itsecurity
OKTOBER 2019

INKLUSIVE
IT-SA
SPEZIAL

E-MAIL-VERSCHLÜSSELUNG

BENUTZERFREUNDLICHE LÖSUNGEN

Günter Esch, SEPPmail Deutschland GmbH

KÜNSTLICHE INTELLIGENZ

Effizienz von Security-Lösungen steigern

DIGITALE INNOVATIONEN

Absicherung statt Schnellschuss

APPLICATION SECURITY

Sicherheit für externe Anwendungen

RISK ADAPTIVE PROTECTION
THOUGHT LEADERSHIP

SECURITY IS FOR SHARING

CERT & SOC Communication Congress auf der it-sa

IT-Security von Experten für Experten – unter diesem Leitgedanken findet im Oktober die international führende IT-Security-Fachmesse it-sa in Nürnberg statt. Mit dem Credo „Security is for sharing" ist operational services auch dieses Jahr ganz vorn mit dabei. Erleben Sie auf dem zweiten CERT & SOC Communication Congress am 09.10.2019 von 9:30 bis 12:30 Uhr die aktuellsten Trends und Herausforderungen im Bereich der operativen IT-Sicherheit. SOC- und CERT-Leiter, digitale Forensiker, Threat-Analysten sowie SIEM-Tuner präsentieren ihre Expertise wie gewohnt offen und produktneutral.

Melden Sie sich noch heute an und seien Sie dabei!

www.operational-services.de/itsa19

CERT & SOC Communication Congress
09.10.2019 // 09:30–12:30 Uhr
letzt anmelden!

COVERSTORY 10

INHALT

BENUTZERFREUNDLICHE LÖ FÜR SICHEREN E-MAIL-VERK

WARUM FÜHRT KEIN WEG AN DER E-MAIL-VERSCHLÜSSELUNG VORBEI?

Am 03. August feierte die E-Mail bereits ihren 35. Geburtstag, doch Unternehmen nutzen E-Mails mehr denn je für geschäftliche Zwecke. Das Thema E-Mail-Verschlüsselung wird allerdings noch immer stiefmütterlich behandelt. So zeigt eine Studie der Bitkom für den Bereich Industrie, dass lediglich 36 Prozent der Befragten eine Verschlüsselungslösung im Einsatz haben. Das Vertrauen in dieses Kommunikationsmittel ist also groß, obwohl sich eine unverschlüsselte E-Mail wie eine Postkarte lesen lässt. Hinzu kommt, dass die Europäische Datenschutz-Grundverordnung (EU-DSGVO) den Schutz personenbezogener Daten, die täglich über elektronische Post versendet werden, eindeutig vorschreibt. Wieso ist die Zahl der Nutzer von E-Mail-Verschlüsselungslösungen also noch so gering? Diese und weitere Fragen beantwortet Günter Esch, Geschäftsführer der SEPPmail Deutschland GmbH, im nachfolgenden Interview mit itsecurity Publisher Ulrich Parthier.

Ulrich Parthier: *Die E-Mail ist nun mitten in den Dreißigern. Insbesondere im Zuge der branchenübergreifenden Digitalisierung hat sich natürlich auch die digitale Kommunikation entwickelt. Wie sehen Sie als Experte die Entwicklung in diesem Bereich?*

Günter Esch: E-Mails sind aus dem Unternehmensumfeld kaum mehr wegzudenken. Der unverschlüsselte Versand elektronischer Nachrichten birgt jedoch auch Sicherheitsrisiken. Der größte Teil der Hackerattacken geht von E-Mails aus. Immer mehr Betriebe werden Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl. Dies kann einen immensen wirtschaftlichen Schaden verursachen. Demnach ist es umso wichtiger, Verschlüsselungslösungen für die Absicherung des E-Mail-Verkehrs einzusetzen. Vor allem im Mittelstand zeigt sich deutlicher Handlungsbedarf, der sich allein schon durch die Vorgaben der DSGVO ergibt.

Ulrich Parthier: *Glauben Sie, dass viele sich noch gar nicht im Klaren darüber sind, wie wichtig es eigentlich ist, E-Mails zu verschlüsseln?*

Günter Esch: Tatsächlich verwenden gerade mittelständische, eigentümergeführte Betriebe eher selten Lösungen zur E-Mail-Verschlüsselung, da sie solche Sicherheitsmaßnahmen als überflüssig erachten. In Gesprächen hört man häufig Fragen wie: „Wie viel Umsatz mache ich denn mehr, wenn ich meine E-Mails verschlüssele?“

Stellen Sie sich einmal folgendes Beispiel vor:

Eine Person fährt ständig über eine rote Ampel. Dies geht ein paar Wochen lang gut. Beim x-ten Mal wird sie jedoch von einem kreuzenden Auto gerammt oder von der Polizei erwischt und erhält eine

> EINE MODERNE LÖSUNG ZUM SCHUTZ VON E-MAILS SETZT SICH IM WESENTLICHEN AUS ZWEI KOMPONENTEN ZUSAMMEN: SIGNATUR UND VERSCHLÜSSELUNG.
>
> Günter Esch, Geschäftsführer, SEPPmail Deutschland GmbH, www.seppmail.de

SUNGEN EHR

Strafe. Übertragen auf den Einsatz einer Verschlüsselungslösung bedeutet dies Folgendes: Ein Unternehmen kann hunderte E-Mails mit sensiblen Inhalten verschicken und keine Probleme bekommen. Irgendwann tritt dann vielleicht der Fall ein, bei dem jemand einen Datenschutzverstoß meldet, der eine saftige Strafe zur Folge hat. Oder ein Hacker verschafft sich Zugang zu den Informationen und schadet dem Unternehmen dadurch. Hier zeigt sich, dass Firmen oftmals erst dann die Wichtigkeit von IT-Sicherheitsmaßnahmen erkennen, wenn es schon zu spät ist.

Es gibt allerdings genauso auch Unternehmen, die verstanden haben, warum E-Mail-Verschlüsselung so wichtig ist. Hinzu kommt derzeit die Motivation, Verschlüsselung einzuführen, um auf diese Weise nicht einen Wettbewerbsvorteil durch zum Beispiel Produktpiraterie zu verlieren.

? **Ulrich Parthier:** *Was sind Ihrer Erfahrung nach die Hauptkriterien, warum sich Entscheider in Unternehmen noch immer gegen Verschlüsselungslösungen zum Schutz ihrer vertraulichen E-Mails aussprechen?*

Günter Esch: Einer der Gründe, warum viele sich gegen solche Lösungen wehren, ist der vermeintlich technische Aufwand. Entscheider gehen oftmals davon aus, E-Mail-Verschlüsselung sei zu kompliziert und benötige übermäßig technisches Know-how. Doch es gibt bereits benutzerfreundliche Verschlüsselungslösungen, die einfach zu implementieren sind. Natürlich spielen auch die Kosten eine Rolle. An dieser Stelle sollte man aber bedenken, dass ein Datenschutzverstoß deutlich teurer ist als die Anbindung einer guten Verschlüsselungslösung, die E-Mails DSGVO-konform sichert.

? **Ulrich Parthier:** *Welche Funktionen sollte eine moderne E-Mail-Verschlüsselungslösung auf jeden Fall bieten? Und worauf ist bei der Wahl einer entsprechenden Lösung besonders zu achten?*

Günter Esch: Eine moderne Lösung zum Schutz von E-Mails setzt sich im Wesentlichen aus zwei Komponenten zusammen: Signatur und Verschlüsselung. Die Signatur stellt sicher, dass die versendete E-Mail auch wirklich vom entsprechenden Absender stammt und der Inhalt unterwegs nicht verändert wurde. Bei der Verschlüsselungslösung ist darauf zu achten, dass sie alle gängigen Standardtechnologien unterstützt. Zudem sollte die Lösung eine Spontankommunikation mit Empfängern zulassen, die selbst noch keine der Standardtechnologien einsetzen.

? **Ulrich Parthier:** *Welchen besonderen Mehrwert bietet SEPPmail im Vergleich zu anderen Herstellern?*

Günter Esch: SEPPmail verfolgt einen ganzheitlichen Ansatz für E-Mail-Sicherheit. Alle als vertraulich gekennzeichneten E-Mails werden auch wirklich verschlüsselt versendet und der Empfänger kann verschlüsselt antworten. Ein großer Vorteil unseres Secure E-Mail Gateway ist, dass wir alle Funktionalitäten unter einer Administrationsoberfläche bündeln: Signatur und mPKI, Verschlüsselung, Large File Transfer sowie Zentrales Disclaimer Management. Zudem unterstützen wir alle Standardtechnologien und überprüfen bei jedem Versand zunächst, ob der Empfänger mit eigenem Schlüsselmaterial ausgestattet ist. Wenn nicht, setzt unsere patentierte GINA-Technologie ein, mit der jeder x-beliebige Kommunikationspartner erreicht werden kann. Die verschlüsselte Datei wird dabei komplett ausgeliefert, ohne dass dafür zusätzliche Technologien auf der Empfängerseite notwendig sind.

? **Ulrich Parthier:** *Viele Unternehmen verlagern ihre Prozesse und Anwendungen in die Cloud. Reichen die Sicherheitsvorkehrungen der Cloud-Anbieter im Bereich der E-Mail-Kommunikation aus?*

Günter Esch: Nein, denn Cloud-Anbietern kann man nicht gänzlich vertrauen. Wenn diese sowohl das E-Mail-Management als auch die E-Mail-Verschlüsselung übernehmen, besitzen sie auch die Schlüssel und können E-Mails mitlesen. Da können wir schützend helfen.

? **Ulrich Parthier:** *Wie sehen Sie die Zukunft der E-Mail-Kommunikation? Können Sie schon einen Ausblick auf Ihre weiteren Pläne geben?*

Günter Esch: Unser aktuelles Motto lautet „SEPPmail goes Cloud". Es zählt der ganzheitliche Ansatz, sowohl interne als auch externe Datensicherheit zu gewährleisten. Der Kunde soll selbst die volle Kontrolle über seine Daten bei voller Cloud-Funktionalität haben. Dazu wird die SEPPmail Cloud-Lösung ständig weiterentwickelt und zukünftig um zum Beispiel eine Wizard-basierende Anmeldung ergänzt. Auch der Betrieb eigener Rechenzentren wird diskutiert.

! **Ulrich Parthier:** *Herr Esch, vielen Dank für das informative Gespräch!*

SENSIBLE INFORMATIONEN ZUVERLÄSSIG SCHÜTZEN

WIE UNTERNEHMEN DANK DATA-LEAK-PREVENTION-LÖSUNGEN VON MAXIMALER DATENSICHERHEIT PROFITIEREN.

UM DIE SICHERHEIT DER DATEN VOLLUMFÄNGLICH ZU GEWÄHRLEISTEN, MÜSSEN UNTERNEHMEN NICHT NUR ANGRIFFE VON AUSSEN ABBLOCKEN. WICHTIG IST GLEICHERMASSEN, BEDROHUNGEN VON INNEN, SO GENANNTE INSIDER THREATS, ABZUWEHREN.

Frank Limberger, Data and Insider Threat Security Specialist, Forcepoint, www.forcepoint.com

Cyber-Attacken werden zunehmend ausgefeilter und komplexer. Eine Herausforderung, der sich besonders Unternehmen stellen müssen, zu deren Kerngeschäft personenbezogene Informationen gehören. Zum Beispiel Banken.

Vermögen, Schulden, Kontobewegungen – Banken verfügen über eine große Menge sensibler personenbezogener Daten. Dementsprechend hoch sind ihre Ansprüche, was den Schutz dieser Daten und die Informationssicherheit im gesamten Unternehmen angeht. Denn die Privatsphäre ihrer Kunden ist ihr oberstes Gut.

Entscheidend für ein erfolgreiches IT-Sicherheitskonzept ist es zu verstehen, wie Menschen mit Daten umgehen und wo sich diese bewegen. Wichtige Informationen wie Art, Ort, Status und Zugriff auf die Daten lassen sich in einer komplexen IT-Landschaft dabei nur mit modernen Technologien erfassen. Um das Risiko von Datendiebstahl zu minimieren, setzen Banken zunehmend auf Data-Leak-Prevention-Lösungen (DLP). Die Finanzunternehmen profitieren dabei von einer hohen Transparenz hinsichtlich des Nutzerverhaltens und können so den Missbrauch sensibler Daten wirksam verhindern.

Die Privatsphäre der Kunden schützen

Um die Sicherheit der Daten vollumfänglich zu gewährleisten, müssen Unternehmen nicht nur Angriffe von außen wie etwa durch Malware oder Ransomware abblocken. Wichtig ist gleichermaßen, Bedrohungen von innen, so genannte Insider Threats, abzuwehren. Es gilt unter allen Umständen zu verhindern, dass sensible Informationen verbotenerweise nach außen gelangen. Dies kann aus unvorsichtigem, fahrlässigem Verhalten von Mitarbeitern ebenso resultieren wie aus vorsätzlichem, illegalem Datendiebstahl.

Um sich vor solchen Gefahren wirksam zu schützen, sind IT-Verantwortliche auf eine passende DLP-Security-Lösung angewiesen, die dem Faktor Mensch (human-centric) Rechnung tragen. Das absolute Vertrauen in die Mitarbeiter steht dabei außer Frage. Allerdings können Unternehmen auch Opfer versehentlicher Datenpannen sein und genau hier setzt DLP an. Mittlerweile empfiehlt auch die Eidgenössische Finanzmarktaufsicht FINMA ausdrücklich die Einführung von technischen Systemen, um bankinterne Informationen wirksam zu schützen.

Auswahl der richtigen Lösung

Werden IT-Teams vor die Aufgabe gestellt, eine geeignete Lösung für das Unternehmen auszuwählen, gilt es die Anforderungen genau zu definieren und nach einem klaren Benchmarking-Prozess vorzugehen. Die auszuwählende Lösung sollte in jedem Fall auch komplexe Security-Aufgaben zuverlässig erkennen und lösen können. Außerdem hilfreich: Ein System, das die Kontrolle direkt an den verschiedenen Workstations der einzelnen Benutzer durchführt. Das gewährleistet maximale Transparenz und einen guten Überblick. Nutzerfreundlichkeit ist ein weiteres wichtiges Stichwort bei der Auswahl einer neuen DLP-Lösung. Das zahlt sich schon bei der Implementierung und später auch bei Wartungsprozessen aus.

Eine große Herausforderung, der sich Banken genau wie alle anderen Unternehmen, die mit besonders schützenswerten Daten arbeiten, gegenüber sehen: Die Aufbewahrung dieser sensiblen Daten. Besonders Unternehmen im Finanzsektor unterliegen weltweiten Kontrollen zahlreicher Aufsichtsbehörden. Deren Datenschutzgesetze schreiben in der Regel vor, dass die betroffenen Daten innerhalb der jeweiligen Landesgrenzen aufbewahrt werden müssen. Eine Möglichkeit für IT-Verantwortliche ist deshalb, die DLP-Software dezentral einzu-

setzen. Dieses Vorgehen ist allerdings relativ komplex und teuer in der Wartung, da alle einzelnen Stellen, an denen die Software im Einsatz ist, einzeln gewartet werden müssen. Die Alternative: ein Security-System, das landesweit zentral über einen Security Manager gehostet wird – jedoch mit dezentralen Richtlinien. Dadurch lassen sich Vorfälle nun problemlos von Mitarbeitern der verteilten Zweigstellen bearbeiten.

Datenfluss über sämtliche Kanäle lückenlos überwachen

Idealerweise ist es mit einer DLP-Lösung möglich, das komplette Management rund um die Sicherheit von Daten und Informationen lückenlos zu koordinieren und über alle Kanäle zu überwachen – besonders diejenigen, die sich nicht blockieren lassen. Dabei sollten sich mehrere administrative Bereiche festlegen lassen, sodass beispielsweise getrennte Richtlinien für verschiedene Standorte definiert und die Verwaltung des Systems an diese delegiert werden kann.

Zudem dient das DLP-System zur strikten Durchsetzung von Richtlinie, wonach Daten nur dann aus einer Bank fließen dürfen, wenn sie eingesehen und geprüft werden können. Überdies übernimmt die Lösung einen Prozess, der in vielen Banken noch manuell stattfindet: Sie kontrolliert private Daten, die Mitarbeiter beim Ausscheiden aus dem Unternehmen mitnehmen möchten. Ein Vorgang, der ohne IT-System die Gefahr von Datenlecks in sich birgt. Mit der richtigen Lösung lassen sich solche Dateien systematisch mit Network-Discovery-Funktionen scannen.

Ein weiterer Vorteil von human-centric DLP-Lösungen: Durch ihren Einsatz sind die Mitarbeiter sensibilisiert. Sie gehen bewusster und vorsichtiger mit den Informationen um, übernehmen mehr Verantwortung für die Datensicherheit. Dennoch lässt sich eine drohende Datenpanne aus Unachtsamkeit nie ganz ausschließen. In diesem Fall kann eine DLP-Lösung verlässlich eingreifen und wirkungsvoll verhindern, dass Bankangestellte Daten unabsichtlich per E-Mail verschicken oder wissentlich auf externe Datenträger kopieren. Ausgehende Nachrichten werden lückenlos gescannt. Dabei erfolgt eine Klassifizierung kritischer Informationen. Das System ist in der Lage, solche klassifizierten Daten automatisiert zu erkennen und den Versand zu blocken.

Datenlecks wirksam verhindern

Immer mehr Banken setzen auf DLP-Lösungen und machen diese zu einem zentralen Bestandteil ihrer Sicherheitsarchitektur. Sie geben einen transparenten Einblick in die Verwendung und den Speicherort von strukturierten und unstrukturierten, sensiblen Daten – sei es von Kunden, Mitarbeitern oder Geschäftspartnern. Unternehmen profitieren dabei von einer umfassenden Kontrolle über ausfließende Daten und können Datenlecks wirksam verhindern. Gerade für Banken ist das wesentlich, um sensible Daten vor Missbrauch zu schützen, die Wahrung der Privatsphäre ihrer Klienten als strategisches Ziel zu realisieren und das Ansehen der Banken selbst langfristig zu sichern.

Frank Limberger

FORCEPOINT DATA LEAK PREVENTION

Eine große Schweizer Bank mit Hauptsitz in Zürich setzt für ihre Cybersicherheit bereits auf die DLP-Lösung von Forcepoint. Der Vorteil: Sie lässt sich über ein Security-System, das in der ganzen Schweiz zentral über den Forcepoint Security Manager gehostet wird, mit dezentralen Richtlinien steuern. Durch die DLP-Lösung ist genau festgelegt, welche Daten von welchen Personen für welche Zwecke verwendet werden dürfen. Das sensibilisiert die Mitarbeiter dafür, achtsam mit Daten umzugehen. Dennoch lassen sich Datenpannen aufgrund von menschlicher Unachtsamkeit nie zu 100 Prozent ausschließen. Die Forcepoint DLP-Lösung greift in solchen Fällen verlässlich ein und es lässt sich wirkungsvoll verhindern, dass Bankangestellte Daten unabsichtlich in die falschen Hände geben.

ACHILLESFERSE SERVICEKONTO

BLACK HAT-UMFRAGE ENTHÜLLT DEN BELIEBTESTEN ANGRIFFSPUNKT DER HACKER.

Obwohl eine vernachlässigte Passwortrotation eines der größten Sicherheitsrisiken in der Verwaltung von privilegierten Accounts darstellt, werden rund 35 Prozent der Passwörter für sensible Servicekonten niemals oder nur nach einem Sicherheitsvorfall geändert. Dies ist das Ergebnis des aktuellen 2019 Black Hat Hacker Surveys von Thycotic.

Die Achillesferse der Unternehmens-IT

Einigkeit herrschte dabei unter anderem in Sachen Angriffsziel: Sowohl Hacker als auch Sicherheitsprofis sehen demnach in Servicekonten einen beliebten Angriffspunkt. Das liegt nicht zuletzt daran, dass diese Accounts Zugriff auf sensible Informationen gewähren und zudem Möglichkeiten der Privilegien-Erhöhung bereithalten. Da Servicekonten selten von menschlichen Usern genutzt werden und ihre Aufgaben dementsprechend „hinter den Kulissen" erfüllen, werden sie selten überprüft. Gleichzeitig zögern IT-Administratoren, Servicekonten zu deaktivieren, da sie ihre Abhängigkeiten oft nur schwer verstehen können und eine störende Betriebsunterbrechung unbedingt vermeiden wollen. Dabei sind Servicekonten in der Cloud, on-premises oder in hybriden Umgebungen gleichermaßen gefährdet, wie die befragten Hacker klarstellen.

Nachlässigkeit bei der Passworthygiene

Eine schlechte Passworthygiene in den Unternehmen spielt den Angreifern bei der Kompromittierung von Service-Accounts oft in die Hände. Beide Gruppen monieren, dass Passwörter für Servicekonten nicht regelmäßig geändert werden, obwohl eine vernachlässigte Passwortrotation eines der größten Sicherheitsrisiken in der Verwaltung von privilegierten Accounts darstellt. In 44 Prozent der Fälle treffen die befragten Hacker bei ihren Angriffen demnach auf Accounts, deren Zugriffsdaten nie oder nur nach einem Security-Vorfall geändert werden. In immerhin 36 Prozent der Fälle rotieren die Passwörter einmal pro Monat, was den Hackern jedoch immer noch rund 30 Tage Zeit gibt, um ihren Angriff durchzuführen und sich lateral im Netzwerk zu bewegen. Diese Angaben decken sich mit den Antworten der befragten Security-Professionals, von denen 36 Prozent zugaben, Servicekonto-Passwörter nie oder nur nach einem Incident zu wechseln. Täglich werden die Passwörter laut Report nur in rund 3,5 Prozent der Fälle gewechselt.

Konsequente Verwaltung

Um privilegierte Accounts wie Service-Konten vor Missbrauch zu schützen, bedarf es neben einer Passwortrotation weiterer Sicherheitsmaßnahmen, darin sind sich Hacker wie IT-Pros einig. Beide Gruppen empfehlen zum einen eine wirksame Identifizierung und Entfernung veralteter und entbehrlicher Accounts, da sie schnell übersehen werden können und ihr Missbrauch lange unentdeckt bleiben kann. Zum anderen sollten IT-Abteilungen alle Aktivitäten von privilegierten Konten streng überwachen, um verdächtiges Verhalten frühzeitig zu erkennen.

www.thycotic.com

WARUM SIND SERVICEKONTEN EIN BEVORZUGTES ZIEL VON HACKERN?