FORCEPOINT
POWERED BY Raytheon

Case Study

EFAFLEX

RISIKEN VON DATENDIEBSTAHL UND INDUSTRIESPIONAGE VERRINGERN

„Die integrierte Data-Loss-Prevention-Lösung von Forcepoint kombiniert Web-, E-Mail- und Datensicherheit und sorgt für eine wirksame Überwachung und Kontrolle unserer anspruchsvollen Sicherheitsanforderungen."

— Karl Weinberger, IT-Leiter bei EFAFLEX in Bruckberg bei Landshut

GESELLSCHAFT
EFAFLEX Tor-und Sicherheitssysteme GMBH & Co. KG

INDUSTRIE
Fertigungsindustrie

PRODUKTE VERWENDET
Forcepoint Web Security Cloud, Forcepoint Email Security Cloud, Forcepoint DLP

ÜBERSICHT

Ob Dienstleister oder Maschinenbauer, jedes Unternehmen produziert täglich Daten, die den Betriebsablauf in Gang halten. Viele davon sind öffentlich zugänglich, manche nur für den internen Gebrauch bestimmt und ein Teil erfordert einen hohen Schutz. In einem Fertigungsunternehmen sind dies auf jeden Fall die Konstruktions- und Entwicklungszeichnungen sowie die damit verbundene Dokumentation. Zusammen gelten sie als die Kronjuwelen eines Betriebes.

Gerade bei mittelständischen, international tätigen Unternehmen aus dem produzierenden Gewerbe sind die Produktdetails zunehmend Ziel von Hackern und Industriespionage. Die Gefahren von außen bilden aber nur die eine Seite der Medaille. Übersehen werden oft die Gefahren innerhalb eines Unternehmens, wenn hochsensible Informationen ungewollt die Firma verlassen. Da muss noch nicht einmal böse Absicht dahinter stecken. Es genügt schon, wenn sich ein Mitarbeiter bei einer E-Mail-Adresse vertippt und schon gelangen die angehängten Pläne für den Prototyp eines neuen Produktes in die falschen Hände.

Um den ungewollten Datenabfluss zu verhindern, nutzt EFAFLEX, der Spezialist für Tor- und Sicherheitssysteme aus Bruckberg im niederbayerischen Landkreis Landshut, eine Data-Loss-Prevention (DLP)-Lösung. Sie erkennt und verhindert die nicht-autorisierte Weitergabe vertraulicher Dokumente und Konstruktionspläne und sorgt so für eine höhere Datensicherheit.

DATENLECKS ERFOLGREICH ABDICHTEN

Unternehmen aus dem produzierenden Gewerbe benötigen wirksame Regeln und Verfahren, um ihr geistiges Eigentum und das Know-how zu schützen. Seit einigen Jahren bereits hat EFAFLEX umfangreiche Maßnahmen in Form technischer Schutzsysteme wie Firewall, Antivirensoftware oder Spamfilter implementiert, um sich vor Hackerangriffen auf das Firmennetz zu schützen und überprüft die Wirksamkeit auch in regelmäßigen Abständen. „Wir arbeiten dabei mit einem auf IT-Compliance spezialisierten Partner zusammen, der unsere Systeme testet", berichtet Karl Weinberger, IT-Leiter bei EFAFLEX. „Gegen Angriffe von außen sind wir sehr gut gewappnet. Der Geschäftsleitung war jedoch bewusst, dass auch gegen eine unkontrollierte und unbeabsichtigte Weiterleitung vertraulicher Daten etwas unternommen werden muss. Diese Gefahren und Risiken galt es einzudämmen, sowie potenzielle Datenlecks zu ermitteln und effizient zu überwachen."
Bei der Suche nach der passenden technischen Lösung erwies sich das Know-how des IT-Compliance-Spezialisten Bösling, Zeh und Partner (BZP) aus dem rheinland-pfälzischen Schifferstadt als sehr hilfreich. Das Unternehmen verfügt über umfangreiche Erfahrungen in den Bereichen IT-Risikoanalyse und IT-Risikomanagement sowie Datenschutz und Sicherheitsberatung

und ist Platin-Partner von Forcepoint. Als technische Plattform empfahl BZP die Einführung von Forcepoint in Form einer V10000 Appliance. Forcepoint TRITON Architecture kombiniert alle bedeutenden Komponenten zur Gefahrenabwehr und dem Schutz vor Datenverlust in einer ganzheitlichen, kon-sistenten Content-Security-Lösung. Dazu zählen Web- und E-Mail-Security sowie Data Loss Prevention. Die Lösung zielt darauf ab, vor heimtückischen Bedrohungen und Datendiebstahl zu schützen – unabhängig davon, ob sie von außen oder von innen ausgehen.

SICHERHEITSREGELN FESTLEGEN UND UMSETZEN

Im Anschluss an die Grundsatzentscheidung installierte die IT-Abteilung von EFAFLEX zusammen mit IT-Sicherheitsspezialisten von BZP Forcepoint und führte einen Proof of Concept durch. Hier ging es unter anderem darum zu überprüfen, ob die Appliance generell den hohen Sicherheitsanforderungen des Fertigungsunternehmens gewachsen ist. Dass dem so ist, stellte sich schon bald heraus.

Besonders schützenswert bei EFAFLEX sind alle Konstruktionszeichnungen, denn in diesen Daten steckt die kreative Ingenieurskunst des Technologieführers von modernen hochentwi-ckelten Toranlagen. In einem ersten Schritt ermittelte das Projektteam per Software, welche CAD-Files, inklusive Dokumentation, vorhanden sind, wo diese gespeichert sind und ordnete die Daten einzelnen Sicherheitsklassen zu. Nur so lässt sich feststellen, was unbedingt schützenswert ist, denn nicht alle Daten müssen sich in einer hohen oder sehr hohen Sicherheitsstufe befinden.

Die Files zu lokalisieren und zu analysieren kann weitgehend automatisiert erfolgen. Wenn es darum geht sie zu klassifizieren, ist neben technischem vor allem auch fachliches Wissen gefragt. Letztlich ist festzulegen, wer welche Daten in welchen Geschäftsprozessen lesen oder ändern darf. Und vor allem: Wer darf welche Daten über welche Kanäle (E-Mail-Anhang, DVD oder anderes Speichermedium) an wen versenden? Dazu entwickelte das Projektteam ein neues Berechtigungskonzept und ergänzend dazu ein neue Richtlinie zur Ablage vertraulicher Daten. Als weitere Auswirkung zeigte sich darüber hinaus, dass es notwendig war, die Geschäftsprozesse, in denen diese Daten genutzt werden, neu zu gestalten.

„Einer der wichtigsten Punkte bei der Einführung einer DLP-Lösung ist die frühzeitige Information der Mitarbeiter“, erläutert Karl Weinberger. „Es kann nicht oft genug betont werden, dass es nicht darum geht, das Verhalten einzelner Mitarbeiter zu analysieren, sondern darum, das geistige Eigentum des Unternehmens zu schützen. Ohne die Akzeptanz der Anwender, und ohne die Information des Betriebsrats, lässt sich eine DLP-Lösung nicht erfolgreich einführen.“

Nachdem in einer ersten Phase die Regeln und das Vorgehen unter allen Beteiligten abgestimmt waren, nutzten die Mitarbeiter die Lösung im Alltag. Das Projektteam wertete die Erfahrungen über einen Zeitraum von rund sechs Monaten aus und nahm Feinjustierungen vor. Seit September 2013 arbeitet die Lösung im Produktivbetrieb.

RISIKEN ÜBERWACHEN UND GEFAHREN RECHTZEITIG ERKENNEN

Aktiv wird die DLP-Lösung dann, wenn ein Mitarbeiter Konstruktions- oder Entwicklungsdaten an einen Partner, Lieferanten oder Kunden per Mail versenden oder auf ein externes Speichermedium kopieren will. Die Grundlage dafür bildet eine Datenbank mit „digitalen Fingerabdrücken" aller als vertraulich klassifizierten Daten. Forcepoint analysiert den „digitalen Fingerabdruck" der Daten, die das Unternehmen verlassen sollen und vergleicht ihn mit dem gespeicherten Wert. Liegt kein Verstoß gegen die Sicherheitsregeln vor, kann der Mitarbeiter die Daten versenden.

Sehen die IT-Mitarbeiter in ihrer zentralen Managementkonsole, mit der sie die DLP-Lösung überwachen, dass es eine Warnung gibt, verständigen sie den fachlichen Vorgesetzten des Mitarbeiters. Meist lässt sich schnell feststellen, ob möglicherweise ein falscher Alarm vorliegt oder der Vorgesetzte zusammen mit der IT mit dem Mitarbeiter den Sachverhalt in einem Gespräch klären muss.

„Die integrierte Data-Loss-Prevention-Lösung von Forcepoint kombiniert Web-, E-Mail- und Datensicherheit und sorgt für eine wirksame Überwachung und Kontrolle unserer anspruchsvollen Sicherheitsanforderungen. Vertrauliche Daten aus der Konstruktion und Entwicklung sind bestmöglich abgesichert", berichtet Karl Weinberger. „In der Zwischenzeit hat die DLP-Lösung eine anfangs gar nicht beachtete Nebenwirkung: Forcepoint bietet umfangreiche IT-Sicherheitsfunktionen. Dadurch konnte die Zahl der Produkte im Bereich Web- und E-Mail-Security am Gateway auf nunmehr nur eine Lösung, nämlich Forcepoint, konsolidiert werden."

- Hauptsitz in Bruckberg im niederbayerischen Landkreis Landshut, Deutschland
- Umsatz von mehr als 100 Millionen Euro
- 900 Mitarbeiter; Tochtergesellschaften in Deutschland, Österreich, Schweiz, Großbritannien, Slowenien, Tschechien, Polen, Belgien und Russland

KONTAKT

www.forcepoint.de
+49 89 99216-427
info@forcepoint.com

ÜBER FORCEPOINT

[CASESTUDY_EFAFLEX_DE]-300017DE.030117