

Globale IT-Sicherheit im TÜV Rheinland

Im Zuge der internationalen Globalisierung der IT stellt der TÜV Rheinland seine IT-Sicherheit weltweit neu auf. Durch die Einführung eines Monitoring-Systems soll der Sicherheitsstatus transparenter gemacht und kontinuierlich verbessert werden.

Der TÜV Rheinland steht für geprüfte Sicherheit und Qualität und begleitet seine Kunden bei der kontinuierlichen Verbesserung von Produkten, Systemen und Prozessen. Wie in der Kundenarbeit gelten auch für die internen IT-Dienstleistungen hohe Maßstäbe. Sicherheit muss überprüfbar sein, Qualität messbar. Deshalb wurde im Bereich IT-Sicherheit ein Projekt zur Einführung der Monitoring-Software AMPEG Security Lighthouse gestartet, die Daten aus Sicherheitssystemen unterschiedlicher Hersteller verarbeiten kann. Damit schafft der TÜV Rheinland in einer weltweit verteilten Organisation die notwendige Transparenz für die IT-Sicherheit.



Projektschritt 1: Technik konsolidieren

Bei der Einführung des Monitoring-Systems Security Lighthouse ist es erforderlich, alle Daten über den Sicherheitsstatus der Clients und Server in einer Microsoft SQL-Datenbank zusammenzuführen. Dazu dienen Collectoren, die auf Basis von SQL-Jobs realisiert sind und aus den Antivirus-Systemen, den Microsoft WSUS-Servern und dem Verzeichnisdienst Active Directory die notwendigen Daten auslesen. Um den Administrationsaufwand möglichst niedrig zu halten und gleichzeitig die Zuverlässigkeit des Gesamtsystems zu optimieren, wurde eine technische Konsolidierung aller Antivirus- und WSUS-Installationen durchgeführt, mit dem Ziel die Gesamtzahl zu senken und mehr Effizienz zu erzielen.

Projektschritt 2: Transparenz schaffen

Durch das Rollenkonzept vom Security Lighthouse ist es möglich, einem größeren Personenkreis Zugriff zum Monitoring-System zu geben und mehr Transparenz zu schaffen. Die einfache Bedienung war deshalb ein maßgebliches Entscheidungskriterium für den TÜV Rheinland: Der Einstieg mit dem Webbrowser über eine Weltkarte des Monitoring-Systems, über die in die einzelnen Länder und Standorte navigiert werden kann, ermöglicht es sowohl einem IT-Administrator als auch einem IT-Manager schnell und intuitiv den aktuellen Sicherheitsstatus zu überblicken.

Alle Benutzer des Monitoring-Systems erhalten in vereinheitlichter Form aktuelle Informationen zum Verteilungsstatus von Virenpattern und Sicherheitsupdates. Im Security Lighthouse werden diese Daten mit den hinterlegten Zielvorgaben abgeglichen. Das Ergebnis der permanenten Soll-Ist-Analyse zeigt die Monitoring-Software in der Security Information Map an: je nach Zielvorgabe und Erfüllungsgrad werden Länder und Standorte in grün, gelb oder rot angezeigt. Ist ein Standort gelb oder rot markiert, können sich die Verantwortlichen anzeigen lassen, welche Systeme nicht das aktuelle Update bekommen haben. Über detailliertere Ansichten in Tabellenform können Abweichungen bis herunter auf das einzelne Gerät sichtbar gemacht, analysiert und korrektive Maßnahmen sofort eingeleitet werden.

Der Weg zur Qualitätssicherung für die IT-Sicherheit

- *Standorte und Systeme erfassen:* Für die Standortinformationen des TÜV Rheinland wurde von AMPEG-Beratern eine Schnittstelle implementiert. Darüber wird das Security Lighthouse einmal täglich automatisch aktualisiert und kann die Zuordnung der Clients und Server zu den einzelnen Standorten vornehmen.
- *Verlorene Systeme zuordnen:* In jedem großen Netzwerk kommt es vor, dass aufgrund fehlender Informationen vereinzelt Systeme keinem Standort zugeordnet sind. In Security Lighthouse können diese sichtbar gemacht und den richtigen Standorten zugeordnet werden.
- *Ausreißer einfangen:* In großen Netzwerken finden sich immer Clients oder Server, die an kein Update-System angeschlossen sind. Diese stellen gefährliche Schwachpunkte im Netzwerk dar, denn sie erhalten keine Virenpattern oder Patches. Sehr wahrscheinlich sind diese Systeme aber im Active Directory registriert. Da das Security Lighthouse das Active Directory auslesen kann und eine Ansicht zur Korrelation der Daten zur Verfügung stellt, können Ausreißer lokalisiert und die Schwachstellen behoben werden.
- *Security Level Management aufsetzen:* Zur Vorbereitung des Qualitätsmanagements müssen Grenz- und Schwellenwerte aus den Security Policies abgeleitet und im Security Lighthouse hinterlegt werden. Zunächst kann aber auch mit Default-Werten, die hinterlegt sind, gearbeitet werden. Damit kann ein Standort beispielsweise mit „grün“ ausgezeichnet werden, wenn 90 oder mehr Prozent aller Systeme mindestens einen der letzten drei Patches erhalten haben.

Weltweiter Rollout

Die Implementierung des Security Lighthouse war mit Unterstützung durch AMPEG in wenigen Wochen abgeschlossen. Auch die Standortdatenbank war nach dieser Phase angeschlossen, die verlorenen Systeme zugeordnet und die Ansichten, Reports und Alerts angepasst.

Kontinuierliche Verbesserung

Durch den schnellen und einfachen Zugriff auf die relevanten Informationen überall auf dem Globus entfallen zeitraubende Aufgaben, wie der Zugriff auf unterschiedliche Produktkonsolen oder manuelle Erfolgsprüfungen. Es entstehen Freiräume, in denen sich die Mitarbeiter voll auf die Maßnahmen der Qualitätssicherung konzentrieren können. Sicherheitslücken werden proaktiv geschlossen und nicht erst, wenn sie durch Vorfälle evident werden. Jeder eliminierte Schwachpunkt im Netzwerk verbessert die IT-Sicherheit und senkt das Restrisiko. Nach und nach wird es möglich sein, mit strengeren Vorgaben und Zielsetzungen für die Systeme zu arbeiten und die IT-Sicherheit weiter zu optimieren. Weil die Verbesserungen der IT-Sicherheit gemessen werden können, wird sich der Erfolg der Qualitätssicherungsmaßnahmen deutlich belegen lassen. Ein derartig organisiertes Security Level Management genügt den hohen Ansprüchen des TÜV Rheinland – ganz nach der Devise: Wer Qualität von seinen Kunden einfordert, muss sie auch selbst vorleben.

Die Lösung wurde realisiert bei:

TÜV Rheinland Service GmbH
Am Grauen Stein, 51105 Köln
<http://www.tuv.com>

Mit Unterstützung von:

AMPEG GmbH
Obernstraße 45-47, 28195 Bremen
<http://www.security-lighthouse.de>