RAT DER EUROPÄISCHEN UNION

Brüssel, den 16. November 2012 (28.11)
(OR. en)

16268/12

CSCI 48
CSC 79

I/A-PUNKT-VERMERK

des	Sicherheitsausschusses des Rates
für den	AStV/Rat
Betr.:	Informationssicherheitskonzept für die Sicherheit während des Lebenszyklus von Informations- und Kommunikationssystemen (CIS)

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

2. Der Sicherheitsausschuss des Rates ist übereingekommen, ein Konzept zu empfehlen, mit dem zum Schutz von EU-Verschlusssachen (EU-VS) in Informations- und Kommunikationssystemen (CIS) hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit sowie gegebenenfalls Authentizität und Nichtabstreitbarkeit Standards für die Sicherheit während des gesamten Lebenszyklus von CIS festgelegt werden.

[1] Beschluss 2011/292/EU des Rates (ABl. L 141 vom 27.5.2011, S. 17).

3. Mit der Angabe verbindlich vorgeschriebener Tätigkeiten, die während des CIS-Lebenszyklus durchzuführen sind, zielt dieses Konzept darauf ab, dass die Partner darauf vertrauen können, dass sichere CIS unter Anwendung eines vereinbarten Verfahrens entwickelt werden, und dass angefallene Ausgaben nach den Kriterien Unternehmensbedarf und Sicherheitsvorgaben zurückverfolgt werden können.

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

absichtliche Leerseite

Informationssicherheitskonzept für die Sicherheit während des Lebenszyklus von Informations- und Kommunikationssystemen (CIS)

IASP L

INHALT

I ZWECK UND ANWENDUNGSBEREICH

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

2. Mit diesem Sicherheitskonzept für den gesamten Lebenszyklus eines Informations- und Kommunikationssystems (CIS) wird das Mindestmaß an sicherheitsbezogenen Tätigkeiten festgelegt, die während des CIS-Lebenszyklus durchzuführen sind.

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

4. Die Mitgliedstaaten sorgen nach Maßgabe ihrer innerstaatlichen Rechtsvorschriften für die Einhaltung der in diesem Sicherheitskonzept für den Schutz von EU-VS 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. Dieses Konzept betrifft nicht ein bestimmtes Modell für den Lebenszyklus von Informations- und Kommunikationssystemen, sondern legt vielmehr allgemeine Phasen eines Lebenszyklus zugrunde; im Einzelnen sind dies
   a) Phase 1: Ermittlung des Unternehmensbedarfs;
   b) Phase 2: Errichtung eines anforderungsgemäßen CIS;
   c) Phase 3: Nutzung und Instandhaltung dieses CIS;
   d) Phase 4: Außerbetriebnahme des CIS.

7. Jede Phase schließt das Mindestmaß an sicherheitsbezogenen Tätigkeiten und Leistungen ein, die das CIS-Personal in das in einer Organisation angewendete spezielle CIS-Lebenszyklusmodell und -konzept (V-Modell, Wasserfallmodell usw.) einbeziehen muss.

8. Die Aufsicht über die Durchführung dieser Tätigkeiten muss Teil jeder Strategie zur Akkreditierung von CIS sein.

9. Die in der Anlage enthaltenen Begriffsbestimmungen werden für die Zwecke dieses Konzepts verwendet.

II SYSTEMSICHERHEIT WÄHREND DES LEBENSZYKLUS

10. Um die ordnungsgemäße Einbeziehung und Aufrechterhaltung der Sicherheit zu gewährleisten, muss der CIS-Lebenszyklus die Tätigkeiten einschließen, die für die nachstehenden Phasen festgelegt sind:
    a) Phase 1: Begründung der Systemsicherheit: der Unternehmensbedarf und die Unternehmensrisiken werden bewertet, um die technologieunabhängigen Sicherheitsanforderungen für das System zu ermitteln;
    b) Phase 2: Gestaltung der Systemsicherheit: das System wird auf die Einhaltung der festgelegten Anforderungen vorbereitet, bevor es dem Eigentümer für den routinemäßigen Gebrauch im Rahmen der für die zulässige Nutzung geltenden Beschränkungen freigegeben wird;
    c) Phase 3: Aufrechterhaltung der Systemsicherheit: das System wird zulassungsgemäß betrieben; es werden verschiedene Tätigkeiten durchgeführt, um es auf einem annehmbaren Sicherheitsstand zu halten;
    d) Phase 4: sichere Außerbetriebnahme: das System wird entsprechend den zugelassenen Verfahren außer Dienst gestellt.

11. In jeder Phase werden das Mindestmaß der (nicht zwangsläufig nacheinander) durchzuführenden Tätigkeiten und die Mindestleistungen festgelegt. Es muss eine geeignete Organisationsstruktur geschaffen werden, um die entsprechenden Resssourcen zur Unterstützung dieser Tätigkeiten bereitzustellen.

12. Jede Phase endet mit einem Entscheidungspunkt, an dem die Akteure übereinstimmend feststellen, dass die Sicherheit einen guten Stand erreicht hat, und die Einleitung der nächsten Phase genehmigen.

13. Es muss eine Unternehmenssicherheitsarchitektur zur Unterstützung dieser Einbeziehung der Sicherheit in den CIS-Lebenszykus entwickelt werden, der ein Verständnis der Bedürfnisse der Organisation zugrunde liegt und die als Bezugsrahmen für die Auswahl der Sicherheitslösungen dient. Damit kann zur Optimierung der Sicherheit von CIS auf organisatorischer Ebene insgesamt beigetragen werden, anstatt dass lediglich eine lokale Optimierung auf der Ebene der Geschäftseinheiten verwirklicht wird.

14. Es können zusätzliche Konzepte oder Leitlinien ausgearbeitet werden, um entweder eine Tätigkeit in einer bestimmten Phase (beispielsweise Softwaresicherheit in der Konzipierungsphase oder kontinuierliche Überwachung in der Aufrechterhaltungsphase) zu unterstützen oder für mehr als eine Phase (wie etwa Konfigurationsverwaltung) oder für den gesamten Lebenszyklus (wie etwa Sicherheitsakkreditierung) Unterstützung zu leisten.

III PHASE 1: BEGRÜNDUNG DER SYSTEMSICHERHEIT

15. Das Hauptziel der Systemsicherheit besteht darin, die Organisationen bei der Erfüllung ihres Auftrags zu unterstützen. Im Hinblick auf ein maßgeschneidertes Sicherheitskonzept sind drei Faktoren zu berücksichtigen:
    a) der Zusammenhang, in dem das System zu errichten und zu nutzen ist;
    b) die in Bezug auf den Unternehmensbedarf zu erreichenden Ziele;
    c) die technischen Kapazitäten und die technische Reife, die für Errichtung und Betrieb des Systems erforderlich sind.

16. Es sind mindestens die folgenden Tätigkeiten auszuführen:

a) Geschäftliche Nutzer und CIS-Personal, das eine Sicherheitsschulung durchlaufen hat, müssen bei der Einrichtung des Systems den funktionellen Unternehmensbedarf des Unternehmens einschließlich des erwarteten zukünftigen Bedarfs bewerten und dabei der Art des Systems Rechnung tragen und berücksichtigen, zu welchem Zweck, von wem, wann, wo, aus welchem Grund und wie es genutzt werden soll.

b) Aus dieser Bedarfsanalyse werden unter Anwendung eines Risikomanagementkonzepts die – sowohl funktionellen als auch nichtfunktionellen – Sicherheitsanforderungen abgeleitet, wobei kontextbezogene Aspekte (Organisationskultur und -strategie, Organisationsressourcen, Sicherheitskonzepte und Rechtsvorschriften, IT- und Sicherheitsrahmenpläne, Ort der Nutzung usw.), die die künftige Lösung beeinflussen, berücksichtigt werden. Es muss eine Methode zugrunde gelegt und die Ergebnisse müssen dokumentiert werden, damit von externer Seite überprüft werden kann, wie diese Anforderungen bestimmt wurden.

c) Es müssen die Strategie und die Maßnahmen durchgeführt werden, die für die Akkreditierung erforderlich sind.

d) Es ist unter dem Aspekt der Informationsflüsse im Unternehmen und der flankierenden Sicherheitsanforderungen eine auf das CIS, das realisierbare Sicherheitsniveau und den Reifegrad der Organisation abgestimmte konzeptionelle Sicherheitsarchitektur zu erarbeiten. Jede Abweichung von der Unternehmenssicherheitsarchitektur ist zu begründen.

17. Es ist mindestens Folgendes zu dokumentieren:

a) der funktionelle Unternehmensbedarf;

b) die Beschreibung des zugrunde zu legenden Kontexts;

c) die Risikobewertung unter Konzentration auf die Risiken für das Unternehmenseigentum und die Unternehmensprozesse;

d) die konzeptionelle Sicherheitsarchitektur;

e) der erste Durchlauf der Aufstellung der systemspezifischen Sicherheitsanforderungen (System-Specific Security Requirement Statement, SSRS);

18. Die zuständigen Stellen (mindestens die Sicherheits-Akkreditierungsstelle (SAA) und die Leitung des CIS) müssen sich auf die Durchführbarkeit und Tragfähigkeit dieser Anforderungen und der Architektur einigen, bevor die nächste Phase beginnen kann.

IV PHASE 2: GESTALTUNG DER SYSTEMSICHERHEIT

19. Die konzeptionelle Sicherheitsarchitektur wird in ein reales CIS umgesetzt, wobei die Unternehmenssicherheitsarchitektur als Hauptbezugspunkt dient. Da unterschiedliche Sicherheitslösungen zu höherer Komplexität und zu höheren Kosten für Unterstützungsleistungen – insbesondere in Bezug auf Sicherheitsverwaltung und -management – führen, ist jede Abweichung von der Unternehmenssicherheitsarchitektur zu begründen. Jede Verwendung neuer Produkte oder Varianten setzt den Nachweis der entsprechenden Leistungsfähigkeit hinsichtlich der Sicherheitskonfiguration und des Sicherheitsbetriebs voraus.

20. Es sind mindestens die folgenden Tätigkeiten auszuführen:
    a) Die konzeptionelle Sicherheitsarchitektur und ihre Sicherheitsanforderungen müssen in Sicherheitsgrundsätze und -kontrollen umgesetzt werden, die unter Einsatz einer adäquaten Kombination von Menschen, Verfahren und Technologien ausgewählt und angewendet bzw. durchgeführt werden. Es müssen beherrschbare IT-Produktkonfigurationen verwendet und gegebenenfalls angepasst werden.
    b) Im Falle einer größeren konzeptionellen Weiterentwicklung müssen Vorführungen stattfinden, damit alle Akteure bestätigen können, dass ihres Erachtens alle Anliegen und Verantwortlichkeiten angemessen berücksichtigt wurden.
    c) Die Bewertung der Sicherheitsrisiken muss schrittweise verfeinert werden, um potenzielle zusätzliche Risiken erkennen zu können. Die den Entscheidungen zur Risikobewältigung zugrunde liegenden Beweggründe sind zu dokumentieren.
    d) Die zur Aufrechterhaltung der Sicherheit während des CIS-Lebenszyklus benötigten Ressourcen (Personal und Know-how, Ausrüstung und Haushaltsmittel) müssen vorausgeplant werden, einschließlich der detaillierten Bedingungen und Garantien für Beschaffung und gegebenenfalls Auslagerung.
    e) Die Sicherheitskontrollen sind entsprechend der Akkreditierungsstrategie schrittweise zu testen, um zu bewerten, ob sie durchgeführt werden und wirksam sind. Diese Tests müssen auf vereinbarten Methoden und Verfahren beruhen. Wenn für die Sicherheit die Mitwirkung der Nutzer erforderlich ist, muss bei diesen Tests auch die Akzeptanz durch die Nutzer bewertet werden.
    f) Die Sicherheitskonfiguration wird in einem Konfigurationsplan dokumentiert, der als offizielle Sicherheitsbezugsgrundlage dient.
    g) In Einsatzplänen wird festgehalten, wie die Sicherheitskontrollen angewendet und gesteuert werden sollen und wie der aktuelle Sicherheitsstand geschützt und aufrechterhalten werden kann.

21. Es ist mindestens Folgendes zu dokumentieren:
    a) die Aufstellung der systemspezifischen Sicherheitsanforderungen (SSRS)
    b) die Sicherheitsbetriebsverfahren einschließlich aller einschlägigen Einsatzpläne;
    c) die Sicherheitstestpläne zur Bewertung des Sicherheitsstands und der Tätigkeiten in Notfällen;
    d) die Planung für die Sicherheitsressourcen (Haushaltsmittel, Verträge usw.).

22. Die SAA muss die Übereinstimmung des vorgeschlagenen CIS mit dem Sicherheitskontext bestätigen, bevor das CIS akkrediert und für den routinemäßigen Betrieb und die Aufrechterhaltung seines Sicherheitsstands förmlich freigegeben werden kann.

V PHASE 3: AUFRECHTERHALTUNG DER SYSTEMSICHERHEIT

23. Während des routinemäßigen Betriebs können sich im CIS vorgenommene Handlungen auf seine Sicherheit auswirken. Die Handlungen müssen im Einklang mit den Sicherheitsbetriebsverfahren vorgenommen werden, damit die Sicherheit der Akkreditierung entspricht. Abweichungen von den zugelassenen Handlungen müssen entdeckt und gegebenenfalls gemeldet werden.

24. Es sind mindestens die folgenden Tätigkeiten auszuführen:
    a) Die Sicherheitsverwaltung muss im Einklang mit den Einsatzplänen erfolgen.
    b) Die Aufrechterhaltung der Sicherheitskonfiguration muss im Einklang mit dem Konfigurationsplan erfolgen. Genehmigte Änderungen und Verbesserungen müssen zu einer Aktualisierung des Konfigurationsplans führen, während Änderungen von erheblicher Tragweite dem CIS und den Aufsichtsstellen zur weiteren (Neu-)Begutachtung vorgelegt werden müssen.
    c) Es müssen regelmäßig Risikomanagementtätigkeiten und Überprüfungen der Einhaltung der Vorgaben durchgeführt werden, um sicherzustellen, dass die Sicherheitskontrollen immer noch wirksam sind und die Lücke zwischen der Sicherheitsausgangslage und dem tatsächlichen Sicherheitsstand immer noch hinnehmbar ist.
    d) Das System ist kontinuierlich hinsichtlich seiner Leistungsfähigkeit in Bezug auf die Sicherheit und der von den einzelnen Einheiten (Benutzer, Prozesse usw.) vorgenommenen Handlungen zu überwachen, damit unerwartete Tätigkeiten entdeckt werden können und auf böswillige Handlungen im Einklang mit den Notfallplänen reagiert werden kann.

25. Es sind mindestens Angaben zu den folgenden Punkten regelmäßig vorzulegen, auch wenn keine Änderung zu melden ist:
    a) böswillige Handlungen;
    b) Verfügbarkeit der für die Sicherheit bestimmten Ressourcen;
    c) Aktualisierungen des Konfigurationsplans.

26. Die SAA muss regelmäßig den Sicherheitsstand des CIS bewerten und bestätigen, dass er seinem Sicherheitskontext und den Sicherheitsanforderungen entspricht.

27. Die zuständigen Stellen können gegebenenfalls die vollständige oder teilweise Außerbetriebnahme des CIS gestatten, wenn sie sich sicher sind, dass sich dies nicht auf den Sicherheitsstand des Systems auswirkt.

VI PHASE 4: SICHERE AUSSERBETRIEBNAHME VON SYSTEMEN

28. Bei Außerbetriebnahme des Systems werden spezifische Tätigkeiten durchgeführt, um sicherzustellen, dass die Sicherheit nicht beeinträchtigt wird.

29. Es sind mindestens die folgenden Tätigkeiten auszuführen:
    a) Die Informationen und die Systemkomponenten sind entsprechend ihrer künftigen Nutzung (Archivierung, Weitergabe, Vernichtung usw.) zu behandeln.
    b) Die Ressourcen sind gegebenenfalls freizugeben.
    c) Die letzte Konfiguration des CIS muss aufgezeichnet und zusammen mit dem Konfigurationsplan archiviert werden.

30. Es müssen mindestens unterzeichnete Bescheinigungen über den Abschluss der Tätigkeiten zur Außerbetriebnahme vorgelegt werden.

31. Die SAA müssen sich vergewissern, dass die Tätigkeiten zur Außerbetriebnahme im Einklang mit den Sicherheitskonzepten durchgeführt wurden, bevor die Sicherheitsaspekte des CIS-Lebenszyklus abgeschlossen werden.

ANLAGE

BEGRIFFSBESTIMMUNGEN

Architektur	Die Grundstruktur eines Systems, die durch seine Komponenten, deren Beziehungen untereinander und zur Umgebung und durch die seine Konzipierung und Entwicklung bestimmenden Grundsätze verkörpert wird.
Konzeptionelle Sicherheitsarchitektur	Anordnung der einzelnen Komponenten und Durchsetzungspunkte der Sicherheitsdienste und ihre Beziehungen zu den zu schützenden Informationen, ohne Bezugnahme auf einzelne Konstruktionsmerkmale.
Unternehmensarchitektur	Die in sich stimmige Gesamtheit der Grundsätze, Methoden und Modelle, die bei der Konzipierung und Verwirklichung der Organisationsstruktur, der Geschäftsprozesse, der Informationssysteme und der Infrastruktur eines Unternehmens zum Tragen kommen.
Unternehmenssicherheitsarchitektur	Sicherheitsaspekt der Unternehmensarchitektur einschließlich sowohl der Steuerung der Sicherheitsprozesse als auch des technischen Konzepts für die Informationssicherheit.
Lebenszyklus	Entwicklung eines Systems, Produkts, Dienstes, Projekts oder einer anderen von Menschen künstlich geschaffenen Einheit von der Konzipierungsphase bis zur Außerbetriebnahme.
Lebenszyklusmodell	In Phasen einteilbarer Rahmen für die mit dem Lebenszyklus zusammenhängenden Prozesse und Tätigkeiten, der auch als gemeinsamer Bezugsrahmen für Kommunikation und Verständigung dient.