Automatisiertes Schwachstellen-Management mit Greenbone und verinice: Effizienter Umgang mit Sicherheitsrisiken in der globalen Unternehmens-IT

Was nicht kontrolliert wird, geht im Alltagsbetrieb leicht unter. Dem Team Corporate Information Security (CIS) beim Kabel-Spezialisten LEONI AG passiert das nicht. Ein zentral gesteuerter Prozess für das Schwachstellen-Management versorgt die IT-Verantwortlichen in den einzelnen Standorten mit konkreten Anweisungen zur Verbesserung ihrer IT-Sicherheit. Durch wiederholte Schwachstellen-Scans entsteht ein sich selbst steuernder Prozess. Das Ergebnis spricht für sich: Die Zahl der Schwachstellen im weltweiten IT-System ist deutlich gesunken.

Der Kunde:
LEONI AG

Das 1917 gegründete Unternehmen mit Hauptsitz im bayerischen Nürnberg gehört heute zu den weltweit größten Herstellern von Draht, Kabel und Bordnetz-Systemen. Es beschäftigt weltweit mehr als 60.000 Mitarbeiter in 32 Ländern und ist im deutschen MDAX notiert.

Die LEONI AG ist auf Erfolgskurs: Neben maßgeschneiderten Kabellösungen bietet LEONI seinen Kunden vermehrt komplette Systeme mit perfekt aufeinander abgestimmten Komponenten – von der Leitung selbst bis zu den erforderlichen Verbindungs- und Befestigungselementen. Hinzu kommt eine in der Branche einmalige Produkt-Wertschöpfungskette, die wertvolle Synergien in sich birgt: Sie beginnt beim feinsten Einzeldraht und der optischen Faser, führt über das Kupfer- oder Glasfaserkabel und endet beim komplexen Bordnetz-System mit integrierter Elektronik. Die Kernmärkte: Automobile und Nutzfahrzeuge, Industrie und Gesundheitswesen, Kommunikation und Infrastruktur, Haus- und Elektrogeräte sowie Drähte und Litzen. Die Geschäfte laufen gut: 2013 betrug der Konzernumsatz 3,92 Milliarden Euro.

Globale IT-Infrastruktur zentral absichern

Erfolgsgeschichten wie diese könnten Begehrlichkeiten wecken. Der Schutz der unternehmensinternen IT-Systeme und Informationen zählt daher zu den geschäftskritischen Aufgaben. Die Abteilung Corporate Information Security der LEONI AG ist sich dieser Verantwortung bewusst und beschloss bereits 2011, eine automatisierte Lösung auf Basis Greenbone Security Manager für das Schwachstellen-Management einzuführen. Sie sollte die Spezialisten in der Zentrale dabei unterstützen, das Sicherheitsniveau der IT-Systeme in den 32 Ländergesellschaften auf einem gleichmäßig hohen Niveau zu halten. Christian Eschenlohr, Corporate Information Security Manager LEONI AG:

> *„Wir konnten die Effizienz der IT-Teams bei der Behebung von Schwachstellen weltweit steigern. Seit dem Projektstart ist die Anzahl der weltweiten Schwachstellen auf ein Zehntel gesunken.“*

„Unser Corporate Network umfasst derzeit etwa 18.000 Windows-Systeme, die rund um den Erdball verteilt sind. Die überwiegende Zahl wird heute bereits regelmäßig auf Schwachstellen gescannt – wir sind also fast am Ziel.“

Schwachstellen erkennen, bevor es andere tun

Für den Greenbone Security Manager sprach, dass er sich transparent in eine bestehende Infrastruktur integrieren ließ und alle Arbeitsschritte weitestgehend automatisierbar sind. Zudem wirkt er präventiv gegen Angriffe und deckt Verstöße gegen die Sicherheitsrichtlinien des Unternehmens oder gegen gesetzliche Vorgaben auf.

Da ein Schwachstellen-Report Hunderte von Einträgen enthalten kann, entschied man sich bei LEONI sehr früh dafür, zusammen mit Greenbone und mit SerNet die vorhandene verinice.PRO-Infrastruktur und den Greenbone Security Manager so eng zu verzahnen, dass sich eine deutliche Effizienzsteigerung bei der Behebung von Schwachstellen ergibt.

Klare Ansagen – überzeugende Ergebnisse

Das Ziel ist klar: Der Prozess von der Analyse der Schwachstellen durch den Greenbone Security Manager bis zum Verwalten der Handlungsanweisungen über verinice.PRO soll so weit als möglich automatisiert ablaufen. Das CIS-Team ergänzt die erkannten Schwachstellen um LEONI-spezifische Handlungsanweisungen. Anschließend werden die Daten in verinice.PRO importiert, gruppiert und als Aufgaben an die verantwortlichen IT-Spezialisten übergeben. Diese werden per E-Mail benachrichtigt.

Der Prozess berücksichtigt die Arbeitsweise der IT-Spezialisten und gruppiert die Schwachstellen der Assets entsprechend des Abarbeitungsprozesses. Erledigte Aufgaben werden durch die IT-Spezialisten bestätigt und von verinice verarbeitet. Die Bestätigung kann über den verinice-Rich-Client oder das verinice-Web-Frontend erfolgen.

Fallstudie Vulnerability Management
LEONI AG

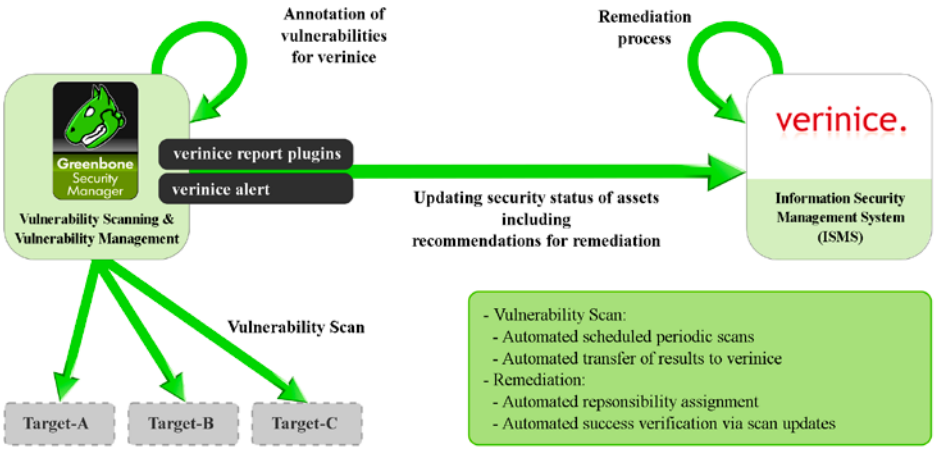
„Wir konnten mit diesem Projekt die IT-Spezialisten sensibilisieren und bei ihrer Arbeit unterstützen.“

Christian Eschenlohr
Corporate Information Security Manager LEONI AG

90 Prozent weniger Schwachstellen
Eschenlohr berichtet: „Wir konnten die Effizienz der IT-Teams bei der Behebung von Schwachstellen weltweit steigern. Denn mit Hilfe des neuen Prozesses übermitteln wir nur Aufgaben, die wir vorqualifiziert und mit Handlungsanweisungen versehen haben. Das kann beispielsweise bedeuten, dass wir gleich das Aufspielen einer neuen Programmversion empfehlen, anstatt 20 einzelne Schwachstellen beheben zu lassen oder die Installation von Sicherheitsupdates erst nach der Freigabe bei LEONI einfordern.“ Trotz reduziertem Zeitaufwand ist das Sicherheitsniveau deutlich gestiegen: Seit dem Projektstart ist die Anzahl der weltweiten Schwachstellen auf ein Zehntel gesunken. Mit der Greenbone-Lösung erfüllt LEONI auch Vorgaben aus dem VDA ISA.

Kein Wunder also, dass die Bilanz von Christian Eschenlohr positiv ausfällt: „Die Einführung der Greenbone-Lösung hat uns deutlich vorangebracht. Sicherheit hat heute in unserem Unternehmen eine höhere Priorität. Wir konnten mit diesem Projekt die IT-Spezialisten sensibilisieren und bei ihrer Arbeit unterstützen.“ Auch von der unkomplizierten Zusammenarbeit mit Greenbone ist der Sicherheitsexperte begeistert: „Alle Partner haben von diesem Projekt gelernt.“

Kontinuierliche Entwicklung lohnt sich
Lukas Grunwald, CTO bei Greenbone, bestätigt: „Bei Projekten dieser Größenordnung mit zahlreichen Netzen in unterschiedlichen Zeitzonen gibt es immer Anforderungen, denen wir zum ersten Mal gegenüberstehen. Der Aufwand lohnt sich für beide Seiten. Für die Kunden, weil die Lösung genau auf ihre Bedürfnisse zugeschnitten ist. Und für uns, weil die Erkenntnisse in unsere Produkte einfließen und so letztendlich dazu beitragen, die Greenbone-Lösungen kontinuierlich zu verbessern.“



„Die Einführung der Greenbone-Lösung hat uns deutlich vorangebracht.“

Eschenlohr nennt einen weiteren Vorteil: „Vor allem die hohe Flexibilität hat uns beeindruckt. Denn die Lösung ist für jeden Standort individuell einstellbar. Das ist wichtig, denn die Gegebenheiten unterscheiden sich von Land zu Land und nach Standortgröße. Je nach Verantwortlichkeit für die IT-Infrastruktur werden verschiedene GSM-Scans erstellt und in verinice zusammengeführt oder getrennt dargestellt. Es war auf jeden Fall richtig, sich für Greenbone zu entscheiden.“

Greenbone Security Manager

GSM 550

Einsatzfelder

- Mittlere bis große Unternehmens-IT
- Größere Zweigstellen
- Steuerung von bis zu 12 Scan-Sensoren
- 500 - 10.000 IPs

Funktionen

- Schlüsselfertige Lösung: Inbetriebnahme innerhalb von 10 Minuten
- Leistungsstarkes Betriebssystem Greenbone OS mit speziell angepasster Kommandozeilen-orientierter Administration
- Integrierter Greenbone Security Feed mit über 33.000 Netzwerk-Schwachstellen-Tests mit täglicher, automatischer Aktualisierung
- Integriertes Backup, Restore, Snapshot und Update
- Integriert Greenbone Security Assistant als zentrale Web-Schnittstelle
- Keine Begrenzung bezüglich Anzahl der Zielsysteme bzw. IPs (die maximal erreichbare Zahl hängt vom Scan-Muster und den Scan-Zielen ab)
- Bezug umfasst sowohl den Austausch defekter Hardware als auch Zugang zum Greenbone Security Feed, Feature-Updates und Support

Greenbone Networks GmbH
Neuer Graben 17,49074 Osnabrück, Germany
Telefon: +49-541-335084-0
Fax: +49-541-335084-99
Email: info@greenbone.net