CERT - Standard

A - Rahmenbedingungen

Aus dem Umsetzungsplan zur Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung entspringt der Auftrag, zur gemeinsamen Abwehr von IT-Angriffen einen gemeinsamen und verbindlichen Mindeststandard „CERT“ zu entwickeln. Die AG-Informationssicherheit des IT-Planungsrats erarbeitet entsprechend dieses Auftrags diesen Standard, der die personellen, technischen, infrastrukturellen und organisatorischen Anforderungen an ein Verwaltungs-CERT mit definierten Kompetenzen und CERT-Diensten beschreibt.

Die Verfügbarkeit der elektronischen Dienste der öffentlichen Verwaltung für Bürgerinnen und Bürger sowie Unternehmen sowie die Sicherheit der dort gespeicherten Daten sind eine zentrale und gemeinsame Herausforderung für Staat und Gesellschaft im nationalen und internationalen Kontext. Der Blick darf aber nicht nur auf die einzelne Behörde fokussiert bleiben. Die Bedrohungen machen in vernetzten Infrastrukturen vor einzelnen Einrichtungen nicht halt. Aus diesem Grund ist ein einheitliches Informationssicherheitsniveau für alle Behörden dieser vernetzten Infrastrukturen anzustreben und durch deren Mitglieder in bzw. mit Unterstützung der jeweiligen CERTs umzusetzen.

Alle Länder haben bereits CERTs und CERT-ähnliche Strukturen (im Folgenden „CERTs“) aufgebaut. Ebenso konnte mit dem Aufbau des Verwaltungs-CERT-Verbundes (VCV) eine föderale, verwaltungsinterne Informationsaustauschplattform der CERTs der öffentlichen Verwaltung zur Verbesserung des Informationsaustausches der bestehenden CERTs des Bundes und der Länder etabliert werden. Nicht alle CERTs sind jedoch ausreichend aufgestellt, um neben Information, Warnung, Alarmierung sowie Vorfallsbearbeitung auch als Mittler zwischen allen zu beteiligenden Stellen zu wirken. Neben dem Fluss notwendiger Informationen ist auch die Koordinierung der sich daraus ergebenden Aktionen und deren Kontrolle sicherzustellen. Durch gezielte Dienstangebote der CERTs, z. B. durch die Bereitstellung kritischer Informationen über zu treffende Abwehrmaßnahmen bei neuen Schwachstellen oder Angriffen, können Vorfälle oder deren Ausbreitung besser verhindert werden. Wenn Sicherheitsvorfälle nicht verhindert werden können, stehen Experten für die Reaktion und Vorfallsbewältigung bereit.

Die in diesem Standard vorgenommenen Festlegungen sind für Bund und Länder verbindlich. Sie werden vom IT-Planungsrat beschlossen und durch die Mitglieder planvoll umgesetzt.

B - Ziele

Die Probleme mangelnder Sicherheit von Informationstechnik in der Verwaltung sind sehr komplex. Die Forderung in Politik und Gesellschaft nach Digitalisierung des Verwaltungshandelns lässt den Durchdringungsgrad der Verwaltungsprozesse mit IT und damit das Risiko für die Aufrechterhaltung der Verwaltungstätigkeit in diesem Bereich steigen. Ebenso bestehen durch die intensive Vernetzung von Behörden und Verwaltungsebenen Gefahren, die eine definierte Organisationsstruktur zur Aufrechterhaltung der Arbeits- und Handlungsfähigkeit der Verwaltung fordern.

Zur operativen Zusammenarbeit und zur besseren Koordinierung von Schutz- und Abwehrmaßnahmen gegen IT-Sicherheitsvorfälle zwischen dem Bund und den Ländern wurde der Verwaltungs-CERT-Verbund gegründet.

Damit diese Zusammenarbeit funktioniert und ein einheitliches Sicherheitsniveau erreicht wird, ist darauf zu achten, dass ein CERT im Verbund die gleichen Aufgaben wahrnimmt und erfüllen kann.

Die Umsetzung der Mindeststandards (Priorität 1 bis 3) soll bis Ende 2022 in den CERTs oder unter Mitwirkung der CERTs erfolgen. Die Umsetzung ist mit den Prioritäten 1 und 2 zu beginnen.

C - Umsetzung

Zur Standardisierung der CERT-Leistungen wurde ein Dienstleistungskatalog entwickelt. Dieser gibt, nach Prioritäten abgestuft, die von den CERTs in Prio 1 direkt und ab Prio 2 ggf. auch unter Mitwirkung bzw. Steuerung durch das CERT zu erbringenden Dienstleistungen wieder.

Priorisierung der Aufgaben:

- Priorität 1: Muss erfüllt sein
- Priorität 2: Muss erfüllt werden, wenn Prioritäten erster Ordnung erfüllt sind
- Priorität 3: Muss erfüllt werden, wenn Prioritäten erster und zweiter Ordnung erfüllt sind
- Priorität 4: Keine Pflichtaufgaben, können erfüllt werden

<u>Priorität 1</u>

a) Vorfallsmanagement (Incident Response Coordination)
b) Betrieb eines Warn- und Informationsdienstes/qualifizierte Weitergabe von Informationen zu Sicherheitslücken und Warnungen (Announcements)
c) Kooperation mit anderen CERTs, dem eigenen ISMS und mit Sicherheitsbehörden

Priorität 2

a) Organisation von Dienstleistungen und Prozessgestaltung (kontinuierlicher Verbesserungsprozess - KVP)
b) Vorbeugende Maßnahmen zur Vermeidung von Vorfällen
c) Information innerhalb des eigenen ISMS im Hinblick auf Vermeidung, Reaktion auf und die Koordinierung bei Vorfällen
d) Einbindung und Koordinierung externer Dienstleister bzw. MIRT des BSI (Incident Response Coordination) bei einem Vorfall
e) Erstellung von Lagebildern
f) Kennzahlenerstellung/Erstellung von Management Summarys (ggf. in Zusammenarbeit mit SOC)
g) Erweitertes Berichtswesen (Zusammenfassung von spezifischen Informationen für einen begrenzten Empfängerkreis)
h) Zentrale Kontaktstelle (nach intern und extern) als Stabsbereich bei Krisen
i) Schwachstellenmanagement (Vulnerability Analysis)
j) allgemeine Securityberatung und -unterstützung für ISB (keine produktspezifische Lösungsberatung)
k) Sicherheitsvorfallanalyse/Forensik (Forensic Analysis)

Priorität 3

a) Erfassung von Bedrohungen (Risikoanalyse - Threat Intelligence)
b) Monitoring/Nutzung von Securitytools und deren Pflege
c) Nutzung von IDS/SIEM

Priorität 4

a) Penetrationstests (Begleitung/Empfehlung)
b) Audits/Revisionen (Begleitung von internen und externen Audits und Revisionen sowie Revision/Audit eigener Untersuchungsgegenstände - Security Audit)
c) Technologiebewertung und Produktbewertung (ggf. auch Produktüberprüfungen - Technology Watch/Product Evaluation)
d) Schulung/Bewusstseinsstärkung der Mitarbeiter der eigenen Landesverwaltung (Mitarbeit/Unterstützung - Awareness Building)
e) Betrieb CERT-eigener Technik
f) KRITIS-Kontaktstelle

Weiterführend sind folgende Aufgaben als Basisaufgaben durch das CERT wahrzunehmen:

a) Management externer Beziehungen (z. B. Zusammenarbeit im VCV)

b) Personalorganisation CERT (eigenorganisierte Personalzuweisung und Festlegung von Verantwortlichkeiten)
c) Entwicklung CERT (Mitarbeit bei strategischer Ausrichtung)

D - Anforderungen

Die CERTs sind für die Wahrnehmung ihrer Aufgaben mit den erforderlichen technischen Werkzeugen und mit ausreichenden Personalkapazitäten auszustatten. Im Rahmen der Etablierung der CERTs sind die Grundsätze zu Entscheidungskompetenzen und -wegen festzulegen. Grundsätzlich kann auch die Delegation einzelner Aufgaben an externe Dienstleister wirtschaftlich sinnvoll oder fachlich notwendig sein. Hierfür sind entsprechende vertragliche Bindungen vorzunehmen. Die Entscheidungskompetenzen sind jedoch in jedem Fall von staatlichen Stellen auszuüben.

Sofern einzelne der oben genannten Aufgaben nicht vom betreffenden CERT wahrgenommen werden, sondern von anderen Stellen der Landesverwaltung, sind die jeweiligen Zuständigkeiten zu regeln und zu dokumentieren.