RAPID7

CASE STUDY

Schwachstellen-Management bei OSRAM Licht AG: Mehr, als „nur“ Security

OSRAM	Herausforderung	Ergebnis
Branche: Elektroindustrie	Schwachstellen-Management über alle Standorte weltweit standardisieren	Abbildung der kompletten Organisationsstruktur und Identifikation aller Assets weltweit
Größe: 23.500 Mitarbeiter	Fehlende Transparenz über vorhandene Assets	Automatisierter Scan-Prozess und zeitnahe Nachbearbeitung
Produkte: InsightVM	IT-Sicherheit als Mehrwert für die Mitarbeiter implementieren	Ans Unternehmen angepasste Risikobewertung und eindeutige Priorisierung

OSRAM, mit Hauptsitz in München, ist ein weltweit führendes Hightech-Unternehmen mit einer über 110-jährigen Geschichte. Die überwiegend halbleiterbasierten Produkte ermöglichen verschiedenste Anwendungen von Virtual Reality bis hin zum autonomen Fahren sowie von Smartphones bis zu vernetzten intelligenten Beleuchtungslösungen in Gebäuden und Städten. Im Bereich Fahrzeug-Lichttechnik ist das Unternehmen globaler Technologie- und Marktführer.

Als ein führendes Hightech-Unternehmen verfolgt OSRAM eine ‘Cloud-first’-Strategie. Steffen Siguda, Corporate InfoSec Officer (CISO) und Datenschutzbeauftragter, verantwortet das globale Informationssicherheitsprogramm, inklusive aller technischen Aspekte sowie die Themen Training und Awareness. Siguda hat ein klares Ziel vor Augen, welches er als ‚Seamless Security‘ bezeichnet. Damit meint er: „Jeder kann seine Arbeit erledigen, indem er einfach nur ein bisschen mitdenkt. Der Rest soll im Hintergrund automatisiert, durch vernünftige Tools und Prozesse ablaufen, so dass das Thema Sicherheit nicht als Belastung wahrgenommen wird, sondern entweder als etwas, was man gerne macht oder was einem einen Mehrwert gibt.“

„Für uns ist ein Problem nur eins, um das sich keiner gekümmert hat.“

Bevor man bei OSRAM anfing, sich mit der Automatisierung und Standardisierung der Schwachstellen-Management-Prozesse auseinanderzusetzen, war es schwer, einen aktuellen Überblick über alle firmeneigenen Assets zu behalten. Man steckte eine Menge Handarbeit in diverse Listen und Tabellen, und trotzdem fehlte as an Transparenz. „Interessanterweise haben immer die Hosts, von denen Probleme ausgingen, in den Listen gefehlt. Und man fragte sich, wo kamen die denn nur her?“, erzählt Steffen Siguda.

Heute setzt man im Unternehmen auf eine dynamische Asset Identifikation durch das monatliche Auslesen der zentralen Routing-Tabelle. Dazu Siguda erklärend: „So haben wir monatsaktuell immer ein Wissen, woraus die Firma gerade besteht. Das war somit unser erster großer Erfolg, den wir mit InsightVM von Rapid7 erzielen konnten.“

Damit die Nachbearbeitung der Scan-Ergebnisse von den zuständigen Mitarbeitern zeitnah erfolgen kann, wird in InsightVM die Organisationsstruktur von OSRAM abgebildet. So weiß man für jedes Asset von welchem Standort aus es gescannt wurde, welcher Business-Unit es zuzuordnen ist und wo es sich gerade befindet, beziehungsweise wem es gehört. Die Scanergebnisse werden somit automatisch an die Organisationseinheiten weitergeleitet, die sich dann um die Beseitigung der Schwachstellen kümmern müssen. Abschließend wird ein Scan zur Kontrolle durchgeführt und das Reporting erstellt.

„Die Ergebnisse der Arbeiten sind stets klar nachvollziehbar. Alle Zuständigen haben sich ihre eigenen Reports gebaut bzw. können auch selbst noch mal scannen, um zu schauen, ob ihre Aktionen erfolgreich waren," erklärt Siguda. „Erst nach zweiwöchiger Bearbeitungszeit erfolgt erneut ein Scan, der dann zeigt, welche Lücken tatsächlich noch vorhanden sind. Und erst dieser Report dient uns als KPI. Denn wir sagen, für uns ist ein Problem nur eins, um das sich keiner gekümmert hat."

„Die Ergebnisse der Arbeiten sind stets klar nachvollziehbar. Alle Zuständigen haben sich ihre eigenen Reports gebaut bzw. können auch selbst noch mal scannen, um zu schauen, ob ihre Aktionen erfolgreich waren."

Ans Unternehmen angepasste Risikobewertung

Bei der Vielzahl an Assets ist es in der Regel nicht möglich allen gefundenen Schwachstellen nachzugehen, weshalb es notwendig ist, die Schwachstellen nach Risiko einzustufen. Dies ist mit Hilfe von Rapid7's Real Risk Scoring möglich, welches neben dem CVSS-Score mehrere zusätzliche Faktoren berücksichtigt, etwa das Alter einer Schwachstelle, existierende Exploits oder vom Unternehmen definierte Kritikalität der Assets. „Wir haben für uns kritische Systeme definiert und Schwellenwerte für die Risikoeinstufung von kritischen Systemen und kritischen Sites hinterlegt. Daraus generiert InsightVM eine Liste nach Risiko sortiert. Auf diese Art fokussieren wir uns, indem wir sagen, das was uns am Ehesten schadet, kommt nach vorne", führt Steffen Siguda aus.

Mehr als „nur" Security

Vom Einsatz der Schwachstellen-Management-Lösung InsightVM profitiert bei OSRAM nicht nur die IT-Security, auch andere Abteilungen bedienen sich gerne der Ergebnisse aus den Scans. So zum Beispiel die CMDB-Verantwortlichen, die überprüfen können, welche Assets es im Unternehmen gibt. Die Systemadministratoren, die sich einen Überblick verschaffen, wo eventuell Assets mit veralteten Versionen laufen. Die Verwaltung, die bei M&A Transaktionen sofort weiß, welche Assets wurden verkauft beziehungsweise welche sind durch einen Kauf hinzugekommen. Zudem kann die korrekte Absicherung von Rechnern in der Produktion durch die Auswertungen des Tools kontrolliert werden. Und nicht zuletzt ist es den Service Managern von OSRAM jetzt möglich nachzuhalten, ob sich Managed Service Provider an vereinbarte SLAs, z.B. für die Systemwartung, halten.

Siguda: „Die Zusammenarbeit mit Rapid7 läuft unter dem Schlagwort erfolgreiche Partnerschaft"

An der Zusammenarbeit mit Rapid7 schätzen Steffen Siguda und sein Team besonders das gegenseitige Vertrauen. „Jeder weiß, wir einigen uns auf etwas und alle Beteiligten halten sich daran. So hat Rapid7 bereits zu Anfang einiges an Vorleistung erbracht und ein gut konfiguriertes, auf unsere Anforderungen passendes Tool präsentiert. Diese große Bereitschaft auf unsere Bedürfnisse zu reagieren, haben wir bei anderen Anbietern nicht wahrgenommen.", resümiert Siguda abschließend.

Erfahren Sie mehr über die Insight-Plattform von Rapid7 und probieren Sie die Lösungen kostenlos aus:

Besuchen Sie uns auf: www.rapid7.com/try