FAQ zum Sicherheitskonzept für Kopfstellen

Fragestellung	Antwort
Muss bei einer ISO-27001- bzw. BSI-IT-Grundschutz Zertifizierung ein Sicherheitskonzept vorgelegt werden?	Ja, es muss in jedem Fall ein Sicherheitskonzept inkl. Netzplan vorgelegt werden. Wenn sich die ISO-27001- bzw. BSI-IT-Grundschutz Zertifizierung auf den Informationsverbund der Kopfstelle beziehen, kann jedoch bei einzelnen Punkten z. B. Räumliche Sicherheit, Patchmanagement und Fernzugriffe im Sicherheitskonzept auf die Zertifizierung verwiesen werden. Die Zertifizierung muss ebenfalls vorgelegt werden.
Muss bei einer ISIS12-Zertifizierung ein Sicherheitskonzept vorgelegt werden?	ISIS12 ist eine "Vorstufe" (weniger Maßnahmen, keine Risikoanalyse, …) zu einem ISMS nach IT-Grundschutz des BSI, ISIS12 bietet keine vergleichbares Sicherheitsniveau zu einer ISO 27001 oder BSI IT-Grundschutz-Zertifizierung. Es ein vollständiges Sicherheitskonzept inkl. Netzplan vorzulegen.
Warum müssen das Gerät und der Nutzer protokolliert werden?	Durch die Protokollierung sollen sicherheitsrelevante Ereignisse erkannt und angemessen darauf reagiert werden können. Ohne die notwendigen Protokollierungsdaten, lassen sich Sicherheitsvorfälle nicht mehr angemessen detektieren. Um nachvollziehen zu können, welche Geräte/Systeme an einem sicherheitsrelevanten Ereignis beteilig sind/waren, müssen diese identifizierbar sein.
Wann müssen die Vorgaben für Fernzugriffe nachgewiesen werden?	Wenn Fernzugriffe aus bzw. über ein anderes/externes Netz z. B. das Internet erfolgen, müssen die Vorgaben des Moduls „Sicherer Fernzugriff auf lokale Netze“ eingehalten und die Umsetzung beschrieben werden. Wenn ausschließlich die eigenen Mitarbeiter der IT-Abteilung ausschließlich innerhalb des eigenen Netzes Remote zugreifen, müssen die Anforderung nicht nachgewiesen werden.
Müssen der Anwendungsserver und das TLS-Gateway in einer DMZ platziert werden?	Die Komponenten, mit denen die Kommunikation mit dem KBA realisiert wird, sind in der DMZ zu platzieren. Je nach Architektur und genutztem Fachverfahren/Verfahrensanbieter/n können das nur der Anwendungsserver, nur das TLS-Gateway oder der Anwendungsserver und das TLS-Gateway sein.
Werden auch Alternativ- oder Ersatzmaßnahmen zugelassen?	Wenn durch andere Maßnahmen mindestens ein vergleichbares oder höheres Sicherheitsniveau sichergestellt ist, kann von den Vorgaben abgewichen werden. Dies ist aber stichhaltig zu begründen und die Maßnahmen sind detailliert im Sicherheitskonzept zu beschreiben. Das KBA entscheidet, ob die Alternativ-/ Ersatzmaßnahmen anerkannt werden.

Könne die Zertifikate auch an Dienstleister einer Behörde verschickt werden?	Nein, Zertifikate dürfen nur an die behördeneigene De-Mail-Adresse verschickt werden, die beim Antrag angeben und geprüft wurde.
Gibt es Alternativen zu OpenFT?	Alle Produkte, die mit openFT kommunizieren können, können eingesetzt werden. Eine Alternative kann das Produkt Log-FT von Logics sein.
Wann sind die neuen Passwortempfehlungen des BSI umzusetzen?	Die neuen Passwortempfehlungen des BSI wurden mit der Version Juli 2020 der Verpflichtungserklärung umgesetzt.
Wir auch ein geteiltes Sicherheitskonzept akzeptiert?	Das KBA bietet an, dass Dienstleister dem KBA ein Sicherheitskonzept (keine Verpflichtungserklärung) für den von Ihm verantworteten Bereich zur Prüfung vorlegen. Nach erfolgreicher Prüfung kann die zugreifende Stelle das Sicherheitskonzept des Dienstleiters beifügen und an den entsprechenden Stellen im Ihrem Sicherheitskonzept auf das des Dienstleisters verweisen.
Ist eine geteilte Verpflichtungserklärung zulässig?	Die Zugreifende Stelle, also der Nutzer der Webservices des KBA, ist für die Einhaltung der Vorgaben der "Information zur netztechnischen Anbindung an das Kraftfahrt-Bundesamt für Behörden" bzw. der Verpflichtungserklärung verantwortlich. Wenn dieser einen Dienstleiter für die Erfüllung einzelner Anforderung beauftragt, liegt die Verantwortung für die Einhaltung der Vorgaben weiterhin bei der zugreifenden Stelle und nicht beim Dienstleister. Die zugreifende Stelle erhält auch das für den Zugriff erforderlich Zertifikat, nicht der Dienstleister. Es ist daher Aufgabe der zugreifenden Stelle sicherzustellen, dass der Dienstleister die Vorgaben einhält. Eine geteilte Verpflichtungserklärung kann daher nicht akzeptiert werden.