Bundesamt
für Sicherheit in der
Informationstechnik

LARS ICS Version 1.0

Light and Right Security ICS - Ein Werkzeug für den leichtgewichtigen Einstieg in industrielle Cyber-Security

Benutzerhandbuch

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6012
E-Mail: ics-sec@bsi.bund.de
Internet: https://www.bsi.bund.de/ICS

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Industrielle Steuerungsumgebungen (im Folgenden als ICS für Industrial Control System bezeichnet) werden immer vernetzter und komplexer. Die Absicherung solcher Systeme wird somit zunehmend eine immer größere Herausforderung. Dabei stehen die Verantwortlichen zunächst vor der Aufgabe, ICS bzgl. Security zu analysieren, um Schwachstellen zu identifizieren und eine bestehende Security-Stufe bestimmen zu können. An dieser Stelle unterstützt das hier vorgestellte Werkzeug den Benutzer.

LARS (Light and Right Security) wurde entwickelt, um die Betreiber von ICS zu unterstützen, diese sicherer zu planen und zu betreiben. Es beinhaltet Funktionalitäten, um ICS und den Umsetzungsgrad von Security-Maßnahmen zu erfassen und die aktuelle Security-Stufe auf Grundlage einer vorgegebenen Metrik zu bewerten. Es können anschließend durch den Benutzer verschiedene Berichte erzeugt werden, z. B. eine Auflistung aller Maßnahmen, die zur Erreichung der nächstbesseren Security-Stufe umgesetzt werden müssen. Nachdem Maßnahmen umgesetzt wurden, können die Änderungen im Werkzeug nachgezogen und deren Auswirkungen auf die Security-Stufe durch das Werkzeug neu ermittelt werden.

Das Werkzeug ist nicht dazu gedacht ein ganzheitliches Information Security Management System (ISMS) zu ersetzen, sondern es soll den Einstieg in die Absicherung von ICS erleichtern und den Weg zur Benutzung eines ISMS wie z. B. IT-Grundschutz oder IEC 62443 bereiten.

Das vorliegende Dokument beschreibt das Werkzeug zur Security-Analyse von ICS. Die im Werkzeug hinterlegte Methodik beinhaltet folgende wesentlichen Elemente:

- Eine Eingabeoberfläche, die den Benutzer bei der Analyse unterstützt.
- Eine Metrik, mit der die Kritikalität von Schwachstellen und die erreichte Security-Stufe für ein Industrial Control System (ICS) transparent für den Benutzer berechnet werden.
- Eine Reporting-Funktionalität, mit der automatisch standardisierte Berichte erzeugt werden können.
- Die Abbildung auf weitere Standards wie IEC 62443 und Grundschutzkataloge des BSI.

Die Methodik ist sehr vereinfacht worden im Vergleich zu klassischen Schutzbedarfs- und Risikoanalysen, um den Einstieg in die Cyber-Sicherheit gerade für mittelständische Unternehmen zu erleichtern sowohl bzgl. der Kenntnisse über Security und Analysetechniken als auch bzgl. der Personalaufwände.

Die durch LARS unterstützte Methodik ersetzt natürlich keine detaillierte Schutzbedarfs- und Risikoanalyse von versierten Fachkräften. Zudem kann das entwickelte Werkzeug in der vorliegenden, ersten Version nur für nicht zu komplexe Umgebungen eingesetzt werden.

Bei der hier veröffentlichten Version handelt es sich um einen Prototypen. Kommentare und Anregungen können gerne an ics-sec@bsi.bund.de geschickt werden.

Es ist der vollständige Quellcode von LARS enthalten. Die Software steht unter der Lizenz Apache 2.0 (siehe Anhang).

2 Installation und Start

2.1 Installation

LARS muss nicht über eine Installationsroutine installiert werden. Um es auszuführen, wird Java 7 oder neuer benötigt; eine entsprechende Laufzeitumgebung für Microsoft Windows (Java SE 8u25) liegt dem Programm bei, sodass LARS auch lauffähig ist, ohne Java installieren zu müssen. Das Programm besteht aus einem Ordner, der alle nötigen Informationen enthält. Im Weiteren wird das Vorgehen unter Windows beschrieben.

Das Archiv LARS.zip kann mit Windows Bordmitteln (Rechtsklick->Alle extrahieren...) oder dem bevorzugten Komprimierungsprogramm an einen beliebigen Ort entpackt werden. Dort entsteht ein Verzeichnis LARS, welches mehrere Unterverzeichnisse sowie unter anderem die Dateien Start.bat, lars.db3 (die Datenbank, in der Maßnahmen und Eingaben verwaltet werden) und die Lizenz für LARS enthält.

2.2 Start

Über die im entpackten Ordner zu findende Datei Start.bat kann das Programm per Doppelklick gestartet werden. Sofern auf dem PC eine passende Java-Laufzeitumgebung installiert ist, kann auch die Datei LARS-ICS.jar direkt zum Starten verwendet werden. Nach dem Starten des Programms wird zuerst die Lizenz sowie eine Sicherheitswarnung angezeigt, bevor der Benutzer und im Anschluss das Projekt erfragt wird.

2.2.1 Benutzerverwaltung

Im Fenster "Benutzerverwaltung" kann in der Liste in der linken Hälfte des Fensters ein Benutzer selektiert und über den Knopf *Wählen* am unteren Rand des Fensters beziehungsweise durch Doppelklick auf das Listenelement ausgewählt werden. Um einen neuen Benutzer anzulegen, müssen die beiden Textfelder in der rechten Hälfte des Fensters mit vollem Namen (oberes Feld) und Kürzel (unteres Textfeld) ausgefüllt werden. Durch Klick auf den Knopf *Neu* links unterhalb der Textfelder wird der neue Benutzer angelegt und erscheint in der Liste. Zum Löschen eines Benutzers muss der entsprechende Benutzer in der Liste selektiert werden und anschließend auf den Knopf *Löschen* rechts unterhalb der Textfelder geklickt werden.

Hinweis: Die Benutzerverwaltung dient nur der Protokollierung für den am Schluss entstehenden Bericht und umfasst keinerlei Sicherheitsfunktionalität.

2.2.2 Projektverwaltung

Im Fenster "Projektverwaltung" kann in der Liste in der oberen Hälfte des Fensters ein Projekt selektiert und über den Knopf *Laden* links unterhalb der Liste beziehungsweise durch Doppelklick auf das Listenelement ausgewählt werden. Um ein neues Projekt anzulegen, muss das Textfeld in der unteren Hälfte des Fensters ausgefüllt werden. Durch Klick auf den Knopf *Neues Projekt* links unterhalb des Textfeldes wird das neue Projekt angelegt und erscheint in der Liste. Projekte können in der aktuellen Version des Werkzeugs nicht gelöscht werden.

2.3 Sicherheitshinweis

Die Datenbank des Programms und alle anfallenden, teils sensiblen Daten sind in keiner Weise geschützt und müssen vom Anwender entsprechend abgesichert werden.

3 Elemente des Werkzeugs

Das Werkzeug unterstützt den Benutzer bei einer Security Analyse eines ICS durch folgende Funktionalitäten:

- Strukturanalyse: Alle erfassten Assets werden in einer Baumstruktur dargestellt .
- Security-Maßnahmen: Nach der Erfassung der Assets werden Security-Maßnahmen automatisch angezogen. Der Benutzer kann den Umsetzungsgrad der Maßnahmen angeben und Erläuterungen einfügen.
- Security-Metrik: Im Werkzeug ist eine Security-Metrik fest hinterlegt. Auf Basis der eingegebenen Daten berechnet das Werkzeug automatisch eine Security-Stufe.
- Berichte: Der Benutzer kann über Menüpunkte verschieden Berichte erzeugen.

Der Benutzer muss seine Eingaben oder Änderungen nicht explizit abspeichern. Eingaben des Benutzers werden automatisch abgespeichert, wenn er zu einem neuen Menüpunkt oder Teilbaum wechselt oder das Programm beendet. Zum Beispiel werden die eingegebenen Daten dann transparent für den Benutzer gespeichert, wenn er zu einer anderen Kategorie, Domäne, zu einem anderen Asset-Typen wechselt oder den Menüpunkt für die Erzeugung von Berichten anwählt oder das Programm schließt.

Die Struktur des Asset-Baumes ist wie folgt:

Asset-Typ
└ Domäne
└ Kategorie
└ Maßnahme

Diese Elemente werden im Folgenden detaillierter beschrieben.

3.1 Asset-Typen

LARS gruppiert die Assets eines ICS nach folgenden Asset-Typen:

- ICS insgesamt
- Kommunikationsverbindungen
- Intelligent Electronic Device (IED)
- Remote Terminal Unit (RTU)
- Speicherprogrammierbare Steuerung (SPS), Master Terminal Unit (MTU)
- Human-Machine-Interface (HMI)
- Data Historian
- Engineering Workstation (EWS)
- Router
- Switch
- Firewall
- Gateway
- Mobile Endgeräte

- Externe Endgeräte
- Mobile Datenträger

Im Moment stehen nur die hier angegebenen Asset-Typen zur Verfügung. Der Asset-Typ ICS insgesamt wird verwendet, um Asset-übergreifende Security-Maßnahmen dem Benutzer anzuzeigen, welche das gesamte ICS betreffen (siehe Abschnitt 3.3), damit er deren Umsetzungsgrad angeben kann.

3.2 Domänen

Die Asset-Typen können in verschiedenen Domänen auftreten. Folgende Domänen sind im Werkzeug hinterlegt:

- Feldebene (Safety)
- Feldebene (Operation)
- Steuerungsebene (Safety)
- Steuerungsebene (Operation)
- Leitebene
- Unternehmensebene
- Externes Netzwerk

Im Standard IEC 62443 entspricht der Begriff „Zone“ in etwa dem hier verwendeten Begriff Domäne.

3.3 Kategorien

Die Maßnahmen für die verschiedenen Kombinationen von Asset-Typ und Domäne sind in Kategorien gebündelt. Kategorien entsprechen Maßnahmenpaketen.

Dem Asset-Typ ICS gesamt sind zum Beispiel folgende übergeordnete Kategorien zugeordnet:

- Security Management
- Network Design & Management
- Malware Protection
- Applikationssicherheit
- Fernzugriff
- Log Monitoring & Management
- Physische Sicherheit
- Personelle Aspekte
- Business Continuity Management
- Prozesse
- Audit & Revision
- Auswahl und Beschaffung von Komponenten

Diese Kategorien treffen auf das gesamte ICS zu. Abhängig von Asset-Typ und Domäne sind weitere Kategorien definiert.

3.4 Vorgegebene Security-Stufe

Die vorgegebenen Maßnahmen sind in vier Kritikalitätsstufen eingeteilt:

- **KO**: Maßnahmen dieser Kritikalitätsstufe müssen unbedingt umgesetzt werden, da sonst die niedrigsten Anforderungen der Security nicht erfüllt sind.
- **1**: Maßnahmen dieser Kritikalitätsstufe müssen umgesetzt werden, um einen Basisschutz zu realisieren.
- **2**: Die Menge dieser Maßnahmen ist umzusetzen (zusätzlich zu den Maßnahmen bis Stufe 1), um ein mittleres Security-Niveau erreichen zu können.
- **3**: Diese Maßnahmen sind umzusetzen (zusätzlich zu den Maßnahmen bis Stufe 2), um ein angemessenes Security-Niveau zu erreichen. Dabei wird hier vorausgesetzt, dass man sich gegen einen qualifizierten Angreifer ausreichend schützen muss.

Folgende Security-Stufen sind möglich:

- Grün: Alle Maßnahmen wurden umgesetzt.
- Gelb: Mindestens eine Maßnahme der Kritikalität 3 wurde nicht umgesetzt, oder mehr als 20% der Maßnahmen mit Kritikalität 3 wurden teilweise umgesetzt.
- Orange: Mindestens eine Maßnahme der Kritikalität 2 wurde nicht umgesetzt, oder mehr als 20% der Maßnahmen mit Kritikalität 2 wurden teilweise umgesetzt.
- Rot: Mindestens eine Maßnahme der Kritikalität 1 wurde nicht umgesetzt, oder mehr als 20% der Maßnahmen mit Kritikalität 1 wurden teilweise umgesetzt.
- Dunkelrot: Mindestens eine Maßnahme der Kritikalität KO wurde teilweise oder nicht umgesetzt.

4 Bedienung

4.1 Beschreibung der Bedienoberfläche

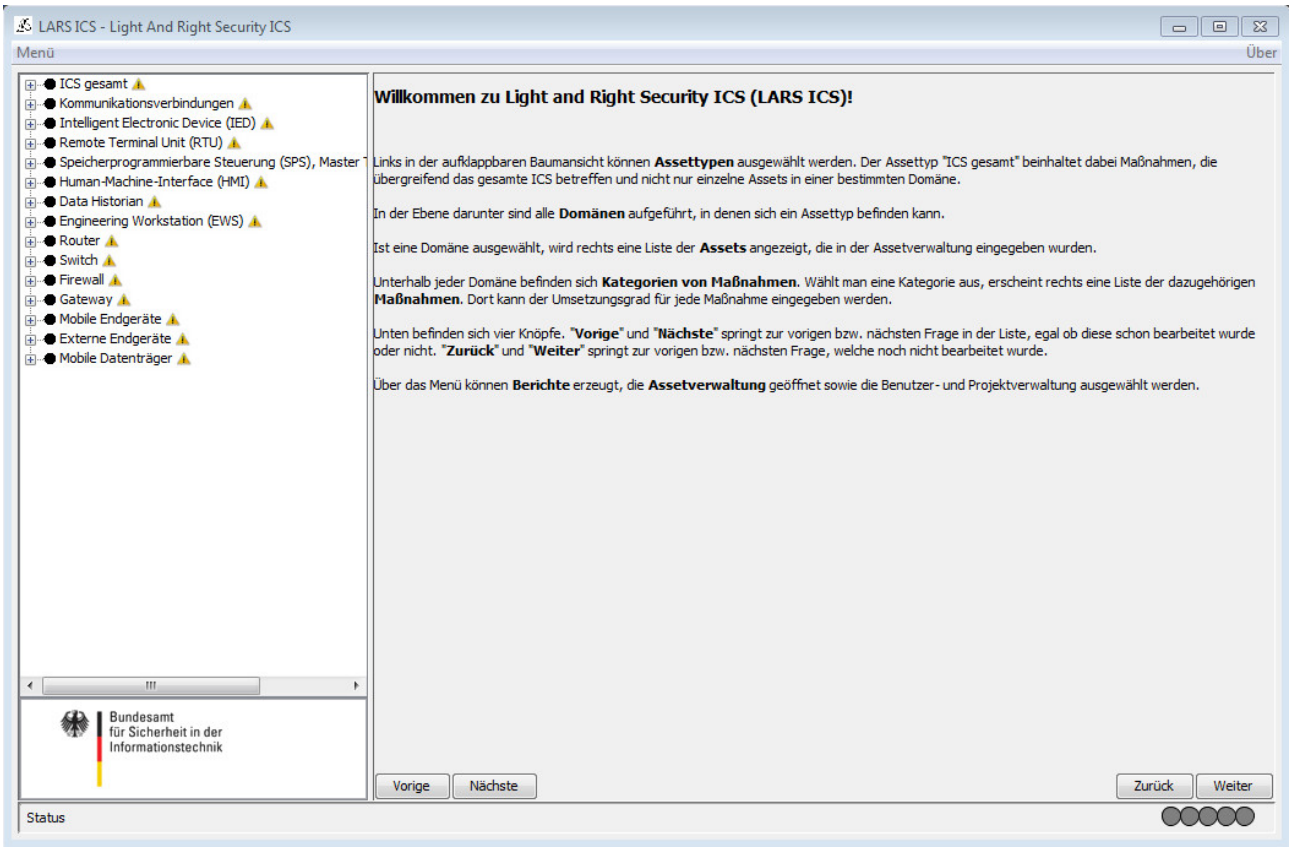

Abbildung 1: Bedienoberfläche nach Programmstart

Abbildung 1 zeigt die Hauptbedienoberfläche von LARS. In der Menüleiste am oberen Fensterrand befindet sich ganz links der Knopf *Menü* für das Hauptmenü. Über das Hauptmenü können die Projekt-, Benutzer- und Asset-Verwaltung geöffnet, sowie Berichte erzeugt und das Programm beendet werden. In der Menüleiste ganz rechts befindet sich der Knopf *Über* für allgemeine Informationen zum Programm und den verwendeten Lizenzen.

In der Spalte am linken Rand des Fensters befindet sich die Baumansicht der Asset-Typen.

Im rechten Bereich des Fensters werden je nach Auswahl in der Baumansicht unterschiedliche Bedienelemente angezeigt. Am unteren Rand des rechten Bereichs werden Bedienknöpfe für die Navigation im Baum der linken Spalte angezeigt. Das Knopfpaar *Vorige*/*Nächste* auf der linken Seite schaltet durch die Kategorien, das Paar *Zurück*/*Weiter* auf der rechten Seite durch die Kategorien, in denen es noch unbeantwortete Fragen gibt.

In der untersten Zeile des Fensters wird an der linken Seite der Pfad des aktuell in der Baumansicht gewählten Elements und an der rechten Seite eine Ampel angezeigt. Die Ampel zeigt die aktuelle Security-Stufe der gesamten Steuerungsumgebung an. Wenn noch nicht zu allen Maßnahmen eine Antwort gegeben wurde, ist die Ampel grau. Andernfalls wird eine der Farben, die in Abschnitt 3.4 definiert wurden, angezeigt.

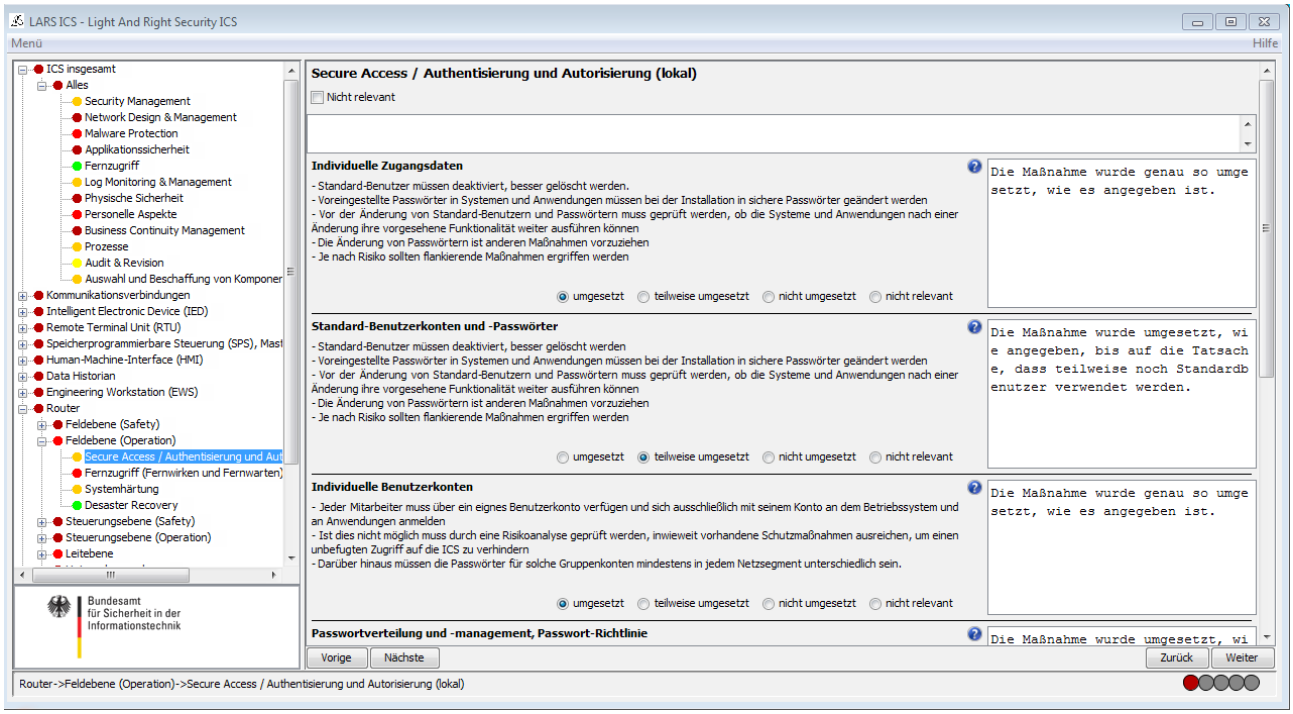

Abbildung 2: Bedienoberfläche mit vollständig ausgefüllten Maßnahmen

Durch Klick auf das Plus- beziehungsweise Minuszeichen vor den Elementen in der Baumansicht oder durch Doppelklick auf ein Element (siehe Abbildung 1) können die Baumteile geöffnet und geschlossen werden. Danach ist der Baum wie in Abbildung 2 aufgeklappt.

Der Kreis an der linken Seite jedes Baumelements in Abbildung 2 zeigt den aktuellen Sicherheitsstatus des Elements an. Wenn der Kreis schwarz ist beziehungsweise an der rechten Seite des Baumelements ein gelbes Warndreieck angezeigt wird, wurde noch nicht zu allen Maßnahmen, die sich im Baum hierarchisch unter dem Element befinden, Antworten gegeben.

Wenn in der Baumansicht eine Domäne ausgewählt wird, werden im rechten Bereich des Fensters die in der Asset-Verwaltung zugeordneten Assets angezeigt.

Wenn in der Baumansicht eine Kategorie ausgewählt wird, werden im rechten Bereich des Fensters die zugehörigen Maßnahmen zur Beantwortung angezeigt (wie dies in Abbildung 2 gezeigt ist). Für jede Maßnahme wird der Titel der Maßnahme, eine Kurzbeschreibung, Eingabemöglichkeiten für die möglichen Antworten zum Umsetzungsstand der Maßnahmen, ein Fragezeichen-Knopf für die Anzeige einer langen Beschreibung der Maßnahme und ein Textfeld für die Eingabe eines Kommentars angezeigt.

Nach Auswahl des Fragezeichen-Knopfs erscheint neben einer ausführlicheren Beschreibung der Maßnahme zusätzlich noch eine Zuordnung zu den entsprechenden Teilen bestehender Standards bzw. Empfehlungen (IEC 62443, IT-Grundschutz [ITGS], ISO 27001 und BSI ICS Security-Kompendium [KOMP]).

4.2 Analyse

Das Werkzeug dient der Unterstützung einer Security-Analyse eines ICS. Folgende Phasen sind bei der Analyse zu durchlaufen:

- Vorbereitung
- Erfassung Assets
- Erfassung Umsetzungsgrad von Security-Maßnahmen
- Erstellung Berichte

Die Phasen „Erfassung Assets“, „Erfassung Umsetzungsgrad von Security-Maßnahmen“ und „Erstellung Berichte“ werden durch das Werkzeug unterstützt.

4.2.1 Vorbereitunsphase

Die Methodik setzt eine Vorbereitungsphase voraus, die der Anwender durchlaufen muss, um die Analyse durchführen zu können. Die Vorbereitungsphase beinhaltet folgende Punkte:

- Teambildung zur Security-Analyse, inkl. Rollendefinition:
  - Entscheider, Business-, Safety- und Security-Experten mit ihren Verantwortlichkeiten
- Scope-Definition
  - Beschreibung des zu untersuchenden ICS
  - Schnittstellen des ICS (zum Beispiel Fernwartung)
  - Abgrenzungen des zu untersuchenden ICS
- Erstellung eines logischen Netzwerkplans des ICS
  - Erfassung der Komponenten (Assets)
  - Kommunikationsverbindungen und Schnittstellen
  - Identifizierung von Safety-relevanten Komponenten und IT-Systemen
- Sammlung und Sichtung relevanter Dokumentation bzgl. Security für
  - das zu untersuchende ICS (Informationen zu Software und Hardware)
  - die zugehörigen Prozesse und Organisation

4.2.2 Erfassung Assets

Zuerst sollten die gefundenen Assets in der Asset-Verwaltung (Menüpunkt *Assetverwaltung*) den entsprechenden Asset-Typen und Domänen zugewiesen werden. Im Asset-Verwaltungsfenster werden von links nach rechts zuerst Asset-Typ und Domäne ausgewählt. Im Anschluss können in der ganz rechten Spalte Assets eingegeben und zu der Liste in der dritten Spalte von links hinzugefügt werden. Mit dem *Löschen*-Knopf unter der Spalte können die zugeordneten Assets wieder gelöscht werden. Die zu erfassenden Assets sollten eindeutige Identifier haben, mit denen sie im logischen Netzwerkplan und im Werkzeug identifiziert werden können.

Die zugewiesenen Assets können durch Auswahl der Domäne betrachtet werden. Wenn im Baum eine Domäne ausgewählt wird, werden die dieser Kombination aus Asset-Typ und Domäne zugewiesenen Assets angezeigt.

4.2.3 Erfassung Maßnahmen

Im Anschluss können die Fragen zu den angebotenen Maßnahmen, die in verschiedenen Kategorien gebündelt sind, beantwortet werden.

Bei Auswahl einer Kategorie kann angegeben werden, ob diese benötigt wird. Ein Kommentarfeld dient zur Angabe von Kommentaren und Begründungen. Wird eine Kategorie nicht benötigt, bedeutet das, dass alle Security-Maßnahmen, die unter dieser Kategorie gebündelt wurden, als nicht relevant für das gerade

untersuchte ICS erachtet werden. Dies muss im Kommentarfeld gut begründet werden. Wenn eine Kategorie als nicht benötigt markiert wird, müssen die zugehörigen Maßnahmen nicht beantwortet werden.

Wenn die Kategorie als benötigt markiert wurde, befinden sich unter dem Eingabefeld für den Kommentar die Eingabemöglichkeiten für die Maßnahmen. Für jede Maßnahme kann erfasst werden, ob sie „umgesetzt", „teilweise umgesetzt", „nicht umgesetzt" oder „nicht relevant ist". Auf der rechten Seite befindet sich ein Eingabefeld, in dem die Auswahl kommentiert werden sollte.

Wenn alle Maßnahmen einer Kategorie bearbeitet wurden, wird in der Baumansicht angezeigt, welche Security-Stufe mit dem eingegebenen Maßnahmenstand erreicht wird. Wenn alle Kategorien einer Domäne bearbeitet wurden, wird die Security-Stufe für die Domäne angezeigt, und wenn alle Domänen eines Asset-Typen bearbeitet wurden, wird die Security-Stufe für den Asset-Typen angezeigt.

Wenn alle Fragen beantwortet wurden, wird über die Ampel im Fenster unten rechts die Gesamt-Security-Stufe des ICS angezeigt.

5 Erstellung von Berichten

Berichte können über den Unterpunkt *Erzeuge Berichte* im Hauptmenü erstellt werden, wenn die notwendigen Informationen eingegeben wurden. Für einige Berichtsarten müssen nicht alle Fragen beantwortet sein. Für die Berichtsarten „*Asset-Typ Domäne Übersicht*“ und „*Domänen Übersicht*“ müssen nur die Fragen für die gewählte Kombination aus Asset-Typ und Domäne beziehungsweise der gewählten Domäne beantwortet sein. Im Falle der „*Domänen Übersicht*“ sind die Fragen möglicherweise über mehrere Asset-Typen verteilt. Für die Berichtsart „*ICS Übersicht*“ müssen nur die Fragen unterhalb des Punktes „ICS insgesamt“ beantwortet sein.

Bei den Berichtarten „*Asset-Typ Domäne Übersicht*“ und „*Domänen Übersicht*“ wird zunächst die gewünschte Kombination aus Asset-Typ und Domäne beziehungsweise die gewünschte Domäne erfragt. Im folgenden Dialog können Ort, Dateiname und Ausgabeformat für den Bericht festgelegt werden.

Die Berichtarten „*ICS insgesamt*“, „*Asset-Typ Domäne Übersicht*“ und „*Domänen Übersicht*“ geben die Maßnahmen aus, durch deren Umsetzung die Security-Stufe um eine Stufe erhöht werden kann. Wenn beispielsweise Maßnahmen der Kritikalität 2 und Maßnahmen der Kritikalität KO als nicht umgesetzt markiert wurden, werden nur die Maßnahmen der Kritikalität KO ausgegeben.

Die Berichtart „*ICS insgesamt*“ gibt die Übersicht der Maßnahmen und deren Umsetzungsstatus aus, die sich im Baum hierarchisch unterhalb des Asset-Typs „ICS insgesamt“ befinden.

Die Berichtsart „*Priorisierter Maßnahmenkatalog*“ gibt alle nicht vollständig umgesetzten Maßnahmen und deren Umsetzungsgrad aus. Die Maßnahmen werden nach Kritikalität sortiert.

Wenn eine Maßnahme in den Berichten das Ergebnis negativ beeinflusst, obwohl der Benutzer der Meinung ist, dass diese Maßnahme keine Kritikalität in dem Ausmaß hat, die das Programm vorgibt, sollte der Benutzer die Antwort auf diese Maßnahme auf „teilweise umgesetzt“, bzw. „nicht relevant“ setzen, um diese Maßnahme aus der Berechnung des Ergebnisses herauszunehmen und dies entsprechend kommentieren.

Anhang

Verwendete Bibliotheken: sqlite JDBC 3.7.2 von xerial, Apache(tm) FOP 1.1

Zur Ausführung von LARS wird eine Java SE Laufzeitumgebung Version 7 oder neuer benötigt. Im Programm enthalten ist Java SE 8u25 für Windows.

5. LIMITATION OF LIABILITY. IN NO EVENT SHALL ORACLE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF ORACLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ORACLE'S ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. $1,000).

6. TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Oracle if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon termination, you must destroy all copies of Software.

7. EXPORT REGULATIONS. You agree that U.S. export control laws and other applicable export and import laws govern your use of the Software, including technical data; additional information can be found on Oracle's Global Trade Compliance web site (http://www.oracle.com/us/products/export). You agree that neither the Software nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

8. TRADEMARKS AND LOGOS. You acknowledge and agree as between you

and Oracle that Oracle owns the ORACLE and JAVA trademarks and all ORACLE- and JAVA-related trademarks, service marks, logos and other brand

designations ("Oracle Marks"), and you agree to comply with the Third

Party Usage Guidelines for Oracle Trademarks currently located at

http://www.oracle.com/us/legal/third-party-trademarks/index.html . Any use you make of the Oracle Marks inures to Oracle's benefit.

9. U.S. GOVERNMENT LICENSE RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation shall be only those set forth in this Agreement.

10. GOVERNING LAW. This agreement is governed by the substantive and procedural laws of California. You and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco, or Santa Clara counties in California in any dispute arising out of or relating to this agreement.

11. SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

12. INTEGRATION. This Agreement is the entire agreement between you and Oracle relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

A. COMMERCIAL FEATURES. You may not use the Commercial Features for running Programs, Java applets or applications in your internal business operations or for any commercial or production purpose, or for any purpose other than as set forth in Sections B, C, D and E of these Supplemental Terms. If You want to use the Commercial Features for any purpose other than as permitted in this Agreement, You must obtain a separate license from Oracle.

B. SOFTWARE INTERNAL USE FOR DEVELOPMENT LICENSE GRANT. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File incorporated herein by reference, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Oracle grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified for the purpose of designing, developing, and testing your Programs.

C. LICENSE TO DISTRIBUTE SOFTWARE. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File, including, but not limited to the Java Technology Restrictions and Limitations on Redistribution of these Supplemental Terms, Oracle grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software, (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that: (a) is a complete, unmodified reproduction of this Agreement; or (b) protects Oracle's interests consistent with the terms contained in this Agreement and that includes the notice set forth in Section H, and (vi) you agree to defend and indemnify Oracle and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software. The license set forth in this Section C does not extend to the Software identified in Section G.

D. LICENSE TO DISTRIBUTE REDISTRIBUTABLES. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the README File, including but not limited to the Java Technology Restrictions and Limitations on Redistribution of these Supplemental Terms, Oracle grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the README File ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified, and only bundled as part of Programs, (ii) the Programs add significant and primary functionality to the Redistributables, (iii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README File), (iv) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (v) you only distribute the Redistributables pursuant to a license agreement that: (a) is a complete, unmodified reproduction of this Agreement; or (b) protects Oracle's interests consistent with the terms contained in the Agreement and includes the notice set forth in Section H, (vi) you agree to defend and indemnify Oracle and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software. The license set forth in this Section D does not extend to the Software identified in Section G.

E. DISTRIBUTION BY PUBLISHERS. This section pertains to your distribution of the JavaTM SE Development Kit Software (“JDK”) with your printed book or magazine (as those terms are commonly used in the industry) relating to Java technology ("Publication"). Subject to and conditioned upon your compliance with the restrictions and obligations contained in the Agreement, Oracle hereby grants to you a non-exclusive, nontransferable limited right to reproduce complete and unmodified copies of the JDK on electronic media (the "Media") for the sole purpose of inclusion and distribution with your Publication(s), subject to the following terms: (i) You may not distribute the JDK on a stand-alone basis; it must be distributed with your Publication(s); (ii) You are responsible for downloading the JDK from the applicable Oracle web site; (iii) You must refer to the JDK as JavaTM SE Development Kit; (iv) The JDK must be reproduced in its entirety and without any modification whatsoever (including with respect to all proprietary notices) and distributed with your Publication subject to a license agreement that is a complete, unmodified reproduction of this Agreement; (v) The Media label shall include the following information: “Copyright [YEAR], Oracle America, Inc. All rights reserved. Use is subject to license terms. ORACLE and JAVA trademarks and all ORACLE- and JAVA-related trademarks, service marks, logos and other brand designations are trademarks or registered trademarks of Oracle in the U.S. and other countries.” [YEAR] is the year of Oracle's release of the Software; the year information can typically be found in the Software's “About” box or screen. This information must be placed on the Media label in such a manner as to only apply to the JDK; (vi) You must clearly identify the JDK as Oracle's product on the Media holder or Media label, and you may not state or imply that Oracle is responsible for any third-party software contained on the Media; (vii) You may not include any third party software on the Media which is intended to be a replacement or substitute for the JDK; (viii) You agree to defend and indemnify Oracle and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of the JDK and/or the Publication; ; and (ix) You shall provide Oracle with a written notice for each Publication; such notice shall include the following information: (1) title of Publication, (2) author(s), (3) date of Publication, and (4) ISBN or ISSN numbers. Such notice shall be sent to Oracle America, Inc., 500 Oracle Parkway, Redwood Shores, California 94065 U.S.A , Attention: General Counsel.

F. JAVA TECHNOLOGY RESTRICTIONS. You may not create, modify, or change the behavior of, or authorize your licensees to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun", “oracle” or similar convention as specified by Oracle in any naming convention designation.

G. LIMITATIONS ON REDISTRIBUTION. You may not redistribute or otherwise transfer patches, bug fixes or updates made available by Oracle through Oracle Premier Support, including those made available under Oracle's Java SE Support program.

H. COMMERCIAL FEATURES NOTICE. For purpose of complying with Supplemental Term Section C.(v)(b) and D.(v)(b), your license agreement shall include the following notice, where the notice is displayed in a manner that anyone using the Software will see the notice:

Use of the Commercial Features for any commercial or production purpose requires a separate license from Oracle. “Commercial Features” means those features identified Table 1-1 (Commercial Features In Java SE Product Editions) of the Java SE documentation accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html

I. SOURCE CODE. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

J. THIRD PARTY CODE. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME file accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME file, the disclaimer of warranty and limitation of liability provisions in paragraphs 4 and 5 of the Binary Code License Agreement shall apply to all Software in this distribution.

K. TERMINATION FOR INFRINGEMENT. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right.

L. INSTALLATION AND AUTO-UPDATE. The Software's installation and auto-update processes transmit a limited amount of data to Oracle (or its service provider) about those specific processes to help Oracle understand and optimize them. Oracle does not associate the data with personally identifiable information. You can find more information about the data Oracle collects as a result of your Software download at http://www.oracle.com/technetwork/java/javase/documentation/index.html.

For inquiries please contact: Oracle America, Inc., 500 Oracle Parkway,

Redwood Shores, California 94065, USA.

Last updated 02 April 2013

Literaturverzeichnis

ITGS	BSI: IT-Grundschutz. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
KOMP	BSI: ICS Security-Kompendium. https://www.bsi.bund.de/DE/Themen/weitereThemen/ICS-Security/Empfehlungen/Empfehlungen_node.html