Beschluss 1/2016
71. Sitzung des AK ITEG am 12. Januar 2016

Der AK ITEG nimmt die Beschlüsse Nr. 07/2015 „Änderung GO“ und Nr. 08/2015 „Sicherheitsmeldungen“ der AG IS zur Kenntnis. Die Ressorts werden gebeten, das auf der Internetseite www.cert.sachsen.de bereitgestellte CERT-Meldeformular für Sicherheitsvorfälle umfassend zu nutzen.

Arbeitsgruppe Informationssicherheit

Beschluss Nr. 08/2015 vom 17. November 2015 – Sicherheitsmeldungen

Die AG IS sieht die zentrale Erfassung wesentlicher Sicherheitsvorfälle innerhalb der Landesverwaltung als wichtige Grundlage vor allem für ein realistisches Lagebild zur Informationssicherheit im Freistaat Sachsen als auch für die effektive und frühzeitige Warnung sowie Unterstützung bei ressortübergreifenden Sicherheitsvorfällen.

Der Aufbau dieses ressortübergreifenden Meldeverfahrens soll in mehreren Stufen erfolgen. Ziele sollen dabei ein möglichst geringer Meldeaufwand durch die automatisierte Einbindung vorhandener Vorfallbearbeitungssysteme und Prozesse in den Ressorts sowie eine möglichst hohe Verbindlichkeit durch die Erarbeitung einer entsprechenden Meldeverordnung durch die AG IS sein.

In einem ersten Schritt soll bereits der Verdacht auf mindestens folgende Ereignisse in den Ressorts und den nachgeordneten Geschäftsbereichen unverzüglich gemeldet werden:

a. Schadwirkung durch ein Schadprogramm,
b. Einbruch in ein System oder Netzwerk,
c. nicht autorisierte Veränderung einer Internetseite,
d. schwerwiegende oder erfolgreiche Überlastungsangriffe auf eine Internetseite,
e. nachgewiesene Abflüsse / Verluste personenbezogener oder vertraulicher Daten,
f. schwerwiegende, über normale Wiederherstellungszeiten hinausgehende ungeplante Ausfälle von bedeutsamen IT-Verfahren.

Sofern in den Ressorts bereits eigene Regeln zum Umgang mit Sicherheitsvorfällen bestehen, sind diese Grundlage für die Meldungen an das CERT. Die Meldung soll mit Hilfe des über die Internetseite des CERT Sachsen bereitzustellenden Meldeformulars an das CERT erfolgen. Verantwortlich für den Meldeprozess ist der BfIS des jeweiligen Ressorts.

Soweit notwendig wird das CERT kurzfristige, anonymisierte Warnmeldungen an die Mitglieder der AG IS verteilen und gemäß den vorhandenen Möglichkeiten unterstützen. Zusätzlich werden alle gemeldeten Vorfälle durch das CERT monatlich anonymisiert zusammengefasst und in Form eines Berichts im Rahmen der AG IS-Sitzung vorgestellt.