mimecast

# Kostspielige Ransomware-Angriffe auf Collaboration-Tools: Eine effektive Abwehr

WHITEPAPER

Um Ransomware-Angriffe erfolgreich abzuwehren, müssen Sicherheitsverantwortliche ein Framework einführen, mit dem sie die Vorgehensweisen der Angreifer nachvollziehen, negative Konsequenzen von Angriffen abschwächen und den Geschäftsbetrieb nach einem Angriff möglichst schnell wiederaufnehmen können. Ein Fokus auf Human Risk ist dabei unerlässlich.

# Einführung

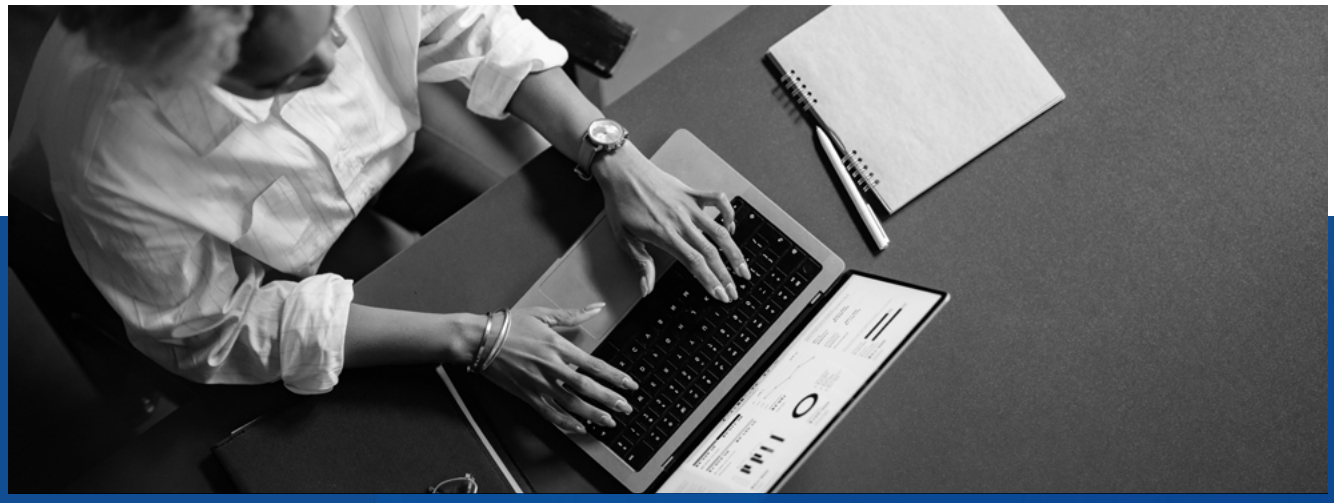
## Nur 8 % der Mitarbeiter sind für 80 % der Vorfälle in Unternehmen verantwortlich.

Die größte Herausforderung für die unternehmerische Cybersicherheit weltweit sind heute nicht mehr technologische Lücken, sondern der Faktor Mensch, also Human Risk – das zeigt der Bericht *„State of Human Risk 2025" von Mimecast,*[1] der auf Interviews mit 1.100 IT-Sicherheitsverantwortlichen und -Entscheidungsträgern basiert. Aus diesem Bericht geht außerdem hervor, dass trotz milliardenschwerer Investitionen in die Stärkung von Technologiestacks die Anzahl an Sicherheitsverletzungen nicht rückläufig ist. Grund dafür sind insbesondere Human Risk. Tatsächlich können die meisten Sicherheitsvorfälle heute auf Insider-Bedrohungen, einen Missbrauch von Zugangsdaten und menschliches Versagen zurückgeführt werden.
Die wichtigste Erkenntnis des Berichts: Menschen sind nach wie vor das schwächste Glied in der Cybersicherheitskette. 60 % der Sicherheitsverletzungen sind auf menschliches Fehlverhalten zurückzuführen, **wobei nur 8 % der Mitarbeiter für 80 % der Vorfälle in Unternehmen verantwortlich sind[2].**

Umso wichtiger ist es, dass CISOs, CIOs und andere Sicherheitsverantwortliche die notwendigen Tools haben, um Ransomware-Angriffen effektiv entgegenzuwirken. In diesem Whitepaper sehen wir uns an, wie Human-Risk-Faktoren und immer raffiniertere Angriffsmethoden Unternehmen besonders verwundbar machen. Des Weiteren erklären wir, wie Unternehmensverantwortliche durch eine adaptive, mehrschichtige Verteidigungsstrategie und ein effektives Human Risk Management (HRM; Umgang mit menschlichen Sicherheitsrisiken) ihre Cyberrisiken mindern, die Auswirkungen von Angriffen reduzieren und ihre Geschäftskontinuität gewährleisten können.

1. State of Human Risk 2025 Report, 2025
2. Exposing Human Risk, ebook, 2024

# Ransomware bleibt eines der größten Cyberrisiken



**44 %**

**Sicherheitsvorfälle betreffen Ransomware**

Ransomware hat sich mittlerweile fest als eines der größten Cyberrisiken etabliert. Laut dem Verizon Data Breach Investigations Report 2025 (DBIR) war Ransomware an 44 % aller untersuchten Sicherheitsverletzungen beteiligt. Ransomware kann nicht nur Systeme sperren, sondern auch die Betriebskontinuität unterbrechen, den Umsatz beeinträchtigen und das Vertrauen in das jeweilige Unternehmen untergraben.
Mit ihrer Ransomware zielen Cyberkriminelle allerdings nicht nur auf Systeme ab. Sobald sie ein System gefährdet haben, greifen sie oft auch die Menschen an, die darauf angewiesen sind. Im Gesundheitswesen beispielsweise soll Ransomware Menschen beeinträchtigen, deren Überleben von bestimmten Systemen abhängig ist. Wenn ein Ransomware-Angriff lebenswichtige Operationen verzögert, werden damit Leben gefährdet. Wenn Systeme durch Ransomware lahmgelegt werden, müssen Notaufnahmen den Betrieb einstellen. Wenn Patienten auf eine dringende Behandlung warten, kann jede Sekunde, die durch einen Ransomware-Angriff verloren geht, den Unterschied zwischen Leben und Tod bedeuten. Wenn Hacker Gesundheitsdaten verschlüsseln, leiden besonders schutzbedürftige Patienten. Die Konsequenzen eines Ransomware-Angriffs im Gesundheitswesen können also nicht auf bloße Zahlen reduziert werden; es geht um Menschenleben, die durch eine verzögerte Versorgung gefährdet werden.

3. 2025 Verizon Data Breach Investigations Report (DBIR), 2025

# Um Menschen zu schützen, reichen Schulungen nicht aus

Damit Sicherheitsverantwortliche ihre Mitarbeiter effektiv schützen können, benötigen sie Einsicht in die Verhaltensweisen und Absichten ihrer Belegschaft. Der DBIR gibt diesbezüglich eine klare Warnung: Fast 60 % der Sicherheitsverletzungen sind auf Human-Risk-Faktoren zurückzuführen – sei es durch Fehler, manipulatives Verhalten oder einen böswilligen Missbrauch. Um Menschen zu schützen, braucht man nicht bloß effektive Tools, sondern eine umfassende Sicherheitsstrategie einschließlich Verhaltens-Insights, maßgeschneiderter Schulungen und adaptiver Maßnahmen zur Reaktion auf riskantes Benutzerverhalten.

Um ihre Cyber Resilience zu stärken und sich vor immer neuen Bedrohungen zu schützen, müssen Unternehmen ihre Belegschaft, Technologien und Workflows miteinander verzahnen. Dabei sollten sie sich immer vor Augen führen, dass riskante Verhaltensweisen wie fehlende Patches oder eine schlechte Klick-Hygiene Angreifern Zugriff auf Systeme geben können.

**60 %**

**Sicherheitsvorfälle entstehen durch Human Risk**

Mitarbeiter verzögern oder ignorieren häufig Software-Updates, wodurch Unternehmenssysteme anfällig für bekannte Schwachstellen werden. Cyberkriminelle können genau diese Sicherheitslücken als Einstiegspunkte für Ransomware-Angriffe ausnutzen. Zum Beispiel kann ein nicht gepatchter Webbrowser durch eine Sicherheitslücke missbraucht werden, sodass Ransomware Sicherheitsprotokolle umgehen kann.

Phishing ist eine der häufigsten Methoden, mit denen Ransomware in Systeme eindringt. Dabei verleiten Cyberkriminelle ihre Opfer dazu, auf schädliche Links oder Anhänge zu klicken, über die Ransomware in das Unternehmensnetzwerk geschleust werden kann. Beispielsweise könnte ein Mitarbeiter eine E-Mail erhalten, die scheinbar von seiner IT-Abteilung stammt und in der er aufgefordert wird, seine Anmeldedaten zu überprüfen. Wenn er dann über einen Link in dieser Nachricht seine Zugangsdaten übermittelt, haben Angreifer den nötigen Zugriff, um Ransomware im Netzwerk zu installieren.

### Präventionstipp

**Automatisieren Sie die Installation von Software-Updates auf allen Unternehmensgeräten und erklären Sie Ihrer Belegschaft, wie wichtig aktualisierte Systeme sind.**

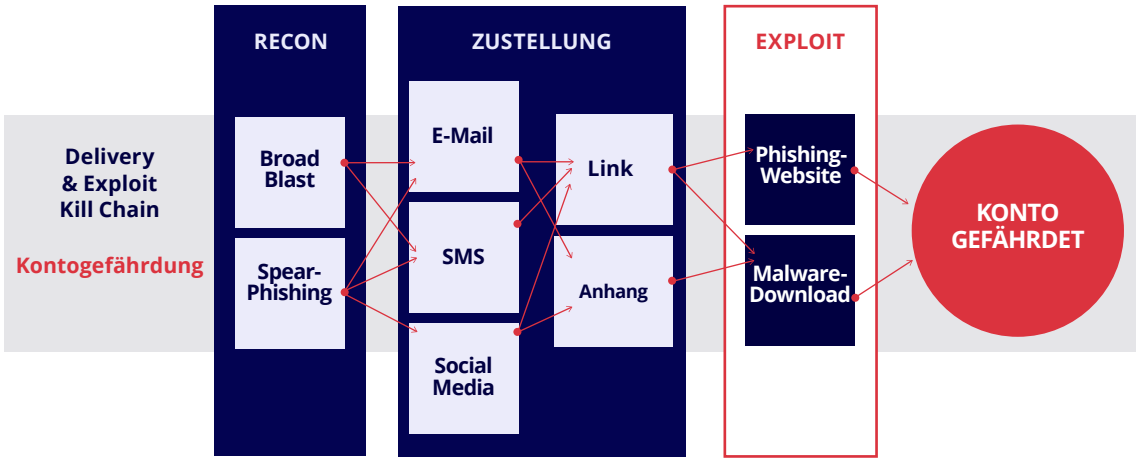
### Präventionstipp

**Schulen Sie Ihre Mitarbeiter darin, Phishing-Versuche zu erkennen, und ermutigen Sie sie, verdächtige E-Mails oder Nachrichten direkt mit der IT-Abteilung gegenzuprüfen.**

4. Verizon: 60 % der Sicherheitsverletzungen sind auf menschliches Versagen zurückzuführen, Blogartikel, 2025

# Analyse von Verhaltensweisen, die Kill Chains ermöglichen – Kontoübernahme

## Kontoübernahme




## Ransomware

**Menschliche Faktoren in einer erfolgreichen Ransomware-Kill-Chain**

- **Ein Klick auf Phishing oder Aufruf einer schädlichen Website**
- **Datei herunterladen und ausführen**
- **Ungepatchtes Gerät**
- **Back-up nicht aktiviert**

Eine der größten Bedrohungen für Unternehmen sind Cyberangriffe (insbesondere mit Ransomware), die auf Collaboration-Tools abzielen. Diese ausgeklügelten Infiltrationsversuche, die es auf E-Mail-, Chat- und Filesharing-Systeme abgesehen haben, entwickeln und verbreiten sich durch menschliches Versagen. Hinzu kommt, dass Ransomware-Kampagnen durch den Einsatz fortschrittlicher Methoden wie generativer KI und Verschleierungstaktiken immer raffinierter werden.

**Indem Unternehmensverantwortliche ihre Mitarbeiter, Technologien und Prozesse aufeinander abstimmen, können sie ihre Cyber Resilience stärken und sich gegen immer neue Bedrohungen schützen.**

# Die zunehmende Bedrohung durch Ransomware

Ransomware entwickelt sich rasant weiter. Angreifer diversifizieren ihre Eintrittspunkte und vergrößern ihre Reichweite. Collaboration-Tools wie E-Mail-, Chat- und Filesharing-Anwendungen sind insbesondere mit der Zunahme von Remote- und Hybrid-Arbeitsmodellen zu Einfallstoren für Angreifer geworden. Cyberkriminelle nutzen Human-Risk-Faktoren aus, indem sie über Collaboration-Tools wie Slack oder Microsoft Teams Unternehmen infiltrieren und in deren Systemen Chaos verursachen.

## Die zunehmende Verbreitung von Ransomware ist nicht zu leugnen:

Ransomware wurde 2025 bei **44 %** der Sicherheitsverletzungen eingesetzt (Verizon DBIR)[5]

KMUs sind mit **88 %** der Ransomware-Angriffe unverhältnismäßig stark im Visier, verglichen mit nur **39 %** bei größeren Unternehmen

5. 2025 Verizon Data Breach Investigations Report (DBIR), 2025

# Hochkarätige Ransomware-Angriffe

Aufsehenerregende Angriffe auf Unternehmen wie Marks & Spencer oder Co-op verdeutlichen die finanziellen und rufschädigenden Kosten von Ransomware. Zielunternehmen werden oft komplett lahmgelegt, sodass die Betriebsinfrastruktur und Kundenbeziehungen erheblich beeinträchtigt werden.

**Die moderne Bedrohungslandschaft und Ransomware-Trends.**
Die Bedrohungslandschaft hat sich in den letzten Jahren bedeutend verändert. Ransomware ist zu einer der am weitesten verbreiteten und schädlichsten Cyberbedrohungen geworden. Angreifer sind nicht mehr bloß opportunistische Akteure; sie haben finanzielle Ressourcen, sind gut organisiert und zielen bewusst auf Sektoren wie den Einzelhandel, das Gesundheitswesen, das Bildungswesen und kritische Infrastruktur ab. Außerdem hat die Verbreitung von Ransomware-as-a-Service (RaaS ) die Cyberkriminalität demokratisiert, sodass heute selbst technisch wenig versierte Akteure verheerende Angriffe starten können. Zusätzlich entstehen immer ausgeklügeltere Techniken für die Verschlüsselung, Datenexfiltration und doppelte Erpressung, sodass die aktuellen Ransomware-Trends keine Anzeichen einer Verlangsamung zeigen.

**Erhöhtes Risiko aufgrund menschlicher und systemischer Schwachstellen.**
Trotz steigender Investitionen in die Cybersicherheit sind Unternehmen weiterhin anfällig für Angriffe, da menschliches Versagen und systemische Schwächen sich nicht ausmerzen lassen. Systemische Probleme – komplexe IT-Umgebungen, veraltete Systeme und eine unzureichende Planung für die Reaktion auf Vorfälle – schaffen blinde Flecken, die Angreifer leicht ausnutzen können . Cybersicherheit ist nicht nur ein technisches Problem; es ist auch eine organisatorische Herausforderung, die Menschen, Prozesse und Technologien auf die Probe stellt.

**Ein robustes Framework für die Prävention, Abwehr und Disaster Recovery mit fortschrittlichen Vorbeugemaßnahmen sowie Fokus auf die Minderung des Human Risk.**
Damit Unternehmen sich effektiv gegen Ransomware schützen können, brauchen sie ein ganzheitliches, widerstandsfähiges Cybersicherheits-Framework mit entsprechenden Richtlinien zur Verhinderung von Datenverlusten, um sensible Daten vor unbefugtem Zugriff oder Datenlecks zu bewahren . Dazu gehört der Einsatz von Firewalls der nächsten Generation, Endpoint Detection and Response (EDR), Netzwerksegmentierung und Echtzeit-Bedrohungsinformationen zur proaktiven Blockierung von Angriffen. Wichtig sind außerdem Schulungen zum Cybersicherheitsbewusstsein, Phishing-Simulationen und eine starke Sicherheitskultur, um die Wahrscheinlichkeit menschlicher Fehler zu reduzieren.

6. Menschliches Versagen als Ursache der jüngsten Ransomware-Angriffe auf britische Einzelhandelsriesen, Blogartikel, 2025
7. Ransomware-Angriffe, Mimecast.com, 2025
8. Human Risk Management: Warum es an der Zeit ist, die Sensibilisierungsschulung zu überdenken, Blogartikel, 2024
9. Warum Ihr Unternehmen eine Sicherheitsrichtlinie zur Vorbeugung von Datenverlusten benötigt, Blogartikel, 2025

# Zunehmende Verbreitung von Ransomware

**88 %**

**Datenschutzverletzungen betrafen KMU**

Der Anteil der Datenschutzverletzungen mit Ransomware stieg von 32 % im Jahr 2024 auf 44 % im Jahr 2025 , was uns Aufschluss über die Absichten wie auch die Strategien heutiger Angreifer gibt. KMUs sind weiterhin unverhältnismäßig häufig Ziel von Ransomware, da sie in der Regel schwächer abgesichert sind. Sie machen 88 % der Angriffsziele aus. Britische Einzelhandelsriesen, darunter Marks & Spencer und Harrods , dienten in jüngster Zeit als abschreckende Beispiele, nachdem sie ihren Betrieb aufgrund von Angriffen auf ihre Collaboration-Tools einstellen mussten.

10. 2025 Verizon Data Breach Investigations Report (DBIR), 2025
11. Menschliches Versagen als Ursache der jüngsten Ransomware-Angriffe auf britische Einzelhandelsriesen, Blogartikel, 2025

# Moderne Angriffstechniken

Ransomware-Angreifer nutzen zunehmend raffinierte Techniken, um Human-Risk-Faktoren auszunutzen und Erkennungsmaßnahmen zu entgehen:

### Phishing und Verschleierungstaktiken

Täglich zirkulieren mehr als 3,4 Milliarden Phishing-E-Mails, und die Zahl der QR-Code-basierten Phishing-Angriffe („Quishing“) hat sich im Vergleich zum letzten Jahr versiebenfacht.[12] Quishing-Angriffe werden von herkömmlichen E-Mail-Filtern nicht erfasst und ihr Erfolg beruht auf einem Fehlverhalten mobiler Beutzer. Daher sind sie schwer zu entdecken und leicht skalierbar.

### Unbemerkte Ransomware-Angriffe

Ransomware-Angriffe penetrieren Unternehmensumgebungen über Messaging-Systeme und -Integrationen und fügen sich nahtlos in Arbeitsabläufe ein. Collaboration-Plattformen wie Slack, Zoom und Microsoft Teams ebenso wie E-Mail-Tools sind bekanntermaßen fester Bestandteil der täglichen Zusammenarbeit. Leider wissen auch Cyberkriminelle, wie stark Unternehmen sich auf diese Tools verlassen, und zielen daher auf alltägliche Interaktionen zwischen Mitarbeitern ab, um Unternehmenssysteme zu gefährden.[13]

### Generative KI (GenAI):

Cyberkriminelle nutzen KI[14], um maßgeschneiderte Phishing-E-Mails sowie schwer fassbare Ransomware-Nutzlasten zu erstellen und Unternehmen mit gestohlenen Daten zu erpressen. Mithilfe von GenAI können Angreifer in beispiellosem Ausmaß die Erstellung schädlicher, personalisierter Inhalte automatisieren. Des Weiteren verwenden sie KI-Tools, um überzeugende Spear-Phishing-E-Mails zu erstellen, polymorphe Malware zu generieren und sogar gestohlene Datensätze zu analysieren und gegen Unternehmen einzusetzen. Dies reduziert drastisch die Zeit und Kompetenzen, die für eine erfolgreiche Kampagne benötigt werden, und erhöht gleichzeitig deren Effektivität.

### Ransomware-as-a-Service (RaaS)[15]

RaaS ermöglicht es selbst technisch wenig versierten Personen, komplexe Angriffe in großem Maßstab durchzuführen. Die Kommerzialisierung von Ransomware über RaaS-Plattformen hat demnach die Eintrittsbarriere zur Cyberkriminalität gesenkt. Selbst Personen mit minimalen technischen Kenntnissen können vorgefertigte Malware-Kits kaufen oder abonnieren, um komplexe Ransomware-Angriffe zu starten. Diese Dienstangebote umfassen häufig sogar einen Kundensupport, Benutzer-Dashboards und eine fachgerechte Zahlungsabwicklung, was die Verbreitung und das Volumen von Angriffen weltweit erhöht.

### Verschiebung der Ziele

Moderne Angriffe zielen zunehmend auf die Datenextraktion und die Unterbrechung des Geschäftsbetriebs[16] ab, statt nur auf die Datenverschlüsselung. Bedrohungsakteure exfiltrieren oft sensible Daten und drohen damit, diese zu leaken oder zu verkaufen, um den Druck auf ihre Opfer sowie ihre Bereitschaft zur Lösegeldzahlung zu erhöhen.

12. Quishing macht sich ein beliebtes Marketinginstrument zunutze, Blogartikel, 2024
13. Schutz vor Bedrohungen in E-Mail- und Collaboration-Tools, Blogartikel, 2025
14. Neue Mimecast-Bedrohungsdaten: Wie ChatGPT E-Mail umkrempelt, Blogartikel, 2025
15. Ransomware-Angriffe, Mimecast.com, 2025
16. Datenexfiltration: Was es ist und wie man es verhindern kann, Blogartikel, 2024

# Die wichtigsten Herausforderungen für Sicherheitsteams

Der E-Mail-Verkehr und Collaboration-Tools wie Slack, Microsoft Teams und Zoom dienen heute als Einstiegspunkte für die Mehrheit der Cyberangriffe. Da BEC-, Phishing-Angriffe und Markenfälschungen immer fortschrittlicher werden, muss sich auch die Technologie weiterentwickeln, mit der Unternehmen diesen Bedrohungen und dem Human Risk, der ihnen Tür und Tor öffnet, begegnen möchten. Zu den konkreten Herausforderungen gehören:

### Beschränkungen bei der Vorfallerkennung und -reaktion

Angreifer verfeinern ständig ihre Methoden zur Verbreitung schädlicher Inhalte, sodass herkömmliche Erkennungstools schnell an ihre Grenzen stoßen. Verschleierte schädliche Links werden mittlerweile häufiger eingesetzt als schädliche Anhänge, was den Bedarf an ausgefeilten Erkennungsmethoden zum Klickzeitpunkt erhöht. (Global Threat Intelligence Report H2 2024[18])

### Betriebskontinuität während eines Angriffs

Ransomware-bedingte Ausfallzeiten in Collaboration-Tools können zu sofortigen Umsatzeinbußen führen – das zeigte auch die Betriebsunterbrechung bei dem Angriff auf Marks & Spencer[19]. Sicherheitsteams kämpfen oft damit, gleichzeitig die Geschäftskontinuität aufrechtzuerhalten und aggressive Eindämmungsmaßnahmen umzusetzen.

### Datenwiederherstellung und betriebliche Widerstandsfähigkeit

Wie schnell ein Unternehmen seinen Geschäftsbetrieb nach einem Angriff wiederaufnehmen kann, wirkt sich entscheidend auf seine Finanz- und Rufschäden aus. Kann der Zugriff auf E-Mails und geschäftlich relevante Dateien schnell wiederhergestellt werden, begrenzt dies das Ausmaß der betrieblichen Auswirkungen nach einem Vorfall.

17. Email & Collaboration Threat Protection, Mimecast.com, 2025
18. Global Threat Intelligence Report H2 2024
19. Menschliches Versagen als Ursache der jüngsten Ransomware-Angriffe auf britische Einzelhandelsriesen, Blogartikel, 2025

# Wichtige Aspekte der Abwehr

Wenn die Sicherheitsstrategie eines Unternehmens sowohl Mitarbeiter als auch Technologien und Prozesse einbindet, können die Sicherheitsverantwortlichen ihre Cyber Resilience stärken und sich besser gegen immer neue Bedrohungen schützen. Der technologische Fortschritt mag zwar ihre Verteidigungsstrategien gestärkt haben, doch menschliche Fehler sind und bleiben eine kritische Sicherheitskomponente, die es nicht zu vernachlässigen gilt.

## Um Human-Risk-Faktoren zu mindern und die allgemeine Sicherheit sowie betriebliche Effizienz zu verbessern, können Unternehmen folgende Methoden anwenden:

- **Integration von Bedrohungsinformationen in SIEM-, XDR- und anderen Tools[20]**
- **Benutzer-Risikoprofile zur Identifizierung hochriskanter Individuen und Rollen**
- **Bedrohungsanalyse zum Zeitpunkt des Klicks, um ausgeklügelte, verschleierte Bedrohungen zu blockieren**
- **Adaptive, granulare Richtlinien, die auf bestimmte Nutzer oder Abteilungen abgestimmt sind.**

20. SIEM vs. SOAR vs. XDR vs. UEBA: Wie unterscheiden sie sich?, Blogartikel, 2024

# Grundlagen einer starken Verteidigung gegen Cyberbedrohungen bei Collaboration-Tools

Collaboration-Tools wie E-Mail-Lösungen, Messaging-Plattformen und gemeinsam genutzte Arbeitsbereiche sind für die Produktivität unerlässlich. Sie stellen jedoch auch attraktive Ziele für Cyberkriminelle dar. Daher können Unternehmen sich nicht mehr nur auf traditionelle Sicherheitsmaßnahmen verlassen, sondern benötigen eine mehrschichtige, strategische Verteidigungsstrategie, die speziell für Collaboration-Umgebungen entwickelt wurde. Eine solche moderne Verteidigungsstrategie integriert eine proaktive Bedrohungserkennung, Sensibilisierungsschulungen für Benutzer, eine Geschäftskontinuitätsplanung und eine schnelle Vorfallreaktion, um zunehmend ausgefeilte Angriffe abzuwehren. Im Folgenden nennen wir die wesentlichen Komponenten einer widerstandsfähigen, adaptiven Sicherheitsarchitektur für die Zusammenarbeit, die sowohl die Infrastruktur als auch Endnutzer schützt:

## Advanced Threat Protection (Erweiterter Bedrohungsschutz) [21]

**Advanced Threat Protection ist eine umfassende, cloudbasierte Sicherheitslösung, mit der Unternehmen ihre E-Mail-Systeme vor Cyberangriffen mit Spam, Viren und Malware schützen. Da diese Cyberbedrohungen ständig weiterentwickelt werden, ist es für Unternehmen jeder Größe wichtig, fortschrittliche Schutzmaßnahmen umzusetzen, wie z.:**

- Echtzeitfilterung von Bedrohungen durch Phishing-Versuche, Markenfälschungen oder Kontogefährdungen
- Schutz vor Links und Anhängen
- Sandbox-Analyse zur Erkennung von verschlüsselten und polymorphen Bedrohungen
- Verhaltensanalysen zur Erkennung von Anomalien vor und nach der Zustellung

## Sicherheitsbewusstsein und -schulungen[22]

**Minimieren Sie reale Risiken und revolutionieren Sie das Sicherheitsbewusstsein mit einem menschenzentrierten Ansatz auf folgende Weise:**

- Implementieren Sie maßgeschneiderte Schulungen für Hochrisikonutzer
- Führen Sie simulierte Phishing- und Social-Engineering-Übungen durch
- Verfolgen und analysieren Sie von Benutzern gemeldete Vorfälle, die beinahe negative Konsequenzen gehabt hätten

21. Advanced Threat Protection, Mimecast.com, 2025
22. Security & Awareness Training, Mimecast.com 2025

## Betriebskontinuität und Datenresilienz [23]

**Ein Cybersicherheitsvorfall kann den Betrieb eines Unternehmens stören, was zu Ausfallzeiten, finanziellen Verlusten, Rufschäden und sogar rechtlichen oder regulatorischen Konsequenzen führen kann. Wie gut die Cyber Resilience eines Unternehmens ist, spielt in diesem Zusammenhang eine entscheidende Rolle. Im besten Fall stellt sie sicher, dass das Unternehmen seine wichtigsten Funktionen auch während und nach einem Vorfall aufrechterhalten kann, um Störungen des Geschäftsbetriebs zu reduzieren.**

- Stellen Sie sicher, dass Ihre Belegschaft stets Zugriff auf E-Mail- und Collaboration-Tools hat – selbst während eines Angriffs
- Führen Sie häufige, automatisierte Back-ups durch und prüfen Sie die Integrität Ihrer Daten
- Entwickeln Sie schnelle Failover-Prozesse für eine nahtlose Wiederherstellung nach Vorfällen

## Vorfallreaktion, Risikobeseitigung und Systemwiederherstellung [24]

- Automatisieren Sie Ihre Arbeitsabläufe, um Untersuchungen zu optimieren und kürzere Reaktionszeiten zu erzielen
- Stellen Sie eine effektive interne Kommunikation während eines Angriffs sicher
- Sorgen Sie dafür, dass Sie den Betrieb kritischer Systeme mit minimalen Ausfallzeiten wiederherstellen können, um wirtschaftliche Verluste zu minimieren

23. Definition of cyber resilience, Mimecast.com, 2025
24. What is threat detection and response? Mimecast.com 2025

# Messung von Erfolg und Renditen

## Sicherheitsrelevante Aktivitäten können durch die folgenden Kennzahlen quantifiziert werden: [25]

- Reduzierung des finanziellen Schadens durch Sicherheitsverletzungen
- Kürzere Wiederherstellungs- und Ausfallzeiten nach einem Angriff
- Metriken für Benutzerrisikobewertungen, Reduzierung der Auswirkungen von Sicherheitsverletzungen und Compliance-KPIs

25. Die 10 wichtigsten Metriken und KPIs für die Cybersicherheit, Blogartikel, 2024

Für die geschäftlichen Abläufe eines Unternehmens ist es heute unerlässlich, Human-Risk-Faktoren zu identifizieren und ein widerstandsfähiges Verteidigungssystem aufzubauen. Allerdings ist der Weg zu einem effektiven Schutz nicht unbedingt linear, und es gibt keinen universellen Konsens darüber, mit welchen Techniken Unternehmen den Fortschritt ihrer Sicherheitsstrategie nachverfolgen sollen. Allerdings kann man sagen, dass Unternehmen, die ihre Risikotoleranz evaluieren und ihr entsprechende KPIs zuweisen, eine viel größere Chance haben, ein gutes HRM-Programm zu entwickeln.

Damit Unternehmen ihr Human Risk Management und ihre Cybersicherheitsmaßnahmen verbessern können, müssen sie stets wachsam bleiben und die richtige Technologie sowie bewährte Schulungsmethoden einsetzen. Es ist nicht immer leicht, nützliche Kennzahlen zu identifizieren und sich ausreichend Sichtbarkeit zu verschaffen, um diese Kennzahlen auf alle IT- und Sicherheitsressourcen eines Unternehmens wie auch auf alle Benutzer anzuwenden. Doch wenn Sicherheitsverantwortliche verstehen, welche Kennzahlen für bestimmte Gruppen relevant sind und welche KPIs die Unternehmensperformance insgesamt fördern, sind sie in der Lage, Risiken zu verringern und potenziell lähmende Angriffe zu vermeiden.

# Die Ausbreitung von Ransomware geht ungebremst weiter

**Ransomware hat sich im letzten Jahrzehnt zu einer der beliebtesten Formen der Cyberkriminalität entwickelt. Ihr Wachstum schreitet unaufhaltsam voran, und fortschrittliche Technologien machen es Cyberkriminellen immer leichter, ihre Spuren zu verwischen.**

## Zu diesen Technologien gehören:

**Anonyme Zahlungsmethoden (Kryptowährung).**
Kryptowährungen wie Bitcoin und Monero ermöglichen es Cyberkriminellen, Lösegeldzahlungen anonym zu erhalten, sodass Behörden das Geld nicht nachverfolgen können.

**Fortschrittliche Verschlüsselungstechniken.**
Durch neue und stärkere Verschlüsselungsalgorithmen kann Ransomware Dateien noch zuverlässiger verschlüsseln.

**KI und maschinelles Lernen.**
KI-gestützte Malware kann ihr Verhalten dynamisch anpassen, sich der Erkennung durch herkömmliche Sicherheitssoftware entziehen und den Zeitpunkt sowie die Ziele von Angriffen optimieren.

**Ausnutzung des Cloud- und Fernzugriffs.**
Unsere zunehmende Abhängigkeit von Cloud-Diensten und Remote-Arbeitsumgebungen bietet neue Angriffsflächen für Ransomware, die Schwachstellen aus der Ferne ausnutzen und sich so schneller verbreiten kann.

**Darknet-Marktplätze und -Tools.**
Die zunehmende Verbreitung von Darknet-Marktplätzen bietet Kriminellen einfachen Zugang zu Ransomware-as-a-Service (RaaS), sodass auch technisch weniger versierte Personen Angriffe starten können, indem sie einfach die erforderlichen Ransomware-Tools mieten.

**Tarntechniken (dateilose Malware, Living-off-the-Land-Binärdateien).**
Malware, die sich im Arbeitsspeicher des betroffenen Geräts versteckt oder legitime Systemtools missbraucht, hilft Angreifern dabei, sich einer Erkennung durch Antiviren- und Endpunktsicherheitslösungen zu entziehen.

# Zukünftige Bedrohungen und strategische Vorausschau

Während Cyberkriminelle mit großer Hartnäckigkeit ihren Ransomware-Ansatz weiterverfolgen, zeigen die jüngsten Angriffe, dass menschliches Versagen in diesem Kontext oft eine wesentliche Schwachstelle ist. Damit Unternehmen ihre Abwehr stärken können, sollten sie daher vorrangig auf präventive Maßnahmen setzen und ihre Belegschaft mit den notwendigen Kenntnissen und Tools ausstatten, um Fehler zu minimieren und ungewöhnliche Aktivitäten genau zu beobachten.[26]

**Des Weiteren müssen sich Unternehmen darauf vorbereiten, dass Ransomware-Angriffe immer ausgeklügelter werden, zum Beispiel durch:**

- **KI-gesteuerte Angriffe über Collaboration-Tools** wie die Infiltrierung von Slack oder Teams durch KI-generierte Mitarbeiter
- **Evasive Bereitstellungsmethoden** wie Prompt-Injections
- **Missbrauch von Anmeldeinformationen,** möglicherweise durch vernachlässigte Integrationen

26. Getting started: How to protect against ransomware, Mimecast.com, 2025

Um Human-Risk-Faktoren in Verteidigungssystemen zu vermindern, brauchen Unternehmen einen umfassenden Präventionsansatz, der nicht nur individuelle Schulungen vorsieht, sondern die gesamte Organisationsstruktur, alle Technologie-Integrationen und auch die Unternehmenskultur einbindet. Während technologische Fortschritte die Verteidigungsfähigkeiten von Unternehmen weiter stärken, bleiben menschliche Eigenschaften wie Kreativität, kritisches Denken und Anpassungsfähigkeit unersetzliche Ressourcen. Ein effektiver Umgang mit Human-Risk-Faktoren sorgt dafür, dass Verteidigungsstrategien nicht nur widerstandsfähig, sondern auch agil genug sind, um eine kontinuierliche Anpassung an die globale Bedrohungslandschaft zu ermöglichen.

Damit Unternehmen ihre Geschäftskontinuität und ihren betrieblichen Erfolg auch zukünftig sichern können, benötigen sie eine adaptive Strategie für den Umgang mit Ransomware, die eine proaktive Prävention mit einer schnellen Disaster Recovery kombiniert. Größte Priorität ist dabei das Human Risk Management. Durch die Schulung von Mitarbeitern, den Schutz von Collaboration-Tools und die Einführung proaktiver Cyber-Resilience-Maßnahmen können Unternehmen sich der Bedrohungslandschaft selbstbewusst stellen.

Mimecast verwendet für die Erkennung von Ransomware einen mehrschichtigen Ansatz, der die Blockierung des Zugriffs auf E-Mails und Daten verhindert . Dazu gehören die automatische Erkennung und Isolierung potenzieller Bedrohungen, wie zum Beispiel verdächtiger Links oder E-Mail-Anhänge. Unser Ansatz befähigt Ihre Mitarbeiter zudem dazu, potenzielle Bedrohungen selbst zu erkennen und grundlegende Cybersicherheitsprotokolle wie das Festlegen starker Passwörter einzuhalten.

**Durch die Schulung von Mitarbeitern, den Schutz von Collaboration-Tools und die Einführung proaktiver Cyber-Resilience-Maßnahmen können Unternehmen sich der Bedrohungslandschaft selbstbewusst stellen.**

27. So führt Human Risk zu Ransomware-Angriffen, Blogartikel, 2025


# HUMAN RISK, SECURED.

**Über Mimecast**

Mimecast ist eine KI-gestützte, API-fähige und vernetzte Human Risk Management-Plattform. Sie wurde entwickelt, um Unternehmen vor dem gesamten Spektrum von Cyberbedrohungen zu schützen. Dafür integriert sie moderne, benutzerfreundliche Technologie mit Strategien für das Erkennen von Risiken und den Aufbau von Sicherheitskompetenz, die immer den Nutzer im Fokus behalten. Darauf ausgelegt, unsichtbare Risiken sichtbar zu machen und Dateneinblicke so aufzubereiten, dass sie als Entscheidungsgrundlage dienen können, eröffnet sie Unternehmen proaktive Handlungsmöglichkeiten. Sie hilft, Kommunikations- und Kollaborationslandschaften zu schützen, kritische Daten zu sichern, Mitarbeiter aktiv in das Risikomanagement einzubeziehen und eine Sicherheitskultur zu fördern, die mit Unternehmenszielen wie Geschäftskontinuität und Steigerung der Produktivität in Einklang steht. Über 42.000 Unternehmen weltweit vertrauen Mimecast, um der sich dynamisch entwickelnden Bedrohungslandschaft einen Schritt voraus zu sein. Von internen Risiken bis hin zu externen Gefahren – Mimecast bietet Kunden mehr.

***Mehr Sichtbarkeit. Mehr Einblicke. Mehr Agilität. Mehr Sicherheit.***