AMPEG

Schott AG

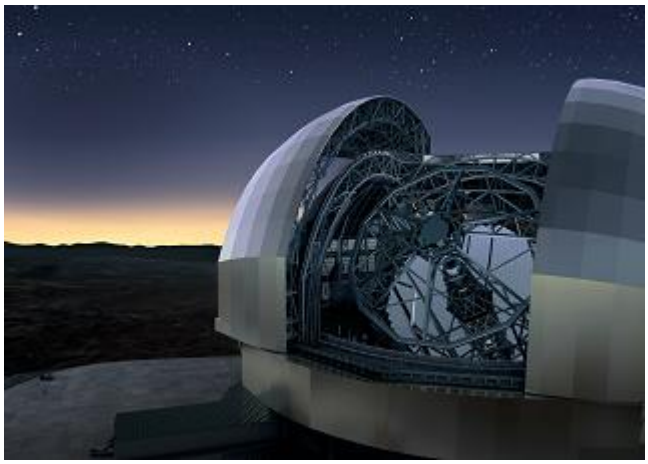
Sicherheit durch Transparenz - für ein Universum aus Glas

A Security Lighthouse Case Study

Sicherheit durch Transparenz - für ein Universum aus Glas

Als Innovator für Spezialglas mit Produktion und Vertrieb auf fast allen Kontinenten stellt die SCHOTT AG ebenso umfassende wie komplexe Anforderungen an die IT-Sicherheit. AMPEG Security Lighthouse ist ein „Argusauge", das jetzt über die internationale Office-IT dieses Traditionsunternehmens und Weltkonzerns wacht. Das Monitoring-System unterstützt mit seinen umfassenden Analysen die Anforderung des Unternehmens an größtmögliche Transparenz.

CERAN® Kochflächen sind weltweit ein Inbegriff. Weniger bekannt ist, dass diese revolutionäre Glaskeramik schon 1971 von SCHOTT entwickelt wurde. Auch auf zahlreichen anderen Gebieten steht SCHOTT für herausragende Pionierleistungen. Als Neil Armstrong 1969 als erster Mensch den Mond betrat, wurde sein legendärer Fußabdruck mit Linsen aus optischem Glas von SCHOTT aufgenommen. Bis heute greift man mit Materialien dieses Unternehmens nach den Sternen: Die größten und modernsten Teleskope der Welt setzen auf ZERODUR® Glaskeramik, um das Rätsel der dunklen Materie zu erforschen oder einen Beweis für außerirdisches Leben zu entdecken.



Vier der fünf Spiegel des Extremely Large Telescopes werden aus ZERODUR® Glaskeramik von SCHOTT gefertigt.
Quelle: SCHOTT

Mehr als 130 Jahre nach Unternehmensgründung repräsentiert SCHOTT ein Portfolio, das beinahe alle Lebensbereiche abdeckt. Der Hidden Champion ist globaler Innovationspartner für die Hausgeräteindustrie, Pharma, Elektronik, Optik, Life Sciences, Automotive und Aviation. Im Geschäftsjahr 2017/18 konnte ein Umsatz von über 2 Milliarden Euro weltweit verbucht werden, davon 86 % außerhalb Deutschlands. An Produktions- und Vertriebsstandorten in 34 Ländern sind rund 15.500 Mitarbeiter beschäftigt. Die Muttergesellschaft hat ihren Hauptsitz in Mainz und ist zu 100% im Besitz der Carl-Zeiss-Stiftung.

Der Schutz der „Kronjuwelen" ist nicht alles

Ein solches Hightech-Unternehmen verfügt über zahlreiche Patente und ein enormes Spezialwissen, das es unter allen Umständen zu behüten gilt. Diesen Schatz zu sichern, war bei SCHOTT denn auch der ursprüngliche Ansatz für den Ausbau der IT-Sicherheit. „Als ich bei SCHOTT begonnen habe, war unser Fokus im Prinzip: Wie schützen wir unsere Kronjuwelen?", erläutert Dirk Ossenbrueggen, Head of Information Governance and Security bei SCHOTT. „Der ganze große Rest ging so ein bisschen im IT-Betrieb unter. Es ist dann aber das Bewusstsein gewachsen, dass es außer den Kronjuwelen auch noch andere Dinge zu schützen gilt und dafür auch Geld in die Hand genommen werden muss. Wir hatten damals vor allen Dingen zu wenig Transparenz. Wir hatten keinen tieferen Einblick in unser Netz, wussten nicht, wie wir aufgestellt sind und wie das Sicherheitsniveau

überhaupt ist. Um dieses Problem zu lösen, habe ich nach Tools gesucht, die mir einen schnellen Überblick über das Sicherheitslevel unserer IT geben."

SCHOTT setzt auf Augmented Reality-Anwendungen und bietet hierfür spezielle optische Gläser für die entsprechenden Brillen. Quelle: SCHOTT

Nachdem Dirk Ossenbrueggen zunächst auf ein anderes Tool gestoßen war, führte ihn die weitere Recherche zum Security Lighthouse von AMPEG. Nach dem Abgleich beider Tools mit den spezifischen Anforderungen von SCHOTT fiel die Entscheidung auf das Security Lighthouse. Das Team um Dirk Ossenbrueggen ließ sich dabei von folgenden Anforderungen leiten: „Wir wollten wissen, wie wir in Richtung Update-Management stehen, was ist drin und was ist nicht drin? Wie aktuell sind unsere Patches? Darüber hinaus stellte sich auch die Frage nach der Endpoint Protection, sprich Anti-Virus. Welche Systeme sind abgedeckt und wie aktuell sind die Signaturen? Das dritte Gebiet war die Festplattenverschlüsselung. Bei allen Fragestellungen hatten wir das Gefühl, dass AMPEG uns mit seinem Security Lighthouse die notwendigen Einblicke geben kann. Neben den Kollektoren für die bereits erwähnten Zielsysteme hatten wir außerdem noch den für Active Directory im Blick, und das war dann auch das initiale Setup, mit dem wir gestartet sind."

Rollout in nur 10 Tagen

Im Proof of Concept (PoC) bestätigte sich rasch, dass AMPEG die von SCHOTT benötigten Kollektoren für Patch-Management, Virenschutz, Encryption und Software Inventory als Schnittstellen „out of the box" bereitstellen konnte. „Die im PoC getesteten Kollektoren erfüllten ihre Funktion wie gewünscht, sodass SCHOTT die Installation unseres Security Lighthouse Systems sofort nach der Testphase in Auftrag gegeben hat", unterstreicht Michael Hänsel, Projektleiter bei AMPEG. „Unser System überprüft aktuell sämtliche Clients und Server im weltweiten Office-Netzwerk der SCHOTT AG und bildet den Sicherheitsstatus auf einer Weltkarte nahezu in Echtzeit ab. Die Installation erfolgte ausgesprochen schnell. Alles in allem, also inklusive PoC und Basisschulung des Personals, hat das Rollout des kompletten Monitoring-Systems lediglich zehn Tage gedauert. Ein wirklich schneller Pfad, wenn man Größe und Umfang des Projekts bedenkt."

Als zielführend hat sich dabei auch die Fähigkeit erwiesen, Lösungswege offen zu diskutieren. „AMPEG hat sich als flexibler Partner erwiesen, der aufgeschlossen für Neuerungen und Verbesserungen ist. Wenn wir als Kunde eine Idee haben und sagen, wir könnten uns dieses oder jenes als neues Feature vorstellen, dann wird das aufgenommen. So haben wir

die Möglichkeit, das Produkt und auch die Roadmap in bestimmten Details mitzugestalten", resümiert Dirk Ossenbrueggen.

Wertvolle Erkenntnisse

Signifikant waren die Erkenntnisse, die SCHOTT aus den von Security Lighthouse detektierten Daten ziehen konnte. „Das Kontrollsystem hat uns klipp und klar aufgezeigt, wo wir stehen", betont Ossenbrueggen. „In gewisser Weise waren die Daten ernüchternd, denn wir hatten gedacht, mit unserer IT-Sicherheit schon weiter zu sein. Dem war aber nicht so. Allerdings, und das war ja das Positive daran, wussten wir jetzt, welche Defizite wir hatten. Wir haben das zum Beispiel sehr deutlich bei unserem IP-Adressmanagement gesehen. Es hat sich schnell rausgestellt, dass unsere Datenqualität hier an einigen Stellen noch sehr verbesserungsbedürftig war. Das ist in der Tat ein zentraler Vorteil des Tools: Es macht unmissverständlich deutlich, welche Baustellen bearbeitet werden müssen."

Der Personenkreis, der das Security Lighthouse bei SCHOTT aktiv nutzt, hat sich inzwischen deutlich erweitert: „Bis vor kurzem wurde das AMPEG Tool ausschließlich von unserem fünfköpfigen Security Team angewendet", so Ossenbrueggen. „Wir haben die im Monitoring gewonnenen Daten gesammelt und die jeweiligen IT-Verantwortlichen dann entsprechend instruiert. Inzwischen sind wir dazu übergegangen, dass auch die IT-Verantwortlichen in den Standorten selbst aktiv mit dem Tool arbeiten. Das Security Lighthouse gibt das ja her. Zum einen werden die Mitarbeiter im Umgang mit dem System geschult, und zum anderen ist das System per se so komfortabel und bedienungsfreundlich gestrickt, dass die Mitarbeiter eigenverantwortlich damit umgehen können. Das ist auch ein Stück Motivation, wenn die Leute merken, schau an, ich kann selbst aktiv dazu beitragen, die IT-Sicherheit zu erhöhen und damit die Situation zu verbessern. Außerdem hoffen wir dadurch einen gewissen sportlichen Ehrgeiz in Sachen IT-Security zu wecken, nach dem Motto: Warum ist der andere Standort grün und meiner nicht?"

Bei SCHOTT bildet das Security Lighthouse den Sicherheitsstatus bis in die einzelnen Standorte hinein über die Security Information Map ab.
Quelle: AMPEG

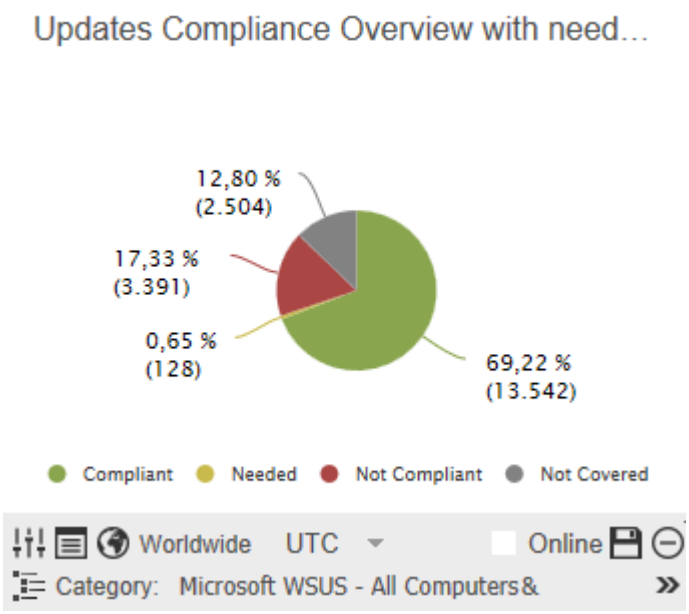
Gewollte Transparenz

Security Lighthouse ist auf maximale Transparenz ausgelegt. Bei SCHOTT bildet es den Sicherheitsstatus im weltweiten Office-Netzwerk bis in die einzelnen Standorte hinein über

die Security Information Map ab. Das System ist mit einer Ampelschaltung in den Symbolfarben Rot, Gelb und Grün hinterlegt. Auch kleinste Defizite und Schwachstellen werden durch das Monitoring systematisch aufgedeckt und visualisiert. Die IT-Abteilung legt die Karten damit auch für das Management des Unternehmens offen auf den Tisch. Für Dirk Ossenbrueggen als Head of Information Governance and Security ist diese „schonungslose" Transparenz absolut gewollt und Teil der Growth Culture des Unternehmens. Mehr noch: Sie ist für ihn das Kernelement des Systems. „Wenn ich diese Transparenz nicht habe und diese Transparenz auch nicht will, dann habe ich eine Mentalität, alles unter den Teppich kehren zu wollen. Und wenn die Dinge dann doch hochkommen, dann müsste ich mich fragen lassen, warum ich es nicht gewusst habe. Mein Weg ist der Weg der Transparenz. Das System zeigt mir die Baustellen, und ich kann an konkreten Plänen arbeiten. Auch wenn die Behebung eines Problems längere Zeit in Anspruch nimmt: Entscheidend ist doch, dass wir das Thema kennen. Das ist mir tausendmal lieber, als von irgendwas überrascht zu werden und mir von anderen Leuten erzählen zu lassen, pass mal auf, du hast deinen Laden nicht im Griff. Also deshalb lieber proaktiv rangehen und die Transparenz des Systems konstruktiv nutzen. Alles andere wäre in meinen Augen eine Scheinlösung."

OT-Sicherheit als zukünftiges Thema

Im Anschluss an die in der Startphase installierten Kollektoren wurden im weiteren Verlauf der Zusammenarbeit zusätzliche Kollektoren in Auftrag gegeben, darunter ein CMDB-Kollektor (Configuration Management Database) zur Erfassung von Informationen über alle Systeme, die im Service Management bekannt sind. Die Erfahrungen im globalen Office-Netz führen bei SCHOTT zu der Überlegung, das Monitoring mit AMPEG auch auf die Sicherheit der Operational Technology (OT) des Unternehmens auszudehnen.

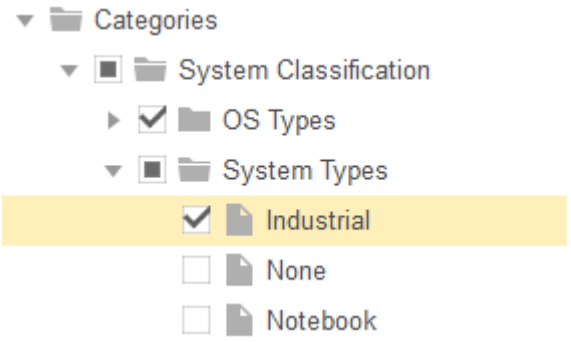


Das weltweite Sicherheitsniveau auf einen Blick. Quelle: AMPEG

„Wir haben das Security Lighthouse im Moment nur in der Office-IT. Wir sehen aber schon jetzt auch einen Teil von der Produktions-IT, nämlich da wo z. B. eine Endpoint-Protection Lösung in place ist, die eigentlich hinter der Firewall ist, aber eben mit der Zentrale telefoniert. Und da sehen wir dann auch Systeme, die eigentlich nicht im Office-Netz sind, sondern dahinter", erklärt Dirk Ossenbrueggen. „Unsere Überlegungen gehen dahin, die Produktion möglicherweise auch tiefergehend in das Monitoring einzubeziehen. Man muss aber schauen, wie praktikabel das auf diesem Sektor ist. Es wird nicht möglich sein, den

Sicherheit durch Transparenz - für ein Universum aus Glas

Systemen in der Produktion dieselben Regeln verordnen zu wollen wie denen im Office-Netz. Denn wenn ich der Produktion sage, ihr müsst eure Maschinen alle vier Wochen patchen, bedeutet das natürlich Maschinenstillstände, die naturgemäß nicht ohne Weiteres machbar sind. Eine Lösung für das Security Lighthouse könnte darin bestehen, dass man bei den Assets unterscheiden kann, ob es sich um IT oder OT handelt. Dann hätte ich zwei Kategorien, die sich unterschiedlich behandeln ließen. In eine solche Richtung könnte es zukünftig gehen."



Kategorisierung für die Analyse der Systeme aus der Fertigung.
Quelle: AMPEG

An dieser Stelle bleibt zu ergänzen, dass AMPEG inzwischen spezielle Kollektoren für den OT-Bereich entwickelt und bereitstellt. Insofern könnte die hier skizzierte Zukunftsvision von SCHOTT, neben der IT auch den OT-Sektor in das Monitoring zu integrieren, durchaus Realität werden.

Die Lösung wurde realisiert bei:

Schott AG
Hattenbergstraße 10
55122 Mainz, Deutschland
https://www.schott.com

Mit Unterstützung von:

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