**Cybersecurity-Prognosen 2024**  
**Das erwarten die Experten von Mimecast für das kommende Jahr**

* *Bei Angriffen werden mehr KI-basierte Tools zum Einsatz kommen.*
* *Angreifer werden verstärkt die großen Hyperscaler ins Visier nehmen.*
* *Die Quanteninformatik birgt neue Risiken, im Besonderen den Diebstahl von Daten „auf Vorrat“ mit dem Ziel der späteren Entschlüsselung mit den Quantenrechnern der Zukunft.*
* *Die Kompromittierung geschäftlicher E-Mails wird weiter zunehmen, und Hacker können dank neuer Technologien immer perfektere Täuschungen schaffen (etwa durch Sprach- und Video-Imitationen von Personen, denen Nutzer vertrauen).*

**MÜNCHEN, 11. Dezember 2023** – [**Mimecast Limited**](https://www.mimecast.com/) (Mimecast) stellte heute seine Prognosen für das Jahr 2024 vor:

**Die wichtigsten Mimecast-Prognosen für 2024 im Überblick**

1. Bei Angriffen werden mehr KI-basierte Tools zum Einsatz kommen.
2. Durch neue KI-Produkte wird es zu einer Zunahme von Datenschutzverletzungen kommen.
3. Unternehmen werden verstärkt Cybersicherheitsdienste als Managed Service in Anspruch nehmen.
4. Marketplace-Modelle sind auf dem Vormarsch.
5. Cybersicherheitsspezialisten werden auf eine effektivere Risikoquantifizierung hinarbeiten.
6. Angreifer werden verstärkt die großen Hyperscaler ins Visier nehmen.
7. Integrierte Cloud-E-Mail-Sicherheitslösungen (ICES) wie Mimecast Cloud Integrated Email Security werden weiter reifen und – als Reaktion auf die wachsenden Bedrohungen – Software-Suites wie Microsoft 365 eine zusätzliche Sicherheitsebene hinzufügen.
8. Die aufkommende Quanteninformatik bietet große Chancen, birgt aber auch neue Risiken, im Besonderen den Diebstahl von Daten „auf Vorrat“ mit dem Ziel der späteren Entschlüsselung mit den Quantenrechnern der Zukunft. Deshalb ist es so wichtig, Daten bereits heute durch quantensichere Kryptografie zu schützen.
9. Die Kompromittierung geschäftlicher E-Mails wird weiter zunehmen, und Hacker können dank neuer Technologien immer perfektere Täuschungen schaffen (etwa durch Sprach- und Video-Imitationen von Personen, denen Nutzer vertrauen).

**Die Prognosen der Mimecast-Experten für 2024 im Detail**

**Name:** Robin Moore

**Titel:** Principal Product Manager, AI & Machine Learning

**Prognose 1**

Als Folge von Joe Bidens Executive Order über sichere und vertrauenswürdige KI und als Reaktion auf den bevorstehenden EU AI Act werden wir im Jahr 2024 eine Vielzahl von Tools, Lösungen und Produkten sehen, die diese Verordnungen adressieren und Unternehmen helfen, ihre Vorgaben einzuhalten. Ich gehe davon aus, dass sich diese Produkt- und Lösungspalette zu einem eigenständigen Bereich des Sicherheitsmarktes entwickeln wird, der auf die sichere Nutzung von maschinellem Lernen und KI abzielt. Unternehmen wie Harmonic, Lakera und einige andere sind Vorreiter dieser Entwicklung.

**Prognose 2**

Wir werden vermutlich erleben, dass immer mehr Tools auf Basis generativer KI eingesetzt werden, um immer raffiniertere und vor allem automatisierte Angriffe gegen Unternehmen und Einzelpersonen durchzuführen. Cyberkriminelle können mit weniger Aufwand hochwertigere und individualisierte Erstkontaktversuche unternehmen. Auch die anschließende Interaktion, die das Ziel hat, dass das Opfer bestimmte Informationen liefert oder die vom Angreifer gewünschten Aktionen durchführt, kann mit Hilfe generativer, KI-gestützte Chatbots automatisiert werden. Die Angreifer sparen Zeit und können so den Umfang ihrer Attacken deutlich erhöhen.

**Name:** Stan de Boisset

**Titel:** Senior Vice President WW Partners

**Prognose 1**  
Gerade KMU werden Cybersecurity-Dienste verstärkt als Managed Service (MSP, MSSP) in Anspruch nehmen.

**Prognose 2**  
Das Aufkommen neuer Cybersecurity-Angebote und deren Nutzung über Marktplätze wird zu einer stärkeren Verbreitung von Marktplatzmodellen führen.

**Name:** Francis Gaffney

**Titel:** Senior Director, Threat Intelligence Engineering

**Prognosen**

1. Kompromittierung der Lieferkette von Software-Abhängigkeiten durch:
   1. Fortgeschrittene Mal-/Desinformationskampagnen
   2. Menschliches Versagen
   3. Ausgelastete Altsysteme in cyberphysischen Architekturen
   4. Qualifikationsdefizite
   5. Missbrauch von künstlicher Intelligenz
   6. Kollaborationstools
   7. Insider-Bedrohungen
2. „Traditionelle“ Sicherheitsstrategien werden nicht ausreichen, um die nötige Anpassungsfähigkeit von Unternehmen aufzubauen und aufrechtzuerhalten.
3. Schatten-IT, Altsysteme, Fusionen und Übernahmen sowie „Bring your own device“ (BYOD) verschärfen das Risiko, da hybrides Arbeiten zur Normalität wird.
4. Das zunehmende Risikobewusstsein wird zu einer Zunahme der Gesetzgebung und der regulatorischen Aktivitäten führen, insbesondere auf den Versicherungsmärkten.
5. Angriffe über Dritte bzw. Lieferketten werden in ihrer Häufigkeit und ihren Auswirkungen weiter zunehmen.
6. Zunahme von Access Brokerage als Angriffsmethode.
7. Verstärkter Einsatz von KI/MI bei der Entwicklung von Angriffsmethoden.
8. Ransomware-Attacken werden weiter stark vertreten sein.
9. Das Security Stacking von mehreren Technologien wird ausgenutzt, während zugleich Konfigurationskonflikte bestehen.
10. Ausgefeiltes Spear Phishing/Whaling (über Pattern of Life-Analyse).
11. Versuche, Daten während der Übertragung abzufangen, werden zunehmen.
12. Zunahme von Malware-as-a-Service.

**Name:** Neil Clauson

**Titel:** Regional CISO

**Prognose**

Cybersicherheitsverantwortliche werden sich weiterhin um eine effektivere Risikoquantifizierung bemühen. Denn es gilt: Cyberrisiko = Finanzielles Risiko = Geschäftsrisiko.

**Name:** James Lee

**Titel:** Vice President, Partners EMEA

**Prognose**

Bad guys 1, Hyperscaler 0: In dem Maß, in dem sich der Markt um die Hyperscaler konsolidiert, konzentrieren sich die Angreifer auf diese Infrastruktur. Jüngste Beispiele von rekordverdächtigen DDOS-Angriffen gegen Azure und andere zeigen, dass die bisherigen „gebündelten“ Sicherheitsfunktionen vieler dieser Anbieter möglicherweise nicht ausreichen. 2024 ist das Jahr, in dem integrierte Cloud-E-Mail-Sicherheitslösungen (ICES) wie Mimecast Cloud Integrated Email Security als zusätzliche Sicherheitsebene in Software-Suites wie Microsoft 365 als Reaktion auf die Bedrohung an Bedeutung gewinnen werden.

**Name:** Jonathan Miles

**Titel:** Principal Threat Response Analyst

**Prognose 1**

Ich bin der Meinung, dass Sicherheitsteams die Bedrohungen der nächsten zwölf Monate antizipieren müssen. Ebenso müssen sie jetzt damit anfangen, die nächsten drei bis fünf Jahre mitzudenken. Ein vorausschauender und proaktiver Ansatz zu Risikoerkennung, -management und -minderung ist kosteneffizienter. Gleichzeitig müssen Unternehmen flexibel genug bleiben, um auf dynamische Cyberrisiken zu reagieren und an dieser Stelle investieren.

**Prognose 2**Risikomanagement-Konzepte sollten in Arbeitsabläufen und Ethos von Unternehmen verankert werden. Bei der Ausrichtung des Risikomanagements auf die strategische Ausrichtung und die Unternehmensführung kann das Risikomanagement sowohl intern als auch extern als eine Notwendigkeit für die Widerstandsfähigkeit eines Unternehmens angesehen werden. Wenn Unternehmen die Risiken kennen und zudem wissen, woher sie kommen könnten und welche Kontrollen erforderlich sind, können sie sie einfacher begrenzen und sich durch Vorbereitung ein gewisses Maß an Resilienz aneignen.

**Prognose 3**Die Zukunft bietet viele Unbekannte. Unternehmen können sich zwar darauf vorbereiten, mit diesen Variablen oder Risiken umzugehen und sie zu bewältigen. Es wird aber unweigerlich Risiken geben, die nicht bewältigt oder gemildert werden können und sich zu Zwischenfällen oder schlimmstenfalls zu Krisen auswachsen.

**Prognose 4**Das Aufkommen von Quantencomputern ist ein bedeutender Wendepunkt. Das Aufkommen der Quanteninformatik im großen Maßstab verspricht eine noch nie dagewesene Geschwindigkeit und Leistung in der Datenverarbeitung und bietet damit enorme Chancen, birgt aber zugleich erhebliche neue Risiken für die derzeitige globale Informationsinfrastruktur. Diese Technologie wird im Lauf des nächsten Jahrzehnts Verschlüsselungsmethoden knacken können, die weithin zum Schutz von Kundendaten, zur Abwicklung von Geschäftstransaktionen und zur Sicherung der Kommunikation eingesetzt werden. Es wird nicht mehr möglich sein, die Integrität und Authentizität übermittelter Informationen zu garantieren, da kompromittierte Daten unentdeckt bleiben könnten: Auch wenn bereits mit Hochdruck an quantensicheren Algorithmen gearbeitet wird, stehlen Hacker zum Teil auch heute verschlüsselte Daten „auf Vorrat“, um sie mit der Computerleistung der Zukunft zu entschlüsseln. Das macht die Aufgabe, unsere Daten JETZT durch quantensichere Kryptografie zu schützen, noch dringlicher.

**Name:** Kiri Addison

**Titel:** Product Manager – Detection, Efficacy and Data Science

**Prognose**

Durch die Übermittlung sensibler Daten an generative KI-Tools wird es zu einer Zunahme von Datenschutzverletzungen kommen.

**Name:** Peter Bauer   
**Titel:** CEO

**Prognose**

Meine Cybersecurity-Prognose für 2024 lautet, dass Angriffe auf geschäftliche E-Mails, bei denen es sich oft um eine Interaktion zwischen einem Angreifer und einem unwissenden Mitarbeiter handelt, noch überzeugender werden, indem sie sowohl Sprach- als auch Video-Imitationen von Personen verwenden, denen die Opfer sonst vertrauen.

**ÜBER MIMECAST**

Mimecast: Work Protected™ Seit 2003 verhindert Mimecast, dass guten Unternehmen Schlimmes widerfährt, indem es ihnen ermöglicht, geschützt zu arbeiten. Wir ermöglichen es über 40.000 Kund:innen, Risiken zu minimieren und die Komplexität einer Bedrohungslandschaft zu bewältigen, die von bösartigen Cyberangriffen, menschlichem Versagen und technologischen Fehlern geprägt ist. Mimecast bringt Email- und Collaboration Security auf das nächste Level.

**PRESSEKONTAKT**

Bernd Hohlweg  
Director Marketing, DACH  
E-Mail: [**bhohlweg@mimecast.com**](mailto:bhohlweg@mimecast.com)  
Telefon: +49 (0)160 91935437

Franziska Kast  
Senior Manager, Media Relations  
E-Mail: [**FKast@webershandwick.com**](mailto:FKast@webershandwick.com)  
Telefon: +49 (0)30 20351247