IT-SICHERHEIT
Management und Technik

BANKMAGAZIN

SPECIAL

IT-Sicherheit in der Banken- und Finanzwelt

Business-Continuity

Warum E-Mail-Archivierung Teil der IT-Strategie sein sollte

Marktüberblick

Relevante Hersteller/Dienstleister und ihre Angebote

DATAKONTEXT

Cybersicherheit im Finanzwesen: **Herausforderungen und Probleme**

Die Banken- und Finanzwelt ist bei der Digitalisierung vergleichsweise weit vorn, nicht zuletzt, um den Wünschen ihrer Kunden gerecht zu werden – und natürlich auch, um Kosten für teure Filialen einsparen zu können. Hinzu kommt der Innovationsdruck durch neue FinTechs, die zum Beispiel Banking und Trading nur noch per Smartphone-App anbieten. Die zunehmende Zahl digitaler Prozesse führt jedoch dazu, dass sich die Angriffsflächen für Cyberkriminelle immer mehr vergrößern.

Vor dieser Gefahr – die Finanzbranche gehört immerhin zu den am häufigsten angegriffenen Zielen – versuchen sich die Banken zu schützen. Laut einer Studie von YesWeHack setzen sie dabei erwartungsgemäß vor allem technische Maßnahmen ein. Zudem führen 66 Prozent der 208 befragten Experten aus Banken, Versicherungen oder Finanzdienstleistern in ihren Unternehmen regelmäßig Sicherheitsschulungen für neue und bestehende Mitarbeiter durch. An dritter Stelle folgen laut Studie punktuelle Sicherheitsaudits und Penetrationstests.

Darüber hinaus fragte man die Experten, für wie effektiv sie bestimmte Maßnahmen halten. Das Ergebnis: Wie häufig Sicherheitsmaßnahmen im Einsatz sind, sagt noch nichts darüber aus, als wie wirksam sie angesehen werden. So halten der Studie zufolge 73 Prozent die Datenverschlüsselung für sehr wirksam, obwohl nur 57 Prozent der Befragten diese Methode einsetzen. Anwendungs- und Gerätekontrollen werden von 68 Prozent als wirksam oder sehr wirksam eingeschätzt, aber nur von 49 Prozent umgesetzt.

Die Probleme, mit denen die Finanzbranche bei der Abwehr von Cyberangriffen zu kämpfen hat, sind – wie in anderen Branchen auch – herausfordernd. Für mehr als die Hälfte der Befragten (51 Prozent) steht laut Studie dabei der Faktor Mensch im Vordergrund: Es fehlen vor allem Cybersicherheits-Experten in den Teams. 49 Prozent sehen in der stetig steigenden Zahl von Cyberattacken die größte Herausforderung, 47 Prozent in den zusätzlichen potenziellen Angriffspunkten, die durch Homeoffice und andere hybride Arbeitsmodelle entstehen.

Mit unserem Banken- und Finanz-Special in Kooperation mit der Zeitschrift BANKMAGAZIN können Sie sich einen Einblick in aktuelle Themen und praxisnahe Lösungen rund um die Cybersicherheit verschaffen. Viel Freude mit dem gemeinsamen Produkt!

Ihr
Sebastian Frank

Sebastian Frank

IMPRESSUM

IT-SICHERHEIT
Management und Technik

www.itsicherheit-online.com

in Kooperation mit

BANKMAGAZIN

www.bankmagazin.de

SPECIAL: IT-Sicherheit in der Banken- und Finanzwelt

Verlag:
DATAKONTEXT GmbH
Standort Frechen
Augustinusstr. 11 A · 50226 Frechen
www.datakontext.com

Chefredaktion:
Sebastian Frank (S.F.)
E-Mail: s.frank@kes.de

Online-Redaktion:
Jessica Herz (Leitung Online)
herz@datakontext.com
+49 2234 98949-80
Lisa Bieder
Konstantin Falke
Silvia Klüglich
Janek Mazac
Chiara Schönbrunn

Gründer: † Bernd Hentschel

Grafik/Layout/Satz:
Michael Paffenholz
Tel.: +49 173 8382572
E-Mail: michael.paffenholz@gmx.de
Objekt- und Anzeigenleitung:
Wolfgang Scharf
Tel.: +49 2234 98949-60
E-Mail: wolfgang.scharf@datakontext.com
zzt. gilt die Anzeigenpreisliste Nr. 29
Vertrieb/Herstellung:
Dieter Schulz
Tel.: +49 2234 98949-99
dieter.schulz@datakontext.com
Abonnement: Jahresabonnement € 129,- inkl. VK (Inland)

Erscheinungsweise: sechs Ausgaben
Alle Preise verstehen sich inkl. MwSt. Der Abonnementpreis wird im Voraus in Rechnung gestellt. Das Abonnement verlängert sich zu den jeweils gültigen Bedingungen um ein Jahr, wenn es nicht mit einer Frist von 8 Wochen zum Ende des Bezugszeitraumes gekündigt wird.
Erscheinungsweise, Bezugspreise und -bedingungen: Abonnement und Bezugspreis beinhalten die Print-Ausgabe sowie eine Lizenz für das Online-Archiv. Die Bestandteile des Abonnements sind nicht einzeln kündbar. Der Preisanteil des Online-Archivs ist auf der Abonnementrechnung separat ausgewiesen.
Aboservice:
Hüthig Jehle Rehm GmbH, München,
Tel.: +49 89 21 83-7110
Druck: Grafisches Centrum Cuno GmbH & Co. KG, Calbe (Saale)

Genderhinweis: Gleichberechtigung ist uns wichtig! Für eine bessere Lesbarkeit unserer Fachtexte verzichten wir jedoch auf die gendergerechte Schreibweise und nutzen das generische Maskulinum als neutrale grammatikalische Form. Personenbezeichnungen beziehen sich auf alle Geschlechter.

Titelbild: Ar_TH - stock.adobe.com, Who is Danny - stock.adobe.com
Fotos: Firmenbilder; DATAKONTEXT; iStock.com/Drazen_; Parradee - stock.adobe.com, vegefox.com - stock.adobe.com, Xilon - stock.adobe.com

29. Jahrgang 2023 · ISSN: 1868-5757

_Inhalt

Anbieter

Warum E-Mail-Archivierung im Bankensektor Teil der IT-Strategie sein sollte

Business-Continuity ist mehr als nur ein Backup

Wie die meisten Unternehmen in Deutschland, Österreich und der Schweiz sind auch Banken als Teil der Finanzbranche dazu verpflichtet, wichtige Dokumente über lange Zeit hinweg zugänglich aufzubewahren - einschließlich des elektronischen Schriftverkehrs. Was dabei zu beachten ist und welche Rolle professionelle E-Mail-Archivierungslösungen dabei spielen, erläutert unser Beitrag.

Jahr für Jahr steigt durch die Digitalisierung das Volumen von strukturierten und unstrukturierten Daten sowie sensiblen und personenbezogenen Inhalten. Darüber hinaus haben sich die IT-Infrastrukturen in Unternehmen – unter anderem bedingt durch das Aufkommen dezentraler und flexibler Arbeitsmodelle – in den letzten Jahren deutlich verändert. IT-Manager müssen stark fragmentierte Informationslandschaften verwalten, und die Daten sind heute auf verschiedene lokale sowie Multi- und Hybrid-Cloud-Systeme verteilt. Für IT-Verantwortliche sind diese Rahmenbedingungen eine echte Herausforderung und erfordern ein gut durchdachtes Informationsmanagement inklusive E-Mail-Management.

Erschwerend kommt hinzu, dass der Gesetzgeber von den meisten Unternehmen verlangt, steuer- und handelsrechtlich relevante Daten – unabhängig ihres Speicherortes – lückenlos aufzubewahren. Das schließt auch elektronische Dokumente mit ein und wird in Deutschland unter Berücksichtigung der „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)“ geregelt.

Strenge gesetzliche Vorgaben

Von diesen Vorgaben sind Unternehmen des Finanzwesens nicht ausgeschlossen. Beispielsweise müssen Banken in Deutschland Bücher, Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, Eröffnungsbilanzen und Buchungsbelege mindestens zehn Jahre verfügbar halten. Bankkunden können demnach Kontoauszüge der letzten zehn Jahre bei der Bank anfragen. Bei Handels- und Geschäftsbriefen liegt die Aufbewahrungsfrist bei sechs Jahren.

Da der Bankensektor ein Teil der regulierten Finanzbranche ist, greifen noch weitere gesetzliche Auflagen. Die zweite Fassung der EU-Direktive zum Wertpapierhandel „Markets in Financial Instruments Directive (MiFID II)“ aus dem Jahr 2018 verpflichtet im EU-Finanzsektor tätige Unternehmen, alle erbrachten Services und durchgeführten Geschäfte sauber und lückenlos zu dokumentieren. Die Aufzeichnungen sollen beispielsweise Aufsichtsbehörden oder der Rechtsabteilung dauerhaft zugänglich sein.

Darüber hinaus sind Unternehmen, die personenbezogene Daten erheben und verarbeiten, grundsätzlich dazu verpflichtet, die Grundsätze der europäischen Datenschutzgrundverordnung (DSGVO) einzuhalten – darunter Zweckbindung, Datenminimierung, Speicherbegrenzung sowie Integrität und Vertraulichkeit. Die geschäftskritischen Dokumente und Korrespondenzen von Unternehmen im Bankensektor enthalten solche sensiblen und personenbezogenen Inhalte, die es besonders zu schützen gilt. Daher greifen neben den für den Finanzmarkt spezifischen Regularien selbstverständlich auch die datenschutzrechtlichen Vorgaben der DSGVO. Im Übrigen gibt es in der Schweiz mit dem Datenschutzgesetz (DSG) sehr ähnliche Regularien.

Datenhoheit und Datenschutz

Bei der Verarbeitung und Speicherung von Daten – und in diesem Kontext besonders E-Mails und ihre Anhänge – müssen sich Unternehmen zwischen eigenen Servern, Software-as-a-Service-(SaaS)-Alternativen oder einer Hybridlösung entscheiden. Ist die Cloud Teil der Informationsmanagementstrategie, müssen sie prüfen, wo sich die jeweiligen Rechenzentren befinden, ob sie dort ausreichend geschützt sind und von wo Instanzen darauf zugreifen können. Gemäß Artikel 44 ff. DSGVO dürfen personenbezogene Daten nur dann an ein Drittland übermittelt werden, wenn das Datenschutzniveau den Anforderungen der EU entspricht. Zudem sind die Richtlinien der Europäischen Bankenaufsichtsbehörde (EBA)

sowie der Europäischen Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersvorsorge (EIOPA) zu berücksichtigen.

Im Zuge eines Vertragsabschlusses mit einem SaaS-Anbieter empfiehlt es sich, einen zusätzlichen Auftragsverarbeitungsvertrag (AVV) abzuschließen, um den Anforderungen des Artikels 28 DSGVO nachzukommen. Dieser ist erforderlich, wenn personenbezogene Daten im Auftrag an Dritte („Auftragsverarbeiter") weitergegeben und verarbeitet werden.

Business-Continuity: Backups sind nicht genug

Vom Gesetzgeber vorgeschriebene Regularien sind jedoch nicht die einzigen Aspekte, die Unternehmen im Bankensektor in ihrer Informationsmanagementstrategie bedenken sollten. Ebenso empfiehlt es sich, potenzielle Systemausfälle aufgrund von Problemen mit der hauseigenen IT-Infrastruktur, Ausfälle aufseiten von IT-Service-Providern, Anwenderfehler, Manipulation durch das absichtliche Löschen von Daten sowie die immer häufiger vorkommenden Cyber-Angriffe zu berücksichtigen. Diese Risiken können nicht nur den allgemeinen Geschäftsbetrieb beeinträchtigen, sondern ebenfalls zu einem erheblichen Datenverlust führen – einschließlich geschäftskritischer und sensibler E-Mail-Inhalte wie Rechnungen, Angebote oder Verträge. Kreditinstitute, Kapitalanlagegesellschaften, Leasinggesellschaften und sonstige Unternehmen des Bankensektors – dazu zählen im Übrigen auch Unternehmen aus dem Versicherungswesen – sollten daher eine entsprechende Lösung implementieren, um im Ernstfall eine umfangreiche Wiederherstellung betroffener Daten vornehmen zu können. Ansonsten drohen ihnen unter anderem juristische Konsequenzen, da entsprechende Aufsichtsbehörden prüfen, ob Datenschutzvorgaben und Aufbewahrungspflichten eingehalten wurden. Wenig überraschend: Bei einem schwerwiegenden Ausfall des E-Mail-Servers ist die Wahrscheinlichkeit hoch, dass dies nicht der Fall ist.

Oftmals gehen Unternehmen davon aus, dass ein Backup-System ausreicht, um sich vor einem Datenverlust zu schützen und die Geschäftskontinuität zu wahren. Das ist jedoch ein Trugschluss. Ein Backup-System legt in vordefinierten, regelmäßigen Abständen Kopien der E-Mail-Daten beziehungsweise des ganzen E-Mail-Servers in der Cloud oder auf einem anderen externen Speichermedium ab. Neue Datenbestände, die nach einem durchgeführten Backup entstanden sind, werden erst im darauffolgenden Backup-Zyklus gesichert und sind bis zu diesem Zeitpunkt dem Risiko ausgesetzt, dauerhaft verloren zu gehen. Ein erfolgreiches Backup kann den E-Mail-Server wieder verfügbar machen, ist aber keine Garantie für eine lückenlose Wiederherstellung des historischen E-Mail-Bestandes. Im Sinne der Disaster-Recovery mag dies für die akute Wiederherstellung von Daten ausreichen, ist jedoch nicht konform mit rechtlichen Vorgaben, die eine vollständige und revisionssichere Aufbewahrung voraussetzen. Zwar sollten Unternehmen im Bankensektor Backup-Lösungen in ihrer Business-Continuity-Strategie selbstverständlich einplanen, sie brauchen ergänzend aber noch eine weitere Lösung, die E-Mails revisionssicher vorhält, bewahrt und dauerhaft verfügbar macht – und das unter Berücksichtigung von datenschutzrechtlichen Rahmenbedingungen.

Revisionssichere E-Mail-Archivierung

Eine professionelle, unabhängige E-Mail-Archivierungslösung bietet sich als Ergänzung zu herkömmlichen Backup-Systemen an. Sie erstellt kontinuierlich Kopien von einzelnen E-Mails samt Anhängen und speichert diese lückenlos, revisionssicher und über einen langen Zeitraum hinweg in einem zentralen Archiv.

Professionelle E-Mail-Archivierungslösungen bieten die Möglichkeit, je nach Bedarf zwischen verschiedenen strategischen Archivierungsansätzen zu wählen. Wenn die rechtskonforme E-Mail-Archivierung im Vordergrund steht, ist die Journalarchivierung die beste Archivierungsoption. Wenn die Entlastung des E-Mail-Servers das Hauptziel ist, ist die Archivierung von Postfächern in Verbindung mit definierbaren Löschregeln die bessere Wahl. Auch eine Kombination beider Ansätze ist möglich, sodass Unternehmen des Bankensektors von beiden Archivierungsansätzen profitieren und die E-Mail-Archivierungslösung als unverzichtbaren Teil ihrer IT-Strategie einsetzen können.

Ein weiterer Vorteil ist, dass die Einsicht in und der Zugriff auf das Archiv auch bei Ausfall des E-Mail-Dienstes möglich ist. Hier erweisen sich Such- und Exportfunktionen besonders im Rahmen von Compliance-Audits oder in Rechtsstreitigkeiten (Stichwort „E-Mail als Beweis vor Gericht") als hilfreich. Auch Mitarbeiter können je nach Konfiguration E-Mail-Bestände eigenständig durchsuchen und Daten bei Bedarf in ein Standardformat exportieren oder wiederherstellen. Dafür müssen sie keine Anfragen mehr an die IT-Abteilung stellen.

Fazit

Eine E-Mail-Archivierungslösung unterstützt Unternehmen in stark regulierten Branchen dabei – wie in diesem Fall Unternehmen des Bankensektors als Teil der Finanzbranche – rechtlichen und damit auch datenschutzrechtlichen Anforderungen nachzukommen. Sie kann die vollständige und revisionssichere Aufbewahrung aller relevanten E-Mails über mehrere Jahre hinweg gewährleisten – Mitarbeiter und Prüfer gleichermaßen können kontinuierlich auf den gesamten archivierten E-Mail-Bestand zugreifen. Diese Vollständigkeit ist ein wichtiger Baustein jeder Business-Continuity-Strategie. Daher sollte eine professionelle E-Mail-Archivierungslösung, ergänzend zu Backup- und Security-Lösungen, in keinem Unternehmen fehlen. ■

Roland Latzel
ist Senior Director of Marketing bei der MailStore Software GmbH.

Ganzheitliches Management-system und internes Kontroll-system (IKS) nach BaFin VAIT bei der HanseMerkur Kranken-versicherung AG

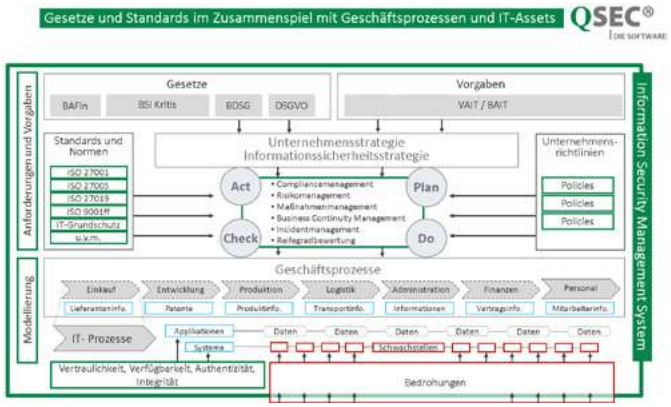
Autorin: Ellen Wüpper,
Geschäftsführung Vertrieb/Marketing der WMC GmbH

Als Versicherungsunternehmen unterliegt die HanseMerkur neben den grundsätzlich geltenden Anforderungen an Informationssicherheit und Datenschutz ergänzend den regulatorischen Bestimmungen der BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht). Im Kontext der Informationssicherheit hat die BaFin die versicherungsaufsichtlichen Anforderungen an die IT, abgekürzt VAIT, im März 2019 veröffentlicht.

Bereits vor dem Inkrafttreten der VAIT-Anforderungen hat sich die HanseMerkur seit 2017 auf künftig steigende Herausforderungen zu Datenschutz, Informationssicherheit und Risikomanagement vorbereitet. Während der intensiv betriebenen IST-Analyse in diesen Themenbereichen wurde deutlich, dass nachhaltige Verfahren und Prozesse für zukünftige Anforderungen mit den bis zu diesem Zeitpunkt etablierten Bordmitteln wie Word, Excel oder PowerPoint nicht sinnvoll und ressourcensparend abgebildet werden können.

Es wurde klar, dass die komplexen Anforderungen toolgestützt deutlich besser zu managen sein würden. Für die Auswahl eines geeigneten Lösungsanbieters war die erklärte Anforderung, einen Partner zu finden, der nicht nur eine im Markt gut etablierte Managementlösung für Datenschutz und Informationssicherheit nach allen Anforderungen der Versicherungsbranche anbietet, sondern auch den gewünschten Zusatznutzen zum Aufbau eines ganzheitlichen internen Kontrollsystems (IKS) innerhalb der Software darstellen kann.

Das im Finanzbereich vielfach eingesetzte GRC und Information Security Management System (ISMS) QSEC bildet die Datenschutz- und ISMS-Anforderungen lückenlos ab und unterstützt unter Berücksichtigung der versicherungsrechtlichen Aspekte aus der BaFin VAIT. Dabei integriert sich das System in die IT-Landschaft des Unternehmens und bereits vorhandene, für die Umsetzung erforderliche Daten, können aus den führenden Systemen übernommen werden.



QSEC-Datenmodelldarstellung-Banken und Finanzen

Die Funktionalitäten von QSEC reichen über Datenschutz und ISMS weit hinaus und bieten alle Möglichkeiten eines internen Kontrollsystems (IKS) unter Berücksichtigung der versicherungsrechtlichen Aspekte nach VAIT. QSEC bietet:

- die Nachweisbarkeit der Compliance
- die transparente und nachhaltige Darstellung von Risiken (reduziert, akzeptiert etc.)
- Best Practice Prozesse (die Methodik wird von QSEC zur Verfügung gestellt)
- Synergien durch die Verbindung von Informationssicherheit und Datenschutz
- die Effizienz im Sicherheitsmanagement bei gleichzeitiger Optimierung von Ressourcen und Investitionen
- Imagegewinne und Wettbewerbsvorteile

QSEC überzeugte u.a. dadurch, dass die HanseMerkur ihre aus der Geschäftsstrategie abgeleiteten Vorgehensweisen zur IT-Strategie in QSEC komfortabel über die Standardfunktionalitäten implementieren konnte. QSEC ermöglicht HanseMerkur die IT Governance, das effiziente Steuern, Überwachen und Weiterentwickeln, aller erforderlicher Maßnahmen.

Mit QSEC hat die HanseMerkur heute deutlich mehr Transparenz über potenzielle Risiken und deren Auswirkungen und kann effizient angemessene Maßnahmen zur Verbesserung und Weiterentwicklung des Reifegrads für alle Anforderungen aus Datenschutz, Informationssicherheit, IKS-Kontrollen und VAIT-Vorgaben entwickeln.

„Mit WMC haben wir einen Partner gewonnen, der unsere „Sprache" spricht und offen auf unsere Anforderungen und Ideen reagiert. Die Partnerschaft mit WMC hat mich durch die gesamte Laufzeit der Zusammenarbeit überzeugt", so Thomas Prigge, Informationssicherheitsbeauftragter der HanseMerkur

Die komplette Case Study: „Ganzheitliches Managementsystem und internes Kontrollsystem (IKS) nach BaFin VAIT bei der HanseMerkur Krankenversicherung AG" finden Sie **hier.**

Mehr dazu hier

HanseMerkur

QSEC® DIE SOFTWARE

Kontaktinfo:
WMC GmbH
Zimmerstraße 1, 22085 Hamburg
Tel: +49 40 650336-0
E-Mail: info@wmc-direkt.de · **www.wmc-direkt.de**

Sicher und einfach: biometrische Authentifizierung für Banken

Autor: Stephan Schweizer

Onlinebanking wird bei Bankkunden immer beliebter. Im Jahr 2022 lag der Anteil der Personen, die ihre Bankgeschäfte über das Internet abwickelten, bei rund **49 Prozent.** Sicherheit ist dabei das wichtigste Thema für die Kunden. In einer **Studie** von SurePay in Zusammenarbeit mit dem ECC Köln gaben knapp 50 Prozent der Befragten an, dass sie einen Wechsel in Betracht ziehen würden, wenn sie sich bei ihrem Finanzinstitut nicht sicher fühlen.

Wichtig ist den Kunden auch, dass die Anmelde- und Transaktionsprozesse möglichst reibungslos funktionieren. Ein wichtiger Bereich ist dabei die Kundenauthentifizierung. Hier gibt es einige Herausforderungen, die aber gelöst werden können.

Stolpersteine bei der Authentifizierung

Bei der Authentifizierung gibt es bei vielen, aber nicht bei allen Banken Probleme. So setzen nicht alle Finanzinstitute auf die aktuelle Form der passwortlosen Authentifizierung nach dem aktuellen und international anerkannten FIDO-Standard. Viele nutzen noch das mTAN-Verfahren oder Hardware-Token. Beides ist weder für die Sicherheit noch für die Benutzerfreundlichkeit ideal.

Ähnliches gilt für Sicherheitsmaßnahmen, die nach dem Login-Prozess etabliert werden. Hierzu zählen insbesondere kontextbasierte Verifikationen wie Device Fingerprint oder verhaltensbiometrische Merkmale. Die Sicherheitssysteme der Banken müssen in der Lage sein, diese Merkmale auszuwerten und bei Abweichungen zum Beispiel durch eine erneute Authentifizierung einzugreifen. Solche Sicherheitsmaßnahmen, die beim Login eines Kunden oder während der Kontositzung implementiert werden, setzen nur die Hälfte der großen Banken ein. Zu groß ist die Angst vor False Positives, die zur ungerechtfertigten Sperrung von Kundenkonten führen können.

Diese Angst ist jedoch unbegründet, da durch ein sicheres und FIDO-konformes Login die zusätzlichen Maßnahmen weniger streng ausfallen können. Diese greifen dann nur bei extremen Abweichungen. Das Kundenerlebnis wird dadurch nicht beeinträchtigt.

Ein reibungsloses Kundenerlebnis und hohe Sicherheit sind kritische Erfolgsfaktoren für Banken. Eine schlechte User Experience kann ausreichen, um 20 Prozent der eigenen Kunden dauerhaft zu verlieren. Eine gute User Experience wird daher heute von den Kunden erwartet – fehlt sie, ist das für die Banken ein handfester Wettbewerbsnachteil.

Dies liegt zum einen am Mangel an qualifiziertem Personal. Zum anderen wird gerade im Bankensektor häufig Individualsoftware eingesetzt, um den hohen Sicherheitsanforderungen gerecht zu werden. Doch meist gehen die bankinternen Richtlinien noch deutlich über die regulatorischen Anforderungen hinaus. Dies führt dazu, dass der Aufwand den Nutzen übersteigt. Entsprechend schwierig ist es, die so entstandenen, sehr sicheren, aber auch extrem abgeschotteten Datensilos zu öffnen, um beispielsweise neue Dienstleistungen anbieten zu können.

Herausforderungen für die Modernisierung abbauen

Banken und Finanzinstitute können es sich auf Dauer nicht leisten, die Modernisierung ihrer Software zu vernachlässigen. Die Lösung liegt im Einsatz modularer CIAM-Software. In den letzten Jahren ist das Angebot in diesem Bereich stark gewachsen und wird von externen Dienstleistern entwickelt. Sie bieten den Banken die notwendige Sicherheit, können aber „out of the box" eingesetzt werden, ohne dass unzählige Erweiterungen programmiert werden müssen. Das vereinfacht Release-Zyklen und eilige Upgrades, wie sie zum Beispiel zur Behebung einer Sicherheitslücke notwendig sein können. So steht einer reibungslosen Customer Journey nichts mehr im Wege. ■

Kontaktinfo:
Nevis Security AG
Birmensdorferstrasse 94
8003 Zürich

Tel.: +41(0)43.50806-81
marketing@nevis.net
www.nevis.net

Mehr dazu hier

nevis®

„Security as a Service" als wirksamer Hebel zum besseren IT-Schutz von Banken

Der Finanzsektor schaut auf ein interessantes Jahr 2023 voller Chancen und Herausforderungen. Was sich aktuell als Baustelle, aber auch als Chance mit langfristiger Wirkung erweist, sind die anstehenden Resilienzvorschriften wie DORA (Digital Operational Resilience Act), NIS-2(Netz- und Informationssicherheitssysteme)-Richtlinie, Richtlinie (EU) 2022/2555 zur Änderung betroffener Richtlinien und Richtlinie (EU) 2022/2556 bezüglich der Resilienz kritischer Einrichtungen. Sie fordern Banken dazu auf, ihre IT-Sicherheit auszubauen und sich dadurch robuster, vertrauenswürdiger und widerstandsfähiger zu gestalten.

Sicherheit nicht in Form von „noch mehr Sicherheits-Tools hinzufügen", sondern als unternehmensübergreifende Sicherheitsstrategie, welche die Führungsebene und alle Abteilungen bis hin zum einzelnen Mitarbeiter einbindet. Die Geldinstitute unterliegen – als kritische Infrastrukturen – bereits strengen Kontrollen und Vorschriften. Regelmäßige Stresstests haben dafür gesorgt, dass die Banken bereits über einen soliden Grundschutz verfügen. Der Finanzsektor gehört nach wie vor zu den Top-5-Zielen von Cyberkriminellen. Die Komplexität und die Präzision der Angriffe nehmen immens zu.

„Zweifellos werden Banken von Straftätern für eine Vielzahl von kriminellen Aktivitäten ins Visier genommen. Das liegt auch an der immer größeren Verfügbarkeit von Hacking-Instrumenten im Dark Web. Es ist einfacher denn je, fertige Module zu kaufen und selbst einen gezielten Angriff durchzuführen oder damit sogar spezialisierte, kriminelle Gruppen für maximale Ausbeute zu beauftragen. Hinzu kommt, dass nicht nur Banken, sondern auch ihre Kunden und Partner immer häufiger gehackt werden,

Bild: iStock.com/Drazen_

wie zum Beispiel beim Bankspoofing. Dadurch geraten die Banken unfreiwillig in die Position eines Beteiligten an diesem Betrug und ihre Vertrauenswürdigkeit wird beeinträchtigt", kommentiert Uwe Dingerkus, Service Owner bei der Sicherheitsfirma GBS.

Die Stärkung der Sicherheit ist ein Muss, jedoch hat sie bekanntlich ihren Preis. Wir untersuchen einige kritische Faktoren, die berücksichtigt werden müssen. Da ist zunächst die Verschärfung der staatlichen Kontrollen über Governance, Compliance und Datenschutz, die die Banken dazu verpflichten, Risiken zu überwachen, den Schutz vor Cyberbedrohungen zu intensivieren und einen umfassenden Überblick sowie eine bessere Kontrolle über alle ihre Sicherheitsmechanismen zu schaffen. Gleichzeitig gibt es (nicht nur) in Deutschland einen Mangel an qualifizierten IT-Fachkräften und einen Bedarf an technischem Know-how in verschiedenen Sicherheitsbereichen. Die hohen Bildungs- und Unterhaltungskosten zur Aufrechterhaltung eines starken Sicherheitsteams kommen erschwerend hinzu.

Eigenes Team versus SaaS

Eine der Alternativen zum Aufbau eines eigenen Sicherheitsteams ist Security SaaS (Software as a Service). Dies kann mehrere Probleme auf einmal lösen.

Unternehmen sind oft besorgt wegen der Kosten für Saas-Lösungen. „Hier geht es nicht um den Vergleich der Anfangskosten, sondern um den Langzeiteffekt sowie die Spanne der erhaltenen Leistungen", so Dingerkus. Ein 24/7-Support für die sofortige Reaktion auf einen Vorfall ist sehr kostenintensiv. SaaS substituiert den Aufbau eines eigenen und teuren IT-Teams. Ein externes Serviceteam verfügt bereits über zahlreiche Experten mit tiefgreifenden Kenntnissen in allen relevanten Sicherheitsbereichen. Dadurch erhalten die Kreditinstitute auch einen Zugang zu erweiterten Technologien, welche das Sicherheitsniveau der Banken deutlich erhöhen.

Ein weiteres Kosteneinsparungspotenzial von SaaS ist die Flexibilität, die Services zu ändern oder zu skalieren. Es wird nur die Leistung bezahlt, die tatsächlich genutzt wird. Mit den bevorstehenden Vorschriften, insbesondere DORA, die mehr Audits und Pentests voraussetzt, erweist sich die Transparenz als ein entscheidendes Kriterium für die Sicherheitsreife einer Bank. Die Überwachung der Performance einzelner Sicherheitsmaßnahmen durch zentral verwaltete Analysetools und Dashboards verschafft daher den nötigen Überblick. Der Verwaltungsaufwand und die Gefahr durch Supply-Chain-Angriffe werden durch die Bereitstellung mehrerer Sicherheitsfunktionen von einem Drittanbieter verringert.

Praxisbeispiel für eine E-Mail Security SaaS

Wie ein SaaS-Produkt in der Praxis funktionieren kann, erläutert Uwe Dingerkus am Beispiel von iQ.Suite, eine GBS-Lösung für umfassende E-Mail-Sicherheit. Die iQ.Suite bietet mehrstufigen Schutz vor jeder Art von Malware und Spam, welche von eingehenden E-Mails stammen, und verhindert dabei, mithilfe von Verschlüsselungen und Kontrollen gegen den Verlust von sensiblen Daten, den Missbrauch von Daten.

Wenn eine infizierte E-Mail bei der Bank eingeht, wird sie von der iQ.Suite in Echtzeit mit bis zu vier namhaften Scannern geprüft. Die E-Mail wird, durch Spam-Filter, nach dem Inhalt und den internen Richtlinien der Bank kategorisiert. Er erkennt sensible Informationen, wie beispielsweise eine Kreditkarten- oder Sozialversicherungsnummer. Der Spam-Filter verwendet dann die Content Disarm and Reconstruction-Technologie (CDR), um alle bösartigen Makros aus den Anhängen zu entfernen und die Datei in ein sicheres PDF-Format zu konvertieren. Das ist besonders nützlich bei der großen Anzahl von Ausweisdokumenten, die eine Bank erhält. Die iQ.Suite gibt Phising und den aktuellen Hacker-Trends, wie bösartige OneNote-Anhänge und Ransomware-E-Mails, die auf intermittierender Verschlüsselung basieren, keine Chance. Wird eine E-Mail als bösartig erkannt, wird sie in Quarantäne gestellt und der Empfänger benachrichtigt.

Wenn ein Bankangestellter eine E-Mail verschickt, unterliegt diese E-Mail ebenfalls den gleichen hohen Sicherheitsstandards. Zunächst wird die E-Mail durch das Data Loss Prevention Tool analysiert. Anomalien im Datenverkehr, die Art der angehängten Dateien, das Dateivolumen oder verdächtige Textmuster können auf unzulässige Vorgänge hinweisen. Unbefugte Mitarbeiter können so keine vertraulichen Informationen – versehentlich oder absichtlich – versenden. Wenn die E-Mail sauber und sicher ist, wird sie automatisch verschlüsselt, um zu verhindern, dass sie von außen abgefangen und manipuliert werden kann. Der Absender wird durch die iQ.Suite sehr entlastet, da alle Schritte automatisch erfolgen.

„Was die iQ.Suite so großartig macht, ist ihr vollautomatischer und selbstständiger Betrieb. Wie ich es gern nenne, ist dies eine ‚walk away security' – man drückt den Knopf und kann gehen, denn sie funktioniert von selbst. Es besteht kein Bedarf an permanenter Betreuung und Überwachung. Wenn Sie es als Dienstleistung erwerben, müssen Sie es nicht einmal einrichten, da die gesamte Einstellung, Überwachung, Wartung und die Updates von unserem Team übernommen werden. Gleichzeitig haben Sie alle Auswertungen und Statistiken über die Leistung in der Hand, die Sie in Ihre Sicherheitsberichte integrieren und den Aufsichtsbehörden vorlegen können. Außerdem erkennen Sie die Leistungstrends und Sicherheitsschwachstellen, beispielsweise sobald eine bestimmte Abteilung plötzlich mehr kompromittierte E-Mails erhält oder bestimmte Benutzer eine erhöhte Anzahl von E-Mails mit sensiblen Informationen empfangen", fasst Dingerkus zusammen. ■

Kontaktinformationen:
GBS Europa GmbH
Zur Giesserei 19-27B
76227 Karlsruhe
Deutschland
Tel.: +49 721 4901-0
E-Mail: info@gbs.com
Internet: **https://www.gbs.com**

Mehr dazu hier

GBS

Sicher aufbewahrt, schnell gefunden:

Professionelle E-Mail-Archivierung für Banken

Banken sind wie andere Unternehmen auch dazu verpflichtet, relevante Dokumente sicher und zugänglich aufzubewahren. Darunter fällt auch die elektronische Kommunikation via E-Mail. Roland Latzel, Senior Director Marketing bei MailStore, zeigt, was es zu beachten gilt und welche Rolle dabei professionelle E-Mail-Archivierung spielt.

Autor: Roland Latzel,
Senior Director Marketing bei MailStore

Der überwiegende Teil der Unternehmen in Deutschland muss Bücher, Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, Eröffnungsbilanzen und Buchungsbelege mindestens zehn Jahre sicher aufbewahren und die Verfügbarkeit dieser Unterlagen gewährleisten. Handels- und Geschäftsbriefe müssen sechs Jahre aufbewahrt werden. Gemäß GoBD (GoBD = Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff) müssen steuer- und handelsrechtlich relevante Daten lückenlos archiviert werden. In Österreich und der Schweiz gelten ähnliche Anforderungen.

Neben diesen allgemeinen Vorgaben gelten für den streng regulierten Finanzsektor noch weitere Vorgaben. Die zweite Fassung der EU-Direktive zum Wertpapierhandel „Markets in Financial Instruments Directive" (MiFID II) aus dem Jahr 2018 sieht beispielsweise eine Dokumentationspflicht für getätigte Geschäfte, erbrachte Services und Leistungen vor. Diese Aufzeichnungen müssen sowohl der eigenen Rechtsabteilung als auch den Aufsichtsbehörden zugänglich sein.

Andererseits fallen die personenbezogenen Daten von Bankkunden unter die Datenschutzgrundverordnung (DSGVO), beziehungsweise das Schweizer Datenschutzgesetz (DSG) und müssen dementsprechend behandelt werden. Das bedeutet, Unternehmen müssen Zweckbindung, Datenminimierung, Speicherbegrenzung sowie Integrität und Vertraulichkeit gewährleisten.

Vor diesen Hintergründen kommt der Archivierung von E-Mails als wichtigstem elektronischen Kommunikationsmittel eine entscheidende Bedeutung zu. Zu bedenken ist auch, dass einerseits das Datenwachstum ungebrochen anhält und sich andererseits Arbeitsmodelle in den letzten Jahren verändert haben. Gerade Remote Work hat die „Cloudifizierung" von Unternehmen enorm beschleunigt. Viele Tools werden mittlerweile als Service aus der Cloud (SaaS) bezogen. Für Anwender und Fachabteilungen, die sich unkompliziert passende Werkzeuge aussuchen können, mag das praktisch sein. Für IT-Manager bedeutet es allerdings, dass sie stark fragmentierte Informationslandschaften verwalten müssen. Daten können sich auf mehrere Server und verschiedene Clouds verteilen. Diese

Rahmenbedingungen verlangen ein ausgeklügeltes Informationsmanagement einschließlich einer ordentlichen E-Mail-Archivierung.

Cloud oder On-Premises?

Unternehmen, die eine E-Mail-Archivierungslösung für ihr E-Mail-Management implementieren möchten, müssen sich zunächst entscheiden, ob sie die Bereitstellung mittels eigener Server umsetzen oder einen Cloud-Service von einem Managed-Services-Provider oder einem der großen Public-Cloud-Anbieter beziehen wollen. Die Kombination von SaaS-Angeboten und Inhouse-Infrastruktur im eigenen Rechenzentrum ist ebenfalls möglich. Cloudbasierte Lösungen haben unter anderem den Vorteil, dass der physische Speicherort der Daten vom eigenen Rechenzentrum entkoppelt ist. Sollte es dort zu Zwischenfällen kommen, sind die in der Cloud archivierten Daten nicht betroffen. Ist die Cloud-Lösung dann auch noch redundant ausgelegt, hat man ein sehr sichereres, hochverfügbares System. Aber auch Cloud-Anbieter sind nicht vor Systemausfällen geschützt – als Beispiele wären hier der Brand im Straßburger Rechenzentrum von OVHCloud im Jahr 2021 und der weltweite Ausfall der Hosted-Exchange-Umgebungen des Hosting-Providers Rackspace im Jahr 2022 genannt, Letzteres bedingt durch eine Ransomware-Attacke.

Vor dem Hintergrund der DSGVO ist allerdings zu beachten, wo sich die Rechenzentren befinden. Gemäß Artikel 44 ff. EU-DSGVO dürfen personenbezogene Daten nur dann in ein Drittland übertragen werden, wenn das Datenschutzniveau den Anforderungen der EU entspricht. Dazu kommen noch weitere Regularien der europäischen Bankenaufsicht EBA. Bei einem Vertragsabschluss mit einem SaaS-Anbieter bietet es sich an, einen zusätzlichen Auftragsverarbeitungsvertrag (AVV) abzuschließen, um den Anforderungen des Artikels 28 EU-DSGVO nachzukommen. Dieser ist notwendig, wenn personenbezogene Daten zur Verarbeitung an Dritte weitergegeben werden.

Mehr als nur Backup

Neben gesetzlichen Vorgaben spricht auch aus der Sicht der Business Continuity vieles für eine professionelle Archivierungslösung. Unternehmen im Finanzsektor müssen Systemausfälle aufgrund von Problemen mit der hauseigenen Hardware, Ausfälle aufseiten von IT-Service-Providern, Anwenderfehler, Manipulation durch das absichtliche Löschen von Daten sowie die immer häufiger vorkommenden Cyberangriffe berücksichtigen und sich dagegen wappnen.

Regelmäßige Backups sind wichtig – doch sie allein reichen nicht aus, um sich umfassend vor Datenverlust zu schützen. Das liegt daran, dass Backups immer zyklisch erfolgen und zu einem bestimmten Zeitpunkt eine Momentaufnahme des Systems abbilden. Neue Daten, die nach dem Backup hinzugekommen sind, werden demzufolge erst im nächsten Zyklus gesichert. So kann es bei einem Systemausfall zu Lücken im Datenbestand kommen. Um die lückenlose Wiederherstellung des historischen E-Mail-Bestandes zu gewährleisten, benötigen Unternehmen zusätzlich noch eine E-Mail-Archivierung, die alle relevanten E-Mails direkt, das heißt, noch vor der Zustellung in die Postfächer, in ein eigens dafür vorgesehenes Archiv kopiert und eine vollständige, revisionssichere und langfristige Aufbewahrung der Daten sicherstellt. Nur so können sie rechtssicher arbeiten und alle Dokumentationspflichten erfüllen. Dabei ist aber nicht zu vergessen: Auch das Archiv sollte Teil des Backup-Plans sein.

MailStore Server: was eine E-Mail-Archivierungslösung bieten muss

Nachdem IT-Entscheider die Rahmenbedingung für die E-Mail-Archivierung gemeinsam mit allen relevanten Stakeholdern wie CISOs/CIOs, Datenschutzbeauftragten oder dem Betriebsrat abgesprochen haben, gilt es, die für ihre Ansprüche beste E-Mail-Archivierungslösung zu finden. MailStore Server verfügt bereits über ein umfangreiches Funktionsrepertoire, mit dem Banken und Finanzdienstleister die Archivierung sensibler Kommunikation rechtssicher realisieren können:

- **Revisionssicher, langfristig, individuell:** Mit MailStore Server können IT-Mitarbeiter individuelle Archivierungs- und Löschregeln definieren, die den gesetzlichen Vorgaben zur revisionssicheren und langfristigen Aufbewahrung von E-Mail-Daten entsprechen.

- **Zugänglich und effizient:** Banken und Finanzdienstleister müssen den permanenten Zugriff auf archivierte Daten ermöglichen. Dafür verfügt MailStore Server über eine leistungsstarke Volltextsuche sowie weitere Funktionen, mit denen sich Daten einfach wiederherstellen und exportieren lassen. Dies spielt vor allem in Compliance-, Audit- und Rechtsangelegenheiten eine große Rolle. Aber auch sobald ein Kunde seine Auskunftsrechte gemäß DSGVO geltend machen möchte, unterstützt die Suchfunktion bei der schnellen Umsetzung. Zudem können Anwender über die Self-Service-Funktion selbstständig auf ihr persönliches Archiv zugreifen und Daten wiederherstellen, ohne die IT-Abteilung involvieren zu müssen. Somit wird auch die Produktivität der Anwender gesteigert.

- **Sicher und zertifiziert:** MailStore Server nutzt moderne Hash- und Verschlüsselungsverfahren, um den archivierten Datenbestand vor Manipulation und Verlust zu schützen. Manuelle Änderungen, die ein Mitarbeiter am Archiv vornimmt, werden via Audit Log dokumentiert und lassen sich dadurch nachverfolgen. MailStore Server ist zudem unabhängig nach **DSGVO und IDW PS 880** zertifiziert und verspricht somit ein hohes Sicherheitsniveau.

Kontakt:
MailStore Software GmbH
Clörather Straße 1–3 • 41748 Viersen (Deutschland)
Tel.: +49-(0)2162-50299-0 • Fax: +49 (0)2162-50299-29
E-Mail: sales@mailstore.com
www.mailstore.com/de

Mehr dazu hier

MAILSTORE® by opentext™

© Gorodenkoff - stock.adobe.com

Verantwortliche IT-Sicherheit direkt erreichen

- Newsletter
- Content-Marketing
- Webinare & Webkonferenzen

Schreiben Sie uns: **wolfgang.scharf@datakontext.com**

www.itsicherheit-online.com