Rat der
Europäischen Union

Brüssel, den 6. Juli 2015
(OR. en)

10416/15

CSCI 43
CSC 162

I/A-PUNKT-VERMERK

des	Sicherheitsausschusses des Rates
für den	AStV/Rat
Betr.:	Sicherheitskonzept für die Informationssicherung bei der Sicherheitsgestaltung von Kommunikations- und Informationssystemen

1. Im Beschluss des Rates über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen[1] ist Folgendes vorgesehen: "Soweit erforderlich, billigt der Rat 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 Standards für die Sicherheitsgestaltung von Kommunikations- und Informationssystemen (CIS) festgelegt werden, nach denen EU-Verschlusssachen (EU-VS) in den CIS hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit sowie gegebenenfalls Authentizität und Nichtabstreitbarkeit zu schützen sind.

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 der Sicherheitsgestaltung von Kommunikations- und Informationssystemen

IASP 5

I 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. Dieses Konzept legt spezifische Sicherheitsgrundsätze und -maßnahmen fest, die in den Gestaltungsrahmen einer Organisation für CIS integriert werden müssen, damit gewährleistet ist, dass Sicherheitsaspekten rechtzeitig bei der Entwicklung von CIS Rechnung getragen wird.

3. Der Rat und das Generalsekretariat des Rates wenden dieses Sicherheitskonzept für den Schutz von EU-VS in ihren Räumlichkeiten und in ihren Kommunikations- und Informationssystemen 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. Die Gestaltung der Systemsicherheit (SSE) muss gewährleisten, dass der Sicherheitsstand eines CIS seinen risikobasierten Sicherheitserwartungen entspricht. Ist dies aufgrund des unerwarteten Vorhandenseins oder Fehlens von Fähigkeiten nicht der Fall, so ergeben sich potenzielle Pfade für den unerkannten Missbrauch des CIS. Dieses Konzept spezifiziert die Mindestgrundsätze und -maßnahmen für die Entwicklungsphase eines CIS (gemäß den Festlegungen des Informationssicherheitskonzepts für die Sicherheit während des Lebenszyklus von CIS[1]), um diese potenziellen Pfade auf der Grundlage eines Risikomanagements zu reduzieren.

[2] Siehe Dok. 16268/12.

7. Dieses Konzept beschreibt keinen spezifischen Rahmen für die Gestaltung der Systemsicherheit. Vielmehr muss die Organisation dieses Konzept in ihren CIS-Gestaltungsrahmen integrieren und gewährleisten, dass einschlägige Ressourcen vorhanden sind, um dessen Umsetzung zu unterstützen. In entsprechenden Leitlinien wird für jedes Sicherheitsziel ein allgemeines Mindestniveau für die Umsetzung dieser Grundsätze und Maßnahmen detailliert festgelegt.

II GESTALTUNG DER SYSTEMSICHERHEIT

Grundsätze für die Gestaltung der Systemsicherheit

8. Die Organisation muss Verfahren zur Umsetzung der nachfolgend festgelegten Grundsätze entwickeln. Jegliche Abweichungen von diesen Grundsätzen müssen in der CIS-Sicherheitsdokumentation begründet werden.
   a) Kontinuierliche Sicherheitsüberprüfung: Sicherheitsannahmen und -nachweise sind regelmäßig – so wie es die Akkreditierungsstelle für zweckmäßig erachtet – zu überprüfen;
   b) sichere Auslegung: bei der Auslegung der Architektur und der Konzeption sind bewährte Verfahren einzuhalten, wobei mindestens die Konzepte der mehrschichtigen Sicherheit, Schichtenarchitektur/Segmentierung, Minimalität und Einfachheit umgesetzt werden müssen. Die Gründe für die Wahl der Auslegung sind zu dokumentieren;
   c) Sicherheitsprodukt: das CIS muss auf anforderungsgerechten Produkten basieren, im Einklang mit dem entsprechenden Sicherheitskonzept und wie in der Unternehmenssicherheitsarchitektur (ESA) niedergelegt. Die Wahl eines Produkts, das dieser Anforderung nicht genügt, muss dokumentiert und von einer für den Betrieb zuständige Stelle für Informationssicherung begründet werden und unterliegt der Genehmigung im Rahmen des Akkreditierungsverfahrens. Die Durchführung wird mithilfe vereinbarter und aktueller Konfigurationen festgelegt und von geschultem Personal geleitet;
   d) Sicherheitstraining: das Personal, das an Gestaltungsmaßnahmen beteiligt ist, die die Sicherheit betreffen bzw. sich auf diese auswirken (z.B. Architektur, Gestaltung, Kodierung, Konfiguration, Tests, Beschaffung usw.) muss auf ein angemessenes Niveau geschult sein; diese Schulungsmaßnahmen sind zu protokollieren;

e) Sicherheitsdienste: jedes CIS muss mindestens die Sicherheitsdienste Identifizierung und Authentifizierung, Zugangskontrolle und Rechenschaftspflicht implementieren. Entsprechende Mechanismen müssen das gemäß der Aufstellung der systemspezifischen Sicherheitsanforderungen (System-specific Security Requirement Statement) geforderte Maß an Widerstandsfähigkeit und Zuverlässigkeit erfüllen;

f) Sicherheitsaufgaben: die Aufgaben der Systementwicklung und Qualitätssicherung (einschließlich Akkreditierung) dürfen nicht von denselben Akteuren durchgeführt werden;

g) Systemtrennung: es sollte zwischen Produktiv- und Testsystem unterschieden werden. Wird das Produktivsystem auch für Upgrade-Tests verwendet (z.B. Patches, neue Softwareversion usw.), so müssen in der Sicherheitsdokumentation alle Aufgaben aufgeführt sein, die auszuführen sind, um eine Beeinträchtigung der CIS-Sicherheitsziele zu verhindern.

Sicherheitskontext-Ansicht eines CIS

9. Die Sicherheit eines CIS kann gefährdet sein, lange bevor das System für den Betrieb freigegeben wird: eine unzureichende Beurteilung möglicher Schwachstellen in der Gestaltung und der künftigen Betriebsumgebungen können die Einbindung (oder das Fortbestehen) von unerwünschten Komponenten oder Funktionalitäten ermöglichen, die den Sicherheitsstand beeinträchtigen könnten.

10. Um diese möglichen Schwachstellen zu ermitteln und korrekt zu bewerten, muss die Organisation eine Sicherheitskontext-Ansicht des CIS entwickeln und auf neustem Stand halten. Die in die Unternehmenssicherheitsarchitektur integrierte Ansicht muss

a) alle während des CIS-Lebenszyklus verwendeten Ressourcen ermitteln und überwachen – sei es in Bezug auf die Technik (z.B. wiederverwendete Algorithmen, Kodierungsstandards, Tools wie Kompilierer usw.), das Personal (z.B. Fachwissen, Ermächtigung usw.), die Anlagen (z.B. Schutzniveau, Zugang usw.) oder die Verfahren (z.B. Beschaffung, Lieferkette, Korrekturen usw.);

b) das diesen Ressourcen zugewiesene Niveau der Vertrauenswürdigkeit festlegen;

c) durch geeignete Verfahren unterstützt werden, um festzulegen, wie Ressourcen eingeführt, geändert oder entfernt werden;

d) hinsichtlich der Sicherheitsannahmen und der Sicherung geprüft werden, damit gewährleistet ist, dass diese kontinuierlich mit der Risikoneigung der Organisation im Einklang stehen.

11. Bei der Entwicklung eines neuen CIS (oder neuer Komponenten eines bestehenden CIS) wird diese Ansicht verwendet, um die in der Begründungsphase entwickelte konzeptionelle Sicherheitsarchitektur mit zusätzlichen Architekturanforderungen zu ergänzen, so dass möglichen Schwachstellen und Bedrohungen entgegengewirkt wird. Auf diese zusätzlichen Anforderungen muss in der systemspezifischen Risikobewertung eingegangen werden und sie sind in der Aufstellung der systemspezifischen Sicherheitsanforderungen (SSRS) zu dokumentieren.

MASSNAHMEN FÜR DIE GESTALTUNG DER SYSTEMSICHERHEIT

12. Damit die Sicherheit ordnungsgemäß in die Systeme eingebunden wird, müssen der Rahmen der CIS-Architektur und die Projektmanagementverfahren der Organisation zumindest folgende Maßnahmen beinhalten:
    a) Auswahl von Sprachen für die Geschäfts- und Architekturmodellierung, die es gestatten, CIS-Sicherheitsprobleme darzustellen;
    b) Erstellung detaillierter Architektur-und Gestaltungsansichten unter Eingliederung von Sicherheitsdiensten und -mechanismen;
    c) Entwicklung eines Rahmens für Sicherheitsanalyseszenarien, der festlegt, wie Anforderungen und diesbezügliche Nachweise zu formulieren und zu testen sind.

13. Die Organisation muss eine Strategie für die Entwicklung von CIS (oder Komponenten davon) entweder durch interne Ressourcen oder externe Dienstleister entwickeln. Diese Strategie geht zumindest auf die Sicherheitsbelange folgender Aspekte ein:
    a) interne Fähigkeit, CIS im Einklang mit spezifischen Sicherheitszielen zu entwickeln;
    b) Kriterien zur Wahl zwischen interner oder externer Entwicklung eines CIS;
    c) Bestimmungen zur Beschaffung, damit bei der Auswahl eines Angebots gewährleistet ist, dass Sicherheitsanforderungen angemessen berücksichtigt werden;
    d) Bestimmungen, die in die Vertragsunterlagen aufzunehmen sind, um die Rechte und Pflichten der Lieferanten festzulegen.

14. Im Rahmen der Entwicklung von CIS muss die Organisation
    a) ein Archiv der dokumentierten und beherrschten Architekturen und Lösungen entwickeln, die die grundlegenden betrieblichen Erfordernisse der Organisation erfüllen;
    b) einen Katalog beherrschter Sicherheitskontrollen festlegen, die verwendet werden können, um einen Sicherheitsstand umzusetzen. Diese Kontrollen müssen von einschlägigen Verfahren dazu gestützt werden, wie die Effizienz nachgewiesen werden kann;
    c) zugelassene Umgebungen für die Entwicklung von CIS festlegen und dabei die Ressourcen (z.B. Anlagen, Software, Tools, Personal usw.) im Einzelnen aufführen, die zu verwenden sind, um die Systemintegrität und die Vertraulichkeit der Tests während seiner Entwicklung zu gewährleisten. Diese zugelassenen Umgebungen werden an die Sicherheitskontext-Ansicht des CIS angeglichen.

15. Während der Entwicklung eines Systems müssen Verfahren sicherstellen, dass
    a) jede Abweichung vom ESA-Archiv begründet werden muss, wobei die Verwendung eines neuen Produkts oder einer neuen Variante entweder durch einen Eignungsnachweis über die Sicherheitskonfiguration und den Betrieb zu belegen oder ausdrücklich durch die Sicherheitsakkreditierungsstelle zu genehmigen ist;
    b) wenn ein komplexes System zerlegt werden muss, die Sicherheitsziele der Komponenten weiterhin mit denen des Gesamtsystems im Einklang stehen;
    c) bei einer wesentlichen Entwicklung einer Architektur oder einer Gestaltung die aktualisierten Ansichten von Interessenträgern gebilligt werden, damit bestätigt ist, dass ihre Sicherheitsanliegen weiterhin angemessen berücksichtigt werden.

TESTEN DER SYSTEMSICHERHEIT

16. Die Organisation muss im Rahmen der Entwicklung des Systems progressiv durchzuführende Sicherheitstests planen. Diese durchzuführenden Tests müssen den CIS-Sicherheitsstand bei Einbau des Systems in die Betriebsanlagen garantieren und sind in den Unterlagen über den Test der CIS-Installation zu dokumentieren. Diese Unterlagen sind Teil der sicherheitsbezogenen Betriebsverfahren ("SecOPs").

17. Es müssen Sicherheitsanalyseszenarien entwickelt werden, um festzulegen, wie Sicherheitsanforderungen durch Nachweise gestützt werden können. Nachweise sollten messbar und reproduzierbar sein und auf konkreten Metriken beruhen. Diese Szenarien müssen sicherstellen, dass Widerstandsfähigkeit und Zuverlässigkeit der Sicherheitsmechanismen den Anforderungen der Aufstellung der systemspezifischen Sicherheitsanforderungen entsprechen.

18. Die Organisation muss gewährleisten, dass
    a) die Testziele, -verfahren und -instrumente mit der Sicherheitsanalyseszenario im Einklang stehen;
    b) die Tests von geschultem Personal durchgeführt werden;
    c) partielle Sicherheitstests so schnell wie möglich im Entwicklungsverfahren durchgeführt werden, damit partielle Entwicklungsentscheidungen vermieden werden, deren Folgen die CIS-Sicherheitsziele beeinträchtigen könnten;
    d) wenn Tests ausgelagert sind, sie von Verfahren gestützt werden, die eine angemessene Kontrolle der ausgeführten Tests und die Klassifizierung der Testdaten gewährleisten.

ERGEBNISSE DER ENTWICKLUNGSPHASE

19. Das für den Betrieb freigegebene System muss mindestens mit folgenden Sicherheitsunterlagen bereitgestellt werden:
    a) SSRS;
    b) SecOPs;
    c) Plänen für die Sicherheitsressourcen zur Aufrechterhaltung der Sicherheit, einschließlich detaillierter Bedingungen und der Gewährleistung der Beschaffung und ggf. der Auslagerung.