

Konzept: Erfahrungsaustausch KRITIS – Audits (ERFA KRITIS – Audits)

Der Erfahrungsaustausch KRITIS – Audits (ERFA KRITIS – Audits, www.erfa-kritis.de) geht auf eine Initiative des Themenarbeitskreises Audits und Standards des UP KRITIS (UPK TAK AS) sowie des KRITIS Erfahrungsaustausches der Schulungsanbieter und Prüfer aus dem Jahr 2020 zurück und soll eine Plattform für einen offenen Kommunikationsaustausch zur Umsetzung des § 8a BSIG zwischen den nachfolgenden und am Prozess beteiligten Parteien im Rahmen der Nachweiserbringung fördern:

- Betreiber Kritischer Infrastrukturen
- Bundesamt für Sicherheit in der Informationstechnik
- Prüfende Stellen gemäß der Orientierungshilfe zu Nachweisen

Neben dem regelmäßigen Erfahrungsaustausch, soll der ERFA KRITIS – Audits an der branchenübergreifenden Entwicklung von möglichen Best-Practices für den Prozess der Nachweiserbringung gemäß § 8a BSIG (bspw. eine Konkretisierung der Orientierungshilfe zum B3S oder zu Nachweisen gemäß § 8a Absatz 3 BSIG) mitwirken und vor allem in Hinblick auf die praktische Umsetzung eruieren. Weitere Themen können bspw. die Evaluierung der Schnittstellen im Rahmen des Geltungsbereiches aus Sicht der Nachweiserbringung (Umgang mit Herstellern oder bspw. der Umgang mit / Abgrenzung von Lieferketten) sein.

Der Erfahrungsaustausch KRITIS – Audits soll als Kooperation zwischen dem Themenarbeitskreis Audits und Standards des UP KRITIS als ERFA-Kreis im Rahmen der Allianz für Cyber-Sicherheit (ACS)¹ etabliert und betrieben werden und steht allen ACS-Teilnehmern² folgender Institutionen offen:

- Betreiber Kritischer Infrastrukturen
- Branchen- und Berufsverbände
- Bundesamt für Sicherheit in der Informationstechnik und weitere Behörden
- Hersteller und Dienstleister
- Prüfende Stellen und Prüfer/Innen gemäß der Orientierungshilfe zu Nachweisen
- Schulungsanbieter "Zusätzliche Prüfverfahrenskompetenz für § 8a BSIG"

Der Mitarbeit liegt eine formlose Erklärung der Institution zur Teilnahme am Erfahrungsaustausch KRITIS unter Berücksichtigung des Code of Conduct (CoC) zu Grunde. Die Teilnehmer treffen sich regelmäßig (halbjährlich) in Form von virtuellen Konferenzen oder Präsenzveranstaltungen. Eine Ausrichtung vor Ort findet im rotierenden Verfahren statt, wobei die Teilnehmer freiwillig eine Veranstaltung ausrichten können.

¹ Weitere Informationen zu ERFA-Kreisen der ACS finden sich auf der Webseite unter <https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Angebote/ERFA-Kreise/erfakreis.html>; letzter Aufruf: 15.11.2020

² Eine Teilnahme an der ACS ist nicht zwingend notwendig, aber aufgrund der TLP-Verpflichtung und Regelungen hinsichtlich des Datenschutzes wünschenswert. Weitere Informationen hierzu und der Teilnahmeantrag zur ACS finden sich unter <https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Registrierung/registrierung.html>; letzter Aufruf: 15.11.2020

Der Erfahrungsaustausch KRITIS – Audits betreibt neben einer Webseite eine zentrale Mailingliste public@list.erfa-kritis.de, die für die Kommunikation zwischen den Teilnehmern eingesetzt werden soll. Die Nachrichteninhalte werden archiviert, wobei der Zugang zum Archiv nur durch die Teilnehmer der Liste möglich sein wird.

Weitere Informationen zur Teilnahme am ERFA KRITIS – Audits sowie die Daten zur Kontaktaufnahme mit dem Lenkungskreis finden sich unter www.erfa-kritis.de.

Code of Conduct (CoC) zum Erfahrungsaustausch KRITIS

0. Präambel

Kritische Infrastrukturen stellen für viele Bereiche der Gesellschaft und des öffentlichen Zusammenlebens eine grundlegende Basis dar. Die dort verwendeten IT-Systeme sind hochgradig vernetzt, komplex und für einen einwandfreien Betrieb der Kritischen Infrastrukturen unabdingbar geworden. Die fortwährende Intensivierung der Angriffe auf IT-Systeme kritischer Infrastrukturen stellt alle beteiligten Akteure vor neue Herausforderungen.

Um diesen Herausforderungen in Zukunft gemeinsam entgegenzuwirken setzt sich der Erfahrungsaustausch KRITIS – Audits (ERFA KRITIS – Audits) vor allem das Ziel, eine Plattform für einen offenen Kommunikationsaustausch zur Umsetzung des § 8a BSIG zwischen den nachfolgenden und am Prozess beteiligten Stakeholdern im Rahmen der Nachweiserbringung zu fördern:

- Betreiber Kritischer Infrastrukturen
- Bundesamt für Sicherheit in der Informationstechnik
- Prüfende Stellen gemäß der Orientierungshilfe zu Nachweisen

Neben dem regelmäßigen Erfahrungsaustausch, soll der ERFA KRITIS – Audits an der branchenübergreifenden Entwicklung von möglichen Best-Practices für den Prozess der Nachweiserbringung gemäß § 8a BSIG (bspw. eine Konkretisierung der Orientierungshilfe zum B3S oder zu Nachweisen gemäß § 8a Absatz 3 BSIG) mitwirken und vor allem in Hinblick auf die praktische Umsetzung eruieren. Weitere Themen können bspw. die Evaluierung der Schnittstellen im Rahmen des Geltungsbereiches aus Sicht der Nachweiserbringung (Umgang mit Herstellern oder bspw. der Umgang mit / Abgrenzung von Lieferketten) sein.

1. Teilnehmer

Der Erfahrungsaustausch KRITIS – Audits soll als Kooperation zwischen dem Themenarbeitskreis Audits und Standards des UP KRITIS als ERFA-Kreis im Rahmen der Allianz für Cyber-Sicherheit (ACS)³ etabliert und betrieben werden und steht allen ACS-Teilnehmern⁴ folgender Institutionen offen:

- Betreiber Kritischer Infrastrukturen
- Branchen- und Berufsverbände
- Bundesamt für Sicherheit in der Informationstechnik und weitere Behörden
- Hersteller und Dienstleister
- Prüfende Stellen und Prüfer/Innen gemäß der Orientierungshilfe zu Nachweisen

³ Weitere Informationen zu ERFA-Kreisen der ACS finden sich auf der Webseite unter <https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Angebote/ERFA-Kreise/erfakreis.html>; letzter Aufruf: 15.11.2020

⁴ Eine Teilnahme an der ACS ist nicht zwingend notwendig, aber aufgrund der TLP-Verpflichtung und Regelungen hinsichtlich des Datenschutzes wünschenswert. Weitere Informationen hierzu und der Teilnahmeantrag zur ACS finden sich unter <https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Registrierung/registrierung.html>; letzter Aufruf: 15.11.2020

- Schulungsanbietern "Zusätzliche Prüfverfahrenskompetenz für § 8a BSIG"

Teilnehmende Institutionen können mehrere Vertreter entsenden, welche aktiv und kontinuierlich am Erfahrungsaustausch mitwirken.

2. Allianz für Cyber-Sicherheit

Mit der Allianz für Cyber-Sicherheit steht das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die nationale Sicherheitsbehörde Unternehmen und Institutionen zur Seite. Bereits seit 2012 arbeitet das BSI intensiv mit Partnern und Multiplikatoren aus Wirtschaft und Forschung zusammen, um strategische und praktische Hilfestellung zur Umsetzung von Informationssicherheit in den Unternehmen zu leisten und so die Cyber-Sicherheit am Wirtschaftsstandort Deutschland zu fördern.

Die wesentlichen Punkte im Hinblick auf den ERFA KRITIS – Audits zusammenfassen dargestellt:

- Die Teilnahme an der Allianz für Cyber-Sicherheit erfolgt auf freiwilliger Basis und ist kostenfrei. Sie kann beidseitig jederzeit ohne Einhaltung von Fristen in schriftlicher Form beendet werden.
- Es ergeben sich keine weiteren rechtlichen Verpflichtungen außer der Zustimmung zu den Bedingungen des Traffic Light Protokolls (TLP), was ebenfalls im Interesse der Mitglieder des ERFA KRITIS – Audits ist.
- Die im Rahmen der ACS verbreiteten Informationen werden, entsprechend ihrer Sensitivität, gemäß dem „Traffic Light Protocol“ (TLP) eingestuft.
- Die Regelungen zum TLP werden durch das Merkblatt „Behandlung vertraulicher Informationen“ festgelegt und erläutert. Alle Zugangsberechtigten aus den teilnehmenden Institutionen haben sich persönlich dazu zu verpflichten, Informationen, welche sie durch oder im Zusammenhang mit der ACS erlangen, entsprechend der Regelungen des TLP zu behandeln und diese unbefugten Dritten nicht zugänglich zu machen.

3. Leitlinien der Zusammenarbeit

Folgende Leitlinien bestimmen die Zusammenarbeit im ERFA KRITIS – Audits:

- Die Kooperation ist freiwillig und kann jederzeit beendet werden.
- Die Vertraulichkeit hat oberste Priorität. Sitzungen bzw. Teile von Sitzungen des ERFA KRITIS – Audits unterliegen den Vertraulichkeitsregelungen des in der ACS verwendeten „Traffic Light Protokolls“. Zusätzlich gilt die „Chatham House Rule“⁵, sofern diese nicht ausdrücklich für einzelne Sitzungen bzw. Tagesordnungspunkte ausgeschlossen wird.
- Informationen und Interessen anderer Mitglieder werden geschützt.
- Es erfolgt ein regelmäßiger Erfahrungsaustausch und eine kontinuierliche Weiterbildung innerhalb des Kreises.

⁵ Chatham-House-Regeln besagen, dass den Teilnehmern die freie Verwendung der erhaltenen Informationen unter der Bedingung gestattet ist, dass weder die Identität noch die Zugehörigkeit von Rednern oder anderen Teilnehmern preisgegeben werden dürfen.

- Durch wechselseitige Beiträge und Informationen sollen die Arbeitsabläufe aller Teilnehmer optimiert werden.
- Die eigene Arbeit und die Zusammenarbeit sollen ein Vorbild für Prüfer, Prüfende Stellen und Betreiber Kritischer Infrastrukturen sein.

4. Kommunikation

Für die Kommunikation unterhält der ERFA KRITIS – Audits, neben einer Webseite mit grundlegenden Informationen und einer Kontaktmöglichkeit des Leitungsgremiums, eine zentrale Mailingliste public@list.erfa-kritis.de, die für die Kommunikation zwischen den Teilnehmern eingesetzt werden soll. Die Nachrichteninhalte werden archiviert, wobei der Zugang zum Archiv nur durch die Teilnehmer der Liste möglich ist.

Daneben ist über die E-Mail-Adresse kontakt@erfa-kritis.de der Lenkungskreis des ERFA-KRITIS erreichbar.

5. Veranstaltungen

Der ERFA KRITIS – Audits führt in regelmäßigen Abständen (halbjährlich) Arbeitstreffen durch. Eingeladen sind alle Teilnehmer des ERFA KRITIS – Audits. Gäste dürfen nach vorheriger Anmeldung beim Lenkungskreis teilnehmen. Die Veranstaltungen können als virtuelle oder Präsenzveranstaltungen stattfinden. Der Umfang beträgt 2 bis 3 Stunden für virtuelle und 6 bis 8 Stunden für Präsenzveranstaltungen. Eine Ausrichtung vor Ort (Präsenzveranstaltung) findet im rotierenden Verfahren statt und basiert auf Freiwilligkeit der Teilnehmer. Bei Präsenzveranstaltungen soll grundsätzlich eine Teilnahme per Remote-Einwahl möglich sein. Entsprechende technische Vorkehrungen sind dabei durch den Ausrichter vorzusehen.

Für allen Veranstaltungen gilt der nachfolgende Rahmen als Agenda, wobei die Finalisierung mit einem Vorlauf von ca. 2 Wochen erfolgt und die finale Agenda an die Teilnehmer verschickt wird:

- Eröffnung und Begrüßung durch den Ausrichter
- Festlegung Moderation und Protokollierung
- Neuigkeiten aus dem BSI
- Neuigkeiten von Betreibern Kritischer Infrastrukturen
- Neuigkeiten von Prüfenden Stellen (KRITIS)
- Ausblick
 - Termin nächstes Treffen
 - Ausrichter der nächsten Runde

6. Gremien (Lenkungskreis)

Als Gremium nimmt der Lenkungskreis eine koordinierende Funktion ein und ist zugleich das Entscheidungsgremium des ERFA KRITIS – Audits. Er besteht aus mindestens fünf und höchstens sieben gewählten Personen aus dem Kreis der teilnehmenden Institutionen, die für eine Dauer von vier Jahren gewählt werden. Die Aufgaben des Lenkungskreises sind u.a.:

- Steuerung der inhaltlichen Weiterentwicklung des ERFA KRITIS – Audits durch das Setzen thematischer Schwerpunkte
- Unterstützung des Wachstums des ERFA KRITIS – Audits z. B. durch aktive, positive Darstellung des ERFA KRITIS – Audits nach außen oder gezielte Ansprache möglicher neuer Teilnehmer
- Aufnahme von neuen Teilnehmern
- Feststellung von Verstößen gegen Vereinbarungen und Beschluss von Sanktionen wie z. B. den Ausschluss
- Protokollierung und Verteilung aller Entscheidungen
- Organisation und Durchführung von Veranstaltungen

Der Lenkungskreis wählt einen Vorsitzenden und einen Stellvertreter aus seinen Reihen. Die Aufgaben des Vorsitzenden umfassen dabei:

- Sammlung der Tagesordnungspunkte und Erstellung, sowie Versand der Agenda
- Versand der Einladungen für die Veranstaltungen
- Leitung der Veranstaltungen
- Kontrolle und Versand des Protokolls an die Teilnehmer

7. Änderungen des CoC

Änderungsvorschläge des Code of Conduct sind schriftlich zu verfassen und mindestens sechs Wochen vor der nächsten Veranstaltung an den Lenkungskreis kontakt@erfa-kritis.de zu adressieren. Die Änderungsvorschläge werden mindestens vier Wochen vor der nächsten Veranstaltung durch den Lenkungskreis an alle Teilnehmer über die offizielle Mailingliste versandt.

Die Entscheidung über Änderungen erfolgt durch die Abstimmung bei der Veranstaltung, wobei eine 2/3 Mehrheit der möglichen Stimmen ausreicht. Die Anzahl der möglichen Stimmen wird zu Beginn der Veranstaltung festgelegt. Nach erfolgter Zustimmung treten die Änderungen der CoC sofort in Kraft. Die überarbeiteten Grundsätze werden allen Teilnehmern über die Mailingliste zur Verfügung gestellt.

8. Auflösung des ERFA KRITIS – Audits

Anträge zur Auflösung des ERFA KRITIS – Audits sind schriftlich zu verfassen und mindestens sechs Wochen vor der nächsten Veranstaltung an den Lenkungskreis kontakt@erfa-kritis.de zu adressieren. Sie sind mindestens vier Wochen vor der nächsten Veranstaltung über die Mailingliste an alle Teilnehmer zu versenden.

Die Entscheidung zur Auflösung des ERFA KRITIS – Audits erfolgt durch die Abstimmung bei der Veranstaltung, wobei eine 3/4 Mehrheit der möglichen Stimmen ausreicht. Die Anzahl der möglichen Stimmen wird zu Beginn der Veranstaltung festgelegt.