Prüfung der Integration der Informatik Gotthard-Basistunnel in die SBB
Bundesamt für Verkehr

## Das Wesentliche in Kürze

Die Eidgenössische Finanzkontrolle (EFK) untersuchte die Wirksamkeit des Vorgehens zur Gewährleistung eines angemessenen IT-Sicherheitsniveaus der Tunnel-Betriebsautomation – unter Ausklammerung der Bahnleittechnik. Zudem betrachtete die EFK das methodische Vorgehen zur Durchführung der Risikoanalyse Gotthard-Basistunnel (GBT) / Ceneri-Basistunnel (CBT) sowie die konsistente Ableitung eines Massnahmenkatalogs und dessen Umsetzung. Die Kosten für die Bereitstellung der Tunnel-Leittechnik beliefen sich auf circa 50 Millionen Franken.

**Die Identifikation und die Minimierung der Risiken waren zielführend, erfolgten jedoch zu spät**

Am 1. Juni 2016 übergab die Erstellerin AlpTransit Gotthard AG (ATG) den GTB an die Betreiberin SBB. Aus Sicht der IT-Sicherheit waren zu diesem Zeitpunkt noch nicht alle notwendigen Massnahmen umgesetzt. Diese sollen entsprechend den ICT-Sicherheitsvorgaben der SBB fertiggestellt werden. Sorgfältig durchgeführte Analysearbeiten der SBB zeigen auf, dass zum Zeitpunkt der Betriebsaufnahme aufgrund der vorhandenen Schwachstellen keine Risiken der Einstufung „ROT“ – d. h. kurz- und mittelfristig untragbar – zu verzeichnen sind. Zudem sind die Risiken aus Sicht der ICT-Security auf den Bereich der Verfügbarkeit des Tunnels beschränkt. Auch hinsichtlich der Betriebssicherheit, etwa Unfallrisiken mit Personenschäden, hat die Analyse keine relevanten Gefährdungen festgestellt.

Während der Bauphase stellte die SBB fest, dass keine übergeordnete Sicherheitskonzeption für ICT-Security bestand. Sie erarbeitete daraufhin in Eigenregie die noch fehlende Sicherheitskonzeption „Teilkonzept (TK) übergeordnete ICT-Security GBT/CBT“. Darauf basierend untersuchte die SBB, mit Unterstützung der ATG, ob die Sicherheitsanforderungen mit der damals vertraglich vorgesehenen Umsetzung des Infrastrukturaufbaus erfüllt würden. In der Folge wurden die dabei festgestellten Schwachstellen durch die SBB aufgrund ihrer Risiken gewichtet. Es war kein Risiko der Stufe „ROT“ zu verzeichnen. ATG und die SBB verfassten einen Plan mit 42 Verbesserungsmassnahmen zur Behebung dieser Schwachstellen. Daraus entstand der Projektänderungsantrag „ICT-Security GBT“ vom 20. Mai 2014, worin die Umsetzung der Massnahmen abgedeckt war. Vor der Eröffnung des GBT überprüfte die SBB den Stand dieser Massnahmen und legte dar, dass erst 12 umgesetzt und von den verbleibenden 30 4 zurückgestellt worden waren. Im Rahmen des Anlage-Übergangs per 1. Juni 2016 sind gemäss ATG weitere Massnahmen umgesetzt worden. Diese sind zum Zeitpunkt der Berichterstellung hinsichtlich ihrer Wirkung noch nicht verifiziert.

**Das Bundesamt für Verkehr ist als Aufsichtsbehörde zu stärken**

Die EFK stellt fest, dass die ICT-Security-Risiken erst spät im Projekt systematisch behandelt wurden. Sie erkennt, dass die Risikoanalyse methodisch in sachgemässer Weise durchgeführt und dokumentiert ist, konstatiert aber, dass die ATG den Fortschritt der Verbesserungsmassnahmen anders beurteilt als die SBB und dass unterschiedliche Beurteilungsgrundlagen seitens der SBB und ATG angewandt werden. Aus Sicht der EFK bestehen dadurch ein Risiko zusätzlicher Kosten wie auch eine Quelle für Verzögerungen. Folglich empfiehlt sie dem Bundesamt für Verkehr (BAV), die Umsetzung der noch offenen Empfehlungen überwachen zu lassen. Ausserdem empfiehlt sie dem BAV, sowohl für den CBT als auch für weitere grosse Bahnbauprojekte mit unterschiedlichem Ersteller

und Betreiber eine Rolle beim Ersteller einzufordern, welche die ICT-Security über alle Phasen des Projektes übergreifend verantwortet und als Schnittstelle zu einer gleichartig gelagerten Rolle beim Betreiber dient. Eine solche Rolle sollte ebenso bei Vorhaben in einer Projektorganisation eingefordert werden, bei denen der Ersteller und der Betreiber die gleiche Gesellschaft sind. Sinngemäss sollte sie dann die Schnittstelle zwischen der Projekt- und der Betriebsorganisation bilden.