

EURORAI-Seminar  
zur Cyber- und Informationssicherheit am 19. April 2018

# **Prüfungsaufgabe: IT-Sicherheit - von der Nische zur Notwendigkeit -**

Direktor beim Landesrechnungshof Brandenburg Thomas Kersting



## Übersicht

1. Aktuelle Berichterstattung zur IT-Sicherheit in Brandenburg
2. Rahmenbedingungen
3. Prüfungsmaßstäbe der Rechnungshöfe
4. Prüfungskapazität
5. Feststellungen des Rechnungshofes Brandenburg
6. Limitierung der Prüfungen
7. Folgen für die Finanzkontrolle

## 1 - Aktuelle Berichterstattung zur IT-Sicherheit in Brandenburg

- Landesverwaltungs-PCs anfällig für Internetangriffe

Zahl der schweren Sicherheitsvorfälle, die nicht durch automatische Filter abgewehrt konnten, stieg in den letzten fünf Jahren um über 200 % - von 2013 bis 2017 insgesamt 320 Cyberattacken.

- „Web-View“-Datenleck

Polizeibeamte veröffentlichten Interna zu Straftaten in einem großen sozialen Netzwerk und leiteten sie auch an die Presse weiter.

## 2 - Rahmenbedingungen

### Rahmenbedingungen der Digitalisierung von Verwaltungsprozessen

- Verfassungsrechtlich garantierte Aufgabenerfüllung
- Rechtsstaatlichkeit
- Integrität des digitalen Staates
- Informationssysteme als kritische Infrastrukturen
- Risiko von finanziellen Schäden und Vertrauensverlust

### Gleichzeitig

- Zunahme der IT-Unterstützung in der öffentlichen Verwaltung
- Weitreichende Vernetzung untereinander und nach außen
- Effiziente Verwaltungsprozesse als Standortvorteil

## 2 - Rahmenbedingungen

Deutschland

Bund

Länder

Kommunen

Vielfalt von IT-Netzen

⇒ Ohne Verpflichtung zur Einhaltung von einheitlichen Mindestsicherheitsstandards

Rechtliches Problem:  
Grundsätzliches Verbot der Mischverwaltung

## 2 - Rahmenbedingungen

Verfassungsrechtlich erzwungene Kooperation  
versus  
(staats-)vertragliche Kooperation

=> Artikel 91 c Grundgesetz

- bestehende IT-Gremien- und Entscheidungsstrukturen vereinfacht
- lückenlose und medienbruchfreie elektronische Kommunikation zwischen den Behörden von Bund, Ländern und Kommunen
- ausschließliche Gesetzgebungskompetenz des Bundes für ein Verbindungsnetz der Verwaltungen von Bund und Ländern

## 2 - Rahmenbedingungen



Quelle: Internet-Präsentationsseiten des IT-Planungsrates, Aufgaben des IT-Planungsrates.

### 3 - Prüfungsmaßstäbe der Rechnungshöfe

Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik („IuK-Mindestanforderungen“)

- wesentliche Handlungsfelder bei IT-Prüfungen
- gemeinsame und transparente Prüfungsmaßstäbe auf Basis von Prüfungserkenntnissen der Rechnungshöfe
- Infrastrukturelle, organisatorische, personelle und technische Maßnahmen zur Informationssicherheit



### 3 - Prüfungsmaßstäbe der Rechnungshöfe

#### Papier der Rechnungshöfe zum Informationssicherheitsmanagement

- Informationssicherheit ist Leitungsaufgabe
- Integration der IT-Sicherheit in die organisationsweiten Prozesse
- Angemessenes / zentrales Informationssicherheitsmanagementsystem (ISMS)
- Kontinuierliche Überwachung und Verbesserung der Wirksamkeit und Umsetzung des Informationssicherheitsmanagementsystems
- IT-Sicherheitsbeauftragte außerhalb des operativen IT-Managements
- ausreichend qualifiziertes Informationssicherheitsmanagement-Personal
- Schutzbedarfs-/ Risikoanalysen
- Beachtung des Grundsatzes der Wirtschaftlichkeit und Sparsamkeit
- Audit-Verfahren oder Revisionen

## 4 - Prüfungskapazität

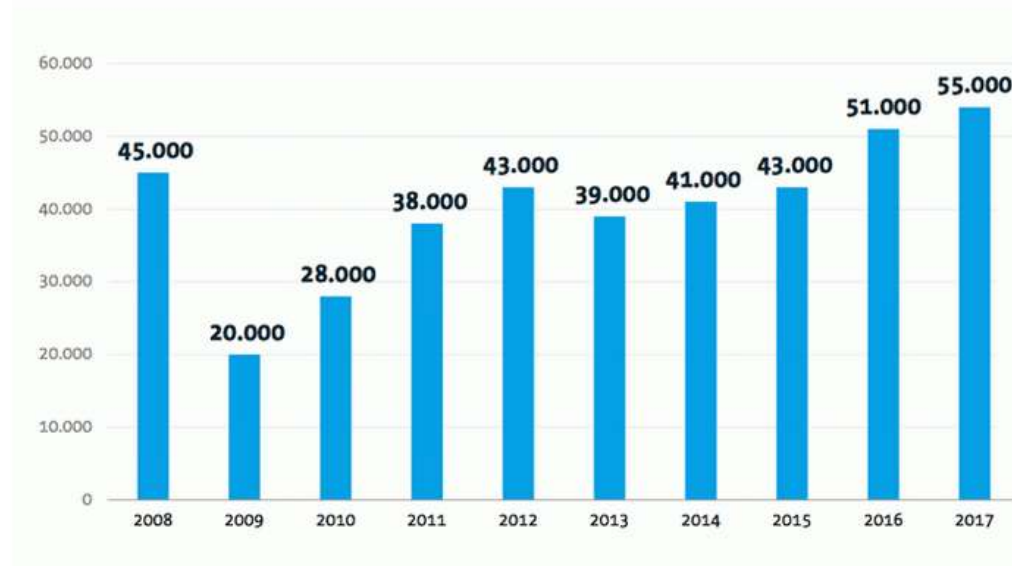
<p>LANDES RECHNUNGSHOF BRANDENBURG</p> <p>Organisationsplan des Landesrechnungshofes Brandenburg ab 1. Januar 2018</p>			
<p><b>Präsidentalabteilung</b> <i>Veit König (8567)</i></p> <p><b>Sekretariat</b> Kathrin Rudolph (8520)</p> <p><b>Pr 1 Personal und Organisation</b></p> <p><b>Pr 2 Haushalt</b></p> <p><b>Pr 3 Informationstechnik</b></p>		<p><b>Präsident</b> <i>Christoph Weiser (8500)</i></p> <p><b>Sekretariat</b> Victoria Hartmann (8501) Lynn Galler (8502)</p> <p><b>Vizepräsidentin</b> <i>Dr. Sieglinde Reinhardt</i></p>	
<p><b>Büro des Präsidenten</b> <i>Katrin Rautenberg (8506)</i></p> <ul style="list-style-type: none"> <li>- Presse und Öffentlichkeitsarbeit</li> <li>- Eingaben Dritter</li> <li>- Organisation der Präsidenten- und Regionalkonferenzen</li> <li>- Sonderaufgaben des Präsidenten</li> <li>- Zentrale Poststelle</li> <li>- Redaktionelle Bearbeitung des Jahresberichts</li> <li>- Planung und Organisation besonderer Anlässe</li> </ul>			
<p><b>I</b> <i>Christoph Weiser (8500)</i></p> <p><b>Sekretariat</b> N. N.</p> <p><b>I 1</b></p> <ul style="list-style-type: none"> <li>- Epl. 12 Ministerium der Finanzen (Allgemeine Bewilligungen und Landeshauptkasse)</li> <li>- Epl. 20 Allgemeine Finanzverwaltung (außer Kommunaler Finanzausgleich, Steuern, Hochwasserkatastrophe, Kommunales Infrastrukturprogramm und Versorgung)</li> <li>- Jahresabschluss, Haushaltsnachweisung und -rechnung</li> <li>- Sondervermögen</li> <li>- Feststellungen zur Haushalts- und Vermögensrechnung</li> <li>- Grundsatzangelegenheiten des Haushaltsrechts, einschließlich Fortentwicklung des Haushaltsrechts sowie der zentrale Belegprüfung</li> <li>- Finanz- und Haushaltsmanagement des Landes</li> <li>- HRR-Verfahren</li> </ul> <p><b>I 2</b></p> <ul style="list-style-type: none"> <li>- Epl. 03 Ministerpräsident/Fraktionen</li> <li>- Epl. 08 Ministerium des Innern (Verfassungsschutz)</li> <li>- Epl. 20 Allgemeine Finanzverwaltung (kommunaler Finanzausgleich)</li> <li>- Lage und Entwicklung der Landesfinanzen</li> <li>- EU-Ansprechpartner (auch für die EU-Prüfungsdienstanalyse)</li> <li>- Internationales Zusammenarbeit (EUROPARCO)</li> <li>- Präsidenten- und Regionalkonferenzen</li> <li>- Personalhaushalt des Landes einschließlich Versorgung und Personalbedarfsplanung</li> <li>- Prüfungsstelle des Landesrechnungshofes</li> </ul>	<p><b>II</b> <i>Thomas Kersting (8600)</i></p> <p><b>Sekretariat</b> Heike Bronowski (8601)</p> <p><b>II 1</b></p> <ul style="list-style-type: none"> <li>- Epl. 01 Landtag</li> <li>- Prüfung der Fraktionen gemäß § 12 Fraktionsgesetz</li> <li>- Epl. 06 Ministerium für Wissenschaft, Forschung und Kultur</li> <li>- nachgeordnete Einrichtungen, Landesbetriebe und Stiftungen im Bereich des Einzelplans 06</li> </ul> <p><b>II 2</b></p> <ul style="list-style-type: none"> <li>- Epl. 08 Ministerium des Innern und für Kommunales (außer Verfassungsschutz)</li> <li>- Epl. 09 Ministerium der Justiz, für Europa und Verbraucherschutz</li> <li>- Amt für Statistik, Berlin Brandenburg</li> <li>- nachgeordnete Einrichtungen, Landesbetriebe und Stiftungen im Bereich der Einzelpläne 03 und 04</li> </ul> <p><b>II 3</b></p> <ul style="list-style-type: none"> <li>- Epl. 05 Ministerium für Bildung, Jugend und Sport</li> <li>- Epl. 14 Verfassungsbereich</li> <li>- nachgeordnete Einrichtungen, Landesbetriebe und Stiftungen im Bereich des Einzelplans 05</li> </ul> <p><b>II 4</b></p> <ul style="list-style-type: none"> <li>- Epl. 12 Ministerium der Finanzen (Allgemeine Bewilligungen und Landeshauptkasse)</li> <li>- Grundsatzangelegenheiten der Informationstechnik</li> <li>- Grundsatzangelegenheiten der Organisation</li> <li>- Digitalisierung</li> <li>- Grundsatzangelegenheiten des Dienst-, Arbeits- und Tarifrechts und Arbeitsstellen Dienstrechts</li> </ul> <p><b>Stabsstelle</b></p> <ul style="list-style-type: none"> <li>- Anforderungen an eine langfristig orientierte Personalstrategie des Landes Brandenburg</li> <li>- Durchführung der zentralen Belegprüfung</li> </ul>	<p><b>III</b> <i>Hans-Jürgen Klees (8510)</i></p> <p><b>Sekretariat</b> Birgit Paulick (8511)</p> <p><b>III 1</b></p> <ul style="list-style-type: none"> <li>- Epl. 08 Ministerium für Wirtschaft und Energie</li> <li>- EU-Strukturfonds (EFRE)</li> <li>- Investitionsbank des Landes Brandenburg</li> <li>- Handwerkslämmern</li> <li>- Industrie- und Handelskammern</li> <li>- nachgeordnete Einrichtungen, Landesbetriebe und Stiftungen im Bereich des Einzelplans 08</li> </ul> <p><b>III 2</b></p> <ul style="list-style-type: none"> <li>- Epl. 07 Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie</li> <li>- Epl. 12 Ministerium der Finanzen (außer Allgemeine Bewilligungen, Landeshauptkasse und Zentrale Bezugsstelle)</li> <li>- Epl. 20 Allgemeine Finanzverwaltung (Steuern)</li> <li>- Prüfung der Abgabenverteilung</li> <li>- Grundsatzangelegenheiten des Steuerrechts</li> <li>- EU-Strukturfonds (ERDF)</li> <li>- nachgeordnete Einrichtungen, Landesbetriebe und Stiftungen im Bereich der Einzelpläne 07 und 12 (außer Brandenburgischer Landesbetrieb für Liegenschaften und Bauen)</li> </ul> <p><b>III 3</b></p> <ul style="list-style-type: none"> <li>- Landesbeihilfen</li> <li>- Rundfunk und Medien, Filmförderung</li> <li>- Ostdeutscher Sparkassenverband</li> <li>- Einvernehmen zur Bestellung der Abschlussprüfer</li> </ul>	<p><b>IV</b> <i>Dr. Sieglinde Reinhardt (8630)</i></p> <p><b>Sekretariat</b> Michaela Tosch (8631)</p> <p><b>IV 1</b></p> <ul style="list-style-type: none"> <li>- Epl. 11 Ministerium für Infrastruktur und Landesplanung</li> <li>- Hochbau und städtebaulich geförderter Hochbau (einschließlich 05F)</li> <li>- Brandenburgischer Landesbetrieb für Liegenschaften und Bauen</li> <li>- nachgeordnete Einrichtungen und Stiftungen im Bereich des Einzelplans 11</li> </ul> <p><b>IV 2</b></p> <ul style="list-style-type: none"> <li>- Epl. 11 Ministerium für Infrastruktur und Landesplanung</li> <li>- Straßen- und Brückenbau</li> <li>- Verkehrsmaßnahmen im Bereich Verkehr</li> <li>- Landesbetrieb Straßenwesen</li> <li>- nachgeordnete Einrichtungen und Stiftungen im Bereich des Einzelplans 11</li> </ul> <p><b>IV 3</b></p> <ul style="list-style-type: none"> <li>- Epl. 10 Ministerium für Ländliche Entwicklung, Umwelt und Landwirtschaft</li> <li>- Landesbetrieb Forst Brandenburg</li> <li>- EU-Strukturfonds (ELER)</li> <li>- nachgeordnete Einrichtungen und Stiftungen im Bereich des Einzelplans 10</li> </ul>

## 4 - Prüfungskapazität

### Fachkräftemangel: Bitkom zählt 55.000 offene Stellen für IT-Spezialisten

07.11.2017 12:20 Uhr - Andreas Wilkens

vorlesen



Entwicklung der Zahl der offenen Stellen für IT-Fachkräfte seit 2008. (Bild: bitkom.org)



### Prüfungsaufgabe: IT-Sicherheit - von der Nische zur Notwendigkeit -

## 4 - Prüfungskapazität

### **IT-Branche schafft tausende neue Arbeitsplätze - und beklagt massiven Fachkräftemangel**

- 45.000 zusätzliche Neueinstellungen von IT-Fachkräften 2017
- Konjunkturausblick sehr positiv
- historisch stärkster Beschäftigungszuwachs innerhalb eines Jahres
- 2018 wird ein Stellenzuwachs um 42.000 erwartet

Artikel vom 14.02.2018 - <https://www.heise.de/newsticker/meldung/Bitkom-IT-Branche-schafft-tausende-neue-Arbeitsplaetze-und-beklagt-massiven-Fachkraeftemangel-3969322.html>

## 5 - Feststellungen des Rechnungshofs (Beispiel Justiz)

- IT-Grundschatz im Geschaftsbereich nicht sichergestellt
  - Brandlasten vorhanden
  - Rauchmelder abgestellt
  - Technikraum als „Fitnessraum“ fur Mitarbeiter umgebaut

(2013)

- Brand- und Katastrophenschutz
  - IT-Sicherheitskonzept erstellt
  - aber in wesentlichen Teilen nicht umgesetzt
    - kein Notfallmanagementkonzept
    - keine Brandmelder im Serverraum
    - Zugang zum Serverraum offen – es soll kalte Luft hereinziehen

(2014)

## 5 - Feststellungen des Rechnungshofs (Beispiel Justiz)

- lokaler Server
  - unverschlossen, für jeden zugänglich
  - ehemalige Sanitäreinrichtung

Trotzdem:

- Aufsichtsbehörde will mangelhaften Zustand zunächst belassen
- kontroverse Diskussion im Parlament
- endgültige Lösung steht noch aus



(2016)

## 5 - Feststellungen des Rechnungshofs (Beispiel Landesrechenzentrum)

Landesrechenzentrum mit erheblichem Ausfallrisiko

Es fehlten

- Notfallmanagement, Risikoanalyse, abgeleitete Schutzmaßnahmen
- stationäre Brandlöschanlage
- Ausreichende Stromversorgung
- Ausreichende Klimatisierung

Keine strikte Trennung von Test-, Integrations- und Produktivumgebung

- Folge: Systemausfall in mehreren Ressorts

Gleichzeitige Nutzung als Schulungsgebäude

- Risiko für Zugangsschutz



## 5 - Feststellungen des Rechnungshofs (Beispiel Landesrechenzentrum)





## 6 - Limitierung der Prüfungen

### Kapazitätsgrenzen für Prüfungen

- korrekte Implementierung von Firewall-Filterregeln, Routingtabellen  
Nachweis, dass Netztopologie den Konzepten/Vorgaben entspricht
- Prüfung implementierter VPN-Lösungen
- Tests der sicheren Härtung von Servern
- Prüfung aller Fachverfahren auf Verwundbarkeit aus dem eigenen und fremden Netzen
- Validierung der Notfallkonzepte in realen Notfallsituationen

## 7 - Folgerungen für die Finanzkontrolle

- Kapazitäten erweitern
- Personalfort- und -weiterbildung
- Personalgewinnung (IT-Kompetenz)
- Externe Beratung
- Kooperation der Rechnungshöfe, um Synergieeffekte zu erzielen
- Interne IT-Sicherheit sicherstellen
  - selbst Standards einhalten, ggfs. externe Begleitung
  - dauerhafte interne Sensibilisierung