Projektabschlussbericht

Möglichkeiten der Zusammenarbeit von Land und Kommunen im IT-Bereich

Teilprojektauftrag:
Gemeinsame Nutzung der Dienstleistungen des niedersächsischen Landes CERT " Niedersachsen-CERT (N-CERT)" durch die niedersächsischen Kommunen

Version: 1.0

Verfasser:

Projektbeteilige N-CERT

Projektbeteiligte Kommunen

Inhaltsverzeichnis

1 Zusammenfassung

Das Projekt ist Teil des Gesamtvorhabens „Möglichkeiten der Zusammenarbeit von Land und Kommunen im IT-Bereich". Projektbeteiligte sind das Land Niedersachsen, der Niedersächsische Städte- und Gemeindebund (NSGB), der Niedersächsische Städtetag (NST), der Niedersächsische Landkreistag (NLT) und weitere von den kommunalen Spitzenverbänden benannte Projektbeteiligte.

Im Rahmen des Projekts wurden sechs Dienstleistungen des Niedersächsischen Computer Emergency Response Teams (N-CERT) evaluiert. Der Warn- und Informationsdienst (WID) stellte sich als erste nutzbare Dienstleistungen heraus.

Es wird vorgeschlagen, im Rahmen eines noch zu gründenden Niedersächsischen CERT-Verbunds (NCV) den weiteren Ausbau des Leistungsportfolios voranzutreiben.

2 Einleitung

Durch die verschärfte Sicherheitslage müssen sowohl das Land als auch die Kommunen mit den vorhandenen Ressourcen erhebliche zusätzliche Anstrengungen unternehmen, um sich zukünftig gegen die Gefahren aus dem Cyberraum zu schützen und damit Ihre Aufgaben ordnungsgemäß wahrnehmen zu können.

Zukünftig werden vermehrt übergreifende IT-Verfahren auf den Ebenen des Bundes sowie der Länder und Kommunen genutzt. Weiterhin streben das Land und die Kommunen eine stärkere gemeinsame Nutzung von IT-Infrastrukturen an. Es ist hierfür ein angemessenes Mindestsicherheitsniveau der IT-Infrastrukturen von Bund, Ländern und Kommunen zu etablieren, um auf sicheren Infrastrukturen diese Verfahren einfach integrieren und gemeinsam betreiben zu können.

Diese Entwicklung erfordert dringend, dass es auf niedersächsischer Ebene zu einer engeren Abstimmung und Zusammenarbeit zwischen dem Land und den Kommunen kommt. Das gemeinsame Vorgehen soll insbesondere sicherstellen, die notwendigen Sicherheitsanforderungen wirtschaftlicher realisieren zu können, als es jeder Einzelne für sich könnte und das Risiko hoher Folgekosten aufgrund von Sicherheitsvorfällen zu reduzieren.

3 Projektauftrag / Projektziel

Das Projekt ist Teil des Gesamtvorhabens „Möglichkeiten der Zusammenarbeit von Land und Kommunen im IT-Bereich". Projektbeteiligte sind das Land Niedersachsen, der Niedersächsische Städte- und Gemeindebund (NSGB), der Niedersächsische Städtetag (NST), der Niedersächsische Landkreistag (NLT) und weitere von den kommunalen Spitzenverbänden benannte Projektbeteiligte.

Das Projekt hat das Ziel, mögliche Formen der Nutzung der Dienstleistungen des N-CERT durch den kommunalen Bereich in Niedersachsen aufzuzeigen. Der Leistungsbedarf der Kommunen sollen erhoben und den Leistungsmöglichkeiten des N-CERT gegenübergestellt werden (siehe Kapitel 4). Dabei sind auch die rechtlichen Möglichkeiten und Grenzen der Zusammenarbeit zu definieren.

Die organisatorische Anbindung der niedersächsischen Kommunen an das Landes-CERT sowie die Art der Zusammenarbeit sind zu definieren. Ein Muster für eine gemeinsame Geschäftsordnung ist zu entwerfen, die die zukünftige Zusammenarbeit regeln könnte. Dabei sind auch die notwendigen Prozesse und Voraussetzung zur Inanspruchnahme der Dienstleistungen zu definieren. Es wurde dazu mit geeigneten kommunalen Organisationen ein sechsmonatiger Pilotbetrieb durchgeführt.

Soweit möglich sind die erforderlichen finanziellen, personellen und technischen Aufwendungen auf Seiten des N-CERT und der Kommunen zu identifizieren und ein Vorschlag für die Kompensation der Aufwände zu erarbeiten („Geschäftsmodell").

Eine Evaluierung hinsichtlich des weiteren Leistungsbedarfs auf Seiten der Kommunen soll erfolgen und auf deren Basis ein Stufenplan zur Umsetzung der Bedarfe erstellt werden.

Des Weiteren ist ein gemeinsames Evaluierungs- und Monitoring- sowie Controllingverfahren zu definieren und umzusetzen.

Abschließend wird eine Handlungsempfehlung über mögliche weitere Ausbaustufen der Zusammenarbeit der Projektpartner zur Verfügung gestellt.

3.1 Projektbeteiligte

Projektbeteiligt sind als Auftraggeber das Land Niedersachsen und die kommunalen Spitzenverbände. Projektbeteiligte sind Vertreter des N-CERT und der niedersächsischen Kommunen und kommunalen IT-Dienstleister.

Die Teilnehmer der kommunalen Seite repräsentieren die Struktur der kommunalen Landschaft von kleineren Kommunen, über große kreisfreie Städte bis hin zu Landkreisen sowie kommunale IT-Dienstleister und sonstige kommunale Zusammenschlüsse wie der Erprobungsraum Nord-West.

Das Projekt startete mit neun Vertretern der Kommunen. Im Projektverlauf sind kommunale Vertreter aus dem Projekt ausgeschieden. So sind der Landkreis Lüneburg, die Gemeinde Uetze und der Landkreis Harburg nicht mehr im Projekt vertreten. Zeitweise konnte sich auch die Stadt Hannover nicht am Projekt beteiligen. Zumeist erfolgte das Ausscheiden aus dem Projekt aufgrund von Ressourcenknappheit für das Thema Cyber-Sicherheit auf kommunaler Seite. Um die Aussagekraft des Pilotbetriebs aufrecht zu erhalten, wurden zur Kompensation sowohl die Stadt Wilhelmshaven als auch der IT-Dienstleister ITEBO im Projektverlauf als Projektbeteiligte aufgenommen.

Abbildung 1: Übersicht Projektbeteiligte

4 Mögliche Formen der Nutzung der Dienstleistungen des N-CERT durch die Kommunen in Niedersachsen

Zunächst wurden die Anforderungen der Kommunen an ein CERT aufgenommen und dem Leistungsportfolio des N-CERTs gegenübergestellt. Dabei wurden sehr schnell unterschiedliche Erwartungshaltungen identifiziert. Wesentlich ist der Punkt, dass das N-CERT kein operatives, sondern ein koordinierendes CERT ist. Mit der aktuellen Struktur und der derzeitigen Ressourcen kann das N-CERT nur einen Teil der von den Kommunen benötigten Leistungen erbringen. Mittels eines Abgleichs der Anforderungen der Kommunen mit dem Leistungsportfolio des N-CERT wurde ein möglicher Leistungskatalog für die Abnahme von Leistung durch die niedersächsischen Kommunen vom N-CERT erarbeitet (siehe Anhang 1).

Im Ergebnis wurden 14 Anforderungen der Kommunen an das N-CERT identifiziert. Acht dieser Anforderungen werden durch die sechs Positionen des Leistungsportfolios, welches N-CERT bereits für das Land Niedersachsen erbringt, abgedeckt. Die verbleibenden sechs Anforderungen können zu Projektbeginn nicht durch das N-CERT erbracht werden, sind jedoch bereits für weitere Ausbaustufen vorgesehen.

Um den Leistungen des Portfolios potentielle Abnehmer zuordnen zu können, wurde die folgende Kategorisierung der Kommunalen Landschaft anhand der Form des IT-Betriebs in Kundenkategorien vorgenommen:

Nr.	Kategorisierung anhand des IT-Betriebs	Erläuterung
1	IT-Betrieb in Eigenregie der Kommune	Fortgeschrittener Reifegrad des Sicherheitsmanagement; benötigte Anzahl/Qualifikation/Verantwortlichkeiten der IT-Mitarbeiter; Incident-Management etabliert
2	IT-Betrieb in Mischform	jegliche Form von Mischbetrieb aus Eigenregie und IT-DL; z.B. über IT-DL gehostete Fachverfahren / Desktop-Infrastruktur in Eigenregie
3	IT-Betrieb komplett über IT-DL	Keinerlei eigene Ressourcen/Kompetenz im Bereich des IT-Betriebs/der IT-Sicherheit
4	IT-DL als Datenzentrale	Betreuung der Kategorien 2 und 3

Tabelle 1: Kategorisierung der kommunalen Leistungsabnehmer

Im Projektverlauf wurde festgestellt, dass alle Leistungen grundsätzlich auch für alle Kategorien abnahmerelevant sein können.

5 Pilotphase – Ergebnisse und Schlussfolgerungen

Während der sechsmonatigen Pilotphase sollte die Erprobung der Nutzung der folgenden Leistungen des N-CERTs durch die Pilotteilnehmer erfolgen:

- Warn- und Informationsdienst
- Sicherheitsberatung
- Koordinierung von ressortübergreifenden Sicherheitsvorfällen
- Zusammenarbeit mit anderen Sicherheitsorganisationen
- Sicherheitslückenmanagement
- Regelmäßiger Sicherheitslagebericht

Der Fokus wurde dabei besonders auf den Warn- und Informationsdienst gelegt.

5.1 Warn-und Informationsdienst

Das N-CERT hat den teilnehmenden Kommunen und kommunalen IT-Dienstleistern über ein Web-Portal den Warn- und Informationsdienst (WID) der Landesverwaltung kostenfrei zur Verfügung gestellt. Innerhalb des Web-Portals konnte eine organisationsspezifische Vorselektion von Meldungen nach den jeweils eingesetzten Produkten und Technologien erfolgen. Dementsprechend wurden an die jeweiligen Empfänger nur relevante Meldungen über das Portal und per Email weitergeleitet.

Die Voraussetzung für die Entgegennahme der Meldungen des N-CERTs ist die Bereitstellung entsprechenden IT-Fachpersonals, da eine individuelle Aufbereitung der Informationen für „IT-Laien" durch das N-CERT nicht geleistet werden kann. Diese Aufbereitung käme einer individuellen Sicherheitsberatung gleich, s. Ziffer 5.1.2.

Der WID stellt in dieser Übermittlungsform für die Kommunen sowie die kommunalen IT-Dienstleister eine wertvolle Zusatzleistung für deren IT-Sicherheit dar. Dem erzielten Nutzen stehen Aufwände auf Seiten der teilnehmenden kommunalen Organisation gegenüber.

Die Projektgruppe empfiehlt, den WID den teilnehmenden Kommunen über den Pilotbetrieb hinaus anzubieten und alsbald eine Entscheidung über den weiteren Ausbau von Teilnehmern auf kommunaler Seite zu treffen.

Als erkanntes Optimierungspotenzial kann der Arbeitsaufwand der N-CERT-Kunden durch eine feinere Gliederung der Filtermöglichkeiten nach eingesetzten Produkten und nach Kritikalität im CERT-Portal auf kommunaler Seite verringert werden.

Außerdem soll geprüft werden, inwieweit auch Warnmeldungen, die nicht für die Landesverwaltung, wohl aber für die Kommunen relevant sind (z.B. kommunale Fachverfahren, IT-Infrastruktur), zur Verfügung gestellt werden können.

Das N-CERT plant eine Nachverfolgung der Cybersicherheitsmeldungen (ohne WID-Portal) zu etablieren. Hierzu sollen innerhalb der teilnehmenden kommunalen Organisationen die Auswirkung von Meldungen sowie notwendige Maßnahmen jeweils bewertet bzw. abgestimmt werden; dies erhöht den Arbeitsaufwand. Dabei ist zu berücksichtigen, dass Cybersicherheitswarnungen üblicherweise, so beispielsweise vom N-CERT in der Landesverwaltung und der Allianz für Cybersicherheit des BSI[1] nachverfolgt werden, um ein valides Lagebild über die derzeitigen Bedrohungen und Risiken zu erhalten. Dem Zuwachs in der (Qualität der) Informationssicherheit stünden jeweils fallabhängige, zusätzliche Aufwände entgegen.

Um komplexere Sicherheitslagen zu bewältigen, wird angenommen, dass Kommunen zum Teil externe Unterstützung benötigen. Hierzu sind entsprechende Kooperationen zu entwickeln und zu vereinbaren. Zu denken wäre hierbei an die Einrichtung von Koope-

1 Bundesamt für Sicherheit in der Informationstechnik

rationen, z.B. auf der Ebene von Landkreisen oder Erprobungsräumen oder an kommunale IT-Dienstleister, die Information für kleinere Kommunen aufbereiten und ggf. bewerten und umsetzen.

Der Warn- und Informationsdienst für kommunale Teilnehmer kann vom N-CERT ohne Mehraufwand abgewickelt werden und somit einer größeren Zahl an Kommunen zur Verfügung gestellt werden.

Der Zusatzservice „Pressespiegel" des N-CERT ist aus Sicht der IT-Organisationen der teilnehmenden Kommunen eine sinnvolle Ergänzung. Da bis auf die Pflege eines Mail-Verteilers beim N-CERT keine weiteren Aufwände entstehen, spricht sich die Projektgruppe für eine Beibehaltung dieses Services aus.

5.2 Sicherheitsberatung

Im Verlaufe der Pilotphase wurden auch Sicherheitsberatungen zu drei konkreten Themenstellungen angefragt. Aufgrund der Aufwände und Komplexität einer Sicherheitsberatung mussten diese Anfragen bereits in der Pilotphase abgelehnt werden. Es wurde schnell deutlich, dass die Sicherheitsberatung derzeit aus Ressourcengründen durch das N-CERT nicht für Kommunen zu erbringen ist.

Es existiert jedoch die Möglichkeit, Experten der entsprechenden Fachthemen zu vermitteln.

5.3 Koordinierung von ressortübergreifenden Sicherheitsvorfällen

Während der Pilotphase sind keine übergreifenden Sicherheitsvorfälle aufgetreten und konnten somit auch nicht an das N-CERT gemeldet werden. Trotzdem muss auch hier festgestellt werden, dass der Schwerpunkt auf der Leistungserbringung für die Landesverwaltung liegt. Eine Koordination übergreifender Sicherheitsvorfälle ist aufgrund der begrenzten Ressourcen des N-CERT derzeit nicht umfassend für die Gesamtzahl der Kommunen leistbar.

Hier kann die Einführung von Zwischenebenen wie Landkreisen, IT-Dienstleistern oder anderen kommunalen Zusammenschlüssen als Ansprechpartner für N-CERT und als Multiplikator für die Kommunen dienen.

5.4 Zusammenarbeit mit anderen Sicherheitsorganisationen

Aufgrund seiner starken Vernetzung kann das N-CERT den Kommunen den Zugang zu Informationen und Experten aus dem VCV (Verwaltungs-CERT-Verbund) und DCV(Deutsche-CERT-Verbund) bieten. Von der direkten Zusammenarbeit mit dem Landeskriminalamt (LKA), der Zentralen Ansprechstelle für Cybercrime (ZAC), dem Verfassungsschutz sowie dem Wirtschaftsschutz können auch die Kommunalen Körperschaften profitieren. Kontakte zum BSI sind für die Kommunen über das N-CERT möglich.

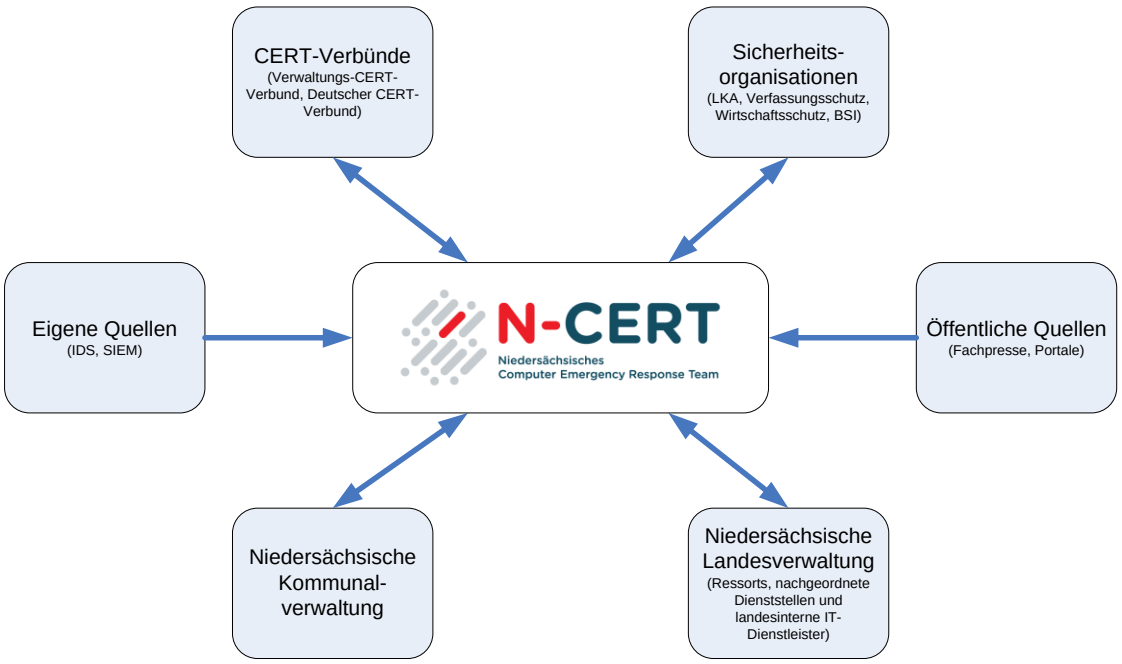

Abbildung 2: Vernetzung N-CERT

5.5 Sicherheitslückenmanagement

Das Sicherheitslückenmanagement ist mit Projektabschluss noch nicht für die Landesverwaltung etabliert. Für die Erbringung dieser Leistung ist mit einem erhöhten Personalaufwand zu rechen.

Aus diesen Gründen kann das Sicherheitslückenmanagement kurz- bis mittelfristig nicht für Kommunen realisiert werden.

5.6 Regelmäßiger Sicherheitslagebericht

Ein regelmäßiger Sicherheitslagebericht des N-CERTs über die Landesverwaltung und die Kommunen befindet sich derzeit im Aufbau. Der Sicherheitslagebericht kann die Basis für die Meldung für übergeordnete Sicherheitslageberichte, z. B. an das BSI, sein. Dieser Bericht wird auch den Kommunen zur Verfügung gestellt.

Einfließen können hier Informationen zu Sicherheitsvorfällen, Cybersicherheitsberichte aus externen Quellen, technische Statistiken aber auch Information aus den Ressorts und Kommunen.

5.7 Zusätzlicher Leistungsbedarf der Kommunen

Im Projektverlauf wurde festgestellt, dass die weiteren Leistungsbedarfe auf dem Gebiet der IT-Sicherheit zwischen einzelnen Kommunen stark variieren.

Weitere Leistungen sollen, abgestimmt auf die Kommunen und vorbehaltlich der finanziellen und personellen Ausstattung des N-CERT zukünftig erbracht werden.

6 Geschäftsordnung / Betriebskonzept

6.1 Art der Zusammenarbeit / Rahmenbedingungen

Die Projektgruppe empfiehlt als Basis für die gemeinsame Zusammenarbeit die Gründung eines Niedersächsischen CERT-Verbundes (NCV). Ein Entwurf für eine mögliche gemeinsame Geschäftsordnung ist als Anhang 2 beigefügt.

6.2 Voraussetzungen für die nds. Kommunalen Körperschaften zur Nutzung von Leistungen des Niedersachsen-CERT

Als Basis für den Zugang wurden die folgenden Voraussetzungen definiert:

Nr.	Voraussetzung	Erläuterung /Details
1	Benennen von mindestens einer Kontaktperson und dessen Vertreter	Adresse, Telefon/Mobiltelefon, Email (Funktionspostfach)
2	Bereitstellen von Informationen über die Form des IT-Betriebs (siehe auch Kategorisierung)	Eigenbetrieb, teilweise IT-Dienstleister (gehostete Fachverfahren / Desktop-Infrastruktur in Eigenregie), komplett über IT-Dienstleister, IT-Dienstleister als Datenzentrale
3	Bereitstellen der Informationen über den Anschluss an das Landesnetz	eigener Anschluss, Dienstleister, IP-Adresskreis
4	Bereitstellen der Informationen über den Anschluss an das Internet	eigener Anschluss, über das nds. Landesnetz, IP-Adresskreis, Internet Domain Name
5	Bereitstellen der Informationen über den Anschluss an das Verbindungsnetz/DOI	eigener Anschluss, über das nds. Landesnetz

Nr.	Voraussetzung	Erläuterung /Details
6	Bereitstellen von Informationen über die genutzten Ebenen übergreifenden Verfahren	Bund, Länder, Kommunen, Verbindungsnetz/DOI
7	Bereitstellen von Informationen über die eingesetzte Hard- und Software	Es liegen keine verlässlichen Informationen über die eingesetzten Hard- und Software-Produkte vor Art des eingesetzten Betriebssystems (Microsoft, Linux/Unix-Derivate, MacOS) Namen der eingesetzten Hard- und Softwareprodukte und deren Hersteller Versionen der eingesetzten Hard- und Software-Produkten
8	Bereitstellen von Informationen über die vorhandenen Sicherheitsmaßnahmen inklusive der eingesetzten Sicherheits-Hard- und –Software	Es liegen keine verlässlichen Informationen über die vorhandenen Sicherheitsmaßnahmen bzw. eingesetzten Sicherheits-Hard- und –Software-Produkte vor. Namen der eingesetzten Sicherheits-Hard- und -Software-Produkten und deren Hersteller Versionen der eingesetzten Sicherheits-Hard- und -Software-Produkten und deren Hersteller Vorhandensein eines Sicherheitskonzepts nach einem anerkannten Sicherheitsstandard (ISO 2700x, BSI IT-Grundschutz) Vorhandensein eines Sicherheitszertifikats nach einem anerkannten Sicherheitsstandard (ISO 2700x, BSI IT-Grundschutz)
9	Definieren wie mit den Informationen aus dem N-CERT (SI-Lücken, SI-Vorfälle, Frühwarnungen) auf kommunale Seite umgegangen wird und wie die Rückkommunikation an das N-CERT erfolgt.	
10	Definieren welche Eigenerkenntnisse an das N-CERT weitergegeben werden (dürfen).	
11	Anwenden eines gemeinsam vereinbarten Maßstabs / Definition von Sicherheitsvorfällen	

Tabelle 2: Zugangsvoraussetzungen Leistungen N-CERT

Das Bereitstellen von Informationen erfordert je nach Ausprägung des IT-Betriebs unterschiedlichen Aufwand auf kommunaler Seite. Teilweise können diese Informationen nicht oder mit erheblichen Aufwand zur Verfügung gestellt werden.

Dies wird entsprechend in der Zusammenarbeit berücksichtigt.

Als Basis für den Informationsaustausch und die Behandlung von Sicherheitsvorfällen dient die gemeinsame Definition eines Sicherheitsvorfalls.

Diese wurde von der Projektgruppe wie folgt erarbeitet:

> **Definition Sicherheitsvorfall:**
>
> Ein „Sicherheitsvorfall" (SI-Vorfall) ist ein ungeplantes Ereignis, das eine Einschränkung oder den Verlust der Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen nach sich ziehen kann.
>
> SI-Vorfälle sind für den CERT-Verbund relevant, wenn sie die Sicherheitsinteressen anderer CERT-Teilnehmer berühren können

6.3 Rechtliche Möglichkeiten und Grenzen der Zusammenarbeit

Die Verwertung von Warn- und Informationsmeldungen kann aus Lizenzgründen nur im Rahmen vertraglich vereinbarter Nutzungsbedingungen erfolgen. Eine kommerzielle Verwertung der Meldungen aus dem WID-Portal ist nicht erlaubt. Eine Verwertung der Informationen durch die IT-Dienstleister für kommunale Kunden ist explizit gestattet.

Um die Vertraulichkeit des Informationsaustausches sicherzustellen, wird für die Kennzeichnung von Verteilungsmöglichkeiten das Traffic Light Protocol (TLP) genutzt und muss von allen Beteiligten als verbindlich anerkannt werden. Auch die Weitergabe an Dritte – soweit gemäß Lizenzierung zulässig- kann nur unter Verpflichtung auf das TLP erfolgen.

Es gilt ebenfalls, dass Information, die von den Kommunen dem N-CERT zur Verfügung gestellt werden, in gleichem Maß vertraulich zu behandeln sind. N-CERT verpflichtet sich darauf, dass die Weitergabe von Information zu Sicherheitsvorfällen nur in einer Form erfolgt, die keinen Rückschluss auf ihre Quelle zulässt.

Für die Zusammenarbeit zwischen dem N-CERT und den niedersächsischen Kommunen ist weiterhin zu beachten, dass keinerlei gegenseitige Weisungsbefugnis besteht.

7 Geschäftsmodell

7.1 Erforderliche finanzielle, personelle und technische Aufwendungen auf Seiten des N-CERT

Der Leistungskatalog des N-CERT hat bei neuen Teilnehmern unterschiedliche Grenzaufwände. Diese steigen proportional bei kundenspezifischen, individuellen Aufwänden ohne Automatisierungspotenzial, wie beispielsweise einer Sicherheitsberatung. Der in diesem Fall entstehende Zusatzaufwand für einen kommunalen Bedarf kann bis auf die Klärung der Frage einer Leistungskompensation nicht geleistet werden.

Wie bereits unter Kapitel 5 aufgeführt, kann der Warn- und Informationsdienst der Landesverwaltung bis auf den Einrichtungsaufwand ohne größeren Mehraufwand durch N-CERT abgewickelt werden.

Für die anderen Leistungen ist die Erbringung für einen größeren Kundenkreis aufgrund begrenzter Ressourcen derzeit nicht möglich. Dies sollte im Rahmen des noch zu gründenden Niedersächsischen CERT-Verbunds und Folgeprojekten erfolgen.

Voraussetzung für die Erbringung weiterer Dienstleistungen ist der Auf-/ Ausbau weiterer Ressourcen im N-CERT.

Die Erweiterung der Personaldecke könnte prinzipiell durch die Stellung von Personalkapazitäten aus Kommunen erfolgen. Die Erfahrungen aus der Pilotphase zeigen jedoch, dass geeignetes Personal im notwendigen Umfang nicht durch die Kommunen gestellt werden kann.

7.2 Erforderliche finanzielle, personelle und technische Aufwendungen auf Seiten der Kommunen

Für die teilnehmenden Kommunen der Pilotphase stellt der durch das N-CERT zur Verfügung gestellte Warn- und Informationsdienst einen Mehrwert in Bezug auf Beurteilung der eigenen IT-Sicherheitslage dar.

Um den Nutzen für die Kommunen zur erhöhen, wird die Umsetzung der in Kapitel 4.1.1 erläuterten Optimierungsmaßnahmen empfohlen.

Für die Nutzung des Warn- und Informationsdiensts entsteht für die kommunalen Teilnehmer kein finanzieller Mehraufwand, da die Kosten der Lizenzierung durch N-CERT getragen werden.

Für die Entgegennahme der Meldungen den N-CERT ist die Bereitstellung entsprechenden IT-Fachpersonals notwendig. Sofern entsprechende Strukturen in den Kommunen vorhanden sind, kann eine Bearbeitung der Meldungen mit Mehraufwand erfolgen. Es wird angenommen, dass in anderen Fällen zum Teil externe Unterstützung benötigt wird.

7.3 Erforderliche finanzielle, personelle und technische Aufwendungen auf Seiten der IT-DL als Kooperationspartner

Aus den im Pilotbetrieb gesammelten Erkenntnissen ergibt sich, dass die über das N-CERT-Portal zur Verfügung gestellten Warn- und Informationsmeldungen ein tieferes technisches Verständnis erfordern. Es ist davon auszugehen, dass nicht bei allen potentiellen kommunalen Teilnehmern das erforderliche Know-how vorhanden ist, um die zur Verfügung gestellten Meldungen in Bezug auf die Informationssicherheit vollständig zu bewerten und ggf. notwendige Maßnahmen abzuleiten und umzusetzen. Um dieser Situation entgegenzuwirken, wäre aus Sicht der Projektgruppe die Einrichtung einer sog.

„Zwischenebene" sinnvoll. Diese Ebene könnte die Meldungen bedarfsgerecht aufarbeiten und weitergehende Hinweise und Informationen für die technischen Ansprechpartner der Kommunen bereitstellen. Auf dieser Basis würden die Kommunen in die Lage versetzt werden, Risiken für die eigene Institution einfacher bewerten und geeignete Maßnahmen umsetzen zu können. Diese Lösung würde aus Sicht der Projektgruppe insbesondere für die Kommunen in Betracht kommen, die in der Tabelle in Kapitel 3 unter den Nummern 1 und 2 aufgeführt sind. Die für die „Veredelung / Aufbereitung" der Meldungen erforderlichen personellen und ggf. technischen Ressourcen (z.B. für einen elektronischen Verteildienst) bei den IT-Dienstleistern, müssten vor der Etablierung eines solchen Dienstes zunächst im Hinblick auf Wirtschaftlichkeit und Machbarkeit geprüft werden

Die hier beschriebenen Lösungsansätze gelten ausschließlich für die Leistung „Warn- und Informationsdienst".

7.4 Gemeinsames Evaluierungs- und Monitoring- sowie Controllingverfahren

Die laufende Zusammenarbeit wird durch das Niedersachsen-CERT (N-CERT) koordiniert. Die Vertreter der Kommunen kommen mindestens zweimal im Jahr zusammen, um sich vertraulich über aktuelle Fragen der IT-Sicherheit auszutauschen (Mitgliedertreffen) sowie entstandene und veränderte Bedarfe zu evaluieren.

8 Handlungsempfehlung

Die Projektgruppe empfiehlt das Thema gemeinsame Zusammenarbeit von Land und Kommunen in Niedersachsen im Bereich Cybersicherheit weiterhin durch die Spitzenverbände voranzutreiben. Dies soll insbesondere durch Information und Sensibilisierung der Führungsebene im kommunalen Bereich erfolgen. Mit diesem Vorhaben soll eine entsprechende Priorisierung der Aufgaben aus dem Bereich IT-Sicherheit und eine entsprechende strategische Ausrichtung innerhalb der Kommunen erreicht werden.

Für den regelmäßigen Austausch zwischen den kommunalen Spitzenverbänden und der Abteilung 4 des nds. Ministerium des Inneren und Sport sollte dieses Thema weiterhin fester Bestandteil der Agenda sein.

Da sich die Entwicklung der Zusammenarbeit zwischen den Kommunen und dem N-CERT als langfristiger Prozess erwiesen hat und innerhalb des Projektzeitraums nicht abgeschlossen werden konnte, wird vorgeschlagen, ein regelmäßiges Anwendertreffen zwischen dem N-CERT und dem kommunalen Bereich zu etablieren. Hierzu wird empfohlen einen gemeinsamen Niedersächsischen CERT-Verbund (NCV) mit dem N-CERT und den niedersächsischen Kommunen als Mitglieder zu gründen.

Die Projektgruppe empfiehlt vor allem im Hinblick auf den Aufbau von Sicherheits-Lösungen auf Landesebene in einem weiteren Projekt ein gemeinsames Sicherheitsniveau von Land und Kommune zu erarbeiten.

Die Entwicklung des N-CERT ist organisatorisch bislang im Land noch nicht abgeschlossen, aufgrund der Sicherheitslage ist ein entsprechender Ausbau zu empfehlen. Ebenso kann der Bedarf der Kommunen an CERT-Leistungen derzeit nur minimal abgedeckt werden. Der WID–Leistungsumfang sollte für kommunale Bedarfe durch das N-CERT angepasst werden. Wünschenswert sind die Verfeinerung der Selektionskriterien und die Erweiterung des Informationsumfangs auf kommunale Anwendungen und Infrastruktur. Der Ausbau des Leistungsportfolios gemäß Anhang 1 sollte dabei durch die Mitglieder des NCV vorangetrieben und durch gemeinsame Folgeprojekte zwischen dem Land Niedersachsen und den nds. Kommunen erprobt werden. Dies kann jedoch nur auf Basis einer gesicherten Finanzierung erfolgen. Dafür müssten entweder verbindliche Vereinbarungen mit dem Land über den Abruf von Beratungsleistungen im Auftrag des N-CERT oder verbindliche Abnahmezusagen von kostenpflichtigen Dienstleistungen durch die Kommunen entwickelt werden.

Anhang 1

Leistungsportfolio des N-CERT für die niedersächsischen Kommunen

Nr.	Anforderung der Kommunen an die CERT-Leistungen	Bezeichnung der N-CERT Leistung	Beitrag des N-CERT	Abnehmer der Leistung*[2]
1	Advisory Management: Bewertung und Verteilung von Sicherheitswarnungen und konkreten Handlungsempfehlungen	Warn- und Informationsdienst	• Liste aller möglichen Systeme • Hinweise über Sicherheitslücken, Patches , direkt zu erwartende Angriffe • Bereitstellung von Sicherheitswarnungen über ein WID-Portal • Bereitstellen von kritischen Sicherheitsmeldungen mittels Email	1,2, 4 -
2	Konkrete Warnhinweise zu Bedrohungslagen, die insbesondere Bezug für öffentliche Verwaltungen/ Infos und Handlungsempfehlungen • über aktuelle Gefahren und Angriffe /Aktive Alarmierung bei akuten Gefährdungen • über den Umgang mit bekannten	Warn- und Informationsdienst	• Liste aller möglichen Systeme • Hinweise über Sicherheitslücken, Patches , direkt zu erwartende Angriffe • Bereitstellung von Sicherheitswarnungen über ein WID-Portal • Bereitstellen von kritischen Sicherheitsmeldungen mittels Email	1,2, 4

[*2] die Nummerierung bezieht sich auf die Kategorisierung der potentiellen Leistungsabnehmer wie in Kapitel 3 Tabelle 1 dargestellt

	Schwachstellen • Filterbar nach kommunal tatsächlich eingesetzten Softwareprodukten.			
3	Koordination bei kritischen Sicherheitsvorfällen.	Koordinierung bei sicherheitsdomänenübergreifenden Sicherheitsvorfällen	• Koordinierende Tätigkeiten bei übergreifenden Sicherheitsvorfällen • Informationsdrehscheibe zu anderen kommunalen Organisationen, Landesorganisationen mit Sicherheitsbezug • CERT wird Bestandteil der besonderen Aufbauorganisation (BAO) im Land • Unterstützung einer Task-Force zur Unterstützung von Kommune bei außergewöhnlichen Ereignissen	1,2, 4
4	Strategisches Bedrohungsradar (Strategic Threat Radar): Identifizierung und Bewertung von Bedrohungen im Kontext mit aktuellen und zukünftigen Kerntechnologien der Kommunen	Sicherheitsberatung	• Information zu marktüblichen Standardlösungen (Gefährdungskatalog)	1,2, (4) – ggf. bei Bedarf
5	Bereitstellung von Management-Reports zur Lage der IT-Sicherheit in Land und Kommunen	Cybersicherheitslagebild	• Darstellung des aktuellen Lagebilds • Bedrohungsszenarien für Sicherheitsdomänen, IT-Infrastruktur, Fachanwendungen • Prüfung, ob bereits umgesetzte Sicherheitsmaßnahmen und Sicherheitsarchitekturen Angriffsszenarien ausreichend unterbinden	1,2, 4
6	Bereitstellung einer niedersächsischen An-	Sicherheitsberatung	• SPOC für Niedersachsen	1,2, 4

	sprechstelle für niedersächsische Verwaltungen, die Hilfestellung bei Sicherheitsvorfällen geben kann (nicht im Sinne unmittelbarer Problemlösung, wohl aber durch Benennung von Lösungsansätzen, geeigneten Dienstleistern,...)		• Garantierte Erreichbarkeit Mo-Do 8-16 Uhr, Fr 8-13 Uhr • Reaktionszeit 4 Stunden • Eigenes Wissen/Schnittstelle zu anderen Expertenquellen • Listen mit geeigneten Dienstleistern	
7	Sicherheitslücken-Management	Sicherheitslückenmanagement	• bewertet bekannte Sicherheitslücken • gibt Risikoeinschätzung, Bewertung und Maßnahmenempfehlung ab • Es wird eine Datenbank über bekannte Sicherheitslücken und ihren Status (offen/geschlossen/nicht relevant) bei den Zielgruppen geführt. • Unterstützt das lokal vorhandene Verwundbarkeitsmanagement	1,2, 4
8	Sicherheitsrisikoanalyse	Sicherheitsrisikoanalyse	• effizienter Maßnahmenkatalog zur Vermeidung von Sicherheitsvorfällen • Entscheidungshilfen für die Einschätzung eines minimal erforderlichen Sicherheitsniveaus	1,2, 4
9	*Schwachstellen-Scanning: Regelmäßige Durchführung von Sicherheits-Scans der aus dem Internet erreichbaren Portale und Systeme*	*Wird derzeit nicht angeboten (nicht in Pilotphase)*	*Automatisierte Überprüfung von Systemen Darstellung in einem Portal Anpassung des aktuellen Vertrags mit dem DFN/DFN-CERT*	*(1), (2)*
10	*Sicherheits-Audits: Überprüfung und Bewertung von Sicherheitsarchitekturen, Sicherheitsprozessen und Systemlandschaft bei Bereichen, die einem erhöhten Gefahrenpo-*	*Wird derzeit nicht angeboten (nicht in Pilotphase)*	*technologisches Audit, kein ISMS-Audit!*	*(1), (2)*

	tential aus dem Internet ausgesetzt sind.			
11	*Durchführung forensischer Analysen sowie Analysen von Schwachstellen und Artefakten*	*Wird derzeit nicht angeboten (nicht in Pilotphase)*	• *Zukünftige Ausbaustufe des N-CERT.*	*(1), (2), (4)*
12	*Erarbeitung technischer Analysen zu Hacker-Angriffen, Malware und Sicherheitslücken*	*Wird derzeit nicht angeboten (nicht in Pilotphase)*	• *Zukünftige Ausbaustufe des N-CERT.*	*(1), (2), (4)*

Anhang 2

ENTWURF EINER GESCHÄFTSORDNUNG FÜR DEN NIEDERSÄCHSISCHEN CERT-VERBUND (NCV)

Präambel

In der Überzeugung, dass es nur eine enge Zusammenarbeit und ein effizienter Informationsaustausch ermöglichen, IT-Angriffe frühzeitig zu erkennen und abzuwehren, gründen das Land Niedersachsen und die niedersächsischen Kommunen den Niedersächsischen CERT-Verbund (NCV).

In dem Wissen, dass die auszutauschenden Informationen gerade für den Betroffenen eines IT-Angriffs besonders sensibel sind, wollen die Beteiligten langfristig partnerschaftlich und vertrauensvoll zusammenarbeiten.

§ 1 Errichtung

Das Land Niedersachsen und die niedersächsischen Kommunen und IT-Dienstleister errichten den Niedersächsischen CERT-Verbund (NCV).

§ 2 Zweck des NCV

(1) Der NCV dient dazu, IT-Angriffe frühzeitig zu erkennen und abzuwehren. Zu diesem Zweck arbeiten das Land Niedersachsen und die niedersächsischen Kommunen und IT-Dienstleister vertrauensvoll zusammen und schaffen mit der Errichtung des NCV geeignete Strukturen zur gegenseitigen Information, Warnung und Alarmierung.

(2) Die Erreichung des Zwecks soll insbesondere durch folgende Maßnahmen gefördert werden:
   (a) Festlegung von übergreifenden Prozessen, von Meldeverfahren und Meldewegen,
   (b) gegenseitige Unterstützung und Hilfeleistung bei IT-Sicherheitsvorfällen,
   (c) regelmäßige Treffen zur gemeinsamen Bewertung der übergreifenden IT-Sicherheitslage und der getroffenen Maßnahmen.

§ 3 Mitglieder

(1) Mitglieder des NCV sind das Land Niedersachsen und die niedersächsischen Kommunen und IT-Dienstleister. Diese wirken im NCV mit. Alternativ können die Kommunen andere geeignete Stellen für die Mitwirkung bestimmen.

(2) Die Mitglieder entscheiden mit Drei-Viertel-Mehrheit über die Aufnahme weiterer Mitglieder oder der Mitwirkung weiterer Stellen des Landes und der Kommunen.

§ 4 Gremien

(1) Die laufende Zusammenarbeit im NCV wird durch das Niedersachsen-CERT (N-CERT) koordiniert.

(2) Die Vertreter der Mitglieder kommen mindestens zweimal im Jahr zusammen, um sich vertraulich über aktuelle Fragen der IT-Sicherheit auszutauschen (Mitgliedertreffen).

§ 5 Mitgliedertreffen

(1) Die Gastgeberrolle bei den Mitgliedertreffen rotiert. Der Gastgeber erstellt unter Mitwirkung der übrigen Mitglieder eine Tagesordnung.

(2) Die Mitgliedertreffen finden grundsätzlich nicht-öffentlich statt. Die Tagesordnung kann vorsehen, dass Dritte im Rahmen eines öffentlichen Teils am Informationsaustausch teilhaben.

§ 6 Organisation der laufenden Zusammenarbeit

(1) Die Kommunen melden an das Niedersachsen-CERT einen jederzeit erreichbaren, zentralen Ansprechpunkt (Single Point of Contact (SPOC)), dessen Funktionspostfach und Gruppenrufnummer. Sie teilen insbesondere mit, ob die Voraussetzungen für den Empfang von nach Traffic Light Protocol (TLP) eingestuften Dokumenten gegeben sind. Informations-, Warn- und Alarmierungsmeldungen sind an den zentralen Ansprechpunkt zu richten.

(2) Die Kommunen können Informations-, Warn- und Alarmierungsmeldungen an ihre Dienstleister weiterleiten, wenn sie mit dem jeweiligen Dienstleister eine Vereinbarung über die Vertraulichkeit geschlossen haben (vgl. § 8).

(3) Informations-, Warn und Alarmierungsmeldungen werden durch das N-CERT an weitere CERTS des Verwaltungs-CERT-Verbundes weitergeleitet. Es bindet alle für die Abwehr von IT-Angriffen zuständigen Stellen der Länder und des Bundes in den IT-Krisenreaktionsprozess ein und vertritt den NCV beim Verwaltungs-CERT-Verbund.

(4) Das Niedersachsen-CERT pflegt Beziehungen zu nationalen und internationalen Partnern auf dem Feld der IT-Sicherheit. Die Kommunen informieren das N-CERT über eigene Aktivitäten auf diesem Gebiet.

(5) Anlassbezogen können durch das N-CERT nationale und internationale Partner eingebunden werden.

§ 7 Inhalte der laufenden Zusammenarbeit

(1) Die Mitglieder unterstützen sich gegenseitig im Rahmen der rechtlichen Möglichkeiten, ihrer Fähigkeiten und ihrer Kapazitäten zur Verwirklichung der in § 2 genannten Zwecke.

(2) Sie tauschen IT-sicherheitsrelevante Informationen, z.B. besondere Auffälligkeiten und klare Abweichungen vom Normalverhalten im Regelbetrieb, sowie Warn- und Alarmmeldungen und spezifische Maßnahmenempfehlungen aus. Diese können nach dem Traffic Light Protocol (TLP) eingestuft sein. Für die nach Satz 1 erforder-

lichen Mitteilungen verwenden die Mitglieder zwischen ihnen abgestimmte Formblätter.

(3) Das N-CERT stellt den übrigen Mitgliedern regelmäßig einen IT-Sicherheitslagebericht zur Verfügung. Die Kommunen tragen hierzu mit Artikeln bei. Diese können sich z. B. mit einem Sicherheitsvorfall mit Beispielcharakter oder einer Analyse befassen. Die Veröffentlichung kann derart erfolgen, dass der Rückschluss auf die betroffene Stelle ausgeschlossen ist.

(4) Die Kommunen berichten in besonderen Lagen oder im IT-Krisenfall an das N-CERT. Das N-CERT nimmt eine Lageschätzung vor, die durch das N-CERT an die SPOCs des NCV verteilt wird.

(5) Die Mitglieder üben das Zusammenwirken im IT-Krisenfall in unregelmäßigen Abständen. Die Übungen werden durch das N-CERT und in Absprache mit den Mitgliedern geplant, durchgeführt und nachbereitet. Das N-CERT stellt den Mitgliedern das für die Bundesverwaltung erstellte Übungsregister zur Verfügung. Die Kommunen tragen nach Verfügbarkeit eigene Übungen zum Übungsregister bei.

§ 8 Vertraulichkeit

(1) Die Mitglieder sind sich einig, dass der offene Austausch von IT-sicherheitsrelevanten Informationen eines Vertrauensverhältnisses bedarf, welches die Gewährleistung der Vertraulichkeit des Informationsaustausches voraussetzt.

(2) Für die Kennzeichnung von Verteilungsmöglichkeiten wird das Traffic Light Protocol (TLP) genutzt. Die Mitglieder erkennen das TLP als verbindlich an. Das TLP wird von den Mitgliedern wird mit der Maßgabe angewandt, dass als „TLP Amber" gekennzeichnete Informationen an vorgesetzte Dienststellen und die Fachaufsicht weitergeben werden dürfen. Sie verpflichten Dritte, an die sie Informationen aus dem NCV weitergeben möchten, auf das TLP.

(3) Information die von den Kommunen dem N-CERT zur Verfügung gestellt werden, werden im gleichem Maß vertraulich behandelt. Die Weitergabe von Information zu Sicherheitsvorfällen erfolgt nur in einer Form, die keinen Rückschluss auf ihre Quelle zulässt.

§ 9 Kosten

Die durch Zusammenarbeit im NCV entstehenden Kosten tragen die Mitglieder selbst.

Die vorstehende Geschäftsordnung wurde durch die Mitglieder des NCV bei der konstituierenden Sitzung am … in … einstimmig beschlossen.