IBM Rational-Sicherheitslösungen für Energieversorgungsunternehmen

Anwendungssicherheit zur Vermeidung von Risiken und zur Einhaltung gesetzlicher Bestimmungen bei Energieversorgern, die mit Smart Grid-Lösungen arbeiten

Highlights

- Hilfestellung für Energieversorgungsunternehmen beim Test von Software aus mehreren Quellen auf Schwachstellen
- Zeit- und Kostenersparnis durch die möglichst frühzeitige Vermeidung von Schwachstellen im Software Delivery Life Cycle (SDLC)
- Entlastung bei Nachweisen zur Einhaltung von NERCCIP-Richtlinien bei Analysen über Sicherheitslücken bei Internetverbindungen

Auf Energieversorgungsunternehmen kommen derzeit neue Chancen aber auch Herausforderungen zu. Sie müssen die Anforderungen im Zusammenhang mit der Einführung einer Advanced Metering Infrastructure (AMI), Home Area Network-Geräten (HAN), Technologien zur Automatisierung von Stromnetzen, der dezentralen Stromerzeugung und Elektrofahrzeugen erfüllen und gleichzeitig weiterhin eine zuverlässige und hochwertige Stromversorgung sicherstellen. Energieversorger müssen Wege finden, um die Zuverlässigkeit und Sicherheit der vorhandenen Systeme aufrechtzuerhalten und dabei die nächste Generation interaktiv gestalteter (und damit risikobehafteter) Lösungen entwickeln – und zwar sowohl für Privatverbraucher als auch für gewerbliche Kunden. IBM Rational-Software bietet die nötigen Tools für die Entwicklung dieser neuen Anwendungen und trägt außerdem zur Vermeidung von Sicherheitsrisiken bei.

Die meisten Energieversorgungsunternehmen arbeiten mit Softwareprodukten unterschiedlicher Anbieter, sodass es schwierig ist, bei Sicherheitsrisiken stets den Überblick zu behalten. Zu diesen Anbietern gehören z. B.:

- **Interne Entwicklungsteams:** Interne Teams müssen häufig komplizierte Aufgabenstellungen mit engen Terminen erfüllen und zahlreichen kritischen Anforderungen gerecht werden. Das bedeutet, dass dem Thema Sicherheit möglicherweise nicht die nötige Beachtung geschenkt wird. Das Sicherheitsdenken ist zudem im Entwicklungsbereich teilweise neu, denn traditionell haben Energieversorger nur wenig in umfassende Initiativen zur Softwareentwicklung investiert. Systemintegratoren zeigen bei der Zusammenarbeit mit Energieversorgern zudem häufig nicht alle Details zu den Grundlagen von Grid-Anwendungen.

- **Anbieter von Standardanwendungen:** COTS-Anwendungen (Commercial off the Shelf) oder Standardanwendungen sind ein wesentlicher Bestandteil in den Infrastrukturen vieler Energieversorgungsunternehmen. Diese Anwendungen wurden jedoch entwickelt, um die Standards der Anbieter zu erfüllen und nicht die branchenspezifischen Standards von Energieversorgungsunternehmen.
- **Externe Entwicklungsteams:** Durch die Auslagerung der Entwicklung können Anbieter auf einen größeren Kreis qualifizierter Fachleute zurückgreifen und möglicherweise Kosteneinsparungen erzielen. Damit die erforderlichen Ergebnisse erreicht werden, müssen allerdings detaillierte Erläuterungen zu den erwarteten Sicherheits-Entwicklungsstandards zur Verfügung gestellt werden.
- **Kostenlose und Open-Source-Software:** Diese Angebote können kostengünstig sein, werden allerdings von Benutzergruppen entwickelt, die möglicherweise nicht die Bestimmungen und Standards erfüllen, die in den Energieversorgungsunternehmen gelten, die mit den Lösungen arbeiten möchten.

Vermeidung von Sicherheitslücken

Es wäre ideal, wenn die gesamte, in Ihren Anwendungen verwendete Software im Rahmen eines sicheren Software Development Life Cycle (SDLC) entwickelt und getestet würde. Dies ist jedoch nur selten der Fall. Zudem unterscheiden sich die Sicherheitsanforderungen der einzelnen Branchen und die jeweils bewährten Verfahren können nicht auf alle Branchen übertragen werden. Angesichts der Tatsache, dass neue Smart Grids auf der Grundlage von Milliarden von Softwarezeilen entwickelt werden, ist es schwer zu bestimmen, ob der gesamte Code umfassend im Hinblick auf die Sicherheit geprüft wurde. Unglücklicherweise beweisen Hacker in regelmäßigen Abständen, dass sie in der Lage sind, Sicherheitskontrollen zu umgehen, indem sie nach Sicherheitslücken in der Software suchen und diese ausnutzen.

Einhaltung der NERC-Bestimmungen

Die CIP-Bestimmung 007 (Critical Infrastructure Protection) der North American Electric Reliability Corporation (NERC) verlangt, dass jährliche Untersuchungen nach Sicherheitslücken stattfinden. Außerdem ist festgelegt, dass Energieversorgungsunternehmen „die Ergebnisse der Untersuchung, den Aktionsplan zur Fehlerbehebung oder Beseitigung von Sicherheitslücken, die während der Untersuchung erkannt wurden, und den Status bei der Umsetzung dieses Aktionsplans dokumentieren müssen“.[1] In künftigen Versionen der CIP-Bestimmungen werden vermutlich noch häufigere Untersuchungen gefordert, die einen wesentlich größeren Teil der Versorgungssysteme betreffen. Eine einheitliche und kostengünstige Durchführung dieser Untersuchungen ist enorm aufwendig. Automatisierte Lösungen können hier für Entlastung sorgen.

Erfüllung der NIST-Richtlinien

Nach jahrelanger Arbeit durch Mitarbeiter aus Industrie, Behörden und Wissenschaft stellte das National Institute for Standards and Technology (NIST) im September 2010 Version 1.0 der „NISTIR 7628: Guidelines for Smart Grid Cyber Security“[2] vor. Sie enthält Anleitungen, um Systeme auf Anwendungsebene von Sicherheitslücken und Designfehlern zu befreien, von denen mehrere explizit aufgeführt sind. Beispiele:

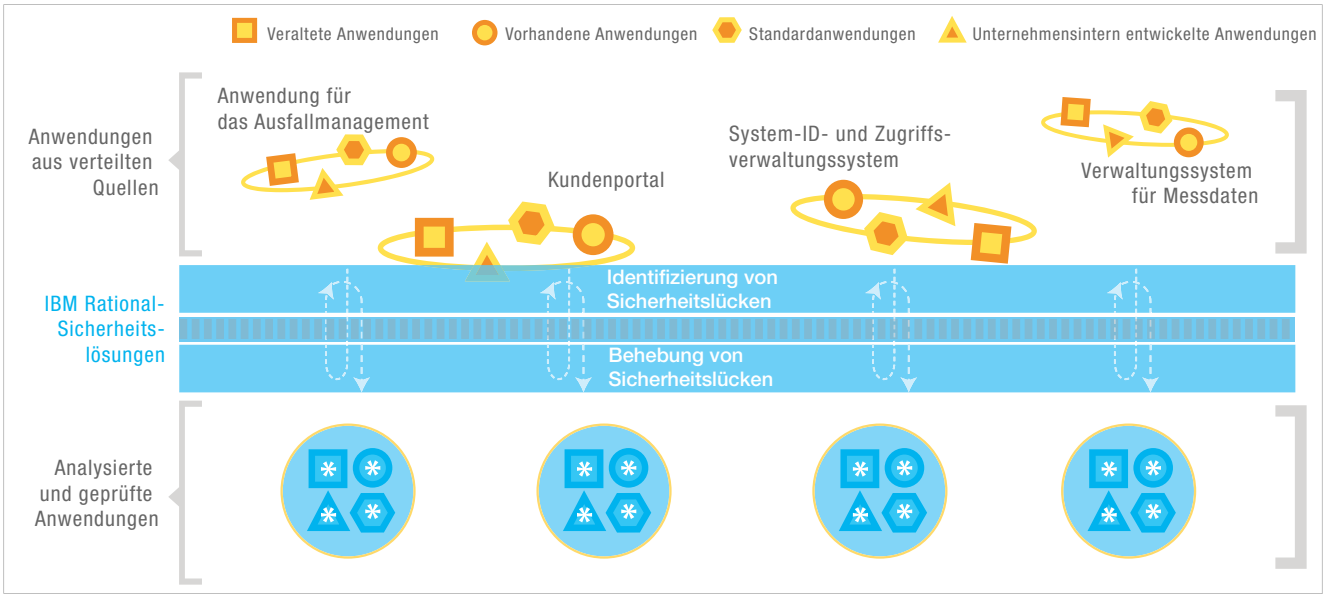
- Ein- und Ausgabeprüfung
- Sicherheitslücken bei der Autorisierung
- Sicherheitslücken bei Kennwörtern und bei der Kennwortverwaltung
- Fehlerbearbeitung
- Sicherheitslücken und Schwachstellen bei der Verschlüsselung
- Probleme bei der Protokollierung und Überwachung

… und vieles mehr

Es ist ungewiss, wie schnell diese Richtlinien in Compliance-Vorschriften von Energieversorgungsunternehmen übernommen werden. Da NISTIR 7628 in den USA jedoch auf große Akzeptanz gestoßen ist (sowohl bei öffentlichen Versorgungseinrichtungen als auch international), sollten sich Energieversorger auf die Umsetzung der Richtlinien vorbereiten.

Kontrolle der Entwicklungskosten

Wenn Ihr Unternehmen die betreffenden Anwendungen intern entwickelt, empfiehlt es sich, Schwachstellen bereits frühzeitig im Entwicklungszyklus zu beseitigen, um das nötige Maß an Sicherheit zu gewährleisten und die Entwicklungskosten zu reduzieren. Durch die Analyse der Anwendungen in der Entwicklungsphase lassen sich Sicherheitslücken am besten ausschließen, sowie spätere Beurteilungen und der Berichtsprozess vereinfachen.



Eine Lösung von IBM Rational-Software

IBM bietet eine Kombination aus Produkten und Services, auf deren Grundlage Ihr Unternehmen das Sicherheitsniveau verbessern und die Entwicklungskosten senken kann:

IBM Rational AppScan Standard Edition

Mit der IBM Rational AppScan Standard Edition können Sie Anwendungen und weborientierte Systeme schnell auf Sicherheitslücken und Konfigurationsfehler prüfen. Wenn Sie ein neues Kundenportal kaufen oder entwickeln, bieten die Funktionen zur Analyse von Webanwendungen der Rational-Software die Möglichkeit, die damit verbundenen Sicherheitsrisiken zu verringern.

IBM Rational AppScan Source Edition

Analysieren Sie den Quellcode frühzeitig im Software Delivery Life Cycle (SDLC), um Sicherheitslücken schnell zu erkennen. Mit der Rational AppScan Source Edition können Sie Sicherheitslücken lange vor der Freigabe der Software identifizieren und beseitigen. Durch die automatische Zuordnung von Analysen, Auswahl und Schwachstellen im Rahmen des Buildprozesses sparen Sie zudem Zeit.

IBM Rational AppScan Enterprise Edition

Schaffen Sie die Grundlagen für die Generierung unternehmensweiter Berichte für das höhere Management, Auditoren und andere wesentliche Beteiligten. Die Verbesserung des Sicherheitsniveaus ist eine Sache, der Nachweis, dass Ihr Unternehmen alle erforderlichen Maßnahmen ergriffen hat, ist eine andere. Dank der automatisierten Berichtsfunktionen der Rational AppScan Enterprise Edition verringert sich der Zeitaufwand für die Erstellung von Berichten, sodass sich Ihre Mitarbeiter mehr auf Anwendungen, Systeme und Kundenservice konzentrieren können.

IBM Rational Professional Services

Entwickeln Sie Prozesse im Hinblick auf aktuelle und künftige NERC-Compliance-Anforderungen. Rational-Sicherheitsexperten konzipieren und erarbeiten gemeinsam mit Ihnen einen individuellen Aktionsplan zur Beseitigung von Schwachstellen, der die Bestimmungen der NERC und anderer Standards erfüllt.

Bewährte Verfahren

Energieversorgungsunternehmen müssen einige Punkte beachten, wenn sie ein Programm zur Anwendungssicherheit auf den Weg bringen. Als Leitfaden bieten sich hierbei Erfahrungswerte aus anderen Branchen an. Zu den ersten Schritten gehören folgende:

- Ermitteln Sie über zentrale Systeme zur Ressourcenerkennung und -verwaltung, welche Anwendungen vorliegen.
- Etablieren Sie als Einstieg Richtlinien, die erläutern, wie Ihr Unternehmen den Software Delivery Life Cycle (SDLC) gewährleistet.
- Priorisieren Sie Anwendungen nach ihrer Bedeutung für das Unternehmen und nach Sicherheitsrisiken, und teilen Sie die ermittelten Schwachstellen so ein, dass die dringendsten zuerst beseitigt werden.
- Nehmen Sie Zielsetzungen und Voraussetzungen in puncto Anwendungssicherheit in Finanzierungsmaßnahmen und -entscheidungen auf.

Anwendungsfälle

Energieversorger in den USA und anderen Ländern erkennen inzwischen, dass die Implementierung und Verknüpfung software-orientierter Systeme mit Risiken behaftet ist. Viele Unternehmen haben hierauf reagiert, indem sie neue Sicherheitsrichtlinien, neue Mitarbeiterschulungen und Initiativen zur Stärkung des Bewusstseins auf den Weg brachten. Mithilfe ausgewählter Tools sollen an wichtigen Terminen darüber hinaus automatisch Sicherheitstests durchgeführt werden. Im Folgenden sind einige Anwendungsfälle aufgeführt:

- Verwendung von Tools zur Identifizierung und Beseitigung kritischer Sicherheitslücken in öffentlichen Anwendungen, z. B. neuen Smart Grid-Kundenportalen
- Durchführung von Sicherheitsanalysen für AMI-Komponenten auf Web- und Quellcode-Ebene
- Durchführung von Sicherheitstests für den Code vor der Freigabe durch Anbieter intelligenter Messgeräte

Ein wichtiger Bestandteil der IBM „Secure by Design"-Initiative

IBM bietet im Rahmen des Software-Frameworks SAFE (Solutions Architecture for Energy) und der „Secure by Design"-Initiative drei primäre Komponenten an, die für die Erstellung und Verwaltung einer sicheren Infrastruktur von entscheidender Bedeutung sind. Dies umfasst z. B. Fachwissen zu Sicherheitsrisiken und -lücken , strukturelle Elemente und kontinuierliche Überprüfungen. In puncto Anwendungssicherheit generieren intelligente Messgeräte und andere Sensoren zur Automatisierung der Versorgungsnetze täglich eine enorme Menge an (häufig sensiblen) Daten, während die Funktionen der Rational AppScan-Softwarefamilie zentral ausgeführt werden. Weitere wichtige und zugehörige IBM Tools und Services:

- Rational Development Lifecycle-Tools für die Fehlerüberwachung und die Quellcodekontrolle sowie Tools zur Bestandskontrolle Ihrer Anwendungen und die Umsetzung Ihrer Sicherheitsrichtlinien
- IBM InfoSphere Optim-Software für die Datenverwaltung und IBM InfoSphere Guardium-Software für die Datensicherheit
- IBM Tivoli IAM-Lösungen (Identity and Access Management)
- IBM WebSphere Data Power für die Sicherheit von Web-Services
- IBM Proventia-Firewalls auf Netzwerk- und Anwendungsebene
- IBM Emergency Response Services (ERS)

Fazit

Energieversorgungsunternehmen müssen derzeit viele sicherheitsspezifische Herausforderungen bewältigen. In der Vergangenheit waren ihre Systeme teilweise dadurch geschützt, dass sie von anderen Systemen isoliert waren. Die Vorteile eines Smart Grids, einer Advanced Metering Infrastructure (AMI) und von Projekten zur Automatisierung von Versorgungsnetzen lassen sich allerdings am besten durch die vollständige Integration und Verknüpfung der IT mit den zugehörigen Prozessen erreichen – sowie durch vertrauenswürdige, zuverlässige und sichere Kommunikationswege mit dem Kunden. Diese bisher nicht vorhandenen Zugriffsmöglichkeiten und Verbindungen müssen über neue Sicherheitskontrollen und -richtlinien verwaltet werden, die zum allergrößten Teil in Softwareprodukte implementiert wurden.

Mit den Sicherheitslösungen von IBM Rational-Software erhalten Energieversorgungsunternehmen bessere Erkenntnisse über die Sicherheitsrisiken ihrer Anwendungen und anderer Softwareressourcen. Sie sparen dadurch wertvolle Zeit und Geld, können fundiertere Entscheidungen im Hinblick auf die Einhaltung gesetzlicher Bestimmungen treffen und bleiben vor Hackerangriffen geschützt.

Weitere Informationen

Wenn Sie mehr über Sicherheitslösungen für Energie- und Versorgungsunternehmen erfahren möchten, wenden Sie sich bitte an den zuständigen IBM Ansprechpartner oder IBM Business Partner, oder besuchen Sie uns unter: **ibm.com**/software/rational/offerings/websecurity/?S_TACT=105AGX23&S_CMP=HP

Finanzierungslösungen von IBM Global Financing bieten Möglichkeiten wie effektive Finanzdisposition, Schutz vor überalterter Technologie, Reduzierung der Gesamtbetriebskosten und einen höheren Return-on-Investment. Zudem helfen unsere Global Asset Recovery Services dabei, durch neue energieeffizientere Lösungen auch dem Umweltschutz Rechnung zu tragen. Weitere Informationen zu IBM Global Financing finden Sie unter: **ibm.com**/financing

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

[1] North American Electric Reliability Corporation, *Standard CIP-007-3 – Cyber Security – Systems Security Management*, 16. Dezember 2009, http://www.nerc.com/files/CIP-007-3.pdf

[2] National Institute of Standards and Technology Interoperability Report (NISTIR) 7628 – *Guidelines for Smart Grid Cyber Security*, *Volume 3*, August 2010, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf