Cybercrime-Herausforderungen und Strategien am 28.05.2019 in Gelsenkirchen IT- und Cyber-Sicherheitskonzept für Kommunen

Udo Zaudig
Stadt Köln, 28.05.2019

Das Amt für Informationsverarbeitung

Der zentrale Dienstleister für die Informations- und Kommunikationstechnik der Kölner Stadtverwaltung

Ca. 361 Mitarbeiterinnen und Mitarbeiter am Verwaltungsstandort Enggasse

Stadthaus Chorweiler

2 Rechenzentren an den Standorten Chorweiler und Kalk

Dienstgebäude Enggasse

RZ-Kalk

IKT - Portfolio Stadt Köln

Anwender / innen der Stadtverwaltung

Büro-arbeitsplatz

Mobiler Zugang

13.609	IT-Arbeitsplätze
17.340	Betreute IT-Nutzer
2.744	Registrierte mobile Geräte

IKT - Portfolio Stadt Köln

Arbeitsplatzinfrastruktur
Basisanwendungen, Dienste

13.183	Full-Clients
426	Terminal-Desk-Clients
1.209	Paketierte Anwendungen
255	Vergabeverfahren (über 100 Lieferanten)
405	Terrabyte Speicherplatz
7.8 Mio	Eingehende E-Mails / Jahr
72 Mio	Internetzugriffe / Jahr
27 Mio	Intranetzugriffe / Jahr

Notwendigkeit zur Einführung eines ISMS bei Behörden

- Datenschutzgesetze (BDSG, LDSG, SGB X,...)
- Hinweise der Rechnungshöfe zur Informationssicherheit
- IT-PLR 8. März 2013

  Informationssicherheitsleitlinie und Umsetzungsplan

  ➢ Leitlinie und ISMS innerhalb von 5 Jahren
- IT-PLR März 2015

  Anschlussbedingungen Verbindungsnetz

  ➢ Umzusetzen bis 31.12.2017

  ➢ Nachzuweisen über Audit bis 31.12.2019
- EU-Datenschutzgrundverordnung in Kraft seit 25.05.2016

  ➢ Wirksamwerden am 25.05.2018

Weitere Beispiele für Schnittstellen zur **Compliance der Informationsverarbeitung**

Allgemeine Vorschriften

- Zivil- und Strafrecht
- TK-Recht
- Arbeitsrecht
- ….

Spezielle Vorschriften

- Signaturgesetz
- Verordnung zum elektronischen Personenstandsregister
- Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme – **GoBS** - Bundesfinanzministeriums 07.11.1995
- SGB
- ….

Gesetz zum Schutz kritischer Infrastrukturen

Vorwort KRITIS-Strategie des Bundes:

Die Gewährleistung des Schutzes dieser Infrastrukturen ist eine Kernaufgabe staatlicher und unternehmerischer Sicherheitsvorsorge und zentrales Thema der Sicherheitspolitik unseres Landes.

Der erste Teil der KRITIS-Verordnung zur Umsetzung des IT-Sicherheitsgesetzes ist am 3. Mai 2016 in Kraft getreten. Betroffene Unternehmen aus den Sektoren Energie, Informationstechnik und Telekommunikation, Wasser sowie Ernährung können sich hier registrieren.

Der zweite Teil der KRITIS-Verordnung mit den Sektoren Finanzen, Transport und Verkehr sowie Gesundheit ist ebenfalls in Kraft getreten.

Nach § 8a Abs. 1 BSIG sind:

„angemessene organisatorische und technische Vorkehrungen und sonstige Maßnahmen zum Schutz derjenigen informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind“.

Da das Thema IT-Sicherheit derzeit eines der brennenden und aktuellen politischen Themen ist, werden auch die Länderparlamente vermutlich entsprechende Gesetze erlassen. Außerdem entsteht durch die NIS-Richtlinie der europäischen Union weiterer politischer Druck, auch die öffentliche Verwaltung in den Ländern und in den Kommunen an die neu definierten gesetzlichen Anforderungen zu binden.

Zu den kommunalen kritischen Infrastrukturen im sinne des Gesetzes gehören in Köln:

- die Stadtentwässerungsbetriebe mit der Abflusssteuerzentrale und dem Großklärwerk Stammheim (Anstalt des öffentlichen Rechts)
  Audit abgeschlossen Mai 2018

- die Verkehrsleittechnik und Tunnelüberwachung (Amt der Stadt Köln)
  Audit geplant Juni 2019

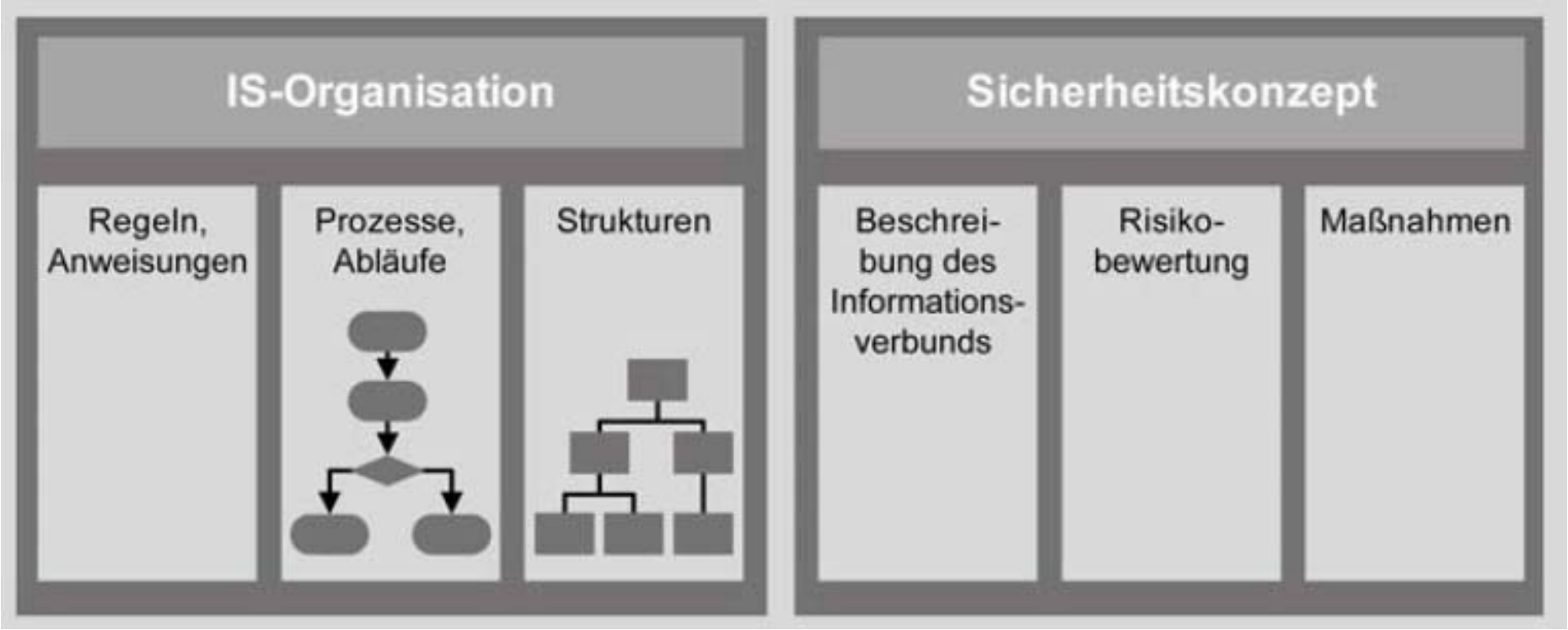
Informationssicherheitsmanagement bei der Stadt Köln

Die sichere Verarbeitung von Informationen ist heutzutage für nahezu alle Unternehmen und Behörden von existenzieller Bedeutung

Ein angemessenes Sicherheitsniveau kann nur durch geplantes und organisiertes Vorgehen aller Beteiligten erreicht und aufrechterhalten werden.

Die dazu notwendigen Planungs-, Lenkungs- und Kontrollmechanismen werden als Informationssicherheitsmanagement/ISMS bezeichnet.

Der Baustein baut auf dem BSI -Standard 100-1 Managementsysteme für Informationssicherheit und BSI-Standard 100-2 Vorgehensweise nach IT-Grundschutz auf und fasst die wichtigsten Aspekte zum Sicherheitsmanagement hieraus zusammen.


IS-Organisation
Regeln, Anweisungen
Prozesse, Abläufe
Strukturen
Sicherheitskonzept
Beschrei-bung des Informations-verbunds
Risiko-bewertung
Maßnahmen

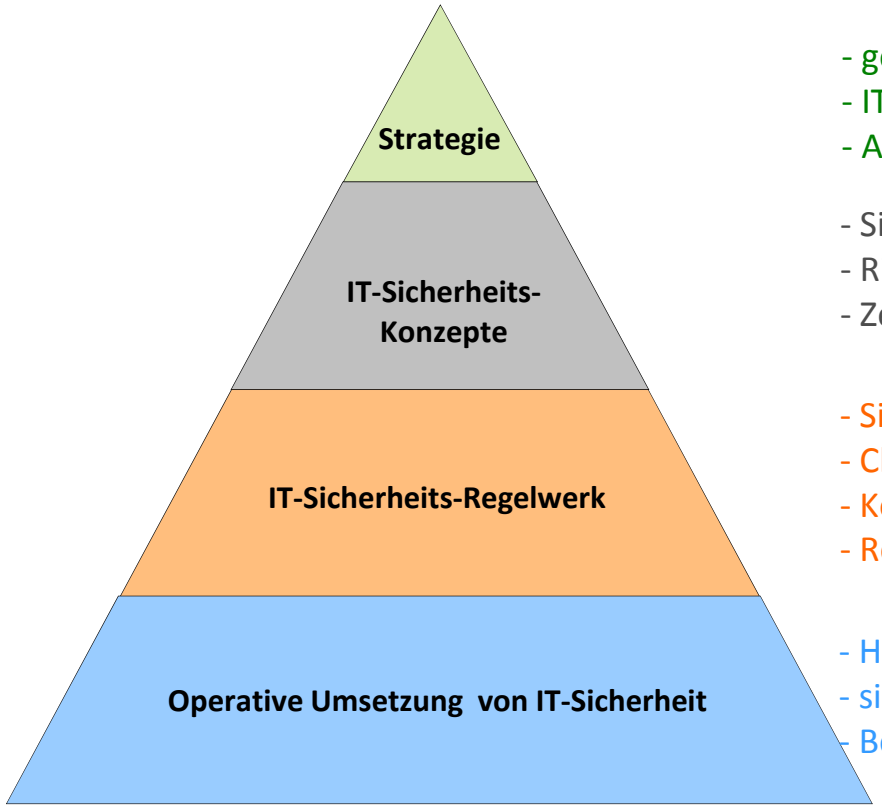
Umsetzung eines ISMS bei der Stadt Köln

1994	Einrichtung einer Arbeitsgruppe für IT-Sicherheit beim damaligen RZ-Betrieb
2001	Aufbau eines Informationssicherheitsmanagementsystems/ ISMS und Einbindung in ITIL
2002.	Einrichtung des Beirat für Sicherheit und Kommunikation mit Informationstechnik (SKIT)
2002.	Dienstanweisungen zum Umgang mit Internet und eMail, sowie zur Nutzung der IT-Infrastruktur
2003	Einrichtung der Funktion IT-Sicherheitsverantwortlicher der Stadt Köln
2005	IT-Sicherheitspolitik (Sicherheitsleitlinie)

2006	Aufbau eines IT- Notfall-Managements
2007	Entscheidung des optimierten Konzeptes zur Erstellung der Sicherheitsanalysen – enge Einbindung der Fachämter
2012	Einrichtung der Arbeitsgruppe der IT-Sicherheitsverantwortlichen des KDN
2014	BSI-Zertifizierung des städtischen Verfahrens „Elektronisches Personenstandsregister“
2015	Einrichtung der Arbeitsgruppe „Cybercrime und Cyberwar – kritische Infrastrukturen im Kölner Raum“
2019	BSI-Zertifizierung des gesamten RZ-Betriebs

IT-Sicherheitskonzept

IT-Sicherheit ist eine Daueraufgabe, kein einmaliges Projekt



- gesetzlich Vorgaben, Datenschutz
- IT-Sicherheitspolitik, Richtlinien IT-Sicherheit
- Awareness (Schulungen, etc.)

- Sicherheitskonzepte, Sicherheitsvorgaben
- Risikoanalysen, Sicherheitsanalysen
- Zertifizierung, Penetrationstests

- Sicherheitsinfrastruktur
- Change-Management, Patchmanagement,
- Konfigurationsmgmt.
- Reglementierung Rechte und Rollen

- Härtung von IT- und TK-Systemen
- sicherer Betrieb von Systemen + Netzwerk
- Beobachtung von Auffälligkeiten

Strategie IT-Sicherheit

Prävention

Entdeckung

Reaktion

- Erste Priorität liegt auf der Vermeidung von Sicherheitsvorfällen
  Prävention durch Technik, Prozesse und durch Personal

- Ein weiteres Augenmerk liegt auf der Erkennung einer möglichen Sicherheitsbedrohung oder eines möglichen Sicherheitsvorfalls
  Entdeckung durch Technik und Bewertung durch Personal

- es folgt die Bearbeitung und Behebung und im Review die Anpassung
  Schwachstelle in Prozessen, technischer Infrastruktur wird bewertet und entweder behoben oder das Risiko muss getragen werden
  Schwachstelle Personal wird nach Möglichkeit aufgelöst, z.B. durch Schulungen

Strategie IT-Sicherheit – externe Kommunikation

Konzept, bzw. Richtlinien zur Kommunikation mit externen Partnern

- Keine Kommunikation zwischen externen Kommunikationspartnern und dem internen LAN (CAN)
- Kommunikation muss immer über die Sicherheitsinfrastruktur erfolgen (Qualitätssicherung)
- Einsatz von Netz-Segmentierung je nach Aufgabe der eingesetzten Systeme (Zonenmodell)
- Kommunikationsstrecken werden bei sensiblen Daten gesichert (z.B. über VPN-Technologie)
- Keine Kommunikation ohne Viren-Scanning (sofern Protokolle es zulassen)
- bei Einsatz von privater Hardware keine Ablage von städtischen Daten auf den Systemen
- Kommunikationsstrecken über nicht-städtische Leitungen werden gesichert (z.B. über VPN-Technologie)
- 2-Faktor-Autentifizierung bei weitrechenden Zugriffen und bei Zugriff auf sensible Daten (z.B. Token, Zertifikate)
- Zugangsnetze können Internet, Standleitungen, geschlossene Netze oder Funknetze sein

à **Abwägung von Handhabbarkeit / Benutzerfreundlichkeit + Sicherheit**

Die Informationssicherheitskonzepte der Stadt Köln ruhen auf fünf Säulen

1. Genaue Dokumentationen der IT-Infrastruktur
2. Umsetzungsstand der empfohlenen BSI-Maßnahmen
3. Sicherheitsanalysen zu Basisprodukten und Fachanwendungen
4. Sicherheitsbewertungen der Fachämter
5. Ständige Qualitätssicherung unter Berücksichtigung aktueller Informationen

Organisationsübergreifende Zusammenarbeit

Informationssicherheit ist eine umfassende und anspruchsvolle Aufgabe. Sie bedarf kontinuierlicher Anstrengungen, da sich sowohl die Bedrohungen und Risiken als auch die möglichen Gegenmaßnahmen ständig weiterentwickeln.

Ein erfolgreiches Risikomanagement kann nur betrieben werden, wenn man die aktuellen Bedrohungen und funktionierende Gegenmaßnahmen kennt.

Durch beständige Zusammenarbeit im Bereich der Informationssicherheit werden Informationen über Attacken und mögliche Gegenmaßnahmen ausgetauscht. Dadurch kann wertvolles Know-how gebündelt und praktikable und wirkungsvolle Schutzmaßnahmen gezielter eingesetzt werden.

Arbeitskreis der IT-Sicherheitsbeauftragten des KDN

Der Arbeitskreis wurde am 15.07.2011 gegründet und besteht aus den Sicherheitsbeauftragten der 32 Mitgliedern des KDN

Aufgaben:

- Entwicklung von gemeinsamen Strategien und Richtlinien
- Entwicklung von Dokumentationsvorlagen
- Erfahrungs- und Informationsaustausch
- Gegenseitige Unterstützung im Krisenfall

Treffen finden vier Mal pro Jahr statt sowie bei aktuellem Bedarf

Aktuelle Beispiele:

- *Erstellung einer Sicherheitsleitlinie für den KDN-Dachverband*
- *Vorgaben und Empfehlungen zum Inhalt von Sicherheitsanalysen*
- *Muster zur Erstellung einer Notfallleitlinie nach BSI*
- *Muster zum Vorgehen bei der Feststellung des Schutzbedarfs für ein IT-Verfahren*
- *Muster zu Regeln und Vereinbarungen für die Datenverarbeitung im Auftrag, einschließlich der nach dem Datenschutzgesetz geforderten Prüfungen vor Ort*
- *Beispiele zur Durchführung von internen Audits*
- *Konzepte zur Sensibilisierung der Endnutzer zur IT-Sicherheit*
- *Etablierung eines KDN-CERT*

Arbeitskreis Cybercrime und Cyberwar - kritische Infrastrukturen im Kölner Raum

Arbeitsaufnahme des Arbeitskreises am 07.01.2015

Teilnehmer

Stadt Köln

- *12*
- *12/1*
- *1300*
- *37*
- *66*

Weitere Interessenten

- *Abfallwirtschaftsbetriebe Köln*
- *Häfen der Stadt Köln*

Partner aus der Region die zur kritischen Infrastruktur im Kölner Raum gehören

- *Rheinenergie*
- *Netcologne*
- *Universitätskliniken Köln*
- *Kliniken der Stadt Köln*
- *Flughafen Köln-Bonn*
- *Bayerwerke*
- *Landeskriminalamt NRW*
- *Polizeipräsidium Köln*
- *Verfassungsschutz NRW*
- *Luftwaffe Köln-Bonn*
- *KVB*

Ziele:

- gemeinsamer Schutz der Infrastruktur vor Cybercrime- und Cyberwar- Angriffen
- Informationsbeschaffung und -bewertung (CERT)
- Workflow und Informationsfluss bei Angriffen und anderen Sicherheitsvorfällen
- Abgestimmte Reaktionen und ggf. gemeinsame Maßnahmen
- Beschreibung von kritischen Szenarien für die Beteiligten und die Erstellung gemeinsamer Maßnahmenpläne

BSI-Grundschutzzertifizierung auf Basis von ISO 27001

- Erteilung des Zertifikat ISO/IEC 27001 für das Verfahren „elektronische Personenstandsregister/ePR“ auf Basis von IT-Grundschutz am 01.10.2014 gültig bis zum 01.10.2017

- Erteilung des Dachzertifikats ISO/IEC 27001 für den gesamten „RZ-Betrieb“ auf Basis von IT-Grundschutz am 07.05.2019 gültig bis zum 06.05.2022
  in diesem Audit wurde auch der Baustein Datenschutz aufgenommen

Deutsches IT-Sicherheitszertifikat
erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-IGZ-0352-2019

ISO 27001-Zertifikat auf der Basis von IT-Grundschutz
Basisdienste Rechenzentrum Stadt Köln
der Stadt Köln
gültig bis: 7. Mai 2022*

Bundesamt für Sicherheit in der Informationstechnik
ISO 27001-Zertifikat
auf der Basis von IT-Grundschutz
Zertifikat Nummer:
BSI-IGZ-0352-2019
Gültig bis 07.05.2022

Vielen Dank für Ihre Aufmerksamkeit.

Ich freue mich nun auf Ihre Fragen.

Udo Zaudig
IT-Sicherheitsverantwortlicher der Stadt Köln

udo.zaudig@stadt-koeln.de