Herzlich Willkommen!

Beteiligung des kommunalen Bereichs am N-CERT

15. Kommunales IuK-Forum Niedersachsen am 03./04.09.2015 in Varel

GovConnect
die IT-Spezialisten für Verwaltungen

Cybersicherheit?

- Steigende Abhängigkeit von IT
- Wachsende Cyber-Bedrohungen
- Verpflichtungen gem. NDSG / BDSG
- Auflagen bei ebenenübergreifenden Verfahren, z. B. NWR
- Entscheidend sind die Risiken für die Schutzziele und der Schutzbedarf der Daten, nicht die Größe der Organisation

Zusammenarbeit Land und Kommunen

- Intensivierung der Zusammenarbeit zwischen Land und Kommunen
- 12/2012–09/2013: Projekt „Gründung eines Cybersicherheitsbündnisses zwischen dem Land und den Kommunen zur Nutzung eines gemeinsamen CERT-Verbundes“
- Ziel:
  - Identifizierung von gemeinsamen Vorhaben, um ein angemessenes Mindestsicherheitsniveau im IT-Bereich von Land und Kommunen zu etablieren
  - **Identifizierung v. Möglichkeiten zur Einbindung des kommunalen Bereichs in die CERT-Struktur des Landes**
  - Abschluss eines gemeinsamen Cyber-Sicherheitsbündnisses

Historie

- Land NDS betreibt seit 01.10.2012 das N-CERT
- Beteiligung des kommunalen Bereichs sinnvoll
  - Im Verbund ist nur eine Kontaktstelle pro Bundesland vorgesehen
  - Übereinstimmung in der Infrastruktur
  - Betrieb gemeinsamer Fachverfahren
  - Nutzung gemeinsamer Netze

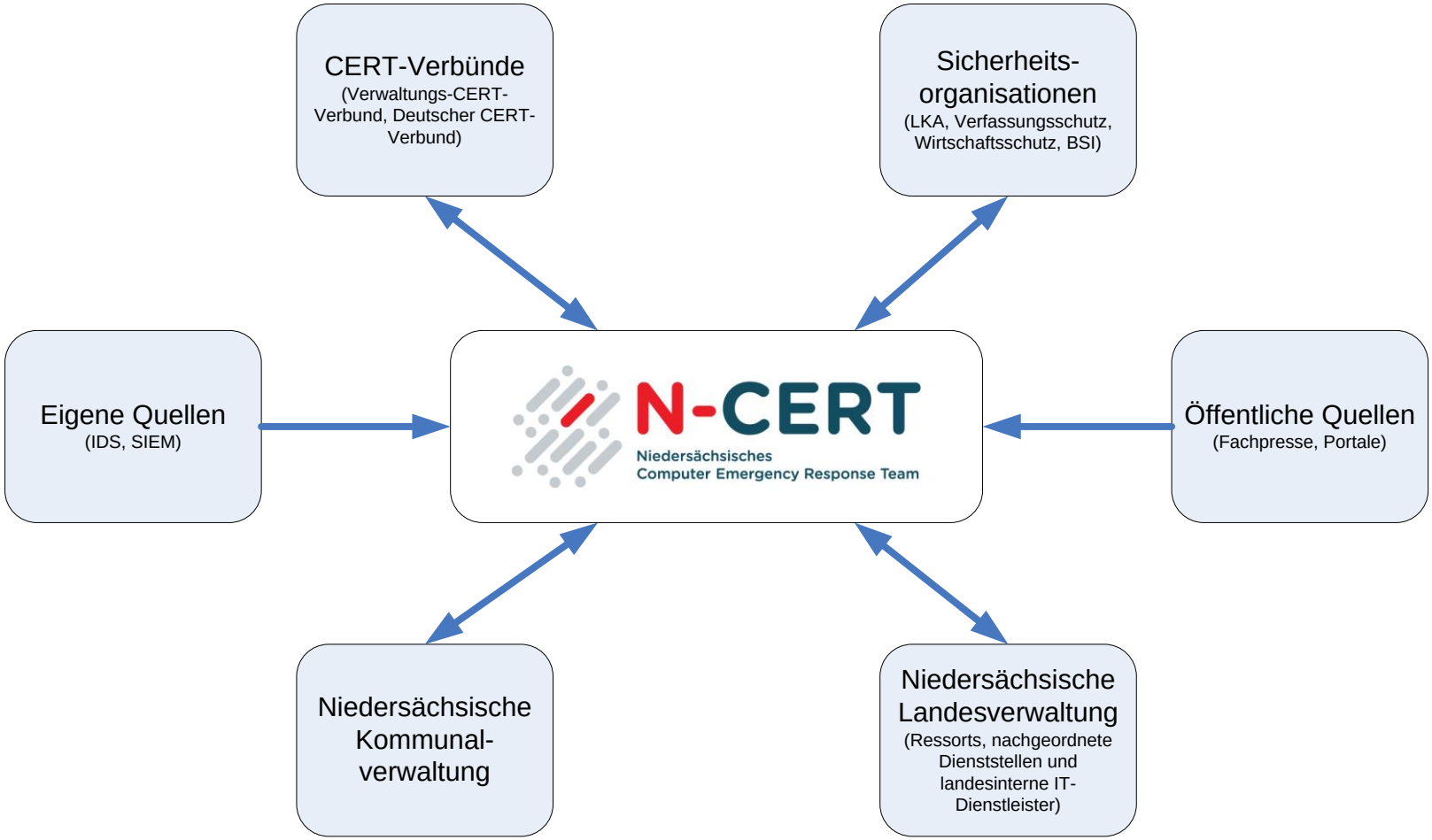
Was ist ein CERT?

- **C**omputer **E**mergency **R**esponse **T**eam
- **Schutzziele der Informationssicherheit:** Vertraulichkeit, Verfügbarkeit, Integrität
- **Zweck des CERT:** Minimierung des Risikos für die Ziele der Informationssicherheit durch proaktive Maßnahmen
- **Ziele des CERT:** Früherkennung von Sicherheitslücken und zielgerichteten Cyberangriffe, effektive Reaktion auf Angriffe durch Beratung der anderen Bereiche – Prävention, Reaktion, Nachhaltigkeit

Was tut ein CERT?

- **C**omputer **E**mergency **R**esponse **T**eam
  - erstellt präventive Handlungsempfehlungen zur Schadensvermeidung
  - Gibt Hinweise zu Schwachstellen in Hard- und Software
  - Liefert Vorschläge zur Behebung von Sicherheitslücken und unterstützt bei der Reaktion auf Sicherheitsvorfälle
  - Empfiehlt Maßnahmen zur Schadensbegrenzung und -beseitigung
  - Ist mit anderen CERTs vernetzt (z.B. CERT-Verbund Deutschland, Verwaltungs-CERT-Verbund)

Wer tauscht Informationen aus?



Leistungen des N-CERT

- Warn-und Informationsdienst
- Sicherheitsberatung
- Koordinierung von ressortübergreifenden Sicherheitsvorfällen
- Zusammenarbeit mit anderen Sicherheitseinrichtungen
- Sicherheitslückenmanagement
- Regelmäßiger Sicherheitslagebericht (im Aufbau)

Leistungsbestandteile des N-CERT für Kommunen definieren

- Warn- und Informationsdienst
  - Advisory Management
    - Bewertung und Verteilung von Sicherheitswarnungen und konkreten Handlungsempfehlungen
      - über aktuelle Gefahren und Angriffe
      - über den Umgang mit bekannten Schwachstellen
      - Filterbar nach kommunal tatsächlich eingesetzten Softwareprodukten (Input der Kommune erforderlich)
- Koordinierung bei sicherheitsdomänenübergreifenden Sicherheitsvorfällen

Leistungsbestandteile des N-CERT für Kommunen definieren

- Sicherheitsberatung
  - Strategisches Bedrohungsradar (Strategic Threat Radar): Identifizierung und Bewertung von Bedrohungen im Kontext mit aktuellen und zukünftigen Kerntechnologien der Kommunen

- Sicherheitsrisikoanalyse
  - effizienter Maßnahmenkatalog zur Vermeidung von Sicherheitsvorfällen
  - Entscheidungshilfen für die Einschätzung eines minimal erforderlichen Sicherheitsniveaus

Leistungsbestandteile des N-CERT für Kommunen definieren

- 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

- Cybersicherheitslagebild
  - Bereitstellung von Management-Reports zur Lage der IT-Sicherheit in Land und Kommunen

Projektbeschreibung

- „Gemeinsame Nutzung der Dienstleistungen des niedersächsischen Landes-CERT „Niedersachsen-CERT (N-CERT)“ durch die niedersächsischen Kommunen“
  - Projektstart: 18.12.2014
  - Geplantes Projektende: 01.04.2016
  - Auftraggeber: NLT, NSGB, NST, MI
  - Teilnehmer: LK Lüneburg, Stadt Göttingen, Stadt Braunschweig, Stadt Hannover, LK Emsland, Stadt Oldenburg/Erprobungsraum Nord-West, HannIT AöR

Meilensteine

- Leistungsbestandteile des N-CERT für Kommunen definieren
- Pilotbetrieb von Modellkommunen planen
- Bewertungskriterien für Pilotbetrieb definieren
- Pilotbetrieb durchführen
- Bewertung des Pilotbetriebs
- Konzept / Leistungskatalog / Verrechnungs- bzw. Beteiligungskonzept vorlegen

Pilotbetrieb

- Zeitraum: 01.07.2015 – 31.12.2015
- Ziel: Identifizierung von potentiellen Mehrwerten für die kommunale Seite und von Hindernissen in der Umsetzung bei allen Beteiligten
- Pilotteilnehmer liefern Input
  - Ansprechpartner
  - Anbindung an Landesnetz und Internet
  - Eingesetzte Hard- und Software
  - Sicherheitsmaßnahmen (inkl. eingesetzte Sicherheitshard- und Software, etc.)
  - Nutzung ebenenübergreifender Verfahren

Projektziel

- Definition der rechtlichen und organisatorischen Grundlagen sowie Rahmenbedingungen für eine Nutzung der Leistungen des N-CERT für die niedersächsischen Kommunen

Ablauf Pilotbetrieb

- Fokus auf Warn- und Informationsdienst
- Meldungen werden vom N-CERT an die Pilotteilnehmer gesendet
- N-CERT erhält Feedback zu Meldungen von den Kommunen

Bewertungskriterien für Pilotbetrieb festlegen

- Werden die angeboten Leistungen erbracht?
- Entsprechen die Leistungen inhaltlich und in der Reaktionszeit den Anforderungen?
- Können die Kommunen die Informationen bewerten und verarbeiten?
- Bestehen weitere Bedarfe auf kommunaler Seite?
- Erfolgen Rückmeldungen entsprechend den Erwartungen des CERT?
- Stellt das DFN-Portal ein geeignetes Werkzeug dar?

Entwurf Betriebs- bzw. Geschäftsmodell

- Zielgruppendefinition
  - Kategorisierung der Abnehmer
    - IT-Betrieb komplett in Eigenregie
    - IT-Betrieb teilweise ausgelagert
    - IT-Dienstleister (auch für IT-Betrieb komplett ausgelagert)
  - Ggf. Bündelungsfunktion über Zwischenebene (z.B. LK oder IT-DL) möglich
- Sichere Kommunikationswege / Informationsaustausch
- Rechtliche Rahmenbedingungen / Geheimhaltungsvereinbarungen
- Finanzierung

Ausblick

- Abschluss Pilotbetrieb für 31.12.2015 geplant
- Künftiger Betrieb über DFN-CERT-Portal
- Evaluation der Ergebnisse
- Erstellung einer Handlungsempfehlung über mögliche Zusammenarbeit und ggf. künftige Ausbaustufen

Vielen Dank.

Axel Köhler
Informationssicherheitsbeauftragter
der Nds. Landesverwaltung (CISO)

Tel: 0511/120-4798
Axel.Koehler@mi.niedersachsen.de

Patricia Pichottki
Unternehmensentwicklung
GovConnect GmbH

Tel: 0511/300 340 36
Pichottki@govconnect.de

Fragen

Vielen Dank
für Ihre Aufmerksamkeit

GovConnect
die IT-Spezialisten für Verwaltungen