

## Joachim Lindenberg

---

**Von:** [REDACTED]  
**Gesendet:** Thursday, 24 June 2021 15:11  
**An:** Joachim Lindenberg  
**Betreff:** AW: Ihre Anfrage nach dem Informationsfreiheitsgesetz

Sehr geehrter Herr Lindenberg,

vielen Dank für Ihre Anmerkungen und Eindrücke. Wir werden Ihre Vorschläge sehr intensiv prüfen. Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen  
Im Auftrag für das IT-Grundschutz-Team

[REDACTED]

---

Referat SZ 13 - BSI Standards und IT Grundschutz Bundesamt für Sicherheit in der Informationstechnik Godesberger Allee 185-189  
53175 Bonn

Telefon: +49 228 99 9582- [REDACTED]  
Fax: +49 228 99 10 9582 [REDACTED]  
E-Mail: [REDACTED]

Internet:  
[www.bsi.bund.de](http://www.bsi.bund.de)

#DeutschlandDigitalSicherBSI

-----Ursprüngliche Nachricht-----

Von: Joachim Lindenberg <[REDACTED]>  
Gesendet: Mittwoch, 23. Juni 2021 17:35  
An: [REDACTED]  
Betreff: AW: Ihre Anfrage nach dem Informationsfreiheitsgesetz

Sehr geehrte [REDACTED],

ich habe noch keinen Audit durch das BSI erlebt, aber einige Audits in der Privatwirtschaft. In der Regel ist der Zeitaufwand den der Auditor investieren kann sehr begrenzt. Also fängt er normalerweise damit an, zu prüfen, ob alle erwarteten Dokumente vollständig vorhanden sind. Danach nimmt er sich einige der Dokumente vor und prüft ob etwas sinnvolles darin steht. Dann sieht er sich stichprobenartig an, ob das auch umgesetzt wurde. Eine vollständige Prüfung ist in der Regel nicht möglich, und selbst bei Abweichungen wird oft ein Zertifikat ausgestellt und im - in der Regel nicht veröffentlichten - Audit-Bericht eine Empfehlung ausgesprochen, was zu verbessern ist. Wann und ob die umgesetzt wird - oft erst kurz bevor der Auditor wiederkommt. Ob die Granularität von IT-Komponenten für Authentifizierungszwecke geeignet ist - ich kann mir nicht vorstellen, dass das tatsächlich regelmäßig beanstandet wird, zumal der Auditor mangels Interpretationshilfe vom BSI gar nicht sicher behaupten kann, dass er mit einer vom Autor der Dokumente abweichenden Meinung Recht hat. Alle mir bekannten Modellierungsinstrumente (insbesondere auch UML) erlauben hierarchische Komponenten, also kann der Autor beim Modellieren seiner Landschaft die Granularität mehr oder weniger willkürlich wählen. Genau das ist bei einem Kunden von mir passiert - er hat die Komponenten einfach größer gewählt als andere Kollegen oder ich das tun würde. Meine Anspielung auf Murphy hatte durchaus einen realen Anlass, und ich wüsste wirklich nicht, was Ihren Optimismus rechtfertigt, gleiches würde in der öffentlichen Hand nicht passieren.

Ihnen ist hoffentlich auch bewusst, dass ich die Kommunikation - nach Schwärzung aller Namen - ganz oder teilweise auf fragdenstaat.de veröffentlichen werden? Aber viel lieber würde ich sehen, dass Sie eine geeignete Definition oder Modellierungshilfe veröffentlichen.

Vielen Dank und viele Grüße

Joachim Lindenberg

-----Ursprüngliche Nachricht-----

Von: [REDACTED]

Gesendet: Wednesday, 23 June 2021 15:14

An: Joachim Lindenberg <[REDACTED]>

Betreff: AW: Ihre Anfrage nach dem Informationsfreiheitsgesetz

Sehr geehrter Herr Lindenberg,

vielen Dank für Ihre Email.

Wie sie sicherlich den BSI-Standards entnommen haben, müssen bei der Umsetzung des IT-Grundschutzes die Anforderungen mit geeigneten Maßnahmen hinterlegt werden. Diese konkreten Maßnahmen werden vor der Erteilung eines IT-Grundschutz-Zertifikats durch einen vom BSI zertifizierten Auditor überprüft. So ist sichergestellt, dass keine Erwartungen unterlaufen werden. Ihre Einschätzung, dass die Daten der öffentlichen Hand nicht ausreichend geschützt sind, können wir daher nicht teilen.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen

Im Auftrag für das IT-Grundschutz-Team

[REDACTED]

---

Referat SZ 13 - BSI Standards und IT Grundschutz Bundesamt für Sicherheit in der Informationstechnik Godesberger Allee 185-189  
53175 Bonn

Telefon: +49 228 99 9582-[REDACTED]

Fax: +49 228 99 10 9582-[REDACTED]

E-Mail: [REDACTED]@bsi.bund.de

Internet:

www.bsi.bund.de

#DeutschlandDigitalSicherBSI

-----Ursprüngliche Nachricht-----

Von: Joachim Lindenberg <[REDACTED]>

Gesendet: Dienstag, 22. Juni 2021 15:33

An: [REDACTED] <[REDACTED]@bsi.bund.de>

Betreff: AW: Ihre Anfrage nach dem Informationsfreiheitsgesetz

Sehr geehrte [REDACTED],

Ihnen ist schon bewusst, dass dieser Interpretationsspielraum Organisationen die Möglichkeit gibt, die Erwartungen zu unterlaufen und damit die Sicherheit der Verarbeitung zu gefährden. Und zu Ihren Kunden zählen insbesondere auch alle öffentlichen Einrichtungen. D.h. ich muss davon ausgehen, dass Daten in öffentlichen Händen nicht ausreichend geschützt sind. Murphy ist Ihnen sicher ein Begriff?

Mit freundlichen Grüßen  
Joachim Lindenberg

-----Ursprüngliche Nachricht-----

Von: [REDACTED] <[REDACTED]@bsi.bund.de>  
Gesendet: Tuesday, 22 June 2021 15:15  
An: Joachim Lindenberg <[REDACTED]>  
Betreff: AW: Ihre Anfrage nach dem Informationsfreiheitsgesetz

Sehr geehrter Herr Lindenberg,

vielen Dank für Ihre Anfrage und Ihr damit verbundenes Interesse am IT-Grundschutz.

Das IT-Grundschutz-Kompodium und die darin enthaltenen Bausteine beleuchten zu verschiedenen Themen relevante Sicherheitsaspekte, die beim Aufbau eines ISMS nach IT-Grundschutz zu beachten sind. Das IT-Grundschutz-Kompodium ist dabei bewusst allgemein gehalten, um den Anwendern bei der Umsetzung der Vorgehensweisen nach den BSI-Standards entsprechende Freiheiten zu geben. Die konkrete Ausgestaltung der einzelnen Anforderungen ist dabei jeweils von der Situation im betrachteten Informationsverbund abhängig.

Im konkreten Fall sehen sie dies zum Beispiel auch an der sehr weitgreifenden Definition des IT-Systems in unserem Glossar : " IT-Systeme sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Mobiltelefone, Smartphones, Tablets, IoT-Komponenten, Router, Switches und Firewalls."

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen  
Im Auftrag für das IT-Grundschutz-Team

[REDACTED]

---

Referat SZ 13 - BSI Standards und IT Grundschutz Bundesamt für Sicherheit in der Informationstechnik Godesberger Allee 185-189  
53175 Bonn

Telefon: +49 228 99 9582 [REDACTED]  
Fax: +49 228 99 10 9582 [REDACTED]  
E-Mail: [REDACTED]@bsi.bund.de

Internet:  
[www.bsi.bund.de](http://www.bsi.bund.de)

#DeutschlandDigitalSicherBSI

-----Ursprüngliche Nachricht-----

Von: Joachim Lindenberg <[REDACTED]>  
Gesendet: Montag, 21. Juni 2021 15:37  
An: [REDACTED] <[REDACTED]@bsi.bund.de>  
Betreff: AW: Ihre Anfrage nach dem Informationsfreiheitsgesetz

Sehr geehrte Damen und Herren,

wenn das auf diesem Weg besser klappt soll es mir natürlich Recht sein. Die Frage war:  
"im Grundschutzbaustein OPR.4 (Edition 2021) schreiben Sie "Benutzer und IT-Komponenten müssen zweifelsfrei identifiziert und authentisiert werden." Oder in ORP.4.A9 Identifikation und Authentisierung [IT-Betrieb] (B) "Der

Zugriff auf alle IT-Systeme und Dienste MUSS durch eine angemessene Identifikation und Authentisierung der zugreifenden Benutzer, Dienste oder IT-Systeme abgesichert sein."

Benutzer ist einfach, ein Mensch. Ein Mensch kann auch mehrere Benutzer haben, soweit klar. Aber leider definieren Sie die Begriffe IT-Komponente, IT-System, und Dienst nicht - oder nicht im Zusammenhang. Was soll ich mir darunter vorstellen? Eine (virtuelle) Maschine, einen Prozess, eine separat installier- und patchbare Einheit? Einen Kubernetes Pod? Eine Menge davon?

Was bedeutet denn zweifelsfrei im Unterschied zu angemessen?"

Vielen Dank und viele Grüße

Joachim Lindenberg

-----Ursprüngliche Nachricht-----

Von: [REDACTED] <[REDACTED]@bsi.bund.de>

Gesendet: Monday, 21 June 2021 13:25

An: Joachim Lindenberg <[REDACTED]>

Betreff: AW: Ihre Anfrage nach dem Informationsfreiheitsgesetz

Sehr geehrter Herr Lindenberg,

vielleicht ist dann die IFG-Anfrage und die Bürgeranfrage nicht der ausreichend fachspezifische Weg. Sie können die Kolleg:innen des IT-Grundschutzes gerne auch direkt (eventuell auch mit detaillierteren Informationen) unter [REDACTED]@bsi.bund.de anschreiben. Vielleicht finden sich doch noch Antworten auf Ihre Fragen.

Mit freundlichen Grüßen

Im Auftrag

[REDACTED]

-----Ursprüngliche Nachricht-----

Von: Joachim Lindenberg <[REDACTED]>

Gesendet: Montag, 21. Juni 2021 12:54

An: [REDACTED] <[REDACTED]@bsi.bund.de>

Betreff: AW: Ihre Anfrage nach dem Informationsfreiheitsgesetz

Sehr geehrte [REDACTED],

ich bin Mitglied der Fachwelt. Der Begriff Komponente ist so überladen und wird in so unterschiedlichen Bedeutungsvarianten verwendet, so dass dieser Begriff an dieser Stelle zu Missverständnissen führt. Ich arbeite gerade bei einem Unternehmen das sich am Grundschutz orientiert, und verschiedene Mitarbeiter interpretieren ihn unterschiedlich. Insofern ist die Frage an den Verfasser der Richtlinie durchaus sinnvoll, um den Interpretationsspielraum eingrenzen zu können, denn für die Umsetzung des Grundschutzes und ggfs. eine Zertifizierung ist das eine ziemlich wichtige Frage.

Im Übrigen ist der Baustein Active Directory hier wesentlich eindeutiger in dem er die Verwendung von (group) managed service accounts empfiehlt. Eine ähnlich klare Empfehlung fehlt in ORP.4.

Vielen Dank und viele Grüße

Joachim Lindenberg

-----Ursprüngliche Nachricht-----

Von: [REDACTED] <[REDACTED]@bsi.bund.de>

Gesendet: Monday, 21 June 2021 12:39

An: [REDACTED]

Cc: [REDACTED] <[REDACTED]@bsi.bund.de>

Betreff: Ihre Anfrage nach dem Informationsfreiheitsgesetz


Sehr geehrter Herr Lindenberg,

anbei übersende ich Ihnen meinen Bescheid zu Ihrer Anfrage nach dem Informationsfreiheitsgesetz (IFG) vom 03.06.2021.

Ich möchte Sie darauf hinweisen, dass es sich bei Ihrer Anfrage inhaltlich nicht um eine Anfrage nach dem Informationsfreiheitsgesetz (IFG) handelt, da es sich hierbei um Verständnisfragen handelt und diese sich nicht auf bereits vorhandene Informationen beziehen. Ich habe die zuständigen Kollegen um Beantwortung Ihrer Fragen gebeten und möchte Ihnen die Antwort untenstehend übersenden:


Der Begriff "IT-Komponente" ist in der Fachwelt allgemein bekannt und kann aus den jeweiligen Zusammenhängen unterschiedlich belegt sein. Das Gleiche gilt für die Begriffe Dienst und IT-System. Der Glossar zum IT-Grundschutz beschränkt sich auf Begriffe aus dem IT-Grundschutz und definiert keine allgemeinen Begriffe der Informationstechnik. Da sich Ihre Fragen auf einen öffentlichen Baustein des IT-Grundschutz bezieht, sind auch alle Umsetzungshinweise und den ganzen Entwicklungsprozess öffentlich verfügbar.

Mit freundlichen Grüßen  
Im Auftrag

  
  
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Godesberger Allee 185 - 189  
53175 Bonn

Telefon: +49 (0)228 99 9582 0

Telefax: +49 (0)228 99 9582 

E-Mail: @bsi.bund.de

Internet: [www.bsi.bund.de](http://www.bsi.bund.de)

#DeutschlandDigitalsicherBSI