14. Kommunales IuK-Forum
Niedersachsen am 03.09.2014
in Varel-Dangast

Niedersachsen

Cybersicherheit in der Landesverwaltung

Axel Köhler
CISO der niedersächsischen Landesverwaltung

N-CERT
Niedersächsisches
Computer Emergency Response Team

Niedersachsen

Cybersicherheit in der Landesverwaltung

- Weiterentwicklung des ISMS in der Landesverwaltung
- Umsetzung des IT-Sicherheitsgesetzes
- Herausforderungen –
  eine Bestandsaufnahme des N-CERT

ISRL – Bebauungsplan

- ISRL sind Mindestanforderungen für den Umgang in Sicherheitsfragen
- ISRL fokussieren den Sicherheitsprozess
  - Keine Produktempfehlung
  - Keine Anforderungsanalyse
- Auf Basis der ISO 27001
  - Matrix aus Assets und Gefahren
  - Abdeckungsbereiche ermittelt
- 14 Richtlinien als strategischer Rahmen

ISRL – Bebauungsplan

- Lebenszyklus
  - ISRL „Konzeption“
  - ISRL „Beschaffung und Outsourcing“
  - ISRL „Lebenszyklus“

ISRL – Bebauungsplan

- Schutzziele: Verfügbarkeit, Vertraulichkeit, Integrität
  - ISRL „Vertraulichkeit und Verbindlichkeit“
  - ISRL „Datensicherung“ (Schutzziel: Verfügbarkeit)
  - ISRL „IT-Nutzung“
  - ISRL „Verfahrensnutzung“
  - ISRL „Web-Nutzung“
  - ISRL „E-Mail-Nutzung“
  - ISRL „Zutritt“

Niedersachsen

ISRL – Bebauungsplan

- Beeinträchtigung von Schutzzielen
  - ISRL „IS-Vorfälle“
  - ISRL „Notfallvorsorge“
  - ISRL „Schadsoftware“
- Personal
  - ISRL „Sensibilisierung“

Niedersachsen

Weiterentwicklung des ISMS

- 6 Richtlinien verabschiedet
  - Im Rahmen der Pflege an den Bebauungsplan anzupassen
- 3 Richtlinien werden erstellt
  - ISRL „Konzeption“
  - ISRL „IS-Vorfälle“
  - ISRL „Vertraulichkeit und Verbindlichkeit“

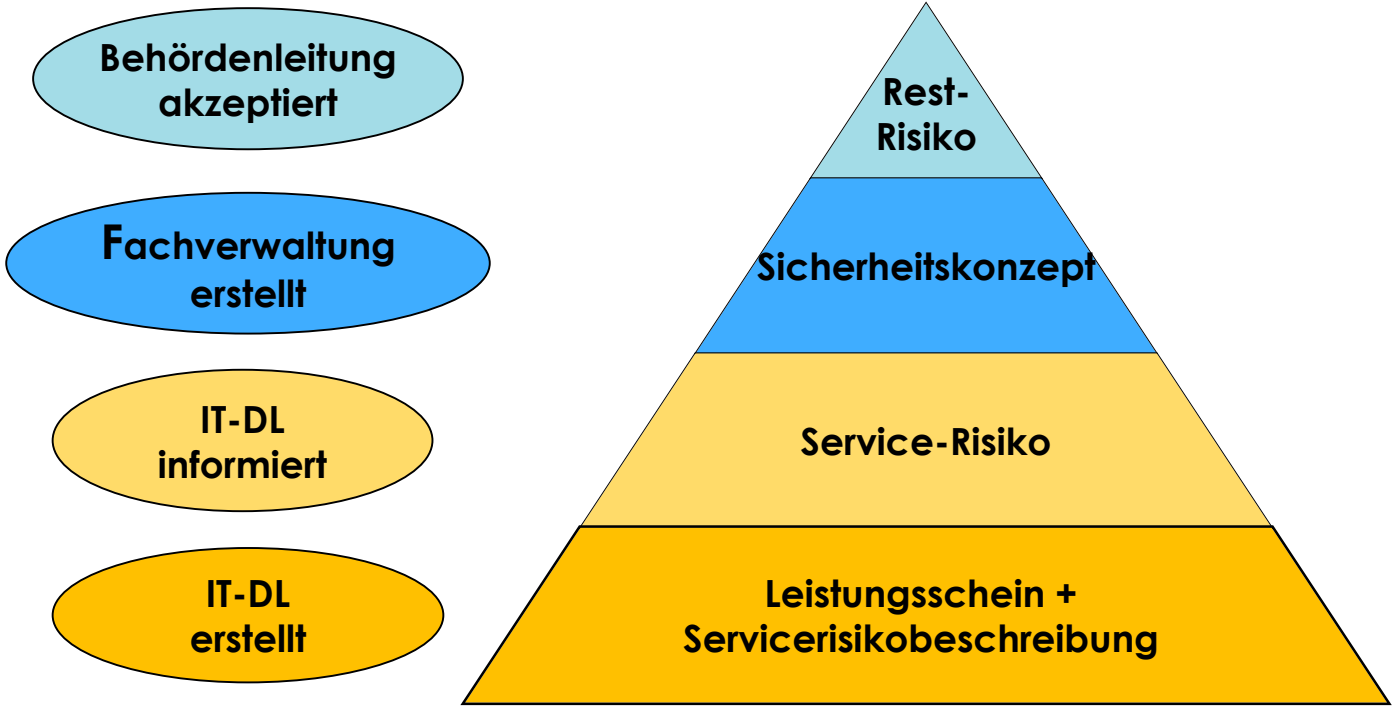
Niedersachsen

Weiterentwicklung des ISMS

- ISRL „Konzeption“
  - risikobasierte Konzeption der Informationssicherheit von Services, Fachverfahren und Sicherheitsdomänen
  - Mindestanforderungen an eine risikoorientierte Vorgehensweise
  - Dokumentenstruktur von Sicherheitskonzepten und von Risikobeschreibungen
  - Informationssicherheit von Services, Fachverfahren und Sicherheitsdomänen ressortübergreifend vergleichbar feststellen und fortlaufend verbessern

Niedersachsen

Exkurs: Risikomanagement



Modularisierung der Risikobetrachtungen

- Generische Risikobewertung (Planung)
  - Standard-Risikokataloge
  - An Restrisiken gemessenes vergleichbares Sicherheitsniveau
- Servicerisikobeschreibungen (SRB)
  - Der Beipackzettel zum Service des Dienstleisters
- Modularisiertes Vorgehen ermöglicht Synergien
  - Standardisierte Prozesse
  - Schlanke Dokumente
  - Identisch für Datenschutz und VSA

Niedersachsen

Modularisierung der Risikobetrachtungen

Sicherheitskonzept (IS-Domäne)
(einschl. Vorabkontrolle*)

SRB
(DS + IS)
Client
(IT.Niedersachsen)

SRB
(DS + IS)
Print
(IT.Niedersachsen)

SRB
(DS + IS)
File
(IT.Niedersachsen)

SRB
(DS + IS)
Mobile Device
(IT.Niedersachsen)

* Vorabkontrolle in den Fällen des § 7 NDSG

Niedersachsen

Modularisierung der Risikobetrachtung

Sicherheitskonzept (IS-Domäne)
(einschl. Vorabkontrolle*)

SiKo + **Vorabkontrolle** HWS (Fachreferat)	SiKo + **Vorabkontrolle** ZEUS (Fachreferat)	SiKo + **Vorabkontrolle** Job-Börse (Fachreferat)	SiKo + **Vorabkontrolle** PMV (Fachreferat)

* Vorabkontrolle in den Fällen des § 7 NDSG

Niedersachsen

Einheitlicher Aufbau der Sicherheitsstruktur

Sicherheitskonzept (IS-Domäne)
(einschl. Vorabkontrolle*)

SiKo + Vorabkontrolle* Job-Börse (Fachreferat)	SiKo + Vorabkontrolle* HWS (Fachreferat)
SRB (DS + IS) Client (IT.Niedersachsen)	SRB (DS + IS) MDM (IT.Niedersachsen)

* Vorabkontrolle in den Fällen des § 7 NDSG

Niedersachsen

Weiterentwicklung des ISMS

- ISRL „IS-Vorfälle“
  - Umgang mit Sicherheitsvorfällen
  - Domäneninterne und –übergreifende IS-Vorfälle
  - Ziel: frühzeitige, gemeinschaftliche und domänenübergreifende Schadensabwehr
  - Keine Statistikgrundlage
- ISRL „Vertraulichkeit und Verbindlichkeit“
  - Stand: Abstimmung des Auftrags und Umfangs

Niedersachsen

IT-Sicherheitsgesetz (IT-SiG)

- In Kraft seit 25.07.2015
- Das Artikelgesetz ändert:
  - Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BSI-Gesetz)
  - Atomgesetzes (AtG)
  - Energiewirtschaftsgesetz (EnWG)
  - Telemediengesetz (TMG)
  - Telekommunikationsgesetz (TKG)
  - Bundesbesoldungsgesetz (BBesG)
  - sowie das BKA-Gesetz.

Niedersachsen

IT-Sicherheitsgesetz (IT-SiG)

- Verbesserung der IT-Sicherheit bei Unternehmen
  - Mindeststandards und Meldepflichten für Kritische Infrastrukturen
- für die Sektoren Kritischer Infrastrukturen von:
  - Energie, Transport / Verkehr, IKT, Finanzen, Gesundheit, Wasser, Ernährung
  - *Staat und Verwaltung*
  - Medien und Kultur

Niedersachsen

IT-Sicherheitsgesetz (IT-SiG)

- Schutz der Bürgerinnen und Bürger in einem sicheren Netz
- Stärkung des BSI
- Erweiterung der Ermittlungszuständigkeiten des BKA

IT-Sicherheitsgesetz (IT-SiG)

- BSIG (neu):
  - BSI-Unterstützung: BSI kann auf Ersuchen beraten und unterstützen
  - Org. / technische Vorkehrungen: Standards / Stand der Technik inkl. Audits (2 Jahre)
  - BSI als zentrale Meldestelle: Kontinuierliches Lagebild mit Pflicht zur unverzüglichen Weitergabe an Betreiber (Alarmierungskontakt in 6 Monaten)
  - Meldepflicht: Bei Störpotential für KRITIS
  - Bußgelder bis 100.000 € bei Zuwiderhandlungen

Niedersachsen

Umsetzung des IT-SiG: Rechtsverordnung

- § 10 BSIG (neu):
  - „(1) Das Bundesministerium des Innern bestimmt durch Rechtsverordnung […] nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit […] unter Festlegung der in den jeweiligen Sektoren […] wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten. “

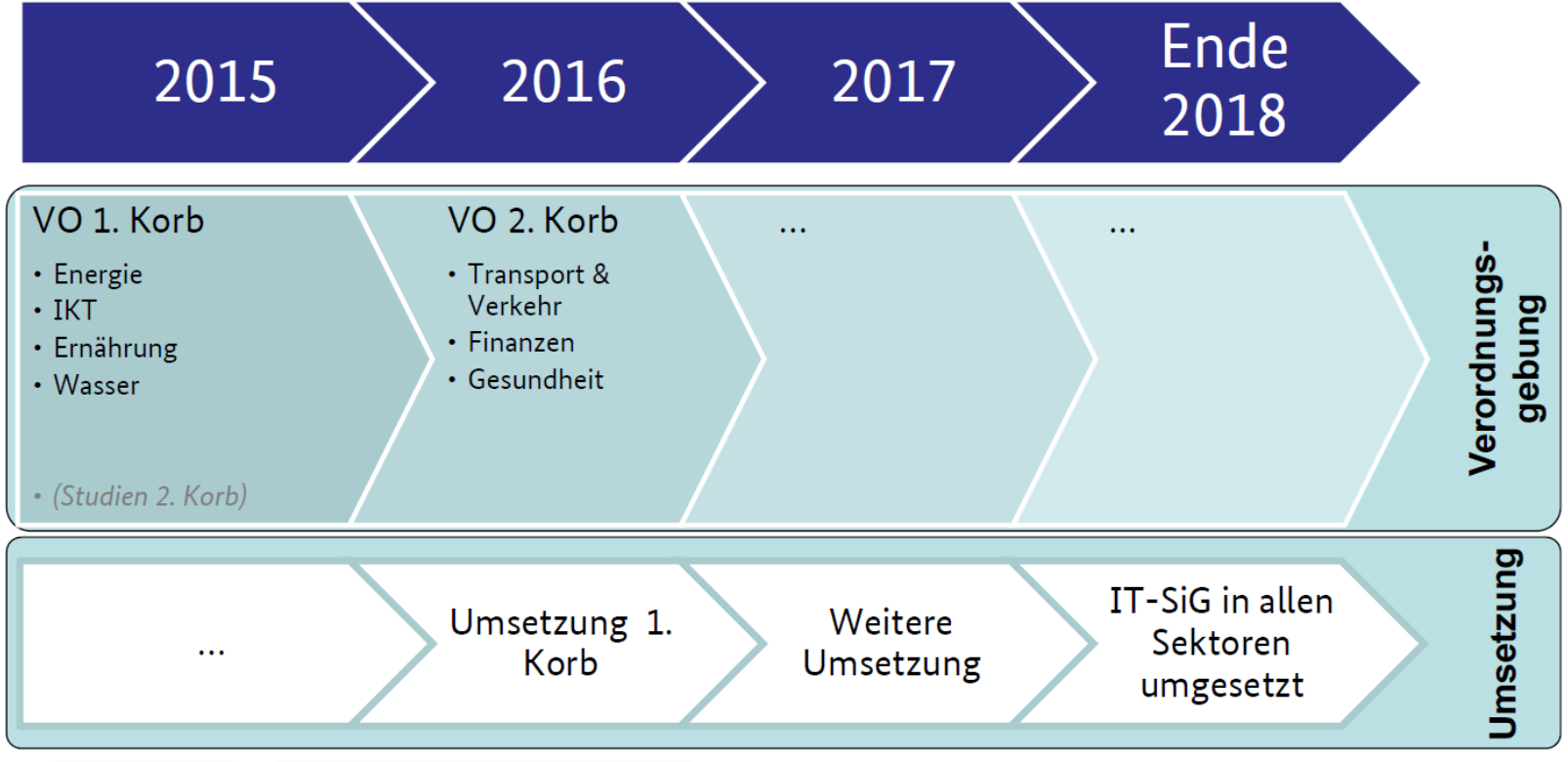
Niedersachsen

Umsetzung des IT-SiG: Rechtsverordnung

- Schwerpunkt auf Versorgung der Gesellschaft mit wichtigen Dienstleistungen (Top-Down) - Ausgestaltung in zwei Schritten:
  - 1. Qualität: Dienstleistungen in den KRITIS-Sektoren, die für die Versorgungskette relevant sind und abstrakte Anlagen
  - 2. Quantität: Schwellenwerte innerhalb dieser Dienstleistungen
- Jedes Unternehmen wird bestimmen können, ob es eine Kritische Infrastruktur im Sinne des IT-SiG betreibt.

Niedersachsen

Umsetzung des IT-SiG: Rechtsverordnung



Umsetzung des IT-SiG: Rechtsverordnung

Dienstleistungen
im Sektor Energie *(vorläufig)*

Dienstleistung	Prozessschritte	Anlagentypen
Stromversorgung	Erzeugung	Kraftwerke, dezentrale Energieerzeugungsanlagen
	Übertragung	Übertragungsnetze, Strombörsen, Speicherkraftwerke
	Verteilung	Verteilnetze, Stromanschlüsse
Gasversorgung	Förderung	Gasaufbereitungsanlagen
	Transport	Ferngasnetze, Speicher, Börsen
	Verteilung	Verteilnetze, Anschlüsse

Umsetzung des IT-SiG: Rechtsverordnung

Dienstleistungen
im Sektor Energie *(vorläufig)*

Dienstleistung	Prozessschritte	Anlagentypen
Treibstoff- und Heizölversorgung	Erdölförderung – und Mineralölproduktion	Ölförderanlagen, Raffinerien
	Öltransport	Öl- und Produktenpipelines, Öl- und Produktenlager
	Treibstoff- und Heizölverteilung	Tankwagenflotte, Tankstellennetze
Fernwärme-versorgung	Erzeugung	Heizwerke, Heizkraftwerke
	Verteilung	Fernwärmenetze

Umsetzung des IT-SiG: Rechtsverordnung

Dienstleistungen
im Sektor IKT *(vorläufig)*

Dienstleistung	Prozessschritte	Anlagentypen
Sprach- u. Datenübertragung	Zugang	Ortsgebundene Zugangsnetze, Mobilfunknetz
	Übertragung	Backbone-Netze, Regionale Netze, Darkfiber/Kabel
	Vermittlung	IXP
	Infrastrukturdienste	DE DNS-Rootserver, Steuerung Telefonie + Mobilfunk, Anlagen zur RIPE-Präfixprüfung
Datenspeicherung und -verarbeitung	Housing	Rechenzentrum
	IT-Hosting	Rechenzentrum
	Internetdienste	

Umsetzung des IT-SiG: Rechtsverordnung

Dienstleistungen
im Sektor Ernährung *(vorläufig)*

Dienstleistung	Prozessschritte	Anlagentypen
Lebensmittel-versorgung	Produktion	Landwirtschafts- und Fischereimaschinen, Produktionsanlagen, Zwischenlager
	Handel	Zentral- und Regionallager, Fahrzeuge zur Distribution, System zur Abwicklung von Zahlungen, Warenwirtschaftssystem
	HoReGa	

Niedersachsen

Umsetzung des IT-SiG – Länderbeteiligung

- Beschluss MPK 18.06.15, TOP 6
  - Länder begrüßen IT-SiG
  - Da die Bestimmung der Betreiber kritischer Infrastrukturen Auswirkungen auf die Betreuungsarbeit der Länderbehörden hat und der Sachverstand der Länder bei der Bestimmung kritischer Infrastrukturen genutzt werden sollte, sind die Länder an der Erarbeitung der geplanten Rechtsverordnung zum IT-Sicherheitsgesetz zu beteiligen. Die Verordnungsentwürfe sind den Ländern nach der Geschäftsordnung der Bundesministerien frühzeitig zur Stellungnahme zuzuleiten. …

Niedersachsen

Umsetzung des IT-SiG – Länderbeteiligung

- Beschluss MPK 18.06.15, TOP 6
  - Enge Zusammenarbeit zwischen Bund und Ländern
  - Abstimmung mit Unternehmen der Kritischen Infrastruktur, werden mit allen zuständigen Fachministerkonferenzen (nicht abschließend: IMK, WMK, FMK, GMK, EMK) abgestimmt. Die Federführung für die Koordinierung der Fachministerkonferenzen bei solchen Aktivitäten wird der Innenministerkonferenz übertragen.

Niedersachsen

Umsetzung des IT-SiG – Länderbeteiligung

- Nächste Schritte
  - Sondersitzung der LAG Cybersicherheit der IMK im Sept. / Okt. 2015
  - Beteiligung der Länder in den Arbeitskreisen des UP KRITIS des Bundes
- Offene Fragen des Landes:
  - Zentrale Meldestelle zur Kommunikation mit dem BSI
  - Entstehende Aufgaben und Aufwände
  - Rolle der Kommunen (auch als Betreiber von KRITIS)

Niedersachsen

Was macht das N-CERT?

- Beteiligung des Kommunalen Bereichs am N-CERT
  - … später mehr.
- Aufbau Next-Generation-Firewall und SOC
  - SOC als zentrale Stelle für Verhaltensanalyse des Systems
  - Aufbau eines IDS / SIEM-Systems (z. Zt. Testbetrieb)
  - Herausforderungen:
    - Kenntnis der Architektur und Infrastruktur
    - Komplexer rechtlicher Rahmen: TKG, PersVG, NDSG
    - Revisionssichere Konfiguration und Betrieb des Analysesystems

N-CERT
Niedersächsisches
Computer Emergency Response Team

Niedersachsen

Leistungen des N-CERTs 2014

- über 5.200 CERT-Meldungen ausgewertet (+77%)
  - ca. 440 Meldungen pro Monat
- über 130 öffentliche und nicht-öffentliche Quellen werden mehrmals täglich gesichtet (+160%)
  - News-Sites, Twitter, Blogs, Foren, etc.
- mehr als 160 Vorgänge bearbeitet (+60%)
  - Si-Vorfälle, Si-Lücken, Warnmeldungen
  - 29 offene Vorgänge
- 19 Cybersicherheitsmeldungen (+171%)

N-CERT
Niedersächsisches Computer Emergency Response Team

Niedersachsen

Leistungen des N-CERTs 2014

- Top 10 Malware 2014
  1. Ledod (Malware Downloader)
  2. Dalexis (Zbot-Familie)
  3. Emotet (Banking Malware)
  4. Roover (Malware Downloader
  5. Ovani (Visual Basic Macro Exploit für Microsoft Office)
  6. Blacole (JavaScript Exploit Kit)
  7. Sharik (Zbot-Familie)
  8. Scarsi (Malware Downloader)
  9. Injecto (Zbot-Familie)
  10. Gamarue (Wurm in Verbindung mit Exploit-Kits wie Blacole)

Haupteinfallswege

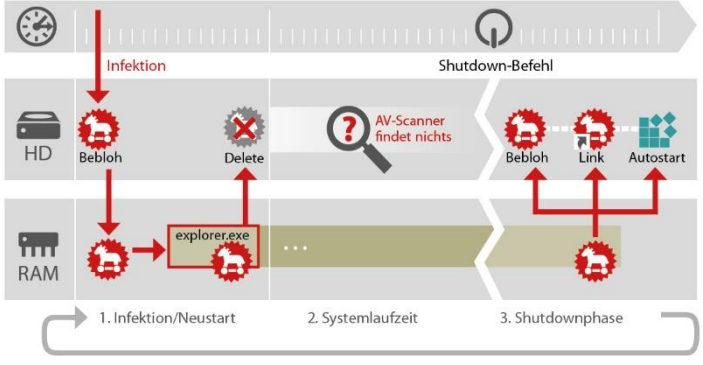
- Emails und Websurfen

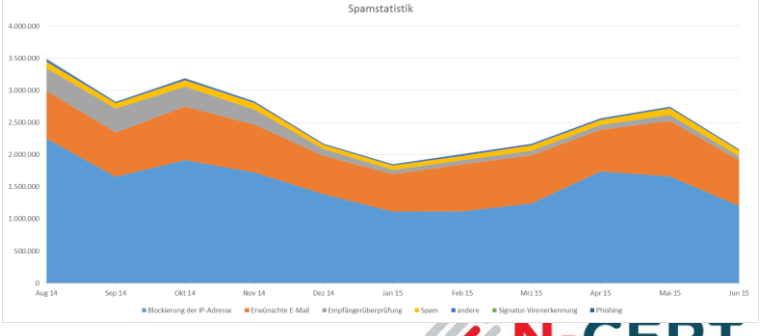
N-CERT
Niedersächsisches Computer Emergency Response Team

Niedersachsen

Leistungen des N-CERTs 2014

- Koordinierung von Sicherheitsvorfällen:
  - Bebloh-Komplex / Kooperation mit Fraunhofer-IT
  - Analyse von Bewerbung_Dezember 2014.pdf.exe
  - Spy Tracking-Programm
  - Analyse von Regin





N-CERT
Niedersächsisches Computer Emergency Response Team

Niedersachsen

Ausblick

- Gemeinsames Projekt Kommunen – Land
  - Start in 2016
  - Definition eines gemeinsamen Sicherheitsniveaus
  - Vorgehensmodell zum Erreichen eines gemeinsames Sicherheitsniveaus
  - Ausgangsbasis:
    - Handreichung zur Ausgestaltung der Informationssicher-heitsleitlinie in Kommunalverwaltungen
    - ISMS des Landes Niedersachsen
    - Beiträge der Kommunen

Niedersachsen

Vielen Dank für Ihre Aufmerksamkeit

Fragen - Diskussion

Kontakt

Niedersachsen-CERT
cert@niedersachsen.de
0511 9898 - 2378

Axel Köhler
axel.koehler@mi.niedersachsen.de
0511 120 - 4798

N-CERT
Niedersächsisches
Computer Emergency Response Team

Niedersachsen