Bundesamt
für Sicherheit in der
Informationstechnik

Konzeptpapier:

Remote-Prüfungen in der Corona-Pandemie

Stand: 30.11.2020

TLP:Green (Organisationsübergreifende Weitergabe)

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: poststelle@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Zweck dieses Dokuments

Das vorliegende Dokument richtet sich an Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber), die gemäß § 8a Absatz 1 BSIG ihre Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind, gegenüber dem BSI auf geeignete Weise nachweisen müssen. Weitere Adressaten sind prüfende Stellen, die von den KRITIS-Betreibern beauftragt werden, die Nachweisprüfungen durchzuführen.

Fester Bestandteil einer solchen Prüfung nach § 8a Absatz 1 BSIG sind Prüfungshandlungen, die die prüfende Stelle beim Betreiber vor Ort vornimmt. Nur so ist sichergestellt, dass die Prüfer die o.g. Vorkehrungen vollständig und umfassend betrachten und beurteilen können. Auf eine Vor-Ort Prüfung kann daher grundsätzlich nicht verzichtet werden.

Aufgrund der derzeitigen Beschränkungen können ausnahmsweise einzelne Prüfungshandlungen jedoch durch Remote-Prüfungshandlungen ersetzt werden. Voraussetzung dafür ist u.a. eine Risikobewertung sowie ergänzende Dokumentation.

Allerdings bleibt die Substitution von Prüfungshandlungen vor Ort durch Remote-Prüfungshandlungen die Ausnahme. Betreiber sind daher gehalten den prüfenden Stellen Zugang zu den Anlagen der von ihnen betriebenen Kritischen Infrastrukturen zu gewähren.

Sollte es einer prüfenden Stelle nicht möglich sein, eine Nachweis-Prüfung vollumfänglich durchzuführen, ist dies als Mangel im Prüfbericht zu vermerken.

Neben der von einem Betreiber beauftragten prüfenden Stelle hat auch das BSI die Möglichkeit, selbst oder durch Dritte, die Einhaltung der Anforderungen nach § 8a Absatz 1 BSIG bei einem KRITIS-Betreiber vor Ort zu überprüfen (siehe § 8a Absatz 4 BSIG).

2 Zulässigkeit von Remote-Prüfungen im Rahmen der Nachweiserbringung

Aus Sicht des BSI stellt die Durchführung einer Vor-Ort-Prüfung bei Betreibern Kritischer Infrastrukturen ein notwendiges Maß an Qualität sicher, damit ein Prüfer mit ausreichender Sicherheit die Absicherung gemäß § 8a Absatz 1 BSIG bestätigen kann. Die Durchführung einer Remote-Prüfung an Stelle einer Vor-Ort-Prüfung bei Betreibern Kritischer Infrastrukturen stellt daher grundsätzlich einen Prüfmangel dar. Aufgrund der Covid-19-Pandemie 2020 möchte das BSI den Betreibern Kritischer Infrastrukturen jedoch flexiblere Möglichkeiten für die Nachweiserbringung gem. § 8a Absatz 3 BSIG bieten, ohne dass die Pandemieschutzmaßnahmen der Betreiber beeinträchtigt werden. Grundsätzlich stellen Remote-Prüfungen eine vorübergehende, situationsbedingte Ausnahme dar.

Voraussetzung für die Zulässigkeit von Remote-Prüfungen:

- Wenn zum Zeitpunkt eines Vor-Ort-Termins für Prüfer und für die geprüfte Stelle keine Indikatoren für eine erhöhte Infektionsgefahr durch das Coronavirus bestehen, dann ist eine Prüfung unter Einhaltung der Hygieneregeln zumutbar. Indikatoren für eine erhöhte Infektionsgefahr sind:
    - Die Prüfer stammen aus einer Region mit erhöhtem Infektionsaufkommen (>35 Fälle pro 100.000 Einwohner gem. RKI 7-Tage-Mittel)
    - Die geprüfte Stelle befindet sich in einer Region mit erhöhtem Infektionsaufkommen
- Da sich die Infektionslage dynamisch fortentwickelt, rät das BSI, Prüfungen als Vor-Ort-Termine vorzubereiten, aber die Möglichkeit einer Lageverschärfung direkt mit zu berücksichtigen; z.B. durch Vorhalten der notwendigen Infrastruktur für Remote-Prüfungshandlungen oder durch Vereinbarungen von möglichen Ersatzterminen.

Sollte ein Betreiber eine Vor-Ort-Prüfung kategorisch ausschließen, so ist dies vom Prüfer zu dokumentieren. Der Betreiber muss eine ausführliche Begründung für den kategorischen Ausschluss liefern und dies muss als schwerwiegender Prüfmangel in der Sicherheitsmängelliste (gem. § 8a Absatz 3 Satz 3 BSIG) des Nachweises festgehalten werden.

3 Durchführung

3.1 Risikobewertung vor der Durchführung einer Remote-Prüfung

Teile einer Vor-Ort Prüfung können durch Remote-Prüfungshandlungen durchgeführt werden. Dafür muss der Prüfer zunächst betrachten, welche Risiken möglicher Fehleinschätzungen aufgrund einer Remote-Prüfung entstehen können. Es muss dabei differenziert bewertet werden, welche Risiken die jeweilige Remote-Prüfungshandlung in Bezug auf den Prüfgegenstand mit sich bringt und dies den potentiellen Gesundheitsrisiken gegenüberstellen. Über die Vorab-Bewertung soll entschieden werden, ob eine Vor-Ort-Prüfung weiterhin erforderlich bleibt oder die Risiken für Fehleinschätzungen gering genug sind, um auf eine Remote-Prüfung zurückzugreifen.

Nachfolgend einige beispielhafte Bewertungen von Prüfungshandlungen:

1. Die zu prüfende Institution ist ein mittelständisches Unternehmen mit weniger als 1000 Mitarbeitern, betreibt nur einen Standort und eine überschaubare, weitestgehend standardisierte IT-Infrastruktur. Es ist vorgesehen, ein Interview durchzuführen. Der Personenkreis der für das Interview benötigten Personen beschränkt sich dabei auf die IT-Leitung, die Informationssicherheitsbeauftragte sowie einen fachlichen Prozesseigener.

   Aufgrund der überschaubaren Teilnehmerzahl könnte das Risiko einer möglichen Fehleinschätzung durch computergestützte Remote-Interviews als **geringes Risiko** eingestuft werden.

2. Um die Situation vor Ort ausreichend einschätzen zu können, muss der Prüfer Logdateien auf dem Bildschirm eines im Serverraum aufgestellten Servers einsehen können.
   Um dies remote abbilden zu können, muss der Bildschirm abgefilmt und das Video live an den Prüfer übertragen werden. Durch bauliche Begebenheiten der Liegenschaft ist die Übertragung des Videos per (Mobil-)funknetz jedoch qualitativ stark eingeschränkt und alternative Optionen sind nicht mit vertretbarem Aufwand umsetzbar.

   Das Risiko einer möglichen Fehleinschätzung könnte durch den Prüfer als **mittleres bis hohes Risiko** eingestuft werden.

Aus Sicht des BSI sind Prüfungshandlungen im Rahmen einer Vor-Ort-Prüfung immer dann erforderlich, wenn die Maßnahmen der Remote-Prüfung mit einem zu großen Risiko für Fehleinschätzungen verbunden sind und der Prüfer sich vorab sicher ist, dass er sich kein ausreichendes Bild von der Lage vor Ort machen kann.

Dokumentationspflicht des Prüfers und des Betreibers:
Ist aufgrund der aktuellen Infektionslage keine Vor-Ort-Prüfung durchführbar und muss sich der Prüfer zunächst auf eine Remote-Prüfung beschränken, dann muss er das Risiko der Fehleinschätzung für das BSI nachvollziehbar dokumentieren. Diese Risikobewertung des Prüfers ist dem BSI im Rahmen der Nachweiserbringung durch den Betreiber vorzulegen.

3.2 Durchführung einer Remote-Prüfung

Vorbereitung:
Um die Qualität der Durchführung einer Remote-Prüfung dem BSI nachvollziehbar darzustellen, muss der Prüfer die folgenden Informationen gegenüberstellen und dokumentieren:

- die normalerweise geplanten Vor-Ort-Prüfungshandlungen und
- die daraus abgeleiteten Remote-(Ersatz-)Prüfungshandlungen

Hinweis: Die Darstellung kann in Form einer Mapping-Tabelle erfolgen.

Sollte eine Remote (Ersatz)-Prüfungshandlung in einem konkreten Einzelfall nicht anwendbar, bzw. keine geeignete Remote (Ersatz)-Prüfungshandlung möglich sein, dann deklariert der Prüfer die fehlende Prüfungshandlung als schwerwiegenden Prüfmangel und erläutert die Nicht-Anwendbarkeit. Der Prüfmangel und dessen Erläuterung müssen in die Sicherheitsmängelliste (gem. § 8a Absatz 3 Satz 3 BSIG) des Nachweises aufgenommen werden.

Hinweis:
Prüfmängel sind eigenständige Mängel, die unabhängig von den inhaltlichen Mängeln in die Mängelliste aufgenommen werden. Sie sollen in erster Linie darstellen, welches Fehleinschätzungsrisiko des Prüfers aufgrund der Remote (Ersatz)-Prüfungshandlungen entstanden ist.

Dokumentationspflicht des Prüfers und des Betreibers:
Nach der Durchführung der Remote-Prüfung muss der Prüfer anhand des tatsächlichen Ablaufs und der Qualität der erhaltenen Ergebnisse abschließend bewerten, wie gut sich die Remote-Prüfung eignete, um die Absicherung gem. §8a Absatz 1 BSIG zu beurteilen. Sollten nur Teile oder einzelne Prüfhandlungen remote erfolgt sein, dann müssen diese Teile bewertet werden.

Nachfolgend einige Beispiele zur Bewertung der Remote Prüfung:

> ***geringfügiger Prüfmangel***
> *„Die Prüfungshandlung „XYZ“ wurde durch die Remote-Prüfungshandlungen „ABC“ ersetzt. Die Remote-Prüfungshandlung war geeignet. Der Prüfer sieht es durch die gewonnenen Erkenntnisse als erwiesen an, dass der Prüfgegenstand den Anforderungen an die Absicherung der Kritischen Infrastruktur §8a Absatz 1 BSIG entspricht. - **Begründung** -“*
>
> ***schwerwiegender Prüfmangel***
> *„Aufgrund der fehlenden Prüfungshandlung „XYZ“ kann trotz Ausschöpfung aller verbliebenen Remote-Prüfungshandlungen keine belastbare Aussage über die Absicherung der Kritischen Infrastruktur gem. §8a Absatz 1 BSIG getroffen werden. - **Begründung** -“*

Nach der Nachweiseinreichung des Betreibers bewertet das BSI aufgrund der darin dokumentierten Risikobewertungen, ob die Einstufung der einzelnen Prüfmängel plausibel ist. Die Betreiber sind aufgefordert, dem BSI zusammen mit der Aufstellung der Prüfmängel einen Plan zur Behebung der Prüfmängel zu übermitteln.

3.3 Umgang des BSI mit schwerwiegenden Prüfmängeln

Nach der Einreichung der Nachweisunterlagen werden diese durch das BSI überprüft. Das BSI behält sich vor, Prüfmängel im Zuge der Mängelbeseitigung u.a. durch folgende individuelle Handlungsoptionen abstellen zu lassen:

- Auf Grundlage der eingereichten Dokumentation beurteilt das BSI, ob weitere Vor-Ort-Prüfungshandlungen oder aufwändigere Remote-Prüfungshandlungen zumutbar und notwendig sind.

- Beispiele für aufwändigere Remote-Prüfungshandlungen:

    - Vor-Ort-Prüfung mit spezifischem Hygienekonzept zur Inaugenscheinnahme bestimmter Räume
    - Prüfung mit Drohnentechnik
    - Prüfung mit Remote-Kamera (Kameraführung durch Mitarbeiter des Betreibers)
    - Prüfung mit Remote-Kamera (Kameraführung durch unabhängige Dritte)
    - Remote geführte Alleinprüfung des Prüfers

Anmerkung:
Die Wahl der Handlungsoptionen hängen im Einzelfall vom jeweiligen Prüfmangel ab. Daher sind die hier aufgeführten Beispiele nicht abschließend.

Anhang A: Formelle Anforderungen an Remote-Prüfung

Nachfolgend sind einige anerkannte Standards und formelle Anforderungen an Remote-Prüfungen aufgeführt. Betreiber Kritischer Infrastrukturen und Prüfer sollten diese Standards im Rahmen der Nachweisführung berücksichtigen.

Die DIN EN ISO 19011 - Leitfaden zum Prüfen von Managementsystemen sieht die folgenden Kategorien vor:

- **Vollständig remote:**
  Die Prüfung findet vollständig, d.h. von der Planung bis zur Verifizierung der Prüfungsfolgemaßnahmen, ohne physische Anwesenheit des Prüfers vor Ort, statt.

- **Teilweise remote:**
  Die Prüfer sind zeitweise physisch am Prüfungsort anwesend und prüfen bestimmte Umfänge mittels Remote-Prüfungshandlungen;

- **Folgemaßnahmen remote:**
  Die Verifizierung von Prüfungsfolgemaßnahmen oder eine Nach-Prüfung findet mittels Remote-Prüfung statt.

Ergänzend zur ISO 19011 existieren unter anderen folgende Normen zur Orientierung:

- **DIN EN ISO/IEC 17021:2015**
  Diese Norm enthält die Anforderungen an Zertifizierungsstellen, die Managementsysteme zum Zwecke der Konformitätsbewertung auditieren und zertifizieren.

- **71 SD 6 016 (IAF MD 4)**
  Verbindliches Dokument zur Verwendung computergestützter Auditverfahren (CAAT) bei der Auditierung von Managementsystemen durch akkreditierte Zertifizierer.

IAF MD 4 bezieht sich im Wesentlichen auf die folgenden computergestützten Prüfverfahren:

- **Durchführung von Telefonkonferenzen;**
- **Sitzungen im Internet;**
- **Interaktive webbasierte Kommunikation;**
- **Elektronischer Fernzugriff auf die Dokumentation des Managementsystems (MS) und/oder auf die MS-Prozesse**