BEHANDLUNGSANWEISUNGEN Nr. 7[1]

MATERIELLER GEHEIMSCHUTZ

1 EINLEITUNG

1) Physischer Geheimschutz bedeutet die Anwendung von materiellen und technischen Schutzmaßnahmen, um unbefugten Zugang zu vertraulichen Informationen zu verhindern sowie Diebstahl und Angriffe zu erschweren.

2) Um Verschlusssachen zu schützen sowie die Tätigkeit des Europäischen Parlaments in Bereichen, die ein bestimmtes Maß an Vertraulichkeit erfordern, auszubauen und zu sichern, werden eine Reihe technischer Mindestsicherheitsmaßnahmen eingeführt und gesicherte Einrichtungen geschaffen.

2 GRUNDSÄTZE

2.1 Schutz von EU-Verschlusssachen (EUCI)

3) Maßnahmen des physischen Geheimschutzes werden überall dort ergriffen, wo Verschlusssachen aufbewahrt und/oder bearbeitet werden. Maßnahmen des physischen Geheimschutzes werden schon in der Anfangsplanung berücksichtigt.

2.2 Umfang des materiellen Geheimschutzes für EU-Verschlusssachen

4) Bei der Auswahl der Maßnahmen des physischen Geheimschutzes wird allen relevanten Faktoren Rechnung getragen, darunter

a) dem Geheimhaltungsgrad der Informationen und/oder Materialien,

b) dem Umfang und der Form (z. B. Papierfassung/elektronischer Datenträger) der jeweiligen Verschlusssachen,

c) der Umgebung und Struktur der Gebäude, in denen die Verschlusssachen aufbewahrt werden,

d) der örtlichen Einschätzung der Bedrohung durch Risikomanagementdienste, die auf die Europäische Union und/oder ihre Mitgliedstaaten abzielen, sowie durch Sabotage, Terrorakte, subversive oder sonstige kriminelle Handlungen.

2.3 Ziele der Sicherheitsmaßnahmen

5) Maßnahmen des materiellen Geheimschutzes werden konzipiert, um

a) ein heimliches oder gewaltsames Eindringen abzuwehren,

[1] Beschluss des Präsidiums des Europäischen Parlaments vom 15. April 2013 über die Regeln zur Behandlung vertraulicher Informationen durch das Europäische Parlament.

b) von Tätigkeiten illoyaler Angehöriger des Personals (Spionage von innen) abzuschrecken beziehungsweise diese zu verhindern und aufzudecken,

c) die Identifizierung des Personals hinsichtlich des Zugangs zu Verschlusssachen entsprechend den erforderlichen Ermächtigungen zu ermöglichen und

d) Sicherheitsverstöße schnellstmöglich aufzudecken und darauf zu reagieren.

2.4 Grundsätze des materiellen Geheimschutzes

6) Der materielle Geheimschutz beruht auf dem Grundsatz der „mehrschichtigen Sicherheit“, d. h. einer Reihe von Sicherheitsmaßnahmen in Form eines mehrschichtigen Abwehrsystems, sowie auf Verzögerungsfaktoren.

7) Auch wenn die Maßnahmen des materiellen Geheimschutzes ortsspezifisch sein sollen, gelten die folgenden allgemeinen Grundsätze:

a) Die schutzbedürftigen Standorte werden ermittelt.

b) Mit Sicherheitsmaßnahmen wird für ein mehrschichtiges Sicherheitssystem und für Verzögerungsfaktoren gesorgt.

c) Mit der äußeren Schicht der Maßnahmen des materiellen Geheimschutzes wird der Schutzbereich festgelegt und unbefugter Zugang abgewehrt.

d) Mit der nächsten Schicht von Maßnahmen wird dafür gesorgt, dass jeder unbefugte Zugang oder Zugangsversuch erkannt und das Sicherheitspersonal alarmiert wird.

e) Durch die innere Schicht der Maßnahmen werden Eindringlinge so lange aufgehalten, bis sie von den Angehörigen des Sicherheitspersonals festgehalten werden können.

f) Die dem Sicherheitspersonal zur Verfügung stehende Zeitspanne hängt unmittelbar von den Maßnahmen des materiellen Geheimschutzes zum Aufhalten von Eindringlingen ab.

g) Die Maßnahmen des materiellen Geheimschutzes sind so konzipiert, dass sie den Eindringling länger aufhalten, als das Sicherheitspersonal für ein gestaffeltes Eingreifen benötigt.

8) Das Referat Technologien/Informationssicherheit der Generaldirektion für Sicherheit (GD Sicherheit) ist für die Umsetzung der technischen Sicherheitsstandards zuständig und führt ein Register dieser Normen und Standards, das für Kontrollen durch die zuständigen Dienststellen der anderen Organe und durch das Referat Verschlusssachen („CIU“) des Parlaments offensteht.

2.5 Gesicherte Einrichtungen

9) Zum materiellen Schutz von Verschlusssachen werden zwei Arten von materiell geschützten Bereichen eingerichtet:

a) gesicherte Bereiche

b) gesicherte Leseräume

10) Für jede gesicherte Einrichtung wird im Rahmen der sicherheitsbezogenen Betriebsverfahren Folgendes festgelegt:

a) der Geheimhaltungsgrad der Verschlusssachen, die dort bearbeitet oder aufbewahrt werden,

b) die einzuhaltenden Überwachungs- und Schutzmaßnahmen,

c) die Personen, die aufgrund der Tatsache, dass sie Kenntnis von Verschlusssachen haben müssen, und aufgrund ihrer Sicherheitsermächtigung unbegleiteten Zugang zu diesem Bereich erhalten,

d) gegebenenfalls die Verfahren für die Begleitung anderer Personen, denen Zugang zu diesem Bereich gewährt wird, bzw. die Verfahren zum Schutz der Verschlusssachen in einem solchen Fall,

e) sonstige einschlägige Maßnahmen und Verfahren.

11) Für jede gesicherte Einrichtung gilt, dass

a) ein sichtbar abgegrenzter und geschützter Bereich mit vollständiger Eingangs- und Ausgangskontrolle eingerichtet wird, die mittels eines Berechtigungsausweises oder eines Systems der persönlichen Identifizierung erfolgt;

b) unbegleiteter Zugang nur ordnungsgemäß ermächtigten Personen gewährt werden darf; bei allen anderen Personen ist eine ständige Begleitung oder eine gleichwertige Kontrolle sicherzustellen;

c) weder elektronische Kommunikationsgeräte noch elektrische oder elektronische Ausrüstung zugelassen sind.

12) Das Sicherheitsorgan bestätigt, dass ein Bereich den jeweiligen Anforderungen genügt, um als gesicherte Einrichtung zu gelten.

2.5.1 Gesicherter Bereich

13) Ein gesicherter Bereich ist ein Bereich, in dem als CONFIDENTIEL UE/EU CONFIDENTIAL oder höher oder gleichwertig eingestufte Informationen bearbeitet oder aufbewahrt werden, was bedeutet, dass das Betreten des Bereichs für alle praktischen Zwecke den Zugang zu Verschlusssachen ermöglicht. Der gesicherte

Bereich ist klar abgegrenzt und geschützt, und alle Ein- und Ausgänge des Bereichs werden kontrolliert.

14) Der gesicherte Bereich umfasst die folgenden Einrichtungen:

a) einen Raum für die Zugangs-Sicherheitsüberprüfung (SAS): ein Empfangsraum, in dem alle Mitarbeiter und Besucher überprüft, identifiziert und kontrolliert werden;

b) einen Leseraum: ein Raum, in dem das Verfahren für die Einsichtnahme in Verschlusssachen – zwecks Wahrung der Vertraulichkeit der darin enthaltenen Informationen – angewandt wird;

c) einen Registrierungsraum: der Raum, in dem als CONFIDENTIEL UE/EU CONFIDENTIAL und höher eingestufte Informationen registriert werden (Verwaltungszone);

d) ein gesichertes Archiv: ein Bereich mit Platz zum Archivieren von Verschlusssachen, der je nach Geheimhaltungsgrad des jeweiligen Dokuments unterschiedliche Standards erfüllt;

e) einen Kommunikationsraum: ein Raum, in dem spezielle Kommunikationsgeräte (Übermittlung und Empfang) und die Hardware der IT-Systeme (Kommunikations- und Informationssystem und andere), die für die Speicherung von Verschlusssachen benötigt werden, untergebracht sind.

15) Der Leseraum, der Registrierungsraum und der Kommunikationsraum werden abhörsicher gestaltet und vor elektromagnetischer Strahlung geschützt. Alle Personen, die den Bereich betreten, und alle Geräte, die in den Bereich gelangen, einschließlich verschlüsselter Nachrichtengeräte, werden kontrolliert, und gemäß den Vorschriften der zuständigen Sicherheitsbehörde in regelmäßigen Abständen einer materiellen Überprüfung/Inspektion unterzogen.

2.5.2 Gesicherte Leseräume

16) Gesicherte Leseräume sind Bereiche, in denen Verschlusssachen bis zum Geheimhaltungsgrad RESTREINT UE/EU RESTRICTED und andere vertrauliche Informationen gemäß den Behandlungsanweisungen 4 und 5 eingesehen und vorübergehend aufbewahrt werden können, wobei sie durch interne Kontrollen vor unbefugtem Zugang geschützt werden.

3 VERFAHREN

17) Der gesicherte Bereich erfüllt spezifische Schutzstandards. Der physische Geheimschutz der gesicherten Einrichtungen erstreckt sich auf mehrere Sicherheitsebenen:

a) Ebene 1: Perimeter

b) Ebene 2: Räumlichkeiten

c) Ebene 3: Tresore

3.1 Ebene 1: Perimeter

18) Zu dieser Ebene gehören:

a) die Festlegung des Perimeters

b) das Zugangskontrollsystem und Einbruchsmeldesystem für den Perimeter

c) das Videoüberwachungssystem

d) die Sicherheitsbeleuchtung

e) Sicherheitspersonal, das bei Zwischenfällen eingreift, Rundgänge durchführt, Besucher kontrolliert und Durchsuchungen an den Ein- und Ausgängen vornimmt.

19) Alle Bauten sind so zu gestalten, dass jeder Versuch eines unbefugten Eindringens erkennbar ist.

3.2 Ebene 2: Räumlichkeiten

20) Zu dieser Ebene gehören:

a) die Festlegung der strukturellen Elemente: Wände, Böden, Decken, Fenster, Türen (einschließlich der Anwendung von Standards für die Widerstandsfähigkeit gegen Angriffe)

b) das Videoüberwachungssystem

c) die Gestaltung der Zugangskontrolle und der Aufenthaltsbedingungen (Akkreditierung)

d) das Einbruchsmeldesystem

e) das Sicherheitspersonal, das bei Zwischenfällen eingreift, Rundgänge durchführt, Besucher kontrolliert und Durchsuchungen an den Ein- und Ausgängen vornimmt

21) Bei den Wänden, Zwischenwänden, Decken und Böden handelt es sich um dauerhafte Bauwerke, die lückenlos miteinander verbunden sind und nicht abgebaut oder entfernt werden können, ohne dadurch zerstört zu werden.

22) Es wird zwischen ausgewiesenen Eingangsstellen (Türen) und ausschließlich für Notfälle vorgesehenen Durchgängen (Notausgängen) unterschieden.

23) Sämtliche Eingangs- und Ausgangsstellen werden je nach Zweckbestimmung mit Einbruchsmelde- und Videoüberwachungssystemen ausgestattet und vor Zweckentfremdung geschützt.

3.3 Ebene 3: Tresore

24) Zu dieser Ebene gehören:

a) Standards für die Schlösser

b) Standards für die Tresorräume

3.4 Technische Sicherheitsmaßnahmen

25) Zu den festzulegenden strukturellen Elementen, die auch die Bestimmung der Standards für die Kapazitäten zur Abwehr von Angriffen nach einschlägigen geltenden europäischen Normen umfassen, zählen

a) Wände

b) Böden und Decken

c) Fenster

d) Türen

e) Schlösser

f) Sonstiges

26) Der Schutz aller technischen Räume und sonstigen Öffnungen (Versorgungsanlagen) erfolgt durch

a) Zugangskontrollen

b) Einbruchsmeldesysteme

c) Besucherkontrollen

- begleitet/unbegleitet
- Besucherverzeichnis
- Videoüberwachungssysteme

3.4.1 Wände

27) Alle Wände bestehen vom Boden bis zur Decke aus Vollziegeln.

3.4.2 Fenster

28) Alle Fenster und Fensterrahmen in dem Bereich erfüllen spezifische Standards.

3.4.3 Zugangstür

29) Der Türblock besteht aus einem Rahmen, einem Mittelblock und Metallbeschlägen. Er ist wie unten beschrieben zertifiziert.

3.4.4 Zugangskontrollsystem

30) Personen, die den gesicherten Bereich betreten oder ihn verlassen, werden – abgesehen von Notfällen – mittels eines Zugangskontrollsystems identifiziert. Das System besteht aus folgenden Komponenten:

a) einem Kontroll-PC, programmierbaren Zugangsstufen, Historienspeichern und einem Drucker

b) passwortgeschützter Software

c) einem einzigen Software-Paket, mit dem die Nutzer vertraut sind

d) einem vollständigen Überblick über das gesamte System zu jeder Zeit

e) integriertem Alarm/Ereignismeldungen

f) einer Verwaltungssoftware mit Kalender-, Zeiterfassungs-, Ereignisprotokoll- und Meldefunktionen

31) Das Zugangskontrollsystem beinhaltet außerdem

a) Ausweisleser mit numerischem Tastenfeld (PIN-Code),

b) Ausweismodi: hinein und hinaus.

32) Die Ausweisleser unterstützen die im Parlament eingesetzte Technologie.

33) Sämtliche Eingangs- und Ausgangsstellen werden gekennzeichnet. Bei den ausgewiesenen Eingangsstellen (Türen) und ausschließlich für Notfälle vorgesehenen Durchgängen wird wie folgt unterschieden:

a) Haupteingangsstelle

b) Nebeneingangsstellen

c) Not(ausgangs-)stelle

34) Sämtliche Eingangs- und Ausgangsstellen werden ausschließlich für ihren Zweck ausgestattet und ferner vor Zweckentfremdung geschützt.

35) Der Betriebsmodus der Zugangskontrolle ist „Fail Secure“, was bedeutet, dass

a) bei normalem Betrieb das Betreten und Verlassen des Bereichs nur unter Verwendung des Ausweises/Ausweislesers möglich sind,

b) bei einem Notfall in dem jeweiligen Raum ein Freigabegerät die Entriegelung der Tür ermöglicht, damit die darin befindlichen Personen den Raum verlassen können,

c) bei einem Stromausfall die Tür des Raumes verriegelt bleibt, das Schloss jedoch weiterhin mit einem dafür vorgesehenen Schlüssel von außen betätigt werden kann.

36) Im Türschloss wird ein Sicherheitszylinder eingebaut. Die Schlüssel für den Sicherheitszylinder werden ausschließlich vom Sicherheitsdienst verwaltet. Das Motorschloss wird mittels eines leichtgängigen Drückers mit Schlüsselreset betätigt.

37) Sämtliche Kontroll-, Steuer- und Regelungskästen werden innerhalb des Schutzbereichs installiert und an das Einbruchsmeldesystem angeschlossen (sabotagesicher).

38) Das Zugangskontrollsystem wird so konzipiert, dass ein unbefugter physischer Zugang (etwa Vandalismus) oder logischer Zugang (etwa über Netzwerke) zu den Geräten (Ausweisleser, Steuergeräte usw.) verhindert wird.

39) Jeder Zugang zum Zugangskontrollsystem wird geprüft und aufgezeichnet, und sämtliche vom System generierten Informationen und Daten werden vom Sicherheitskontrollraum überwacht.

40) Die Sicherheit beim Zugang zu gesicherten Bereichen könnte erhöht werden, indem zusätzlich eine Einrichtung zur biometrischen Kontrolle eingesetzt wird, mit der Personen anhand physischer Eigenschaften identifiziert werden können.

41) Der Anschlusskasten wird innerhalb des Bereichs und über der Tür eingebaut. Sämtliche Kabel für die Tür (Magnetkontakt, grüner Kasten und Summer) werden dort an ein Endgerät angeschlossen, das an das zum Anschlusskasten des Bereichs verlaufende Hauptkabel angeschlossen ist.

42) Das Hauptsystemgehäuse enthält die Einbruchsmeldeanlage, die Türsteuerungen, die Ausziehvorrichtung, den Netzanschluss, die Relais, den Feuerkontakt, das Fernverwaltungsnetz, nummerierte Anschlusspunkte und alle anderen Elemente, die für den ordnungsgemäßen Betrieb des Systems erforderlich sind, wobei alles an einer Montageplatte befestigt wird. Alle Kabel und Drähte werden gekennzeichnet. Das Gehäuse wird mit Kabeltüllen ausgestattet und belüftet. Es ist abschließbar und sabotagesicher. Der Anschlusskasten des Bereichs ist netzbetrieben (230 V/50 Hz/16 A) (Hauptquelle); bei einem Netzausfall wird er durch Batterien betrieben, die in ein separates Batterie-Panel eingebaut sind (Sekundärquelle).

43) Bei den Batterien handelt es sich um versiegelte, wartungsfreie Nickel-Kadmium- oder Bleibatterien mit einer Lebensdauer von fünf Jahren. Ihre Kapazität reicht aus, um die uneingeschränkte Betriebsfähigkeit des Systems zu gewährleisten. Die Batterie für die Zugangstüren muss 30 Stunden halten.

44) Mithilfe geeigneter Ladegeräte sind die Batterien in geladenem Zustand zu halten. Das Umschalten zwischen den Quellen erfolgt über einen Schalter. Ein Netzanschluss und die dazugehörige Batterie versorgen die Haupteinheit. Der andere Netzanschluss und die dazugehörige Batterie dienen der Slave-Steuerung. Die Reservebatterien können in einem separaten Gehäuse neben dem Hauptsystemgehäuse untergebracht werden. Die Batterien dürfen nicht aufeinandergelegt werden. Die Gehäuse werden mit Kabeltüllen ausgestattet und belüftet. Sie sind abschließbar und sabotagesicher.

3.4.5 Einbruchsmeldesystem

45) Der gesicherte Bereich wird durch ein unabhängiges Einbruchsmeldesystem geschützt. Alle benötigten Peripheriegeräte werden daran angeschlossen, wobei es eine Betriebsüberwachung sowie eine Sabotage- und Abschaltkontrolle gibt.

46) Das Einbruchsmeldesystem wird an die Fernverwaltungskontrollstelle angeschlossen. Der Datenverkehr zwischen diesen beiden Stellen wird mittels der Internet-Protokollsuite abgewickelt, also den Protokollen, die für die Übermittlung von Daten über das Internet verwendet werden, nämlich dem Transmission Control Protocol (TCP) und dem Internet Protocol (IP). Das Einbruchsmeldesystem wird mit den Bewegungsdetektoren und den Magnetkontakten an der Tür verbunden. Es umfasst alle Geräte, die benötigt werden, um Einbrüche innerhalb des kontrollierten Bereichs festzustellen, und reagiert entsprechend, wenn es sich im Überwachungsmodus befindet.

47) Sabotagekontakte müssen vorhanden sein; Tastenfelder, Bewegungsdetektoren, der Anschlusskasten und die Haupteinheit werden durch einen Ziehschutz geschützt, und die Schaltkreise, die die einzelnen Bauteile und das Einbruchsmeldesystem verbinden, sind permanent an die Überwachungsschleife angeschlossen.

48) Das Einbruchsmeldesystem erfüllt die folgenden Kriterien:

a) Vertraulichkeit

Die Anlagedaten zur Verbesserung und Inbetriebnahme des Systems gelten als vertraulich.

b) Signalübertragung

Die Daten werden in Echtzeit digital an eine Überwachungsstelle übermittelt, die Industriestandards erfüllt, sowie an die Fernverwaltungskontrollstelle der Direktion Sicherheit. Die folgenden Informationen werden übermittelt:

i) Einbruchsmeldung

ii) Status „Überwachung eingeschaltet“ (ganz oder teilweise)

iii) Sabotage

iv) Ausfall der Batterie- und Netzversorgung

v) Status „Überwachung eingeschaltet“ und „Überwachung ausgeschaltet“ (ganz oder teilweise) (passives Ein-/Ausschalten)

vi) Übertragungstest mindestens alle 24 Stunden

vii) Status „Überwachung spät eingeschaltet“ und „Überwachung früh ausgeschaltet“, wobei der Überwachungsstelle die Identität des Nutzers bekanntgegeben wird (aktives Ein-/Ausschalten)

c) Steuertastenfeld

Sämtliche Funktionen des Einbruchsmeldesystems werden über das numerische Steuertastenfeld aktiviert. Insbesondere werden Art und Ort jedes Ereignisses angezeigt. Außerdem verfügt das Tastenfeld über ein lokales Alarmsignal (Summer). Es ertönen akustische Signale, wenn bestimmte Funktionen aktiviert werden, während der Verzögerungszeit beim Betreten und Verlassen des Raums und wenn Zifferntasten gedrückt werden (Validierung).

Das numerische Steuertastenfeld zum Scharf-/Unscharfschalten des Bereichs wird entweder hinter oder vor – in jedem Fall jedoch in der Nähe – der Zugangstür des Bereichs angebracht.

Das in dem gesicherten Bereich eingebaute Alarmsystem muss von dem Einbruchsmeldesystem des Gebäudes getrennt sein.

Das Referat Verschlusssachen wird von jeder Meldung in dem gesicherten Bereich unverzüglich in Kenntnis gesetzt.

d) Bewegungsmelder mit Dualtechnologie

Der Bereich wird mit Dualtechnologie- oder bivolumetrischen Bewegungsmeldern ausgestattet, die in ein und derselben Einheit Höchstfrequenz- und Passiv-Infrarotmelder vereinen, wobei das System über eine Mikroprozessor-Steuerung verfügt und für jede Umgebung geeignet ist. Die Aktivierung bzw. Deaktivierung erfolgt mittels Überbrückungen: Alarmspeicher, Impulszählung, PIR- oder Mikrowellendetektion.

49) Das Einbruchsmeldesystem umfasst

a) eine Bedienung für das Alarmsystem: lokale Steuerbefehle, Befehle per Fernsteuerung

b) PIN-Code-Verwaltung

c) volumetrische Bewegungsmelder: Dualtechnologie mit Antimask-Funktion

d) Magnetkontakte für

i) Türen

ii) Fenster

iii) sonstige Öffnungen

iv) Gehäuse, gesicherte Behälter, Schränke

e) Körperschallmelder an Fenstern und Wänden

f) Glasbruchmelder an Fenstern

g) Summer (lokales Alarmsignal)

50) Sämtliche Kontroll-, Steuer- und Regelungskästen werden innerhalb des Schutzbereichs angebracht und an das Einbruchsmeldesystem angeschlossen (sabotagesicher).

51) Das Einbruchsmeldesystem wird so konzipiert, dass ein unbefugter physischer Zugang (etwa Vandalismus) oder logischer Zugang (etwa über Netzwerke) zur Kamera und zu den aufgezeichneten Bildern verhindert wird.

52) Jeder Zugang zum Einbruchsmeldesystem wird geprüft und aufgezeichnet, und sämtliche vom Einbruchsmeldesystem generierten Informationen und Daten werden vom Sicherheitskontrollraum aus überwacht.

3.4.6 Videoüberwachungssystem

53) Die Zugangstür zum gesicherten Bereich wird per Videoüberwachungssystem überwacht; die Bilder werden an den Empfang des Gebäudes und die Fernverwaltungskontrollstelle der Direktion Sicherheit übermittelt. Die Kamera ist an ein Bildaufnahmesystem angeschlossen, so dass die Bilder zu einem späteren Zeitpunkt von befugten Personen eingesehen werden können. Sie wird an einem als sicherheitsrelevant geltenden Ort angebracht. Beim Öffnen der Tür – von innen oder von außen – wird eine Aufnahmesequenz ausgelöst.

54) Die Kameras erfüllen die erforderlichen Standards, weisen die erforderlichen Merkmale auf und sind vandalismussicher.

55) Die Aufzeichnung erfolgt in Übereinstimmung mit der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr.

56) Der Zugang zum Aufnahmesystem ist durch Benutzernamen und Passwörter geschützt. Die Aufnahmen dürfen nur von Personen angesehen werden, die vom CIU entsprechend ermächtigt wurden, und nur der zuständige Administrator darf Videosequenzen löschen.

57) Das Videoüberwachungssystem

a) erfasst den Perimeter, die Eingangs- und Ausgangsstellen sowie die Kontrollstellen außerhalb des Bereichs,

b) erfasst die Eingangs- und Ausgangsstellen, Kontrollstellen, Räume sowie wichtige Anlagen und Geräte innerhalb des Bereichs,

c) legt die Art der Kameras nach Standort fest, wobei es sich um statische Kameras, PTZ-Kameras oder Infrarotkameras handeln kann,

d) legt zu Einstellungszwecken für jede Kamera die erforderliche Identifizierungsebene fest, wobei dies das Gesicht, die Person, die Tätigkeit oder die allgemeine Szenerie sein kann,

e) umfasst Betriebs- und Visualisierungsgeräte (Computer, Bildschirme),

f) umfasst Aufnahme- und Speichergeräte sowie Backup-Möglichkeiten,

g) verfügt über ausreichend Licht, um eine optimale Überwachung zu gewährleisten (mindestens 1 Lux).

58) Sämtliche Kontroll-, Steuer- und Regelungskästen werden innerhalb des Schutzbereichs angebracht und an das Einbruchsmeldesystem angeschlossen (sabotagesicher).

59) Das Videoüberwachungssystem wird so konzipiert, dass ein unbefugter physischer Zugang (etwa Vandalismus) oder logischer Zugang (etwa über Netzwerke) zur Kamera und zu den aufgezeichneten Bildern verhindert wird.

60) Jeder Zugang zum Videoüberwachungssystem wird geprüft und aufgezeichnet, und sämtliche vom Videoüberwachungssystem generierten Informationen und Daten werden vom Sicherheitskontrollraum aus überwacht.

3.5 Überwachung

61) Für die Überwachung der Sicherheitsausrüstung ist die Direktion Sicherheit zuständig:

a) vor Ort

b) Arbeitsplan: 24 Stunden am Tag, 7 Tage die Woche, 365 Tage im Jahr

c) Einrichtung von Kommunikationsmitteln

d) Betriebsverfahren für Notfälle

e) Betriebsverfahren für den Betrieb der technischen Geräte

62) Die Überwachung erfolgt durch entsprechend geschultes und qualifiziertes Sicherheitspersonal mit Sicherheitsermächtigung, und es sollten Betriebsverfahren für Notfälle, Rundgänge und Inspektionen eingeführt werden.

3.6 Gehäuse

63) Planung und Beschaffung von Gehäusen oder gesicherten Behältern, in denen alle Überwachungsgeräte zusammengefasst werden:

a) das Zugangskontrollsystem

b) das Einbruchsmeldesystem

c) das Videoüberwachungssystem

d) Die Gehäuse und gesicherten Behälter werden an das Einbruchsmeldesystem angeschlossen.

3.7 Stromversorgung

64) Es wird ein Notstromaggregat eingerichtet, mit dem die Sicherheit mindestens 24 Stunden lang gewährleistet wird, falls die Stromversorgung über das normale Stromnetz ausfällt.

65) Eine batteriegestützte, unterbrechungsfreie Lösung, die in einem separaten und geeigneten Schrank untergebracht und an das Einbruchsmeldesystem angeschlossen ist (sabotagesicher), wird eingerichtet und die gesamte Stromversorgung wird überwacht.

3.8 Tresore und Schlösser

66) Die gesicherten Schränke und Behälter sind mit mechanischen oder elektronischen Kombinationsschlössern oder einer gleichwertigen Vorrichtung ausgestattet und erfüllen die dem Geheimhaltungsgrad der Informationen, die darin aufbewahrt werden sollen, entsprechenden Standards. Sie werden innerhalb des gesicherten Bereichs aufgestellt.

67) Die Behälter werden nach ihrer Widerstandsfähigkeit gegen gewaltsames und heimliches Eindringen klassifiziert. Dabei können vier verschiedene Arten von Behältern verwendet werden.

a) Behälter vom Typ 4: Diese Behälter sind für die Aufbewahrung aller EU-Verschlusssachen, einschließlich der als TRES SECRET UE/EU TOP SECRET eingestuften Informationen, innerhalb des gesicherten Bereichs zugelassen. Sie bieten ein hohes Maß an Schutz vor einem Eindringen durch

Anwendung von Gewalt oder den Einsatz diverser Hand- und Maschinenwerkzeuge sowie vor unbemerktem und heimlichem Eindringen. Sie halten dem Aufbrechen von Türen, Schubladen und Klappen zum Zwecke des „Herausangelns“ oder Durchsuchens stand.

b) Behälter vom Typ 3: Diese Behälter sind für die Aufbewahrung von als CONFIDENTIEL UE/EU CONFIDENTIAL und SECRET UE/EU SECRET eingestuften Informationen innerhalb des gesicherten Bereichs zugelassen. Sie bieten ein gewisses Maß an Schutz vor einem Eindringen durch Anwendung von Gewalt oder den Einsatz eines begrenzten Spektrums von Handwerkzeugen sowie vor unbemerktem und heimlichem Eindringen. Sie halten Verbiegungen, Verdrehungen und Stößen stand, durch die der Körper deformiert und das Einführen von Sonden oder Geräten ermöglicht werden könnte, um sich Zugang zum Inneren des Behälters zu verschaffen.

c) Behälter vom Typ 2: Diese Behälter sind für die Aufbewahrung von als CONFIDENTIEL UE/EU CONFIDENTIAL eingestuften Informationen innerhalb des gesicherten Bereichs zugelassen. Ihre Ausführung und Bauweise sind robust und sie halten Gelegenheitseindringlingen stand, die die Tat nicht vorbereitet haben und nur griffbereite Gegenstände verwenden können.

d) Behälter vom Typ 1: Diese Behälter sind für die Aufbewahrung von als RESTREINT UE/EU RESTRICTED eingestuften Informationen zugelassen. Ihre Ausführung weist zwar keine besonderen Sicherheitsmerkmale auf, sie können jedoch gesichert werden und bieten ein gewisses Maß an Sicherheitsintegrität.

68) Die Schlösser für die Behälter werden danach klassifiziert, inwieweit sie zur Abwehr von unbefugtem Öffnen geeignet sind. Dabei können vier verschiedene Arten von Schlössern verwendet werden:

a) Schlösser vom Typ 4: Diese Schlösser bieten ein hohes Maß an Schutz vor einem fachmännischen und professionellen Eindringen mithilfe exklusiv entwickelter Fertigkeiten und Hilfsmittel, die als nicht im Handel erhältlich gelten.

b) Schlösser vom Typ 3: Diese Schlösser bieten ein hohes Maß an Schutz vor einem fachmännischen und professionellen Eindringen mithilfe exklusiv entwickelter Fertigkeiten und Hilfsmittel, die als für einen Berufsschlosser im Handel erhältlich gelten.

c) Schlösser vom Typ 2: Diese Schlösser bieten ein gewisses Maß an Schutz vor einem geschickten Eindringling mit minimalen Hilfsmitteln.

d) Schlösser vom Typ 1: Diese Schlösser bieten ein moderates Maß an Schutz vor unbefugtem Öffnen.

69) Die Schlösser für die Behälter vom Typ 3 oder 4 können geprüft werden.