

Sicherheitsüberprüfungen im Kontext internationaler Verschlusssachenaufträge

Ing. Gerald Trost, B.Sc.(hons)
Informationssicherheitsbüro / BKA

Inhalt

- Verschlusssachen – Rechtsgrundlagen und Verpflichtungen
- Informationssicherheitskommission im BKA / Aufgaben
- Industrielle Sicherheit / Verschlusssachenaufträge
 - Rechtliche Grundlagen und Verpflichtungen
 - Innerstaatliche Funktionen und Stellen (NSA, DSA)
- Personelle Sicherheit
 - Personenüberprüfungen
 - Sicherheitsunbedenklichkeitsbescheinigung / PSC
- Materielle Sicherheit (physischer Geheimschutz)
 - Organisatorische Voraussetzungen
 - Technische Absicherungsmaßnahmen
 - Sicherheitsunbedenklichkeitsbescheinigung für Unternehmen / FSC
- Zusammenfassung / Ausblick

Rechtsgrundlagen und Verpflichtungen

Übermittlung und Zugang zu Verschlusssachen (klassifizierte Informationen), die Österreich aufgrund völkerrechtlicher Verpflichtungen erhält

- *EU-Mitgliedschaft (Beschluss des Rates über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen, 2011/292/EU)*
- *NATO (Partnerschaft für den Frieden (PfP) 1995, Sicherheitsvorschriften der NATO (C-M(2002)49))*
- *bilaterale Verschlusssachenabkommen mit EU-Mitgliedstaaten, Drittstaaten, internationalen Organisationen, etc.*

Verpflichtung zur Einrichtung innerstaatlicher Funktionen und Stellen zur Sicherstellung des Schutzes von klassifizierten Informationen

- *zuständige Sicherheitsbehörde (NSA – National Security Authority)*
- *DSA (Designated Security Authority)*
- *Sicherheits-Akkreditierungsstelle (SAA – Security Accreditation Authority)*
- *Krypto-Verteilungsstelle (NDA – National Distribution Authority)*

...

Verschlussachen / klassifizierte Informationen

- Verschlussachen / Klassifizierte Informationen:

"Geheimhaltungsbedürftige Tatsachen im öffentlichen Interesse, welche ihrer Schutzbedürftigkeit von einer amtlichen Stelle (Urheber) einer Klassifizierungsstufe zugeordnet werden"

- Klassifizierungsstufen

EU	NATO	National
RESTREINT UE/EU RESTRICTED	NATO RESTRICTED	EINGESCHRÄNKT
CONFIDENTIEL UE / EU CONFIDENTIAL	NATO CONFIDENTIAL	VERTRAULICH
SECRET UE / EU SECRET	NATO SECRET	GEHEIM
TRES SECRET UE / EU TOP SECRET	COSMIC TOP SECRET	STRENG GEHEIM

Nationale Umsetzung

Informationssicherheitsgesetz, InfoSiG

Bundesgesetz über die Umsetzung völkerrechtlicher Verpflichtungen zur sicheren Verwendung von Informationen (BGBl. I Nr.23/2002, 16.1.2002)

- ISK „Informationssicherheitskommission“ -> National Security Authority
 - Kommission im Bundeskanzleramt (Vorsitz BKA)
 - Informationssicherheitsbeauftragte der Ressorts
- Geschäftsführung: ISB – Informationssicherheitsbüro, BKA

Informationssicherheitsverordnung, InfoSiV

Verordnung der Bundesregierung über die Informationssicherheit.

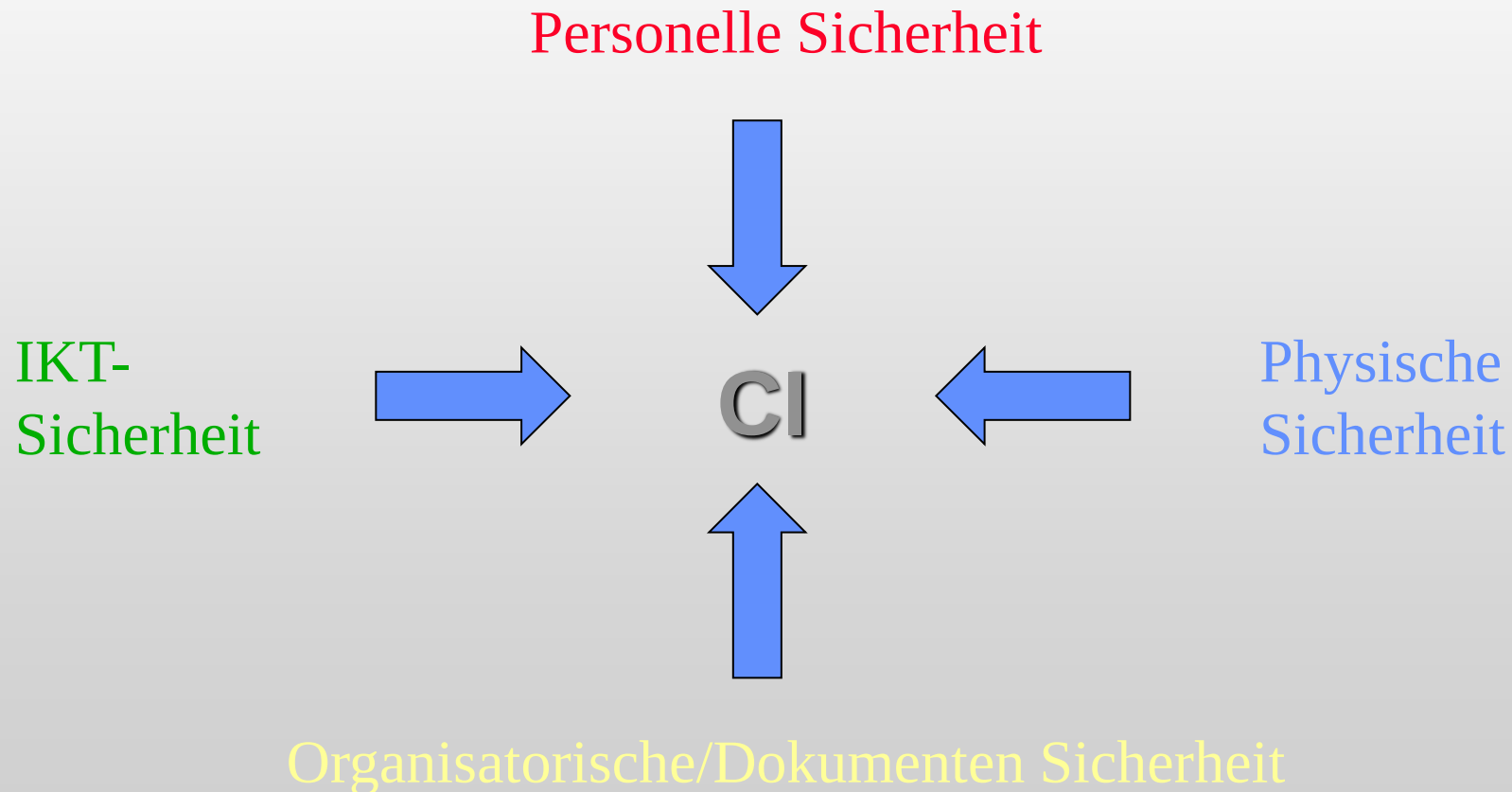
(BGBl. II Nr. 548/2003, 28.11.2003; Änderung BGBl. II Nr. 67/2012, 14.03.2012)

- Vorschriften über die Informationssicherheit
- Maßnahmen zum Schutz klassifizierter Informationen nach internationalen Standards und Vorgaben

Informationssicherheitskommission (NSA)

- Kommission im Bundeskanzleramt (Vorsitz BKA; Informationssicherheitsbeauftragte der Ressorts)
- Aufgabenstellung
 - Koordination einheitlicher Maßnahmen zum Schutz klassifizierter Informationen die AT aufgrund völkerrechtlicher Verpflichtungen erhält (EU, NATO, bilaterale Abkommen, etc.)
 - Ausarbeitung von Richtlinien und Empfehlungen (z.B. Kryptostrategie, materielle Sicherheit, abhörsicher Räume, Vernichtung von Festplatten, etc.)
 - **Belange der industriellen Sicherheit - Ausstellung von PSCC und FSC**
 - Erfahrungsaustausch; nationaler und internationaler Eingangspunkt für alle Belange der Informationssicherheit in AT; Koordination von Inspektionen (GSC, NATO)
 - Bericht an Bundesregierung
 - SAA (Security Accreditation Authority)
 - Vertretung ATs in „Sicherheitsrelevanten Gremien im In- und Ausland“
- Informationssicherheitsbeauftragte
 - Verantwortung für Informationssicherheit in den einzelnen BMs; Umsetzung

Internationale und nationale Anforderungen an die Informationssicherheit - Verschlusssachen



Internationale und nationale Anforderungen (1)

Grundprinzipien und Mindeststandards für die Sicherheit in Bezug auf den Schutz klassifizierter Informationen (CI) sind zu beachten in den **Bereichen** (geregelt in der InfoSiV):

- **Personelle Sicherheit** (Need to Know-Prinzip, ev. Sicherheitsüberprüfung (gemäß SPG, MBG), Belehrung über den Umgang mit CI)
- **Physische Sicherheit** (materielle und technische Schutzmaßnahmen um unbefugten Zugang zu verhindern; Gebäude, Büros, Behältnisse, etc.)
- **Organisatorische Sicherheit** (Erstellung, Registrierung, Vervielfältigung, Beförderung von CI, etc.)
- **Schutz in Kommunikations-und Informationssystemen** (elektronische Verarbeitung, Verschlüsselung, Authentifizierung, Akkreditierung, Zusammenschaltung von Netzwerken, etc.)

Internationale und nationale Anforderungen (2)

Schutzmaßnahmen für klassifizierte Informationen in
Abhängigkeit der **Klassifizierungsstufe**:

- **Eingeschränkt** (Need to Know-Prinzip, Belehrung über den Umgang mit CI; Verarbeitung in Verwaltungsbereichen)
- **Vertraulich** (Personenüberprüfung, Registrierungspflicht, Akkreditierung von IT-Systemen, Tresore, Verarbeitung in besonders geschützten Bereichen)
- **Geheim** (wie Vertraulich, jedoch zusätzliche Schutzmaßnahmen in den Bereichen Physische und IKT-Sicherheit sowie Organisatorische Sicherheit)
- **Streng Geheim** (wie Geheim, jedoch zusätzliche Schutzmaßnahmen in den Bereichen Physische und IKT-Sicherheit sowie Organisatorische Sicherheit)

Anforderungen im Bereich industrieller Sicherheit

Industrielle Sicherheit:

- Ausstellung einer **Sicherheitsunbedenklichkeitsbescheinigung** (Facility Clearance - FSC) für Unternehmen und Anlagen
- Für internationale Verschlusssachenaufträge ab der Stufe **VERTRAULICH**
- Rechtsgrundlage: Änderung InfoSiG 2003 und 2006
- Erfüllung der in der jeweiligen völkerrechtlichen Verpflichtung vorgesehenen Auflagen und Bedingungen durch den Antragsteller (Unternehmen)
- Ausstellung der Bescheinigung durch die jeweils innerstaatlich zuständige Behörde
- International gegenseitige Anerkennung derartiger Bescheinigungen
- In Verbindung mit Personenüberprüfungen, die mit dem Auftrag Kenntnis der Verschlusssachen erlangen (PSC – Personnel Security Clearance)

Sicherheitsunbedenklichkeitsbescheinigung für Personen und Unternehmen (gemäß InfoSiG)



- **Personnel Security Clearance (PSC)**

“staatliche Bestätigung im bi- und multilateralen Bereich, dass eine Person, die nachweislich Kenntnis von klassifizierten Informationen haben muss, bis zu einem bestimmten Datum und bis zu einer bestimmten Klassifizierungsstufe Zugang gewährt werden kann”

- **Facility Security Clearance (FSC)**

“staatliche Bestätigung im bi- und multilateralen Bereich, dass ein Unternehmen den gesetzlich vorgesehenen Schutz für klassifizierte Informationen der beantragten Klassifizierungsstufe in den Räumlichkeiten des Unternehmens sicherstellen kann”

Innerstaatliche Funktionen und Stellen

- Antrag auf sicherheitspolizeiliche Überprüfung beim zuständigen BM
- Überprüfung durch BMI/BVT auf Basis der Zustimmung und der Erklärung des Betroffenen (kostenpflichtig)
- Ausstellung einer international gültigen Bescheinigung (Personnel Security Clearance Certificate, PSCC) durch das BKA, Informationssicherheitskommission, als nationale Sicherheitsbehörde (NSA – National Security Authority)

Militärischer Bereich:

- Überprüfung und Ausstellung einer derartigen Bescheinigung durch das BMLVS /AbwA als DSA (Designated Security Authority)

Personelle Sicherheit



Voraussetzungen für den Zugang zu Verschlusssachen:

- **Need-to-Know**
(Zugang zu klassifizierten Informationen nur im Rahmen der Erfüllung der dienstlichen Aufgabe)
- **Nachweisliche Unterweisung im Umgang mit CI**
Belehrung im Umgang mit klassifizierten Informationen; gesetzliche Grundlagen (völkerrechtlich und unionsrechtlich), Strafbestimmungen, Verpflichtungen wie Meldepflicht, etc.
- **Sicherheitsüberprüfung (nach SPG bzw. MBG)**
 - ab der Klassifizierungsstufe VERTRAULICH
 - für Systemadministratoren (eine Stufe höher als die verarbeitete klassifizierte Information)
- **Security Officer (Informationssicherheitsbeauftragter)**
 - Sicherstellung der Einhaltung der Schutzmaßnahmen
 - Ansprechpartner für sicherheitsrelevante Abläufe im Unternehmen
 - Schnittstelle zur nationalen Behörde bei klassifizierten Aufträgen (Meldung sicherheitsrelevanter Änderungen; z.B. personell und baulich)

Materielle Sicherheit



„Mindestanforderungen an den materiellen Schutz von Gebäuden, Büros, Räumen und sonstigen Bereichen, in denen EU-VS bearbeitet und aufbewahrt werden, einschließlich Bereichen, in denen Kommunikations- und Informationssysteme untergebracht sind“.

Umsetzungsmaßnahmen sind abhängig von:

- **Klassifizierungsgrad der Information**
- **Umgebung und Struktur der Gebäude**
- **Einschätzung der Bedrohungslage (Risikomanagementprozess)**

Bereiche:

- **Verwaltungsbereiche**
- **Besonders geschützte Bereiche**
- **Besonders geschützte Bereiche mit Abhörschutz**

Organisatorische Sicherheit / Dokumentensicherheit

Administrative Behandlung klassifizierter Informationen:



Kennzeichnung:

Kennzeichnungsvermerk gemäß national oder völkerrechtlicher Verpflichtungen (Klassifizierungsstufe, Urhebervermerk, Verteilungseinschränkungen, etc.)

Dokumentation (Registrierung):

- Führung einer eigenen Registratur (ab der Stufe VERTRAULICH)
- Lückenlose Nachvollziehbarkeit des Umlaufs der klassifizierten Information (Eingang, Ausgang, Kopien, Vernichtung, etc.)

Verwahrung:

- Entsprechende Räumlichkeiten (administrativer Bereich, besonders geschützter Bereich)
- Verwahrung in versperrenbaren Behältnissen (Büromöbel, Tresore, etc.)

Organisatorische Sicherheit / Dokumentensicherheit



Schlüsselmanagement (Kontrolle und Kombinationen)

- Ausgabeprozeduren, Ersatzschlüssel, Wechsel der Kombinationen, ...)

Übermittlung, Weiterleitung:

- Kuvertierung
- Mündliche Übermittlung
- Persönliche Übermittlung
- Übermittlung durch Zustelldienste

Meldeverfahren und Notfallpläne

INFOSEC (InformationAssurance)



„Verarbeitung von klassifizierten Informationen in Informations- und Kommunikationssystemen ist durch besondere Sicherungsmaßnahmen zu schützen“

Schutzmaßnahmen sind abhängig von:

- **Der Klassifizierungsstufe**
- **Grad der Abstrahlsicherheit der Geräte (TEMPEST)**
- **Art und Ausmaß der Vernetzung**
- **Örtlichen Gegebenheiten**

Beschreibung der Anforderungen in *ÖNORM S 2450* (Umgang mit klassifizierten Informationen – Anforderungen an den Schutz von Verschlusssachen)

Facility Security Clearance (FSC)



- Antrag auf Sicherheitsunbedenklichkeitsbescheinigung für Unternehmen und Anlagen beim zuständigen BM
- Im Zuge eines Verschlusssachenauftrages bzw. einer Forschungstätigkeit
- Prüfung des Unternehmens:
 - Organisatorische Sicherheit (Unternehmensdaten, Geschäftsführung, Sicherheitsorganisation, Security Officer, ...)
 - Materielle Sicherheit (Überprüfung der Schutzmaßnahmen in den Räumlichkeiten des Unternehmens sofern Verschlusssachen verarbeitet werden)
 - Personelle Sicherheit (SÜ für Personen, die am Verschlusssachenauftrag beteiligt sind und Kenntnis der Verschlusssachen erlangen) -> Ausstellung von PSCC
- Ausstellung einer international gültigen Bescheinigung (FSCC) durch das BKA, ISK, zur Erlangung eines Verschlusssachenauftrages

Zusammenfassung / Ausblick

- Zunahme internationaler Verschlusssachenausschreibungen
- Rechtzeitig Vorkehrungen treffen (Wettbewerbsfähigkeit)
- Überblick über Verpflichtungen verschaffen (z.B. ÖNORM S 2450, InfoSiG, InfoSiV, div. Richtlinien, etc.)
- Personenüberprüfungen, Ausstellung von PSCC (ab VERTRAULICH)
- Ansuchen um Ausstellung einer FSCC (ab VERTRAULICH)
- Interne Vorbereitungen im Bereich der Informationssicherheit (org., physisch, Information Assurance (IA))
- Ausrichtung der eigenen Informationssicherheit an internationalen Standards

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

*Ing. Gerald Trost, B.Sc.(hons)
Informationssicherheitsbüro / BKA*