Rat der
Europäischen Union

Brüssel, den 6. März 2015
(OR. en)

6488/15

CSCI 9
CSC 45

I/A-PUNKT-VERMERK

des	Sicherheitsausschusses des Rates
für den	AStV/Rat
Betr.:	Sicherheitskonzept für die Informationssicherung bei Zusammenschaltungen

1. Nach dem Beschluss des Rates über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen[1] billigt der Rat – soweit erforderlich – "auf Empfehlung des Sicherheitsausschusses Sicherheitskonzepte mit Maßnahmen zur Anwendung dieses Beschlusses" (siehe Artikel 6 Absatz 1).

2. Der Sicherheitsausschuss des Rates ist übereingekommen, ein Konzept zu empfehlen, mit dem für die Zusammenschaltung von Kommunikations- und Informationssystemen (CIS), mit denen EU-Verschlusssachen (EU-VS) bearbeitet werden, Standards hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit sowie gegebenenfalls Authentizität und Nichtabstreitbarkeit festgelegt werden.

3. Vorbehaltlich der Bestätigung durch den AStV wird der Rat ersucht, das beigefügte Sicherheitskonzept zu billigen.

[1] Beschluss 2013/488/EU des Rates (ABl. L 274 vom 15.10.2013, S. 1).

Absichtliche Leerseite

Sicherheitskonzept für die Informationssicherung bei Zusammenschaltungen

IASP 3

INHALT

1. ZWECK UND ANWENDUNGSBEREICH

1. Dieses Konzept, das vom Rat gemäß Artikel 6 Absatz 1 der Sicherheitsvorschriften des Rates (im Folgenden "SVR") gebilligt wurde, legt Standards für den Schutz von EU-Verschlusssachen (EU-VS) fest. Es soll dazu beitragen, dass die SVR in einheitlicher Weise angewandt werden.

2. Mit diesem Konzept sollen die Regeln und Beschränkungen für die Zusammenschaltung eines Kommunikations- und Informationssystems (CIS), in dem EU-VS bearbeitet werden, mit einem anderen CIS festgelegt werden. Im Rahmen des Konzepts wird ferner ein Modell definiert (siehe Anlage I), das als gemeinsame Sprachregelung für die Beschreibung einer Zusammenschaltung dienen soll. In dem Dokument werden nur die zusätzlichen Risiken für CIS aufgrund der Zusammenschaltung behandelt.

3. Der Rat und das Generalsekretariat des Rates wenden dieses Sicherheitskonzept für den Schutz von EU-VS in ihren Räumlichkeiten und in ihren CIS an.

4. Die Mitgliedstaaten sorgen nach Maßgabe ihrer innerstaatlichen Rechts- und Verwaltungsvorschriften für die Einhaltung der in den Sicherheitskonzepten festgelegten Standards, wenn EU-VS in nationalen Strukturen – einschließlich nationaler CIS – bearbeitet werden.

5. Die im Rahmen des Titels V Kapitel 2 EUV errichteten Agenturen und Einrichtungen der EU sowie Europol und Eurojust sollten dieses Sicherheitskonzept als Bezugsrahmen für die Anwendung der Sicherheitsvorschriften in ihren eigenen Strukturen verwenden.

6. Eine Systemzusammenschaltung wird definiert als die direkte[2] Verbindung von zwei oder mehr IT-Systemen für die gemeinsame Nutzung von Daten[3] und anderen Informationsressourcen (beispielsweise Kommunikation); die Verbindung kann unidirektional oder multidirektional sein. Hauptgrund für die Zusammenschaltung von Systemen ist die Erbringung oder Inanspruchnahme der folgenden Arten von Diensten:

   (a) ein Dienst, der den Austausch von Informationen zum Gegenstand hat,

   (b) ein Dienst, der die Bereitstellung einer technischen Kommunikationsinfrastruktur zum Gegenstand hat (ein Informationsaustausch ist nicht beabsichtigt).

7. Dieses Konzept gilt nicht für den Austausch von Informationen mit Hilfe von Wechseldatenträgern.

8. Dieses Konzept gilt für CIS, mit denen EU-VS bearbeitet werden und die mit einem anderen Informationssystem (IS) zusammengeschaltet sind, mit dem nicht notwendigerweise EU-VS bearbeitet werden müssen.

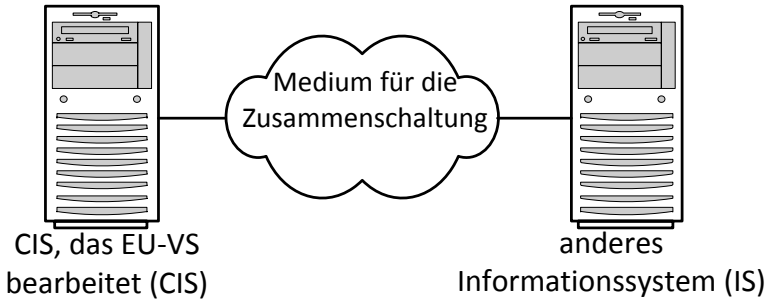

Abbildung 1: Allgemeines Modell für eine Zusammenschaltung

[2] Im Gegensatz zur kaskadierten Verbindung.

[3] Im Rahmen dieses Dokuments ist unter Daten die spezifische Darstellung von Informationen (z.B. eine Reihe von Bytes) zu verstehen; dabei muss einem vorgegebenen Format entsprochen werden, mit dem festgelegt wird, wie die Kodierung der Informationen erfolgt.

9. Eine Verbindung zwischen zwei IT-Systemen ist als Zusammenschaltung zu betrachten, wenn sich die Systeme in mindestens einem der folgenden Merkmale unterscheiden:

(a) höchster Geheimhaltungsgrad der bearbeiteten EU-VS,

(b) Sicherheitsziele[4],

(c) Sicherheitsmodus des Betriebs,

(d) einschlägige Sicherheits-Akkreditierungsstelle (SAA),

(e) geltende Sicherheitskonzepte (z.B. EU-System und nationales System eines Mitgliedstaats),

(f) für den Betrieb des Systems zuständige Stellen (z.B. Generalsekretariat des Rates, dezentrale EU-Agentur),

(g) rechtliche Anforderungen,

(h) sonstige einschlägige Sicherheitsparameter (Grundsatz "Kenntnis nur, wenn nötig" oder Interessengemeinschaft, Beschränkungen, spezifische Protokolle, technisch überholte Anlagen, Umfang des materiellen Schutzes, Art des Unterstützungsnetzes, Eigentum an den verbreiteten Informationen).

Jede Änderung im CIS, mit der neue Komponenten[5] eingeführt werden und die keinem der vorstehenden Kriterien entspricht, wird grundsätzlich nicht als Zusammenschaltung betrachtet.

In allen anderen Fällen muss die Entscheidung, ob eine Verbindung oder ein interner Link eine Zusammenschaltung darstellt oder nicht, von der bzw. den zuständigen SAA getroffen werden.

---

4 Entsprechend der Festlegung in der Aufstellung der systemspezifischen Sicherheitsanforderungen.

5 Z.B. ein neues Arbeitsplatzgerät, neue Netzausrüstung usw.

10. Ungeachtet der vorgesehenen Richtung des Informationsflusses kann die Zusammenschaltung einen bidirektionalen Kommunikationskanal[6] zwischen den beiden CIS öffnen und potenziell Zugang zu vielen Diensten und Informationen gewähren, die ungewollt über den Umfang der betrieblichen Anforderungen hinausgehen.

11. Die Zusammenschaltung kann daher folgende Änderungen der CIS-Risikobewertung bewirken:

    (a) Die Bedrohungsquellen für das IS können auf das CIS übertragen werden.

    (b) Die Schwachstellen im IS können die Wahrscheinlichkeit einiger Risikoszenarien und/oder deren Auswirkungen auf das CIS erhöhen.

    (c) Die Schwachstellen im IS und die Zusammenschaltung selbst können eine Reihe neuer Risikoszenarien für das CIS hervorrufen.

    (d) Die Zusammenschaltung schafft eine Abhängigkeit sowohl auf betrieblicher als auch auf technischer Ebene und kann daher Verfügbarkeitsrisiken hervorrufen.

    (e) Die umfassende Ausnutzung der Funktionalitäten und Schwachstellen der beiden zusammengeschalteten Systeme kann Synergien erzeugen und neue Angriffsvektoren eröffnen.

    (f) Die Komponenten, die für die Herstellung der Zusammenschaltung und/oder zur Verringerung der durch die Zusammenschaltung hervorgerufenen Risiken verwendet werden, können selbst Ziele eines Angriffs werden und neue Schwachstellen entstehen lassen.

12. Der Dienst für den Schutz von Systemübergängen (Boundary Protection Service, BPS) ist ein Dienst, der die durch die Zusammenschaltung entstehenden Sicherheitsrisiken verringert. Die Kontrolleinrichtungen, die den BPS bereitstellen, werden Komponenten für den Schutz von Systemübergängen (Boundary Protection Components, BPC) genannt; dies können beispielsweise Datensicherungsprozeduren, Antivirenprogramme oder physische Zugangskontrollen sein. Spezielle BPC, die Informationsflüsse regeln und/oder die Sicherheitsdienste am Zusammenschaltungspunkt erbringen, werden Vorrichtungen für den Schutz von Systemübergängen (Boundary Protection Devices, BPD, z.B. Firewall, Datendiode) genannt.

---

6 Z.B. wenn die Zusammenschaltung auf dem Übertragungskontrollprotokoll (Transmission Control Protocol – TCP) beruht.

2. DAS KONZEPT

13. Ein CIS muss jedes mit ihm zusammengeschaltete IS zunächst als nicht vertrauenswürdig behandeln; daher müssen sämtliche Annahmen in Bezug auf das IS im Rahmen des Risikomanagementprozesses angemessen berücksichtigt werden. Das CIS muss geeignete Kontrollen (z.B. Dienstgütevereinbarungen (SLA), Dienste für den Schutz von Systemübergängen) durchführen, um sicherzustellen, dass die Annahmen in Bezug auf das IS zutreffen.

14. Der Entscheidung über die Zusammenschaltung von CIS muss ein zutreffendes betriebliches Erfordernis zugrunde liegen.

15. Das CIS muss den Austausch von Informationen und den Zugang zu Diensten unterbinden, die im Rahmen der betrieblichen Anforderungen nicht ausdrücklich festgelegt sind. Es muss sichergestellt sein, dass ein System mit niedrigerem Vertraulichkeitsgrad nicht an Informationen oder Dienste mit höherem Vertraulichkeitsgrad gelangen kann.

16. Eine Zusammenschaltung zwischen einem CIS und einem IS mit einem niedrigeren bzw. gar keinem Vertraulichkeitsgrad ist nur dann zulässig, wenn das CIS mit zugelassenen Diensten für den Schutz von Systemübergängen zwischen dem CIS und dem IS ausgestattet ist, beispielsweise durch Verwendung einer zugelassenen Datendiode. Der gewählte Dienst für den Schutz von Systemübergängen muss die ermittelten Risiken auf ein akzeptables Maß verringern.

17. Die Zusammenschaltung ist einem Akkreditierungsverfahren zu unterziehen und bedarf der Genehmigung durch die zuständige SAA.

18. Der Risikomanagementprozess für das CIS muss bei jeder neuen Zusammenschaltung wiederholt werden. Im Rahmen des Prozesses müssen zumindest die in Anlage II beschriebenen Aspekte berücksichtigt werden.

19. Bringt eine Zusammenschaltung neue als hoch einzuschätzende Risiken für das CIS mit sich, so kann dies eine Neuakkreditierung des CIS erfordern. Die Neuakkreditierung des CIS ist erforderlich, wenn es mit einem nicht akkreditierten IS zusammengeschaltet wird.

20. Ein CIS, das für die Bearbeitung von Verschlusssachen des Geheimhaltungsgrads "TRÈS SECRET UE/EU TOP SECRET" akkreditiert ist, darf nicht mit einem ungeschützten oder öffentlichen Netz (weder direkt noch indirekt – über ein anderes IS) zusammengeschaltet werden.

21. Wenn das IS lediglich eine Kommunikationsinfrastruktur für die Übertragung der Daten bietet und die Daten durch ein gemäß Artikel 10 der SVR zugelassenes kryptografisches Produkt verschlüsselt werden, gilt eine derartige Verbindung nicht als Zusammenschaltung.

22. Sind neue Zusammenschaltungen mit einem IS geplant, das bereits mit einem CIS zusammengeschaltet ist, so muss die für das CIS zuständige Sicherheits-Akkreditierungsstelle (SAA) darüber unterrichtet werden. Im Falle einer erneuten Zusammenschaltung des CIS ist die für das IS zuständige SAA in gleicher Weise zu unterrichten.

23. Es dürfen nur die Protokolle, Netzdienste sowie Informations- oder Datenflüsse installiert, konfiguriert und im Rahmen der Zusammenschaltung genutzt werden, die zur Durchführung der betrieblichen Aufgaben erforderlich sind (Minimalitätsprinzip).

24. Für Nutzer und Verfahrensabläufe, welche die Zusammenschaltung nutzen bzw. Teil davon sind, dürfen nur die Berechtigungen und Genehmigungen erteilt werden, die für die Erfüllung ihrer Aufgaben und Pflichten erforderlich sind (Prinzip der minimalen Zugriffsrechte).

25. Für ein zusammengeschaltetes CIS müssen Maßnahmen zum Abblocken aller Tätigkeiten und Informationsflüsse durchgeführt werden, die kein rechtmäßiger Bestandteil der mit der Zusammenschaltung verknüpften Abläufe sind (Prinzip des Selbstschutzes).

26. Für verschiedene Komponenten der Zusammenschaltungsarchitektur[7] müssen Schutzmaßnahmen durchgeführt werden, um dafür zu sorgen, dass nicht nur eine einzige Verteidigungslinie besteht (Prinzip des mehrschichtigen Sicherheitssystems).

27. Die Herstellung einer Zusammenschaltung muss von der zuständigen SAA bei der erstmaligen Herstellung der Zusammenschaltung und danach in regelmäßigen Abständen überprüft[8] werden. Die SAA sollte bereits während der Planungs- und Konzeptionsphase einbezogen und auch an der Risikobewertung der Zusammenschaltung beteiligt werden.

---

7 Neben der eigentlichen Zusammenschaltung umfasst die Architektur auch das CIS und das IS.

8 Dabei wird überprüft, ob die Herstellung der Konzeption und den Beschlüssen über die Aufnahme von Kontrollen in den Risikomanagementprozess entspricht.

28. Die Entwicklung einer Zusammenschaltung ist entweder ein Teil des CIS-Entwicklungsprojekts oder aber ein separates Projekt, wenn die Zusammenschaltung einem bereits bestehenden CIS hinzugefügt wird. Die Projektmanagementmethodik, die Diensteverwaltung und der Lebenszyklus der Zusammenschaltung werden im Rahmen dieses Dokuments nicht behandelt. Allerdings beinhaltet der Lebenszyklus der Zusammenschaltung die im IASP-L[9] beschriebenen Phasen des Sicherheits-Lebenszyklus:

(a) Begründung der Sicherheit der Zusammenschaltung: Ziel der Sicherheitsbegründung ist die Herausarbeitung aller Sicherheitsanforderungen an die Zusammenschaltung und der für das IS notwendigen Sicherheitsanforderungen.

(b) Gestaltung der Sicherheit der Zusammenschaltung: Die Anforderungen an die Betriebssicherheit werden in Sicherheitsgrundsätze und -kontrollen umgesetzt, die unter Einsatz einer adäquaten Kombination von Menschen, Verfahren und Technologien ausgewählt und angewendet bzw. durchgeführt werden. Am Ende dieser Phase sollte die Zusammenschaltung in der Betriebsumgebung einsatzbereit und im erforderlichen Umfang akkreditiert sein.

(c) Aufrechterhaltung der Sicherheit der Zusammenschaltung: Die Zusammenschaltung muss nach ihrer Fertigstellung aktiv instandgehalten und überwacht werden, damit sichergestellt ist, dass sie ordnungsgemäß und sicher funktioniert.

(d) Sichere Außerbetriebnahme der Zusammenschaltung: Wenn die Notwendigkeit der Zusammenschaltung nicht länger gegeben ist oder eines der zusammengeschalteten CIS die Phase der Außerbetriebnahme erreicht, wird die Zusammenschaltung entsprechend den zugelassenen Verfahren außer Dienst gestellt.

9 IASP-L IA Security Policy on Security throughout the CIS Life Cycle (Dok. 14968/2012).

BEGRIFFSBESTIMMUNGEN

Akkreditierung	das Verfahren, das zu einer förmlichen Erklärung der Sicherheits-Akkreditierungsstelle (SAA) führt, wonach ein System für den Betrieb mit einem definierten Geheimhaltungsgrad, in einem bestimmten Sicherheitsmodus in seiner Betriebsumgebung und bei einem akzeptablen Risikoniveau unter der Voraussetzung zugelassen wird, dass ein anerkanntes Bündel von Sicherheitsmaßnahmen in den Bereichen Technik, physischer Schutz, Organisation und Verfahren durchgeführt wird.
Authentizität	die Garantie, dass die Informationen echt sind und aus Bona-fide-Quellen stammen.
Verfügbarkeit	der Umstand, dass die Informationen auf Anfrage einer befugten Stelle verfügbar und nutzbar sind.
Kommunikations- und Informationssystem	ein System, das die Bearbeitung von Informationen in elektronischer Form ermöglicht. Zu einem Kommunikations- und Informationssystem gehören sämtliche für seinen Betrieb benötigten Voraussetzungen, einschließlich der Infrastruktur, der Organisation, des Personals und der Informationsressourcen. Siehe Artikel 10 Absatz 2 der SVR.
CIS	ein Kommunikations- und Informationssystem, mit dem EU-VS bearbeitet werden.
Vertraulichkeit	der Umstand, dass die Informationen nicht gegenüber unbefugten Personen, Stellen oder Verarbeitungsprozessen offengelegt werden.
EU-Verschlusssachen (EU-VS)	alle mit einem EU-Geheimhaltungsgrad gekennzeichneten Informationen oder Materialien, deren unbefugte Weitergabe den Interessen der Europäischen Union oder eines oder mehrerer ihrer Mitgliedstaaten in unterschiedlichem Maße schaden könnte. Siehe Artikel 2 Absatz 1 der SVR.
Integrität	der Umstand, dass die Genauigkeit und die Vollständigkeit der Informationen und Werte gewährleistet sind.
Nichtabstreitbarkeit	die Fähigkeit, nachzuweisen, dass ein Vorgang oder ein Ereignis stattgefunden hat, so dass dieser Vorgang oder dieses Ereignis nicht nachträglich abgestritten werden kann.
Risiko	die Möglichkeit, dass bei einer bestimmten Bedrohung die internen und externen Schwachstellen einer Organisation oder eines der von ihr verwendeten Systeme ausgenutzt und dadurch die Organisation und ihre materiellen und immateriellen Werte geschädigt werden. Gemessen wird das Risiko als die Kombination der Wahrscheinlichkeit des Eintretens von Bedrohungen und ihrer Auswirkungen.

ANLAGE I

MODELL FÜR EINE ZUSAMMENSCHALTUNG

1. In dieser Anlage wird ein denkbares Modell für die Beschreibung einer Zusammenschaltung definiert. Anhand dieses Modells sollen die Risiken aufgezeigt werden, die sich für ein CIS durch die Zusammenschaltung ergeben.

2. Eine Zusammenschaltung lässt sich durch zwei Parameter beschreiben, nämlich die "Sicherheitsvoraussetzungen" und die "Funktion" (siehe Abbildung 2), wobei die "Sicherheitsvoraussetzungen" ein Bündel von Attributen darstellen wie etwa unterschiedliche Akkreditierungsstufen, Eigentum, Betriebsmodi usw. und "Funktion" die Funktion des CIS bei der Zusammenschaltung beschreibt, die definiert wird durch

   (a) die "Flussrichtung" (Richtung des Informationsflusses) aus Sicht des CIS und

   (b) die "Diensterbringung", d.h. die Funktion des CIS bei der Erbringung oder Nutzung des durch die Zusammenschaltung bereitgestellten Dienstes.

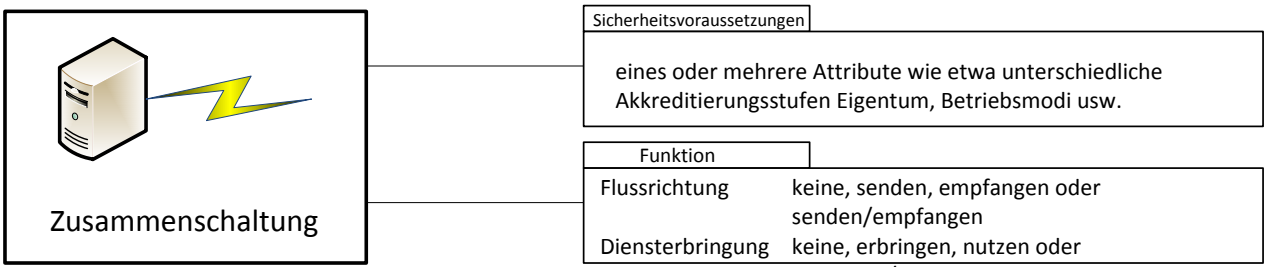

Abbildung 2: Die eine Zusammenschaltung beschreibenden Parameter

3. Das auf der Betriebsebene (logischen Ebene) benötigte Zusammenschaltungsmodell sollte bei der technischen Umsetzung gewahrt bleiben. Dies bedeutet, dass die technische Umsetzung nicht dazu führen sollte, dass mehr Flussrichtungen oder Dienste als notwendig angeboten werden. Alle Abweichungen von den Betriebserfordernissen auf technischer Ebene sollten als Risiko behandelt und von den Diensten für den Schutz von Systemübergängen in geeigneter Weise minimiert werden.

4. Die Werte des Attributs "Funktion" sind nachstehend in Tabelle 1 erläutert.

Attribut	**Wert**	**Beschreibung**
Flussrichtung	keine	Es besteht kein Betriebserfordernis für den Austausch von Informationen zwischen dem CIS und dem IS. Es kann jedoch eine Zusammenschaltung auf der Infrastrukturebene geben (die einen unbeabsichtigten Informationsfluss hervorrufen kann).
	empfangen	Das CIS empfängt Informationen vom IS.
	senden	Das CIS sendet Informationen an das IS[10].
	senden/empfangen	Das CIS sendet und empfängt Informationen.
Diensterbringung	keine	Da kein Dienst genutzt oder erbracht wird, besteht kein betrieblicher Grund für die Zusammenschaltung von zwei Systemen. Dies wäre nicht zulässig, weshalb keine Zusammenschaltung erfolgen darf.
	nutzen (Dienstnutzer)	Das CIS nutzt einen vom IS erbrachten Dienst. Bei den meisten Umsetzungen wird das CIS als Client des IS agieren (allerdings sind verschiedene Modelle möglich).
	erbringen (Diensterbringer)	Das CIS erbringt einen Dienst für das IS. Ziel des Dienstes kann ein Informationsaustausch oder die Bereitstellung von Infrastruktur (z. B. Kommunikationsinfrastruktur) sein. Im Falle eines Informationsaustausches fungiert das CIS normalerweise als Server (allerdings sind verschiedene Modelle möglich).
	erbringen/nutzen	Das CIS muss Dienste erbringen und erwartet gleichzeitig Dienste vom IS.

Tabelle 1: Mögliche Werte des Attributs "Funktion" bei der Zusammenschaltung

10 Hinweis: Eine Empfangsbestätigung (soweit erforderlich) wird als Informationsfluss vom Empfänger zum Absender betrachtet.

5. Die Beschränkungen und Erfordernisse für zusätzliche Sicherheitsmaßnahmen für die "Funktionen" und die "Sicherheitsvoraussetzungen" werden in begleitenden Sicherheitsleitlinien für Informationssicherung beschrieben.

6. Die Tatsache, dass zwei verschiedene Zusammenschaltungen durch dieselbe "Rolle" und dieselben "Sicherheitsvoraussetzungen" beschrieben werden, führt dazu, dass die Zusammenschaltungen unter dem Gesichtspunkt der Sicherheit einander ähneln, was jedoch nicht bedeutet, dass sie identisch sind. Deshalb muss neben der Prüfung, ob die Leitlinien eingehalten werden, die Entscheidung darüber, ob eine Zusammenschaltung "sicher genug" ist oder nicht, in jedem Fall auf der Grundlage eines Risikomanagementprozesses getroffen werden.

ANLAGE II

BEIM RISIKOMANAGEMENT ZU BERÜCKSICHTIGENDE ASPEKTE

1. Die Auswirkungen der Zusammenschaltung auf das Risikomanagement (des CIS) hängen in erheblichem Maße von den tatsächlichen Umständen (betriebliche Anforderungen, technische Umsetzung) ab. Diese Anlage enthält eine allgemeine Liste mit Anliegen, die gegebenenfalls berücksichtigt werden müssen. Die Einzelheiten zu bestimmten Modellen und Umsetzungen werden in den Leitlinien festgelegt.

2. Der Umfang des Risikomanagementprozesses wird sich höchstwahrscheinlich ändern, wenn eine neue Zusammenschaltung erfolgt; in einem solchen Fall müssen insbesondere die nachstehend aufgeführten Elemente analysiert werden:

   (a) Datenbestände – sie sind im Rahmen des Risikomanagementprozesses möglicherweise als neue Bestände zu betrachten;

   (b) Betriebsprozesse – höchstwahrscheinlich werden ein oder mehrere Betriebsprozesse geändert, um die Zusammenschaltung zu rechtfertigen;

   (c) vertragliche Verpflichtungen – die Zusammenschaltung kann eine vertragliche Verpflichtung für den Eigentümer des CIS mit sich bringen;

   (d) Schnittstellen – die Zusammenschaltung stellt eine neue Schnittstelle dar;

3. Im Rahmen des Prozesses zur Feststellung des Bedrohungspotenzials sollten folgende unerwünschte Ereignisse berücksichtigt werden:

   (a) unberechtigte Benutzer oder Programme, die im IS angemeldet sind bzw. ausgeführt werden, versuchen, auf Dienste des CIS zuzugreifen;

   (b) unberechtigte Benutzer oder Programme, die im CIS angemeldet sind bzw. ausgeführt werden, versuchen, auf Dienste des IS zuzugreifen;

   (c) Informationen, die nicht an das IS übertragen werden dürfen, werden (irrtümlicherweise oder absichtlich) an das IS übertragen;

(d) Informationen, die nicht an das CIS übertragen werden dürfen, werden vom IS übertragen;

(e) das IS steht nicht mehr zur Verfügung (hat dies Auswirkungen auf das CIS?);

(f) der vom IS angebotene Dienst erfordert einen hohen Zeit- oder Ressourcenaufwand oder seine Ausführung erreicht nie ein Ende;

(g) die vom IS erhaltenen Informationen werden (absichtlich oder versehentlich) manipuliert, um Schwachstellen im CIS auszunutzen;

(h) die vom CIS zum IS gesandten Informationen werden manipuliert, um Schwachstellen im IS auszunutzen;

(i) die Nutzer des IS erlangen Kenntnis davon, dass eine Transaktion (z.B. ein Informationsaustausch) stattgefunden hat;

(j) die Transaktionen (z.B. Absendung oder Empfang) werden vom IS verweigert;

(k) das CIS ist nicht in der Lage, vom IS übermittelte Informationen zu empfangen oder zu verarbeiten (z.B. weil ein Dienst nicht zur Verfügung steht);

(l) der Umfang der Informationen oder die Zahl der Anfragen, die vom IS an das CIS gesandt werden, ist größer als erwartet und bewirkt eine Vollauslastung;

(m) der Dienst für den Schutz von Systemübergängen und andere zur Herstellung der Zusammenschaltung verwendete Komponenten weisen Schwachstellen auf, die für Angriffe auf das CIS genutzt werden können;

(n) die Nutzer des IS erlangen Kenntnis von Informationen über Technologien, die Infrastruktur oder Schwachstellen in der Architektur des CIS;

(o) ein Angriff auf das IS ist erfolgreich und wird Ausgangspunkt für einen Angriff auf das CIS;

(p) die vereinbarten Protokolle über den Austausch von Informationen werden nicht eingehalten.

4. Da ein Dienst für den Schutz von Systemübergängen allein wahrscheinlich nicht in der Lage ist, ausreichenden Schutz gegen alle etwaigen Angriffe zu bieten oder solche Angriffe zu erkennen, müssen folgende Kontrollen beim Risikomanagement in Betracht gezogen werden:

   (a) die Architektur des CIS muss möglicherweise überarbeitet werden (z.B. damit ein ausreichendes mehrschichtiges Sicherheitssystem implementiert werden kann);

   (b) möglicherweise müssen die Nutzer und die Administratoren des Systems sensibilisiert und geschult werden, um ihnen die neuen Risiken bewusst zu machen und ihnen zu erläutern, welche Verantwortung ihnen im Hinblick auf die Zusammenschaltung obliegt.

_____