Security Patch Management in Großunternehmen

Lukas Braune · Manuel Ifland · Klaus Lukas

Siemens AG
{lukas.braune | manuel.ifland | lukas}@siemens.com

Zusammenfassung

Aufgrund von Anforderungen aus Cyber-Security-Standards werden Unternehmen immer mehr in die Pflicht genommen, für ihre Produkte und Lösungen einen umfangreichen Patch Management Prozess zum Behandeln von Security-Schwachstellen in kommerziellen sowie Open-Source-Komponenten von Drittanbietern umzusetzen. Für Produkthersteller ist Beschaffung von Informationen über vorhandene Patches für Komponenten von Drittanbietern dabei ein wichtiges Element. Dies stellt vor allem in Großunternehmen eine organisatorische sowie technische Herausforderung dar, insbesondere aufgrund verteilter Produktentwicklungen, inhomogener Kundenanforderungen und einer Vielzahl an unterschiedlichsten Komponenten. Ein permanentes Beobachten der Informationen über Security-Schwachstellen aller verbauten Komponenten von Drittanbietern ist für Produktverantwortliche mit sehr viel Aufwand verbunden. Als Lösung wird daher ein zentralisierter Monitoring-Ansatz in Kombination mit der Integration der Informationen in bestehende Workflow-Systeme vorgestellt. Dies erlaubt einen effizienten Einsatz auf breiter Basis. In dem vorliegenden Artikel beschreiben die Autoren ihre gesammelten Erfahrungen beim Aufbau sowie Betrieb eines unternehmensweiten Monitoring-Dienstes am Beispiel der Siemens AG. Der Artikel geht auf die Probleme und Herausforderungen ein und beleuchtet auf der anderen Seite deren Lösungsmöglichkeiten.

1 Was ist Security Patch Management?

In Produkten, Lösungen und Dienstleistungen (im Folgenden übergreifend „Produkt“ genannt) werden zunehmend Komponenten von Drittanbietern verbaut. Es handelt sich hierbei um sogenannte OEM (Original Equipment Manufacturer)-Komponenten, d. h. bereits entwickelte und am Markt verfügbare Software oder Hardware anderer Hersteller. Dies beinhaltet sowohl Open Source als auch kommerzielle Komponenten. Der Einsatz derartiger OEM-Komponenten ist eine gebräuchliche Methode, um den Entwicklungsaufwand bei komplexen Projekten deutlich zu reduzieren. Allerdings unterliegen auch OEM-Komponenten aufkommenden Security-Schwachstellen. Diese Security-Schwachstellen in den OEM-Komponenten können schwerwiegende Auswirkungen auf das gesamte Produkt und dessen Betrieb haben. Während beim klassischen Patch Management i. A. Fehler behoben werden, zielt das Security Patch Management spezifisch auf Sicherheitsfunktionalitäten ab, die einen sicheren Betrieb im Rahmen der IT-Sicherheit gefährden können. Beim Security Patch Management spielt vor allem die Zeit, d. h. die schnelle Reaktion auf Security-Schwachstellen, eine wichtige Rolle, da zu öffentlich bekannten Security-Schwachstellen häufig auch Exploits zeitnah verfügbar werden. Exploits sind Programme, die benutzt werden, um eine Security-Schwachstelle auszunutzen. Produkte sowie Endkunden, die diese OEM-Komponenten einsetzen, sind damit potenziell gefährdet, bis

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 25-35.

durch das Einspielen eines Patches die Security-Schwachstelle geschlossen wird. Dafür benötigt der Produkthersteller im Rahmen des Prozesses für Security Patch Management allerdings zeitnah Informationen über vorhandene Patches für OEM-Komponenten um eine Bewertung über die Auswirkung durchführen zu können. Der Security Patch für die OEM-Komponente kann dann dem Endkunden zur Verfügung gestellt werden, so dass ein schnelles Patchen möglich ist. Selbstverständlich funktioniert das nur, solange vom Hersteller der OEM-Komponente Security Patches bereitgestellt werden. Beispielweise wurde der Support für Microsoft Windows XP seitens Microsoft am 14. April 2014 offiziell eingestellt[1]. Wie damit umgegangen wird, wenn ein Hersteller einer OEM-Komponente keine Security Patches mehr liefert, erfordert eine gesonderte Betrachtung und ist nicht Teil dieser Veröffentlichung. Bei der Behebung von Security-Schwachstellen werden ggf. auch Änderungen an Funktionalitäten notwendig, auf die jedoch im Weiteren nicht spezifisch eingegangen wird. Eine weitere große Herausforderung stellt ferner das Ausrollen eines Security Patches innerhalb einer Anlage sowohl für eine einzelne Baugruppe als auch für die gesamte Anlage dar. Speziell bei Safety-relevanten Umgebungen, bei denen Ablauf- und Ausfallsicherheit eine übergeordnete Rolle spielen, sowie bei Zertifizierungen/Abnahmen in der Pharmaindustrie oder in der Verkehrstechnik, muss Security Patch Management in enger Abstimmung mit dem Kunden und den betrieblichen Anforderungen erfolgen, so dass Safety-Nachweise erhalten bleiben. Diese Anlagen haben oft auch im Bereich Netzwerk- und physischer Sicherheit erweiterte Schutzmechanismen, die bei der Reaktionszeit auf Security-Schwachstellen mit berücksichtigt werden müssen. Bei der vorliegenden Veröffentlichung geht es ausschließlich um die Informationsbeschaffung- und Verteilung im Bezug auf Security-Schwachstellen in OEM-Komponenten aus Sicht des Produktlieferanten.

2 Motivation und Herausforderungen

Für IT-Unternehmen und Technologiekonzerne mit komplexen Produkten im Portfolio ist es in vielerlei Hinsicht von Vorteil, wenn nicht die komplette Produktfunktionalität selbst entwickelt wird, sondern sich auf die Kernfunktionalität konzentriert werden kann. Auf der einen Seite können damit der Aufwand sowie die Kosten für die Entwicklung reduziert werden, weil bestimmte Grundfunktionen bereits durch auf dem Markt verfügbare OEM-Komponenten anderer Hersteller abgedeckt werden. Selbstverständlich entstehen hierfür in der Regel Kosten für Lizenzen, diese liegen allerdings deutlich unter denen für eine Eigenentwicklung der gleichen gewünschten Funktionalität. Auf der anderen Seite gelingt es auf diese Weise die Fehleranfälligkeit zu reduzieren, wenn weit verbreitete und ausgiebig getestete OEM-Komponenten eingesetzt werden. Im Übrigen können bei Problemen bei Integration oder Betrieb auch die entsprechenden Hersteller der OEM-Komponenten mit einbezogen werden. Als Beispiel benötigt heutzutage so gut wie jede Applikation mit komplexerem Funktionsumfang eine Datenbank, in der unter anderem Prozess- oder Logging-Daten gespeichert werden. Für einen Hersteller einer derartigen Applikation macht es in der heutigen Zeit wenig Sinn, die Datenbanksoftware im Rahmen der Applikationsentwicklung selbst zu entwickeln, insbesondere, da auf dem Markt bereits verschiedenste ausgereifte Datenbankprodukte anderer Hersteller existieren. Die durch den Einsatz einer Datenbank in Form einer OEM-Komponente eines anderen Herstellers gewonnene Zeit kann wiederum in die Entwicklung der Kernfunktionalität investiert werden. Weitere Beispiele für häufig eingesetzte OEM-Komponenten im Rahmen von Produkten sind unter anderem Betriebssysteme, Webserver oder Bibliotheken mit spezifischer Funktionalität. So wie

[1] Windows XP support has ended http://windows.microsoft.com/en-us/windows/end-support-help

auf der einen Seite durch den Einsatz von OEM-Komponenten Zeit und Fehleranfälligkeit reduziert werden können, entstehen auf der anderen Seite allerdings neue Herausforderungen.

2.1 Security-Schwachstellen in OEM-Komponenten

Eine Tatsache ist, dass OEM-Komponenten – wie alle Software-Komponenten – früher oder später Security-Schwachstellen aufweisen können, die den Betrieb beeinträchtigen. Hiermit sind Schwachstellen gemeint, die von Angreifern entweder über das Netzwerk oder lokal ausgenutzt werden können, um Funktionalitäten zu beeinflussen oder gar zu schädigen. Am Ende kommt es nicht selten zur Beeinträchtigung der Informationssicherheit wodurch die wichtigen Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität nicht mehr gewährleistet werden können. Security-Schwachstellen werden heutzutage im Allgemeinen weltweit eindeutig durch sog. Common Vulnerabilities and Exposures (CVE)[2] Nummern der MITRE Corporation identifiziert. CVE-Nummern haben das Format *CVE-YYYY-NNNN*, wobei *YYYY* für das Jahr der Nummer und *NNNN* für eine natürliche Zahl steht. Genutzt werden CVE-Nummern unter anderem von der National Vulnerability Database (NVD)[3], einer Datenbank für das Security-SchwachstellenManagement. Beispiele hierfür gibt es viele, wie der Trend der Anzahl öffentlich gemeldeter Security-Schwachstellen zeigt (vgl. Abbildung 1). Dass derartige Security-Schwachstellen auch ausgenutzt werden, sieht man unter anderem an der Kompromittierung einer US-Sicherheitsfirma [4] oder dem Missbrauch über verwundbare Netzwerkkomponenten[5]. Sobald eine OEM-Komponente in einem Produkt von einer Security-Schwachstelle betroffen ist, kann dies umfangreiche Auswirkungen auf die Angriffssicherheit des gesamten Produkts haben. Dies kann insbesondere weitreichende Auswirkungen haben, wenn ein Produkt im Rahmen von kritischen Infrastrukturen eingesetzt wird. Wenn eine schwerwiegende Security-Schwachstelle wie der Heartbleed Bug[6] aufgedeckt wird, kann es sein, dass für eine komplette kritische Infrastruktur die Informationssicherheit nicht mehr ausreichend gewährleistet werden kann.

2.2 Patches für OEM-Komponenten

Verantwortungsvolle Hersteller von OEM-Komponenten veröffentlichen im Falle von gefundenen Security-Schwachstellen zeitnah entsprechende Patches, die es zu installieren gilt. Damit werden der sichere Betrieb sowie das Niveau der Angriffssicherheit wieder erreicht. Insbesondere wenn Produkte in kritischen Infrastrukturen eingesetzt werden, ist es absolut notwendig, derartige auftretende Security-Schwachstellen in den OEM-Komponenten z. B. im Rahmen eines Patch Management Prozesses, so schnell wie möglich zu prüfen und ggf. zu beheben. Ein derartiger Patch Management Prozess erlaubt die schnelle und effiziente Behebung von bekannten Security-Schwachstellen [BRIL+11]. Dies wird zu Recht sowohl von Endkunden als auch von gängigen IT-Security-Standards wie der ISO 27001 [ISO05], dem BDEW Whitepaper [BDE08] sowie der NERC [ner14b, NER14a] gefordert. Für die Industrieautomatisierung und Kontrollsysteme[7] existiert insbesondere das Dokument IEC/TR 62443-2-3 [IEC14] zum Thema Patch Management in diesem Bereich. Im Gegensatz zu einem üblichen PC mit Internetverbindung, bei dem die Security Patches automatisch installiert werden können, ist die Behebung von

[2] Common Vulnerabilities and Exposures (https://cve.mitre.org/)
[3] National Vulnerability Database (http://nvd.nist.gov/)
[4] Anonymous kompromittiert US-Sicherheitsfirma (http://heise.de/-1195082)
[5] Fritzbox-Angriff analysiert: AVM bietet erste Firmware-Updates an (http://heise.de/-2108862)
[6] The Heartbleed Bug (http://heartbleed.com/)
[7] Industrial automation and control systems (IACS)

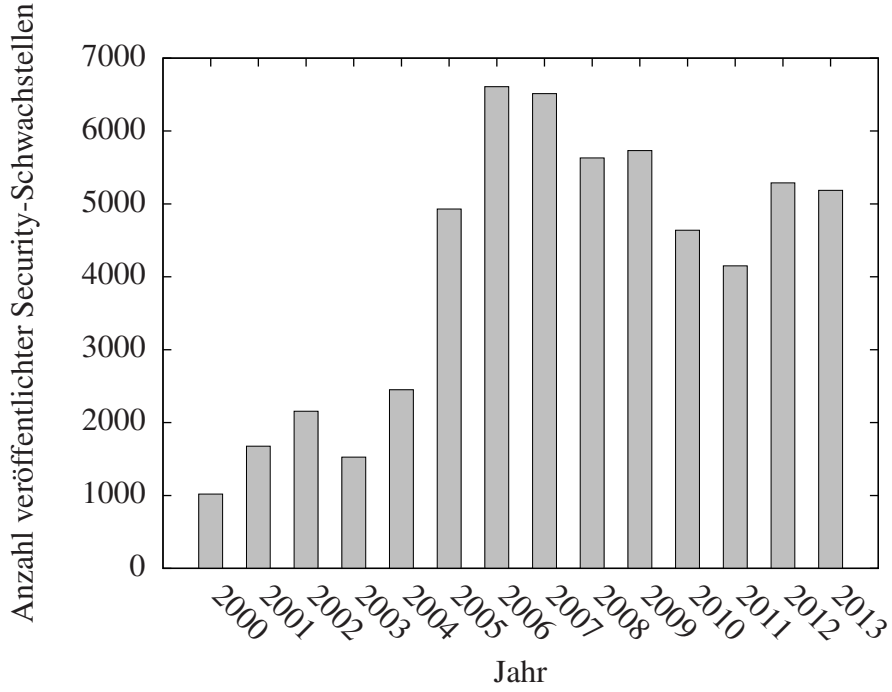

Abb. 1: Anzahl öffentlich gemeldeter Security-Schwachstellen in OEM-Komponenten [NVD14]

Security-Schwachstellen bei den in kritischen Infrastrukturen eingesetzten Produkten allerdings deutlich komplexer und damit aufwendiger. Grund dafür ist, dass zum einen eine große Vielzahl an verschiedenen OEM-Komponenten eingesetzt wird, zum anderen jedes Produkt anders aufgebaut ist und unterschiedliche Kundenanforderungen abdeckt. Nicht selten handelt es sich bei kritischen Infrastrukturen um hochverteilte Systeme die im 24/7-Betrieb laufen und nicht ohne Weiteres unterbrochen werden können.

2.3 Informationsbeschaffung

Damit die Produktverantwortlichen im Unternehmen in die Lage versetzt werden, bekannt gewordene Security-Schwachstellen in eingesetzten OEM-Komponenten durch die Installation von Security Patches beheben zu können, müssen sie erst einmal darüber Kenntnis erlangen. Die Informationsbeschaffung ist damit auch ein sehr wichtiger Teil eines Patch Management Prozesses und sollte insbesondere mehrere verschiedene Quellen zum Informationsbezug umfassen. Dies wird unter anderem von einigen üblichen Industriestandards für das Patch Management gefordert [BRIL+11]. In vielen Fällen ist die Einbindung verschiedener Quellen nur möglich, indem man die Internet-Seiten der unterschiedlichen Hersteller überwacht oder sich, sofern möglich, bei dem jeweiligen Hersteller registriert, um aktiv informiert zu werden. Microsoft zum Beispiel bietet die Möglichkeit, sich über aktuelle Security-Informationen via E-Mail aktiv informieren zu lassen[8]. Dennoch hat jeder Hersteller einer OEM-Komponente unterschiedliche Datenformate zur Meldung von Security-Schwachstellen und Patches. Insbesondere in einem Unternehmen mit verteilten Produktentwicklungen müsste sich jede Einheit für alle ihre Produkte und die darin eingesetzten OEM-Komponenten selbst um die Beschaffung der notwendigen Informationen kümmern. Als mögliche Lösung stehen Informationsdienste wie z. B. die NVD zur Verfügung und melden Security-Schwachstellen sowie dazugehörige Informationen. Um den Produktentwicklungen allerdings einen großen Teil der Arbeit abzunehmen,

[8] Microsoft Technical Security Notifications (http://technet.microsoft.com/en-us/security/dd252948)

ist es notwendig, dass ein derartiger Informationsdienst eine Vorfilterung der Daten vornimmt. Andernfalls werden die Produktentwicklungen und Produktverantwortlichen mit Informationen überflutet und müssen am Ende selbst entscheiden, welche Meldungen für sie relevant sind oder nicht. Damit eine Vorfilterung möglich ist, muss der Informationsdienst allerdings über die in den Produkten eingesetzten OEM-Komponenten detaillierte Kenntnis haben. Da diese Information einen Zusammenhang zwischen einer Security-Schwachstelle und einem konkreten Produkt herstellt, ist sie als vertraulich einzustufen. Aus diesem Grund ist es in vielen Unternehmen eine gängige Anforderung, die Information über Security-Schwachstellen in Produkten nur geschützt zu übertragen.

3 Lösungsansatz

Aus den Erfahrungen bei der Umsetzung eines Security Patch Managements bei der Siemens AG zeigte sich, dass ein zentralisierter Ansatz vorteilhaft ist. Der zentralisierte Lösungsansatz zielt darauf ab, Informationen über OEM-Komponenten sowie darin enthaltene Security-Schwachstellen bzw. verfügbare Patches durch einen unternehmensinternen und -weiten Monitoring-Dienst zu aggregieren, zu verarbeiten und zu verteilen, um Synergieeffekte nutzen zu können. Abbildung 2 veranschaulicht die im Folgenden beschriebene Vorgehensweise. Die in der Abbildung verwendeten Kennzeichnungen werden darüber hinaus auch in der Tabelle 1 kurz beschrieben.

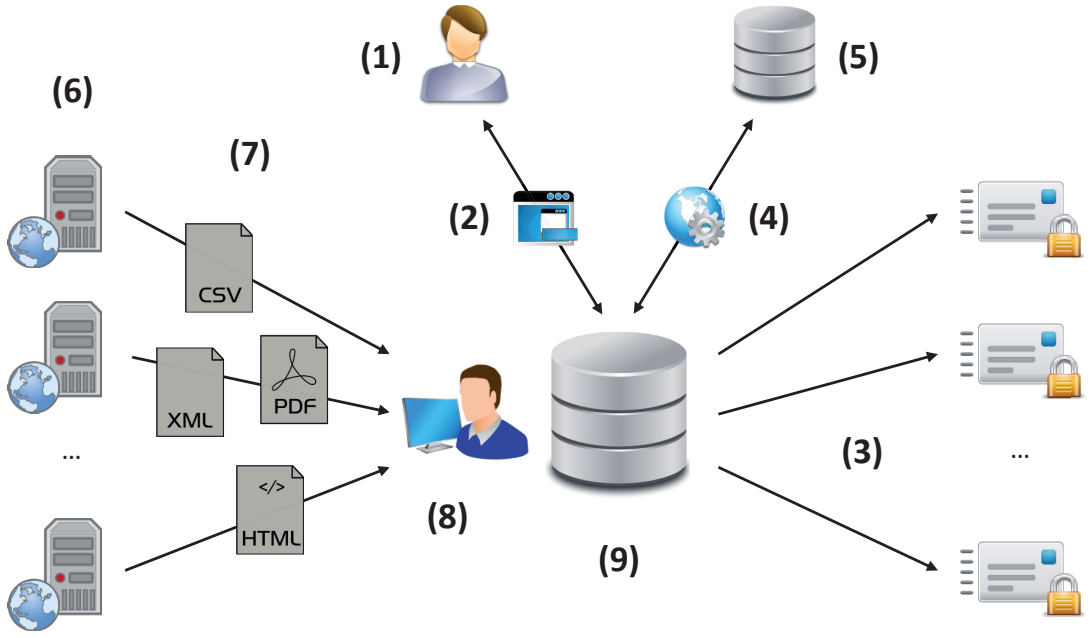

Abb. 2: Schema des zentralisierten Lösungsansatzes (vgl. Tabelle 1 sowie die Abschnitte 3.1 und 3.2)

3.1 Sicht der Produktverantwortlichen

Den Produktverantwortlichen (1) in den verschiedenen Einheiten wird eine Webapplikation (2) zur Verfügung gestellt, mit welcher sie eigenständig die zu monitorenden OEM-Komponenten ihrer Produkte verwalten können. Dies umfasst sowohl die Zuordnung von OEM-Komponenten aus einer Komponenten-Datenbank (vgl. Abbildung 3) als auch das Definieren von Verantwortlichkeiten (vgl. Abbildung 4). Sollte eine OEM-Komponente noch nicht in der Datenbank

Tab. 1: Kurze Beschreibung der Kennzeichnungen aus Abbildung 2

Nr.	Beschreibung
1	Produktverantwortliche
2	Webapplikation
3	Informationen zu Security-Schwachstellen via verschlüsselter E-Mails
4	Web-Service-Schnittstelle
5	Workflow-Systeme
6	Informationsdienste für Security-Schwachstellen
7	Vom Monitoring-Dienst verarbeitbare Datenformate für Security-Schwachstellen
8	Manuelle Verarbeitung von Security-Schwachstellen
9	Zentrale Datenbank

existieren, kann sie mit Unterstützung der Webapplikation zur Aufnahme angefordert werden. Die Verantwortlichkeiten bestimmen insbesondere die Berechtigungen eines Benutzers auf das hinterlegte Produkt.

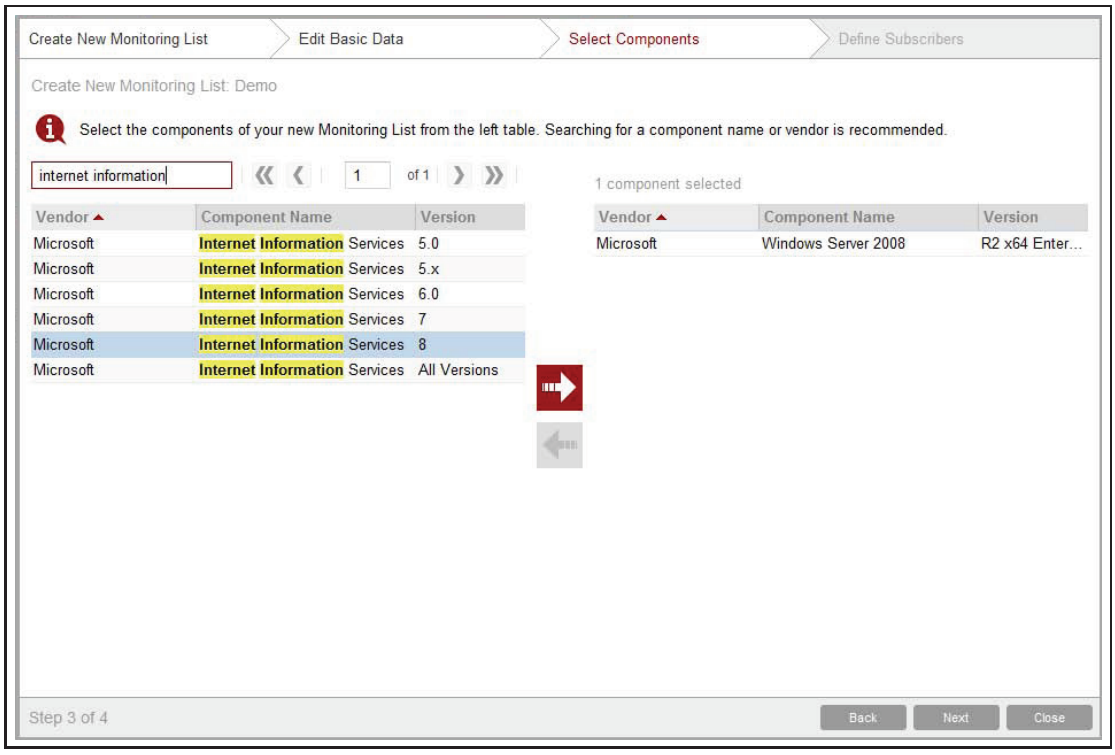

Abb. 3: Auswahl von OEM-Komponenten unter Verwendung einer Webapplikation

Informationen über Security-Schwachstellen werden basierend auf benutzerkonfigurierbaren Zeitplänen via verschlüsselter E-Mails (3) an die Produktverantwortlichen zugestellt. Des Weiteren besteht über eine Web-Service-Schnittstelle (4) die Möglichkeit, alle Funktionalitäten der Webapplikation (2) (semi-)automatisiert zu nutzen. Der Hauptanwendungsfall ist das automatisierte Abrufen und Einpflegen von Informationen über Security-Schwachstellen in bestehende Workflow-Systeme (sog. integriertes Patch Management) (5). Die Web-Service-Schnittstelle ermöglicht den Zugriff auf sensible Daten und wird deshalb via Zwei-Faktor-Authentifizierung basierend auf einer Public-Key-Infrastruktur (PKI) geschützt. Als Archi-

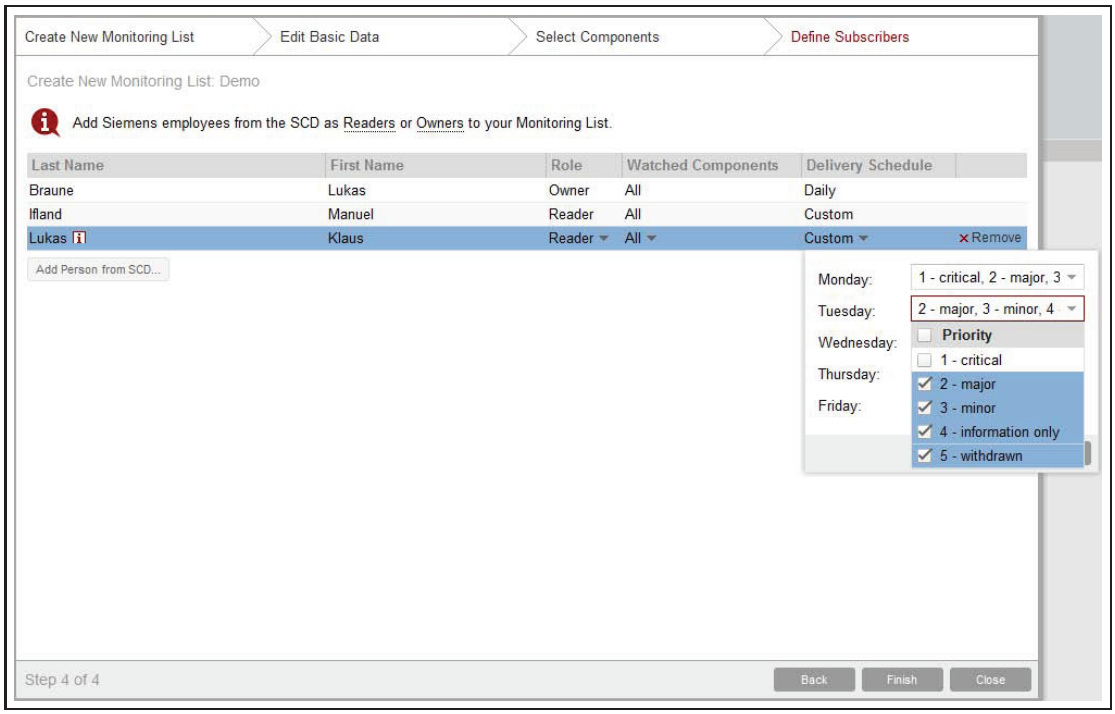

Abb. 4: Definieren von Verantwortlichkeiten für die zu überwachenden OEM-Komponenten

tekturstil für die Web-Service-Schnittstelle stellt REST[9] [Fiel00] ein geeignetes Paradigma dar, weil dieses im Allgemeinen als besonders leichtgewichtig und verständlich gilt und clientseitig verhältnismäßig einfach angebunden werden kann. Letzteres ist wichtig, um Produktverantwortliche zur Nutzung der Schnittstelle zu motivieren. Ein automatisierter Abruf von Informationen über Security-Schwachstellen zu einem im System hinterlegten Produkt soll im Folgenden exemplarisch dargestellt werden. Eine Client-Anwendung einer Produkteinheit fragt in regelmäßigen Abständen die Web-Service-Schnittstelle unter Angabe einer Produkt-Kennung nach zugeordneten Security-Schwachstellen ab. Die Rückgabe der Server-Anwendung im JSON-Format [JSO14] liefert eine Liste aller den OEM-Komponenten des jeweiligen Produkts zugeordneten Security-Schwachstellen in Form einer eindeutigen ID, des Datums der Veröffentlichung sowie ggf. des Datums der letzten Aktualisierung:

```
[
  {
    id: "21870",
    publish_date: "2013-09-18T09:35:22Z",
    last_update:  "2013-10-16T14:26:16Z"
  },
  {
    id: "22793",
    publish_date: "2014-01-09T13:53:28Z",
    last_update:  null
  }
]
```

9 Abkürzung für „Representational State Transfer“

Mit diesen Informationen kann eine Client-Anwendung zunächst feststellen, ob neue bzw. aktualisierte Security-Schwachstellen vorliegen. Anschließend können mit Hilfe der eindeutigen IDs detaillierte Informationen zu den Security-Schwachstellen abgerufen werden, wie die folgende Antwort der Server-Anwendung veranschaulicht:

```
{
  title: "Red Hat RHEL 5, 6 - java-1.6.0-openjdk Multiple Vulnerabilities",
  description: "These packages provide the OpenJDK 6 Java Runtime ...",
  priority: 2,
  impact: "Security Bypass, Exposure of Sensitive Information",
  vendor_advisories: [
    {
      name:   "RHSA-2014:0097-1",
      url:    "http://rhn.redhat.com/errata/RHSA-2014-0097.html",
      vendor: "Red Hat"
    }
  ],
  cve_references: [
    {
      year:   2013,
      number: 5878
    },
    ...
  ],
  cvss_v2_metrics: {
    base_score:     "6.8",
    temporal_score: "5.0",
    overall_score:  "5.0",
    vector:         "(AV:N/AC:M/Au:N/C:P/I:P/A:P/E:U/RL:OF/RC:C)"
  },
  ...
}
```

Produktverantwortliche haben in jeder Arbeitsphase die Möglichkeit, zu den gemeldeten Security-Schwachstellen sowie zu OEM-Komponenten Support durch IT-Security-Experten des Monitoring-Dienstes zu erhalten.

3.2 Infrastruktur des Monitoring-Dienstes

Security-Schwachstellen werden automatisiert von mehreren Informationsdiensten (6) im Internet aggregiert. Dabei werden gängige Datenformate (7) wie z. B. XML, HTML, JSON und PDF unterstützt. Im Anschluss findet eine zentralisierte und einheitliche Verarbeitung der Security-Schwachstellen statt, welche aufgrund ihrer hohen Komplexität nicht vollständig automatisiert werden kann. Stattdessen wird diese Aufgabe Tool-gestützt von Mitarbeitern des Monitoring-Dienstes (8) übernommen. Dadurch wird eine unternehmensweit einheitliche Erst-Priorisierung und Beschreibung der Security-Schwachstellen erreicht. Verarbeitete Security-Schwachstellen werden in einer zentralen Datenbank (9) abgelegt und können jederzeit über die Webapplikation und über die Web-Service-Schnittstelle abgerufen werden.

4 Erfahrungen bei der Implementierung

Bei der Umsetzung eines Security Patch Management Systems in der Siemens AG konnten in den vergangenen Jahren viele praktische Erfahrungen gesammelt werden. Im Folgenden werden exemplarisch Kernpunkte dargestellt, die einen wichtigen Beitrag zum Erfolg der Umsetzung lieferten.

4.1 Eindeutige Identifikation der OEM-Komponenten

Um eine effiziente Informationsbeschaffung auf Basis der Daten über eingesetzte OEM-Komponenten zu ermöglichen, müssen bestimmte Voraussetzungen geschaffen werden. Der Crawler, der die diversen Informationsquellen abruft und auswertet, benötigt für die Suche die korrekten und allgemein bekannten Namen jeder OEM-Komponente. Andernfalls besteht das Risiko, dass wichtige Informationen nicht gefunden werden, weil der Name einer OEM-Komponente in der Datenbank nicht korrekt ist. Bei der Vielfalt an OEM-Komponenten, zu denen nicht selten Bibliotheken und unbekannte Komponenten zählen, ist daher eine korrekte und vor allem eindeutige Benennung der Komponenten essenziell. Aus diesem Grund empfiehlt es sich, bei der Benennung der Komponenten ein Standardformat zu wählen, welches im Idealfall weltweit einheitlich ist und sich auch noch maschinell verarbeiten lässt. In dieser Hinsicht hat sich die insbesondere im Zusammenhang mit Security-Schwachstellen verknüpfte Common Platform Enumeration (CPE)[10] als sehr hilfreich erwiesen. Die CPE bietet ein strukturiertes Namensschema für Technologien, Software und Pakete in Form von sog. Uniform Resource Identifiers (URI). Da die CPE-Datenbank bereits sehr viele Komponenten beinhaltet und von CVE-Nummern referenziert wird, eignen sich CPE-Namen hervorragend als Basis für die Suche.

4.2 Einheitliche Schnittstellen und Verteilung

In einem großen Unternehmen mit verteilten und inhomogenen Organisationseinheiten ist es unvermeidbar, dass unterschiedliche Tools und Umgebungen zum Einsatz kommen. Damit jede Einheit von der Information eines zentralen und unternehmensweiten Monitoring-Dienstes profitieren kann, müssen einheitliche und standardisierte Schnittstellen zum Datenaustausch geschaffen werden. Dies ist insbesondere notwendig, wenn im Sinne eines integrierten Patch Managements verschiedene Workflow-Systeme angebunden werden. Es hat sich daher als ratsam erwiesen, Standardschnittstellen anzubieten, die wiederum über Standardprotokolle verfügbar sind. Beispiele hierfür sind Web Services, welche z. B. auf dem SOAP-Protokoll [SOA14] basieren oder RESTful APIs, die das JSON-Format nutzen. Web Services kommunizieren über HTTP, lassen sich aber auch über SSL/TLS (HTTPS) nutzen, sind damit verschlüsselt und problemlos auch hinter Firewalls nutzbar.

4.3 Schutz vertraulicher Information

Die Produktverantwortlichen in den Einheiten werden per E-Mail informiert, wenn eine OEM-Komponente in ihrem Produkt von einer Security-Schwachstelle betroffen sein sollte bzw. wenn ein Patch verfügbar ist. Selbstverständlich ist diese Information vertraulich, da hier ein Bezug zwischen Security-Schwachstellen und dem Produkt hergestellt werden kann. Aus diesem Grund sollten E-Mails mit derartigen Informationen, auch wenn sie innerhalb des Unternehmens übertragen werden, ausschließlich verschlüsselt an die Empfänger ausgeliefert werden.

[10] Common Platform Enumeration (http://cpe.mitre.org/)

Um allerdings eine derartige personenbezogene E-Mail-Verschlüsselung in einem Großunternehmen zu realisieren, ist eine Public-Key-Infrastruktur (PKI) notwendig. Die verschlüsselten E-Mails können nur vom Empfänger mit dessen privaten Schlüssel entschlüsselt werden. Auch wenn die Bereitstellung einer PKI mit großem Aufwand verbunden ist, kann diese hier zum Schutz der verteilten Informationen ideal genutzt werden.

4.4 Organisation in einem Großunternehmen

Eine großflächige Umsetzung eines Security Patch Management Systems in einem heterogenen Großunternehmen ist nur durch klare, durchdringende und in allen Organisationseinheiten verankerte Verantwortlichkeiten realisierbar. Projektbasierte Ansätze erzeugen zwar rasch lokale Lösungen in der jeweiligen Organisation, die Nutzung von Synergieeffekten auch monetärer Art sind nur durch den breitflächigen, zentralen Ansatz zu heben. Die Siemens AG beschäftigt sich bereits seit vielen Jahren mit der IT-Security (u. a. Angriffssicherheit) der angebotenen Produkte, Lösungen und Dienstleistungen. Die Bündelung dieser Aktivitäten wurde durch das Management entschieden und damit die Siemens-weite Product & Solution Security Initiative (PSS Initiative) gegründet. Diese PSS Initiative hat die Aufgabe, unternehmensweit die Etablierung von „must have“-Themen wie z. B. Security Vulnerability Monitoring voranzutreiben. Das Ziel der Product & Solution Security Initiative ist die Stärkung der reaktiven und proaktiven Fähigkeiten, u. a. betrifft dies die Themen Personal, Kommunikation, Prozesse und Technologien. Unter proaktiven Maßnahmen sind z. B. Aktivitäten wie Durchführung von Threat-and-Risk-Analysen, Definition und Anwendung von Architekturvorgaben oder auch Simulation von Hackerangriffen zu sehen. Auf dem Gebiet der reaktiven Maßnahmen hat die PSS Initiative z. B. einen unternehmensweiten Ansatz zum Security Vulnerability Monitoring definiert und flächendeckend ausgerollt. Ein entscheidender Erfolgsfaktor für das Gelingen in einem heterogenen Großunternehmen war die Findung, Verabschiedung und Nutzung eines einheitlichen, detaillierten Prozesses, welcher das Zusammenwirken zwischen den einzelnen Organisationseinheiten bzw. Produktverantwortlichen und dem zentralen Monitoring-Dienst festlegt. Zur fairen Kostenverteilung der finanziellen Aufwände des zentralen Monitoring Dienstes wurde ein Kooperationsmodell etabliert. Mit Hilfe des Mandats und der Verantwortlichkeiten innerhalb der PSS Initiative ist der Breitenrollout deutlich einfacher und schneller.

5 Zusammenfassung und Ausblick

Aus den Ausführungen wird ersichtlich, dass Security Patch Management nach wie vor eine organisatorische und technische Herausforderung darstellt. Speziell in Großunternehmen mit verteilten Entwicklungsstrukturen zeigt sich, dass ein zentralisierter Ansatz für die Beschaffung, Aufbereitung und Qualität der Informationen über Security-Schwachstellen als vorteilhaft erweist. Ein unternehmensweiter Ansatz ist sinnvoll, da ansonsten viele verschiedene Einzellösungen zum Security Patch Management entstehen und Synergien daraus nur bedingt genutzt werden können. Auch Änderungen in Standards und Regularien, welche die Anforderungen an den Security Patch Management Prozess betreffen, können zentral für viele Entwicklungsabteilungen eingebracht werden und erlauben eine breite, gewinnbringende Nutzung der Prozessverbesserungen. Da die Bewertung von Security-Schwachstellen im Bezug auf die Relevanz für ein konkretes Produkt immer noch fundiertes IT Security Know-how erfordert, ist ein unternehmensweites Mandat, wie die Product & Solution Security Initiative bei der Siemens AG, mit definierten Rollen, Kompetenzen und Ausbildungsmaßnahmen für eine sinnvolle Umsetzung eines Security Patch Managements unabdingbar. Das dargelegte Beispiel anhand eines

konkreten Großunternehmens zeigt, dass Security Patch Management auch in einem derartig komplexen Umfeld durchaus machbar ist, allerdings einen nicht zu vernachlässigenden Aufwand bedeutet. Hierbei müssen breite, unternehmensweit koordinierte organisatorische sowie technische Maßnahmen umgesetzt werden.

Literatur

[BDE08] Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme. BDEW Bundesverband der Engergie- und Wasserwirtschaft e.V., Berlin (2008).

[BRIL+11] M. Buehler, G. Rohrmaier, M. Ifland, N. Lode, K. Lukas: D-A-CH Security 2011: Ein standardkonformer Patch Management Prozess. Peter Schartner and Juergen Taeger, Berlin (2011).

[Fiel00] R. T. Fielding: Architectural Styles and the Design of Network-based Software Architectures. Dissertation (2000).

[IEC14] IEC/TR 62443-2-3 Ed.1: Industrial communication networks - Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment. (2014).

[ISO05] ISO27001: Information Security Management System (ISMS) standard. In: *Online: http://www.27000.org/iso-27001.htm* (2005).

[JSO14] JSON (JavaScript Object Notation), a lightweight data-interchange format. http://www.json.org/ (2014).

[NER14a] Critical Infrastructure Protection (CIP). http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (2014).

[ner14b] North American Electricity Reliability Corporation. http://www.nerc.com (2014).

[NVD14] National Vulnerability Database – CVE and CCE Statistics Query Page. http://web.nvd.nist.gov/view/vuln/statistics (2014).

[SOA14] Simple Object Access Protocol (SOAP) Version 1.2 Part 1: Messaging Framework (Second Edition). http://www.w3.org/TR/soap12-part1/ (2014).