ANSSI.lu

Agence nationale de la sécurité des systèmes d'information Luxembourg

Leitlinie zur Informationssicherheit des Luxemburger Staates

Jerry Caye, ANSSI

Agenda

Der politische Wille, Cybersecurity zu unterstützen.

- Chronologischer Überblick;
- Allgemeine Organisation (Großherzogliches Dekret: AGD 10/2/2015);
- Aufgaben der ANSSI;
- Zeitplan.

Die PSI (Politique de sécurité de l'Information de l'État luxembourgeois) – Allgemeine Leitlinie (PSI-LU).

- Die 10 Grundsätze der PSI;
- Die Leitlinien nach Bereich.

Das Informationssicherheitsmanagementsystem des Luxemburger Staates (PSI-SMSI).

Wann umsetzen ?

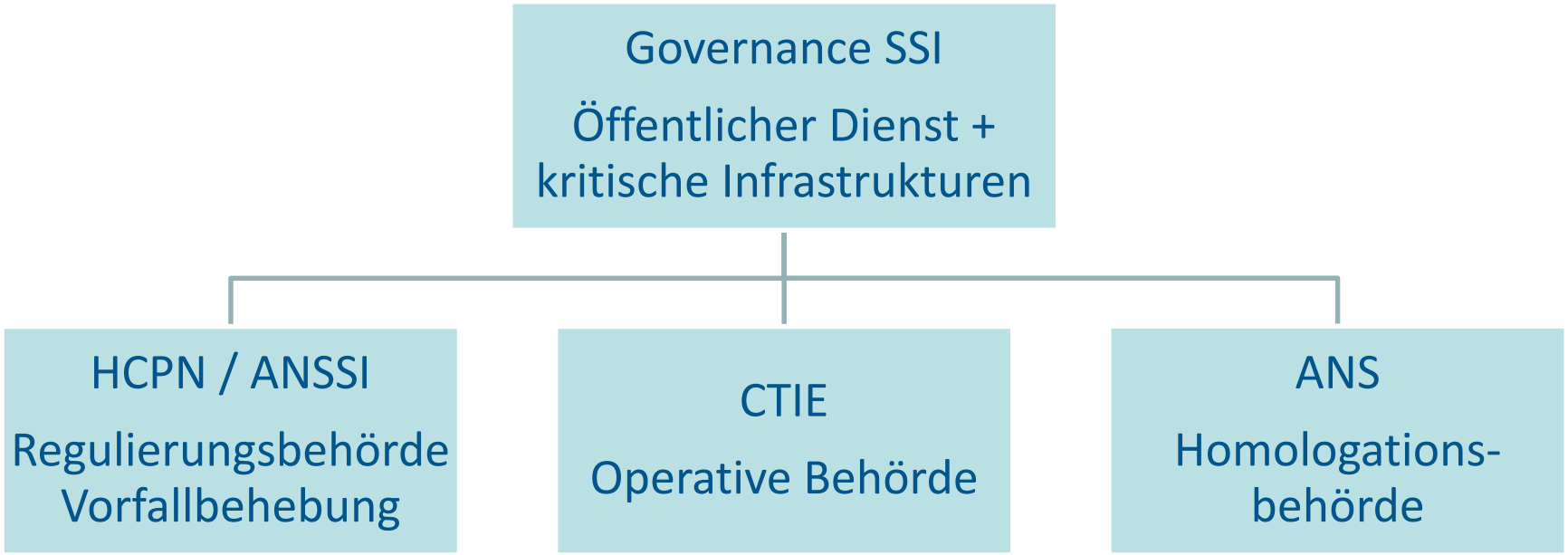
- Umsetzungsplan für staatliche Einheiten.

Der politische Wille

Chronologischer Überblick

- Erstellung einer nationalen Cybersecurity-Strategie in 2012, basierend auf 4 Pfeilern.
- Erstellung einer Version II in 2015:
  - Schutz der privaten und staatlichen Einheiten gegen Cyberbedrohungen durch Festlegung von 7 Zielen und die dazugehörigen Aktionspläne;
  - Umsetzung bis Ende 2017.
- Großherzogliches Dekret (AGD) vom 10/2/2015 zur Erschaffung einer Nationalen Behörde für Informationssicherheit (ANSSI).

Allgemeine Organisation(GD decree)



Aufgaben der ANSSI

Die ANSSI hat folgende Aufgaben:

- Leitlinien und Richtlinien zur Informationssicherheit (von klassifizierten und nicht klassifizierten Informationen) erstellen und deren Wirksamkeit überwachen.
- Umsetzung von Sicherheitsmaßnahmen überwachen und deren gesicherte Anwendung überprüfen.
- Informations- und Kommunikationstechnlogien (Systeme, Dienstleistungen, Infrastrukturen, oder Räumlichkeiten) zertifizieren.
- Die national Regierungs-CERT betreiben.
- Schulungen über Sicherheit von klassifizierten und nicht klassifizierten Informationen koordinieren.
- Passende Sicherheitssensibilisierung über besondere Risiken, insbesondere Risiken der ICT und von Cyberangriffen sicherstellen.
- Die Nationale TEMPEST Behörde (TA) betreiben.
- Die nationale Kryptographie-Genehmigungsbehörde betreiben (Crypto Approval Authority (CAA)).

ANSSI – Zeitplan

Thema	Datum
Erste Schritte - Gründung der ANSSI - Kooperationsabkommen - Personal Rekrutierung - Externe Beratung vorbereiten	Feb – Juni 2015
Sicherheitsleitlinie und Anforderungen ausarbeiten (mit externem Berater)	2015 S2
Sicherheitsleitlinie und Anforderungen mit Partnern besprechen und bestätigen	Dez. 2015 – Mai 2016
Annahme der PSI-LU durch Regierungsrat	16/3/2016
Unterschrift der PSI - Allgemeine Leitlinie durch Staatsminister X . Bettel	24/03/2016

Die PSI-LU

Politique de sécurité de l'Information de l'État luxembourgeois – Politique générale (PSI-LU)

Leitlinie zur Informationssicherheit des luxemburger Staates – Allgemeine Leitlinie

Ansatz

- Erstellung mit einem externen Berater (itrust consulting).
- Beratung mit Regulierungsbehörden und Partnern wie:
  - ILR (Telecom-Regulierer), CSSF (Bankaufsichtsbehörde), ILNAS (Akkreditierung- und Überwachungsstallen), CNPD (Datenschutzbehörde).
  - SMILE G.I.E. (Sicherheitsberatungsstelle des Wirtschaftsministeriums), CTIE (Staatliches Rechenzentrum), l'ANS (Sicherheitsbehörde)and GovCert.
  - Datenschutzbeauftragter der Regierung.
- Feststellung des Reifegrades durch Umfrage bei allen staatlichen Einheiten (75% Feedback).

Die PSI-LU

Sicherheitsziele

- Allgemeine Ziele und Grundsätze festlegen.
- Richlinien zum Schutz aller wichtigen Informationen des luxemburger Staates.

Anwendungsbereich

- Alle Ministerien, Verwaltungen und Dienststellen des Luxemburger Staates.
- Betreiber kritischer Infrastrukturen (nach Umsetzung der EU NIS Direktive).
- Ausgenommen:
  - Parlament und Justiz
  - Gemeindeverwaltungen
  - Gemeinnützige Anstalten

Die 10 Grundsätze

1. Eine gutverstandene Sicherheit dank Sensibilisierungsprogramm.
2. Einhaltung der Normen, Gesetze und Verträge (ISO 27001).
3. Risikoanalyse und -management (zur Auswahl der Schutzmaßnahmen).
4. Quantifizierung, Planung und Identifizierung von Ressourcen.
5. Kontinuierliche Verbesserung bis zur Exzellenz (durch kontinuierliche Veränderung des Umfeldes).
6. Integrierte und transversale Sicherheit als integraler Teil aller Tätigkeiten (sowohl in geordneten Projekten, als auch bei täglichen Aufgaben).
7. Kommunikation und Teamarbeit (gegenseitige Hilfe, um Sicherheitsziele zu erreichen).
8. Auftragsvergabe an vertrauenswürdige Serviceanbieter unter Aufrechterhaltung der Aufsicht.
9. Zielerfüllung und Einhaltung der Regeln und Anforderungen der PSI durch nachvollziehbare Dokumentierung aller Tätigkeiten und Entscheidungen.
10. Eine Sicherheitspolitik als Weg zur Sicherheitskultur.

Die PSI-LU

Allgemeine Leitlinien nach Bereich (1/2)

Id.	Acron.	Title	Titel	Kommentar
0.0	PSI-LU	**General Policy**	Allgemeine Leitlinie	Übergeordnete Leitlinie aller staatlichen Einheiten und kritischen Infrastrukturen.
1-0	PSI-SMSI	**Information security management system**	Informations-sicherheitsman-agementsystem	Umsetzung der ISO 27001 Anforderungen.
2-0	PSI-Perso	**Privacy policy**	Datenschutz-leitlinie	Umsetzung der zusätzlichen Anforderungen aus der EU Datenschutzregulierung (GDPR).
3-0	PSI-PSDC	**Archiving policy**	Archivierungs-leitlinie	Umsetzung des Gesetzes und der Regulierung vom 2. Juli 2015 über Dematerialisierung und elektronische Archivierung.
4-0	PSI-Déontologie	**Code of Ethics**	Ehrenkodex	Erst in Planung
5-0	PSI-Risques	**Risk Management Policy**	Risiko Management	Umsetzung von Zielen und Richtlininen (nach ISO 27005) fürs Riskomanagement der Informationssicherheit.
6-0	PSI-ORG	**Security Organisation**	Sicherheitsorgani-sation	Beschreibung von Rollen und Verantwortlichkeiten; Prozedure für Ausnahmeregelung zur PSI. Umsetzung einer Organisation nach ISO 27002.
7-0	PSI-RH	**Human resource security**	Personalsicherheit	Ziele und Anforderungen bezüglich Personalmanagement nach ISO 27002.
8-0	PSI-Actifs	**Asset management**	Asset Management	Ziele und Anforderungen bezüglich Asset Management nach ISO 27002 (insb. Informationsmanagement) Inventar, Klassifizierungschema, Sicherheitsreglen je nach Datenklassifizierung.
9-0	PSI-Accès	**Access control**	Zugangskontrolle	Ziele und Anforderungen zur Zugangskontrolle, z.B. starke Authentisierung.

Die PSI-LU

Allgemeine Leitlinien nach Bereich (2/2)

Id.	Acron.	Title	Titel	Kommentar
10-0	PSI-Crypto	**Cryptography**	Cryptographie	Ziele und Anforderungen nach ISO 27002.
11-0	PSI-Physique	**Physical and environmental security**	Physikalische und Umweltsicherheit	Ziele und Anforderungen nach ISO 27002.
12-0	PSI-Exploit	**Operations security**	Betriebssicherheit	Ziele und Anforderungen nach ISO 27002 zum Betrieb von ICT Systemen.
13-0	PSI-Comm	**Communications security**	Kommunikationssicherheit	Ziele und Anforderungen nach ISO 27002 zur Netzwerksicherheit.
14-0	PSI-Systèmes	**System acquisition, development and maintenance**	System-Akquisition, Entwicklung und Wartung	Ziele und Anforderungen nach ISO 27002 zum Einkauf, Entwicklung und Wartung von Informationssytemen.
15-0	PSI-Fournisseurs	**Supplier relationships**	Lieferantenbeziehungen	Ziele und Anforderungen nach ISO 27002 zur Verwaltung von Lieferanten, insbesonders bei Outsourcing.
16-0	PSI-Incidents	**Information security incident management**	Verwaltung von Sicherheitsvorfällen	Ziele und Anforderungen nach ISO 27002 zur Verwaltung von Vorfällen in Verbindung mit der Informationssicherheit.
17-0	PSI-Continuité	**Business continuity management**	Notfallvorsorge und Aufrechterhaltung der Geschäftstätigkeit	Ziele und Anforderungen nach ISO 27002 und ISO 22301 zu Verwaltung der Geschäftskontinuität bei Notfällen.
18-0	PSI-Conformité	**Compliance**	Einhaltung der Sicherheitsleitlinien	Ziele und Anforderungen nach ISO 27002 zur Einhaltung der Leitlinien, gesetzlichen Vorgaben und Richtlinien.
19-0	PSI-Class	**Security policy for classified information**	Leitlinie zum Umgang mit klassifizierten Daten	Ziele und Anforderungen nach Vorgaben der Partnerstaaten und unter Berücksichtigung der nationalen Interessen.

Das neue ISMS

Informations-Sicherheits-Management-System (SMSI)

Definition SMSI

„Teil des globalen Managementsystems, das auf Grundlage des Geschäftsrisikoansatzes für die Definition, Umsetzung, Nutzung, Überwachung, Prüfung, Erhaltung und Verbesserung der Informationssicherheit verantwortlich ist.“

Ein SMSI fußt auf einer Risikoevaluierung und auf Festlegung von Stufen für tragbares Risiko.

Definition Informationssicherheit (IS)

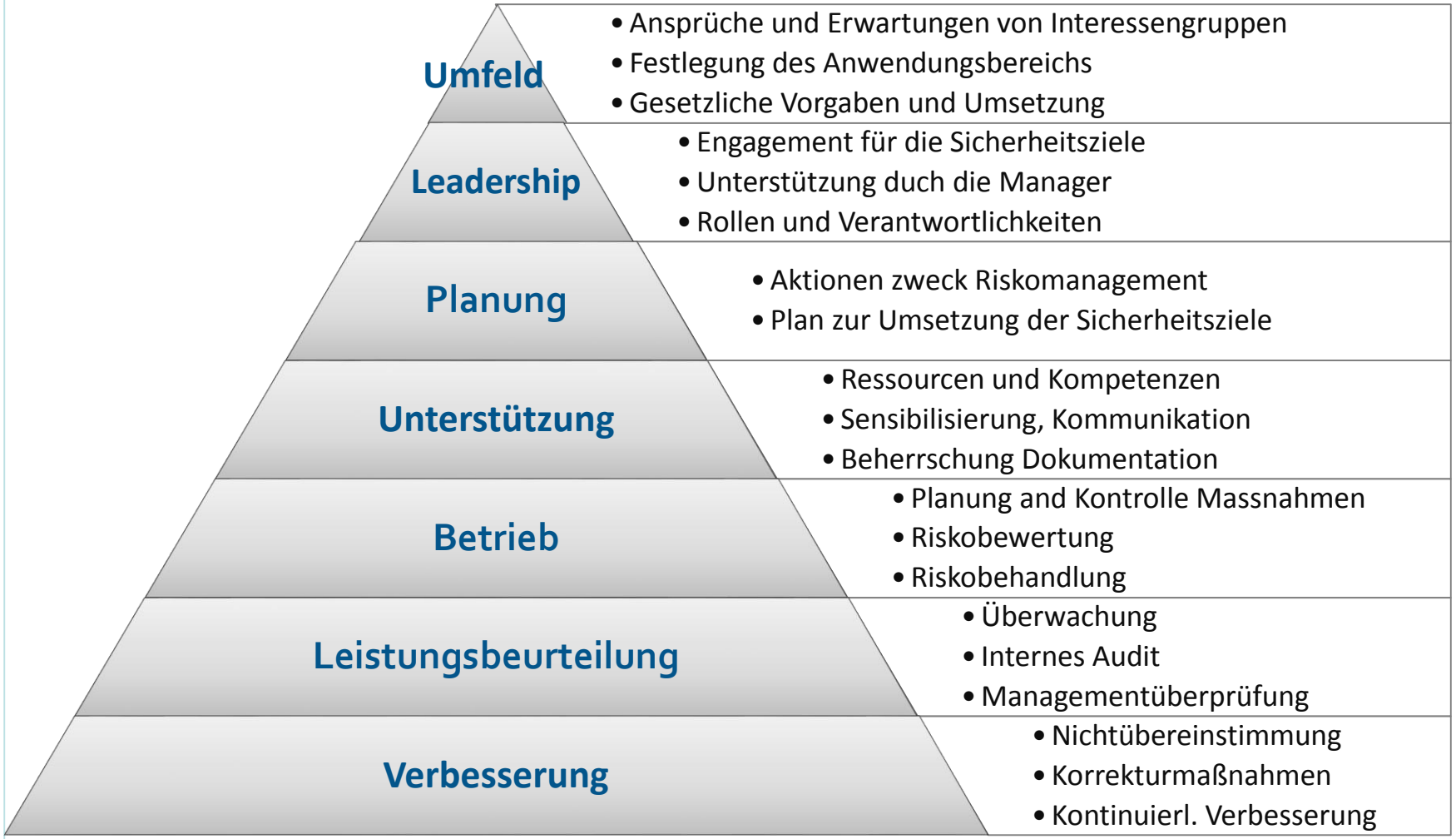
„ Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Daten, jedoch können weitere Eigenschaften, beispielsweise Authentizität, Verantwortlichkeit, Unleugbarkeit und Zuverlässigkeit, ebenfalls betroffen sein. “

Ziele der PSI-SMSI

- Einhaltung von ISO/IEC 27001, welche alle staatliche Einheiten, groß oder klein betrifft.
- Festlegung der nationalen Anforderung (nach diesem Standard).

Das neue ISMS

Anforderungen nach Bereich (nach ISO 27001)



Wann umsetzen?

Umsetzungsplan für staatliche Einheiten

Übergangsphase bis Ende 2017

- CTIE setzt die PSI bis Ende 2016 als Proof-of-Concept um.
- Schnelltest Risikobewertung in verschiedenen Einheiten.
- Nach Auswertung wird die ANSSI ein erster Umsetzungsplan Anfang 2017 vorlegen.
- 2017: andere Einheiten (mit eigener ICT und bestimmter Wichtigkeit) müssen die PSI umsetzen.
- 2017: ANSSI unterstützt die verbleibenden Einheiten beim Schnelltest der Risikobewertung. Festlegung der Prioritäten zweck vollständiger Umsetzung in 2018.

Die ANSSI legt Anforderungen fest. Jedoch ist jeder Verwaltungsleiter verantwortlich und kann Ausnahmen zu diesen Anforderungen bestimmen, vorausgesetzt dass diese begründet, punktuell, und formal beschrieben sind.

Weitere Information?

info@anssi.etat.lu

Tel. 247-88935

Vielen Dank für die Aufmerksamkeit

Jerry Caye