FORCEPOINT
POWERED BY Raytheon

Case Study

Hypo Landesbank Vorarlberg

GESELLSCHAFT
Hypo Landesbank Vorarlberg

INDUSTRIE
Banken und Finanzdienstleistungen

PRODUKTE VERWENDET
Forcepoint™ Data Security Suite

DATENDIEBSTAHL UND -VERLUST WIRKSAM VERHINDERN

„Die DLP-Lösung auf Basis der Websense Data Security Suite schützt durch eine schnelle und zuverlässige Datenanalyse vor Datenverlust und sorgt für eine wirksame Einhaltung unserer anspruchsvollen Sicherheitsvorschriften“

—Johannes Lutz, Leiter der dezentralen IT bei der Hypo Landesbank Vorarlberg in Bregenz

Finanzinstitut öffentlich eingestehen, dass auf dem Postweg eine CD mit Tausenden von Kundendaten verlorenging. Egal welche Informationen – Namen, Geburtsdaten, Adressen, Kontendaten – darauf alle gespeichert waren, der Imageschaden war enorm. Ob die Daten auf der CD verschlüsselt waren oder nicht, der Verlust ist unerfreulich genug. Passieren kann so etwas natürlich auch beim E-Mailversand: Ein Bankmitarbeiter vertippt sich bei der E-Mailadresse und schon geraten sensible Daten in die falschen Hände.

Damit so etwas nicht vorkommt, nutzt die Hypo Landesbank Vorarlberg eine Data-Loss-Prevention (DLP)-Lösung. Deren Aufgabe ist es, die Datensicherheit zu erhöhen und den Datenverlust zu verhindern, indem sie die nicht-autorisierte Weitergabe vertraulicher Daten erkennt und blockiert.

SICHERHEITSLÜCKE E-MAIL SCHLIESSEN

Gerade Finanzinstitute, die mit hochsensiblen Daten arbeiten, müssen alle nur möglichen vorbeugenden Maßnahmen treffen, damit vertrauliche Daten weder absichtlich noch unabsichtlich an Unbefugte weitergeleitet werden können. „Organisatorische Regeln darüber, wer was, wie und mit wem nach außen kommunizieren darf, gab es schon lange Zeit. Dem Vorstand aber war dies nicht genug“, berichtet Johannes Lutz, Leiter der dezentralen IT bei der Hypo Landesbank Vorarlberg in Bregenz. „Auch in der IT war uns bewusst, dass der E-Mail-Datenverkehr ein Sicherheitsrisiko darstellt. Unsere Vorstellungen von einer Lösung und der Auftrag des Vorstands, die organisatorischen Regeln technologisch abzusichern, haben sich daher sehr gut ergänzt.“ Datenverlust am E-Mail-Ausgang zu verhindern, führte das Projektteam eine Marktrecherche bei IT-Sicherheitsspezialisten und Systemhäusern durch. Wichtige Voraussetzung: Die Lösung musste mit der vorhandenen E-Mail-Infrastruktur, basierend auf IBM Notes und Domino, zusammenarbeiten.

Eine der Informationsquellen war der Magic Quadrant for Content-Aware Data Loss Prevention des Marktforschungsunternehmens Gartner. Als Ergebnis der Voruntersuchung blieben drei Anbieter übrig, von denen zwei einem ausführlichen Praxistest unterzogen wurden. Das Projektteam der IT-Abteilung installierte die Produkte beider Hersteller und führte anschließend mit den Daten aus dem E-Mail-Archiv umfangreiche Tests durch. Am Ende des Tages bot Forcepoint die organisatorisch ausgereiftere und technisch elegantere Lösung.

SICHERHEITSVORSCHRIFTEN DEFINIEREN UND WIRKSAM KONTROLLIEREN

Die eigentliche technische Implementierung der Software – die Forcepoint Data Security Suite – und die zusätzlichen Maßnahmen erwiesen sich dann doch als aufwändiger als ursprünglich veranschlagt. Aus organisatorischer Sicht wurde noch einmal

überprüft, welche Daten für die Hypo Landesbank Vorarlberg von kritischer Bedeutung sind und vor einer unbeabsichtigten Weitergabe geschützt werden müssen. Ermittelt wurde beispielsweise, in welchen Geschäftsprozessen die sensiblen Daten genutzt werden und welche Regeln es für den Umgang mit persönlichen und sensiblen Daten gibt. Denn alle diese Sicherheitsregeln müssen in der DLP-Lösung berücksichtigt werden.

Im Kern ging es um die Fragen: Welche Daten müssen geschützt werden? Wer darf in welchen Geschäftsprozessen welche Daten nutzen, lesen oder ändern? Wohin dürfen sensitive Daten sicher versandt werden? Bei sämtlichen organisatorischen Maßnahmen, die die Mitarbeiter der Bank betreffen, war von Anfang an der Betriebsrat involviert, denn die neue Lösung analysiert Mailinhalte, nicht aber das Verhalten der Mitarbeiter.

Technisches Herzstück der DLP-Lösung, realisiert mit der Forcepoint Data Security Suite, ist ein „digitaler Fingerabdruck" der zu schützenden operativen Daten. Dazu werden ausgewählte Merkmale aus dem Produktionsdatenbestand zusammengefasst. Die Data Security Suite speichert die digitalen Fingerabdrücke aller sensiblen Daten in einer zentralen, einmal täglich aktualisierten Datenbank. Sie dient als Referenz für die Überwachung aller Aktivitäten, die mit den sensiblen Daten vorgenommen werden.

MISSBRAUCH RECHTZEITIG ERKENNEN

Die DLP-Lösung von Forcepoint greift dann aktiv in das Geschehen ein, wenn als vertraulich charakterisierte Daten die Bank per IBM Notes Mail verlassen wollen. Zunächst berechnet die DLP-Lösung die Fingerprints der Daten in der E-Mail und vergleicht das Ergebnis mit den Werten in der Fingerabdruck-Datenbank und den damit verknüpften Sicherheitsvorschriften. Liegt kein Regelverstoß vor, können die Daten verschickt werden.

Zeigt sich dagegen, dass der Absender diese Daten nicht verschicken darf, erhält er eine Benachrichtigung und der Zustellvorgang wird gestoppt. Gleichzeitig erhält die Compliance-Abteilung der Bank eine Nachricht über den Vorgang. Sie bittet den Absender um eine Stellungnahme, warum die Daten verschickt werden sollen. Kann er dies begründen, wird die E-Mail verschickt.

Durch die Verbindung der digitalen Fingerabdrücke mit einer Kontrolle der Sicherheitsregeln, die festlegen, wer welche Daten wohin versenden darf, verhindert die DLP-Lösung Datenpannen. „Ein entscheidender Aspekt für die Akzeptanz der Lösung: Die Sicherheitsmaßnahmen müssen so dosiert sein, dass sich die Mitarbeiter in ihren Alltagsaktivitäten nicht beeinträchtigt fühlen", erläutert Andreas Schelling, zuständig für die IBM-Notes-Mail-Infra-struktur bei der Hypo Landesbank Vorarlberg.

Die Forcepoint Data Security Suite läuft seit Ende 2011 bei der Bank als eine unter VMware virtualisierte Software-Instanz auf einem Rechner mit Windows Server 2008. Die Mails selbst werden aus einem Rechenzentrum verschickt, das über eine SMTP-Strecke mit der Zentrale verbunden ist. „Die DLP-Lösung auf Basis der Forcepoint Data Security Suite schützt durch eine schnelle und zuverlässige Datenanalyse vor Datenverlust und sorgt für eine wirksame Einhaltung unserer anspruchsvollen Sicherheitsvorschriften", resümiert Johannes Lutz. „Sensible Bankdaten bleiben effizient geschützt. Als willkommener Nebeneffekt trägt die Lösung entscheidend zur Bewusstseinsbildung bei den Mitarbeitern bei, dass Bankdaten ein wertvolles Unternehmensgut sind."

CONTACT
www.forcepoint.com/contact

ABOUT FORCEPOINT

[CASESTUDY_HYPO_LANDESBANK_DE]-300026DE.011416