

dataport

Risikosituation - worin sich die öffentliche Verwaltung von der Wirtschaft unterscheidet

Unterschiede in der Risikosituation und Praxisbeispiele

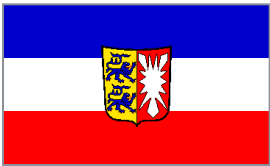




Agenda

- Kurzvorstellung Dataport
- Das politische Umfeld
- Auswertung von Schutzbedarfsfeststellungen und Risikoanalyse
- Auswertung von Sicherheitsvorfällen
- Herausforderungen in der Umsetzung von IT-Grundschutz

Dataport: Fünf-Länder-Anstalt



Eigentümer / Träger

- Freie und Hansestadt Hamburg (34,48%)
- Schleswig-Holstein (34,48%)
- Freie Hansestadt Bremen (6,9%)
- Mecklenburg-Vorpommern (6,9%)
- Niedersachsen (17,24%)

Anstalt öffentlichen Rechts

Gründung durch Staatsvertrag



Dataport ist der Dienstleister für Informations- und Kommunikationstechnik der öffentlichen Verwaltung in Schleswig-Holstein, Hamburg und Bremen sowie für die Steuerverwaltung in Mecklenburg-Vorpommern und Niedersachsen.

Dataport: Auftrag & Portfolio

Auftrag

Dataport unterstützt die öffentlichen Verwaltungen in dem Land Schleswig-Holstein, einschließlich der Kommunalverwaltungen, der Freien und Hansestadt Hamburg und der Freien Hansestadt Bremen sowie weiterer Träger (§ 1 Abs. 1 Satz 4) durch Informations- und Kommunikationstechniken.

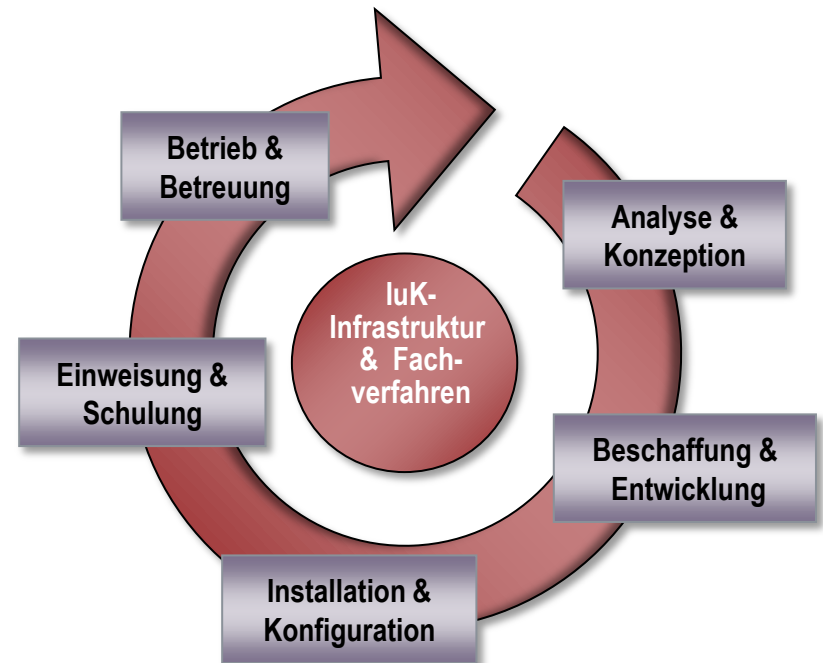
Sie fungiert insbesondere als zentrale IT-Dienstleisterin des Landes Schleswig-Holstein, der Freien und Hansestadt Hamburg und der Freien Hansestadt Bremen. [...]

Für die Länder Mecklenburg-Vorpommern und Niedersachsen ist Dataport durch das Data Center Steuern im Bereich der IT-Unterstützung der Steuerverwaltung tätig.

Dataport unterstützt seine Träger im Bereich Druck durch das an mehreren Standorten betriebene Druckzentrum, für Mecklenburg-Vorpommern gilt dies nur für den Bereich Data Center Steuern.

Staatsvertrag, § 3 Absatz 1

Portfolio



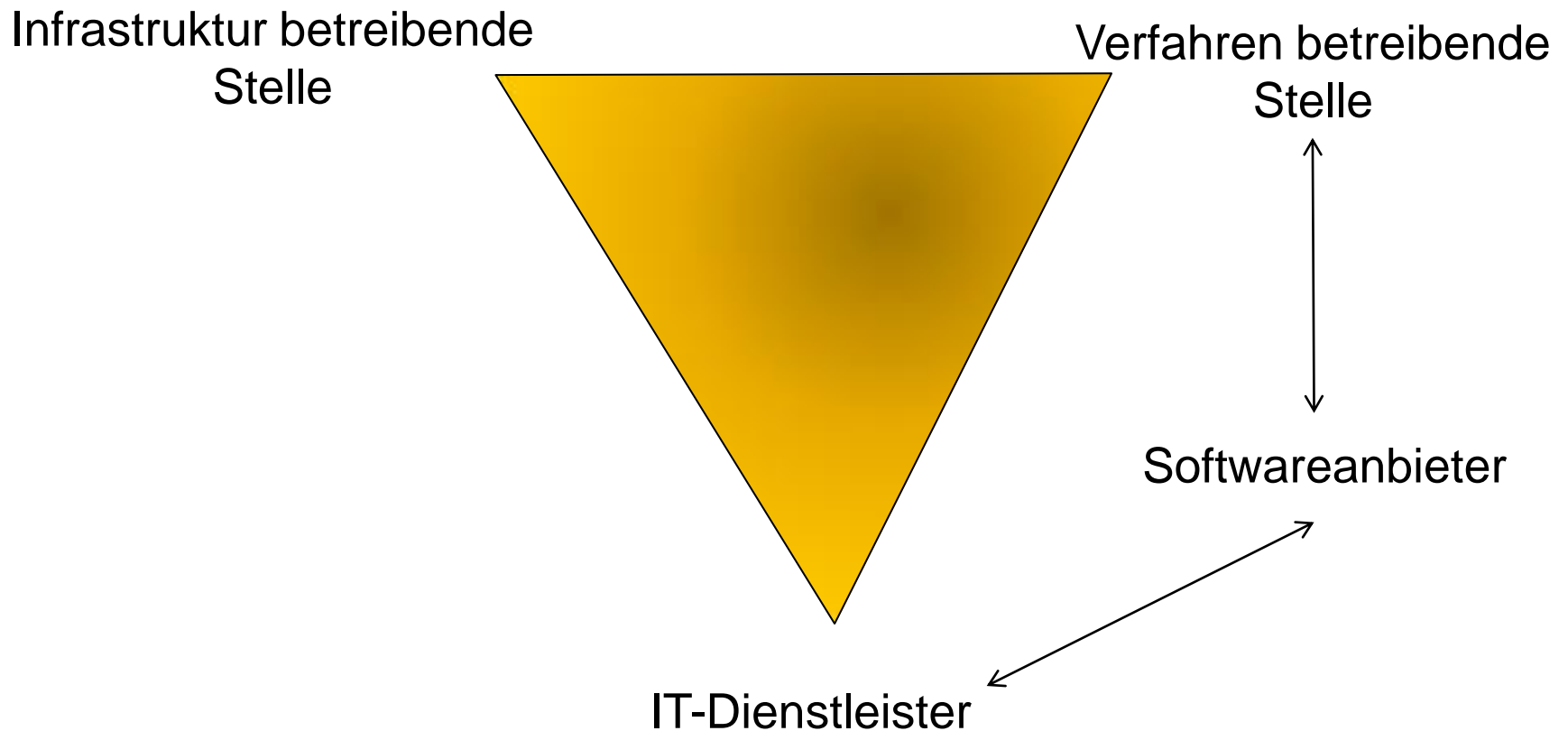


Abgrenzung unserer Aufträge

- Hochschulen betreiben ihre pädagogischen oder Forschungsnetze in Eigenregie.
- Geheimdienste haben eine eigene IT-Infrastruktur.
- Dies gilt weitgehend auch Behörden, die Bedarf für hohe VS-Klassen (VS-Vertraulich, VS-Geheim etc.) haben.



Das politische und technische Umfeld





Das politische und technische Umfeld (Fortsetzung)

- Teilweise weitreichende Autonomie der Behörden
- Heterogenität der Anforderungen und IT-Möglichkeiten
 - Behördenstruktur reicht von kleinen, ländlichen Kommunen (ab ca. 30 MA) bis hin zu zentralistischen Stadtstaaten (über 60.000 MA)
 - Schutzbedarfe liegen zwischen normal und hoch – Schutzbedarf sehr hoch ist eine absolute Ausnahme
- Große Breite der Prozesse und Anwendungen
 - Beispiel: In der Freien und Hansestadt Hamburg werden für die Umsetzung von ca. 500 Verfahren 1500 Anwendungen eingesetzt
 - Die Mehrzahl dieser Anwendungen sind Spezialanwendungen (Beispiel: Software für Meldeämter) oder sie sind stark für den Einsatz in der öffentlichen Verwaltung gecustomized (z.B. SAP)



Das politische und technische Umfeld (Fortsetzung)

- Grundsätzlich sind Zuständigkeiten und Verantwortlichkeiten klar geregelt auf
 - Behördenebene (Welche Behörde hat welche gesetzliche Aufgaben?)
 - Mitarbeiterenebene (Geschäftsverteilungspläne)



Welche Faktoren erhöhen den Schutzbedarf?

- Grundsätzlicher Trend des Ersetzens „Elektronischer Begleitverfahren“ durch eGovernment-Verfahren
 - Schutzbedarf normal ist hinsichtlich der Verfügbarkeit für die absolute Mehrheit der Verfahren nicht mehr akzeptabel
 - Treibende Faktoren: Gesetzliche Ansprüche der Bürger, weniger Arbeitsausfall
- Das Definieren finanzieller Grenzen fällt im Unterschied zur Privatwirtschaft (Rücklagen / Kapitaldeckung / Insolvenzrecht) schwer:
 - Ab wann ist ein finanzieller Schaden für eine Kommune / ein Bundesland existenzbedrohend?
 - In der Folge führen potentielle finanzielle Schäden nur in Ausnahmefällen zu hohem Schutzbedarf



Welche Faktoren erhöhen den Schutzbedarf? (Fortsetzung)

- Rufschäden spielen eine Rolle
 - finanziell sind sie meist nicht konkret fassbar (kein Umsatzverlust), aber politisch qualitativ bewertbar

- Mögliche Personenschäden wirken sich v.a. hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität aus
 - (Rettungs-) Leitstellen
 - Verfahren im Bereich Jugend, Familie und Soziales
 - Polizeiverfahren



Welche Faktoren erhöhen den Schutzbedarf? (Fortsetzung)

- Wichtige Faktoren für hohen Schutzbedarf insb. hinsichtlich Vertraulichkeit und Integrität:
 - Datenschutz (Indiz: Verarbeitung besonderer Arten personenbezogener Daten)
 - Gesetzliche Vorgaben zum Schutz der Bürger in Form von
 - bereichsspezifischen Amtsgeheimnissen (z.B. Steuergeheimnis, Statistisches Geheimnis, Sozialgeheimnis etc.) und
 - konkreten technischen Vorgaben (z.B. Vorgabe zum Einsatz bestimmter Arten elektronischer Signaturen)



Welche Faktoren erhöhen den Schutzbedarf? (Fortsetzung)

Fazit:

- Hoher Schutzbedarf ist in diesem Umfeld überwiegend verursacht durch
 - gesetzliche Vorgaben und darin ausgedrückt
 - die Interessen Dritter (Betroffene im Sinne des Datenschutzrechtes, Bürger)

- Ein „Verwaltungsgeheimnis“ in Analogie zum Betriebs- oder Geschäftsgeheimnis spielt praktisch keine Rolle
 - Informationsfreiheitsgesetze



Vorbemerkung zur Auswertung von Sicherheitsvorfällen

Sicherheitsvorfälle unterscheiden sich nach unserem Verständnis von betrieblichen Störungen (Incidents nach ITIL) durch

- Verlust von Vertraulichkeit, Verfügbarkeit oder Integrität
- bei gleichzeitigem Verstoßcharakter

Als eCrime verstehen wir (wirtschafts-)kriminelle Handlungen unter Einsatz von Computer- oder Kommunikationssystemen

Traditionelle, in der Verwaltung auftretende Rechtsverstöße werden im Sicherheitsmanagement nicht bearbeitet und erfasst:

- Korruption
- Betrug / Manipulation von Vergabeverfahren
- Amtsmissbrauch / Strafvereitelung im Amt

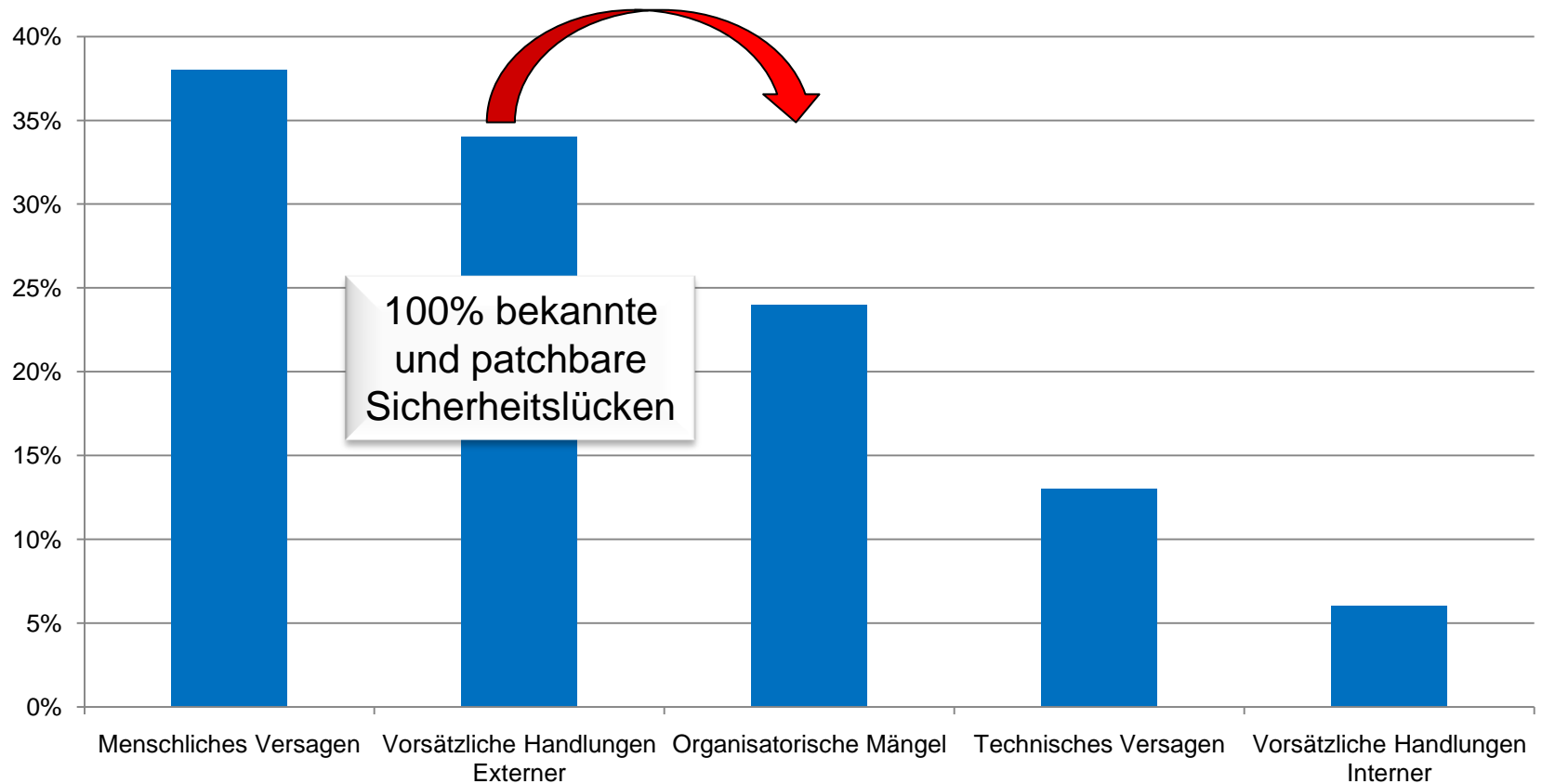


Statistische Daten aus dem Umfeld

eCrime und e(Wirtschafts-) Spionage gewinnen erheblich an Bedeutung

- Statistiken von PwC, KPMG und dem BMI
- Ziel sind v.a. Forschungsergebnisse / Wissen / Patente angegriffener Organisationen
- Bedeutende Angriffswege sind
 - Interne Mitarbeiterinnen und Mitarbeiter
 - Einsatz von Schadsoftware durch Externe
 - Dienstleister / Leiharbeiter

Alle Sicherheitsvorfälle 2010 in deren Bearbeitung Dataport involviert war und ihre Ursachen



(Stand 20.01.2011, Mehrfachzuordnungen möglich)



Externe Quellen und Zwischenfazit

Das Bundesverfassungsschutz hat keine Erkenntnisse darüber, dass eSpionage im Bereich der Landesverwaltungen derzeit eine signifikante Rolle spielt.

Das stellt sich in bestimmten Bereichen der Bundesverwaltung deutlich anders dar.

Zwischenfazit:

eCrime und eSpionage spielen in der Landes- und Kommunalverwaltung noch keine große Rolle



Plausibilisierung

Was sind die Ziele von eCrime?

- Gewinnerzielung bei geringem (Technik-) Einsatz und Risiko; Methoden:
 - Umleitung/Manipulation von Geldströmen
 - Aufwändig, da Zahlungen anders als beim Homebanking abgewickelt werden
 - Erpressung (z.B. via DDoS, Datenverschlüsselung, „Datendiebstahl“ und Drohung mit Veröffentlichung)
 - Erpressung des Staates mit erheblichen Risiken verbunden
 - Erpressung via DDoS derzeit wenig wirksam, da Verwaltungsprozesse noch wenig auf das Internet angewiesen sind
 - „Diebstahl“ von Know-How, Verkauf oder Nutzung zur Verbesserung der eigenen Marktposition (Umsatz, Gewinn)
 - Marktwert von Verwaltungsdaten nicht mit Produkt- oder Vertriebsdaten aus der Wirtschaft vergleichbar



Plausibilisierung (Fortsetzung)

- Gewinnerzielung bei geringem (Technik-) Einsatz und Risiko;
Methoden:
 - SPAM-Versand
 - Nutzung fremder IT-Ressourcen für die o.g. Zwecke
 - beide Ziele auch für die öffentliche Landes- und Kommunalverwaltung relevant
 - Landesnetze stellen erhebliche, relativ einheitlich konfigurierte IT-Ressourcen mit breitbandiger Internetanbindung zur Verfügung – kurz alles was ein BotNet braucht

Fazit: Die Beobachtungen aus dem IT-Sicherheitsvorfallmanagement hinsichtlich eCrime und eSpionage sind ursächlich nachvollziehbar



Herausforderungen in der Umsetzung von IT-Grundschutz

Die Vielzahl der beteiligten Partner in den Sicherheitsmanagementsystemen führt zu erheblichen Herausforderungen auf Ebene sicherheitsrelevanter Prozesse

- Folge: Hoher Anteil an Sicherheitsvorfällen, die unmittelbar oder mittelbar auf organisatorische Mängel zurückzuführen sind
- Überprüfung und Verbesserung dieser Prozesse ist eine wesentliche Aufgabe eines ISMS in diesem Umfeld

Die Abhängigkeit von Behörden von elektronischer Datenverarbeitung steigt im Zuge der Ausweitung von eGovernment erkennbar

- Redundanzkonzepte gehören somit in fast jedes Sicherheitskonzept
- die öffentliche Verwaltung folgt damit zeitlich verzögert dem in der Wirtschaft schon länger zu beobachtenden Trend



Herausforderungen in der Umsetzung von IT-Grundschutz

eCrime und eSpionage spielen in diesem Umfeld noch keine große Rolle

- Dies schlägt sich in den Konzepten zum Schutz vor Schadsoftware nieder

Hoher Schutzbedarf bezogen auf Integrität und Vertraulichkeit, aber auch Verfügbarkeit, folgt oft unmittelbar aus gesetzlichen Vorgaben

- Compliance spielt eine noch deutlich größere Rolle als in der Wirtschaft
- kryptografische Methoden haben im Rahmen von Risikoanalysen herausragende Bedeutung

Vielen Dank für Ihre Aufmerksamkeit!

dataport 

The logo graphic consists of six horizontal red bars stacked vertically, positioned to the right of the word 'dataport'.