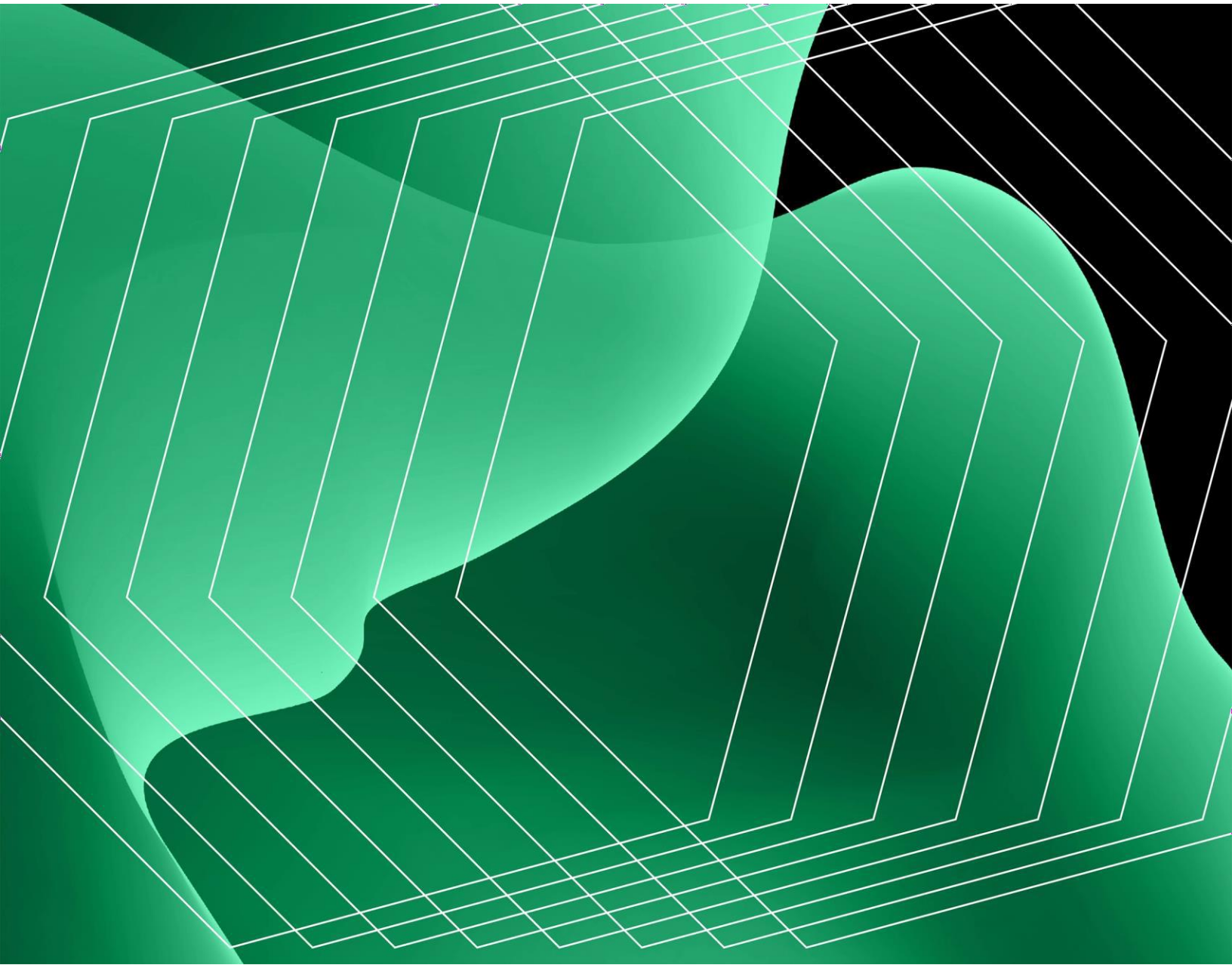
FORRESTER®

Der gesamte wirtschaftliche Nutzen™ von Mimecast

Kosteneinsparungen und geschäftliche Vorteile durch Mimecast

EINE FORRESTER STUDIE ÜBER DIE WIRTSCHAFTLICHEN AUSWIRKUNGEN IM AUFTRAG VON MIMECAST, JULI 2024



Inhaltsverzeichnis

Beratungsteam:

Andrew Nadler

ÜBER FORRESTER CONSULTING

Forrester bietet unabhängige und objektive , forschungsbasierte Beratung , um Führungskräfte dabei zu unterstützen, wichtige Ergebnisse zu erzielen. Auf der Grundlage unserer kundenorientierten Forschung arbeiten die erfahrenen Berater von Forrester mit Führungskräften zusammen, um ihre spezifischen Prioritäten mithilfe eines einzigartigen Beratungsmodells umzusetzen, das eine nachhaltige Wirkung gewährleistet. Weitere Informationen finden Sie unter forrester.com/consulting.

Zusammenfassung

Unternehmen sehen sich mit einer zunehmend komplexen und unsicheren Bedrohungslandschaft im Bereich der Cybersicherheit konfrontiert. 78 % der Unternehmen hatten in den letzten 12 Monaten mindestens einen Vorfall zu verzeichnen und mehr als die Hälfte dieser Unternehmen schätzt die Kosten eines Vorfalls auf mehr als 1 Million Dollar.[1] E-Mail ist nach wie vor die von den Mitarbeitern am häufigsten genutzte Anwendung und stellt daher für Angreifer ein wichtiges Einfallstor dar, da sie ihnen direkten Zugang zu den Endbenutzern ermöglicht.[2] Unternehmen, die gängige Cloud-E-Mail-Infrastruktur-Anbieter nutzen, wenden sich einem mehrschichtigen Ansatz mit Sicherheitslösungen zu, um die Art und Weise, wie sie kommunizieren und zusammenarbeiten, zu schützen.[3] Der Einsatz einer E-Mail-Sicherheitslösung für Unternehmen wie Mimecast in Verbindung mit nativen E-Mail-Sicherheitsangeboten kann eine größere Effizienz und Effizienzen als bei einer rein nativen E-Mail-Sicherheit, während gleichzeitig das Konzentrationsrisiko verringert und die Zuverlässigkeit erhöht wird.[4]

Mimecast Advanced Email Security ist eine KI-gestützte E-Mail-Sicherheitslösung für Unternehmen, die E-Mail-basierte Bedrohungen wie Phishing, Malware und die Kompromittierung geschäftlicher E-Mails (BEC) mit flexiblen Bereitstellungsmethoden abwehrt, darunter Email Security Cloud Integrated, eine Cloud-native, API-fähige E-Mail-Sicherheitslösung (CAPES), und Email Security Cloud Gateway, eine sichere E-Mail-Gateway-Lösung (SEG). Die Mimecast-Produktsuite umfasst auch Email Archive und Security Awareness Training. Kunden können Advanced Email Security mit Support, Services und Add-ons wie DMARC Analyzer und Collaboration Security weiter ausbauen.

Mimecast beauftragte Forrester Consulting mit der Durchführung einer TEI-Studie (Total Economic Impact™) und der Untersuchung der potenziellen Kapitalrendite (ROI), die Unternehmen durch den Einsatz von Mimecast erzielen können.[5] Der Zweck dieser Studie besteht darin, den Lesern einen Rahmen zur Verfügung zu stellen, um die potenziellen finanziellen Auswirkungen von Mimecast auf ihre Unternehmen zu bewerten.

Rentabilität der Investition (ROI)
255%

Nettogegenwartswert
$1.53M

Um die Vorteile, Kosten und Risiken, die mit dieser Investition verbunden sind, besser zu verstehen, hat Forrester sieben Vertreter von sechs Unternehmen befragt, die Erfahrungen mit Mimecast haben und sowohl CAPES- als auch SEG-Bereitstellungsmethoden einsetzen. Für die Zwecke dieser Studie hat Forrester die Erfahrungen der Befragten zusammengefasst und die Ergebnisse zu einem einzelnen Composite zusammengefasst. Bei diesem Unternehmen handelt es sich um ein globales Unternehmen mit 2.500 Nutzern, die es mit Mimecast als Erweiterung seiner eigenen E-Mail-Infrastruktur schützen möchte, indem es die Bereitstellungsmethode Email Security Cloud Integrated von Mimecast verwendet.

Die Befragten gaben an, dass ihre Unternehmen vor dem Einsatz von Mimecast in der Regel entweder ältere Lösungen vor Ort, andere E-Mail-Sicherheitslösungen oder einfach eine eigene E-Mail-Sicherheitsinfrastruktur verwendeten. Frühere Versuche waren jedoch nur begrenzt erfolgreich, so dass sie mit Herausforderungen in Bezug auf die Effektivität, Effizienz und Zuverlässigkeit der E-Mail-Sicherheit konfrontiert waren.

Nach der Investition in Mimecast profitierten die Unternehmen der Befragten von einer erhöhten Sicherheitseffizienz, einer verbesserten Effizienz der IT- und Sicherheitsteams sowie der Endbenutzer und einem allgemeinen geschäftlichen Nutzen durch verbesserte Sicherheit.

SCHLÜSSELFINDEN

Quantifizierter Nutzen. Der dreijährige, risikobereinigte Gegenwartswert (PV) des quantifizierten Nutzens für die zusammengesetzte Organisation umfasst:

- **Verbesserte Sicherheit gegen bösartige E-Mails.** Das Verbundunternehmen implementiert Mimecast, um die Wirksamkeit seiner nativen E-Mail-Plattform zu erhöhen und E-Mail-basierte Bedrohungen abzuwehren, einschließlich Angriffen, die darauf abzielen, mit der nativen E-Mail-Sicherheitsinfrastruktur erfolgreich zu sein. Dank dieser gesteigerten Effizienz vermeidet das Unternehmen externe Angriffe und die damit verbundenen Kosten wie Geldbußen, Geschäftsunterbrechungen und Umsatzverluste. Forrester hat die Daten der Befragten und die Forrester Analytics Business Technographics Security Survey 2023 verwendet, um diesen Wert zu berechnen. Über einen Zeitraum von drei Jahren ist die verbesserte Sicherheit für das Unternehmen 1,1 Millionen Dollar wert.
- **Verbesserte Effizienz der Sicherheitsabläufe mit 24% Zeitersparnis bei der Bekämpfung von E-Mail-basierten Angriffen und 50% Zeitersparnis bei der Verwaltung der E-Mail-Plattform.** Die Sicherheits- und IT-Teams des Verbundunternehmens profitieren von der Sicherheitseffizienz von Mimecast, seinen APIs und Integrationen, der Automatisierung und

„Wir hatten keine Verstöße oder böswillige Angriffe.“ [mit Mimecast]."

IT-ADMINISTRATOR, GESUNDHEITSWESEN

mehr, so dass sie Zeit für höherwertige Aufgaben haben. Diese Zeitersparnis basiert auf den sieben Sicherheitsmitarbeitern und einem IT-Mitarbeiter, die insgesamt 2.267 Stunden pro Jahr produktiv umverteilen, wie die Daten der Umfrage und der Befragten belegen. Über einen Zeitraum von drei Jahren ist dieser Produktivitätsvorteil Folgendes wert 337.000 $ an die Organisation.

- **Verbesserte Effizienz der Endbenutzer mit 24% Zeitersparnis bei E-Mail-basierten Angriffen.** Dank der Wirksamkeit von Mimecast profitieren die Endbenutzer von weniger unerwünschten und bösartigen E-Mails in ihren Posteingängen, so dass sie die eingesparte Zeit für wertvollere Aufgaben nutzen können. Forrester berechnet den Wert dieser verbesserten Effizienz anhand von Umfrage- und Befragungsdaten mit den 2.500 Endbenutzern des zusammengesetzten Unternehmens, die mit jedem vermiedenen Vorfall Stunden an Produktivität sparen. Über einen Zeitraum von drei Jahren ist dieser Produktivitätsvorteil für das Unternehmen $727.000 wert.

Nicht bezifferte Vorteile. Zu den Vorteilen, die einen Wert für das Unternehmen darstellen, aber für diese Studie nicht quantifiziert wurden, gehören:

- **Geschäftliche Vorteile, einschließlich Schutz des Rufs.** Durch die verstärkte Sicherheit mit Mimecast verringert das Unternehmen das Risiko, kompromittiert zu werden, und vermeidet so nicht nur die mit Sicherheitsverletzungen verbundenen Verluste, einschließlich Umsatzeinbußen, Vertragskündigungen und Geldstrafen, sondern schützt auch seine Marke und seinen Ruf, indem es unerwünschte E-Mail-Versendungen und negative Publicity vermeidet. Darüber hinaus helfen die Funktionen von Mimecast, einschließlich des DMARC Analyzer, der die DMARC-Authentifizierung für Domains überwacht, dem Unternehmen beim Schutz

seine Marke und seinen E-Mail-Ruf noch weiter zu verbessern, indem er sicherstellt, dass seine Domains vertrauenswürdig sind. Dies erhöht das Vertrauen der Kunden und führt zu potenziellen Vorteilen beim E-Mail-Marketing und zu Umsatzwachstum.

- **Mimecast-Services, -Support und -Kundenerfahrung.** Das Unternehmen nutzt die Vorteile der Mimecast-Services und kann so Mimecast schneller implementieren. Außerdem nutzt es den technischen Support von Mimecast, um seine Geschäftsziele zu erreichen.

Kosten. Dreijährige, risikobereinigte PV-Kosten für die zusammengesetzte Organisation umfassen:

- **Lizenzkosten von 438.000 $.** Zusätzlich zu der Lizenzgebühr pro Benutzer und Jahr für Mimecast erwirbt das Unternehmen Advanced Support und Guided Implementation Services und hat die Möglichkeit, Add-ons zu erwerben.
- **Kosten für Implementierung, Schulung und laufende Verwaltung in Höhe von 163.000 $.** Nachdem sich das Unternehmen für Mimecast entschieden hat, nimmt es sich die Zeit, die E-Mail-Sicherheitslösung zu implementieren, zu schulen und zu trainieren und die Lösung kontinuierlich zu verwalten.

Die repräsentativen Befragungen und die Finanzanalyse ergaben, dass eine zusammengesetzte Organisation über einen Zeitraum von drei Jahren Vorteile in Höhe von 2,13 Millionen Dollar gegenüber Kosten in Höhe von 602.000 Dollar erfährt, was einen Nettogegenwartswert (NPV) von 1,53 Millionen Dollar und einen ROI von 255% ergibt.

Rentabilität der Investition (ROI)

255%

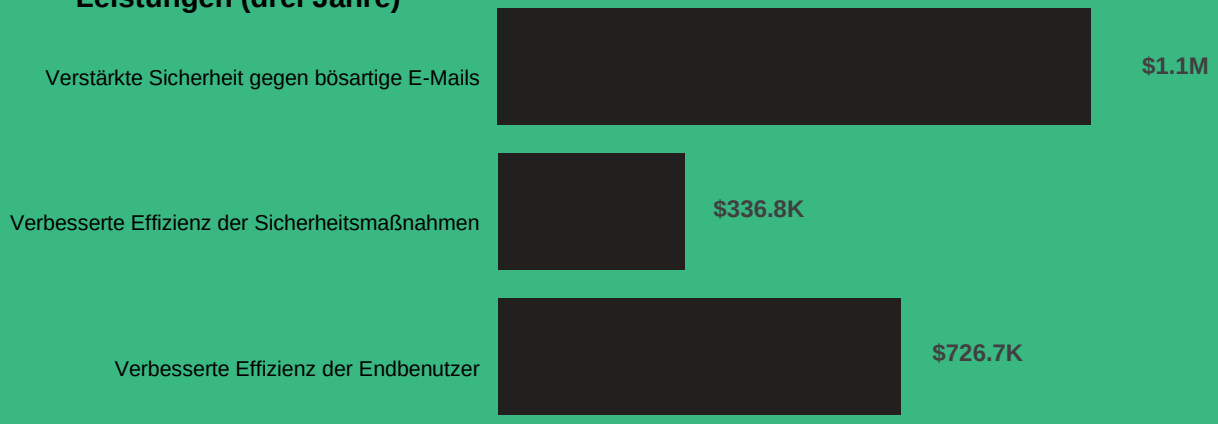
Vorteile PV

$2.13M

Nettogegenwartswert (NPV)

$1.53M

Leistungen (drei Jahre)



TEI RAHMEN UND METHODIK

Aus den Informationen, die in den Interviews zur Verfügung gestellt wurden, hat Forrester einen Rahmen für die wirtschaftlichen Auswirkungen™ für Unternehmen erstellt, die eine Investition in Mimecast in Betracht ziehen.

Das Ziel des Rahmens ist es, die Kosten-, Nutzen-, Flexibilitäts- und Risikofaktoren zu identifizieren, die die Investition beeinflussen Entscheidung. Forrester hat einen mehrstufigen Ansatz gewählt, um die Auswirkungen zu bewerten, die Mimecast auf ein Unternehmen haben kann.

ANGABEN

Die Leser sollten Folgendes beachten:

Diese Studie wurde von Mimecast in Auftrag gegeben und von Forrester Consulting durchgeführt. Es ist nicht dazu gedacht, als Wettbewerbsanalyse verwendet zu werden.

Forrester macht keine Annahmen über den potenziellen ROI, den andere Unternehmen erhalten werden. Forrester rät den Lesern dringend, ihre eigenen Schätzungen innerhalb des in der Studie vorgegebenen Rahmens zu verwenden, um die Angemessenheit einer Investition in Mimecast zu bestimmen.

Mimecast hat die Studie geprüft und Forrester Feedback gegeben. Forrester behält jedoch die redaktionelle Kontrolle über die Studie und ihre Ergebnisse und akzeptiert keine Änderungen an der Studie, die den Ergebnissen von Forrester widersprechen oder die Bedeutung der Studie verschleiern.

Mimecast stellte die Kundennamen für die Interviews zur Verfügung, nahm aber nicht an den Interviews teil.

1. **Due Diligence**
   Befragung von Mimecast-Stakeholdern und Forrester-Analysten, um Daten über Mimecast zu sammeln.
2. **Interviews**
   Wir haben sieben Vertreter von sechs Unternehmen befragt, die Mimecast nutzen, um Daten über Kosten, Nutzen und Risiken zu erhalten.
3. **Zusammengesetzte Organisation** Entwarf eine zusammengesetzte Organisation auf der Grundlage der Merkmale der Organisationen der Befragten.
4. **Finanzmodellrahmen** Konstruierte ein Finanzmodell, das für die Interviews repräsentativ ist, unter Verwendung der TEI-Methode und passte das Finanzmodell auf der Grundlage der Fragen und Bedenken der Interviewpartner an.
5. **Fallstudie**
   Bei der Modellierung der Auswirkungen von Investitionen wurden vier grundlegende Elemente des TEI verwendet: Nutzen, Kosten, Flexibilität und Risiken. Angesichts der immer ausgefeilteren ROI-Analysen im Zusammenhang mit IT-Investitionen bietet die TEI-Methode von Forrester ein vollständiges Bild der gesamten wirtschaftlichen Auswirkungen von Kaufentscheidungen. Weitere Informationen über die TEI-Methode finden Sie inAnhang A.

Die Mimecast Customer Journey

Beweggründe für die Investition in Mimecast

Interviews			
Rolle	**Branche**	**Region**	**Geschützte Benutzer**
SOC Architekt	Gesundheitswesen	Anzahl der	135,000
Leiter der Abteilung Infrastrukturbetrieb	Multi-Industrie	Naher Osten, Afrika und Asien	25.000
IT-Direktor, Anwendungsadministration	Lebensmittel	Anzahl der	15,000
Vizepräsident für IT	Informationsmaterial	Nordamerika	1000
Infrastrukturmanager Sicherheitsmanager	Unterhaltung	Europa	400
IT-Administrator	Gesundheitswesen	Nordamerika	50

SCHLÜSSELHERAUSFORDERUNGEN

Vor Mimecast verwendeten die befragten Unternehmen in der Regel entweder eine ältere Lösung vor Ort, eine andere E-Mail-Sicherheitslösung oder eine eigene E-Mail-Sicherheitsinfrastruktur. Nachdem sie sich gemeinsamen Herausforderungen gegenüber sahen, entschieden sie sich für Mimecast als E-Mail-Sicherheitslösung für Unternehmen, wobei sie je nach Umgebung und Bedarf entweder die SEG- oder die CAPES-Bereitstellungsmethode verwendeten.

Die Befragten stellten fest, dass ihre Organisationen mit gemeinsamen Herausforderungen kämpften, darunter:

- **Probleme mit der Wirksamkeit bei bösartigen und unerwünschten E-Mails.** Die Befragten sagten Forrester, dass die größte Herausforderung, mit der sie vor Mimecast zu kämpfen hatten, die Wirksamkeit ihrer E-Mail-Sicherheitslösungen war. Außerdem sagten sie, dass das Volumen bösartiger und unerwünschter E-Mails immer weiter zunimmt. Der SOC-Architekt eines Gesundheitsunternehmens erklärte: „Phishing war ein Albtraum. Nichts wurde erkannt, und die Phishing-E-Mails wurden zugestellt … Die URL-Erkennung war [auch] nicht gut.“ Ähnlich äußerte sich der Leiter des Infrastrukturbetriebs eines branchenübergreifenden

Organisation sagte: „Wir hatten Vorfälle, die [unsere vorherige] E-Mail-Sicherheitslösung nicht erkennen konnte.“

> „E-Mail ist eine große Bedrohung für die Cybersicherheit.“
>
> IT-DIREKTOR, ANWENDUNGSVERWALTUNG, LEBENSMITTEL

- **Sicherheitsteams werden durch ineffiziente Tools belastet.** Die Befragten gaben an, dass die IT- und Sicherheitsteams ihrer Unternehmen nicht nur mit bösartigen und unerwünschten E-Mails zu kämpfen haben, sondern auch mit der Effizienz ihrer Arbeit. Sie sprachen von übermäßigem Zeitaufwand für die Untersuchung bösartiger und unerwünschter E-Mails, ineffizientem E-Mail-Sicherheitsmanagement, unzureichend granularem Zugriff für die Verwaltung von E-Mails und Richtlinien, unzureichenden Integrationen und mehr.
- **Zuverlässigkeitsprobleme mit Ausfällen, verspäteten E-Mails und mangelndem Support.** Darüber hinaus berichteten die Befragten, wie ihre Unternehmen mit Herausforderungen in Bezug auf die Zuverlässigkeit konfrontiert waren. Sie berichteten von Ausfällen und mangelndem Support. Der Leiter des Infrastrukturbetriebs in einem Unternehmen, das mehrere Branchen abdeckt, sagte: „Wir hatten Probleme mit Ausfällen. Manchmal erhielten wir E-Mails verspätet. Es fehlte auch an Proaktivität und Support.“ Der IT-Direktor für Anwendungsadministration eines Lebensmittelunternehmens, der das Add-on Mailbox Continuity von Mimecast zusammen mit einer SEG-Implementierung verwendet, fügt hinzu: „E-Mail-Kontinuität ist wichtig. Ich verwende jetzt Mimecast, um meinen E-Mail-Verkehr fortzusetzen.“

> „E-Mail ist der erste Angriffsvektor in jedem Unternehmen. Wir wollen zwei Schichten haben, um in der Tiefe verteidigen zu können.“
>
> SOC ARCHITEKT, GESUNDHEITSWESEN

LÖSUNGSANFORDERUNGEN/INVESTITIONSZIELE

Die befragten Organisationen suchten nach einer Lösung, die dies ermöglicht:

- Bieten Sie effektiven, cloudbasierten und kosteneffizienten Schutz vor bösartigen und unerwünschten E-Mails in Verbindung mit Ihrer eigenen E-Mail-Sicherheitsinfrastruktur.
- Bieten Sie je nach den Bedürfnissen Ihres Unternehmens sowohl CAPES- als auch SEG-Einsatzmethoden an.
- Erfüllen Sie mehr als nur die Anforderungen an die E-Mail-Sicherheit, indem Sie die gewünschten Funktionen und andere Produkte für die Archivierung von Informationen, Sicherheitsbewusstsein und Schulungen (SA&T) und mehr anbieten.
- Bieten Sie Benutzerfreundlichkeit und Verwaltung mit einer einzelnen Glasscheibe und ausreichender Granularität.
- Von einem Anbieter unterstützt werden, dem sie vertrauen.

> „Wir hatten eine starke Empfehlung von unserem Informationssicherheitsteam … [Mit unserer Nutzung einer gemeinsamen E-Mail-Plattform] … sie empfahlen eine Lösung eines Drittanbieters [wie Mimecast].“
>
> **LEITER DER ABTEILUNG INFRASTRUKTURBETRIEB, MULTI-INDUSTRIE**

Marktübersicht

E-Mail-Sicherheit für Unternehmen

Forrester definiert **E-Mail-Sicherheit für Unternehmen** als Technologien, die die E-Mail-Kommunikation von Unternehmen schützen, um die Auswirkungen von E-Mail-Angriffen abzuschwächen und zu vermindern. Dazu gehören lokale oder cloudbasierte E-Mail-Gateways und Lösungen, die in die Cloud-basierte E-Mail-Infrastruktur integriert werden. Zu den Funktionen gehören Anti-Spam, Anti-Malware, Anti-Phishing, Data Loss Prevention (DLP), Verschlüsselung, Phishing Aufklärung, Schutz vor kompromittierten geschäftlichen E-Mails (BEC) und Spoofing, Erkennung bösartiger URLs und E-Mail-Authentifizierung.[6]

Anbieter von E-Mail-Infrastrukturen stellen Unternehmen ihre zentrale E-Mail-Infrastruktur zur Verfügung, zusammen mit APIs, die es anderen E-Mail-Sicherheitslösungen für Unternehmen ermöglichen, die integrierten Sicherheitsfunktionen durch zusätzliche Funktionen zu ergänzen.[7]

Lösungen für sichere E-Mail-Gateways (SEG) sind einem E-Mail-Infrastrukturanbieter oder einer lokalen E-Mail-Infrastruktur vorgeschaltet.[8]

Cloud-native API-fähige E-Mail-Sicherheitslösungen (CAPES) lassen sich in E-Mail-Infrastrukturanbieter integrieren, um deren native Sicherheitsfunktionen zu erweitern.[9]

VERBUNDUNTERNEHMEN

Auf der Grundlage der Interviews erstellte Forrester einen TEI-Rahmen, ein zusammengesetztes Unternehmen und eine ROI-Analyse, die die finanziell betroffenen Bereiche veranschaulicht. Die zusammengesetzte Organisation ist repräsentativ für die sechs befragten Organisationen und wird für die Darstellung der aggregierten Finanzanalyse im nächsten Abschnitt verwendet. Die zusammengesetzte Organisation hat die folgenden Merkmale:

Beschreibung von Composite. Die Composite-Organisation ist ein globales Unternehmen mit 2.500 Mitarbeitern. Dazu gehören sieben Vollzeitkräfte, die

Sicherheitsvorfälle verwalten, und eine Vollzeitkraft E-Mail verwalten. Vor Mimecast hat sich das Unternehmen ausschließlich auf seine eigene E-Mail-Sicherheitsinfrastruktur verlassen und wollte eine CAPES-Lösung hinzufügen, um die Funktionalität und Sicherheitseffizienz seines eigenen E-Mail-Infrastrukturanbieters zu erweitern. Es ist der Kunde einer Cloud-basierten Produktivitätsplattform.

Merkmale der Bereitstellung. Das gemischte Unternehmen beginnt mit der Nutzung von Mimecast im Jahr 1, nach einer Implementierungsphase. Es entscheidet sich für Mimecasts Email Security Cloud Integrated Bereitstellungsmethode. Diese Implementierung deckt 100% aller 2.500 Mitarbeiter in allen Regionen ab.

Wichtige Annahmen

Mimecast Email Security Cloud Integrated Bereitstellungsmethode

2.500 Benutzer mit Mimecast geschützt

> „Mein Team hat [Mimecast] letzten Monat mit [anderen E-Mail-Sicherheitslösungen] verglichen. Sie sagten, Mimecast sei noch besser.“
>
> IT-DIREKTOR, ANWENDUNGSVERWALTUNG, LEBENSMITTEL

Analyse der Vorteile

Quantifizierte Nutzendaten, die auf das Kompositum angewendet werden

Vorteile insgesamt						
Ref.	**Profitieren Sie von**	**Jahr 1**	**Jahr 2**	**Jahr 3**	**Gesamt**	**Barwert**
Atr	Verstärkte Sicherheit gegen bösartige E-Mails	$430,166	$430,166	$430,166	$1,290,499	$1,069,760
Btr	Verbesserte Effizienz der Sicherheitsmaßnahmen	$135,443	$135,443	$135,443	$406,328	$336,826
Ctr	Verbesserte Effizienz der Endbenutzer	$292,205	$292,205	$292,205	$876,616	$726,671
	Gesamtleistungen (risikobereinigt)	$857,814	$857,814	$857,814	$2,573,443	$2,133,257

VERSTÄRKTE SICHERHEIT GEGEN BÖSARTIGE E-MAILS

Beweise und Daten. Die Befragten gaben Forrester gegenüber zuversichtlich an, dass der Einsatz von Mimecast zusammen mit ihrer nativen E-Mail-Sicherheitsinfrastruktur die Sicherheit ihrer Unternehmen vor bösartigen E-Mails im Vergleich zu ihren früheren Umgebungen erhöht hat. Angesichts der Tatsache, dass E-Mail ein wichtiger Bedrohungsvektor ist, sagten sie, dass Mimecast eine erste Verteidigungslinie (in Verbindung mit ihrer nativen E-Mail-Sicherheitsinfrastruktur) darstellt, um externe Angriffe abzuwehren.

- Die Befragten gaben an, dass die Wahrscheinlichkeit einer Sicherheitsverletzung hoch ist und weiter zunimmt. Außerdem erklärten sie, wie kostspielig Verstöße sind. Der SOC-Architekt einer Organisation des Gesundheitswesens hat zum Beispiel die Kosten von BEC genau beschrieben: „Wir leisten gute Arbeit beim Schutz vor Identitätsmissbrauch [mit Mimecast], was für unser Unternehmen sehr wertvoll ist, denn wir haben in der Vergangenheit Fälle erlebt, in denen uns das mehrere tausend Euro gekostet hat.“ Sie fügten hinzu: „Wenn wir über schlechte Anhänge sprechen, könnten die Auswirkungen [eines möglichen Verstoßes] dort am größten sein. Wir setzen Mimecast ein, um viele Erweiterungen zu verbieten.“ Sie erläuterten auch die weiteren Auswirkungen eines möglichen Verstoßes und sagten: „[Es könnte] Auswirkungen auf die Produktion, die Auslieferung und die Pharmakovigilanz haben, die eine unserer Hauptaktivitäten ist. Wir müssen für Krankenhäuser und LKW-Lieferungen rund um die Uhr verfügbar und erreichbar sein in

falls es ein Problem gibt. Wir haben alle unsere Pharmakovigilanz-Aktivitäten zu Mimecast migriert, um die Kontinuität dieser Aktivitäten zu gewährleisten, denn diese Aktivitäten dürfen niemals aufhören."

- Bei der Betrachtung der Hauptbedrohungsvektoren für Angriffe in ihren Unternehmen verwiesen die Befragten auf E-Mail. Der Sicherheitsmanager eines Unterhaltungsunternehmens sagte: „Die Hauptoberfläche für Angriffe ist die E-Mail. Der erste Weg, auf dem sich [externe Angreifer] Unternehmen nähern, ist jetzt immer die E-Mail." Ähnlich äußerte sich der Vizepräsident der IT-Abteilung einer Bildungseinrichtung: „[E-Mail] ist unser wichtigster Kontaktpunkt intern und mit Anbietern."

> „Social Engineering ist die wichtigste Methode für Angreifer, in Ihr System einzudringen. Mimecast ist entscheidend, um Social Engineering zu verhindern."
>
> **VP OF IT, BILDUNG**

- Darüber hinaus wiesen die Befragten darauf hin, dass die Nutzung gängiger E-Mail-Plattformen auch ihren Bedrohungsvektor erhöhen könnte. Der SOC-Architekt einer Organisation des Gesundheitswesens fügte hinzu: „Wir wollen Verteidigung in der Tiefe. Wir brauchen zwei Lösungen [einschließlich unserer eigenen E-Mail-Sicherheitsinfrastruktur]. Mimecast leistet eine wunderbare erste Filterschicht."
- Die Befragten erörterten auch, wie Mimecast angesichts des erheblichen Risikos von E-Mail-basierten externen Angriffen und gängigen E-Mail-Plattformen als E-Mail-Sicherheitslösung wirksam wurde. Sie betonten den Schutz vor Phishing, die Abwehr von BEC, den Schutz vor Malware und mehr. Der Vizepräsident der IT-Abteilung einer Bildungseinrichtung erklärte: „Sie sind die erste Verteidigungslinie nach außen, sie strippen Malware, blockieren Phishing Versuche, fangen [Inhalte] ab, die ein- oder ausgehen, und korrigieren schlechtes Verhalten. Mimecast automatisiert den größten Teil davon und gibt uns dennoch die Kontrolle über die Stücke, die uns am Herzen

liegen, um sie von einer zweiten Person überprüfen zu lassen. Das ist die erste Verteidigungslinie.“

- Der SOC-Architekt einer Organisation des Gesundheitswesens hob die Anpassungsfähigkeit von Mimecast als Hauptgrund für die erhöhte Effizienz hervor: „Mimecast filtert Bedrohungen auf mehreren Erkennungsebenen und ermöglicht eine Menge Anpassungen.“

> „Mimecast [und native E-Mail-Sicherheitsinfrastruktur zusammen] ist besser.“
>
> **SICHERHEITSMANAGER, UNTERHALTUNG**

- Insgesamt äußerten sich die Befragten sehr positiv über die Effizienz von Mimecast. Der IT-Direktor für die Anwendungsadministration eines Lebensmittelunternehmens sagte: „Wir hatten noch nie einen Verstoß aufgrund von E-Mail.“ Der SOC-Architekt einer Organisation des Gesundheitswesens sagte: „Wir haben einen enormen Rückgang der schlechten URLs in den Posteingängen festgestellt.“ Der Sicherheitsbeauftragte eines Unterhaltungsunternehmens sagte: "Wir sehen keinerlei Hinweise darauf, dass Malware per E-Mail eingeht [mit Mimecast], und wir schauen nach." Der Leiter des Infrastrukturbetriebs eines branchenübergreifenden Unternehmens sagte: „[Mimecast] ist sehr wertvoll, weil es vor vielen bösartigen Angriffen und Malware schützt.....Sie ist besser als unsere vorherige Lösung.“ Sie fügten hinzu: „Blockieren ist fast 100%.“
- Der IT-Administrator einer Organisation im Gesundheitswesen sagte: „Der Wert liegt in der Kontrolle der bösartigen Kommunikation, die in meine Umgebung gelangt … Ich habe keinerlei Angriffe erlebt.“
- Darüber hinaus sagten die Befragten, dass die Effizienz von Mimecast, die durch KI unterstützt wird, im Laufe der Zeit nur noch besser geworden ist. Der

IT-Administrator einer Gesundheitseinrichtung erklärt: "Diese Definitionen werden immer besser und besser. Die Umwelt wird jeden Tag stärker … Es hat uns ein Sicherheitsnetz geboten. Wir hatten keine Verstöße."

> „Der Wert von Mimecast liegt in weniger Verwaltungsaufwand und mehr Schutz.“
>
> **LEITER DER ABTEILUNG INFRASTRUKTURBETRIEB, MULTI-INDUSTRIE**

Modellierung und Annahmen. Auf der Grundlage der Interviews geht Forrester von den folgenden Annahmen über die zusammengesetzte Organisation aus:

- Die Wahrscheinlichkeit, dass eine oder mehrere Sicherheitsverletzungen pro Jahr auftreten, liegt bei 72%.[10]
- Die durchschnittlichen kumulativen Kosten der Unternehmen für Sicherheitsverletzungen betragen 2.892.000 $.[11]
- Der Prozentsatz der Verstöße durch externe Angriffe liegt bei 49%.[12]
- Der Anteil der externen Angriffe, die per E-Mail ausgeführt werden können, wie Phishing und Social Engineering, liegt bei 50%.
- Das Unternehmen reduziert sein Risiko eines externen Angriffs, der mit E-Mail adressiert werden kann, um 99%, da Mimecast so effektiv ist, wie von den Befragten beschrieben.

Risiken. Diese Leistung kann je nach dem variieren:

- Die Wahrscheinlichkeit eines Verstoßes und die durchschnittlichen kumulativen Kosten von Verstößen. Dies kann je nach Branche, geografischer Lage, Größe des Unternehmens, früherem Umfeld und anderen Faktoren variieren.
- Die Ausgereiftheit und Effizienz von Lösungen und Prozessen in der vorherigen Umgebung eines Unternehmens.

Ergebnisse. Um diesen Risiken Rechnung zu tragen, hat Forrester diesen Nutzen um 15 % nach unten korrigiert. Daraus ergibt sich ein risikobereinigter Gesamt-PV für drei Jahre (abgezinst mit 10 %) von 1,1 Millionen US-Dollar.

99 %

Wirksamkeit von Mimecast bei Angriffen von außen

„Neunundneunzig Prozent der [bösartigen und unerwünschten E-Mails] werden auf Anhieb erkannt … Ich bin sicher, dass es sogar mehr als 99% sind.“

VP OF IT, BILDUNG

Verstärkte Sicherheit gegen bösartige E-Mails					
Ref.	**Metrisch**	**Quelle**	**Jahr 1**	**Jahr 2**	**Jahr 3**
A1	Wahrscheinlichkeit von einem oder mehreren Verstößen pro Jahr	Forrester's Sicherheitsstudie, 2023 Basis: 335	72%	72%	72%
A2	Mittlere kumulative Kosten für Verstöße	Forrester's Sicherheitsstudie, 2023 Basis: 237	$2,892,000	$2,892,000	$2,892,000
A3	Prozentsatz der Verstöße durch externe Angriffe	Forrester's Sicherheitsstudie, 2023 Basis: 830	49%	49%	49%
A4	Adressierbarer Anteil von externen Angriffen mit E-Mail	Forrester Forschung	50 %	50 %	50 %
A5	**Zwischensumme: Jährliches Risiko, das mit Mimecast adressiert werden kann**	**A1*A2*A3*A4**	**$511,190**	**$511,190**	**$511,190**
A6	Wirksamkeit von Mimecast bei Angriffen von außen	Interviews	99 %	99 %	99 %
Unter	Verstärkte Sicherheit gegen bösartige E-Mails	A5*A6	$506,078	$506,078	$506,078
	Risikoanpassung	↓15%			
Atr	Verbesserte Sicherheit gegen bösartige E-Mails (risikoadjustiert)		$430,166	$430,166	$430,166
	Drei Jahre insgesamt: $1.290.499			**Dreijähriger Barwert: $1.069.760**	

VERBESSERTE EFFIZIENZ DER SICHERHEITSMASSNAHMEN

Beweise und Daten. Die Befragten berichteten Forrester, wie Mimecast dazu beigetragen hat, die Effizienz der Sicherheits- und IT-Funktionen in ihren Unternehmen zu verbessern. Sie erklärten, wie die Automatisierung von Mimecast und die verstärkte Sicherheit vor bösartigen E-Mails Zeit bei der Überprüfung von E-Mails und der Abwehr von E-Mail-basierten externen Angriffen sparten. Die Mitglieder des Sicherheitsteams konnten diese Zeitersparnis nutzen, um sich anderen Risiken zu widmen. Die IT-Teams gaben an, dass die Integrationen und APIs, die Automatisierung und das allgemeine Design von Mimecast zu weniger Supportbedarf, weniger Verwaltungsaufgaben und allgemeinen Effizienzsteigerungen bei der E-Mail-Verwaltung führten, so dass die Teams mehr Zeit für höherwertige IT-Aufgaben aufwenden konnten.

- Der Sicherheitsmanager eines Unterhaltungsunternehmens sagte: „Wir müssen keine Zeit für E-Mail-Probleme aufwenden. Wenn wir das tun, ist es eine 5-minütige Überprüfung in Mimecast, und wir sind fertig. Der alte

Prozess wäre viel manueller gewesen und hätte sich darauf verlassen, dass der Benutzer informiert und meldet, dass die Mitarbeiter das Ticket aufheben, den Inhalt überprüfen, die E-Mail recherchieren und sie dann manuell zu einer Sperrliste hinzufügen.“ Sie fuhren fort: „Mimecast kümmert sich automatisch um die unteren Ebenen und überlässt es uns, uns um die höheren Ebenen zu kümmern. im Hintergrund, und alles, was es tun wird, ist, den Benutzer zu alarmieren.“

- Der Leiter des Infrastrukturbetriebs eines Unternehmens aus mehreren Branchen beschreibt, wie sein Team mit Mimecast an Produktivität gewonnen hat: „[Erstens] führt Mimecast proaktive Prüfungen in Bezug auf die Verfügbarkeit durch. Zweitens gibt es nicht viele E-Mail-Vorfälle, so dass Sie sich nicht mit P1- oder P2-Problemen herumschlagen müssen. ...Es gibt eine Menge Die Zeit, die wir bei administrativen Aufgaben einsparen, ist mit Mimecast viel einfacher als vorher.“

> „Wir haben [früher] viel Zeit mit der Verwaltung verbracht, aber nach einem Jahr Mimecast sehe ich nicht mehr viele Probleme. [Wir sind] komplett rationalisiert.“
>
> **IT-DIREKTOR, ANWENDUNGSVERWALTUNG, LEBENSMITTEL**

- Der SOC-Architekt einer Organisation des Gesundheitswesens stellte fest, wie die APIs und Integrationen von Mimecast zu mehr Effizienz führten: „[Mit den APIs von Mimecast] können unsere Analysten … direkt von der Quelle aus handeln, um Benutzer einzuschränken, Partner einzuschränken und Dateitypen zu ändern … All diese Vorgänge haben sich mit Mimecast vereinfacht. Wir haben eine Menge integriert, um meinen Kollegen das Leben zu erleichtern und ihre Zeit zu sparen. Wir haben auch gemeinsam genutzte Dienste, die z. B. nachts und an Wochenenden auf Vorfälle reagieren und die nicht unbedingt mit der Mimecast-Konsole selbst vertraut sind. Also abstrahieren [die Integrationen] all diese Ebenen der Komplexität."
- Der Sicherheitsmanager eines Unterhaltungsunternehmens erläuterte den Wert dieses Produktivitätsgewinns: „Wir sind ein technisches Unternehmen. Wir

machen Bleeding-Edge Entwicklung, und wir brauchen Zeit, um [unsere Entwickler] zu unterstützen und uns nicht um [E-Mail] zu kümmern.“

> „Wir sehen einen geringeren Bedarf an Zeit für unser Team [dank Mimecast].“
>
> **SICHERHEITSMANAGER, UNTERHALTUNG**

Modellierung und Annahmen. Auf der Grundlage der Interviews geht Forrester von den folgenden Annahmen über die zusammengesetzte Organisation aus:

- Die zusammengesetzte Organisation hat sieben Vollzeitbeschäftigte im Bereich Sicherheit, die sich um Sicherheitsvorfälle kümmern, und einen Vollzeitbeschäftigten im Bereich IT, der E-Mail-Plattformen verwaltet.
- Dank der Wirksamkeit von Mimecast bei externen Angriffen per E-Mail sparen die Sicherheits-FTEs Zeit bei der Bekämpfung von Angriffen per E-Mail.
- Das IT-FTE spart Zeit bei der Verwaltung von Mimecast im Vergleich zur vorherigen Umgebung des Unternehmens.
- Das voll belastete Jahresgehalt eines Sicherheitsanalysten liegt bei 141.750 Dollar und das voll belastete Jahresgehalt eines IT-Managers bei 125.688 Dollar.
- Fünfzig Prozent der Zeit, die beide Rollen einsparen, wird in produktive Arbeit umgewandelt.

Risiken. Diese Leistung kann je nach dem variieren:

- Die Zeit, die die Sicherheitsmitarbeiter eines Unternehmens bei E-Mail-basierten externen Angriffen einsparen, wenn man die Merkmale, die vorherige Umgebung und das Risikoprofil eines Unternehmens berücksichtigt.
- Die Anzahl der Teammitglieder, die mit dieser Arbeit beschäftigt sind, ihre Aufgaben und die damit verbundenen voll belasteten Jahresgehälter sowie die Fähigkeit der Teammitglieder, die eingesparte Zeit für produktive Arbeit zu verwenden.

Ergebnisse. Um diesen Risiken Rechnung zu tragen, passte Forrester diesen Nutzen um 10 % nach unten an, was einen risikobereinigten Gesamt-PV für drei Jahre (abgezinst mit 10 %) von 337.000 $ ergab.

50 %

Zeitersparnis bei der Verwaltung der E-Mail-Plattform dank Mimecast

„Der größte Teil [der Verwaltung unserer E-Mail-Plattform] kann in [Mimecast] in weniger als einem Viertel der Zeit erledigt werden, die wir [vorher] benötigten.“

VP OF IT, BILDUNG

Verbesserte Effizienz der Sicherheitsoperationen					
Ref.	**Metrisch**	**Quelle**	**Jahr 1**	**Jahr 2**	**Jahr 3**
B1	Sicherheitspersonal für die Verwaltung von Sicherheitsvorfällen	Komposit	7	7	7
B2	SecOps Zeitersparnis bei der Bekämpfung von E-Mail-basierten Angriffen dank Mimecast	A3*A4*A6	24 %	24 %	24 %
B3	Security Operations Analyst voll belastetes Gehalt	TEI-Standard	$141,750	$141,750	$141,750
B4	Produktivitätsrückgewinnungsrate	TEI-Standard	50 %	50 %	50 %
B5	**Zwischensumme: Vermiedene Kosten für die Untersuchung und Behebung von E-Mail-Vorfällen**	**B1*B2*B3*B4**	**$119,070**	**$119,070**	**$119,070**
B6	FTEs für die Verwaltung von E-Mails	Komposit	1	1	1
B7	Zeitersparnis bei der Verwaltung der E-Mail-Plattform dank Mimecast	Interviews	50 %	50 %	50 %
B8	IT-Manager voll belastetes Gehalt	TEI-Standard	$125,688	$125,688	$125,688
B9	Produktivitätsrückgewinnungsrate	TEI-Standard	50 %	50 %	50 %
B10	**Zwischensumme: Produktivitätssteigerung bei der E-Mail-Verwaltung**	**B6*B7*B8*B9**	**$31,422**	**$31,422**	**$31,422**
Bt	Verbesserte Effizienz der Sicherheitsmaßnahmen	B5+B10	$150,492	$150,492	$150,492
	Risikoanpassung	↓10%			
Btr	Verbesserte Effizienz der Sicherheitsoperationen (risikoadjustiert)		$135,443	$135,443	$135,443
	Drei Jahre insgesamt: $406.328			**Dreijähriger Barwert: $336.826**	

VERBESSERTE EFFIZIENZ DER ENDBENUTZER

Beweise und Daten. Neben der Verbesserung der Effizienz der Sicherheitsabläufe in ihren Unternehmen berichteten die Befragten Forrester auch, wie Mimecast die Effizienz der Endbenutzer verbessert hat. Die Befragten erklärten, dass die Endbenutzer weniger bösartige E-Mails erhalten und dadurch weniger Vorfälle erlebt haben, wodurch unproduktive Zeiträume vermieden wurden. Außerdem erhielten die Endbenutzer weniger unerwünschte E-Mails, was eine Zeitersparnis bei der E-Mail-Verwaltung ermöglichte. Die Befragten merkten auch an, dass die Endbenutzer mit Mimecast ihre E-Mails selbst freigeben konnten und dass sie mit Mimecast weniger Tickets einreichten, was für alle Beteiligten Zeit sparte. Für die Endbenutzer bedeutete diese Zeitersparnis, dass sie mehr Zeit für relevante geschäftsrelevante E-Mails oder andere produktive Arbeiten hatten.

- Der IT-Direktor der Anwendungsadministration eines Lebensmittelunternehmens sagte: „[Unsere Endbenutzer] haben die Möglichkeit, E-Mails zu veröffentlichen.

Sie brauchen kein Ticket zu erstellen.“ In diesem Zusammenhang sagte der Leiter des Infrastrukturbetriebs in einem Unternehmen aus mehreren Branchen: „Insgesamt haben wir unsere Tickets im Zusammenhang mit der E-Mail-Archivierung oder der Sicherheit um mehr als 50 bis 60 % reduziert.“

- Der VP der IT-Abteilung einer Bildungseinrichtung sagte: „Aus Sicht der Endbenutzer hat sich das E-Mail-Aufkommen um mindestens 40 % verringert. Wann auch immer sie sind 40 % der Zeit, die sie mit der Durchsicht ihres Posteingangs verbracht haben, haben sie zurückgewonnen.“

Modellierung und Annahmen. Auf der Grundlage der Interviews geht Forrester von den folgenden Annahmen über die zusammengesetzte Organisation aus:

- Die zusammengesetzte Organisation hat 48.987 Sicherheitsvorfälle pro Jahr.[13]
- Endbenutzer verlieren pro Vorfall 3,4 Stunden Produktivität aufgrund von E-Mail-Angriffen.[14]
- Dank der Wirksamkeit von Mimecast bei externen Angriffen per E-Mail vermeiden die Endbenutzer stundenlange Produktivitätsverluste.
- Der durchschnittliche, voll belastete Stundensatz für einen durchschnittlichen Endverbraucher beträgt $43,[15]
- Die Endbenutzer des Composites setzen 20% der eingesparten Zeit für produktive Arbeit ein.

Risiken. Diese Leistung kann je nach dem variieren:

- Die Anzahl der Sicherheitsvorfälle pro Jahr hängt von der Größe einer Organisation, ihrer Branche, ihrem Risikoprofil und anderen Faktoren ab.
- Der Umfang der verlorenen produktiven Zeit pro Endbenutzer.
- Der Anteil der Vorfälle, bei denen es sich um externe Angriffe handelt und/oder die mit E-Mail-Sicherheitslösungen angegangen werden können.
- Die voll belasteten Stundensätze der Endnutzer und ihre Fähigkeit, die eingesparte Zeit für produktive Arbeit zu nutzen.

Ergebnisse. Um diesen Risiken Rechnung zu tragen, passte Forrester diesen Nutzen um 15 % nach unten an, was einen risikobereinigten Gesamt-PV für drei Jahre (abgezinst mit 10 %) von 727.000 $ ergab.

24 %

Zeitersparnis für Endbenutzer bei spezifischen Angriffen per E-Mail

„Egal, ob es sich um Junk-Werbung oder um bösartige Werbung handelt, [Mimecast] stoppt sie … Jede einzelne dieser E-Mails bedeutet [Zeit].“

SICHERHEITSMANAGER, UNTERHALTUNG

Verbesserte Effizienz der Endbenutzer					
Ref.	**Metrisch**	**Quelle**	**Jahr 1**	**Jahr 2**	**Jahr 3**
C1	Sicherheitsvorfälle in der zusammengesetzten Organisation pro Jahr	Kundenspezifische Forschung von Forrester	48,987	48,987	48,987
C2	Verlorene Produktivität der Endbenutzer pro Jahr und Vorfall aufgrund von E-Mail-Angriffen (Stunden)	Kundenspezifische Forschung von Forrester	3.4	3.4	3.4
C3	Zeitersparnis bei gezielten Angriffen per E-Mail	A3*A4*A6	24 %	24 %	24 %
C4	Durchschnittliche Kosten pro Stunde für den Endverbraucher bei voller Belastung	US Bureau of Labor Statistics, Dezember 2023	$43	$43	$43
C5	Produktivitätsrückgewinnungsrate	TEI-Standard	20 %	20 %	20 %
Ct	Verbesserte Effizienz der Endbenutzer	C1*C2*C3*C4*C5	$343,771	$343,771	$343,771
	Risikoanpassung	↓15%			
Ctr	Verbesserte Effizienz der Endverbraucher (risikoangepasst)		$292,205	$292,205	$292,205
	Drei Jahre insgesamt: $876.616		**Dreijähriger Barwert: 726.671 $**		

NICHT BEZIFFERTE VORTEILE

Die Befragten erwähnten die folgenden zusätzlichen Vorteile, die ihre Organisationen erfahren haben, die sie aber nicht quantifizieren konnten:

- **Geschäftliche Vorteile, einschließlich Schutz des Rufs.** Angetrieben von der verbesserten Sicherheit und dem Funktionsumfang von Mimecast, einschließlich DMARC Analyzer, erzählten die Befragten Forrester von umfassenderen geschäftlichen Vorteilen, einschließlich des Schutzes der Marke und des Rufs, auch wenn sie den Wert nicht quantifizieren konnten. Insgesamt trägt die Cybersicherheit dazu bei, dass die Unternehmen in der Lage sind, Einnahmen zu generieren.[16] Der IT-Direktor für die Anwendungsadministration eines Lebensmittelunternehmens erklärte: „Wenn jemand eine E-Mail mit unserem Namen verschickt, ist das ein Reputationsproblem.“ Er fügte hinzu: „[Mimecast] schützt unsere Marke, indem es diese E-Mail nicht versendet, da wir mit Millionen von Kunden interagieren. Es gibt uns den Ruf, unsere ausgehenden E-Mails zu schützen.“

  Der SOC-Architekt einer Organisation des Gesundheitswesens erklärte die Vorteile von DMARC und BIMI für das Kundenvertrauen: „Dank Mimecast haben wir DMARC und BIMI [Brand Indicators for Message Identification] implementiert … [das verifizierte Logo oder die Grafik von BIMI] veranlasst unsere Kunden dazu, mehr E-Mails zu öffnen.“[17]

- **Mimecast Dienstleistungen, Support und Kundenerfahrung.** Die Befragten hoben den Wert der professionellen und verwalteten Dienste von Mimecast, die Supportangebote und das Engagement für die Kundenerfahrung hervor. Der SOC-Architekt einer Organisation im Gesundheitswesen sagte: „Sie hören auf unser Feedback.“ Der Sicherheitsmanager eines Unterhaltungsunternehmens sagte: „Der Support ist gut. Sie müssen sicherstellen, dass Sie sie nutzen.“ Der IT-Administrator eines Gesundheitsunternehmens fügte hinzu: „Sie haben sich beim Kundenservice sehr viel Mühe gegeben.“

> „[Mimecasts] Support ist ausgezeichnet. Sie sind jederzeit bereit, sich um alles zu kümmern. “
>
> IT-DIREKTOR, ANWENDUNGSVERWALTUNG, LEBENSMITTEL

FLEXIBILITÄT

Der Wert der Flexibilität ist für jeden Kunden einzigartig. Es gibt mehrere Szenarien, in denen ein Kunde Mimecast implementieren und später zusätzliche Nutzungs- und Geschäftsmöglichkeiten realisieren kann, darunter

- **Höhere Sicherheitseffizienz bei allen Produkten durch den Austausch von Bedrohungen.** Die Befragten sprachen nicht nur über verstärkte Sicherheit, sondern beschrieben auch die Nutzung der APIs und Integrationen von Mimecast, um Bedrohungswissen zwischen Mimecast und anderen Sicherheitslösungen auszutauschen. Die Befragten gaben an, dass ihre Unternehmen durch den einfachen Austausch von Daten zwischen den Lösungen eine höhere Sicherheitseffizienz erzielen können als durch den Einsatz von Einzellösungen, wodurch das Risiko weiter reduziert und gleichzeitig ein größerer Nutzen aus allen Sicherheitsinvestitionen gezogen wird. Neben der gesteigerten Effektivität könnten die Integrationen von Mimecast auch die Effizienz der verschiedenen Lösungen erhöhen.

> „Ich speise Informationen oder Warnungen von Mimecast in meine Sicherheits- und SIEM-Lösung ein und umgekehrt, so dass meine SIEM-Lösung die von Mimecast kommenden Informationen sehen und verwenden kann, wenn sie entscheidet, ob eine Aktivität bösartig ist.“
>
> SICHERHEITSMANAGER, UNTERHALTUNG

- **Erweiterte Funktionen zum Schutz von Menschen und Daten.** Die Befragten erzählten Forrester, wie ihre Unternehmen neben dem Schutz von E-Mail und Zusammenarbeit auch menschliche Risiken mindern und Daten schützen können.

  Der Einsatz von Mimecast als Plattform für die Informationsarchivierung mit Email Archive half den befragten Unternehmen, E-Mail-Daten langfristig zu bewahren und die Effizienz bei der Durchführung von E-Discovery und anderen Untersuchungen zu steigern.[18] Für E-Discovery berichtete der VP der IT-Abteilung einer Bildungseinrichtung: „Was für eine einzelne Person 4 bis 6 Stunden gedauert hätte, können wir in 15 Minuten erledigen.“ Der SOC-Architekt einer Organisation des Gesundheitswesens sagte: „Mit Mimecast können wir die Nachrichten und Postfächer der Endbenutzer viel schneller abrufen.“ Der IT-Direktor für die Anwendungsadministration in einem Lebensmittelunternehmen stellte fest: „Ich habe einen starken Schutz, dass niemand ohne meine Zustimmung E-Mails löscht.“

  Die Befragten sprachen auch über den Einsatz von Mimecast als Human Risk Management (HRM) Lösung mit Security Awareness Training. HRM-Lösungen können Unternehmen dabei helfen, menschliches Sicherheitsverhalten und die damit verbundenen Risiken zu erkennen, Menschen in großem Umfang zu schützen und das menschliche Risiko in das gesamte Cyber-Risiko einzubeziehen und dabei Silos aufzubrechen.[19] Der Vizepräsident der IT-Abteilung einer Bildungseinrichtung sagte: „Das Cyber-Bewusstsein war ein großer Vorteil.“ Und weiter: „Diejenigen, die an den Schulungen teilgenommen haben, haben sehr positives Feedback erhalten und bestätigt, dass sie einige ihrer Verhaltensweisen aufgrund dieser Schulungen geändert haben.“

- **Die Fähigkeit, schnell zu skalieren.** Die Befragten aus Organisationen, die von kleinen Unternehmen bis hin zu Großkonzernen reichen, äußerten sich zuversichtlich über die Fähigkeit von Mimecast, mit dem Wachstum ihrer Organisationen mitzuwachsen, unabhängig von der Bereitstellungsmethode. Der IT-Administrator eines Gesundheitsunternehmens erklärte, dass er mit dem Wachstum seines Unternehmens in der Lage sein wird, „so viele Mitarbeiter in [Mimecast] einzubinden, wie nötig sind“.

Die Flexibilität würde auch quantifiziert werden, wenn sie im Rahmen eines spezifischen Projekts bewertet wird (ausführlicher beschrieben in Anhang A).

> „[Mimecast] lässt sich leicht skalieren.“
>
> SICHERHEITSMANAGER, UNTERHALTUNG

Analyse der Kosten

Quantifizierte Kostendaten, die auf den Verbundstoff angewendet werden

Gesamtkosten							
Ref.	**Kosten**	**Ursprünglich**	**Jahr 1**	**Jahr 2**	**Jahr 3**	**Gesamt**	**Barwert**
Dtr	Lizenzierung	$1,650	$175,533	$175,533	$175,533	$528,248	$438,173
Etr	Implementierung, Schulung und laufende Verwaltung	$6,732	$63,015	$63,015	$63,015	$195,776	$163,440
	Gesamtkosten (risikoadjustiert)	$8,382	$238,547	$238,547	$238,547	$724,023	$601,613

LIZENZIERUNG

Beweise und Daten. Die Hauptkosten für die befragten Organisationen waren die Gebühren für Mimecast. Sie basierten auf der Anzahl der Benutzer und den Kosten pro Benutzer des ausgewählten Plans, zusätzlich zu den erworbenen Add-ons, professionellen oder verwalteten Diensten und dem Support.

Modellierung und Annahmen. Auf der Grundlage der Interviews geht Forrester von den folgenden Annahmen über die zusammengesetzte Organisation aus:

- Das Verbundunternehmen wählt den Comprehensive Defense Plan von Mimecast für seine 2.500 Benutzer.
- Es erwirbt zunächst einen Guided Implementation Service und kauft dann Advanced Support für alle drei Jahre.

Risiken. Diese Kosten können je nach dem variieren:

- Die Anzahl der Benutzer, die ein Unternehmen mit Mimecast schützen möchte.
- Der ausgewählte Plan und die damit verbundenen Kosten pro Benutzer.
- Die Add-Ons, Services und Supportleistungen, die ein Unternehmen erwirbt.
- Die Preise können variieren. Kontaktieren Sie Mimecast für weitere Details.

Ergebnisse. Um diesen Risiken Rechnung zu tragen, passte Forrester diese Kosten um 10 % nach oben an, was einen risikobereinigten Gesamt-PV für drei Jahre (abgezinst mit 10 %) von 438.000 $ ergab.

> „[Der Support von Mimecast] ist von hervorragendem Wert.“
>
> INFRASTRUKTURMANAGER, UNTERHALTUNG

Lizenzierung						
Ref.	**Metrisch**	**Quelle**	**Ursprünglich**	**Jahr 1**	**Jahr 2**	**Jahr 3**
D1	Lizenzierung	Mimecast	$1,500	$159,575	$159,575	$159,575
Dt	Lizenzierung	D1	$1,500	$159,575	$159,575	$159,575
	Risikoanpassung	↑10%				
Dtr	Lizenzierung (risikoadjustiert)		$1,650	$175,533	$175,533	$175,533
	Drei Jahre insgesamt: $528.248		**Dreijähriger Gegenwartswert: $438.173**			

IMPLEMENTIERUNG, SCHULUNG UND LAUFENDE VERWALTUNG

Beweise und Daten. Einige Befragte gaben an, dass ihre Unternehmen Mimecast mit der Bereitstellungsmethode Email Security Cloud Integrated in nur einem Tag oder einer Woche implementieren konnten. Die Dauer der Implementierung hing von der Größe und Komplexität des Unternehmens, den vorherigen Zuständen, den gewählten Bereitstellungsmethoden und den erworbenen Add-ons ab. Andere Befragte, darunter auch diejenigen, die die Bereitstellungsmethode Email Security Cloud Gateway verwenden, beschrieben mehrmonatige Proofs of Concept (POCs) und Anlaufphasen, in denen ihre Unternehmen Domänen und Benutzergruppen methodisch migrierten. Unabhängig von der Größe und Komplexität des Unternehmens beschrieben die

Befragten die Der Implementierungsprozess verlief reibungslos und einfach, insbesondere dank des Supports und der Dienstleistungen von Mimecast.

Nach der Implementierung sagten die Befragten, der laufende Arbeitsaufwand sei minimal. Sie diskutierten über Schulungen, Planungssitzungen mit Mimecast und die allgemeine Verwaltung, die auch die Fehlerbehebung und die Verwaltung von Bedrohungen und Richtlinien umfassen könnte.

Modellierung und Annahmen. Auf der Grundlage der Interviews geht Forrester von den folgenden Annahmen über die zusammengesetzte Organisation aus:

- Die zusammengesetzte Organisation plant zunächst 90 Stunden für die Implementierung von Mimecast, die Schulung des Teams und die Erstellung von Schulungsunterlagen für die Endbenutzer ein.
- Nach der Implementierung benötigt das Team des Verbundunternehmens im Durchschnitt 1 Stunde pro Woche für die Mimecast-Administration, die Verwaltung von Bedrohungen und Richtlinien, laufende Schulungen, Fehlerbehebung und Planung.
- Das zusammengesetzte Unternehmen entscheidet sich dafür, seine Endbenutzer über die besten Praktiken zur E-Mail-Sicherheit aufzuklären. Sie beträgt durchschnittlich 30 Minuten pro Benutzer und Jahr.
- Der durchschnittliche Stundensatz für einen Security Operations Analysten beträgt $68.
- Der durchschnittliche, voll belastete Stundensatz für einen Endbenutzer beträgt $43.

Risiken. Diese Kosten können je nach dem variieren:

- Die Dauer der Implementierung, die involvierten Aktivitäten, die benötigten Stunden, die Anzahl der beteiligten Teammitglieder und die damit verbundenen Rollen und voll belasteten Stundensätze dieser Teammitglieder.
- Die Aktivitäten, die ein Unternehmen nach der Implementierung durchführt, die für diese Aktivitäten benötigten Stunden, die Anzahl der benötigten Teammitglieder und die damit verbundenen Rollen und Stundensätze dieser Teammitglieder.

Ergebnisse. Um diesen Risiken Rechnung zu tragen, passte Forrester diese Kosten um 10 % nach oben an, was einen risikobereinigten Gesamt-PV für drei Jahre (abgezinst mit 10 %) von 163.440 $ ergab.

„[Die Implementierung von Mimecast] war ein sehr reibungsloser Prozess.“

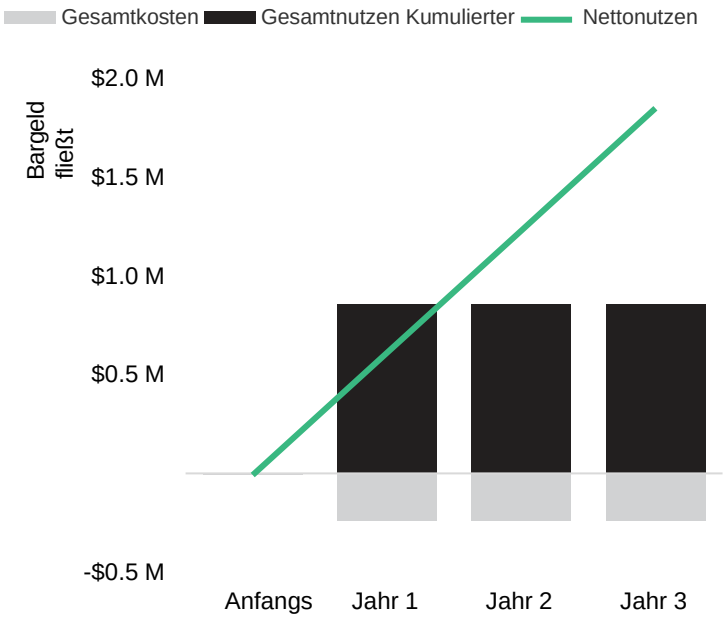
IT-DIREKTOR, ANWENDUNGSVERWALTUNG, LEBENSMITTEL

Implementierung, Schulung und fortlaufende Verwaltung						
Ref.	**Metrisch**	**Quelle**	**Ursprünglich**	**Jahr 1**	**Jahr 2**	**Jahr 3**
E1	Implementierung und Einführungsschulung (Stunden)	Interviews	90	0	0	0
E2	Administration, Verwaltung von Bedrohungen und Richtlinien, fortlaufende Schulungen, Fehlerbehebung und Planung (Stunden)	Interviews	0	52	52	52
E3	Schulung und Ausbildung von Endbenutzern zu bewährten Verfahren (Stunden)	Komposit	0	1,250	1,250	1,250
E4	Kosten pro Stunde für einen voll ausgelasteten Analysten für Sicherheitsoperationen	TEI-Standard	$68	$68	$68	$68
E5	Durchschnittliche Kosten pro Stunde für den Endverbraucher bei voller Belastung	C4	$43	$43	$43	$43
Et	Implementierung, Schulung und laufende Verwaltung	((E1+E2)*E4) +(E3*E5)	$6,120	$57,286	$57,286	$57,286
	Risikoanpassung	↑10%				
Etr	Implementierung, Schulung und laufende Verwaltung (risikoadjustiert)		$6,732	$63,015	$63,015	$63,015
	Drei Jahre insgesamt: $195.776		**Dreijähriger Gegenwartswert: $163.440**			

Finanzielle Zusammenfassung

Konsolidierte dreijährige, risikobereinigte Metriken

Cashflow-Diagramm (risikoadjustiert)



Die in den Abschnitten Nutzen und Kosten berechneten finanziellen Ergebnisse können verwendet werden, um den ROI, den NPV und die Amortisationsdauer für die Investition des zusammengesetzten Unternehmens zu bestimmen. Forrester geht bei dieser Analyse von einem jährlichen Diskontsatz von 10% aus.

Diese risikobereinigten ROI-, NPV- und Amortisationszeitwerte werden durch Anwendung von Risikoanpassungsfaktoren auf die unbereinigten Ergebnisse in jedem Nutzen- und Kostenabschnitt ermittelt.

Cash Flow Analyse (risikoadjustiert)

	Ursprünglich	Jahr 1	Jahr 2	Jahr 3	Gesamt	Barwert
Gesamtkosten	($8,382)	($238,547)	($238,547)	($238,547)	($724,023)	($601,613)
Vorteile insgesamt	$0	$857,814	$857,814	$857,814	$2,573,443	$2,133,257
Netto Nutzen	($8,382)	$619,267	$619,267	$619,267	$1,849,420	$1,531,644
ROI						255%

ANHANG A: GESAMTWIRTSCHAFTLICHE AUSWIRKUNGEN

Total Economic Impact ist eine von Forrester Research entwickelte Methode, die die technologischen Entscheidungsprozesse von Unternehmen verbessert und Anbietern dabei hilft, ihren Kunden das Wertversprechen ihrer Produkte und Dienstleistungen zu vermitteln. Die TEI-Methode hilft Unternehmen dabei, den greifbaren Wert von IT-Initiativen sowohl gegenüber der Geschäftsleitung als auch gegenüber anderen wichtigen Geschäftsinteressenten zu demonstrieren, zu rechtfertigen und zu realisieren.

Ansatz der wirtschaftlichen Gesamtauswirkungen

Der Nutzen ist der Wert, den das Produkt für das Unternehmen hat. Die TEI-Methode gewichtet die Messung des Nutzens und die Messung der Kosten gleich, so dass die Auswirkungen der Technologie auf die gesamte Organisation umfassend untersucht werden können.

Die Kosten berücksichtigen alle Ausgaben, die notwendig sind, um den vorgeschlagenen Wert oder Nutzen des Produkts zu erzielen. Die Kostenkategorie innerhalb der TEI erfasst die Mehrkosten gegenüber der bestehenden Umgebung für die mit der Lösung verbundenen laufenden Kosten.

Die Flexibilität stellt den strategischen Wert dar, der für einige zukünftige zusätzliche Investitionen, die auf den bereits getätigten Anfangsinvestitionen aufbauen, erzielt werden kann. Die Fähigkeit, diesen Nutzen zu erfassen, hat einen schätzbaren Wert.

Risiken messen die Unsicherheit von Nutzen- und Kostenschätzungen, die gegeben sind: 1) die Wahrscheinlichkeit, dass die Schätzungen den ursprünglichen Projektionen entsprechen und 2) die Wahrscheinlichkeit, dass die Schätzungen im Laufe der Zeit verfolgt werden. Die TEI-Risikofaktoren basieren auf einer "Dreiecksverteilung".

Barwert (PV)

Der gegenwärtige oder aktuelle Wert von (diskontierten) Kosten- und Nutzenschätzungen, die mit einem Zinssatz (dem Diskontsatz) angegeben werden. Die PV von Kosten und Nutzen fließen in den Gesamtbarwert der Cashflows ein.

Nettogegenwartswert (NPV)

Der gegenwärtige oder aktuelle Wert der (abgezinsten) zukünftigen Netto-Cashflows unter Berücksichtigung eines Zinssatzes (des Diskontsatzes). Ein positiver Kapitalwert des Projekts bedeutet normalerweise, dass die Investition getätigt werden sollte, es sei denn, andere Projekte haben einen höheren Kapitalwert.

Rentabilität der Investition (ROI)

Die erwartete Rendite eines Projekts in Prozent. Der ROI wird berechnet, indem der Nettonutzen (Nutzen abzüglich Kosten) durch die Kosten geteilt wird.

Diskontsatz

Der in der Cashflow-Analyse verwendete Zinssatz, um den Zeitwert des Geldes zu berücksichtigen. Unternehmen verwenden in der Regel Abzinsungssätze zwischen 8% und 16%.

Amortisationsdauer

Der Break-even-Punkt für eine Investition. Dies ist der Zeitpunkt, an dem der Nettonutzen (Nutzen minus Kosten) den ursprünglichen Investitionen oder Kosten entspricht.

Die Spalte Erstinvestition enthält Kosten, die zum „Zeitpunkt 0“ oder zu Beginn von Jahr 1 anfallen und nicht abgezinst werden. Alle anderen Cashflows werden mit dem Abzinsungssatz am Ende des Jahres abgezinst. PV-Berechnungen werden für jede Gesamtkosten- und Nutzenschätzung berechnet. Die NPV-Berechnungen in den Übersichtstabellen sind die Summe der Anfangsinvestition und der diskontierten Cashflows in jedem Jahr. Die Summen und Barwertberechnungen der Tabellen Gesamtnutzen, Gesamtkosten und Cashflow addieren sich möglicherweise nicht genau, da es zu Rundungen kommen kann.

ANHANG B: ERGÄNZENDES MATERIAL

Verwandte Forrester-Forschung

What 2023's Most Notable Breaches Mean For Tech Execs, Forrester Research, Inc., May 31, 2024

Zusammenarbeit mit Sicherheit To Select Trustworthy Tech, Forrester Research, Inc., 1. März 2024

Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 2023, Forrester Research, Inc., Februar 28, 2024

The Tech Exec's Guide To The Top Cyberthreats, 2023, Forrester Research, Inc., November 28, 2023

The Forrester Wave™ : Security Awareness And Training Solutions, Q1 2022, Forrester Research, Inc., 16. März, 2022

The Business Case For Privacy And Data Protection, Forrester Research, Inc., August 2, 2021

ANHANG C: ENDNOTEN

[1] Quelle: Top Cybersecurity Threats In 2024, Forrester Research, Inc., April 5, 2024.

[2] Quelle: The Enterprise Email Security Landscape, Q1 2023, Forrester Research, Inc., 3. Februar, 2023.

[3] Quelle: The Forrester Wave™ : Enterprise Email Security, Q2 2023, Forrester Research, Inc., 12. Juni 2023.

[4] Quelle: The CISO's Guide To Microsoft Investments, Forrester Research, Inc., September 28, 2023.

[5] Total Economic Impact (TEI) ist eine von Forrester Research entwickelte Methode, die die technologischen Entscheidungsprozesse von Unternehmen verbessert und Anbietern dabei hilft, ihren Kunden das Wertversprechen ihrer Produkte und Dienstleistungen zu vermitteln. Die TEI-Methode hilft Unternehmen, den greifbaren Wert von IT-Initiativen gegenüber der Geschäftsleitung und anderen wichtigen Geschäftsinteressenten zu demonstrieren, zu rechtfertigen und zu realisieren.

[6] Quelle: Forrester Glossar, Forrester Research, Inc.

[7] Quelle: Now Tech: Unternehmen E-Mail Sicherheit Anbieter, Q3 2020, Forrester Research, Inc., 14. Juli 2020

[8] Ebd.

[9] Ebd.

[10] Quelle: Security Survey, 2023, Forrester Research, Inc., Oktober 2023.

[11] Ebd.

[12] Ebd.

[13] Quelle: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021.

[14] Ebd.

[15] Quelle: US Bureau of Labor Statistics, Dezember 2023

[16] Quelle: Top Recommendations For Your Security Program, 2024, Forrester Research, Inc., March 4, 2024.

[17] Quelle: Bolster Brand Resilience With DMARC, Forrester Research, Inc., August 27, 2021; Jess Burn, Apple's BIMI Support = Time To Get Serious About DMARC Enforcement, Forrester Blogs, September 19, 2022.

[18] Quelle: The Information Archiving Platforms Landscape, Q2 2024, Forrester Research, Inc., April 3, 2024.

[19] Quelle: The Human Risk Management Solutions Landscape, Q1 2024, Forrester Research, Inc., 18. März, 2024.

FORRESTER®