




AMPEG Security Level Management

Keep the attack surface small 

 ZF Friedrichshafen AG

Unternehmensdrehzscheibe
für das Security Level
Management

A Security Lighthouse Case Study

▶ Unternehmensdrehzscheibe für das Security Level Management

Bei ZF dient das AMPEG Security Lighthouse als verlässliches Prüfinstrument für das Sicherheitsniveau des gesamten Unternehmens. Zugleich bewährt sich das System als interaktive Plattform für die Vermittlung der jeweils gültigen Anforderungen an die IT-Sicherheit. Die einzelnen Security Teams setzen das Werkzeug ihrerseits als Basis für ihre Arbeitsplanung und Erfolgsmessung ein.

ZF ist ein weltweit führender Technologiekonzern für Antriebs- und Fahrwerktechnik sowie für aktive und passive Sicherheitstechnik. 2015 hat ZF den US-amerikanischen Anbieter TRW Automotive übernommen und als Division „Aktive & Passive Sicherheitstechnik“ in den Konzern eingegliedert. Mit seinem Hauptstandort in Friedrichshafen am Bodensee zählt ZF international zu den größten Automobilzulieferern und ist mit rund 135.000 Mitarbeitern an etwa 230 Standorten vertreten, die sich auf rund 40 Länder verteilen.

Die weltweite IT-Infrastruktur von ZF zählt zusammen mit dem Bestand aus dem neu hinzugekommenen Anteil von TRW rund 80.000 Endgeräte und 10.000 Server. Die Serverlandschaft ist zu etwa 90 Prozent virtualisiert, bei den Clients handelt es sich um klassische Hardware. Wie viele Unternehmen im Bereich der industriellen Fertigung verfügt auch ZF über eine große Anzahl an Produktionsanlagen mit bereits langfristig genutzten IT-Komponenten. Auch diese müssen gepflegt und von der IT-Sicherheit betreut werden, da die Systeme als Ganzes ihre geplante Lebensdauer bei weitem noch nicht erreicht haben.



Zentrale Vorgaben effizient kontrolliert

Die gesamte IT des Unternehmens wird zentral von Deutschland aus gesteuert. Die am Hauptstandort entwickelten Vorgaben gelten weltweit und sollen der internationalen Belegschaft auf faire und kooperative Weise vermittelt werden. Die Mitarbeiter sollen die Richtlinien und Standards verstehen und akzeptieren und bei der Umsetzung als Partner der IT-Leitung agieren.

*Der ZF-Innovation Truck – ein Lkw-Prototyp mit mehr als 25 Metern Länge – lässt sich bequem per Tablet-Fernsteuerung sowie lokal emissionsfrei rangieren.
Quelle: ZF FRIEDRICHSHAFEN AG*

Auch die Informationssicherheit ist zentral organisiert und operiert von Friedrichshafen aus. Die übergeordnete Kontrollfunktion übernimmt der Konzernbeauftragte für IT-Sicherheit. Organisatorisch hat ZF die Security-Abteilung in die produktive IT eingebettet. „Der Vorteil dieses Modells ist, dass die IT-Sicherheit immer direkt an der Projektplanung der IT teilnimmt“, erklärt Michael Schrank, Head of IT Security bei ZF. „IT und IT-Security ziehen

▶ Unternehmensdrehzscheibe für das Security Level Management

deshalb an einem Strang. So finden ihre Entscheidungen die nötige Beachtung und werden weltweit auch wirklich umgesetzt.“ Für Schrank bietet die klare, einfach gegliederte Organisation auch einen echten Sicherheitsgewinn: „Müssen wir kurzfristig Maßnahmen ergreifen, weil es die aktuelle Gefahrenlage notwendig macht, geschieht dies schnell und ohne lange Verzögerungen. Unternehmen, die beispielsweise mit mehreren CISOs für unterschiedliche Organisationseinheiten arbeiten, benötigen für solche Prozesse weitaus länger.“

2014 begann ZF mit der Suche nach einem Werkzeug, das seinem Sicherheitsteam jederzeit einen verlässlichen Überblick über den jeweiligen Sicherheitsstatus aller IT-Komponenten im weltweiten Netzwerk bieten sollte. In diesem Bereich sahen die Spezialisten des Technologiekonzerns noch erheblichen Verbesserungsbedarf: „Wir haben versucht, den Gesamtstatus manuell über die verschiedenen Konsolen der System- und Security Management Tools zu ermitteln“, berichtet Schrank, „aber diese Vorgehensweise erwies sich als zu komplex und zeitraubend. Auch die Qualität der Ergebnisse stellte uns nicht zufrieden.“



*Am ZF-Standort Saarbrücken werden 8-Gang-Automatgetriebe für Pkw gefertigt.
Quelle: ZF FRIEDRICHSHAFEN AG*

Auf der Suche nach Abhilfe evaluierte das Team die Lösung „Security Lighthouse“ von AMPEG. Das Monitoring System koppelt sich mit „Kollektoren“ an die System- und Security Management Tools im Netzwerk an, erhebt und korreliert die dort gewonnenen Statusinformationen nahezu in Echtzeit und gleicht sie mit den unternehmensinternen Sicherheitsvorgaben ab. Die Resultate bereitet das System unter anderem auf einer Weltkarte visuell auf und symbolisiert den

Sicherheitsstand einzelner Lokationen anhand von Ampelfarben. Zeigen sich an einem Standort Unstimmigkeiten oder Fehler – wie etwa nicht ausgerollte Virensignaturen, fehlende Softwareupdates, ausgelassene Patches oder verspätete System-Rückmeldungen – kann der Operator den Problemen sofort per Mausklick auf den Grund gehen und dabei immer detailliertere Informationen über Netzwerksegmente bis hinab zu den Einzelsystemen abrufen.

Anpassungsfähig durch Kollektor-Konzept

„Das Konzept von Security Lighthouse kam unseren Vorstellungen gleich auf mehreren Ebenen entgegen“, erinnert sich Michael Schrank. „Der erste Aspekt waren die Kollektoren: Dieses Architekturmerkmal versprach aus unserer Sicht einen guten Ansatzpunkt für mögliche Erweiterungen, individuelle Anpassungen und die Umsetzung eigener Ideen. Die

▶ Unternehmensdrehzscheibe für das Security Level Management

zweite Eigenschaft, die uns auffiel, war die gelungene Visualisierung, die den Operatoren zu einer schnellen Einschätzung und Lokalisierung eventueller Problembereiche verhilft.“ Darüber hinaus interessierte sich Schrank für das rollengestützte Zugriffsmodell. Es erlaubt, Zugriffsrechte für einzelne Sektoren und Segmente einer IT-Infrastruktur granular zu vergeben, sodass Administratoren jeweils nur Einblick in diejenigen Bereiche einer IT-Landschaft bekommen, für die sie verantwortlich sind. ZF sah hier die Chance für einen flexiblen und verteilten Einsatz des Werkzeugs.

In allen drei Fällen erfüllten sich die Erwartungen von ZF. Bereits beim Proof of Concept (PoC) zeigte sich, dass AMPEG für fast alle wichtigen ZF-Systeme, die eingebunden werden sollten, Kollektoren als Schnittstellen „out of the box“ zur Verfügung stellen konnte. „Die Tatsache, dass der PoC vor diesem Hintergrund überaus glatt verlief und dass an keinerlei Stellschrauben gedreht werden musste, ließ uns ein pflegeleichtes Produkt erwarten“, erzählt Schrank. Auch die Zusammenarbeit mit dem Anbieter gestaltete sich von Anfang an durchweg positiv: „Als zu Beginn ein Wert bei der Statureinschätzung nicht passte, reichte ein Anruf beim Support – und binnen kürzester Frist wurde das Problem analysiert und behoben, ganz ohne Wartezeiten und lange Diskussionen.“

Produktive Kooperation zwischen Anbieter und Kunde

Die endgültige Entscheidung für Security Lighthouse fiel daraufhin schnell. „Bereits vier Wochen nach dem Start stand ein lauffähiges System zur Verfügung, das sich nützlich machte“, ergänzt Schrank, „und nach einem Jahr war der Vollausbau mit weltweitem Fokus



Bei ZF wird in der Security Information Map des Security Lighthouse der aktuelle Sicherheitsstatus in nahezu Echtzeit eingesehen.

Schnittstelle im Bereich des Konfigurations-Managements. „Die Kooperation verlief von der Idee über deren Bewertung bis zur Fertigstellung ebenso effektiv wie partnerschaftlich“,

erreicht – inklusive der Schulung der Mitarbeiter.“ Bei ZF erhebt und korreliert AMPEG Security Lighthouse nun Daten aus Quellen wie dem Active Directory, dem Update- und Inventory Management, Paketverwaltungs-Tools, Configuration Management (CMDB, Security Instructions) und zwei Virenschutzprodukten.

„Einen Kollektor“, weiß Schrank zu berichten, „haben wir zusammen mit AMPEG neu entwickelt.“ Es handelt sich um eine

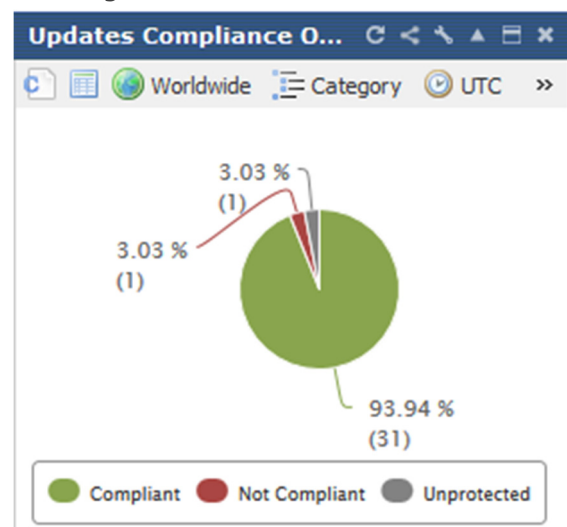
▶ Unternehmensdrehseife für das Security Level Management

fährt der ZF-Spezialist fort: „AMPEG hat die Anregung sofort aufgenommen und der neue Kollektor war bereits nach einem Vierteljahr einsatzbereit.“ Inzwischen hat AMPEG das so entstandene Interface in sein Repertoire vorgefertigter Kollektoren aufgenommen. „ZF nutzt außerdem unseren neuen CVE-Katalog (Common Vulnerabilities and Exposures)“, merkt Michael Hänsel an, Projektleiter bei AMPEG: „Diese Ressource hilft bei der Bewertung von Schwachstellen, die das Security Lighthouse mit den bereits erhobenen Daten aus dem Update- und Inventory Management korreliert.“

Im erhofften Maße bewährt hat sich auch die praxisorientierte und flexible Visualisierung der sicherheitsrelevanten Informationen durch das Security Lighthouse. ZF setzt das System unter anderem im Security Operations Center (SOC) ein, wo es die Analysten heranziehen, um bei Alerts die möglichen Auswirkungen einer bekannten Bedrohung auf die Systeme im Netz besser einschätzen und die Events und Incidents exakter klassifizieren zu können. „Für uns von großer Bedeutung ist außerdem das Reporting“, erläutert Schrank, „wir können damit heute ohne großen Aufwand jederzeit zeigen, ob und wie wir die vereinbarten Key Performance Indicators (KPIs) für den Sicherheitsstand einhalten. Die Messungen und der Abgleich sind automatisiert und die Aufbereitung der Ergebnisse wird dem Bedarf des Managements voll und ganz gerecht.“

Verteilte Nutzung dank Rollenkonzept

Auf der Basis des Rollenkonzepts gelang es auch, Security Lighthouse auf die von ZF gewünschten Arbeitsprozesse rund ums Security Level Management abzustimmen. „Bei uns arbeitet nicht etwa nur eine zentrale Kontrollinstanz mit Security Lighthouse. Weltweit sind nicht weniger als 150 Mitarbeiter berechtigt, auf das System zuzugreifen“, beschreibt Schrank das Einsatzmodell. „Wir verstehen das Monitoring Tool nicht als Ein-Richtungs-System, das lediglich die Forderungen einer übergeordneten Instanz nach unten durchreicht. Wir setzen Security Lighthouse als ein Werkzeug ein, das zwischen der Zentrale und den Verantwortlichen für einzelne IT-Bereiche eine kooperative Zusammenarbeit zur Erhöhung des Sicherheitsniveaus ermöglicht.“ Dazu werden die Vorgaben und Schwellenwerte für den jeweils angestrebten Sicherheitsstand in Friedrichshafen eingepflegt. Die weltweiten Teams nutzen Security Lighthouse dann selbstständig als Informationsplattform, in der sich die Mindeststandards ablesen lassen, und orientieren sich mithilfe des Monitoring Tools auch darüber, ob ihre Maßnahmen zur Einhaltung der Vorgaben und zum Schließen der Sicherheitslücken auch tatsächlich fruchten.



Das weltweite Sicherheitsniveau auf einen Blick

Unternehmensdrehseibe für das Security Level Management

Die nächsten Schritte für ZF sind die Entwicklung weiterer spezifischer Kollektoren – und die Einbindung der IT-Landschaft aus der neuen Division Aktive & Passive Sicherheitstechnik ins Status-Monitoring.

Die Lösung wurde realisiert bei:

ZF FRIEDRICHSHAFEN AG
Graf-von-Soden-Platz 1
88046 Friedrichshafen, Deutschland
<http://www.zf.com/>

Mit Unterstützung von:

AMPEG GmbH
Stavendamm 22
28195 Bremen, Deutschland
<https://www.ampeg.de/>