



UL SETZT NEUE STANDARDS FÜR CYBERSECURITY

IoT realisierbar machen:
Mit standardisierten Kriterien Software-
Schwachstellen aufdecken und beurteilen.



UL CAP DAS UL CYBERSECURITY ASSURANCE PROGRAMM

IoT realisierbar machen: Mit standardisierten Kriterien
Software-Schwachstellen aufdecken und beurteilen.

Einleitung

Cybersecurity
und kritische
Infrastrukturen

Identifizierung von
Schwachstellen in der
Software-Lieferkette

Minimierung von
Schwachstellen in der
Software-Lieferkette

UL Cybersecurity
Assurance Program und
die UL 2900 Standards

Cybersecurity in
industriellen Steue-
rungssystemen (ICS)

Zusammenfassung



Ingo Rübenach
Vice President, DACH & Eastern Europe
UL International Germany GmbH

„Betrachtet man alle die Felder in der Industrie 4.0, auf denen durch das Internet der Dinge neue Technologien hervorgehen, dann stehen uns revolutionäre Umwälzungen bevor.

In der Fabrik von morgen sind die Lieferketten durchgängig und transparent und neue Services mit künstlicher Intelligenz gestalten die Produktion hocheffizient, Stichwort Advanced Manufacturing.

Aber viele Perspektiven müssen noch beleuchtet werden. Hierbei ist Cybersecurity ein zentrales Thema. Es geht jedoch weiter mit Interoperabilität und hört bei Mensch-Maschine-Kommunikation, welche die Sicherheit am Arbeitsplatz in ein neues Licht rückt, noch lange nicht auf.

*In all diesen Fällen ist Sicherheit ein Kern des Umsetzungsprozesses. Die Mission von UL (Underwriters Laboratories) dabei: **Wir wollen Industrie 4.0 realisierbar machen.**“*

CYBERBEDROHUNGEN DURCH DAS IOT

Von RFID zur industriellen Revolution

1999 prägte Kevin Ashton den Begriff „Internet der Dinge“. Der britische Technologie-Pionier stellte ein System mit RFID-Chips vor, das „Dinge“ miteinander kommunizieren ließ⁽¹⁾. Den Begriff Internet der Dinge verwendete er das erste Mal bei einer Präsentation, in der er die Bedeutung der RFID-Technik für die Logistik demonstrierte.

Seitdem sind Sensoren wesentlich günstiger und kleiner geworden. Sie liefern die Daten, die sich durch Cloud Computing in alle Richtungen des Internets verbreiten. Wir sind Zeugen, wie ein enormes dezentrales Netzwerk von Geräten, Anwendungen und Diensten entsteht. Heute ist das Internet der Dinge ein Schlüsselement in der Digitalen Transformation.

Für die Industrie bieten diese Veränderungen große Chancen, man spricht sogar von einer weiteren industriellen Revolution. Aus cyber-physischen Systemen entstehen Fertigungsanlagen, die umfassend miteinander vernetzt sind. Solche IoT-Systeme haben starken Einfluss auf die Geschäftsmodelle. Wer eine IoT-Plattform erfolgreich für die horizontale Wertschöpfung etabliert, beherrscht seinen Markt.

Vernetzte Geräte für Angriffe nutzen

Die Schattenseite dieser Entwicklung: Die umfassende Vernetzung und durchgängige, standardisierte Anwendungen erleichtern es Angreifern und Schadsoftware, auf die Systeme zuzugreifen. Und wir sprechen von Geräten, die weltweit verteilt sind. Lassen sich Millionen von Devices manipulieren und zu einer Plattform zusammenführen, können sie eine kraftvolle Distributed Denial of Service Attack (DDoS) durchführen. Einige Angriffe und Simulationen weisen heute in diese Richtung und zeigen, dass man diese Geräte genauso zusammenschalten kann wie PCs.

Daher ist es eine Herausforderung für alle Beteiligten und eine große Aufgabe für Forschung, Wirtschaft und Normierung, gemeinsam geeignete Sicherheitsanforderungen zu definieren. Wie diese Anforderungen aussehen können, ist schon gut ersichtlich Anhand der Bemühungen zur Sicherung von kritischen Infrastrukturen.

Kritische Infrastrukturen sind meist historisch gewachsene Systeme – wie viele industrielle Plattformen. Sie bestanden bislang aus autarken Steuerungs- und Automatisierungsanlagen und werden nun zunehmend über das Internet vernetzt. Das macht kritische Infrastrukturtypen besonders anfällig für Cyber-Vorstöße.

Open-Source-Software als Angriffspunkt

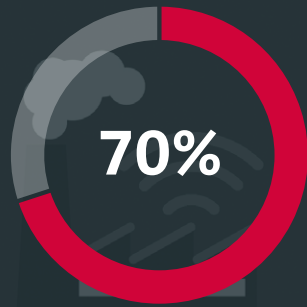
Ein besonderes Augenmerk ist dabei erforderlich bei der Nutzung von Software von Drittanbietern wie Open-Source-Software, bei vom Hersteller bereitgestellter Software oder von Code-Schnipsel, die aus Online-Quellen stammen. Denn mehr als 80 Prozent der heute verfügbaren Softwareanwendungen bestehen aus Open-Source-Komponenten⁽²⁾. Daher müssen Unternehmen ein besonderes Augenmerk legen auf ihre Software-Supply-Chain-Management-Systeme und Verfahren, um das potenzielle Risiko aus Anwendungen von Drittanbietern abzumildern.

Dieses eBook bietet im zweiten Kapitel einen Überblick über allgemeine Cybersicherheitsrisiken von kritischen Infrastrukturindustrien und erläutert, warum es wichtig ist, die Sicherheit und Integrität der Software-Lieferkette zu validieren. Kapitel 3 zeigt, welche Vorteile es bringt, dabei gemeinsame technische Kriterien anzuwenden, die von unabhängigen Dritten überprüft werden können. Welche Schritte möglich sind, um potenzielle Schwachstellen zu mildern, die Software zuzuschreiben sind, erfahren Sie im Kapitel „UL Cybersecurity Assurance Program und die UL 2900 Standards“.

(1) <http://www.rfidjournal.com/articles/view?4986>

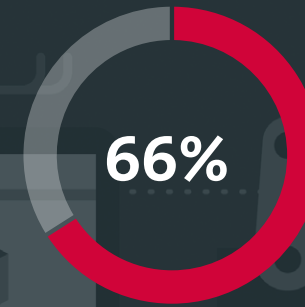
(2) “Protecting the open source software supply chain”, posted on GCN, <https://gcn.com/Articles/2016/07/22/software-supply-chain.aspx>.

CYBERBEDROHUNGEN DURCH DAS IOT



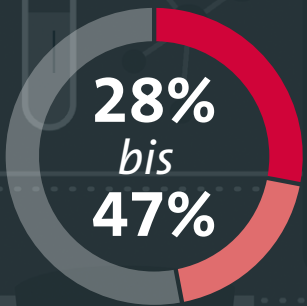
70% der IoT-Geräte sind anfällig für Angriffe

Quelle: HP



Bis 2018 wird in 66% aller Netzwerke eine IoT-Sicherheitsverletzung aufgetreten sein

Quelle: IDC Research



Bei 28% bis 47% aller Organisationen sind bereits Sicherheitsverstöße im IoT-Kontext aufgetreten

Quelle: Forrester/CISCO

2014 2015 2016



Im Jahr 2016 lagen die durchschnittlichen konsolidierten Gesamtkosten einer Datenschutzverletzung bei 4 Mio. USD

Quelle: 2016 Ponemon Study

FORSCHUNG IM AUFTRAG DES US-VERTEIDIGUNGSMINISTERIUMS

Es war eine US-Behörde, welche die Grundlagen für das Internet schuf. Sie hatte Ende der 60-er Jahre Forscher zusammengezogen, die das ARPANET entwickelten, aus dem später das Internet hervorging. Diese Behörde ist die DARPA, die Defense Advanced Research Projects Agency. Sie investiert im Auftrag des US-Verteidigungsministeriums in Forschungsprojekte, die im Interesse der Nationalsicherheit liegen, und fördert dabei technische Innovationen – von Biologie über Mikroelektronik bis hin zu unbemannten Fluggeräten.

Cybersicherheit von IoT-Gateways für industrielle Steuerungssysteme

Wie wichtig die Software-seitige Sicherung von kritischen Infrastrukturen ist, zeigt ein aktuelles Projekt der DARPA, zu deren Aufgaben es auch gehört, kritische Infrastrukturen wie Krankenhäuser oder Industrieanlagen zu sichern.

Ende 2016 hat die DARPA UL beauftragt, die Cyber Security von IoT-Gateways für industrielle Steuerungssysteme zu erforschen. Der Auftrag ging über neun Monate. Um alle Anforderungen zu überblicken, hatte das Cybersecurity-Team von UL die gesamte IoT-Architektur im Fokus, also sämtliche Software von

Micro-Chips, den Komponenten und Systemen. Dabei führten die UL-Ingenieure strukturierte Penetration-Tests durch und untersuchten, wie Systeme auf Remote-Geräte zugreifen und Software-Updates durchführen.

UL wurde gewählt, weil es seit über 20 Jahren im Sicherheitsbereich tätig ist. Das Unternehmen hat bereits für die US-Regierung Sicherheitsstandards für Kryptografiemodule spezifiziert und an weiteren Sicherheitsstandards mitgearbeitet. In seinem Cyber Assurance Program (CAP) untersucht UL seit vier Jahren Risiken von Industrie-4.0-Systemen in den

Bereichen Automobil, Fabrikautomation, Medizin und Beleuchtungsindustrie.

Die Konzepte, die in dem DARPA-Projekt erarbeitet wurden, wird UL auch in die Industrie zurückspielen. Sie haben eine große Chance, in der Praxis genutzt zu werden. Für das Projekt hat UL sein eigenes Cybersecurity Assurance- und Assessment vertieft und seine Fähigkeit in den Testprozessen von Industrie- und Factoring-Automatisierungskomponenten gestärkt. Denn UL erwartet künftig ein hohes Maß an Automatisierung, um IoT Geräte und Produkte sicher zu managen.

INDUSTRIE 4.0 ERFORDERT EINE DYNAMISCHE ZERTIFIZIERUNG

DAS AUFKOMMEN VON INDUSTRIE 4.0 HAT AUCH AUSWIRKUNGEN AUF DAS GESCHÄFT VON ZERTIFIZIERUNGSUNTERNEHMEN.

Bislang hat man in der Industrie ein Gerät hergestellt und nicht mehr angefasst. Für solche Geräte reichte ein einmaliger Zertifizierungsvorgang. Heute wird preiswerte Standard-Hardware genutzt, um die Vernetzung zu ermöglichen. Das bringt fortlaufend Software-Updates mit sich. Welche Auswirkungen diese Updates auf die Sicherheit haben, lässt sich mit einer einmaligen klassischen Zertifizierung nicht mehr beantworten.

ZUDEM SIND IOT-KOMPONENTEN SO KRITISCH, DASS ES EINEN KONSEQUENTES LIFECYCLE MANAGEMENT ERFORDERT. WAS PASSIERT, WENN EINE KOMPONENTE AM ENDE IHRER PRODUKTION IST?

Unternehmen benötigen ein sicheres Nachfolgeprodukt, schließlich kann die Komponente millionenfach

im Einsatz sein. Ein verantwortungsbewusster Komponentenhersteller sollte also Prozesse definieren, wie er hier verfährt – und eine Zertifizierung von Komponenten muss diese Prozesse natürlich enthalten. Solche Überlegungen bedeuten für UL einen Übergang von der statischen hin zu einer dynamischen Zertifizierung. Eine dynamische Zertifizierung erfordert Prozesse, um reagieren zu können, wenn sich etwas am Produkt verändert – und unterstützt damit auch IT-Verantwortliche, die heute schon ein stetes Monitoring ihrer IoT-Landschaft benötigen.

Wie solche Prozesse aussehen können, zeigt das eBook im Kapitel

„UL CYBERSECURITY ASSURANCE PROGRAM (CAP) UND DIE UL 2900 STANDARDS“

Eine Anwendung des UL 2900-Standards für industrielle Steuerungssysteme bietet schließlich das Kapitel

„CYBERSECURITY IN INDUSTRIELLEN STEUERUNGSSYSTEMEN (ICS)“



CYBERSECURITY UND KRITISCHE INFRASTRUKTUREN

Ein Schwerpunkt bei den Bemühungen zum Schutz vor Bedrohungen der Cybersicherheit liegt auf Unternehmen, die als Teil der kritischen Infrastruktur zu betrachten sind. Kritische Infrastruktur lässt sich wie folgt definieren:

“

IT-EINRICHTUNGEN, -NETZWERKE, -DIENSTE UND -INSTALLATIONEN, DEREN BESCHÄDIGUNG ODER ZERSTÖRUNG SCHWERWIEGENDE AUSWIRKUNGEN AUF DIE GESUNDHEIT, SICHERHEIT ODER DAS WIRTSCHAFTLICHE WOHLERGEHEN DER BEVÖLKERUNG UND DAS EFFIZIENTE FUNKTIONIEREN DER REGIERUNG UND BEHÖRDEN EINES LANDES HAT.⁽³⁾

“

(3) "ICS-CERT Fiscal Year 2015: Final Incident Response Statistics," ICS-CERT Monitor, published by the U.S. Department of Homeland Security, November/December 2015. Web. 8 August 2016. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2015_S508C.pdf.

Cybersecurity und kritische Infrastrukturen

Zu den Branchen, die am häufigsten als Teil der kritischen Infrastruktur bezeichnet werden, gehören Verteidigung, Energieerzeugung und -versorgung, Wassersysteme, Transport und Logistik, Finanzdienstleistungen, Gesundheitswesen und öffentliche Sicherheit.

Es liegt auf der Hand, dass die zur kritischen Infrastruktur zählenden Branchen aufgrund ihrer zentralen Rolle im Alltagsleben ein bevorzugtes Ziel für Cyberangriffe darstellen.

Schätzungen des Industrial Control System Cyber Emergency Response Team (ICS-CERT) des US-Heimatschutzministeriums (U.S. Department of Homeland Security) zufolge wurden im Jahr 2016 in den USA 290 Vorfälle gemeldet. ⁽⁴⁾

Mit jeweils ca. 20% aller gemeldeten Cyberangriffe waren Produktionsbetriebe (63 Vorfälle), der Kommunikationssektor (62 Vorfälle) und der Energiesektor (59 Vorfälle) am häufigsten betroffen. Spear Phishing war mit 26% die häufigste Art von Cyberangriffen. Zudem hatte das ICS-CERT Team es 2016 mit dem ersten bekannten Cyberangriff zu tun, der physische Auswirkungen auf ein Stromnetz hatte.

Aufgrund ihrer strategischen Bedeutung wird von Unternehmen, deren Geschäftsaktivitäten den Branchen innerhalb der kritischen Infrastruktur zuzurechnen sind, erwartet, dass sie vorgeschriebene oder empfohlene Cybersicherheitsanforderungen und -praktiken einhalten. So richtet sich beispielsweise in der Europäischen Union (EU) das Europäische Programm zum Schutz kritischer Infrastrukturen (European Programme for Critical

Infrastructure Protection, EPCIP) schwerpunktmäßig an Unternehmen, die Teil der kritischen Infrastruktur innerhalb der Transport- und Energiebranche sind. Das Programm definiert spezifische Anforderungen, die für die Unternehmen in diesen Branchen gelten.

Zu diesen Anforderungen gehört die Ausarbeitung eines Sicherheitsplans des Betreibers, der wichtige Infrastruktureinrichtungen identifiziert, eine detaillierte Gefahrenabschätzung auf der Grundlage von Schwachstellen der Einrichtungen umfasst und Gegenmaßnahmen zur Abwehr von Cyberbedrohungen enthält. In einigen EU-Mitgliedstaaten, darunter Deutschland, gelten für Unternehmen, die zur kritischen Infrastruktur zählen, noch zusätzliche Anforderungen an die Cybersicherheit.

(4) 2016 ICS-CERT report https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf.



Hacker-Angriffe auf kritische Infrastrukturen

In den vergangenen Jahren gab es eine Reihe bekannter Beispiele dafür, wie Schwachstellen in Software bei Unternehmen in den Branchen der kritischen Infrastruktur schwerwiegende Konsequenzen haben können:



Im Dezember 2015 haben Hacker in einem koordinierten Angriff die Umspannstationen von drei regionalen **Stromversorgern in der Ukraine** erfolgreich abgeschaltet, sodass Hunderttausende von Menschen keinen Strom hatten. Berichten zufolge übernahmen die Hacker via Fernzugriff die Kontrolle über die Rechner der Leittechnik der Umspannstationen. Dies erfolgte mithilfe von Remote Administration Tools auf Betriebssystemebene bzw. mit einer Client-Software für industrielle Fernsteuerungssysteme über die VPN (Virtual Private Network) Verbindungen ⁽⁵⁾ der Leittechnik.

(5) "Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure," issued by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of the U.S. Department of Homeland Security, February 25, 2016. Web. 8 August 2016. <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01>.

Im Oktober 2015 wurden Datensätze von etwa 15 Millionen Kunden entwendet, die bei **T-Mobile USA** einen Kredit beantragt hatten. Die Überprüfung der Kreditwürdigkeit von T-Mobile-Kunden wurde von **Experian** durchgeführt, der weltgrößten Agentur zur Überprüfung der Bonität privater Verbraucher. Berichten zufolge war es im Kreditinformations-Support-Portal des Unternehmens möglich, Anhänge zu Anträgen hochzuladen, ohne dass die Benutzer zuvor validierte Anmeldedaten angeben mussten. So konnten Hacker auf einfachem Weg Malware einschleusen ⁽⁶⁾.

(6) "At Experian, Security Attrition Amid Acquisitions," KrebsonSecurity blog posting, 8 October 2015. Web. 8 August 2016. <http://krebsonsecurity.com/tag/experian-breach/>.

Ende 2014 übernahmen Hacker die Kontrolle über Produktionsanlagen in einem **Stahlwerk in Deutschland** und manipulierten via Fernzugriff Steuerungssysteme, um die Abschaltung des Hochofens zu verhindern. Nach einem Bericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) haben sich die Hacker Zugriff auf das Softwarenetzwerk der Werksverwaltung verschafft und dann über diesen Zugang die Steuerung der Produktionsmanagement-Software des Werks übernommen. Berichten zufolge entstand dadurch ein erheblicher Schaden an der Infrastruktur des Werks ⁽⁷⁾.

(7) "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," Wired Magazine, January 8, 2015. Web. 8 August 2016. <https://www.wired.com/2015/01/german-steel-mill-hack-destruction/>.

FAKTOREN BEI DEN SCHWACHSTELLEN IN SOFTWARE-LIEFERKETTEN

Viele Unternehmen integrieren Software von Drittanbietern in Betriebssysteme oder Endprodukte mit unzureichend robuster Sicherheit und riskieren unwissentlich, dass diese gehackt oder anderweitig kompromittiert werden können. Drittanbieter-Software wird jedoch häufig nicht als Ursache für Cyberattacken erkannt.

Produktentwickler greifen vermehrt auf Standard-Softwarekomponenten zurück, um die Entwicklung eigener Software und Anwendungen zu beschleunigen. Dabei stammen die am meisten verwendeten Softwareprodukte, einschließlich Webservern, Internetbrowsern, Kommunikations- und Verschlüsselungsbibliotheken, von etablierten Software-Herstellern.

Auch wenn sich mit Softwarekomponenten von Drittanbietern die Produktivität bei den eigenen Entwicklungsbemühungen steigern und sogar eine bessere Produktqualität erzielen lassen, so haben ihr vermehrter Einsatz auch neue, höhere Cyberrisiken aufgeworfen und Unternehmen noch anfälliger gegenüber Cyberangriffen werden lassen.

Unternehmen benötigen geeignete Systeme und Verfahren zur Beurteilung und Kontrolle von Softwareprodukten, -komponenten und der Software-Lieferkette. Denn die Sicherheit von IoT Produkten ist nicht nur für Verbraucher von Bedeutung, sondern wird zunehmend zu einer Angelegenheit von nationalem Interesse.

Zu den spezifischen Risikofaktoren der Cybersicherheit im Zusammenhang mit der Software-Lieferkette zählen:

DOMINANZ VON DRITTANBIETER-SOFTWARE

Wie bereits erwähnt, sind Unternehmen überwiegend auf Softwareprodukte, -komponenten und -codes von Drittanbietern angewiesen, um ihre elementaren Geschäftsabläufe zu steuern und eine solche Software in ihre Endprodukte zu integrieren. Selbst Unternehmen, die proprietäre Softwareplattformen entwickeln oder betreiben, setzen oft auf Softwarekomponenten oder -codes von Drittanbietern, um die eigene Entwicklung zu beschleunigen und die Zuverlässigkeit zu erhöhen.

WACHSENDE ANZAHL VON HERSTELLERN VON DRITTANBIETER-SOFTWAREPRODUKTEN UND -KOMPONENTEN

Software-Lieferketten bilden in zunehmendem Maße traditionelle Lieferketten in ihrer Länge und in der Anzahl der beteiligten Lieferanten nach. Darüber hinaus gewinnen Anbieter von Software-as-a-Service (SaaS) Lösungen verstärkt an Bedeutung, da immer mehr Unternehmen ihre Infrastrukturkosten besser steuern wollen, indem sie kritische IT-Systeme auf Cloud-basierte Alternativen verlagern.

UNTERSCHIEDLICHE STUFEN DER SOFTWARE-QUALITÄTSKONTROLLE

Der verstärkte Einsatz von Drittanbieter-Software und SaaS-Anbietern führt folglich zu großen Unterschieden in der Qualität und Sicherheit der verfügbaren Softwareprodukte, Komponenten und Dienste. Da es für diese

Eigenschaften keine standardisierten Metriken gibt, müssen sich Unternehmen auf die Zusicherungen von Softwareanbietern verlassen oder ihre eigenen unabhängigen Bewertungsverfahren durchführen.

BEKANNTE UND UNBEKANNTE SCHWACHSTELLEN VON SOFTWARE

Laut einer Schätzung sind 97 Prozent der Vorfälle im Bereich der Cybersicherheit darauf zurückzuführen, dass es versäumt wurde, Schwachstellen in vorhandener Software oder vorhandenen Softwareanwendungen zu beheben⁽⁸⁾. In einer Software, die mehrere Komponenten von Drittanbietern enthält, kann sich dieses Risiko entsprechend rechnerisch erhöhen. Unberücksichtigt bleiben zudem auf dieser Ebene der Risikobewertung Schwachstellen, die sich erst dann identifizieren lassen, wenn die Software bereits freigegeben ist und im realen Praxiseinsatz angegriffen wird.

GEFÄLSCHTE SOFTWARE

Ebenso birgt der Einsatz von Drittanbieter-Software das Risiko, dass unwissentlich gefälschte Versionen authentifizierter Softwareprodukte oder -komponenten heruntergeladen oder verwendet werden. Gefälschte Software könnte Malware enthalten, die auf kritische Systemdaten zugreifen kann. Rechtmäßige Softwareanbieter befassen sich regelmäßig mit bekannten Schwachstellen, indem sie Patches bereitstellen, die Fälschern nicht zur Verfügung stehen.

UNZULÄNGLICHE PRAKTIKEN IM LIEFERANTEN-MANAGEMENT UND RISIKOMANAGEMENT

Zahlreiche Unternehmen sind nicht in der Lage, ausreichend robuste Programme und Praktiken für das Lieferantenmanagement und das Risikomanagement zu implementieren und beizubehalten, mit deren Hilfe potenzielle Gefahren für die Cybersicherheit erkannt werden können, die von den von Drittanbietern bezogenen Softwareprodukten und -komponenten ausgehen, oder mit denen die Fähigkeit eines Lieferanten beurteilt werden kann, schnell auf neu identifizierte Schwachstellen zu reagieren.

Diese Risikofaktoren unterstreichen umso mehr, wie wichtig es ist, die Software-Lieferkette auf Schwachstellen zu analysieren und Programme zu implementieren, mit denen sich die Cyber Risiken in Verbindung mit Software von Drittanbietern verringern lassen.

(8) "2016 Data Breach Investigation Report," Verizon, April 2016. Web. 8 August 2016. <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>.

MINIMIEREN VON SCHWACHSTELLEN IN DER SOFTWARE-LIEFERKETTE

Einleitung

Cybersecurity
und kritische
Infrastrukturen

Identifizierung von
Schwachstellen in der
Software-Lieferkette

Minimierung von
Schwachstellen in der
Software-Lieferkette

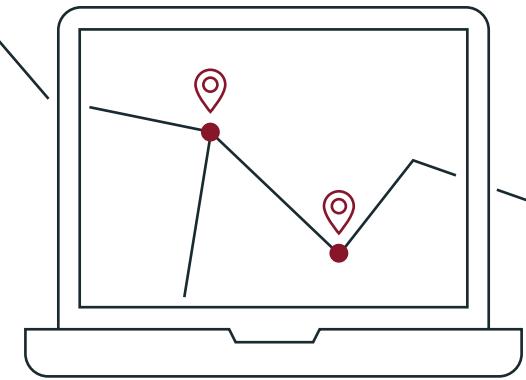
UL Cybersecurity
Assurance Program und
die UL 2900 Standards

Cybersecurity in
industriellen Steue-
rungssystemen (ICS)

Zusammenfassung

BEST PRACTICES ZUR MINIMIERUNG VON RISIKEN DER SOFTWARE-LIEFERKETTE

Jedes Unternehmen ist anders. Dennoch gibt es einige grundlegende Prinzipien und Best Practices, die universell anwendbar sind und mit denen sich Sicherheitsrisiken, die sich durch die Aktivitäten in der Software-Lieferkette ergeben, entschärfen lassen. Ein effektives Programm für das Management der Software-Lieferkette sollte auf jeden Fall folgende Bestandteile haben:



FORMALE SICHERHEITSVORGABEN

Die Ausarbeitung formaler Sicherheitsvorgaben und -anforderungen für alle Softwareprodukte und -komponenten von Drittanbietern. Diese Vorgaben sind durch entsprechenden Verweis in jede Ausschreibung und Lieferantenvereinbarung aufzunehmen.

AKTUALISIERUNGSVERFAHREN

Ein formelles Verfahren für das regelmäßige Aktualisieren von Softwareanwendungen und das Anwenden von Patch-Releases, um den Schutz vor neu identifizierten Bedrohungen sicherzustellen.

ZUGANGSBESCHRÄNKUNG

Ein nach dem Need-to-Know-Prinzip (Kenntnis nur bei Bedarf) beschränkter Zugang einzelner Softwareanbieter zu Informationen über die gesamte Softwarestrategie des Unternehmens oder aktuelle bzw. geplante Softwaresysteme.

PRÜFUNG NEUER LIEFERANTEN

Eine Due-Diligence-Prüfung neuer Lieferanten in der Software-Lieferkette, um zu ermitteln, ob sie über angemessene Sicherheitsvorkehrungen zur Minimierung von Cyberrisiken im Zusammenhang mit der Verwendung ihrer Software verfügen. Dazu zählen auch regelmäßige Follow-up-Audits.

SOFTWARE VALIDIERUNGSTESTS

Anfängliche und danach regelmäßige Validierungstests von Softwareprodukten und -komponenten zur Einhaltung der Sicherheitsanforderungen des Unternehmens. Wann immer möglich, sollten diese Tests automatisiert werden, um die mit dem menschlichen Eingreifen verbundenen Risiken zu verringern.

LIEFERANTENRICHTLINIEN

Klare Richtlinien für die Softwareanbieter mit eindeutig festgelegten Konsequenzen bei Nichteinhaltung der vorgeschriebenen Vorgaben oder der Verwendung gefälschter Softwareprodukte oder -komponenten.

BESCHAFFUNGSRICHTLINIE

Eine Beschaffungsrichtlinie, die eine unabhängige Validierung der Software von Drittanbietern auf einen ausreichenden Schutz vor Sicherheitsmängeln und -lücken für alle Softwareanwendungen fordert, um potenzielle Schwachstellen zu identifizieren, die zu einem Sicherheitsvorfall führen könnten.

TRACK&TRACE-PROGRAMME

Implementierung von Track&Trace-Programmen zur Erfassung und Überwachung der Quellen aller Softwareprodukte, -komponenten und -codes, um einen effizienten Zugriff auf Updates und Sicherheits-Patches zu ermöglichen und den laufenden Support von älteren Produkten sicherzustellen.

MITARBEITERSCHULUNG

Fortlaufende Schulung der Mitarbeiter zur Schärfung und Aufrechterhaltung des Bewusstseins für effektive Sicherheitspraktiken im Rahmen der Software-Lieferkette, die Auswahl von Softwareprodukten und -komponenten von Drittanbietern und die Überwachung von Softwaresystemen auf potenzielle Schwachstellen.

DAS UL CYBERSECURITY ASSURANCE PROGRAM (CAP) UND DIE NORMENREIHE UL 2900

Es gibt derzeit eine Reihe von Normen, die sich den wichtigsten Aspekten des Schutzes und der Sicherheit von netzwerkfähigen Produkten und Systemen widmen. Diese Normen können zwar bei der Beseitigung allgemeiner potenzieller Schwachstellen hilfreich sein, sie befassen sich jedoch nicht direkt mit den Cyberbedrohungen, die sich im Zusammenhang mit Software ergeben können. Zudem liefern diese Normen keine eindeutigen und objektiven Kriterien zur Beurteilung der tatsächlichen Wirksamkeit von Softwaredesign oder -funktionen, die auf die Software gerichtete Cyberangriffe verhindern sollen.

Mit Einführung seines Cybersecurity Assurance Program (CAP) will UL diese Lücke schließen. Das UL CAP verfolgt einen ganzheitlichen Ansatz zur Risikominimierung, der sowohl die produktspezifische als auch die systembedingte Immunität gegenüber Cyberbedrohungen beurteilt. Dieser Ansatz kann eine umfassendere Absicherung hinsichtlich der Sicherheit von Softwareprodukten und -komponenten von Drittanbietern bieten.

Ganzheitlicher Ansatz umfasst Produkte und Prozesse

Grundlage des UL CAP sind verschiedene UL-Prüfungsübersichten (UL Outlines of Investigations), die nachprüfbare Kriterien für die Bewertung von Schwachstellen der Cybersicherheit von netzwerkfähigen Produkten und Systemen liefern. Besonders die Normenreihe

UL 2900 „Standard for Software Cybersecurity of Network-Connectable Devices“ (Norm für Software-Cybersicherheit von netzwerkfähigen Geräten) ist auf eine Vielzahl miteinander verbundener Geräte und Systeme anwendbar.

NETZWERKFÄHIGE PRODUKTE UND SYSTEME

Industrielle Steuerungssysteme
Roboter
Medizinische Geräte
Automobile
Heizung/Klima
Beleuchtung
Smart Home
Hausgeräte
Alarmsysteme
Brandschutzsysteme
Gebäudeautomation
Intelligente Zähler

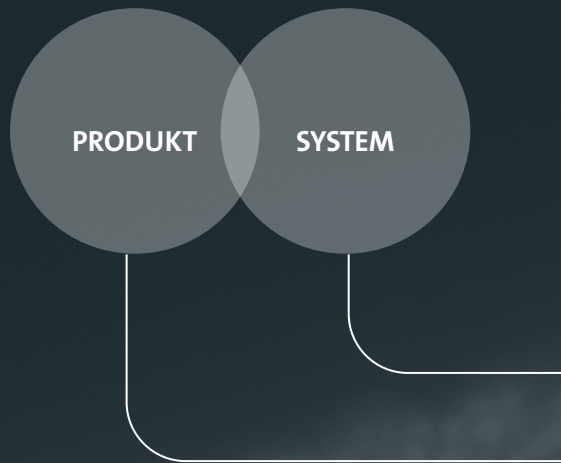
Die Normenreihe UL 2900 umfasst derzeit Normen in den folgenden Kategorien:



IHR VERNETZBARES PRODUKT UND/ODER SYSTEM

UL 2900 CAP LEISTUNGSSPEKTRUM

IHR BERICHT UND/ODER IHRE ZERTIFIZIERUNG



PRÜFUNG

Bewertung bestimmter Abschnitte der Norm oder der gesamten Norm.

- Fuzz Prüfung
- Bekannte Sicherheitslücken
- Code- und Binäranalyse
- Zugriffskontrolle und Authentifizierung
- Kryptografie
- Fernkommunikation
- Software-Updates
- Strukturierter Penetrationstest

BERATUNG

... zur Unterstützung der UL 2900

SCHULUNG

... für die Risikobewertung
(Threat Modeling, Risikobewertung, Quellcode-Analyse, Schwachstellenbewertung)

GAP-BEWERTUNG

... zur Einhaltung der UL 2900



DAS UL CYBERSECURITY ASSURANCE PROGRAM (CAP) UND DIE NORMENREIHE UL 2900

UL 2900-1

ALLGEMEINE PRODUKTANFORDERUNGEN

Die Normen in dieser Kategorie umfassen UL 2900-1, Prüfungsübersicht für Software-Cybersicherheit von netzwerkfähigen Produkten, Teil 1: Allgemeine Anforderungen. Die Norm UL 2900-1 bewertet Software auf das Vorhandensein von Kontrollvorrichtungen für Sicherheitsrisiken in ihrer Architektur und ihrem Design und verwendet vorgeschriebene Testmethoden, um Schwachstellen, Softwaremängel und Malware zu bewerten.

UL 2900-2

BRANCHENSPEZIFISCHE ANFORDERUNGEN

Die Normen in der Kategorie Software-Cybersicherheit von netzwerkfähigen Produkten umfasst drei Teile: Teil 2-1: Besondere Anforderungen für netzwerkfähige Komponenten von Gesundheitssystemen, Teil 2-2: Besondere Anforderungen für industrielle Steuerungssysteme, Teil 2-3: Besondere Anforderungen für Signal- und Sicherheitstechnik für Hersteller, Eigentümer und Integratoren. Diese Normen bewerten Schwachstellen von Software, die netzwerkfähigen Geräte und Systeme eingesetzt werden. Weitere Normen für diese Kategorie sind in Entwicklung.

UL 2900-3

ALLGEMEINE PROZESSANFORDERUNGEN

Die Norm UL 2900-3 wird derzeit noch entwickelt, Prüfungsübersicht für Softwaresicherheit von netzwerkfähigen Produkten, Teil 3: Allgemeine Anforderungen. Berücksichtigung finden sollen in dieser Normenreihe die allgemeinen Tests von organisatorischen Systemen und Prozessen für die Durchführung der Risikobewertung, die zur Ermittlung möglicher softwarebasierter Cyberbedrohungen erforderlich ist, und die Fähigkeit von Teams, Sicherheitsaspekte in den Produktentwicklungsprozess einfließen zu lassen.

Zusammengefasst bietet die UL 2900 Normenreihe einen effektiven und effizienten Rahmen für die Beurteilung des Gesamtkonzepts eines Unternehmens für die Softwaresicherheit sowie der spezifischen Schwachstellen einzelner Softwareprodukte und -komponenten von Drittanbietern. Die Normenreihe bietet damit Unternehmen die erforderlichen Kriterien zur Messung und Bewertung der Sicherheitsmerkmale von Produkten, der eingesetzten Technologien und des Risikos, dass Schwachstellen ausgenutzt werden könnten.

WIE UL CAP DIE CYBERSECURITY IN INDUSTRIELLEN STEUERUNGSSYSTEMEN (ICS) SICHERT

Hersteller oder Anlageneigentümer können Cyberrisiken minimieren, indem sie Steuerungssysteme verwenden, die gemäß IEC 62443 oder UL 2900 -2-2 getestet und zertifiziert sind. Die neue Norm UL 2900-2-2 bietet im Rahmen des UL Cybersecurity Assurance Programms (UL CAP) nachprüfbare Kriterien für die Cybersicherheit, mit denen Softwareschwachstellen beurteilt, deren Ausnutzbarkeit minimiert, bekannte Schadsoftware bekämpft, Sicherheitsmechanismen überprüft und allgemein das Sicherheitsbewusstsein gesteigert werden kann.

Die UL Cybersecurity Lösungen tragen zur Transparenz und Validierung der Komponenten von Zulieferern bei. Denn Cybersecurity beginnt auf der Komponentenebene. Mit seinen sofort anwendbaren, skalierbaren Cybersecurity Beratungs-, Test- und Zertifizierungslösungen kann UL Herstellern oder Systemintegratoren von Industrie-

steuersystemen (ICS) dabei helfen, ihre Cyber-Bereitschaft – sowohl hinsichtlich ihrer organisatorischen Sicherheitspraktiken als auch ihrer Systemsicherheit – zu demonstrieren.

UL CAP bietet vertrauenswürdige, neutrale Unterstützung und die Möglichkeit, die Sicherheit von Produkten, die an das Netzwerk und die Systeme angeschlossen werden, wie auch von Anbieterprozessen für die Entwicklung und Pflege von Produkten und Systemen im Hinblick auf ihre Sicherheit zu bewerten. Das Programm unterstützt Unternehmen dabei, den steigenden Anforderungen des Marktes gerecht zu werden.

Unternehmen können aus folgenden UL CAP-Dienstleistungen für Fabrikautomations- und Industriesteuerungssysteme auswählen:

Prüfung von Sicherheitskriterien auf Basis der Norm UL 2900-2-2 für Cybersicherheit oder anhand spezifizierter Anforderungen

Prüfung mit dem Ziel der Zertifizierung nach der Norm UL 2900-2-2 für Cybersicherheit

Beurteilung und Risikobewertung von Lieferantenprozessen für die Entwicklung und Aufrechterhaltung von Sicherheitsprodukten und -systemen

Schulung des Sicherheitsbewusstseins bei der Produktentwicklung und bei der Beschaffung von Komponenten bei Drittanbietern

Wie UL CAP die Cybersecurity in industriellen Steuerungssystemen (ICS) sichert

Unternehmen können Cyberrisiken in neuen oder nachgerüsteten Systemen durch das Testen oder Zertifizieren nach IEC 62443 oder UL 2900-2-2 Standard reduzieren. Zur Prüfung und Validierung der

Cybersicherheit ist UL 2900-2-2 dafür vorgesehen, die Sicherheitskriterien der IEC 62443 auf Produkte und Systeme anzuwenden. Grundlage der Messungen sind Metriken der Sicherheitstechnik.

Maßgeschneiderte Produktprüfung und Zertifizierung



Leistungen

Zertifizierung

Certificate of
Compliance nach
UL 2900-2-2
und/oder
IEC 62443

Testreport

Basierend auf
ausgewählten oder allen
UL 2900-2-2 / IEC 62443
Kriterien oder auf
kundenspezifischen
Kriterien

Beratung

Über den UL 2900
Standard für industrielle
Steuerungssysteme (ICS)
und/oder den IEC 62443
Standard

Warum UL

Die skalierbaren UL Beratungs-, Prüf- und Zertifizierungslösungen für Cyber-Sicherheit helfen dabei, eine Markendifferenzierung zu schaffen und die Präferenz Ihrer Produkte zu steigern.

UL's Cybersecurity Know-How und Integrität unterstützen Sie dabei, Transparenz und Sicherheit in der Lieferkette zu erlangen und für eine sichere und widerstandsfähige Betriebsumgebung zu sorgen.

ZUSAMMENFASSUNG UND FAZIT

Das Internet der Dinge, zu dem auch ganze Fabriken mit ihren digitalisierten, vernetzten Produktionsprozessen und cyber-physischen Systemen gehören, ist einer steigenden Gefahr von Cyberangriffen ausgesetzt, die sowohl Komponenten und Produkte als auch Software, Prozesse und Infrastrukturen betrifft. Diese Angriffe werden auch andere Konzepte gefährden – von der Smart Factory hin zum Smart Home und zur Smart City. All diese Bereiche werden so umfassend vernetzt, dass sowohl Hersteller als auch Integratoren gefordert sind, Sicherheit von Grund auf zu betrachten.

Folglich ist es für Unternehmen extrem wichtig, robuste Strategien für das Risikomanagement aufzustellen und aufrechtzuerhalten, mit denen sie ihre Anfälligkeit gegenüber potenziellen Cyberbedrohungen aus der Software- oder Komponenten-Lieferkette verringern können. Mit solchen Strategien und wirksamen Abwehrmechanismen lassen sich ungeplante Ausfallzeiten von unternehmenskritischen Prozessen, der Verlust oder die Kompromittierung geschützter Daten sowie potenzielle Schäden an anderen Assets eindämmen.

Das UL Cybersecurity Assurance Program (CAP) und die Normenreihe UL 2900 basieren auf der umfassenden Erfahrung von UL in der Sicherheitswissenschaft, Normenentwicklung, Prüfung und Zertifizierung auf. Mit beiden Bausteinen lassen sich die Cyberrisiken verringern. Sie bilden einen Rahmen, in dem Unternehmen im Bereich der für sie kritischen Infrastruktur Sicherheitskriterien für Komponenten, Produkte, Software und Prozesse festlegen und überprüfen können. Zudem bietet das UL CAP einen effektiven Ansatz zur Verbesserung der gesamten „Cyberhygiene“ über sämtliche Aktivitäten innerhalb der Lieferkette hinweg.



<

UL International Germany GmbH
Admiral-Rosendahl-Strasse 9
63263 Neu-Isenburg

Telefon: +49.69.489810.0
Fax: +49.69.489810.161
E-Mail: CustomerService.de@ul.com

Germany.UL.com/Industrie-4.0
UL.com