Nachprüfung der Umsetzung der Netzwerk Security Policy der Schweizerischen Informatikkonferenz durch die Kantone
Bundesamt für Informatik und Telekommunikation

Das Wesentliche in Kürze

Die Eidgenössische Finanzkontrolle (EFK) hatte im Jahr 2009 geprüft, wie weit in den Kantonen die von der Schweizerischen Informatikkonferenz (SIK) vorgegebene Network Security Policy (NSP) umgesetzt worden war[1]. Aufgrund der Resultate wurde dem Bundesamt für Informatik und Telekommunikation (BIT) eine Empfehlung abgegeben, welche nach Ansicht der EFK bisher nicht umgesetzt ist. Die Verträge zwischen dem BIT und den Kantonen sollten mit Sicherheitselementen ergänzt werden. Zudem sollten die Kantone verpflichtet werden, Nachweise über die Umsetzung der vereinbarten Sicherheitsanforderungen in ihren Netzwerken zu erbringen. Wenn sie diesen Vereinbarungen nicht nachkommen, so hätte das BIT oder von ihm beauftragte Dritte entsprechende Sicherheitsaudits durchzuführen.

Das BIT hat diese Empfehlung so weit möglich in den *Service Level Agreement* (SLA) mit den Kantonen umgesetzt. Es sieht sich jedoch weder in der Lage noch in der Pflicht bei den Kantonen Prüfungen in sicherheitsrelevanten Bereichen durchzuführen. Dazu fehlen im föderalistischen System der Schweiz die Rechtsgrundlagen, welche einem Bundesamt das Recht geben würden, in die Hoheit der Kantone einzugreifen oder umgekehrt. Die EFK wird daher die noch offene Empfehlung als erledigt ablegen.

Jede Partei muss ihre Netze selber vor Bedrohungen schützen

Seit dem Bericht der EFK haben sich die Bedrohungslage und das daraus resultierende Risikopotenzial verschärft. Früher herrschte die Tendenz, sich innerhalb von Netzstrukturen gegenseitig zu vertrauen. Heute steht im Vordergrund, dass die sensitiven Daten der Verwaltungseinheiten sehr gezielt geschützt werden müssen. Daher werden nicht nur die Aussengrenzen eines Netzwerkes mit möglichst hohen Barrieren versehen, es wird auch innerhalb desselben der Datenverkehr laufend überwacht.

Das zwischen den Kantonsnetzwerken und dem Bundesnetzwerk liegende Transportnetz (KOMBV-KTV) gilt aus Bundessicht als Fremdnetz. Die Kantone haben über dieses Netz eine hoch verfügbare und leistungsfähige Verbindung, um auf Bundesanwendungen im Rahmen ihrer gesetzlichen Aufgaben zugreifen zu können. Für den Zugriff braucht es als erste Sicherheitshürde eine Zwei-Faktoren-Authentifikation. Aufgrund des damit verbundenen personifizierten Profils werden als zweites Sicherheitselement nur die Zugriffsrechte auf Anwendungen freigeschaltet, die diese Person auch haben darf. Die Vertraulichkeit der übertragenen Daten wird durch Verschlüsselung gewährleistet.

Die Umsetzung von Netzwerksicherheit ist Kantonshoheit

Die Sicherheit der Kantonsnetzwerke müsste aufgrund eigener Interessen zum Schutz ihrer Daten auf ähnlichem Niveau wie beim Bund gehandhabt werden. Nebst der NSP-SIK bestehen weitere

[1] „Prüfung der Umsetzung der Netzwerk Security Policy der Schweiz. Informatikkonferenz (NSP-SIK) durch die Kantone“, 8421, 2009

Grundlagen bzw. Vorgaben, die es jedem Kanton ermöglichen, die minimalen Sicherheitsvorkehrungen treffen zu können. In verschiedenen Gremien der SIK findet zudem eine Zusammenarbeit zwischen Bundes- und Kantonsvertretern statt, immer mit dem Ziel eines einheitlichen Vorgehens. Es fehlt jedoch eine übergeordnete Instanz, welche die Umsetzung von verbindlichen Vorgaben regelmässig kontrolliert bzw. diese auch durchsetzen kann. Diesen Anforderungen soll bei der Überarbeitung der NSP-SIK mehr Beachtung geschenkt werden, was die EFK begrüsst.