STAATSMINISTERIUM
DES INNERN

Freistaat
SACHSEN

Informationssicherheit in der öffentlichen Verwaltung

BfIS-Land – Informationssicherheit in der Landesverwaltung

Warum Informationssicherheit?

- Die überwiegende Mehrzahl aller Verwaltungsprozesse in Kommunalverwaltungen wird heute elektronisch unterstützt. Damit hängt die Arbeitsfähigkeit jeder Verwaltung essentiell von der Sicherheit und Verfügbarkeit der dazu notwendigen Daten und IT-Infrastrukturen ab.

- Umfragen der SAKD zur IT-Infrastruktur sächsischer Kommunalverwaltungen ergaben, dass **nur in ca. 30 % aller Verwaltungen IT-Sicherheitskonzepte vorliegen** und nur ca. **20 % der Verwaltungen einen namentlich benannten IT-Sicherheitsbeauftragten haben**.

- Diese Situation wird der Bedeutung der Informationssicherheit für das Funktionieren einer modernen Verwaltung nicht gerecht.

Verwaltungen im Visier von Hackern

Wegen Jazenjuk-Besuch: Hacker legen Website der Bundeskanzlerin lahm

Angela Merkel und der ukrainische Ministerpräsident Arseni Jazenjuk bei einem Treffen in Kiew: Website des Bundestags zeitweise lahmgelegt

DPA

Webseiten offline

07. Januar 2015 17:32 Uhr

Hacker attackieren bundestag.de und Merkel-Seite

Eine Cyber-Attacke trifft Internetseiten der Bundesregierung. Der Verursacher gibt sich zu erkennen: Prorussische Hacker wollen ein Zeichen setzen zum Berlin-Besuch des ukrainischen Regierungschefs.

Vorübergehend geschlossen

Autozulassungsbehörden melden Hackerangriff

23.06.2015, 08:14 Uhr | dpa

...ttacke geschlossen: Dutzende Kfz-Zulassungsstellen in Hessen und Rheinland-Pfalz sind lahmgelegt. (Quelle: dpa)

23. JUNI 2015

NACH HACKER-ANGRIFF

Warten auf die Zulassung

Von JUDITH KÖNEKE

Bundestags-Hack: Zehntausende Internetseiten für Abgeordnete gesperrt

heise online 26.06.2015 14:17 Uhr

(Bild: Mike Macke, CC BY 2.0)

Als Reaktion auf den Hackerangriff hat die Bundestagsverwaltung den Parlamentscomputern nun angeblich den Zugriff auf Zehntausende Internetseiten gesperrt. Das soll weitere Trojaner-Infizierungen verhindern.

14. Juni 2015, 11:25 Uhr Hackerangriff auf den Bundestag

Gesamtes IT-Netz des Bundestages muss ausgetauscht werden

ANZEIGE

Der Schaden nach dem Hackerangriff auf den Bundestag ist höher als bislang angenommen. Experten zufolge könnte die Installierung eines neuen IT-Systems mehr als ein Jahr dauern.

29. Dezember 2014, 14:46 Uhr Trojaner "Regin"

Regierung dementiert Gefährdung von Computern im Kanzleramt

Spähen aufs Kanzleramt: Auf dem Computer einer Merkel-Mitarbeiterin ist die Spähsoftware "Regin" aufgetaucht. (Foto: picture alliance / dpa)

Regin

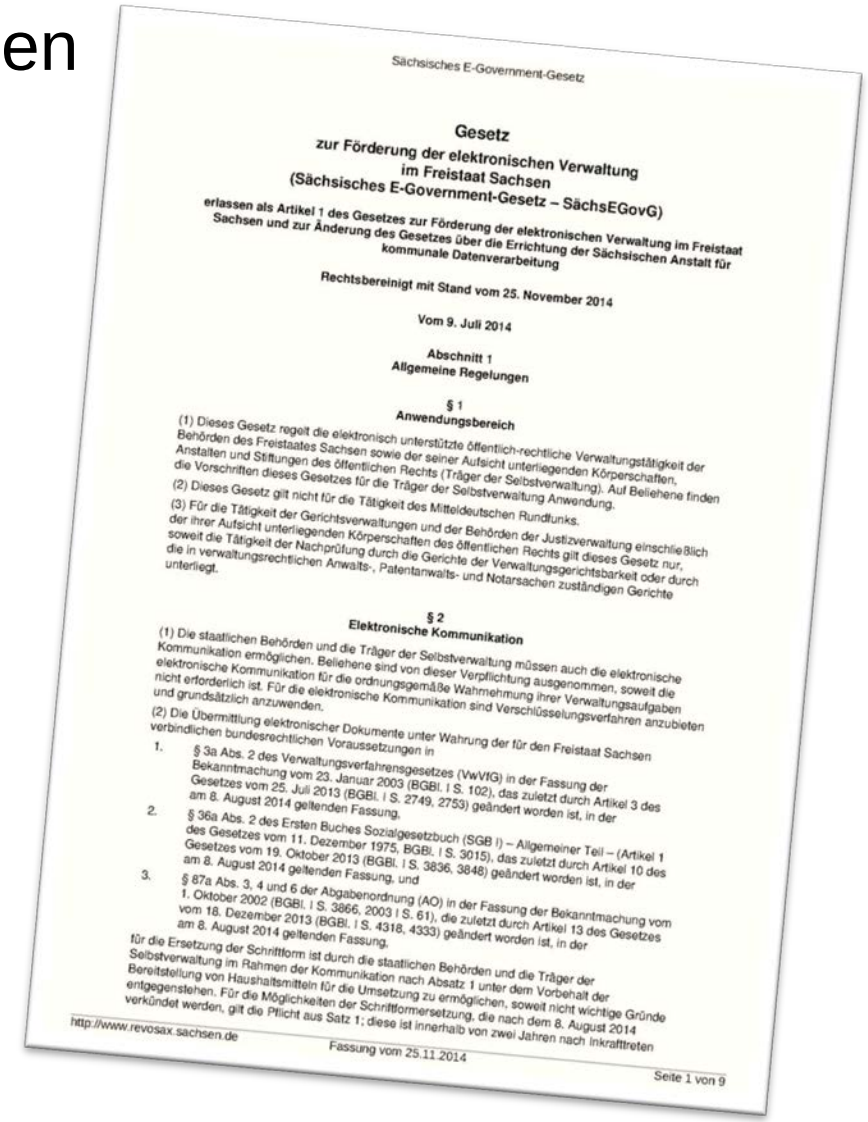
Trojaner-Alarm im Kanzleramt

Auf dem privaten USB-Stick einer Kanzleramtsmitarbeiterin wurde eine raffinierte Spionagesoftware entdeckt. Ein Fall von Fahrlässigkeit?

„Funktionierende IT-Sicherheit als Rückgrat der Gesellschaft“

Quelle: BMI

Grundlage Informationssicherheit für Kommunen in Sachsen



Sächsisches E-Government-Gesetz

Gesetz
zur Förderung der elektronischen Verwaltung im Freistaat Sachsen (Sächsisches E-Government-Gesetz – SächsEGovG)

erlassen als Artikel 1 des Gesetzes zur Förderung der elektronischen Verwaltung im Freistaat Sachsen und zur Änderung des Gesetzes über die Errichtung der Sächsischen Anstalt für kommunale Datenverarbeitung

Rechtsbereinigt mit Stand vom 25. November 2014

Vom 9. Juli 2014

Abschnitt 1
Allgemeine Regelungen

§ 1
Anwendungsbereich

(1) Dieses Gesetz regelt die elektronisch unterstützte öffentlich-rechtliche Verwaltungstätigkeit der Behörden des Freistaates Sachsen sowie der seiner Aufsicht unterliegenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts (Träger der Selbstverwaltung). Auf Beliehene finden die Vorschriften dieses Gesetzes für die Träger der Selbstverwaltung Anwendung.

(2) Dieses Gesetz gilt nicht für die Tätigkeit des Mitteldeutschen Rundfunks.

(3) Für die Tätigkeit der Gerichtsverwaltungen und der Behörden der Justizverwaltung einschließlich der ihrer Aufsicht unterliegenden Körperschaften des öffentlichen Rechts gilt dieses Gesetz nur, soweit die Tätigkeit der Nachprüfung durch die Gerichte der Verwaltungsgerichtsbarkeit oder durch die in verwaltungsrechtlichen Anwalts-, Patentanwalts- und Notarsachen zuständigen Gerichte unterliegt.

§ 2
Elektronische Kommunikation

(1) Die staatlichen Behörden und die Träger der Selbstverwaltung müssen auch die elektronische Kommunikation ermöglichen. Beliehene sind von dieser Verpflichtung ausgenommen, soweit die elektronische Kommunikation für die ordnungsgemäße Wahrnehmung ihrer Verwaltungsaufgaben nicht erforderlich ist. Für die elektronische Kommunikation sind Verschlüsselungsverfahren anzubieten und grundsätzlich anzuwenden.

(2) Die Übermittlung elektronischer Dokumente unter Wahrung der für den Freistaat Sachsen verbindlichen bundesrechtlichen Voraussetzungen in

1. § 3a Abs. 2 des Verwaltungsverfahrensgesetzes (VwVfG) in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102), das zuletzt durch Artikel 3 des Gesetzes vom 25. Juli 2013 (BGBl. I S. 2749, 2753) geändert worden ist, in der am 8. August 2014 geltenden Fassung,
2. § 36a Abs. 2 des Ersten Buches Sozialgesetzbuch (SGB I) – Allgemeiner Teil – (Artikel 1 des Gesetzes vom 11. Dezember 1975, BGBl. I S. 3015), das zuletzt durch Artikel 10 des Gesetzes vom 19. Oktober 2013 (BGBl. I S. 3836, 3848) geändert worden ist, in der am 8. August 2014 geltenden Fassung, und
3. § 87a Abs. 3, 4 und 6 der Abgabenordnung (AO) in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866, 2003 I S. 61), die zuletzt durch Artikel 13 des Gesetzes vom 18. Dezember 2013 (BGBl. I S. 4318, 4333) geändert worden ist, in der am 8. August 2014 geltenden Fassung,

für die Ersetzung der Schriftform ist durch die staatlichen Behörden und die Träger der Selbstverwaltung im Rahmen der Kommunikation nach Absatz 1 unter dem Vorbehalt der Bereitstellung von Haushaltsmitteln für die Umsetzung zu ermöglichen, soweit nicht wichtige Gründe entgegenstehen. Für die Möglichkeiten der Schriftformersetzung, die nach dem 8. August 2014 verkündet werden, gilt die Pflicht aus Satz 1; diese ist innerhalb von zwei Jahren nach Inkrafttreten

http://www.revosax.sachsen.de Fassung vom 25.11.2014 Seite 1 von 9

Datenschutz (un)gleich Informationssicherheit

§ 5 Datenschutz

(1) Zur Gewährleistung des Datenschutzes erstellen und pflegen die staatlichen Behörden und die Träger der Selbstverwaltung, die personenbezogene Daten automatisiert verarbeiten, Datenschutz und Informationssicherheitskonzepte.

Handreichung:

Fokus ist darauf gerichtet, solche Konzepte erstellen zu müssen, wenn **personenbezogene Daten** automatisiert verarbeitet werden, das **Informationssicherheitskonzept ist in diesem Fall auf den Datenschutz bezogen**.

- Ziel des Datenschutzes ist der Schutz personenbezogener Daten und deren gesetzeskonforme Verwendung. Die **Anforderungen zur IT-Sicherheit gehen darüber hinaus**. Hier ist die gesamte Infrastruktur unter dem Aspekt zu betrachten, alle Daten zugriffssicher verfügbar zu haben und im Katastrophenfall wiederherstellen zu können.

Informationssicherheit – für wen zu beachten?

§ 13 Interoperabilität und Informationssicherheit

(1) Für die an E-Government beteiligten Träger der Selbstverwaltung gilt **§ 9** Abs. 2 Satz 1 und 2 entsprechend.

§ 9 Interoperabilität und Informationssicherheit

(1) Die staatlichen Behörden haben die informationstechnischen Systeme zur Unterstützung ihrer Verwaltungsprozesse unter dem Vorbehalt der Bereitstellung von Haushaltsmitteln für die Umsetzung durch den Landtag so auszugestalten, dass ein medienbruchfreier Datenaustausch (Interoperabilität) zwischen ihnen ermöglicht und die Interoperabilität im Verhältnis zu anderen Verwaltungsebenen gefördert wird.

(2) Die staatlichen Behörden treffen angemessene organisatorische und technische Vorkehrungen und sonstige Maßnahmen zur Einhaltung der in § 9 Abs. 2 SächsDSG definierten Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz für die in ihren informationstechnischen Systemen verarbeiteten Daten. Solche Maßnahmen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen einer Verletzung der Schutzziele steht. Zur Erreichung und Aufrechterhaltung dieses Informationssicherheitsniveaus sind für die staatlichen Behörden die Standards und Kataloge des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils aktuellen Fassung maßgeblich.

Schutzziele der Informationssicherheit

Diese **Regelung geht über Verpflichtungen im Datenschutz hinaus**. Hier werden Anforderungen für alle Daten in den informationstechnischen Systemen der staatlichen Behörden getroffen. So ist über den konkreten Personenbezug hinaus für alle Daten zu gewährleisten, dass

- nur Befugte Daten zur Kenntnis nehmen können (**Vertraulichkeit**);
- Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (**Integrität**);
- Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (**Verfügbarkeit**);
- jederzeit Daten ihrem Ursprung zugeordnet werden können (**Authentizität**);
- festgestellt werden kann, wer wann welche Daten in welcher Weise verarbeitet hat (**Revisionsfähigkeit**) und dass
- die Verfahrensweisen bei der Verarbeitung Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (**Transparenz**).

Schutzziele nach Augenmaß

- Allerdings: Die Notwendigkeit alle sechs Schutzziele einzuhalten, ist zumindest zu prüfen. Stichwort: angemessene Vorkehrungen. Wenn Schutzmaßnahmen unverhältnismäßig aufwendig, ergibt sich aus der Nennung der sechs Schutzziele keine Notwendigkeit stets für alle benannten Ziele Schutzmaßnahmen vorzusehen.

- Aus Sicht der Informationssicherheit insbesondere die ersten drei Ziele wichtig: **Vertraulichkeit, Integrität, Verfügbarkeit**

Umsetzung Informationssicherheit: Organisatorisch und technisch

- Umsetzungsempfehlung: **Musterleitlinie der SAKD**, die keine Anwendung von BSI-Grundschutz vorgibt, jedoch Orientierung an BSI-Grundschutz als Praxisleitfaden empfiehlt.

- Deshalb: Paralleles Vorgehen angeraten!
  - 1) das formelle und gesetzlich vorgeschriebene Vorgehen nach BSI konsequent angehen
  - 2) im Tagesgeschäft die praktische Abwehr von Informationssicherheitsrisiken verfolgen

Musterleitlinie SAKD

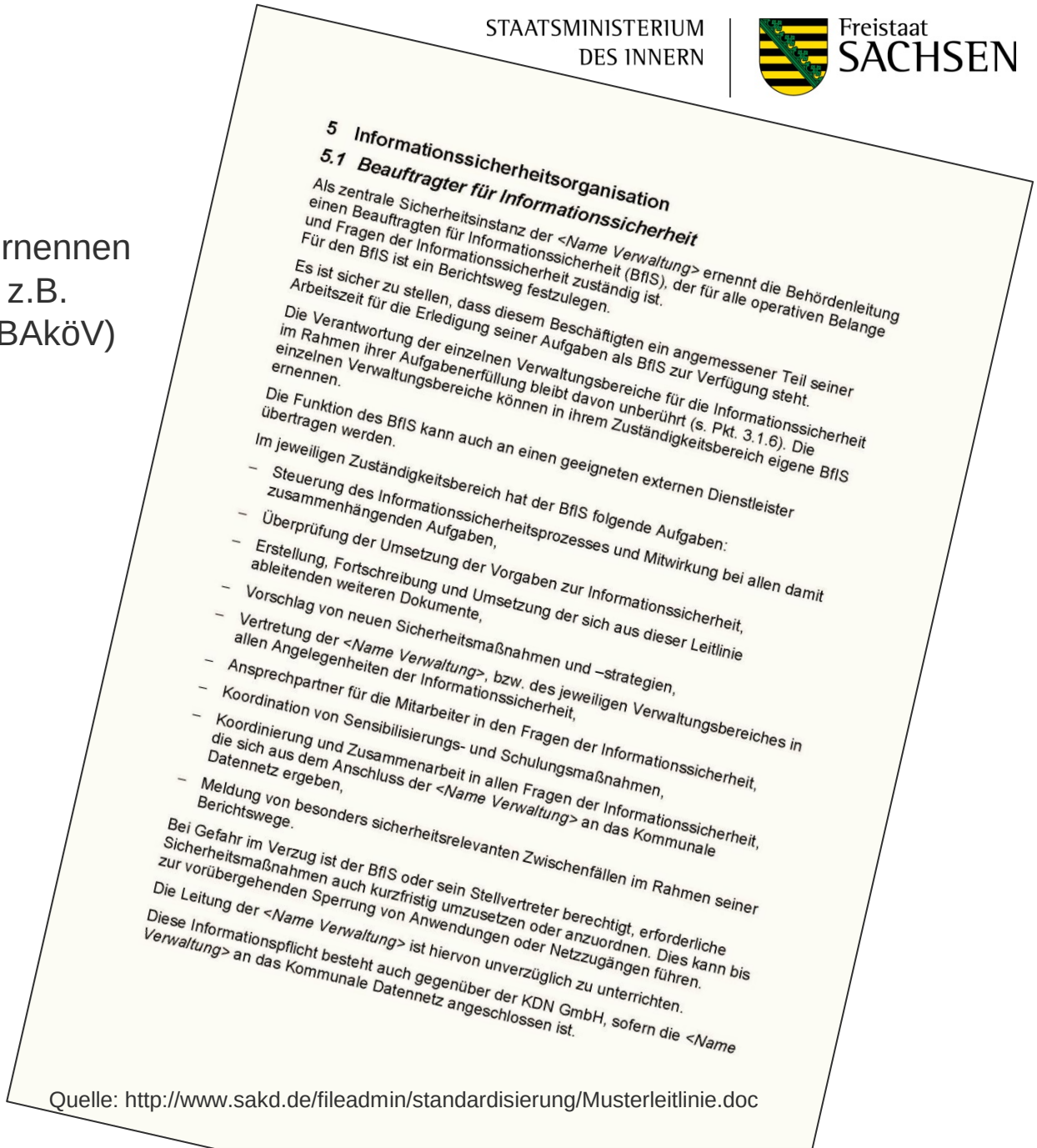
- Diese Musterleitlinie zur Gewährleistung der Informationssicherheit für sächsische Kommunalverwaltungen fordert nach dem **Grundsatz "IT-Sicherheit ist Leitungssache"** das Bekenntnis der Behördenleitung zur Informationssicherheit als strategisches Prinzip der Verwaltungsorganisation. Sie wendet sich vordergründig an kreisangehörige Stadt- und Gemeindeverwaltungen mit und ohne Anschluss an das Kommunale Datennetz.

- Sie orientiert sich soweit möglich an der "Verwaltungsvorschrift der Sächsischen Staatsregierung zur Gewährleistung der Informationssicherheit in der Landesverwaltung" vom 7. September 2011 und ist leicht **an die Gegebenheiten jeder Kommunalverwaltung anpassbar** (z. B. hinsichtlich der Erweiterung des Geltungsbereichs auf Eigen- oder Zweckbetriebe oder kommunale Gesellschaften).

- Die enthaltenen Grundsatzaussagen zur Informationssicherheit sind in weiteren Detaildokumenten wie Sicherheitskonzepten, Checklisten, Dienstanweisungen, Strukturplänen bis hin zu Betriebshandbüchern konkret zu untersetzen.

ISMS aufbauen

- Beauftragten für Informationssicherheit ernennen (ggf. fachlich ausbilden, z.B. „Sommerakademie der BAköV)
- Meldewege etablieren



STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

5 Informationssicherheitsorganisation

5.1 Beauftragter für Informationssicherheit

Als zentrale Sicherheitsinstanz der <*Name Verwaltung*> ernennt die Behördenleitung einen Beauftragten für Informationssicherheit (BfIS), der für alle operativen Belange und Fragen der Informationssicherheit zuständig ist.
Für den BfIS ist ein Berichtsweg festzulegen.
Es ist sicher zu stellen, dass diesem Beschäftigten ein angemessener Teil seiner Arbeitszeit für die Erledigung seiner Aufgaben als BfIS zur Verfügung steht.
Die Verantwortung der einzelnen Verwaltungsbereiche für die Informationssicherheit im Rahmen ihrer Aufgabenerfüllung bleibt davon unberührt (s. Pkt. 3.1.6). Die einzelnen Verwaltungsbereiche können in ihrem Zuständigkeitsbereich eigene BfIS ernennen.
Die Funktion des BfIS kann auch an einen geeigneten externen Dienstleister übertragen werden.
Im jeweiligen Zuständigkeitsbereich hat der BfIS folgende Aufgaben:

- Steuerung des Informationssicherheitsprozesses und Mitwirkung bei allen damit zusammenhängenden Aufgaben,
- Überprüfung der Umsetzung der Vorgaben zur Informationssicherheit,
- Erstellung, Fortschreibung und Umsetzung der sich aus dieser Leitlinie ableitenden weiteren Dokumente,
- Vorschlag von neuen Sicherheitsmaßnahmen und –strategien,
- Vertretung der <*Name Verwaltung*>, bzw. des jeweiligen Verwaltungsbereiches in allen Angelegenheiten der Informationssicherheit,
- Ansprechpartner für die Mitarbeiter in den Fragen der Informationssicherheit,
- Koordination von Sensibilisierungs- und Schulungsmaßnahmen,
- Koordinierung und Zusammenarbeit in allen Fragen der Informationssicherheit, die sich aus dem Anschluss der <*Name Verwaltung*> an das Kommunale Datennetz ergeben,
- Meldung von besonders sicherheitsrelevanten Zwischenfällen im Rahmen seiner Berichtswege.

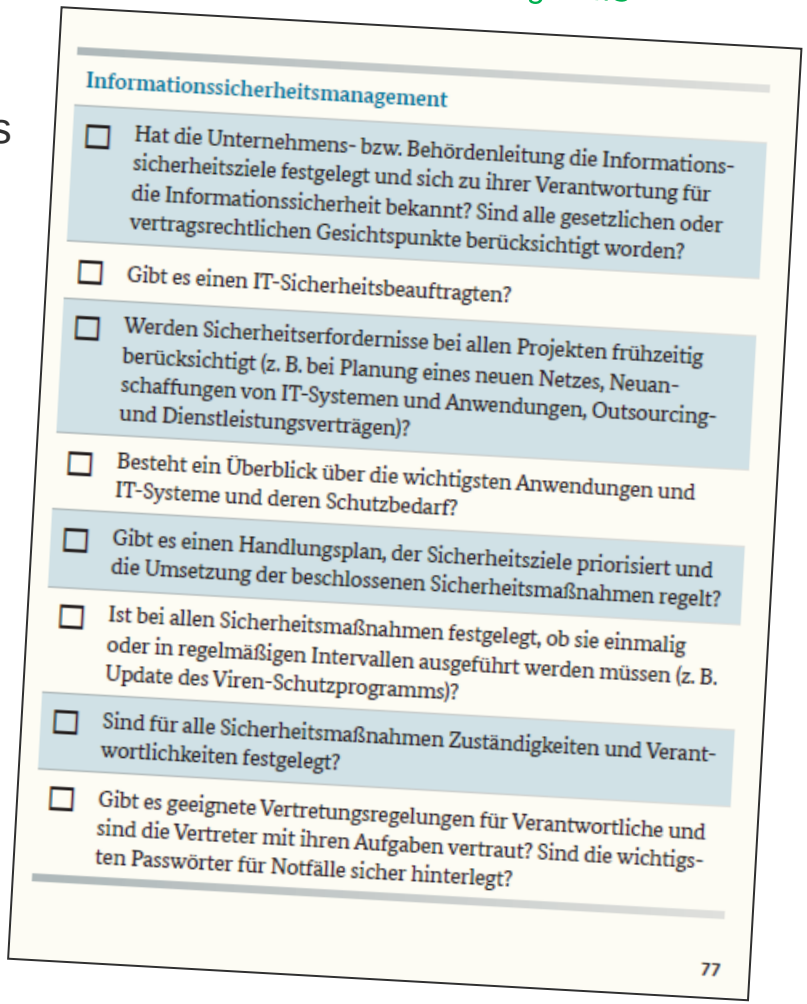
Bei Gefahr im Verzug ist der BfIS oder sein Stellvertreter berechtigt, erforderliche Sicherheitsmaßnahmen auch kurzfristig umzusetzen oder anzuordnen. Dies kann bis zur vorübergehenden Sperrung von Anwendungen oder Netzzugängen führen.
Die Leitung der <*Name Verwaltung*> ist hiervon unverzüglich zu unterrichten.
Diese Informationspflicht besteht auch gegenüber der KDN GmbH, sofern die <*Name Verwaltung*> an das Kommunale Datennetz angeschlossen ist.

Quelle: http://www.sakd.de/fileadmin/standardisierung/Musterleitlinie.doc

Organisatorische Umsetzung mit BSI-Grundschutz

- Aufbauend auf Leitlinie: Umsetzung BSI-Grundschutz:
  - Entwicklung eines Sicherheitskonzepts gemäß IT-Grundschutz-Vorgehensweise,
  - Umsetzung durch Beseitigung vorhandener Schwachstellen und Einführung der im Konzept vorgesehenen Maßnahmen,
  - Aufrechterhaltung und kontinuierliche Verbesserung durch Prüfung von Wirksamkeit, Angemessenheit und Aktualität der vorhandenen Konzepte und eingeführten Maßnahmen

Checkliste zur Umsetzung ISMS



Informationssicherheitsmanagement

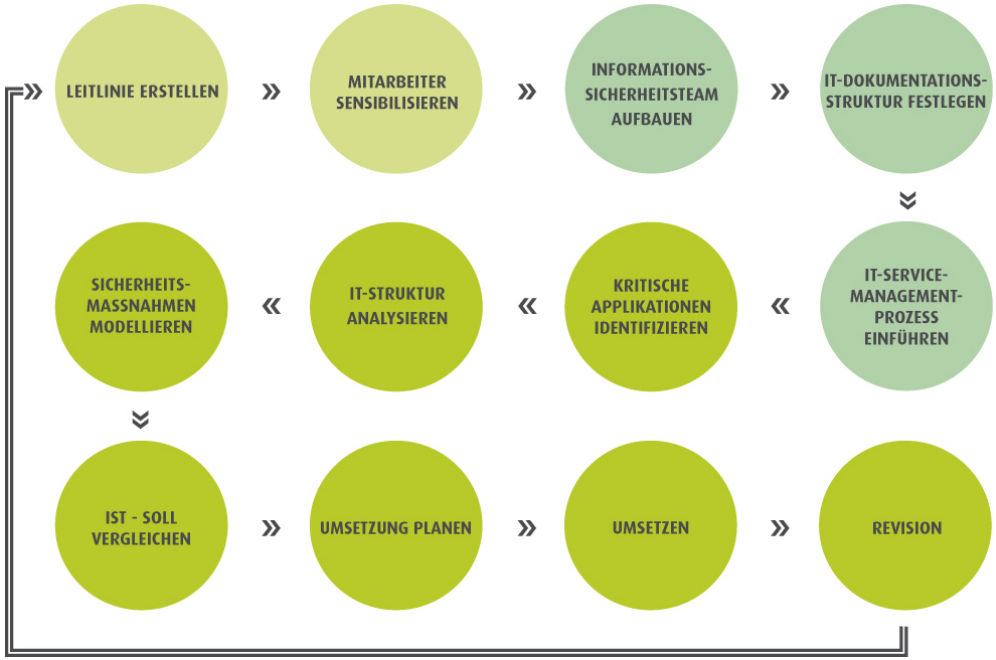
- ☐ Hat die Unternehmens- bzw. Behördenleitung die Informationssicherheitsziele festgelegt und sich zu ihrer Verantwortung für die Informationssicherheit bekannt? Sind alle gesetzlichen oder vertragsrechtlichen Gesichtspunkte berücksichtigt worden?
- ☐ Gibt es einen IT-Sicherheitsbeauftragten?
- ☐ Werden Sicherheitserfordernisse bei allen Projekten frühzeitig berücksichtigt (z. B. bei Planung eines neuen Netzes, Neuanschaffungen von IT-Systemen und Anwendungen, Outsourcing- und Dienstleistungsverträgen)?
- ☐ Besteht ein Überblick über die wichtigsten Anwendungen und IT-Systeme und deren Schutzbedarf?
- ☐ Gibt es einen Handlungsplan, der Sicherheitsziele priorisiert und die Umsetzung der beschlossenen Sicherheitsmaßnahmen regelt?
- ☐ Ist bei allen Sicherheitsmaßnahmen festgelegt, ob sie einmalig oder in regelmäßigen Intervallen ausgeführt werden müssen (z. B. Update des Viren-Schutzprogramms)?
- ☐ Sind für alle Sicherheitsmaßnahmen Zuständigkeiten und Verantwortlichkeiten festgelegt?
- ☐ Gibt es geeignete Vertretungsregelungen für Verantwortliche und sind die Vertreter mit ihren Aufgaben vertraut? Sind die wichtigsten Passwörter für Notfälle sicher hinterlegt?

77

Quelle: BSI: Leitfaden Informationssicherheit - IT-Grundschutz kompakt

Organisatorische Umsetzung mit ISIS12

- BSI-Grundschutz „light“
- ISIS12 als Vorgehen, das in 12 Schritten den Einstieg in Entwicklung und Gestaltung von Informationssicherheitsleitlinien aufzeigt
- Empfehlung vom IT-Planungsrat: Demnach entspricht ISIS12 der Leitlinie für Informationssicherheit des IT-PLR
- Verfahren als Vorstufe zur BSI IT-Grundschutz-Zertifizierung



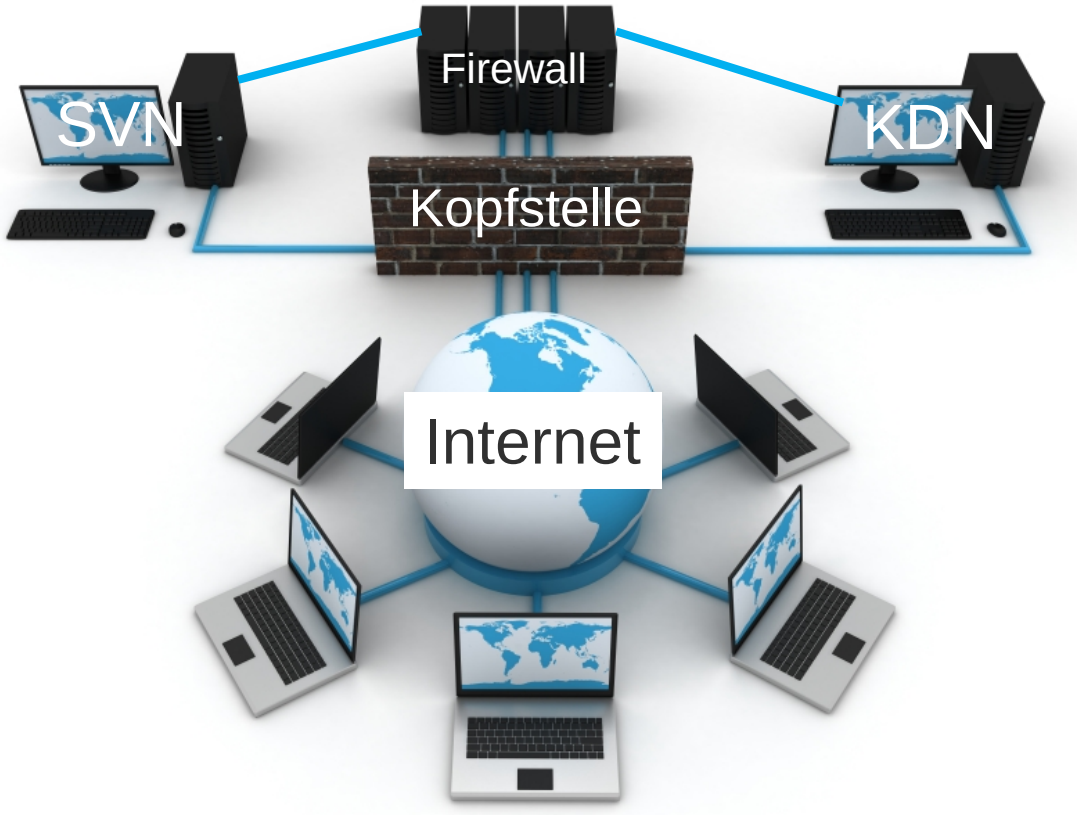
Quelle: http://www.it-sicherheit-bayern.de/produkte-dienstleistungen/isis12/vorgehensmodell.html

Technische Umsetzung Informationssicherheit

- Sofortmaßnahmen:
  - Anschluss an das KDN!!!
  - Fehlerhafte Zertifikate auf HTTPS-Seiten ersetzen (Handlungsanleitungen)
  - Verschlüsselte E-Mail-Kommunikation (Handlungsanleitungen)
  - Abschaltung stark unsicherer, weil veralteter Verschlüsselungsprotokolle SSLv2 und SSLv3 auf Internetseiten
  - Einsatz von Verschlüsselungsverfahren (Handlungsanleitung)

Technische Sofortmaßnahmen: Vollständiger Anschluss an das KDN

- Im SVN und KDN implementierte Schutzmaßnahmen wie hochwertige Schadsoftware-Scanner und moderne Angriffserkennungssysteme sind sehr wirkungsvoll
- 12.000 abgewehrte Angriffe, 1,5 Mrd. abgewiesene Spam-E-Mails, Ausfilterung von 175.000 Viren und 340.000 Schadprogrammen in den letzten 5 Jahren
- Ebenbürtiges Schutzniveau in einem eigenen Netzwerk kaum finanzierbar



Technische Sofortmaßnahme: Fehlerhafte https-Zertifikate ersetzen

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

- Alle Kommunen stellen, soweit möglich, die von ihnen betriebenen HTTPS-Seiten mit fehlerhaften Zertifikaten auf Zertifikate der Sachsen Global CA um. Alle Zertifikats-fehler werden beseitigt.

Technische Sofortmaßnahme: Verschlüsselte Kommunikation

- Verschlüsselte E-Mail-Kommunikation zwischen eigenen Servern und denen der Kommunikationspartner: Wo möglich wird die Verschlüsselungsoption STARTTLS für den serverseitigen E-Mail-Empfang und –Versand durchgängig umgesetzt.
- Interne flächendeckende Umstellung auf verschlüsselte Kommunikation zwischen den E-Mail-Clients und E-Mail-Servern
- Sofortige Abschaltung der stark unsicheren Verschlüsselungsprotokolle SSLv2 und SSLv3 auf Internetseiten und -diensten
- Berücksichtigung der vom AK ITEG für die Landesverwaltung beschlossenen Handlungsempfehlungen und des Umsetzungsplan der AG IS zum verbesserten Einsatz von Verschlüsselungsverfahren

Kontakt

SÄCHSISCHES STAATSMINISTERIUM DES INNERN
Referat 65:
Informationssicherheit in der Landesverwaltung, Cybersicherheit
Wilhelm-Buck-Straße 4 | 01097 Dresden
bfis-land@smi.sachsen.de

Kostenfreie IT-Serviceberatung für Kommunen:
Sächsische Anstalt für kommunale Datenverarbeitung
Herr Nikol
Tel. 03594 7752-46
E-Mail: nikol@sakd.de