E-Mail-Sicherheit im Finanzwesen

Geld, Investitionen & PII sind ein Traumziel für Hacker

Abschnitt

eins.

Finanzdienstleister — Unternehmen, Wertpapierfirmen und Fintechs — sind ein gefundenes Fressen für Cyberkriminelle.

Schnelle digitale Transformation führt zu größerer Cyber-Schwachstelle

Geld, Investitionen und jede Menge sensibler personenbezogener Daten bieten ein großes Potenzial für Bedrohungsakteure. Weltweit haben Finanzdienstleister in letzter Zeit einen starken Anstieg der digitalen Transaktionen, des mobilen Bankings und des gesamten E-Mail-Volumens zu verzeichnen, was sie dazu veranlasst hat, ihre bestehenden Kernsysteme durch skalierbare Cloud-basierte Systeme zu ergänzen - insbesondere für E-Mail. Infolgedessen hat sich das Potenzial für Verstöße gegen die Cybersicherheit erhöht. Jede neue E-Mail könnte ein Phishing- oder Malware-Maulwurf oder ein Tunnel für Ransomware sein.

Neben dem Wachstum der digitalen Kommunikation und Transaktionen erweitern zwei weitere Faktoren die Cybersicherheitslandschaft für Finanzdienstleistungen: neue Datenschutzbestimmungen und die COVID-19 Pandemie.

Neue Vorschriften, beginnend mit der Allgemeinen Datenschutzverordnung (DSGVO) der Europäischen Union, das neu eingeführte südafrikanische Gesetz zur Cyberkriminalität und einige Gesetze der US-Bundesstaaten, bieten allesamt Standards für den Schutz personenbezogener Daten, die das Vertrauen und die Sicherheit bei digitalen Transaktionen verbessern sollen.

Und für die britischen Finanzdienstleister ist die Financial Conduct Authority (FCA) die wichtigste Regulierungsbehörde für Cyberrisiken. Das Handbuch der FCA legt weitreichende Anforderungen für Unternehmen fest, um das Risiko von Sicherheitslücken zu bewältigen, ihre Kunden zu schützen und mit den Regulierungsbehörden zusammenzuarbeiten.

Cyberangriffe können zu irreparablen Reputationsschäden für Finanzinstitute führen, für die das Kundenvertrauen elementar ist. Die sozialen Distanzierungsverfahren während COVID-19 führten zu einem beunruhigenden und eifrigen Wechsel von Arbeitskräften und eröffneten eine Fülle von Nischen für Cyberkriminelle.

Cybersicherheitsherausforderungen sind nicht neu für Finanzinstitute, aber Schweregrad, Volumen und Raffinesse von Angriffen haben sich verändert. Cyberangriffe können ein Unternehmen vom Netz nehmen, Kunden in Panik versetzen oder den Betrieb vorübergehend einstellen, was alles zu finanziellen Verlusten führt. Nach einer Schätzung des Ponemon Institut belaufen sich die durchschnittlichen Kosten einer Datenschutzverletzung in einem US-Finanzinstitut auf 5,9 Mio.$, das sind 52% mehr als der Durchschnitt in anderen Sektoren.[1]

$5.9 Millionen

betragen die durchschnittlichen Kosten einer Datenschutzverletzung für US-Finanzinstitute – 52% höher als in anderen Branchen.

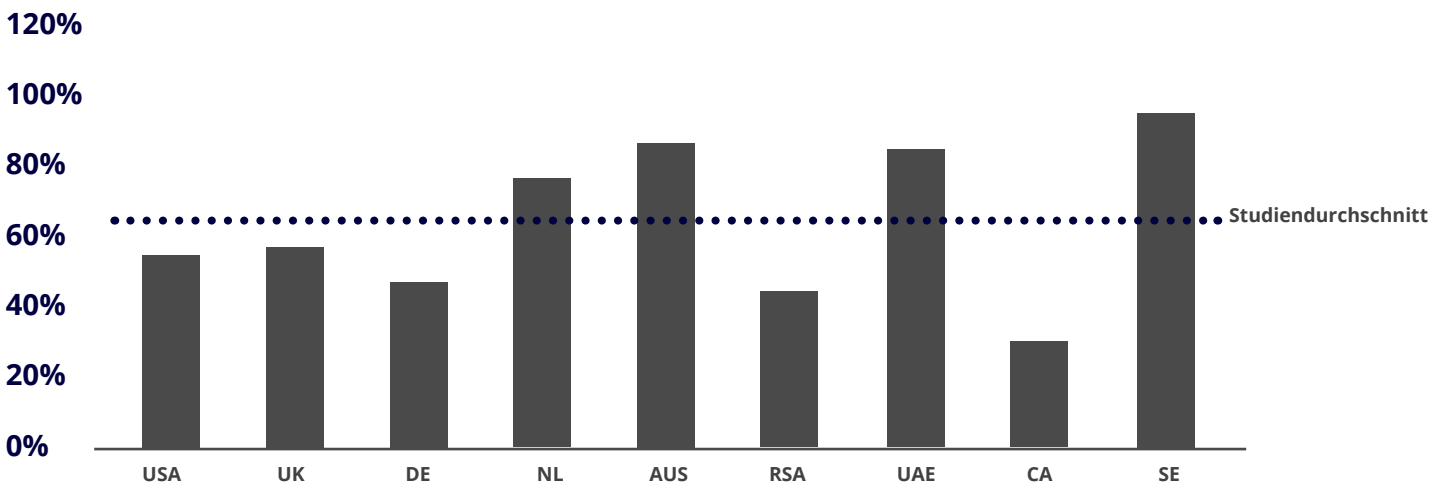
Um einen Einblick in die Cybersecurity-Herausforderungen von Finanzinstituten zu erhalten, haben wir 153 Finanzdienstleister im Rahmen des Mimecast-Berichts State of Email Security 2021 (SOES) befragt, einer weltweiten Umfrage unter 1.225 Fachleuten aus den Bereichen Informationstechnologie und Cybersecurity. Zu den wichtigsten Ergebnissen gehört, dass 62% der befragten Finanzdienstleister glauben, dass es wahrscheinlich, sehr wahrscheinlich oder unvermeidlich ist, dass ihr Unternehmen im Jahr 2021 negative geschäftliche Auswirkungen durch einen E-Mail-Angriff erfahren wird, obwohl sie den Ruf haben, zu den am besten geschützten Branchen zu gehören.

Die Besorgnis über die Folgen eines E-Mail-Angriffs war bei den 25% der Befragten am größten, die in der Firma sitzen und auf C-Level (CIO, CTO oder CISO) agieren. Und wie das nebenstehende Balkendiagramm aller befragten Finanzdienstleister zeigt, war sie auch global.

62%

der befragten Finanzdienstleister halten es für wahrscheinlich, sehr wahrscheinlich oder unvermeidlich, dass ihr Unternehmen im Jahr 2021 negative Auswirkungen auf das Geschäft durch einen E-Mail-Angriff haben wird.

Wahrscheinliche und unvermeidliche, negative Auswirkungen auf das Geschäft durch einen E-Mail-Angriff nach Land



Abschnitt

zwei.

Finanzdienstleistungs-unternehmen sind unter Beschuss

Die Finanzdienstleistungsbranche, zu der Banken, Versicherungen, Investmentfirmen und Fintech-Unternehmen gehören, ist ein ständiges Ziel von E-Mail-Angriffen. Dies liegt an der Art des Umgangs mit Geld, dem großen Kundenstamm und den wertvollen persönlichen Daten der einzelnen Kunden, wie Sozialversicherungsnummern oder nationale Identifikationsnummern, Bankdaten, Kontakt- und Einkommensdaten. Bei Finanzdienstleistungen steht mehr auf dem Spiel und der potenzielle Wert eines Diebstahls ist größer. Laut der Studie des Ponemon Institut gehörten die Kosten von Datenschutzverletzungen in der Finanzdienstleistungsbranche - einschließlich der Kosten für die Behebung, Wiederherstellung und entgangene Geschäfte - in den letzten sechs Jahren jeweils zu den höchsten.[2]

In der Zwischenzeit haben mehrere Trends das Wachstum von digitalen Transaktionen und E-Mails angekurbelt und die Zahl der potenziellen Angriffe ebenso

- Finanzunternehmen haben Online- und mobile Kanäle , die von ihren Kunden sehr gut angenommen werden.
- COVID-19 hat mehr Kunden dazu gebracht, auf kontaktlose und bargeldlose Weise Geschäfte zu tätigen und noch mehr digitales Volumen zu einem bereits wertvollen Ziel hinzugefügt.
- Die Anzahl sensibler E-Mails zwischen Institutionen und Kunden sowie zwischen Mitarbeitern innerhalb von Institutionen hat zugenommen.

Darüber hinaus ist die Finanzdienstleistungsbranche durch die Verlagerung auf Online- und Mobilkanäle mit technologischen Herausforderungen konfrontiert. Viele Institutionen mussten ihre neuen digitalen Fähigkeiten auf bestehenden Systemen aufbauen, die bereits seit Jahrzehnten im Einsatz sind. Die daraus resultierenden hybriden Systeme schaffen eine größere Angriffsfläche, was das Schadenspotenzial erhöht.

E-Mail ist der Angriffsvektor Nummer eins

Unternehmen kommunizieren mit ihren Kunden, Lieferanten und Mitarbeitern auf viele Arten, aber E-Mail ist die wichtigste davon. Dies gilt umso mehr im Jahr 2021, da sich die Belegschaften auf immer neue Formen der Heimarbeit und hybride Arbeitsformen verstreuen. Über 25% der befragten Finanzunternehmen haben weltweit E-Mail-Anwender – mehr als jede andere Branche im SOES-Bericht. Laut der Studie ist das E-Mail-Volumen der globalen Finanzunternehmen im vergangenen Jahr um 81% gestiegen. Mit der Zunahme des E-Mail-Volumens und -Gebrauchs steigt auch die Zahl der E-Mail-basierten Bedrohungen durch Cyber-Kriminelle. Cyberangriffe steigen in allen Branchen und Finanzdienstleistungen sind nicht immun. Tatsächlich erwarten 57% der Befragten aus dem Finanzsektor, dass das Volumen der Angriffe eine der größten Herausforderungen für die E-Mail-Sicherheit im Jahr 2021 sein wird. Bedenken hinsichtlich des Angriffsvolumens waren in Südafrika und den Vereinigten Arabischen Emiraten am höchsten.

Die Raffinesse von E-Mail-Angriffen nimmt ebenfalls zu, was 64% der Befragten aus dem Finanzsektor dazu veranlasst, das Problem als ein komplexer werdendes zu sehen.

In Regionen, in denen weniger Befragte erwarteten, dass das gesamte E-Mail-Volumen steigt, wie Deutschland und Großbritannien, glaubten aber mehr Befragte, dass die größere Raffinesse der Angriffe auch ihr größeres Problem sei. Die Raffinesse der Angriffe war jedoch selbst in den beiden Regionen, in denen das E-Mail-Volumen voraussichtlich am stärksten zunehmen wird - den Niederlanden und Schweden - mindestens genauso besorgniserregend wie die Anzahl der Angriffe.

Das steigende Volumen der Angriffe und die zunehmende Raffinesse sind mit Sicherheit ein doppelter Schlag. Drei von fünf Befragten aus dem Finanzdienstleistungssektor (62%) glauben, dass ihr Unternehmen im Jahr 2021 unter den negativen Auswirkungen eines Angriffs per E-Mail leiden könnte. Diese Befürchtung wird durch Daten des Internationalen Währungsfonds untermauert, die zeigen, dass sich die Zahl der Cyberangriffe in den letzten 10 Jahren verdreifacht hat und dass die Finanzdienstleistungsbranche am stärksten davon betroffen ist.[3]

81% **der Finanzdienstleister verzeichneten ein wachsendes E-Mail-Volumen.**

Ransomware und E-Mail-Sicherheit

E-Mails sind eine verbreitete Art und Weise, wie Ransomware in ein Netzwerk eindringt, das sich um die Daten-Hostage dreht. Und da ein Netzwerk nur so sicher ist wie sein schwächstes Glied – und das ist in der Regel der Mensch – kann die Wahrscheinlichkeit eines naiven Klicks auf den falschen E-Mail-Link hoch sein.

Es ist zu einem relativ häufigen Vorfall geworden, dass das Opfer eines Angriffs eine Kettenreaktion für seine Geschäftspartner auslösen kann. Dies führt zu Folgendem:

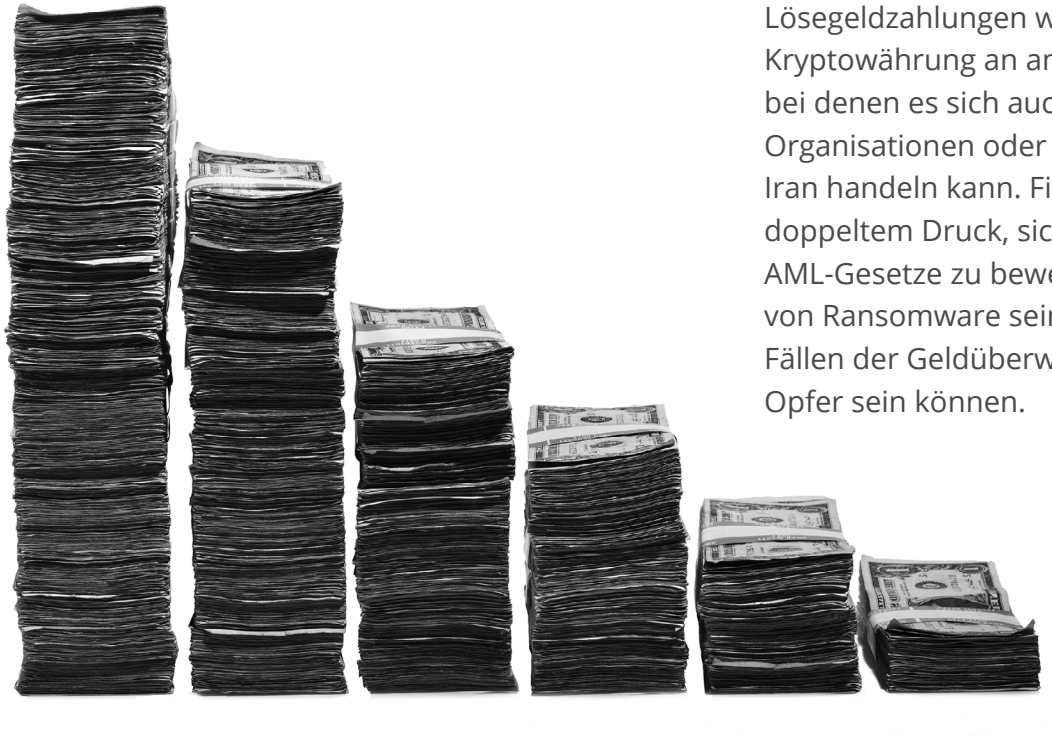
- **erhöhte Kosten für die Gewinnung neuer Kunden**
- **Reputationsverluste und reduzierten Goodwill**
- **Umsatzverluste durch Systemausfallzeiten**
- **Störungen im Geschäftsbetrieb**
- **verlorene Kunden**

Die Kosten eines solchen Angriffs sind überwältigend, und die Ausfallzeit ist von entscheidender Bedeutung. Zum Beispiel gaben 30% der Befragten an, dass ihre Finanzunternehmen in den letzten Monaten zwischen 4 und 12 Wochen Betriebsausfallzeiten durch einen Ransomware-Angriff erlebt haben. Unternehmen jeder Größe stehen vor der Entscheidung, ob sie das Lösegeld zahlen sollen oder nicht. Experten bemerken, die zunehmende Inzidenz und die Raffinesse von Ransomware-Angriffen habe sich während der COVID-19-Pandemie noch beschleunigt, was wahrscheinlich auf weniger sichere Arbeitsumgebungen von zu Hause aus und die verstärkte Nutzung von Geräten für soziale Kontakte, zurückzuführen ist. [4]

53%

der befragten Finanzdienstleister halten es für wahrscheinlich, sehr wahrscheinlich oder unvermeidlich, dass ihr Unternehmen im Jahr 2021 negative Auswirkungen auf das Geschäft durch einen E-Mail-Angriff haben wird.

Ransomware-Angriffe sind in der Finanzdienstleistungsbranche allgegenwärtig. Mehr als die Hälfte (53%) der befragten Unternehmen gab an, dass ein Ransomware-Angriff ihr Geschäft in den letzten 12 Monaten etwas oder erheblich beeinträchtigt hat. Die Vereinigten Arabischen Emirate, Schweden und Australien liegen mit 60-88% an der Spitze, was den globalen Charakter der Ransomware-Problematik verdeutlicht.



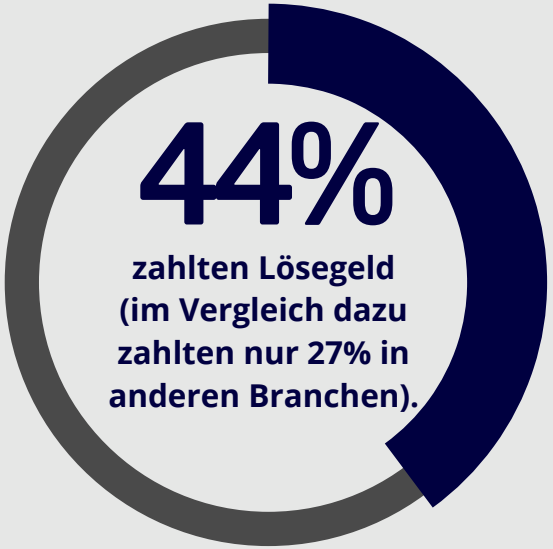
Interessanterweise rangieren zwei dieser Länder auch am höchsten in Bezug auf die Zahlung von Lösegeld. Eine taktische Strafverfolgungsbehörde (z. B. Europol, die niederländische Nationalpolizei und das FBI) beraten sie.[5] Denn schwierig ist, dass die Zahlung von Lösegeld bestimmte Vorschriften zur Bekämpfung von Geldwäsche/Kundenkenntnis (AML/KYC) auslösen kann, die sicherstellen sollen, dass die Kontoinhaber identifiziert werden können und die Geldströme eindeutig sind. Diese Regeln sind so eingerichtet, dass sie die Finanzierung fehlerhafter Akteure jeder Art reduzieren. Lösegeldzahlungen werden in der Regel in Kryptowährung an anonyme Empfänger gefordert, bei denen es sich auch um sanktionierte Personen, Organisationen oder Gebiete wie Nordkorea oder Iran handeln kann. Finanzinstitute stehen unter doppeltem Druck, sich auf der richtigen Seite der AML-Gesetze zu bewegen, da sie sowohl Opfer von Ransomware sein können als auch in anderen Fällen der Geldüberweisungsagent für ein anderes Opfer sein können.

Bezahlen oder nicht bezahlen: Transaktion ist eine Herausforderung.

Finanzdienstleister zahlen möglicherweise häufiger Lösegeld als andere Branchen:

Finanzunternehmen im SOES-Bericht die in den letzten 12 Monaten von einem Ransomware-Angriff betroffen waren, zahlten 44%. Im Vergleich dazu haben in einer anderen globalen Studie 27% der Unternehmen aus anderen Branchen gezahlt.[6] Finanzdienstleister sind möglicherweise eher bereit, sich von Ransomware erpressen zu lassen um die Aufmerksamkeit der Öffentlichkeit und den damit verbundenen potenziellen Rufschaden für ihr Unternehmen zu vermeiden.

Eine Studie zeigt, dass Drohungen mit der Veröffentlichung gestohlener Daten, die manchmal als "doppelte Erpressung" bezeichnet werden, eine Vorgehensweise bei 77% der Ransomware-Angriffe ist.[7] Finanzdienstleister auf der ganzen Welt sollten jedoch die lokalen Gesetze sorgfältig beachten: Das südafrikanische Gesetz gegen



Cyberkriminalität ist zwar noch nicht in Kraft getreten, sieht aber eine Meldepflicht vor, die zu hohen Geldstrafen führen kann.

Es gibt eine interessante Lücke zwischen dem, was die befragte Gruppe geschätzt hat und was in den letzten 12 Monaten tatsächlich bei Ransomware-Angriffen geschehen ist: 61% glauben, dass sie ihre Daten wiederherstellen können, ohne das Lösegeld zu bezahlen, aber nur 47% haben dies bei früheren Angriffen geschafft.

Da zu erwarten ist, dass sowohl die Ransomware-Aktivitäten als auch die Lösegeldbeträge weiter zunehmen werden, gehört der Schutz der Daten durch strenge Backup- und Aufbewahrungsrichtlinien zu den besten Lösungen, um den dauerhaften Verlust von Daten für Finanzunternehmen zu verhindern.

61%

glauben, dass sie ihre Daten wiederherstellen können, ohne das Lösegeld zu bezahlen.

47%

haben dies bei früheren Angriffen geschafft.

Phishing & Marken-Spoofing

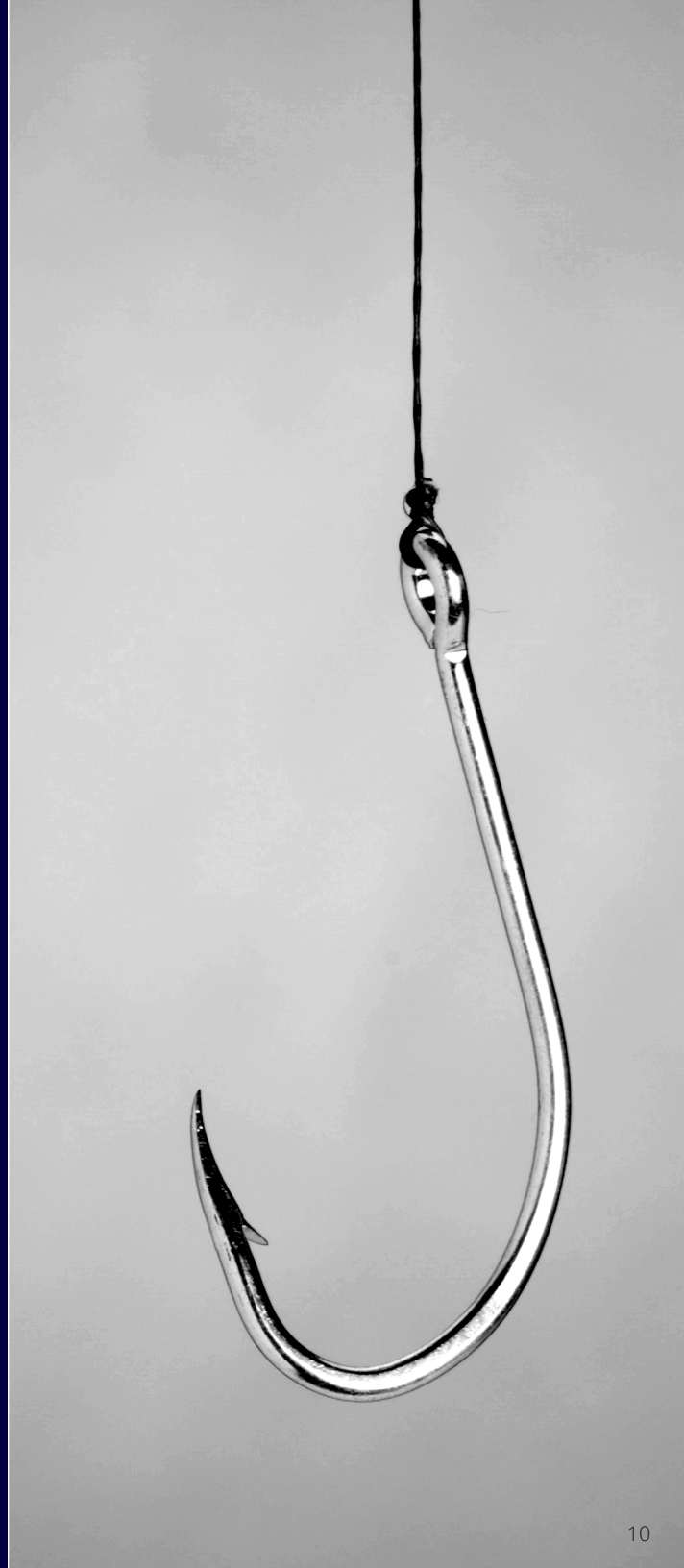
Die Zunahme des E-Mail-Volumens hat dazu geführt, dass Unternehmen ihre lokalen Lösungen aufgeben und ihre E-Mail-Sicherheit auf Cloud-Dienste verlagern. [8] Genau auf diese Schnittstelle, an der sich E-Mail- und Cloud-Konten überschneiden, zielen moderne Angriffe ab.

Im Bereich der Finanzdienstleistungen stellten 60% der SOES-Befragten im vergangenen Jahr eine Zunahme von Phishing mit bösartigen Links oder Anhängen fest (darunter 24%, die von einer “starken” Zunahme sprachen), und 42% verzeichneten eine Zunahme des Missbrauchs ihrer Marken sowohl über E-Mails als auch über gefälschte, geklonte Webdomänen. Was den Missbrauch der Marke angeht, umfassten diese 42% der Befragten

18% der Befragten sahen einen starken Anstieg des Missbrauchs ihrer Marke durch geklonte Websites und 11% sahen Einen tieferen Einblick in dieses Thema über alle Branchen hinweg bietet der The State of Brand Protection 2021 Report.

In Übereinstimmung mit den Antworten der SOES 2021 waren Finanzdienstleistungen die Branche, die im vierten Quartal 2020 am häufigsten Ziel von Phishing-Angriffen war. [9] Wie bei allen Phishing-Angriffen werfen die Täter ein weites Netz aus, in der Hoffnung, ein paar ahnungslose Opfer zu erwischen. Auf diese Weise stehlen sie Passwörter, Kontoanmeldungen und persönliche Daten - alles wichtige Informationen, insbesondere für Bankkonten, Anlagekonten oder Versicherungspolicen.

60% **der Finanzdienstleistungsunternehmen verzeichneten eine Zunahme von bösartigem Phishing.**



In einer bereits stark regulierten Branche bewerten verschiedene Unternehmen die Verbraucherschutzvorschriften neu, von denen derzeit kaum welche die Finanzdienstleister belangen, wenn ihre Kunden, Opfer von Phishing, Smishing oder Vishing (per E-Mail, SMS oder Telefon) werden. Allerdings haben die vier größten britischen Banken einen freiwilligen Verhaltenskodex unterzeichnet, den Code Contingent Reimbursement Model (CRM), der genau das tut. Was wiederum die Kosten für Unternehmen, die Opfer von Betrugsversuche werden, erhöht.

Bei Betrug mit gefälschten oder geklonten Webdomänen wird eine Kopie der Website des Finanzinstituts so erstellt, dass sie wie das Original aussieht und mit bösartigen Links versehen ist. Die Links zielen darauf ab, die Benutzer zur Eingabe vertraulicher Informationen über ein täuschend echt aussehendes Anmeldeportal zu verleiten oder Malware auf ihr Gerät herunterzuladen. Dies ist ein echtes Problem in Finanzdienstleistungsunternehmen, sowohl für Marketingfachleute, die eine vertrauenswürdige Marke aufbauen und fördern, als auch für Sicherheitsteams, die mit Kundenauthentifizierung beauftragt sind. Eine regionale Bank CISO erklärte, dass sie jeden Monat 10 oder 11 solcher Angriffe über die Website, mobile Apps oder Social-Media-Konten erlebt. Wenn diese nicht kontrolliert werden, “verschmutzen sie Ihre Marke”, sagte der Sprecher und fügte hinzu, dass IT-Sicherheit und Marketing zusammenarbeiten sollten, um ihre Marke zu schützen. Eine Möglichkeit hierfür besteht darin, Domainnamen-Registrierungen zu überwachen.

Schädliche Links zielen darauf ab, Benutzeraccounts durch das Eingeben vertraulicher Informationen zu duplizieren.

Ein echt aussehendes Anmeldeportal zu öffnen oder Malware auf ihr Gerät herunterzuladen.

10 oder 11

solcher Angriffe jeden Monat über Websites, betrügerische mobile Anwendungen oder Konten in sozialen Medien.

Abschnitt

drei.

Können Finanzdienstleister mehr cyber-resilient sein?

Als Branche haben viele Finanzunternehmen bereits aktive Cyber-Resilience-Pläne, daher besteht die Herausforderung darin, sie kontinuierlich weiterzuentwickeln, um mit der fortschrittlichen Raffinesse von Angriffen Schritt zu halten. Darüber hinaus müssen sie den sich ändernden Vorschriften immer einen Schritt voraus sein. Ihre Cyber-Resilience-Pläne erfordern wahrscheinlich die Schichtung von Cloud-E-Mails, die Neubewertung der verteilten Belegschaftstechnologie und die Verbesserung ihrer Sicherheitskultur.

Schichtweise Cloud-E-Mail

Banken, Versicherungen und Wertpapierfirmen haben Cloud-basierte E-Mail-Systeme eingeführt - vor allem Microsoft 365 - um den enormen Anstieg des E-Mail-Volumens zu bewältigen.

Neben den Vorteilen, die cloudbasierte E-Mail-Lösungen mit sich bringen, wie z. B. Kosteneffizienz, kurze Implementierungszeit, erweiterter Zugriff und Skalierbarkeit, gibt es jedoch auch ein Sicherheitsproblem: die "Single-Lock"-Monokultur. Wenn Microsoft 365 die einzige Form der E-Mail-Sicherheit für eine Institution darstellt, ist ein bösartiger Akteur in der Lage, diese zu überwinden.

Drei Faktoren verschärfen diese Herausforderung der Sicherheitsmonokultur:

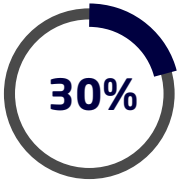
Die Dominanz von Microsoft macht es zum Hauptziel, auf das sich Cyberangreifer konzentrieren

Cyberangreifer selbst nutzen oft Microsoft-Dienste, von denen aus sie Angriffe starten, um sie legitim erscheinen zu lassen

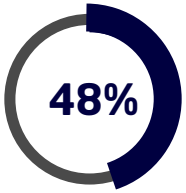
Weniger als 25% der befragten SOES-Finanzdienstleister glauben, dass Microsoft 365 erstklassige E-Mail-Sicherheit bietet

Infolgedessen entscheiden sich viele Finanzdienstleister dafür eine zusätzliche Sicherheitssoftware zu installieren.

Tatsächlich haben 30 % bereits eine zweite Ebene eingerichtet und weitere 48 % planen die Einrichtung einer solchen. Auf diese Weise können die Finanzinstitute die Sicherheitserwartungen ihrer Kunden und die Anforderungen der Aufsichtsbehörden besser erfüllen.



haben bereits eine zweite Schicht installiert



haben Pläne, eine zweite Schicht zu installieren

Zurück zu den Grundlagen: Schulung für eine gute Sicherheitshygiene

Eine der Möglichkeiten, wie Finanzdienstleister die wachsende Bedrohung durch Cyberangriffe per E-Mail bekämpfen können, ist der Aufbau einer starken Sicherheitskultur unter den Mitarbeitern. Die Überprüfung der Technologie und die Schulung des Personals in Sachen Sicherheit sind zwei Möglichkeiten, dieses Ziel zu erreichen.

Das Tempo der pandemischen Verbreitung führte dazu, dass sich Unternehmen schnell in verteilte Arbeitsumgebungen verlagern mussten, oft erforderliche innovative Taktiken, die die Hygiene der Cybersicherheit außer Betrieb nehmen.

Zum Beispiel kauften einige IT-Abteilungen Laptops im Einzelhandel für Mitarbeiter ohne die Konfigurations- und Sicherheitsstandards abzuschliessen, um die Verfügbarkeit schnell sicherzustellen.

Und dann werden diese Sub-Standard-Laptops über anfällige Remote-Zugriffsverbindungen in Netzwerke geschleppt. All dies erhöhte die Anfälligkeit für Angriffe. In Zukunft müssen die Sicherheitsteams diese “vorübergehenden” Lösungen überprüfen und die fortbestehenden auf den neuesten Stand bringen.

Vor diesem Hintergrund ist es verständlich, dass 72% der befragten Finanzdienstleister der Meinung sind, dass ein erhöhtes Risiko besteht, dass Mitarbeiter mit ihren persönlichen E-Mails einen schwerwiegenden Sicherheitsfehler begehen können. Schlechte Passworthygiene ist bei 71% der Befragten im Finanzwesen ebenfalls ein Problem.

72% glauben, dass ein erhöhtes Risiko besteht, dass Mitarbeiter bei ihren persönlichen E-Mails einen schwerwiegenden Sicherheitsfehler begehen können. Schlechte Passworthygiene ist bei 71% der Befragten im Finanzwesen ebenfalls ein Problem.

Der andere Teil der Bemühungen umfasst die Schulung der Mitarbeiter, um ihr Bewusstsein für Fragen der Cybersicherheit zu schärfen. Diese Schulungsprogramme, die darauf abzielen, das Sicherheitsbewusstsein und das Änderungsverhalten zu erhöhen, sind eine hochpriorisierte Taktik zwischen zwei Dritteln der IT. Interessanterweise heben sich Finanzdienstleistungsunternehmen in dieser Hinsicht nicht von der Konkurrenz ab, obwohl sie ein äußerst zielgerichteter Sektor sind.

Nur 44% der Finanzunternehmen bieten Schulungen für Sicherheitsbewusstsein auf monatlicher oder häufigerer Basis im Vergleich zu 46% der Unternehmen in allen anderen Branchen, an. Die größte Konzentration von Finanzunternehmen – 37% – bietet nur vierteljährliche Schulungen an.

Was die Methoden der Sicherheitsschulung anbelangt, so sind die Ergebnisse in der Finanzdienstleistungsbranche gemischt, wobei drei Methoden den Durchschnitt aller Branchen anführen und drei zurückbleiben (siehe Abbildung). Die Branche ist besser als die meisten anderen, wenn es um automatisierte Taktiken wie Online-Tests, interaktive Videos und Eingabeaufforderungen geht.

Sie liegt jedoch hinter der Kurve, wenn es um Gruppen- und Eins-zu-Eins-Schulungen und gedruckte Referenzmaterialien geht.

37% **der Finanzdienstleistungsunternehmen bieten ihren Mitarbeitern nur vierteljährlich Schulungen an**

	Gesamt		Finanzdienstleister	
Gesamt	**1225**	**100%**	**153**	**100%**
Gruppenschulungen mit unserem IT- oder IT-Sicherheitsteam	700	57%	77	50%
Ein formaler Online-Test, um sich über Bedrohungen zu informieren und Fragen zu stellen, die zu beantworten sind	574	47%	79	52%
Eine gemailte oder gedruckte Liste mit Tipps, die Sie beachten sollten	525	43%	64	42%
Interaktive Videos, die die besten und schlechtesten Praktiken hervorheben, die zu beachten sind	523	43%	79	52%
Persönliche Schulungen mit unserem IT- oder IT-Sicherheitsteam	498	41%	79	52%
Vor dem Besuch bestimmter Websites erhalte ich Aufforderungen, zu überprüfen, ob ein Link „sicher“ ist oder nicht.	463	38%	67	44%
Sonstiges	4	0%	1	1%
Mein Unternehmen bietet keine Schulungen an	15	1%	1	1%

Die Vorbereitung auf die Cyber-Resilienz macht einen echten Unterschied

Wie bei den meisten Dingen im Leben kann auch bei der Cybersicherheit eine gute Vorbereitung den entscheidenden Unterschied ausmachen.
Die gute Nachricht ist, dass Finanzdienstleister besser vorbereitet sind als die meisten anderen: 53% der befragten Finanzunternehmen verfügen bereits über eine Strategie zur Cyber-Resilienz.

53%

der befragten Finanzunternehmen verfügen bereits über eine Strategie zur Cyber-Resilienz.

Wie viel besser? Dreißig Prozent der Finanzunternehmen MIT einer Strategie zur Cyber Resilience berichteten, dass keine der folgenden negativen Folgen eines Cyberangriffs zu verzeichnen war. Fast neun von zehn Finanzdienstleistern (89 Prozent) ohne eine Strategie zur Cyber Resilience erlebten eine oder mehrere:

- **geschäftliche Unterbrechung**
- **Datenverlust**
- **finanzielle Verluste**
- **Rufschädigung**
- **Auswirkungen auf die Einhaltung von Vorschriften**
- **Auswirkungen auf die Produktivität der Mitarbeiter**

Ebenso zeigen bestimmte Branchen, die verstärkt **Collaboration-Tools** einsetzen, eine höhere Besorgnis über deren Sicherheit. Dazu gehören das Baugewerbe, der Energiesektor, Verbraucherdienstleistungen und Unternehmensdienstleistungen, wo der Grad der Besorgnis zwischen 76% (Baugewerbe) und 86% (Unternehmens- und professionelle Dienstleistungen) der Befragten lag.

Noch schlimmer ist, dass einige Unternehmen, die keine Strategie für die Widerstandsfähigkeit gegenüber Cyberangriffen haben, zwei oder mehr der aufgeführten Auswirkungen zu spüren bekamen - und ein Unternehmen berichtete, dass es unter allen sechs Auswirkungen zu leiden hatte.

Erfreulicherweise planen weitere 39% der befragten Finanzdienstleister, die noch nicht über eine Cyber-Resilienz-Strategie verfügen, die Einführung einer solchen Strategie innerhalb des nächsten Jahres, wodurch sich die Zahl der Finanzunternehmen mit einer Resilienz-Strategie auf 92% erhöhen würde (im Vergleich zu 90% bei allen Befragten).

39% **der Finanzdienstleistungsunternehmen, die noch keinen Plan für die Widerstandsfähigkeit gegenüber Cyberangriffen haben, erwarten, dass sie innerhalb des nächsten Jahres einen solchen Plan einführen werden.**

Wichtigste Erkenntnisse

Da digitale/mobile Finanzdienstleistungsaktivitäten wohl auch zukünftig rasant weiter steigen, wird auch die Anzahl und die Rafinesse von Cyberanriffen auf Finanzunternehmen weiter steigen. Außerdem werden Cyberkriminelle weiterhin die Folgen von COVID-19 und die verstreuten Arbeitskräfte in den Unternehmen ausnutzen. Der Weg in eine sicherere Zukunft für Finanzdienstleistungsunternehmen führt über diese fünf zentralen Ansätze:

.01 Bauen Sie eine mehrschichtige Verteidigung auf.

Da E-Mails nach wie vor der häufigste Bedrohungsvektor sind und ihr Volumen voraussichtlich noch zunehmen wird, müssen Finanzunternehmen mehrere Sicherheitstechnologien einsetzen, um ihre E-Mail-Systeme zu schützen. Eine mehrschichtige Verteidigung bietet die beste Chance, diese wachsende Bedrohung zu neutralisieren.

.02 Bewerten Sie die Technologie während der Pandemie neu.

Für Cyberkriminelle sind E-Mails nach wie vor die gängigste Methode, um ihre Angriffe durchzuführen, und insbesondere Phishing ist seit Beginn der Pandemie sehr viel bösartiger geworden. Um die immer ausgefeilteren Angriffe abzuwehren, müssen verschiedene Technologien eingesetzt werden. Diese mehrschichtigen Verteidigungen ergänzen sich gegenseitig. Wenn eine erste Verteidigung einen Angriff nicht vollständig abwehren kann, greifen die weiteren Maßnahmen, die die Bedrohung neutralisieren können.

.03 Schenken Sie Ransomware besondere Aufmerksamkeit.

Die Bedrohung durch Ransomware, ihre potenziellen Kosten und die Komplexität von AML nehmen weiter zu. Die meisten dieser Angriffe erfolgen per E-Mail, und mehrschichtige Verteidigungsmaßnahmen können helfen, Daten durch strenge Backup- und Aufbewahrungsrichtlinien zu schützen. Repositorys außerhalb des Netzwerks, sind wichtige Lösungen zur Minderung des dauerhaften Datenverlusts für Finanzunternehmen. Die Wahrung des Kundenvertrauens und des guten Rufs sind für den Geschäftserfolg eines Finanzunternehmens von entscheidender Bedeutung.

.04 Verbessern Sie die Schulung zum Sicherheitsbewusstsein.

Der größte potenzielle Unterschied kann durch die Stärkung der schwächsten Glieder der Cybersicherheit erzielt werden: die Menschen. Finanzunternehmen müssen ihre führenden Schulungspraktiken für Sicherheitsbewusstsein mit personalisierteren/individuelleren Schulungen und größerer Häufigkeit erweitern.

.05 Beschleunigung der Entwicklung von Strategien für die Widerstandsfähigkeit im Internet.

Finanzdienstleister scheinen besser als die meisten anderen auf Cyberrisiken vorbereitet zu sein. Allerdings sind noch nicht alle Unternehmen so weit. Diejenigen, die noch keine Resilienzstrategien haben, sollten ihre Entwicklung beschleunigen. Und für diejenigen, die dies bereits tun, wird die Bedeutung nachhaltiger Wachsamkeit, Aktualisierung und Aufrechterhaltung ihrer Cyber-Resilience-Strategien weiter wachsen.

mimecast®

Relentless protection. Resilient world.™

2.Ebd.
3.“Cyber Risk is the New Threat to Financial Stability,” IMF Blog
4.“Ransomware is growing at an alarming rate, warns GCHQ chief,” ZDNet
5.Combatting Ransomware Institute for Security and Technology
6. Global Sicherheitseinstellung Umfrage, Crowdstrike
7.“Ransomware Attacks a Growing Global Security and Financial Threat,” FitchRatings
8.“Cloud-basierte E-Mail Sicherheit Markt- Wachstum, Trends, Covid-19 und Forecasts (2021-2026)” Mordor Intelligence”
9.“Online Branchen Die meisten Gezielt von Phishing Anschläge wie von das 4. Quartal 2020“, Statista

Mimecast ist ein Anbieter für Cybersicherheit, der Tausenden von Unternehmen weltweit hilft, E-Mails sicherer zu machen, das Vertrauen wiederherzustellen und ihre Cyber Resilience zu stärken. Die erweiterte Cloud-Suite von Mimecast ermöglicht es Unternehmen, eine umfassende Cyber-Resilience-Strategie zu implementieren. Von E-Mail- und Websicherheit, Archivierung und Datenschutz bis hin zu Awareness Training, Sicherung der Betriebsbereitschaft und mehr – Mimecast hilft Unternehmen, sich angesichts von Cyberangriffen, menschlichem Versagen und technischen Fehlern zu behaupten.

CE-3361