FACHBEREICH
SICHERHEIT – SCHUTZ
UND ZUVERLÄSSIGKEIT

Berlin, 17. Februar 2023

Stellungnahme

des Fachbereichs Sicherheit – Schutz und Zuverlässigkeit – der Gesellschaft für Informatik e.V.

zur Anhörung gemäß § 8a Abs. 5 BSIG zu den grundsätzlichen Anforderungen im Nachweis-verfahren (GAiN)

des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Ansprechpartner und Autor:
Bernhard C. Witt, Sprecher des GI-Fachbereichs „SICHERHEIT“ und zugleich selbst Prüfteamleiter nach § 8a Abs. 3 BSIG, bcwitt@it-sec.de

Einleitung

Mit Schriftsatz vom 27. Januar 2023 hat das Bundesamt für Sicherheit in der Informationstechnik insbesondere Vertreter der betroffenen Betreiber und der betroffenen Wirtschaftsverbände nach § 8a Abs. 5 BSIG dazu aufgerufen, Stellungnahmen zum Entwurf Anforderungen nach § 8a Abs. 5 BSIG – Grundsätzliche Anforderungen im Nachweisverfahren (GAiN) mit Stand vom 23.01.2023 per Mail an kritis-buero@bsi.bund.de einzureichen. Darin enthaltende Angaben werden ggf. im Zuge einer beabsichtigten Synopse im Internet veröffentlicht, einschließlich der dazugehörigen Nennung der Institution des Stellungnehmenden.
Der Fachbereich Sicherheit – Schutz und Zuverlässigkeit – der Gesellschaft für Informatik e.V. nimmt diese Gelegenheit gerne wahr und nimmt unter Einbeziehung von Beiträgen aus seiner Fachgruppe Management von Informationssicherheit zu dem vorgelegten Entwurf wie folgt Stellung und willigt hiermit ausdrücklich ein, dass diese Stellungnahme vollständig bzw. auszugsweise als auch die darin enthaltenen personenbezogenen Kontaktdaten des Sprechers im Internet vom BSI veröffentlicht werden dürfen.

Zu D.4A.01, D.4A.02 und D.PE.04

Gemäß Entwurf der GAiN müssen im 4-Augen-Prinzip die Prüfung des Vorgehens des Betreibers zu Risikoanalyse und Risikobehandlung vorgenommen werden (D.4A.01). Die Mitglieder des Prüfteams müssen insbesondere zu diesem Zweck unabhängig voneinander hinreichend qualifiziert sein, um den zu prüfenden Sachverhalt zu beurteilen (D.4A.02).
Wenn folglich mindestens zwei beteiligte Prüfer unabhängig voneinander nachweislich dazu qualifiziert sein müssen, KRITIS-Betreiber-spezifische Risikoanalysen und Risikobehandlungen eigenständig und unabhängig voneinander zu beurteilen, setzt dies faktisch Kenntnisse als Fachexperte im betroffenen Sektor voraus, da die üblicherweise zum Einsatz kommenden Methoden höchst sektorspezifisch in der Praxis angelegt sind. Darüber hinaus gibt es derzeit nahezu keine fachspezifische Ausbildung zum Risikomanagement (unbeachtlich der allgemeinen Personalzertifizierungen als CRISC oder als Risk Manager). Auf dem Markt als auch innerhalb interner Revisionen lassen sich derzeit nicht genügend Prüfer mit einer solchen Qualifikation finden.
Faktisch schränkt damit diese Anforderung die Zusammenstellung des Prüfteams unangemessen ein, zwingt darüber hinaus den KRITIS-Betreiber, seine Beschreibung zur Festlegung der angewandten Risikoanalyse und Risikobehandlung i.d.R. vorab dem Prüfteam zur Verfügung zu stellen, erhöht merklich zu tragende Prüfungskosten ohne erkennbaren Mehrwert und erschwert zudem das Prüfhandeln, da die Mitglieder des Prüfteams demnach unabhängig voneinander entsprechende Bewertungen ihrer unmittelbaren Sachverhaltsprüfung abgeben sollen.

Es wird daher empfohlen, Ziffer 3 aus D.4A.01 ersatzlos rauszustreichen und „unabhängig voneiner“ in Ziffer 1 aus D.4A.02 durch „insgesamt im Prüfteam“ zu ersetzen.

Gerade die Ziffern 2 (Erstellen der Beurteilung voneinander unabhängig) und 5 (gleichwertige Grundlage für das Prüfergebnis) aus D.4A.02 sind in diesem Zusammenhang ein praxisuntauglicher Overhead (und daraus resultierend unnötig zusätzliche Prüfungskosten) ohne nennenswerten Nutzen und steht überdies im Einzelfall auch gegen die Widerspruchsfreiheits-Anforderung aus D.PE.04, falls die beteiligten Prüfer hier zu einem unterschiedlichen Ergebnis kommen.

Es wird daher empfohlen, den Halbsatz „insbesondere erstellen sie ihre Beurteilungen auch voneinander unabhängig“ in Ziffer 2 aus D.4A.02 sowie Ziffer 5 aus D.4A.02 ersatzlos rauszustreichen.

In der Praxis ist im Übrigen die Vorgehensweise zur Risikoanalyse und Risikobehandlung tatsächlich gar nicht ausschlaggebend für eine ausreichende Absicherung der kritischen Dienstleistung, sondern deren tatsächliche Umsetzung und Anwendung.
Dies wiederum kann dagegen i.d.R. nur im Rahmen der Vor-Ort-Prüfung bzw. im Rahmen einer zugehörigen Videokonferenz einzelfallbezogen überprüft werden!
Gerade ausgehend von den Erfahrungen, die im Zuge der Pandemie gemacht wurden, ist nicht nachvollziehbar, warum nunmehr in D.4A.01, Ziffer 5 ausschließlich von einer Vor-Ort-Prüfung die Rede ist. Gerade in diesem Zusammenhang macht es faktisch keinen Unterschied, ob vor Ort auf einen entsprechenden Datensatz geblickt wird oder via Webkonferenz. Anders verhält es sich dagegen hinsichtlich der physischen Sicherheit. Generell fehlt damit in den Anforderungen zum 4-Augen-Prinzip daher die durchaus eingeschränkte Möglichkeit einer Remote-Prüfung, ergänzend zur Vor-Ort-Prüfung.

Es wird daher empfohlen, in Ziffer 5 aus D.4A.01 „Vor-Ort-Prüfung“ zu ersetzen durch „Prüfung vor Ort bzw. via Videokonferenz“.

Zu N.BN.01 und N.BN.11
Gemäß Entwurf der GAiN sind bei der Nachweiserbringung alle Dokumente und Unterlagen unter Einsatz der vom BSI zur Verfügung gestellten Formulare und Vorlagen im vorgegebenen Dateiformat zu verwenden; eine abweichende Einreichung bedarf der schriftlichen Zustimmung des BSI (N.BN.01).
Es ist jedoch schlicht nicht sinnvoll, dass entweder durch das BSI für jedes sinnvoll einsetzbare Dateiformat ein Muster bereitgestellt wird, damit entsprechende Inhalte strukturell in der gewünschten Abfolge dargestellt werden, oder dass der Einsatz von Textverarbeitungssystemen auf diesem Weg ausdrücklich festgeschrieben wird. Dies ist eine untaugliche und unpraktische Vorgabe! Hier ist besser zu unterscheiden zwischen den Formularen, die selbstverständlich vollumfänglich zu verwenden sind, wie dies für Verwaltungsverfahren soweit durchaus üblich ist, wohingegen bei den Vorlagen faktisch nur die generelle Struktur, sprich zugehörige Parameter des Inhalts, vorgeschrieben werden sollten, da in der Praxis die Formatvorgaben z.B. je nach verwendeter Prüfgrundlage und weiteren Sektorspezifika schlicht untauglich sind, um noch lesbare Prüfberichte und Mängellisten erstellen zu können. In der Praxis ist daher die faktische Abweichung beim Dateiformat sogar überwiegend notwendig, um z.B. Manipulationen von Ergebnissen vorbeugen zu können, und schwerlich ein Ausnahmefall, der auch

noch einer ausdrücklichen Genehmigung bedarf. Ein solches Prozedere wird daher sogar als Verschwendung öffentlicher Mittel angesehen!

Es wird daher empfohlen, „Vorlagen im vorgegebenen Dateiformat“ in N.BN.01 rauszustreichen und nach „verwenden“ folgenden Halbsatz anzufügen: „und Vorgaben über darzustellenden Inhalt aus Vorlagen zu berücksichtigen“.

Gemäß Entwurf der GAiN sind im Prüfplan bei Zusatzprüfungen vollständige Verweise auf zugehörige Auditberichte aufzunehmen (N.BN.11).
Sektorspezifisch kann dies erhebliche Probleme aufwerfen, da entsprechende Auditberichte vorgeschriebener Prüfstellen entweder dem Betreiber gar nicht vorliegen, da nur abweichende Feststellungen darin ausgewiesen sind, oder aber ein entsprechendes Mapping führt zu unverhältnismäßiger Ausweitung im Prüfplan.

Es wird daher empfohlen, den letzten Satz in N.BN.11 ersatzlos rauszustreichen.

Über den Fachbereich Sicherheit – Schutz und Zuverlässigkeit – der Gesellschaft für Informatik e.V.

Der GI-Fachbereich "Sicherheit -Schutz und Zuverlässigkeit" wurde im Februar 2002 gegründet und vernetzt zwei "Communities" miteinander: Während die „Safety-Community“ vor allem den Schutz der Umwelt vor IT-Systemen (beispielsweise Sicherheit des Menschen vor schwerwiegenden Systemfehlern in Flugzeugen, Kernreaktoren und Kraftwerken) sowie Fehlertoleranzmaßnahmen (z.B. Systemausfälle als Folge von Ermüdungserscheinungen, Softwarefehlern und Naturereignissen) im Blick hat, beschäftigt sich die „Security-Community“ hauptsächlich mit dem Schutz der IT-Systeme und ihrer Umgebung vor Bedrohungen von außen, insbesondere vor Gefahren, die von bösartigen Angriffen (durch Menschen) ausgehen. Der Fachbereich bietet ein Forum, in dem alle auf dem Gebiet der Sicherheit informationstechnischer Systeme arbeitenden Menschen ihr Fachthema, organisiert in Fachgruppen, wiederfinden. Neben der rein wissenschaftlichen Arbeit ermöglicht der Fachbereich einen fachlichen Austausch zwischen Wissenschaft und Praxis. Mehr Information über den Fachbereich Sicherheit der GI kann der Webseite https://fb-sicherheit.gi.de/ entnommen werden.

Über die Gesellschaft für Informatik e.V.

Die Gesellschaft für Informatik e.V. (GI) ist mit rund 20.000 persönlichen und 250 korporativen Mitgliedern die größte und wichtigste Fachgesellschaft für Informatik im deutschsprachigen Raum und vertritt seit 1969 die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Wirtschaft, öffentlicher Verwaltung, Gesellschaft und Politik. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Weitere Informationen finden Sie unter www.gi.de.