RAT DER EUROPÄISCHEN UNION

Brüssel, den 30. März 2012 (12.04)
(OR. en)

8408/12

CSCI 11
CSC 20

I/A-PUNKT-VERMERK

des	Sicherheitsausschusses des Rates
für den	AStV/Rat
Betr.:	Sicherheitskonzept für die Netzwerkverteidigung im Rahmen der Informationssicherung

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 Standards für die Netzwerkverteidigung zum Schutz von EU-Verschlusssachen (EU-VS) in den Informations- und Kommunikationssystemen (CIS) 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 2011/292/EU des Rates (ABl. L 141 vom 27.5.2011, S. 17).

absichtliche Leerseite

Sicherheitskonzept für die Netzwerkverteidigung im Rahmen der Informationssicherung

IASP 4

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. Dieses Konzept legt Mindeststandards fest, die zum Zweck der Netzwerkverteidigung in Bezug auf Informations- und Kommunikationssysteme (CIS) und deren Vernetzungen zu beachten 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 Informations- und Kommunikationssystemen 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. Unter Netzwerkverteidigung[2] ist ein koordiniertes Bündel von Maßnahmen, Verfahren und Tätigkeiten zu verstehen, mit dem

   a) die Widerstandsfähigkeit von CIS gegen Cyberangriffe verstärkt wird;
   b) eine frühzeitige Erkennung von Cyberbedrohungen und Schwachstellen von CIS ermöglicht wird;

[2] Die Begriffe Netzwerkverteidigung und Cyberverteidigung sind im Prinzip austauschbar, jedoch bezieht sich Cyberverteidigung in der Regel nur auf Angriffe von außen, während Netzwerkverteidigung sich üblicherweise sowohl auf interne als auch auf externe Angriffe bezieht.

c) die frühzeitige Erkennung von Angriffen und die rasche Reaktion darauf ermöglicht wird, um den Schaden für die CIS zu minimieren;

d) die Bewertung der tatsächlichen Tragweite von Verletzungen der Sicherheitsvorschriften ermöglicht wird.

7. Maßnahmen der Netzwerkverteidigung sind notwendig aufgrund der zunehmenden Komplexität und gegenseitigen Abhängigkeit von CIS, der weit verbreiteten Verfügbarkeit eines leistungsstarken Instrumentariums für Cyberangriffe, der zunehmenden Rolle von kriminellen Organisationen und Nachrichtendiensten mit Zugang zu umfangreichen Ressourcen sowie der immer häufigeren grenzüberschreitenden, gezielten und technisch ausgefeilten Angriffe auf CIS.

II. DAS KONZEPT

8. Maßnahmen der Netzwerkverteidigung sind für jedes CIS durchzuführen. Die Maßnahmen müssen sich auf den laufenden Risikomanagementprozess und die Strategie für die Sicherheitsakkreditierung jedes CIS stützen und darin integriert werden.

9. Die Maßnahmen der Netzwerkverteidigung werden regelmäßig überprüft, um sicherzustellen, dass sie ausreichend und dem bestehenden Bedrohungsszenario angepasst sind. Sie werden ferner überprüft, wenn eine Änderung des Bedrohungsszenarios für das betreffende CIS eintritt, sowie nach einem Vorfall, der Auswirkungen auf die Sicherheit der durch das betreffende CIS bearbeiteten Informationen hat.

10. Im Hinblick auf die Netzwerkverteidigung werden für jedes CIS folgende Maßnahmen getroffen:

a) Das CIS wird unter Einsatz der technisch verfügbaren integrierten Überwachungsfunktionen eingerichtet, wobei die rechtlichen Verpflichtungen und Anforderungen in Bezug auf die Sammlung und Speicherung personenbezogener oder sensibler Überwachungsdaten zu beachten sind;

b) auf der Grundlage eines Risikomanagementkonzepts und des Werts der durch das CIS bearbeiteten Informationen wird eine Rangfolge des Umfangs und der Ausführlichkeit der Meldung der von den obengenannten Überwachungsfunktionen erfassten Ereignisse festgelegt; gestützt auf diese Analyse werden Warnmeldungen von unterschiedlicher Dringlichkeit und Bedeutung generiert;

c) Informationen, die im Rahmen der Routineüberwachung sowie im Zuge von Ermittlungen zu Vorfällen erhoben werden, müssen gesichert und in einer Weise bearbeitet werden, die ihre spätere Verwendung in internen oder strafrechtlichen Verfahren gegen identifizierte Urheber von Sicherheitsvorfällen ermöglicht;

d) die CIS-Nutzer aller Ebenen werden geschult, damit sie die mit dem jeweiligen CIS verbundenen Sicherheitsrisiken verstehen und wissen, was zu tun ist, wenn sie ein unerwartetes oder anomales Verhalten feststellen.

11. Die Sicherheitsstelle ist letztlich für das korrekte Funktionieren und die Durchführung der Maßnahmen der Netzwerkverteidigung verantwortlich.

12. Zur Unterstützung der Tätigkeiten zur Netzwerkverteidigung wird Folgendes bereitgestellt:

a) ausreichendes Personal mit einschlägigen Fachkenntnissen, die im Rahmen der Erstausbildung und ständiger beruflicher Weiterbildung erworben wurden;

b) Prozesse und Verfahren für den Aufbau und die Erhaltung der Sicherheit der CIS und ihrer Widerstandsfähigkeit gegen Störungen oder Angriffe;

c) Instrumente zur Feststellung und Meldung von Störungen der CIS und zur Einleitung von Echtzeitmaßnahmen zur Beendigung oder Eindämmung der Störung;

d) Prozesse für den Umgang mit Ereignissen, bei denen es sich um CIS-Sicherheitsvorfälle handeln könnte;

e) Prozesse für die Benachrichtigung von betroffenen Parteien und anderen Partnern über Sicherheitsereignisse;

f) Verwaltungsunterstützung und Überprüfung.

13. Mit den Maßnahmen der Netzwerkverteidigung soll Folgendes sichergestellt werden:

a) Gewährleistung der Sicherheit:
   i) Konzeption und Entwicklung im Hinblick auf den Aufbau von CIS, die in der Lage sind, unbeabsichtigte und/oder böswillige Vorfälle festzustellen, abzuwehren und zu überstehen, wobei mittels Systemhärtung die Angriffsfläche verringert und ein tief gehender Schutz bereitgestellt wird;
   ii) Bereitstellung technischer Schutzmaßnahmen wie
      - Zugangskontrolle durch das Minimalitätsprinzip und das Prinzip der minimalen Zugriffsrechte sowie durch Logging und Protokollierung aller erfolgreichen und nicht erfolgreichen Zugriffe;
      - Erkennen und Verhindern von unberechtigtem Eindringen, sowohl für ein- als auch für ausgehende Daten an den internen und externen Schnittstellen der CIS;
   iii) Sensibilisierung und funktionelle Schulung der Nutzer für die sichere Nutzung der CIS sowie für die Feststellung und Meldung von ungewöhnlichem Verhalten;

b) Sicherheitspflege:
   i) Anlagen-, Konfigurations- und Änderungsmanagement, vorzugsweise mit Aufzeichnung der genauen Konfiguration sämtlicher Komponenten der CIS in jeder Phase ihres Lebenszyklus;
   ii) Erfassung, Mapping und Überwachung der Netzwerke, um mindestens Folgendes zu erkennen:
      - unerlaubte Änderungen;
      - erfolgreiche oder nicht erfolgreiche Versuche eines unerlaubten Zugriffs;
      - Schwachstellen von Komponenten der CIS in Bezug auf bekannte Angriffsmethoden und
      - unerwartetes oder ungewöhnliches Systemverhalten;
   iii) Verwaltung der Schwachstellenmeldung[3] und zeitnahe Abhilfemaßnahmen gegen bekannte Schwachstellen von CIS-Komponenten;

[3] Spezielle Meldedienste der Komponentenanbieter sollten verwendet werden, wenn dies erforderlich und durch die Sicherheitsstufe der CIS gerechtfertigt ist, um frühzeitige Meldungen zu erhalten.

c) Wiederherstellung der Sicherheit:

i) Prozesse zur Reaktion auf Vorfälle;

ii) Prozesse zur Untersuchung und Nachbearbeitung von Vorfällen;

iii) Notfall-, Kontinuitäts- und Rückgewinnungsprozesse;

iv) Prozesse zur Sicherstellung der Dokumentation einschlägiger Informationen über Sicherheitsvorfälle;

v) Kommunikationsverfahren für den Informationsaustausch mit internen und externen CIS-Nutzern, mit den CIS-Verwaltern und – sofern erforderlich – mit der Öffentlichkeit;

d) Engagement, Einbeziehung und Folgemaßnahmen der Verwalter.

14. Maßnahmen der Netzwerkverteidigung für ein CIS umfassen gesicherte Mechanismen für den zeitnahen Informationsaustausch mit künftigen institutionellen Computer-Notfallteams (CERT) und gegebenenfalls mit vertrauenswürdigen internen und externen Partnern, z.B. staatlichen CERT. Die Partner sollten sich gleichermaßen verpflichten, Informationen über ihre eigenen Ereignisse und Gegenmaßnahmen im Bereich der Netzwerkverteidigung bereitzustellen.

15. Informationen über CIS-spezifische Maßnahmen sollten als RESTREINT UE/EU RESTRICTED eingestuft werden; sie können aber auch in einen höheren Geheimhaltungsgrad eingestuft werden, wenn das betreffende CIS hierfür akkreditiert ist.