT-Kopfstelle die bevorzugte Reihenfolge der Abarbeitung direkt ermittelt werden. Da davon auszugehen ist, dass die Zahl der gleichzeitig als „offen“ geführten Vorfälle nicht sehr hoch sein wird, hat diese Einstufung nur in Zeiten eine Bedeutung, wo zahlreiche Vorfälle zu Zielkonflikten bei der Zuordnung von Ressourcen führen können.

Um besonderen Einschätzungen Rechnung zu tragen, können individuell angepasste Einstufungen in die Bestimmung der Rangreihenfolge mit einbezogen werden. Beispiele hierfür sind situationsbezogenene Einschätzungen (Niedersachsentag mit Besuch des Ministerpräsidenten) oder eine grundlegende Bedeutung von Fachanwendungen (Personalmanagement oder das Haushaltswirtschaftssystem) oder eines Ressorts (Polizei mit Aufgaben zur Wahrung der inneren Sicherheit).

Insgesamt können übergreifende Leitlinien für Vorfälle definiert werden, die unabhängig von der genauen Einschätzung eines bestimmten Angriffs oder Vorfalls Gültigkeit besitzen:

- Vorfälle mit rein lokalem, isoliertem, Charakter sind nicht Aufgabe des CERT-Niedersachsen, auch wenn im Einzelfall Know-How zur Verfügung gestellt oder dieses angefragt wird. Die Verantwortung verbleibt im Ressort oder bei der verantwortlichen Organisationseinheit.
- Da die Lokalität von Vorfällen schwer abzuschätzen ist, muss eine vertrauensvolle Zusammenarbeit den möglichst weitgehenden Informationsaustausch ermöglichen. Hierdurch muss sichergestellt werden, dass die verfügbaren Informationen in jedem Fall zu den verantwortlichen Personen vor Ort gelangen.

- Um den Übergang zu einem übergreifenden (insbesondere dem nicht-IT gebundenen) Krisenmanagement zu erlauben, muss auch hier der entsprechende Informationsaustausch etabliert sein und die Schnittstellen zwischen allen Beteiligten verbindlich vereinbart werden.
- Das CERT-Niedersachsen wird in Bezug auf Angriffe und Vorfälle immer dann aktiv, wenn:
    - Eine Außenwirkung gegeben ist
    - Ein Vorfall übergreifenden Charakter hat
    - Ein Ressort überfordert ist
    - Informationen mit Relevanz für die primäre Zielgruppe verfügbar werden

6 Betriebsmodell für das CERT-Niedersachsen

Um die in dem vorherigen Kapitel ausgeführten CERT-Leistungen anzubieten, bedarf es einer erfolgreichen Implementierung. Ein wichtiger Faktor für den Erfolg sind die Ressourcen, die durch die Implementierung gebunden werden und dementsprechend bereitgestellt werden müssen. Es gibt aber auch andere Faktoren, die über Erfolg und Misserfolg entscheiden und daher nicht außer Acht gelassen werden dürfen. Dies betrifft insbesondere die Modelle für den Betrieb, durch die die grundlegenden Faktoren mitbestimmt werden.

6.1 Auswahl eines geeigneten Betriebsmodells

Traditionell gibt es drei Betriebsmodelle für die Realisierung von CERT-Leistungen wie beim CERT-Niedersachsen:

1. Zentralisierte Erbringung aller CERT-Leistungen.
2. Dezentralisierte Erbringung aller CERT-Leistungen.
3. Kombination von Modellen 1 und 2 (dezentralisiertes Team mit zentraler Kopfstelle).

Es gibt bisher keine Aktivitäten für eine übergreifende Koordinierung von IT-Sicherheitsvorfällen, so dass es in dieser Hinsicht keinen Betrieb gibt, der entsprechend der Anforderungen ausgebaut werden könnte. Somit stellen sich verschiedene Fragen, die nun betrachtet werden sollen, bevor eine Empfehlung gegeben wird:

- **Es gibt beim zentralen IT-Dienstleister kein eigenes CERT-Team:**

  Das Informatikzentrum Niedersachsen (IZN) als zentraler IT-Dienstleister der Landesverwaltung hat eine herausragende Bedeutung für die IT-Sicherheit bzw. Informationssicherheit insgesamt. Die Sicherheitsaufgaben werden wahrgenommen und mit dem jeweils zuständigen Betriebspersonal erbracht, allerdings hat es bisher nicht die Notwendigkeit gegeben, ein Sicherheitsteam oder CERT aufzubauen. Eine übergeordnete und übergreifende, über die Grenzen der Landesverwaltung hinweg reichende, Koordination bei ressortinternen und -übergreifenden Sicherheitsvorfällen gehört jedoch nicht zum originären Aufgabenbereich des IZN.
- **Es gibt keine zentrale Instanz, die die Interessen <u>aller</u> der Zielgruppe zuzuordnenden Einheiten bei Sicherheitsvorfällen auf praktisch-technischem Niveau vertritt:**

  Die Verantwortung für die Geschäftsprozesse, das Risikomanagement und damit auch für Informationssicherheit in der Landesverwaltung obliegt den Ressorts. Deshalb kann es keine zentrale Vertretung geben. Auch wenn durch die neue IT-Organisation und den entsprechenden Dokumenten zur Informationssicherheit eine übergeordnete Sicht des Landes definiert und formuliert wird, verbleiben viele Aufgaben und Einzelregelungen auch aufgrund des „Ressort-Prinzips“ bei den Ressorts. Auch wenn das IZN auf vielfältige Art und Weise in den operativen Betrieb – und damit in die IT-Sicherheit – eingebunden und beteiligt ist, ergibt sich damit nicht automatisch eine zentrale CERT-Rolle. Gegen eine gedanklich naheliegende Übertragung der zentralen CERT-Rolle an die Polizei spricht deren Auftrag zur Strafverfolgung. Dadurch besteht generell eine große Befangenheit, die der für ein CERT notwendigen, vertrauensvollen Zusammenarbeit mit deren Zielgruppen entgegenwirken würde, oder diese im schlimmsten Fall sogar verhindert. Außerdem kann keine Vertraulichkeit bzgl. behandelter Vorfälle zugesichert werden.

- **Bestimmte CERT-Leistungen/Aufgaben müssen vor Ort erfüllt werden:**
  Aufgrund der räumlichen Verteilung der Landesverwaltung muss bei einer rein zentral ausgerichteten Erbringung ein Vor-Ort-Einsatz aus wirtschaftlichen Gründen stark eingeschränkt werden. Ebenso ist die Abdeckung der notwendigen Expertise, gerade bei den Fachverfahren, zentralisiert nur sehr schwer darzustellen und erfordert viele Ressourcen.
- **Es gibt kein entsprechendes Dienstleistungsangebot des DFN-CERTs:**
  Das DFN-CERT als neutraler Koordinator im Wissenschaftsnetz erbringt verschiedene Dienstleistungen für alle DFN-Anwender, die allerdings deutlich von dem für das CERT-Niedersachsen entwickelten Spektrum abweichen. Im Gegensatz zu der Ausrichtung des CERT-Niedersachsen, das die spezifischen Probleme der Landesverwaltung adressieren muss, ist die DFN-Dienstleistung auf alle DFN-Anwender gleichermaßen ausgerichtet.[14]

Abschließend als Bewertung ist damit festzustellen, dass niemand sich in einer Position befindet, die die Übernahme der Zuständigkeit und Verantwortung für die Zielgruppe der Landesverwaltung als „natürlich“ oder „zwingend“ erscheinen lässt. Allerdings wurde bei den Überlegungen während der Projektarbeit, ob ein zentraler IT-Dienstleister wie das IZN aufgrund der Unabhängigkeit der Ressorts (Organisationshoheit, Fachverfahren) und deren unterschiedlichen kritischen Geschäftsprozessen alleine die Versorgung mit CERT-Leistungen übernehmen kann, dessen Abhängigkeit von der Zuarbeit und Einbindung der Ressorts bei der Gesamtproblematik wiederholt angesprochen. Ebenso werden auf technischer Ebene und in Hinblick auf eine Vor-Ort-Unterstützung Schwierigkeiten zu erwarten sein, wenn es keine dezentralen Komponenten gibt.

Die Ausführungen zeigen weiter, dass für den Aufbau des CERT-Niedersachsen keine "klassische" Form der Implementierung alleine als Erfolg versprechend anzusehen ist. Anhand der Ausführungen kann allerdings das dritte Modell Erbringung durch ein „dezentralisiertes Team mit zentraler Kopfstelle“ als Erfolg versprechend eingeschätzt werden. Dieses Modell wird dem entsprechend auch für den Aufbau empfohlen.

6.2 Ressourcen für das CERT

Die Kosten eines CERTs sind natürlich nur nach Abschluss einer Feinplanung und den Verhandlungen mit möglichen Leistungserbringern genau zu erfassen, aber insgesamt gibt es verschiedene Kostenpunkte, die zu betrachten sind.

Innerhalb der Kopfstelle werden 2 Vollzeitstellen, allerdings bei anteiligen Vollzeitstellen[15] auf 3 Personen verteilt, benötigt. Für Administrationsaufgaben werden im Bereich der IT eine 0,5 Vollzeitstellen und im Bereich der (Büro-)Organisation sowie für das Management und Berichtswesen weitere 0,5 Vollzeitstellen benötigt.

Es gibt verschiedene Betrachtungsweisen, in wieweit die Aufgaben auf mehrere Personen verteilt werden sollte bzw. kann. Generell gilt:

- Verteilung erleichtert die Identifikation geeigneten Personals und Abdeckung verschiedener Know-How-Bereiche

[14] Das Angebot spezifischer Dienstleistungen durch das DFN-CERT ist damit nicht ausgeschlossen, allerdings ist dies nicht im normalen DFN-Angebot enthalten, bedingt weitere Kosten und bedarf konkreter vertraglicher Ausgestaltungen.

[15] Zu einem nicht wesentlichen Anteil werden andere Aufgaben wahrgenommen. Hierbei sind Interessenskollisionen (Zielkonflikte) auszuschließen.

- Zentralität erleichtert die alltägliche Kooperation und Übernahme von Aufgaben, die von anderen erledigt werden sollte
- Vollzeit konzentriert Prioritäten und Expertise
- „Teilzeit“ ermöglicht Verteilung der Expertise, bedingt aber Konflikt zwischen verschiedenen Aufgaben

Innerhalb der Ressorts bzw. nachgeordneten Behörden werden für den operativen Betrieb personelle Ressourcen benötigt. Dies betrifft insbesondere die folgenden Aufgaben:

- Bearbeitung von Vorgängen
- Abdeckung der Erreichbarkeit
- Beteiligung am Expertenverzeichnis
- Ad-hoc Besetzung im Rahmen des Krisenmanagement

Weitere signifikante Kostenpunkte sind:

- **Infrastruktur**
  - Büro
  - Telekommunikation
  - Internet
  - Hotline / Helpdesk
- **Externer Dienstleister**
  - 24 / 7 Erreichbarkeit gegenüber 8 / 7 oder 8 / 5
  - CERT spezifische Leistungen, z. B. Sicherheitsmeldungen
- **Weitere Kosten**
  - Web-Auftritt im Landes-CMS, Logo
  - Reisekosten für Teilnahme CERT-Verbund etc.
  - Weiterbildung / Ausbildung des CERT-Personals
  - Honorare für Experten im Rahmen der Bewusstseinsbildung („Awareness Building“)
  - Beiträge für Mitgliedschaften, Gebühren
  - Fachliteratur
  - Broschüren für Marketing

Insbesondere die Werkzeugunterstützung muss an dieser Stelle erwähnt werden, da diese weit reichende Bedeutung für die tägliche Arbeit hat. Hierbei ist zu einem großen Teil die Skalierbarkeit der gewählten Lösung zu beachten, da u. U. größere Nutzerzahlen berücksichtigt werden müssen. Daher werden hier die Werkzeuge auch in Bezug auf die zu berücksichtigenden Nutzerkreise diskutiert:

- **Öffentliche Nutzerkreise**
  - Mailinglisten
  - CMS für den Webauftritt
- **Nutzer aus den Landesbehörden**
  - Mailinglisten
  - Alarmierungsmöglichkeiten, auch ohne Landesdatennetz bzw. Internet

- Verteiler für Security Advisories
- CMS für den Webauftritt
- Forum innerhalb eines Webauftritts

- **CERT-interne Nutzung**
  - Mailinglisten
  - Alarmierungsmöglichkeiten, auch ohne Landesdatennetz bzw. Internet
  - Interner Dateiserver
  - Vorgangs- und Vorfallsbearbeitung
  - PGP zur Kommunikation in CERT-Foren

6.3 Rollenmodell für beteiligte Organisationseinheiten

Die zentrale Rolle im CERT-Niedersachsen wird durch die Kopfstelle erbracht, die im Rahmen der Fach- und Dienstaufsicht direkt dem CISO[16] unterstellt sein muss. Die Aufgaben der Kopfstelle lassen sich in verschiedene Bereiche einteilen, dieses sind:

- CERT-Dienstleistungen
- Supportaufgaben des technischen Betriebs
- Unterstützende Aufgaben des Managements

Bei den CERT-Dienstleistungen zeichnet die Kopfstelle direkt verantwortlich für die folgenden Aufgaben. Dies deutet bereits an, dass der Betrieb durch Dritte erfolgen kann, ohne dass dies in Bezug auf die Verantwortlichkeit Unterschiede machen würde:

- **EB1: Sicherheitsbulletins**
  - EB 1.2: Verteilung
  - EB 1.3: Auswertung
- **EB 2: Reaktion**
  - EB 2.1: Unterstützung bei Angriffen und Vorfällen
  - EB 2.2: Koordinierung der von einem Vorfall betroffenen Parteien
  - EB 2.3: Unterstützung bei Sicherheitsproblemen mit Fachverfahren
  - EB 2.5: Vermittlung von Kontakten
- **EB 3: Anfragen**
  - EB 3.1: Sicherheitsrelevante Anfragen
  - EB 3.3: Probleme mit Produkten und Fachverfahren
  - EB 3.4: Bündelung der Herstellerkommunikation
- **EB4: Training und Schulung**
  - EB 4.1: Erweiterung der Wissensbasis

Auch technische Betriebsaufgaben gehören zu den Aufgaben der Kopfstelle:

- **B3: Infrastruktur**

[16] Solange kein CISO („Chief Information Security Officer“) beim Land Niedersachsen bestellt ist, verbleibt die Zuständigkeit für das IT-Sicherheitsmanagement implizit beim CIO („Chief Information Officer“).

  - o B 3.1: Technische Infrastruktur
  - o B 3.2: WWW-Angebot
  - o B 3.3: Newsletter
  - o B 3.4: Kommunikationsinfrastruktur
- **B4: CERT-Systeme**
  - o B 4.1: Vorfallsbearbeitungssystem
  - o B 4.3: Expertenverzeichnis

Auch Managementaufgaben sind der Kopfstelle zuzuordnen, die sich direkt aus der ausgezeichneten Position sowie der Außenvertretung ergeben:

- **B1: Integration nationales Umfeld**
- **B2: Erschließung der Zielgruppe**
  - o B 2.1: Kommunikationswege
  - o B 2.2: „Awareness Building“
  - o B 2.3: Veranstaltungen
- **B4: CERT-Systeme**
  - o B 4.2: Dokumentation und Statistik
  - o B 4.4: Expertendiskussion

Wie bereits oben ausgeführt wurde, muss unter wirtschaftlichen Gesichtspunkten auch die Unterstützung durch Dritte berücksichtigt werden. Aufgrund der verschiedenen Fakten der heutigen Lage bietet sich dies bzgl. folgender Leistungen konkret an. Wie zu ersehen ist, verbleibt die Versorgung der Nutzergruppen alleine in der Verantwortung der Kopfstelle, die herangezogenen Dritten können prinzipiell für die Nutzer transparent durch andere Dienstleister ersetzt werden, so dass hier weit reichende Handlungsoptionen erhalten bleiben:

- **EB1: Sicherheitsbulletins**
  - o EB 1.1: Erstellung
- **EB2: Reaktion**
  - o EB 2.4: Technische Analyse
- **EB3: Anfragen**
  - o EB 3.2: Technische Analyse
- **EB4: Training und Schulung**
  - o EB 4.1: Erweiterung der Wissensbasis

Für die Einbindung der Ressorts bzw. anderer beteiligter Organisationseinheiten im CERT-Niedersachsen und koordiniert durch dessen Kopfstelle bietet es sich an, abhängig von dem Maß an möglicher Unterstützung folgende Rollen zu differenzieren. Die Einstufung, als welche Rolle die Integration in das CERT erfolgt, hat unmittelbare Auswirkungen auf die Erwartungshaltung bzgl. Antwortzeiten und zugesichertem Aufwand, der vorgehalten wird.

Abhängig von den weiteren Feinplanungen, Entscheidungen auf Landesebene und den Absprachen mit den Organisationseinheiten kann dieses Rollenmodell auch benutzt werden, um z. B. eine bestimmte Unterstützung in ausgewählten Organisationseinheiten festzuschreiben.

Drei verschiedene Rollen sind zu betrachten, die im Weiteren näher erläutert werden:

- Computer-Notfallteam
- Sicherheitsteam
- Systemverantwortlicher

Für die Einrichtung eines eigenen Computer-Notfallteams spricht vor allem die Institutionalisierung der Dienstleistungen innerhalb des Verantwortungsbereichs einer Organisationseinheit. Ausgehend von der Erkenntnis, dass unabhängig von Vorfällen auf Landesebene auch lokal auftretende Ereignisse in gleicher Weise bearbeitet und behandelt werden müssen, bietet sich die Einrichtung eines Computer-Notfallteams allerdings nur dann an, wenn bereits verschiedene Personen(-gruppen) intern mit IT-Sicherheit befasst sind und es übergreifende Koordinierungsaufgaben gibt, die wahrgenommen werden müssen. Diese Koordinierung und die damit verbundene Außenvertretung macht ein Computer-Notfallteam zum „natürlichen“ Partner für die Einbindung in das CERT-Niedersachsen.

Sicherheitsteams agieren sehr viel enger in den operativen Betrieb eingebunden und sind tagtäglich mit IT-Sicherheitsaufgaben beschäftigt. Sie sorgen für die IT-Sicherheit auf operativ / taktischer Ebene entsprechend der Vorgaben. Die Reaktion auf Vorfälle und Angriffe gehört damit bereits zu ihren Aufgaben, wenn ihr Aufgabenbereich unmittelbar betroffen ist (z. B. Angriff auf die Firewall). Um die Integration in das CERT-Niedersachsen zu gewährleisten, kann dies in diesem Fall durch die Erweiterung eines bereits bestehenden Dienstes geschehen. Dieses Vorgehen ist wirtschaftlich, erfordert aber, die Prioritäten innerhalb des Teams neu zu regeln. Die neu hinzukommenden Koordinierungsfunktionen müssen eine mindest gleichrangige Priorität wie die Erledigung der bisherigen Aufgaben erhalten. Dies ist durch die Zuweisung neuer Ressourcen oder entsprechende Anpassungen zu gewährleisten.

In den Organisationseinheiten ohne eigenes Computer-Notfallteam oder Sicherheitsteam verbleiben die IT-Sicherheitsaufgaben bei den Systemverantwortlichen. Analog zu den Sicherheitsteams gehören damit auch alle Angriffe und Vorfälle innerhalb des Verantwortungsbereichs bereits zu dessen Aufgaben, ohne dass allerdings für die Koordinierung oder eine Unterstützung des CERT-Niedersachsen Ressourcen bereit stehen würde. Bei den Systemverantwortlichen handelt es sich daher auch um den schwierigsten hier zu betrachtenden Fall, da es sich hierbei in der Regel um bereits stark ausgelastete Personen handelt, die nicht einfach von anderen Aufgaben befreit werden können, um diese zusätzlichen „Mehraufgaben“ zu übernehmen. Daher sind die Erwartungen bzgl. dieser Rolle nur sehr eng zu fassen.

Mittel- und Langfristig kann die Situation, dass Systemverantwortliche mit IT-Sicherheitsaufgaben über Gebühr befasst sind, nur zur Schaffung eines Sicherheitsteams führen, durch das Expertise und Kapazität gleichermaßen bereitgestellt werden können.

Für die Erwartungshaltung gilt gemäß obigen Ausführungen, dass die Art des Teams das Service-Level bestimmt.

- Hohe Erwartungen: Computer-Notfallteam
- Angemessene Erwartungen: Sicherheitsteam
- Niedrige Erwartungen: Systemverantwortlicher

Aufgrund der Erkenntnisse des Projekts richtet sich das Hauptaugenmerk auf die Integration von Sicherheitsteams, da der Bedarf für ein eigenes Computer-Notfallteam, also CERT, in der Regel bei den Ressorts und anderen Organisationseinheiten nicht gegeben ist.

- **Allgemein hohes Service-Level –** Die folgenden Dienstleistungen gehören aufgrund der Rolle bereits zu den Standardaufgaben und werden mit hoher Priorität ausgeführt:
  - EB 1.3: Auswertung
  - EB 2.1: Unterstützung bei Angriffen und Vorfällen
  - EB 2.2: Koordinierung betroffener Parteien
- **Für eingesetzte Produkte und betriebene Fachverfahren –** Aufgrund der vorhandenen Expertise und der tagtäglichen Beschäftigung können die folgenden Dienstleistungen ohne hohen Zusatzaufwand erbracht werden:
  - EB 2.3: Unterstützung bei Sicherheitsproblemen mit Fachverfahren
  - EB 3.1: Sicherheitsrelevante Anfragen
  - EB 3.3: Probleme mit Produkten und Fachverfahren
- **Zusammen mit der CERT-Kopfstelle –** werden im Rahmen der Koordinierung und der dazu notwendigen Absprachen folgende Dienstleistungen mit erfasst:
  - B 2.1: Kommunikationswege
  - B 2.2: „Awareness Building“
  - B 3.2: WWW-Angebot
  - B 3.4: Kommunikationsinfrastruktur
  - B 4.2: Dokumentation und Statistik
  - B 4.4: Expertendiskussion

Ein sich aus der Leitlinie für Informationssicherheit ergebender Gesichtspunkt, der abschließend betrachtet werden muss, ist die Einbindung des IT-Sicherheitsbeauftragten (IT-SiBe). Dieser trägt gemäß der Leitlinien die Verantwortung für den „IT-Sicherheitsprozess“ als Ganzes auf taktischer / strategischer Ebene. Damit nimmt er auch für – vorhandene – Sicherheitsteams die Fachaufsicht wahr und bestimmt die Vorgaben für die Vorgehensweisen. Hierzu muss er die Abstimmung mit der für ihn zuständigen Leitungsebene bzw. den Verantwortlichen der Geschäftsprozesse suchen und koordinieren.

Aufgrund der hohen Bedeutung für die IT-Sicherheit und die Ausrichtung des CERT-Niedersachsen ist eine enge Kooperation mit den IT-SiBe sowohl im Einzelnen als auch als Gruppe aufzubauen und zu festigen. Daher wurde bereits in der Betrachtung der zu leistenden Integration das Konzept entwickelt, eng mit dem sich u.a. aus den obersten IT-SiBe der Ressorts zusammensetzenden IT-Sicherheitsmanagement Team (IT-SiMa) zusammenzuarbeiten.

7 Aufbau, Pilotierung und Betriebsübergang

Für den erfolgreichen Aufbau des CERT-Niedersachsen werden mit diesem Abschlußbericht wichtige Erfolgsfaktoren vorgegeben – insbesondere Abschnitt 4.3 stellt konkrete Anforderungen an die Unterstützung innerhalb der „Organisationsstruktur für IT-Sicherheit“ vor – die vorab sicherzustellen sind. Ausgehend von der Annahme, dass die dazu notwendigen Maßnahmen umgesetzt wurden, stellt sich dann die Frage, wie weiter vorzugehen ist. Wie es die Überschrift bereits suggeriert, muss dies in aufeinander aufbauenden Teilschritte – Aufbau, Pilotierung und Betriebsübergang – erfolgen und nach einer überschaubaren Übergangszeit zu einem stabilen Dienstleistungsangebot führen. Jeder dieser Teilschritte kann als Einzelprojekt angesehen werden, allerdings ist eine strikt sequentielle Bearbeitung abzulehnen. Vielmehr wird eine überlappende Herangehensweise empfohlen, in denen explizit Reviews verankert sind, die der Anpassung der Konzepte an veränderte Anforderungen dienen. Nur so kann sichergestellt werden, dass insgesamt ein tragfähiges, leistungsfähiges sowie vor allem den aktuell gültigen Anforderungen entsprechendes Dienstleistungsangebot mit Ende des Betriebsübergangs entstanden ist.

Eine schematische Sicht soll diese überlappende Herangehensweise sowie die Platzierung der Reviews für die insgesamt veranschlagte Zeit von 36 Monaten verdeutlichen.

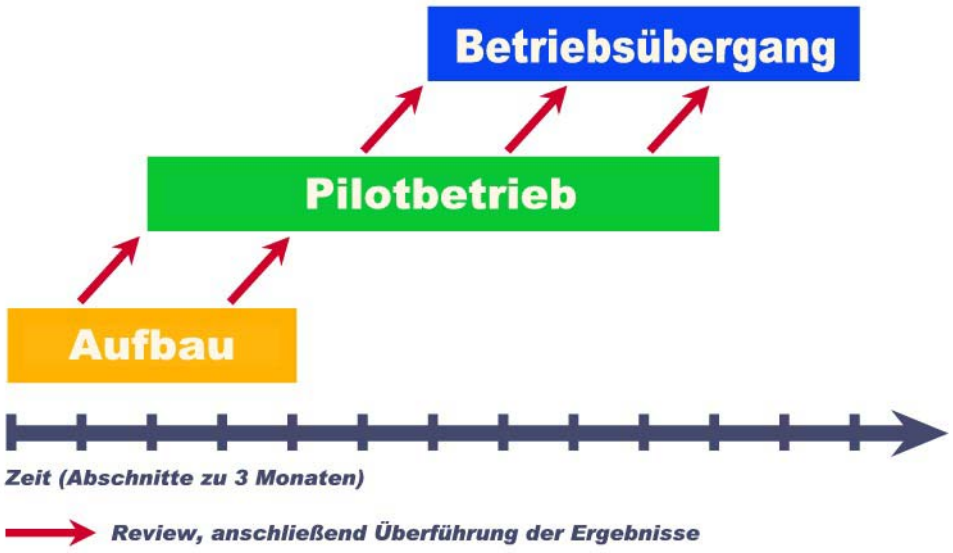

Abbildung 4 : Struktur der Projektphasen

Mit Beginn der Phase „Aufbau“ kann mit der Vorbereitung und Umsetzung der weiteren inhaltlichen Ausgestaltung begonnen werden. Konzeption, Spezifikation und Aufbau einzelner Leistungen kann hierzu parallel erfolgen. Hierfür ist die Phase „Pilotbetrieb“ vorgesehen, die die Ergebnisse der vorherigen Phase und die Ergebnisse der Reviews einschließt. Nachdem einzelne Dienstleistungen erfolgreich im Pilotbetrieb erbracht wurden, erfolgt in der letzten Phase der „Betriebsübergang“ sowie die sukzessive Überführung der pilotierten Dienstleistungen in einen Regelbetrieb. Wiederum werden hierzu die Ergebnisse der vorherigen Phase sowie die Resultate der Reviews verwendet. In den drei folgenden Abschnitten werden die drei Phasen detaillierter erläutert und dargestellt.

7.1 Phase Aufbau (Monat 1 bis 6)

Innerhalb dieser Phase müssen die notwendigen Grundlagen für die erfolgreiche Umsetzung des Konzepts gefestigt und detailliert werden. Dies betrifft insbesondere die Ausgestaltung der Basis- und erweiterten Basisdienstleistungen.

In der Tabelle am Ende dieses Abschnitts sind alle Ergebnisse und Meilensteine zusammengefasst, die in der Projektplanung erfasst werden müssen. Um die Darstellung übersichtlich zu halten, wurden jeweils Zeiträume von drei Monaten betrachtet.

Bei den meisten CERT-Leistungen schließt sich daran eine kontinuierliche Fortführung dieser Arbeiten an (z. B. Pflege der Informationssysteme, Erschließung der Zielgruppe, Beantwortung von Sicherheitsfragen, Erstellung der Newsletter, usw.). Diese Fortführung ist jedoch bereits der Phase „Pilotierung“ zuzuordnen. Insofern sind initial sehr viele Entwicklungsaufgaben notwendig, die mit zunehmendem Projektverlauf abnehmen. Allerdings ist die Konzeption der erweiteter Basisleistungen erst nach 12 Monaten abgeschlossen.

Zeitpunkt	Neu zu beginnende Arbeiten bzw. Status
Beginn des ersten Monats	- Konzeption und Aufbau der gesicherten technischen Infrastruktur (Web-Server, Mailinglisten) - Konzeption der erweiterten Basisleistungen beginnt - Aufbau von Kontakten zu nationalen CERTs und Positionierung im nationalen Bereich - Institutionalisierung eines "Roundtables" mit IT-Sicherheits-beauftragten und Sicherheitsteams der primären Nutzergruppe mit regelmäßigen, halbjährigen Workshops mit Fachvorträgen - Erstellung von Informationsmaterial über die allgemeinen Ziele und Nutzergruppen des CERT-Niedersachsen
Nach 3 Monaten	- Web-Server und Mailinglisten sind aufgebaut - Weitere Konzeption und Ausbau der gesicherten technischen Infrastruktur um die Funktionen für Vorfallsbearbeitung, etc. - Zentrale Kopfstelle ist per Mail, Telefon, Fax erreichbar - Auf dem Web-Server sind allgemeine Informationen vorhanden - Die Dienstleistung EB1 ist als eine der ersten erweiterten Basisleistungen konzeptioniert, so dass mit der Auswahl eines externen Dienstleisters für EB1.1 begonnen werden kann - Erstellung von zielgruppenoptimiertem Informationsgehalt mit Erklärungen der Basisleistungen und wie diese in Anspruch genommen werden können

Zeitpunkt	Neu zu beginnende Arbeiten bzw. Status
Nach 6 Monaten	- Ergebnisse des ersten Reviews liegen vor und werden für das Kick-Off der Pilotierung verwendet (→ Phase 2). Anpassungen an den Konzepten, sofern dies notwendig ist, werden vorgenommen. - Ein externer Dienstleister für die Erbringung der Dienstleistung EB1.1 wurde ausgewählt. Dieser Dienst geht in die Pilotphase über (→ Phase 2) - Konzept für die erweiterte Basisdienstleistung EB2 liegt vor, die Auswahl eines externen Dienstleisters für EB2.4 kann beginnen - Auf dem Web-Server sind für auf die Zielgruppen abgestimmte, nützliche Informationen vorhanden - Die Kontakte im nationalen Bereich sind etabliert und die Positionierung ist abgeschlossen, Pflege der Kontakte erfolgt innerhalb der Phase 2
Nach 9 Monaten	- Konzept für die erweiterte Basisdienstleistung EB3 liegt vor, die Auswahl eines externen Dienstleisters für EB3.2 kann beginnen - Ein externer Dienstleister für die Erbringung EB2.4 wurde ausgewählt. Dieser Dienst geht in die Pilotphase über (→ Phase 2) - Das Angebot für die Zielgruppen auf dem Web-Server wird ausgeweitet, Überführung in die Pilotphase ist abgeschlossen - Vorbereitung des „1. CERT-Niedersachsen Workshops“ ist abgeschlossen
Nach 12 Monaten	- Konzept für die erweiterte Basisdienstleistung EB4 liegt vor, mögliche Externe als Unterstützung im Rahmen von EB4.1 sind identifiziert (→ Phase 2) - Ein externer Dienstleister für die Erbringung EB3.2 wurde ausgewählt. Dieser Dienst geht in die Pilotphase über (→ Phase 2) - Durchführung des „1. CERT-Niedersachsen Workshops“ war erfolgreich - Nachbereitung zum „1. CERT-Niedersachsen Workshop“ wird mit allen Beteiligten durchgeführt und die Ergebnisse werden zur Verbesserung der zukünftigen Organisation protokolliert (→ Phase 2) - Bericht zu dem zweiten Review liegt schriftlich vor und kann für die weitere Arbeit herangezogen werden (→ Phase 2)

7.2 Phase Pilotbetrieb (Monat 7 bis 30)

In den ersten drei Quartalen werden sukzessive die verschiedenen erweiterten Basisleistungen in die Pilotierung übernommen. Hierzu werden aus der Phase 1 die Konzepte, Prozesse und die ausgewählten Dienstleister übergeben.

Nach der ersten Phase zeichnet sich die zweite Phase durch die ca. halbjährlich durchgeführten Reviews aus, die der Anpassung und stetigen Verbesserung der Leistungen dienen.

Neben den neu zu beginnenden Arbeiten und Konzepten gibt es eine Reihe von Standardaufgaben, die eher dem Betrieb bzw. den Routinetätigkeiten zuzuordnen sind.

Diese werden deshalb im Weiteren nicht mehr in den folgenden Tabellen, sondern hier einmalig aufgeführt:

- Zentrale Kopfstelle ist per Mail, Telefon, Fax erreichbar
- Der Kontakt zu nationalen und internationalen CERTs wird gepflegt. Das CERT-Niedersachsen ist aktiver Partner im CERT-Verbund
- Die gesicherte technische Infrastruktur ist verfügbar – Web-Server, Mailinglisten, Vorgangsbearbeitungssystem – und wird betrieben
- Informationsmaterial über die allgemeinen Ziele und Nutzergruppen des CERT-Niedersachsen wird gepflegt und im Zuge der Aufnahme neuer Dienstleistungen ständig erweitert
- Der zielgruppenoptimierte Informationsgehalt mit Erklärungen der Basisleistungen und wie diese in Anspruch genommen werden können wird gepflegt und im Zuge der Aufnahme neuer Dienstleistungen ständig erweitert
- Fortführung der "Roundtables" mit IT-Sicherheitsbeauftragten und Sicherheitsteams der primären Nutzergruppe mit regelmäßigen, halbjährigen Workshops mit Fachvorträgen (jeweils einmal in den Monaten 7-9, 13-15, 19-21, 25-27 und 31-33)

Zeitpunkt[17]	Neu zu beginnende Arbeiten bzw. Status
Beginn des siebten Monats	- Kickoff für die Pilotierung im Rückgriff auf die Konzepte aus Phase 1 sowie den Ergebnissen des ersten Reviews - Aufnahme der erweiterten Basisleistung EB1 in Kooperation mit dem ausgewählten externen Dienstleister für EB1.1
Nach 9 Monaten	- Aufnahme der erweiterten Basisleistung EB2 in Kooperation mit dem ausgewählten externen Dienstleister für EB2.4 - Beginn der konkreten Maßnahmen zur Erschließung der primären und sekundären Zielgruppe mit dem Ziel, Warnungen und Alarme in alle Organisationseinheiten der primären Nutzergruppe zu verteilen - Das Angebot für die Zielgruppen auf dem Web-Server wurde im Rahmen des Aufbaus ausgeweitet, Überführung in die Pilotphase wurde abgeschlossen
Nach 12 Monaten	- Aufnahme der erweiterten Basisleistung EB3 in Kooperation mit dem ausgewählten externen Dienstleister für EB3.2 - Aufnahme der erweiterten Basisleistung EB4. Nach Maßgabe werden externe Partner im Rahmen von EB4.1 eingebunden - Ergebnisse des zweiten Reviews liegen vor und werden für die Optimierung der weiteren Pilotierung verwendet. Anpassungen an den Konzepten, sofern dies notwendig ist, werden vorgenommen

[17] Zählung der Monate erfolgt ausgehend vom ersten Monat des ersten Teilschritts.

Zeitpunkt[17]	Neu zu beginnende Arbeiten bzw. Status
Nach 15 Monaten	- Die Ergebnisse zur Erschließung der primären und sekundären Zielgruppe mit dem Ziel, Warnungen und Alarme in alle Organisationseinheiten der primären Nutzergruppe zu verteilen, werden analysiert. - Ausgehend von den Ergebnissen gibt es zwei Ansätze: - Erschlossene Organisationseinheiten werden für weitere Leistungen sensibilisiert - Nicht erschlossene Organisationseinheiten wurden identifiziert und individuell angesprochen
Nach 18 Monaten	- Ergebnisse des dritten Reviews liegen vor und werden für die Optimierung der weiteren Pilotierung verwendet. Anpassungen an den Konzepten, sofern dies notwendig ist, werden vorgenommen. - Das dritte Review wird außerdem für die Überführung von EB1 in den Regelbetrieb herangezogen (→ Phase 3)
Nach 21 Monaten	- Vorbereitung des „2. CERT-Niedersachsen Workshops“ ist abgeschlossen
Nach 24 Monaten	- Durchführung des „2. CERT-Niedersachsen Workshops“ - Ergebnisse des vierten Reviews liegen vor und werden für die Optimierung der weiteren Pilotierung verwendet. Anpassungen an den Konzepten, sofern dies notwendig ist, werden vorgenommen - Das vierte Review wird außerdem für die Überführung von EB2 in den Regelbetrieb herangezogen (→ Phase 3)
Nach 27 Monaten	- Die Abdeckung der primären und sekundären Zielgruppe wird erneut analysiert. Die noch nicht abgedeckten Organisationseinheiten werden – ausgehend von den Leitungsfunktionen der Ressorts – konzentriert angesprochen mit dem Ziel, die Integration bis zum 30ten Monat abzuschließen
Nach 30 Monaten	- Ergebnisse des fünften Reviews liegen vor und werden für die Optimierung der weiteren Pilotierung verwendet. Anpassungen an den Konzepten, sofern dies notwendig ist, werden vorgenommen - Das fünfte Review wird außerdem für die Überführung von EB3 und 4 in den Regelbetrieb herangezogen (→ Phase 3)

7.3 Phase Betriebsübergang (Monat 19 bis 36)

Im der dritten Phase steht nunmehr der Regelbetrieb im Vordergrund. Dabei werden die pilotierten Leistungen sukzessive in den Regelbetrieb überführt, so dass ein stufenweiser Aus- und Aufbau gelingen kann

Analog zur zweiten Phase gehören eine große Anzahl von Routinetätigkeiten zum Regelbetrieb (siehe dort), die hier nicht weiter ausgeführt werden sollen. Mit der abgeschlossenen Institutionalisierung nimmt entsprechend die Zahl der „herausragenden“ neuen Arbeiten kontinuierlich ab.

Die ständige Prüfung, wie weit die Abdeckung der primären und sekundären Zielgruppe erreicht wurde, ermöglicht die Beurteilung, in wie weit die Arbeit des CERT-Niedersachsen erfolgreich war und ist, und wie sie zukünftig erfolgreich gestaltet werden kann. Daher müssen Maßnahmen zur Motivierung und Integration der Zielgruppen in alle anderen

Maßnahmen einfließen bzw. dabei berücksichtigt werden. Dies ist aber weniger an einzelne Aktionen – z. B. Roundtable oder Workshop – festzumachen als vielmehr an die gesamte Kommunikation mit den betreuten Organisationseinheiten.

Zeitpunkt[18]	Neu zu beginnende Arbeiten bzw. Status
Beginn des 19ten Monats	- Kickoff für den Regelbetrieb im Rückgriff auf die Pilotphase und die Ergebnisse des dritten Reviews - Übernahme der erweiterten Basisleistung EB1 in Kooperation mit dem ausgewählten externen Dienstleister für EB1.1 in den Regelbetrieb
Nach 21 Monaten	(ohne besondere Arbeiten)
Nach 24 Monaten	- Übernahme der erweiterten Basisleistung EB2 in Kooperation mit dem ausgewählten externen Dienstleister für EB2.4 in den Regelbetrieb
Nach 27 Monaten	(ohne besondere Arbeiten)
Nach 30 Monaten	- Übernahme der erweiterten Basisleistung EB3 und EB4 in Kooperation mit dem ausgewählten externen Dienstleister für EB3.2 und den für EB4.1 identifizierten Partnern in den Regelbetrieb
Nach 33 Monaten	- Vorbereitung des 3. CERT-Niedersachsen Workshops ist abgeschlossen
Nach 36 Monaten	- Durchführung des 3. CERT-Niedersachsen Workshops

Mit Abschluss des 36ten Monats sind alle Konzepte fertig gestellt, alle Dienstleistungen wurden mehrere Monate pilotiert und anschließend in den Wirkbetrieb überführt. Dabei wurden durch die integrierten Reviews, Workshops und Roundtables sowie die explizite Abdeckung der primären und sekundären Zielgruppen sichergestellt, dass die vorliegenden Erkenntnisse eingepflegt und berücksichtigt werden können.

Damit sind die Voraussetzungen für einen langfristig stabilen, wirkungsvollen und den Anforderungen der Zielgruppe Rechnung tragenden Wirkbetrieb geschaffen worden.

[18] Zählung der Monate erfolgt ausgehend vom ersten Monat des ersten Teilschritts.

8 Zusammenfassung und Empfehlungen

Abschließend kann auf Basis der Projektarbeit zum Thema „CERT-Niedersachsen“ das Ergebnis wie folgt zusammengefasst werden:

Empfehlung 1: Der Aufbau eines CERT-Niedersachsen wird empfohlen.

CERTs - im Deutschen bekannt als Computer-Notfallteams - sind eine der wichtigsten Neuerungen im Risiko- und Sicherheitsmanagement. Gerade bei einer übergreifenden Koordinierung ergibt sich durch sie die angestrebte Vorwarnfunktion, d. h. die Verteilung proaktiver Informationen, durch die Vorfälle verhindert werden können.

Mit dem CERT-Niedersachsen kann ein deutlicher Beitrag zur Reaktion auf aktuelle Angriffe und Vorfälle bezogen auf die IT-unterstützen Geschäftsprozesse in der Landesverwaltung sowie beim zentralen IT-Dienstleister IZN geleistet werden. Dadurch wird die Informationssicherheit effektiv und nachhaltig verbessert.

Empfehlung 2: Nur zentrale und erweiterte Basisleistungen zusammen bilden ein CERT.

Basierend auf nationalen und internationalen Erfahrungen und Erkenntnissen wurden die verschiedenen Basisleistungen identifiziert, die minimal benötigt werden. Darüber hinaus gehende Zusatzleistungen sind möglich.

Die Basisleistungen können differenziert werden: „Zentrale Basisleistungen“ sind die Grundlage für eine erfolgreiche Etablierung des CERT-Niedersachsen. Sie stellen die Erschließung der Zielgruppe sowie deren Versorgung mit elementaren Informationen sicher. Bereits hierdurch kann die Sicherheit deutlich verbessert werden.

Die „erweiterten Basisleistungen“ ergänzen das Angebot, indem sie die konkrete Unterstützung bei Angriffen und Vorfällen ermöglichen.

Empfehlung 3: Für den Aufbau wird ein Zeitraum von drei Jahren empfohlen.

Die Aufteilung der Basisleistungen erlaubt ein stufenweises Vorgehen, bei dem zunächst die „zentralen Basisleistungen“ aufgebaut werden. Die Erschließung der Zielgruppe bildet dann die Voraussetzung für den erfolgreichen Aufbau der weiteren CERT-Leistungen, da eine Anpassung an die spezifischen Anforderungen möglich wird.

Um die CERT-Leistungen und ihre Akzeptanz in der Zielgruppe zu verankern, ist eine längerfristige Kontinuität sicherzustellen.

Nach diesem Zeitraum sollte das Gesamtkonzept und sein Erfolg einer kritischen Überprüfung unterzogen werden.

Empfehlung 4: Das CERT-Niedersachsen soll CERT-Leistungen zukaufen.

Abweichend von der traditionell üblichen Vorgehensweise bei Neugründungen von CERTs wird empfohlen, zunächst auf den Aufbau zusätzlichen Personals zu verzichten, sofern es sich um Aufgaben handelt, die durch einen externen Dienstleister mit gleicher Qualität erbracht werden können. Hier sind vor allem die Erstellung von Sicherheitsinformationen und Advisories zu nennen, die problemlos übernommen werden können.

Auszunehmen sind hiervon Aufgaben, die zentral in der Verantwortung des Landes bzw. der Ressorts verbleiben müssen. Insbesondere darf keineswegs die Kommunikation und Koordination innerhalb der Landesverwaltung an Externe vergeben werden, da die Verantwortung hierfür nicht delegiert werden kann.

Für den Aufbau der zentralen Kopfstelle sowie im begrenzten Ausmaß für die Tätigkeiten der dezentralen Komponenten im CERT-Niedersachsen sind jedoch zusätzliche Personalkapazitäten einzuplanen.

Empfehlung 5: Im Rahmen des empfohlenen Betriebsmodells sind Qualität und Neutralität des CERT-Niedersachsen sicherzustellen.

Um die Neutralität und Qualität der Dienstleistung sicherzustellen, soll eine fachliche Struktur etabliert werden, in die das CERT eingebettet ist. Diese Einbettung soll zudem die Anpassung an die spezifischen Anforderungen der Zielgruppe sowie die Kommunikation in die Zielgruppe hinein unterstützen.

Empfehlung 6: Das CERT-Niedersachsen stellt einen gleichberechtigten Partner für andere CERTs in Deutschland dar.

Die Präsenz des CERT-Niedersachsen erlaubt die nationale Einbindung in existierende CERT-Strukturen. Hier ist besonders die enge Zusammenarbeit mit CERTs in Deutschland zu betonen, insbesondere mit DFN-CERT und CERT-BUND, mit denen aufgrund der Vernetzung und Rolle ein direkter Informationsaustausch nötig ist.

Auf Basis dieser Aussagen und des vorliegenden Berichts wird des weiteren empfohlen, die Planungen für das CERT-Niedersachsen weiter voranzutreiben.

9 Literaturhinweise

[CSIHW 1/1989] Invitational Workshop on Computer Security Incident Response / Carnegie Mellon University, Software Engineering Institute. - Pittsburgh, PA, August 1991.

[KOM(2001)298] Sicherheit der Netze und Informationen : Vorschlag für einen europäischen Politikansatz / Kommission der europäischen Gemeinschaften. - Brüssel, Juni 2001. - KOM(2001)298 endgültig.

[Kossakowski 1992] Klassifikation und Abwehr von Computer-Würmern in Netzwerken / Klaus-Peter Kossakowski. - Diplomarbeit am Fachbereich Informatik, Universität Hamburg. - August 1992.

[Kossakowski et al. 1999] Responding to Intrusions / Klaus-Peter Kossakowski ; Julia Allen ; Christopher Alberts ; Cory Cohen ; Gary Ford ; Barbara Fraser ; Eric Hayes ; John Kochmar ; Suresh Konda ; William Wilson. - Security Improvement Module CMU/SEI-SIM-006. - Pittsburgh, PA: Carnegie Mellon University, 1999.

[Kossakowski 2000] Information Technology Incident Response Capabilities / Klaus-Peter Kossakowski. - Doctoral Thesis. - January 2000. - ISBN: 3-8311-0059-4.

[Kossakowski, Stikvoort 2000] A Trusted CSIRT Introducer in Europe - An empirical approach towards trust inside the European Incident Response scene - the replacement of trust by expectations / Klaus-Peter Kossakowski ; Don Stikvoort. - Amersfoort, NL: M&I/Stelvio, 2000.

[OECD] OECD Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security. Paris: OECD, July 2002. http://www.oecd.org

[Pethia van Wyk] Computer Emergency Response : An International Problem / Richard D. Pethia ; K. R. van Wyk. - CERT Coordination Center. - Pittsburgh, PA, o. J.

[Salus 1995] Early Insecurity / Peter H. Salus. - Vortrag auf der *UNIX Network Security Conference* in Washington DC, November 1995. [Tagungsunterlagen]

[Scherlis et al. 1990] Computer Emergency Response / W. L. Scherlis ; S. L. Squires ; Richard D. Pethia. - In: *Computers Under Attack* / Peter J. Denning (Hrsg.). - Reading, MA: Addison-Wesley, 1990. [S. 495-504]

[Schultz Jr. 1990] The Computer Incident Advisory Capability / E. Eugene Schultz Jr. - September 1990. [Eingereicht für die *Office Information Management Conference (OIM)*, New Orleans, LA, 24.-26. Oktober 1990]

[Schultz Jr. et al. 1990a] Computer Emergency Response Teams : Lessons Learned / E. Eugene Schultz Jr. ; Richard D. Pethia ; J. R. Dalton. - Vortrag auf der *13. National Computer Security Conference*. - S. 634-640. [Tagungsunterlagen]

[Schultz Jr. 1991] The Computer Emergency Response Team System (CERT-SYSTEM) / E. Eugene Schultz Jr. - Livermore, Calif., Oktober 1991. [Eingereicht für die *14th National Computer Security Conference (NCSC)*, Washington DC, 1.-4. Oktober 1991]

[RFC 2350] Expectations for Computer Security Incident Response / Nevil Brownlee ; Erik Guttman. - Request For Comments 2350. - Juni 1998. - [Elektronisch veröffentlicht unter http://ds.internic.net/rfc/rfc2350.txt]

[West-Brown et al. 1998] Handbook for Computer Security Incident Response Teams (CSIRTs) / Moira J. West-Brown ; Don Stikvoort ; Klaus-Peter Kossakowski. - CMU/SEI-98-HB-001. - Pittsburgh, PA: Carnegie Mellon University, 1998.

[West-Brown, Kossakowski 1999] International Infrastructure for Global Security Incident Response / Moira J. West-Brown ; Klaus-Peter Kossakowski. - Pittsburgh, PA: Carnegie Mellon University, 1999.

Anlage A Einstufung der Kritikalität von Ereignissen

Stufe	Definition	Beschreibung der Kritikalitätsstufe	Typische Fallbeispiele
K1	hoch	***Kritische Systeme oder Informationen*** *der Polizei des Landes Niedersachsen.* • mit dem Potential des Totalausfalles • mit existenzgefährdenden Auswirkungen bzw. • der nachhaltigen Hinderung an der Wahrnehmung des gesetzlichen Auftrages • Gefahr für Leib und Leben	• vorsätzlich herbeigeführte Überlastsituation eines IuK-Systemes oder Dienstes (Verlust der Verfügbarkeit) =>Denial of Service Angriff • Kompromitierte Information (kritisch) • Externes Hacking (aktiv) • Virus / Wurm (Ausbruch/Befall) • Zerstörung von Eigentum / Infrastruktur (hoch kritisch) • Ungesetzliche Aktivitäten • Totalausfall
K2	mittel	***Systeme oder Informationen*** *der Polizei des Landes Niedersachsen.* • mit dem Potential schwerwiegender, jedoch nicht existenzgefährdender Auswirkungen, • mit dem Potential die Wahrnehmung des gesetzlichen Auftrages einzuschränken oder stark zu behindern.	• Internes Hacking (nicht aktiv) • Externes Hacking (nicht aktiv) • Unberechtigter Zugriff • Verletzung von (Sicherheits-) Richtlinien • Ungesetzliche Aktivitäten • Kompromitierte Information (nicht kritisch) • Zerstörung von Eigentum / Infrastruktur (nicht hoch kritisch)

K3	niedrig	***Systeme oder Informationen*** *der Polizei des Landes Niedersachsen* auch kritische Systeme und Informationen, wenn Backup-Konzept oder Ausweichstrategie vorhanden
		• Beeinträchtigung möglich bzw. vorhersehbar
		• reguläre bzw. geplante, vorhersehbare Beeinträchtigung,
			• e-Mail
			• Verletzung von (unkritischen Sicherheits-) Richtlinien
			• Systemwartungen
			  ○ Betriebsmeldungen
			  ○ Geplante Wartungsfälle

[1] Als Ereignisse = Incidents werden angesehen:

- bereits eingetretene oder voraussehbare Beeinträchtigungen von Verfahren, Basisdiensten oder Infrastrukturbereichen.
- Informationen über Beeinträchtigungen