mimecast®

The Connected Human Risk Management Platform

EXPOSING. human risk

Einführung

In unserer aktuellen Cybersicherheitslandschaft, in der Bedrohungsakteure mit klangvollen Namen wie „Volt Typhoon“ und „Dark Scorpius“ auftreten, ist es bedauerlich, dass alltägliche Nutzer in der Risikobewertung oft übersehen oder unterschätzt werden.

Fragt man Sicherheitsverantwortliche jedoch, welche Cybersicherheitsgefahren ihnen am meisten Bauchschmerzen bereiten – also wo sie sich am stärksten gefährdet fühlen –, werden sie wahrscheinlich die Risiken aus dem eigenen Unternehmen nennen.

Mit diesem Bericht möchten wir das Narrativ rund um Human Risk umkehren – sie aufdecken, um unsere eigene Gefährdung zu minimieren. Wir werfen mit den umfangreichen Telemetriedaten von Mimecast ein Licht darauf, wie risikoreiches Verhalten aussieht, wie häufig es vorkommt und wer daran beteiligt ist.

Im Folgenden finden Sie eine Auswahl unserer Erkenntnisse.

HAUPTERKENNTNISSE.

48% Fast die Hälfte der Mitarbeiter zeigte Verhaltensweisen, die ihre Organisationen Cyberrisiken aussetzten.

1/3 **WEB BROWSING** der Nutzer verstieß gegen Web-Browsing-Richtlinien, die zu ihrem Schutz gedacht sind.

5% **PHISHING ANGRIFFE** Rechnen damit, dass etwa 5 % Ihrer Belegschaft jährlich auf Phishing-Angriffe hereinfallen.

13% **PHISHING EMAILS** Die Klickrate auf Phishing-E-Mails lag bei den Nutzern im Durchschnitt bei 13 %. Schulungen verringern diese um 25 %.

Etwa **1 VON 7** malware-anfälligen Mitarbeitern löste jeweils mehr als **10+** Ereignisse aus.

WER SIND DIESE RISIKOBEHAFTETEN MITARBEITER?

Führungskräfte, Vertrieb und der Vorstand stehen an der Spitze unserer Liste der risikobehafteten Gruppen. Lesen Sie weiter, um andere „phishy“ Profile basierend auf Rolle und Berufserfahrung zu entdecken.

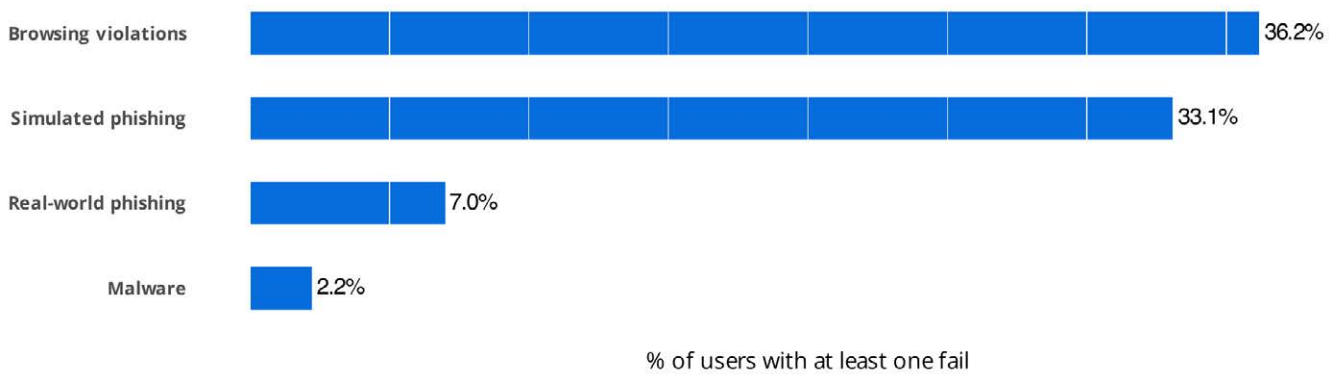
Benchmarking Risikoverhalten

Dieser Abschnitt misst, wie häufig Mitarbeiter Verhaltensweisen zeigen, die ihre Organisationen verschiedenen Cybersicherheitsbedrohungen aussetzen.

RISIKO

Wir konzentrieren uns auf drei Arten risikobehafteten Verhaltens: das Klicken auf Phishing-E-Mails, das Herunterladen oder Ausführen von Malware und das Verstoßen gegen Web-Browsing-Richtlinien. Diese schließen sich natürlich nicht gegenseitig aus, und wir werden die Rückfallraten in einem späteren Abschnitt näher untersuchen. Insgesamt zeigte fast die Hälfte (48 %) aller Nutzer während des Analysezeitraums mindestens eines dieser Verhaltensweisen. Verstöße gegen Browsing-Richtlinien traten am häufigsten auf (36 % der Nutzer), während Malware-Ereignisse mit etwa 2 % der Nutzer am seltensten waren.

Abbildung 1: Prozentsatz der Nutzer, die risikobehaftetes Verhalten zeigen



Wir haben in der Grafik zwei Kategorien für Phishing aufgenommen: eine für das Klicken auf echte, bösartige Phishing-Versuche und eine für simulierte Phishing-Übungen, die von ihren Organisationen durchgeführt werden, um sie gegen echte Angriffe zu immunisieren.

Wenn Sie sich fragen, wie gut das funktioniert, behalten Sie diesen Gedanken – wir kommen noch darauf zurück. Für den Moment sollten Sie nur beachten, dass Nutzer weniger wahrscheinlich auf echte Phishing-Angriffe hereinfallen als auf gefälschte.

Phishing in der realen Welt

Obwohl Phishing laut der obigen Abbildung 1 nicht am häufigsten vorkommt, beginnen wir hier, da es beim Thema Human Risk oft als erstes in den Sinn kommt. Und das aus gutem Grund. Der langjährige und weithin anerkannte Data Breach Investigations Report von Verizon listet Phishing regelmäßig als eine der größten Bedrohungen. Die Information Risk Insights Study des Cyentia Institute zeigte, dass Phishing in 18 von 20 Sektoren zu den drei häufigsten Techniken für den ersten Zugriff gehörte.

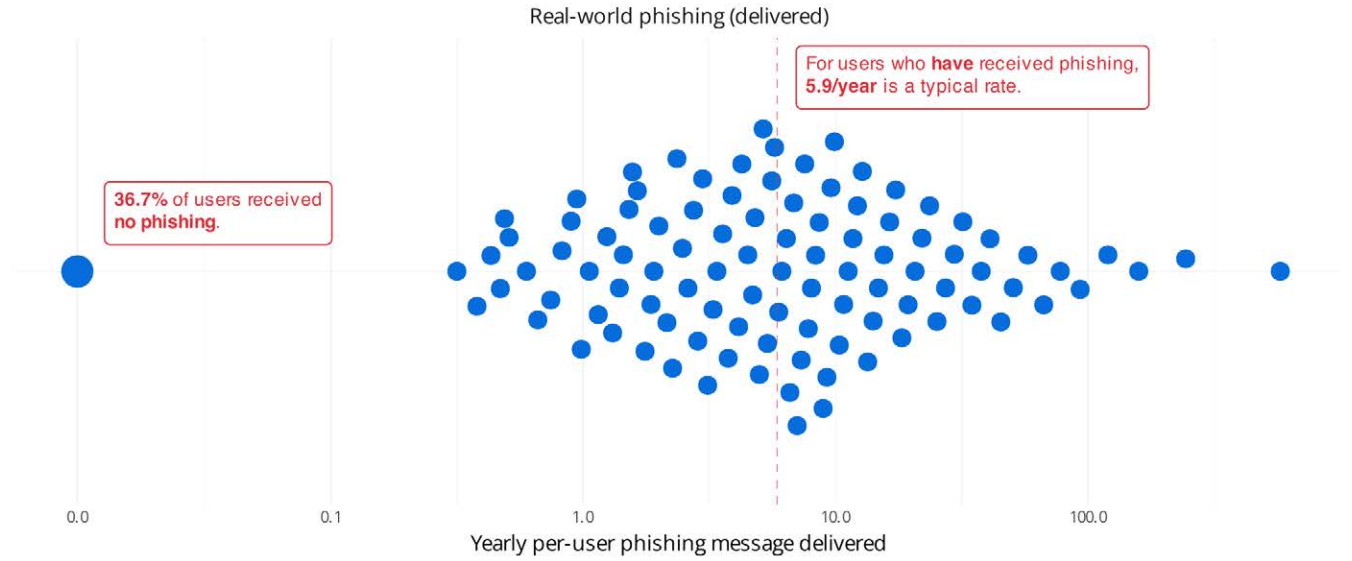
Wie häufig treten Phishing-Angriffe bei Mimecast auf? Wie wahrscheinlich ist es, dass Nutzer darauf klicken? Wie viele Phishing-Fehler sollte Ihre Organisation in einem Jahr erwarten? Wir liefern Antworten auf diese Fragen und mehr.

Festgestellte Phishing-Versuche

Wir haben bereits gezeigt, dass 7 % aller Nutzer auf mindestens eine Phishing-E-Mail hereingefallen sind. Lassen Sie uns jedoch einen Schritt zurückgehen und einige grundlegende Kennzahlen festlegen. Mehr als ein Drittel (36,7 %) der Nutzer haben während des Zeitraums, in dem historische Ereignisdaten verfügbar sind (dies variiert je nach Organisation und Nutzer), keinen einzigen echten Phishing-Versuch erhalten.

Unter den Nutzern, die Phishing-Versuche erhalten haben, lag die typische Rate bei etwa sechs pro Jahr, obwohl diese Zahl innerhalb der Nutzergruppe variiert. Dies lässt sich in Abbildung 2 unten erkennen (jeder Punkt repräsentiert 1 % der Nutzer). Etwa 13 % der Nutzer erhielten weniger als eine Phishing-E-Mail pro Jahr, aber 4 % von ihnen wurden mit mehr als 100 E-Mails gezielt angegriffen. Wer sind die Nutzer, die am häufigsten von Phishing angegriffen werden? Gute Frage – wir gehen später darauf ein.

Abbildung 2: Verteilung der Phishing-Versuche pro Nutzer pro Jahr. Jeder Punkt repräsentiert 1 % der Nutzer.



Welche Art von Phishing-Angriffen kursiert?

Die Erkennungen von Mimecast umfassen mehr als 42.000 Organisationen weltweit und decken alle Arten von Phishing-Angriffen ab. Diese werden in die Subtypen unterteilt, die in Abbildung 3 auf der linken Seite zu sehen sind. Wir vergleichen die normalisierten Erkennungsraten (pro Nutzer pro Jahr) für jeden Subtyp nach Branchen, wobei die Schattierung in der Tabelle hilft, die häufigsten Phishing-Arten für jede Branche hervorzuheben.

Ihr Blick wird wahrscheinlich von dem dunklen, roten Band für Credential Harvesting angezogen, das sich ununterbrochen über alle Sektoren erstreckt. Falls Sie noch mehr Beweise dafür brauchen, dass Angreifer legitime Benutzeranmeldeinformationen als Mittel zur Erlangung und Erhöhung des Zugriffs auf Zielumgebungen anstreben, finden Sie diese hier.

Impersonation ist ebenfalls eine häufige Phishing-Art in allen Branchen (besonders im Gesundheitswesen und im Bildungsbereich) und untermauert diesen Punkt weiter. Dies liefert mehr Beweise dafür, dass Insider weitaus häufiger als Angriffsvektoren fungieren, statt die Täter hinter den Angriffen zu sein.

Beachten Sie, dass wir Subtypen für blockierte und Phishing-URLs in einer separaten Ebene der Tabelle aufgenommen haben. Dies haben wir getan, weil diese Erkennungen explizit durch das Klicken von Nutzern auf Phishing-Nachrichten ausgelöst werden, was zu Versuchen führt, sich mit bösartigen Seiten zu verbinden. Daher stellen sie eine ausgehende, statt einer eingehenden Sicht auf Phishing-Aktivitäten dar. Wir haben auf eine zusätzliche Farbmarkierung verzichtet, um diesen Unterschied weiter hervorzuheben, aber es ist bemerkenswert, dass die Erkennungsrate für blockierte URLs in allen Sektoren relativ hoch ist.

Abbildung 3: Vergleich der Erkennungsraten von Phishing-Subtypen nach Sektor

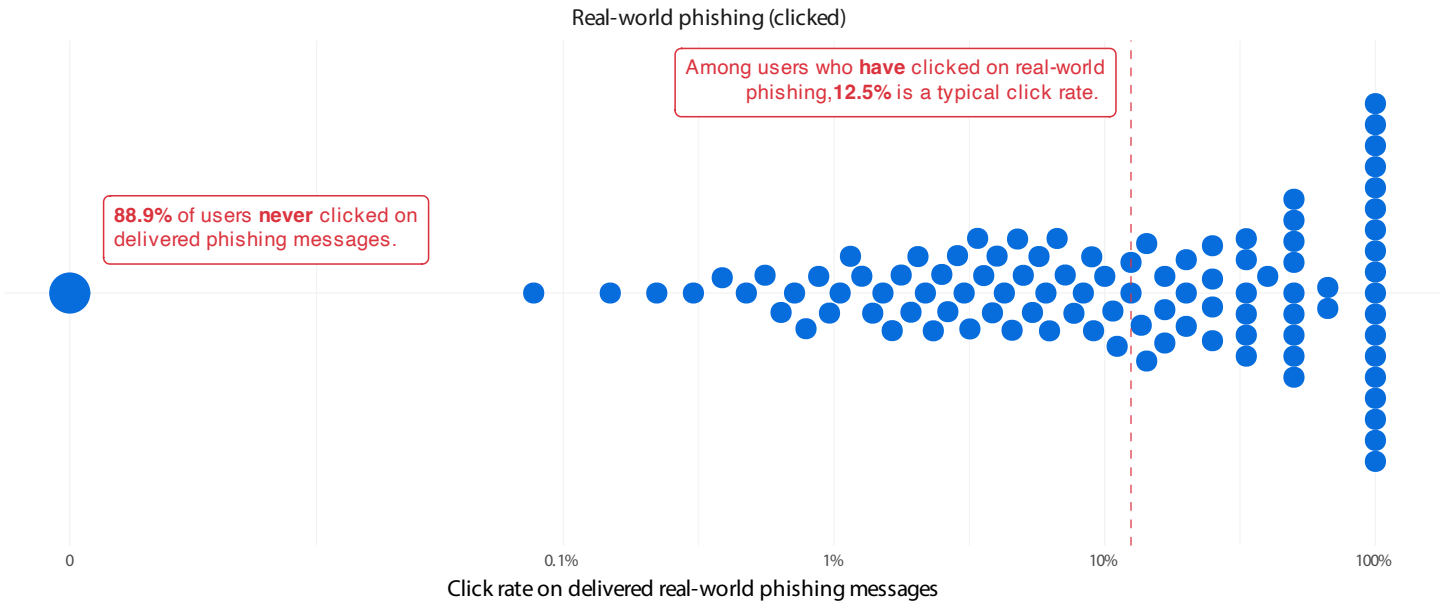
		PS	IT	Retail	Sci/Tech	Education	Finance	Manufacturing	Government	Construction	Healthcare
	Abused Fee Fraud	0.008	0.005	0.008	0.006	0.002	0.009	0.005	0.014	0.009	0.003
	Abused Fee Scam	0.057	0.058	0.062	0.061	0.011	0.073	0.038	0.090	0.067	0.024
	Abused Legitimate Services	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	BEC Whaling	0.003	0.004	0.005	0.004	0.000	0.004	0.004	0.000	0.005	0.001
	Credential Harvesting	0.986	1.182	1.074	1.125	0.045	1.491	0.941	0.332	1.683	0.347
	Dating	0.001	0.001	0.002	0.001	0.000	0.001	0.001	0.001	0.002	0.001
	Exploit	0.004	0.005	0.004	0.004	0.000	0.011	0.004	0.001	0.008	0.002
	Fraud	0.099	0.113	0.097	0.077	0.007	0.122	0.087	0.028	0.107	0.042
	Impersonation	0.491	0.893	0.563	0.599	0.041	0.712	0.542	0.134	0.720	0.379
	Low Reputation	0.015	0.012	0.014	0.011	0.000	0.020	0.012	0.002	0.018	0.006
	Malicious File	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	Malspam	0.001	0.001	0.000	0.000	0.000	0.001	0.001	0.000	0.000	0.000
	Monitored Actor	0.202	0.204	0.197	0.201	0.008	0.274	0.180	0.069	0.272	0.065
	Romance Fraud	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.001	0.000
	Sending MTA Detection	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
	Suspected Spam	0.050	0.049	0.049	0.048	0.002	0.260	0.040	0.028	0.048	0.015
	Suspicious Message Content	0.001	0.003	0.001	0.001	0.000	0.001	0.001	0.002	0.001	0.001
	Unsolicited Bulk Mail	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Require user action:	Blocked URL	1.669	2.604	1.292	1.066	0.142	2.054	1.431	0.491	1.568	0.700
	Phishing URL	0.012	0.009	0.009	0.004	0.001	0.075	0.011	0.005	0.016	0.009

Phishing Klickraten

Phishing-E-Mails zu erhalten ist das eine, darauf hereinzufallen das andere. Laut unserer Analyse klickten 89 % der Nutzer, die echte Phishing-Nachrichten erhielten, niemals auf eine davon. Bravo!

Von den Nutzern, die anbissen, lag die typische Klickwahrscheinlichkeit bei 12,5 %, obwohl wir erneut eine große Spreizung unter ihnen beobachteten. Einige Nutzer hatten Klickraten von nur 0,1 %, während andere bei jedem Phishing-Versuch voll hineinfielen.

Abbildung 4: Verteilung der Klickraten unter Nutzern für Phishing-Versuche

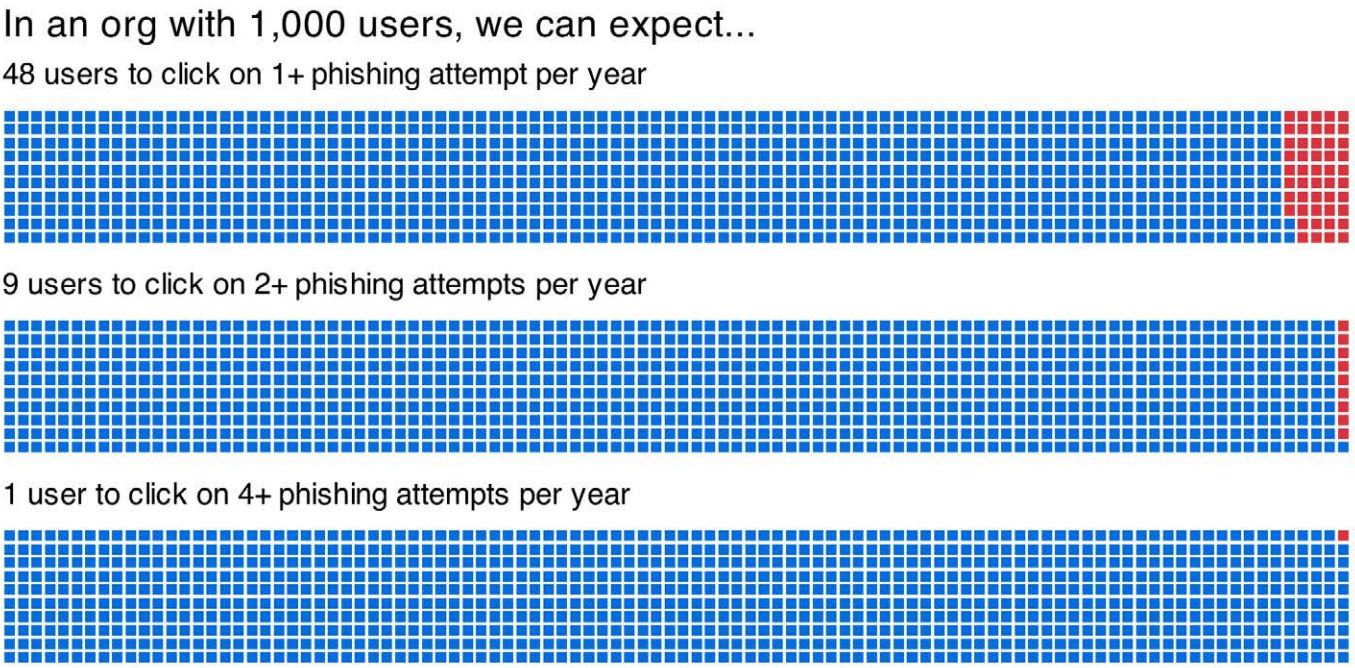


Erwartete Häufigkeit erfolgreicher Phishingangriffe

Wie viele Phishing-E-Mails werden in Ihrer Organisation im nächsten Jahr Klicks erzielen? Nun, das ist schwer zu beantworten, ohne mehr über Ihre spezifische Organisation zu wissen. Aber was wir tun können, ist etwas Mathematik anzuwenden (genauer gesagt, Empirical Bayes) um unsere Daten zu historischen Zustell- und Klickraten zu nutzen und die erwartete Häufigkeit erfolgreicher Phishing-Angriffe zu modellieren.

Mit diesem Modell können wir einige Projektionen für eine Organisation mit 1.000 Personen anstellen. Etwa 50 Nutzer (48) werden mindestens eine Phishing-Nachricht pro Jahr anklicken. Neun Mitarbeiter werden auf zwei oder mehr Phishing-Nachrichten hereinfallen, und ein unglücklicher Nutzer wird mehrmals "angebissen" werden. Abbildung 5 veranschaulicht diese Informationen.

Abbildung 5: Modellierte Häufigkeit erfolgreicher Phishing-Angriffe pro Jahr



Kann Schulung helfen, die Klicks zu verhindern?

Es gibt Hinweise darauf, dass Mitarbeiter in gewissem Maße darin geschult werden können, ihre Klickgewohnheiten zu verringern, aber die Beweise zeigen auch, dass „Klicker immer klicken werden".

Wir haben die Klickraten für Phishing vor und nach der Schulung untersucht. Nutzer mit niedrigen Klickraten zeigten keine Verbesserung, während bei denen mit hoher Klickneigung die Klickraten um durchschnittlich 25 % sanken.

Organisationen sollten in Erwägung ziehen, Schulungen und Maßnahmen für die Mitarbeiter zu verstärken, die am meisten zum Klicken neigen. Dies kann rechtzeitige Eingriffe umfassen, die an tatsächliche Klicks und riskante Ereignisse gekoppelt sind.

Diese Ergebnisse legen nahe, dass Schulungen zwar nicht das Klicken vollständig aus Ihrer Organisation verbannen werden, aber zumindest dabei helfen können, dieses Verhalten bei den risikoreichsten Nutzern einzudämmen. Sie deuten auch darauf hin, dass ein gezielter, maßgeschneiderter Ansatz für Schulungen und andere Maßnahmen wahrscheinlich erfolgreicher sein wird als ein einheitlicher Ansatz für alle.

Abbildung 11: Vergleich der durchschnittlichen Reduktion der Phishing-Klickraten nach Schulung

Malware

Schadliche Software, oder Malware, ist das Multitool der Cyberkriminellen-Welt. Sie bietet die Moglichkeit, remote zu kommunizieren, Befehle zu erteilen, Hinterturen zu erlangen, Daten zu finden und abzuziehen, Systeme zu zerstoren, Spuren zu verwischen und vieles mehr.

Wah rend Angreifer zunehmend versuchen, “vom Land zu leben” und bestehende Tools fur ihre illegalen Aktivitaten zu nutzen, ist es immer noch eine sehr gangige Taktik, Mitarbeiter dazu zu bringen, Malware herunterzuladen und/oder auszufuhren. Das ist zweifellos ein riskantes Verhalten, das Organisationen vermeiden wollen.

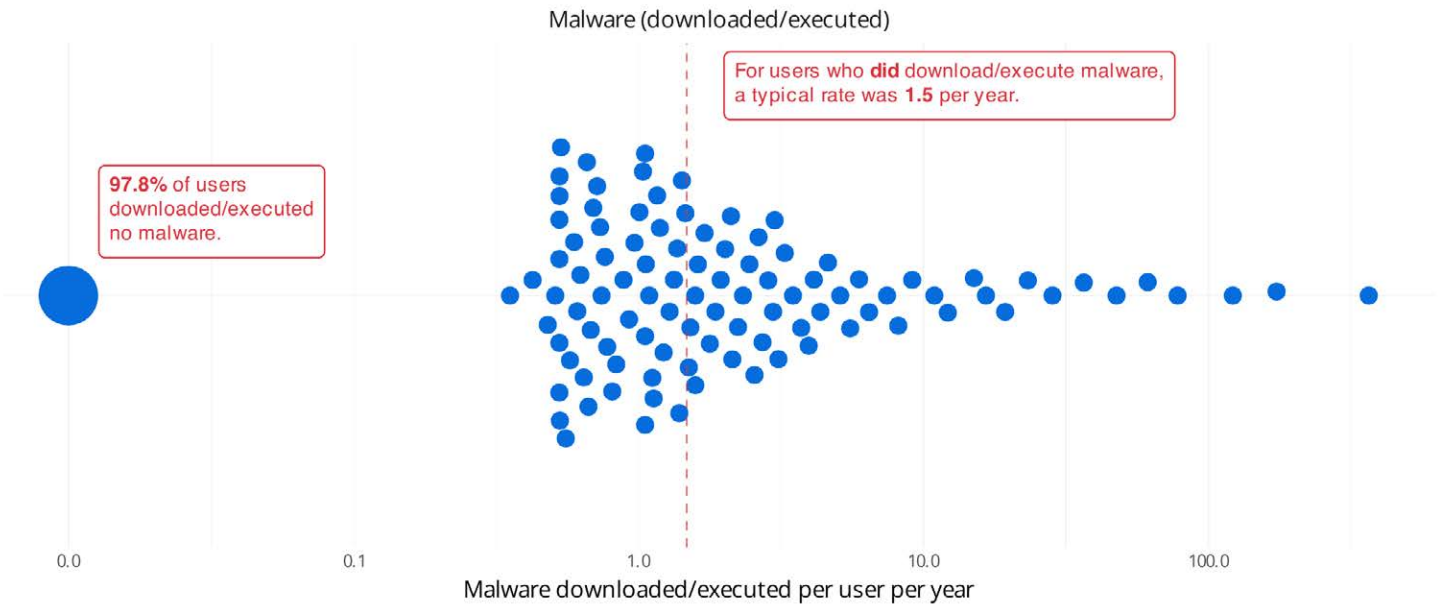
Schauen wir mal, wie es ihnen geht.

Beobachtete Malware-Begegnungen

Gute Nachrichten sind in Berichten über Cyber-Bedrohungen oft schwer zu finden. Daher sollten wir zunächst einmal anerkennen, dass fast alle Mitarbeiter (98 %) in unserem Stichprobenzeitraum eine makellose Bilanz bei Malware-Ereignissen vorweisen konnten. Das spricht für die vielen Anti-Malware-Schutzmaßnahmen, die zwischen den Benutzern in modernen Unternehmen und dem von Malware verseuchten Internet um sie herum bestehen.

Aber die 2 % der Nutzer, die Malware heruntergeladen oder ausgeführt haben, können natürlich nicht ignoriert werden. Die typische Häufigkeit von Malware-Ereignissen bei diesen Nutzern lag bei etwa 1,5 pro Jahr. Wie schon beim Phishing gibt es auch bei dieser Rate große Schwankungen (siehe Abbildung 6). Etwa einer von sieben Mitarbeitern war allein für die Auslösung von 10 oder mehr Malware-Ereignissen verantwortlich.

Abbildung 6: Verteilung der Malware-Downloads/Ausführungen pro Nutzer und Jahr



Welche Art von Malware ist im Umlauf?

Die Mimecast-Sensorsammlungen bieten zusätzliche Informationen über die Arten von Malware, mit denen Mitarbeiter bei ihren Tätigkeiten konfrontiert werden. Die wichtigste Kategorie für die meisten Bereiche sind Malware-Samples, die mit bekannten Bedrohungsakteuren in Verbindung gebracht werden. Wer sich für Beispiele spezifischer Malware interessiert, die von verschiedenen Bedrohungsgruppen verwendet wird, findet diese in Hülle und Fülle auf der MITRE ATT&CK site.

Schwachstellen in Software und Hardware stehen in diesem Sektor an erster Stelle, was möglicherweise daran liegt, dass Finanzdienstleister in der Regel über ausgereiftere Kontrollen verfügen. Schwachstellen öffnen Löcher in diesen ansonsten starken Abwehrmechanismen, die von Malware schnell als Waffe eingesetzt und ausgenutzt werden können.
Im Allgemeinen sind die Unterschiede zwischen den Organisationen größer als zwischen den Branchen. Es stimmt zwar, dass die Mehrheit der Fertigungsunternehmen häufiger mit Malware konfrontiert ist als Bildungseinrichtungen, aber die sich überschneidenden Verteilungen zeigen, dass dies nicht immer der Fall ist.

Abbildung 7: Vergleich der Raten der entdeckten Malware-Subtypen nach Sektor

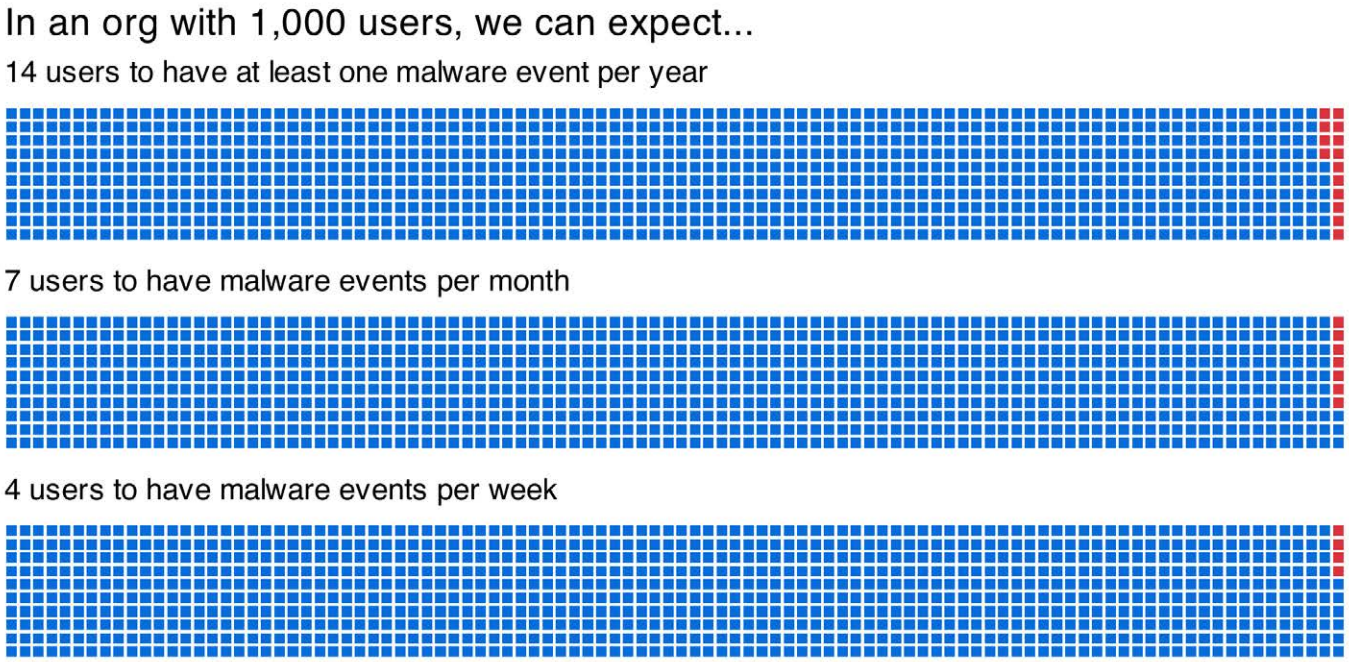
Malware subtype detections per seat per year											
	Malware Subtype	IT	Education	Manufacturing	Retail	Healthcare	PS	Finance	Government	Construction	Sci/Tech
	Exploit	0.075	0.002	0.049	0.059	0.027	0.056	0.619	0.014	0.090	0.059
	Malicious File	0.018	0.001	0.017	0.017	0.006	0.012	0.030	0.014	0.015	0.023
	Malspam	0.080	0.004	0.080	0.098	0.032	0.081	0.089	0.039	0.084	0.083
	Monitored Actor	0.346	0.010	0.282	0.307	0.131	0.310	0.310	0.050	0.303	0.207
	Unclassified	0.021	0.001	0.026	0.026	0.005	0.018	0.030	0.004	0.034	0.026
Require user action:	Blocked URL	0.587	0.044	0.205	0.283	0.218	0.434	1.180	0.232	0.472	0.271

Erwartete Häufigkeit

Wir haben den gleichen grundlegenden Ansatz wie bei Phishing verwendet, um die Häufigkeit von Malware-Ereignissen zu modellieren und eine normalisierte Schätzung abzuleiten. In einem Unternehmen mit 1.000 Mitarbeitern gehen wir davon aus, dass 14 Mitarbeiter Malware herunterladen oder ausführen. Sieben dieser Mitarbeiter werden monatlich Malware-Ereignisse auslösen, und vier werden wöchentlich mit bösartiger Software in Berührung kommen.

Wenn Ihnen das wie eine kleine Anzahl von Benutzern hinter einer großen Anzahl von Ereignissen vorkommt, haben Sie einen wichtigen Aspekt des Human Risk erkannt: Es ist nicht gleichmäßig über alle Mitarbeiter verteilt. Wir werden diesen Aspekt im nächsten Abschnitt näher beleuchten, aber lassen Sie uns zunächst unser Trio riskanter Verhaltensweisen mit Verstößen beim Surfen abschließen.

Abbildung 8: Modellierte Häufigkeit von Malware-Downloads/-Ausführungen



Browser-Verstöße

Browsing-Verstöße unterscheiden sich in zweierlei Hinsicht von Phishing- und Malware-Vorfällen.
Erstens haben sie im Allgemeinen keine direkten Auswirkungen auf die Sicherheit. Aber dieses Verhalten erhöht die Wahrscheinlichkeit, dass Mitarbeiter auf Malware stoßen, die in zwielichtigen (oder sogar legalen) Websites eingebettet ist, oder dass sie auf den neuesten Online-Betrug hereinfallen.

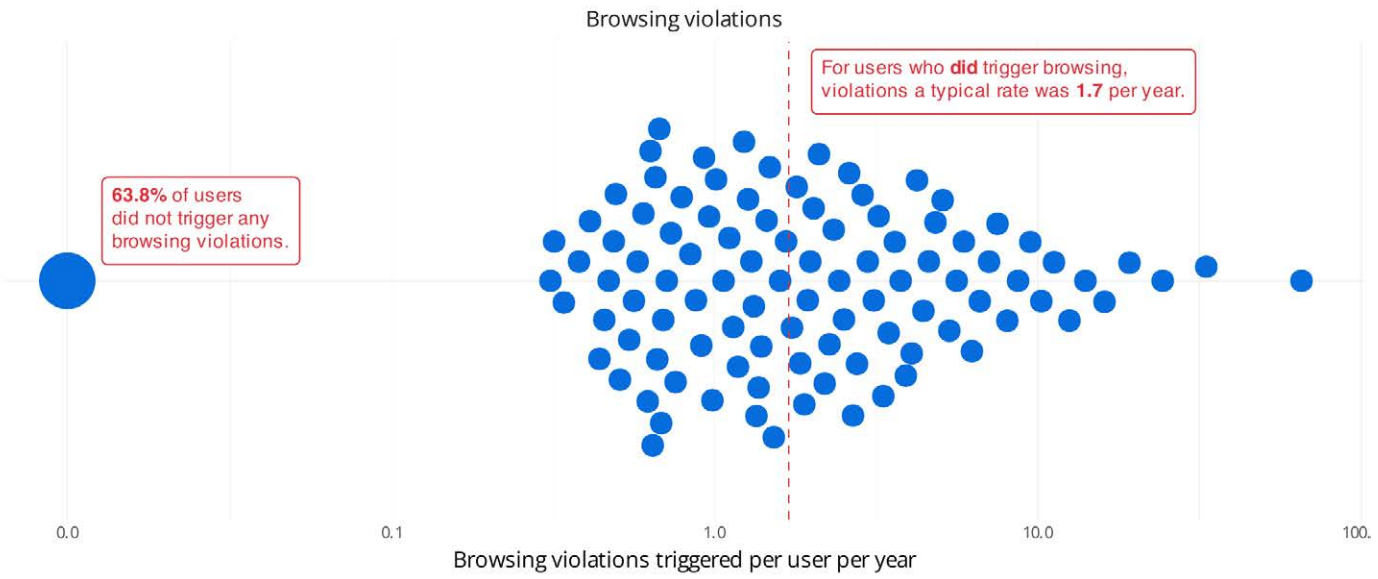
Zweitens: Während die Definition von Malware weitgehend objektiv ist, hängen Verstöße beim Surfen von den Richtlinien der einzelnen Organisationen ab. Was eine Organisation als „schlechte Website“ betrachtet, kann für andere völlig in Ordnung sein und umgekehrt.

Jeglicher Aufruf verstößt gegen die Unternehmensrichtlinien und ist daher unerwünscht, unabhängig vom Website-Inhalt.

Beobachtete Häufigkeit

Wie in Abbildung 1 zu sehen ist, sind Verstöße gegen das Browsing wesentlich häufiger als Phishing- und Malware-Vorfälle. Benutzer, die dieses Verhalten an den Tag legen, sind jedoch immer noch in der Minderheit - 64 % von ihnen haben in unserem Beobachtungszeitraum nie eine Verletzung ausgelöst. Die Mitarbeiter, die Verstöße beim Browsen protokollierten, verzeichneten im Durchschnitt weniger als zwei pro Jahr (siehe Abbildung 9 für die vollständige Verteilung).

Abbildung 9: Verteilung der Verstöße gegen die Browsing-Richtlinien pro Nutzer und Jahr

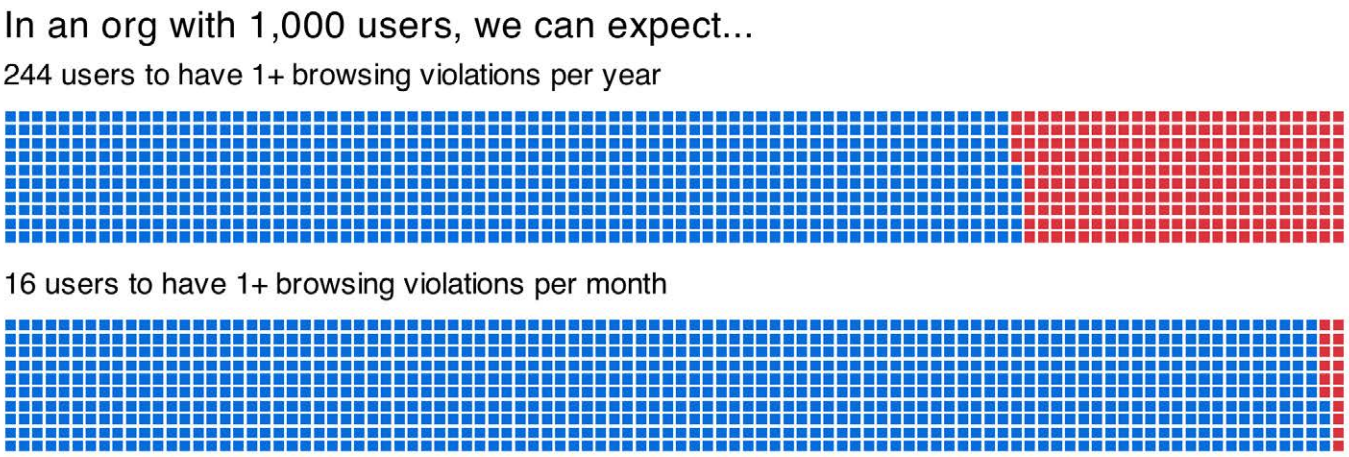


Erwartete Häufigkeit

Da es bei diesem Verhalten keinen Zwischenschritt wie das Klicken auf einen Phishing-Link oder das Ausführen eines Malware-Anhangs zu messen gibt, gehen wir direkt von der beobachteten zur erwarteten Häufigkeit über. Wir haben den gleichen Ansatz wie bei den beiden vorangegangenen Verhaltensweisen angewandt, um die Häufigkeit von Browsing-Verstößen zu modellieren und eine normalisierte Schätzung abzuleiten.

In einem Unternehmen mit 1.000 Mitarbeitern ist davon auszugehen, dass in einem Jahr 244 Benutzer gegen die Web-Browsing-Richtlinien verstoßen. Sechzehn dieser Mitarbeiter werden wahrscheinlich jeden Monat gegen die Browsing-Richtlinien verstoßen.

Abbildung 10: Modellierte Häufigkeit von Verstößen gegen die Browsing-Richtlinien



Wenn Risiko zur Gewohnheit wird

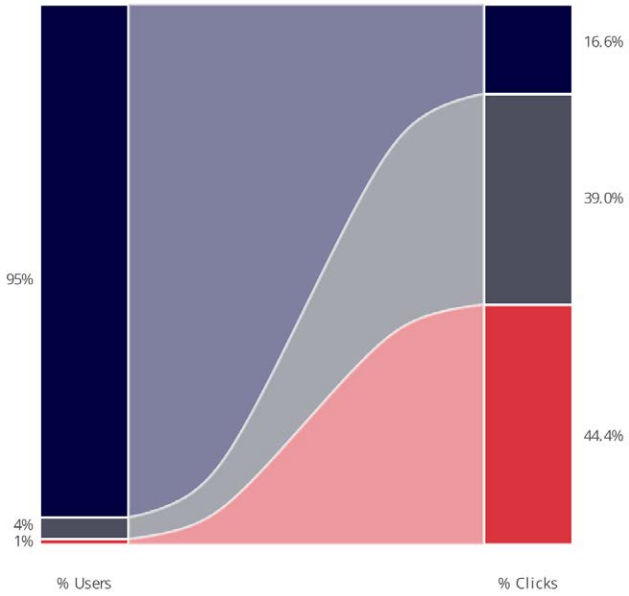
Im letzten Teil ist Ihnen vielleicht ein allgemeiner und wichtiger Trend aufgefallen: Die Mehrheit der Mitarbeiter halt sich von riskanten Verhaltensweisen fern, aber eine Teilmenge macht sie zur Gewohnheit. Einige Wiederholungstater tun immer wieder das Gleiche (z. B. durch Phishing angelockt), wahrend andere mehrere unerwunschte Verhaltensweisen an den Tag legen (Phishing, Herunterladen von Malware usw.). Schauen wir uns die verschiedenen Formen von Risikonutzern genauer an.

Wiederholtes risikoreiches Verhalten

Die nächsten beiden Diagramme zeigen, dass eine kleine Anzahl von Nutzern für einen ungewöhnlich großen Anteil an riskantem Verhalten verantwortlich sein kann. Das ist ein Grund zur Sorge für jeden, der mit Human Risk umgeht. Auf der anderen Seite bietet dies die Möglichkeit, durch die Änderung des Verhaltens einiger weniger Personen einen großen Einfluss auf die Risikoexposition zu haben.

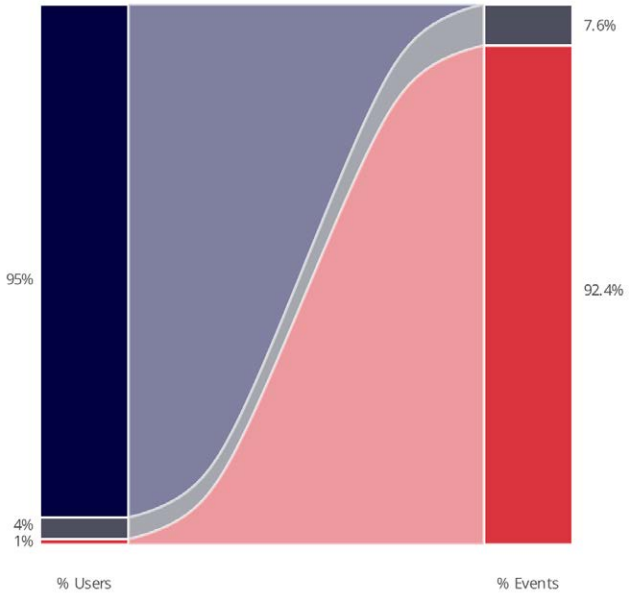
Wir haben uns entschieden, es hier nicht zu zeigen, aber Verstöße gegen das Browsing-Verhalten zeigen ein ähnliches, wenn auch nicht so ausgeprägtes, Muster der Dominanz durch wenige. Die oberen 5 % der risikobehafteten Browser haben 62 % aller Verstöße gegen die Browsing-Richtlinien verursacht. Wenn wir alle drei riskanten Verhaltensweisen (Phishing, Malware und Browsing) betrachten, sind 5 % der Nutzer für 75 % aller erkannten Vorfälle verantwortlich.

Abbildung 12: Phishing-Vorfälle bei Nutzern



- Nur 1 % der Nutzer sind für 44 % aller angeklickten Phishing-E-Mails verantwortlich. 5 % der Nutzer sind für 83,4 % aller Klicks verantwortlich.
- Die verbleibenden 95 % der Nutzer machen gemeinsam weniger als 17 % der erfolgreichen Phishing-Angriffe aus.

Abbildung 13: Malware-Vorfälle bei Nutzern



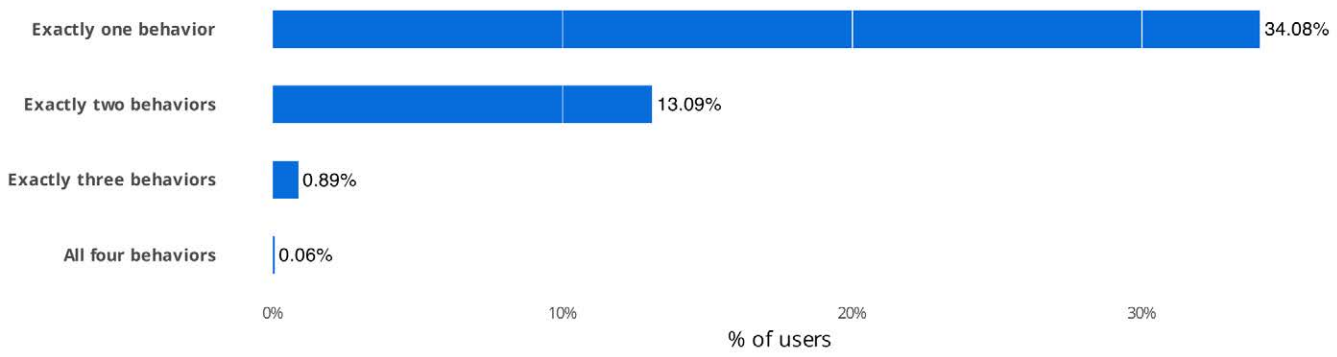
- 1 % der Nutzer sind für 92 % aller Malware-Vorfälle verantwortlich!
- 5 % der Nutzer sind für ALLE Malware-Vorfälle verantwortlich. Die verbleibenden
- 95 % hatten einen sauberen Verlauf. Malware ist deutlich stärker „unausgewogen“ als die anderen Vorfallarten.

Mehrfaches risikoreiches Verhalten

Nachdem festgestellt wurde, dass wenige Nutzer den Großteil der riskanten Vorfälle verursachen, stellt sich die Frage, ob dieselbe Nutzergruppe, die immer wieder auf Phishing-Angriffe hereinfällt, auch Malware herunterlädt und die Browsing-Richtlinien in hohem Maße verletzt. Werfen wir einen Blick darauf.

Unter den 48 % der Mitarbeitenden, die sich in irgendeiner Form riskanten Verhaltens gewidmet haben, beschränkten sich die meisten auf nur eine Art (Abbildung 14). Der Anteil der Nutzer, die in zwei Verhaltenskategorien auffielen, sinkt auf 13 %. Weniger als 1 % begingen Verstöße in drei oder mehr riskanten Verhaltensweisen.

Abbildung 14: Prozentsatz der Nutzer, die mehrere riskante Verhaltensweisen zeigen

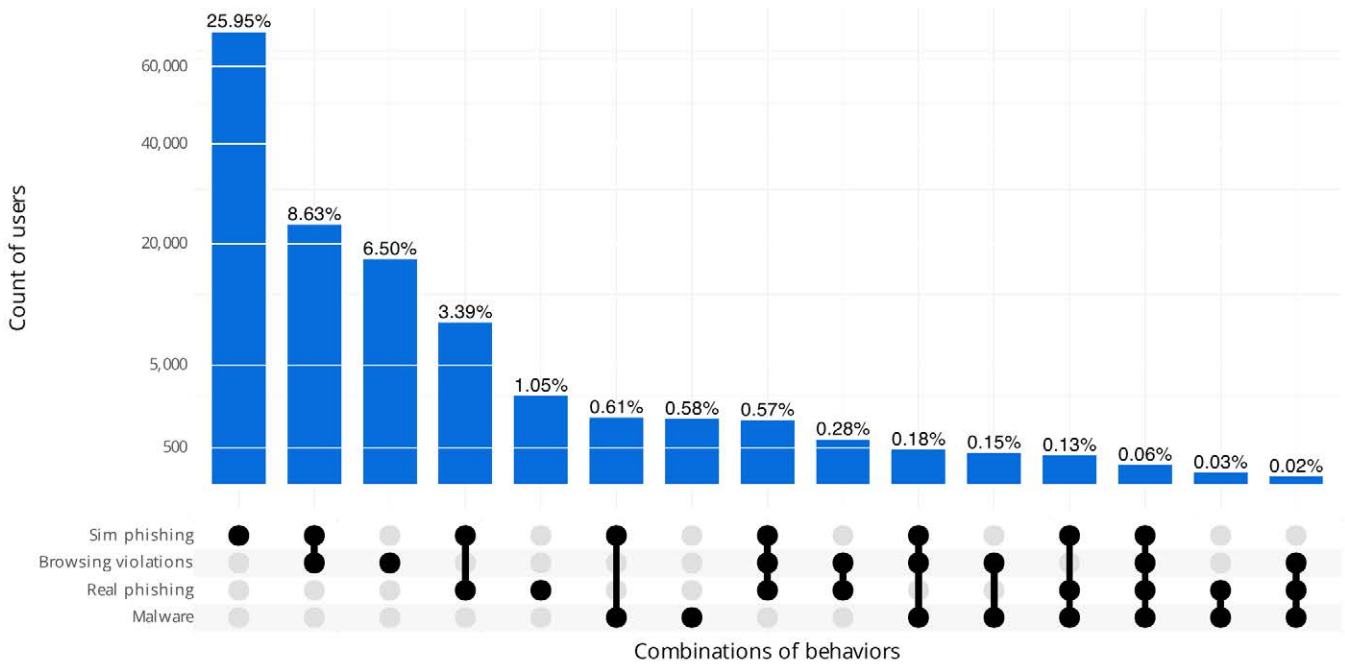


Nun fragen Sie sich vielleicht, welche Arten von Fehlverhalten tendenziell gemeinsam auftreten. Zumindest war das der nächste Gedankengang, der zur Erstellung des „UpSet“-Diagramms auf der nächsten Seite führte.

Abbildung 15 zeigt eine Aufschlüsselung der 48 % aller Mitarbeitenden in unserem Datensatz, die sich in irgendeiner Form unerwünschten Verhaltens gezeigt haben (die Balken für die 52 %, die einen sauberen Verlauf hatten, sind weggelassen). Leser könnten bestimmte Schnittmengen von Verhaltensweisen aus unterschiedlichen Gründen mehr oder weniger interessant finden. Wir möchten auf etwas hinweisen, das uns aufgefallen ist, und überlassen es Ihnen, Ihre eigenen Schlüsse zu ziehen.

Es ist nicht überraschend, dass der größte Balken echtes Phishing und simuliertes Phishing umfasst (3,39 %). Interessant ist, dass der zweitgrößte Balken die Nutzer betrifft, die echtes Phishing, aber nichts anderes verpasst haben (1,05 %). Alle Kombinationen, bei denen echtes, aber kein simuliertes Phishing verpasst wurde, machen 1,38 % aus. Das ist zwar nicht viel, aber auch nicht zu ignorieren. Warum entkommen diese Mitarbeitenden den Simulationen? Sind die simulierten Phishing-Nachrichten zu schwer?

Abbildung 15: Überschneidungen bei riskanten Verhaltensweisen unter Nutzern



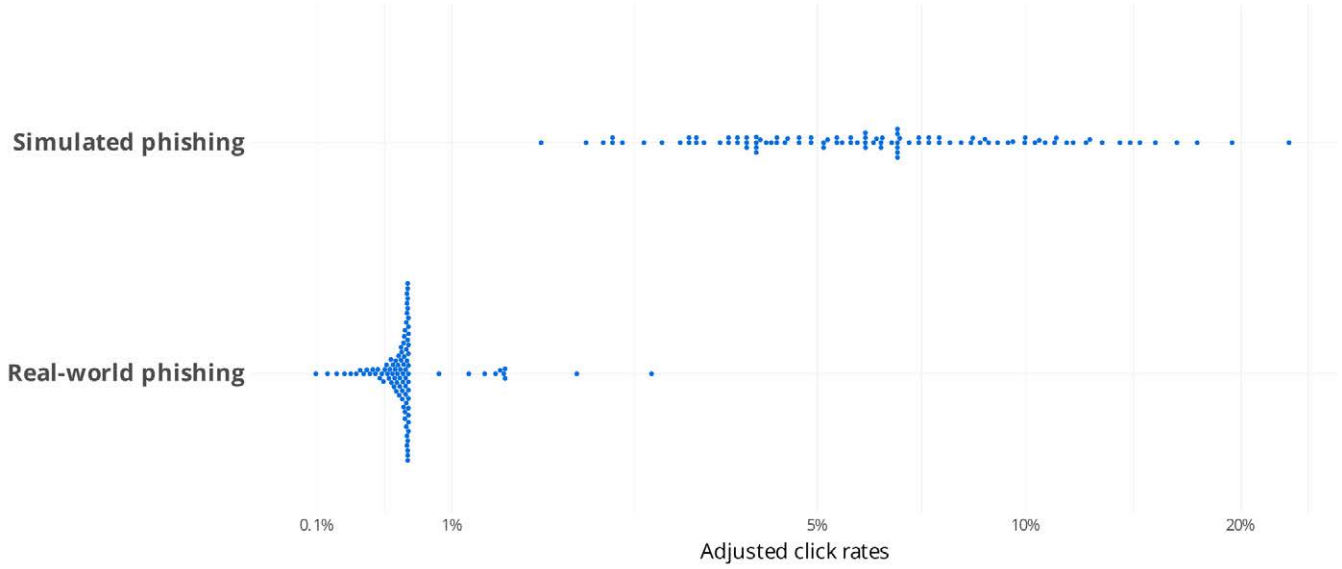
Sind simulierte Phishing-Nachrichten zu schwierig?

Die am Ende des vorherigen Absatzes gestellte Frage war nicht nur rhetorisch. Wir nehmen sie hier genauer unter die Lupe. Idealweise sollten regelmäßige simulierte Phishing-Tests alle Mitarbeitenden aufdecken, die anfällig dafür sind, auf den Köder hereinzufallen, damit sie lernen, bei echten Angriffen nicht zuzubeißen. Im Laufe der Zeit würden wir erwarten, dass die Klickraten bei simulierten und echten Phishing-Versuchen ähnlich sind, wenn die Tests die tatsächlichen Angriffe nachahmen. Doch genau das sehen wir in den Daten nicht.

Laut Abbildung 16 sind die Klickraten bei simulierten Phishing-Tests deutlich höher als bei realen Phishing-Angriffen. So sehr, dass ihre Verteilungen kaum überlappen (was von Statistikern als Hinweis darauf interpretiert wird, dass es sich um grundsätzlich unterschiedliche Dinge handelt).

Eine mögliche Erklärung für das, was wir hier sehen, ist, dass echte Phishing-Nachrichten für Mitarbeitende leichter erkennbar sind als ihre simulierten Pendants. Zumindest scheinen die Simulationen nicht gut kalibriert zu sein. Wir fragen uns, ob diese Diskrepanz die Mitarbeitenden in die Irre führen könnte, was echte Phishing-Nachrichten angeht, sodass Angreifer durch die Simulationen hindurchschlüpfen können.

Abbildung 16: Vergleich der Klickraten von Nutzern zwischen echten und simulierten Phishing-E-Mails



Risikonutzer: Ziel oder Täuschung?

Die letzten beiden Unterabschnitte haben sich auf Verhaltensweisen konzentriert, die dazu führen, dass einige Mitarbeitende ein höheres Risiko darstellen als andere. Aber beruht das Human Risk ausschließlich auf dem, was Nutzer tun? Oder gibt es auch einen Aspekt von „wer sie sind“, der das Risikoprofil eines Nutzers von dem eines anderen unterscheidet?

Die Phishing-Telemetrie von Mimecast bietet eine nützliche Perspektive, um diese Frage zu untersuchen, da wir das Empfangen von Phishing-E-Mails (Zielgerichtetheit) vom Akt des Hineinfallens und Klicken auf diese unterscheiden können. Wir beginnen mit einem rollenbasierten Vergleich dieser Messgrößen.

Laut Abbildung 17 sind Manager viel häufiger Ziel von Phishing-Angriffen als reguläre Mitarbeitende oder Auftragnehmer. Das spiegelt wahrscheinlich ihre öffentlichere Rolle und höhere Zugriffs- bzw. Einflussmöglichkeiten wider. Dennoch sind Manager am wenigsten geneigt, auf diese Phishing-Nachrichten zu klicken. Trotzdem zeigt die letzte Spalte, dass sie die höchste erwartete Rate erfolgreicher Phishing-Vorfälle (pro Nutzer, pro Jahr) haben. Es ist jedoch wichtig zu beachten, dass die höhere Zielgerichtetheit das Risikoprofil der Manager erhöht. Das deutet darauf hin, dass es effektiver sein könnte, sie vor diesen Angriffen zu schützen, anstatt zusätzliche Schulungen zu verlangen.

Abbildung 17: Vergleich der Phishing-Risiko-Metriken nach organisatorischen Rollen

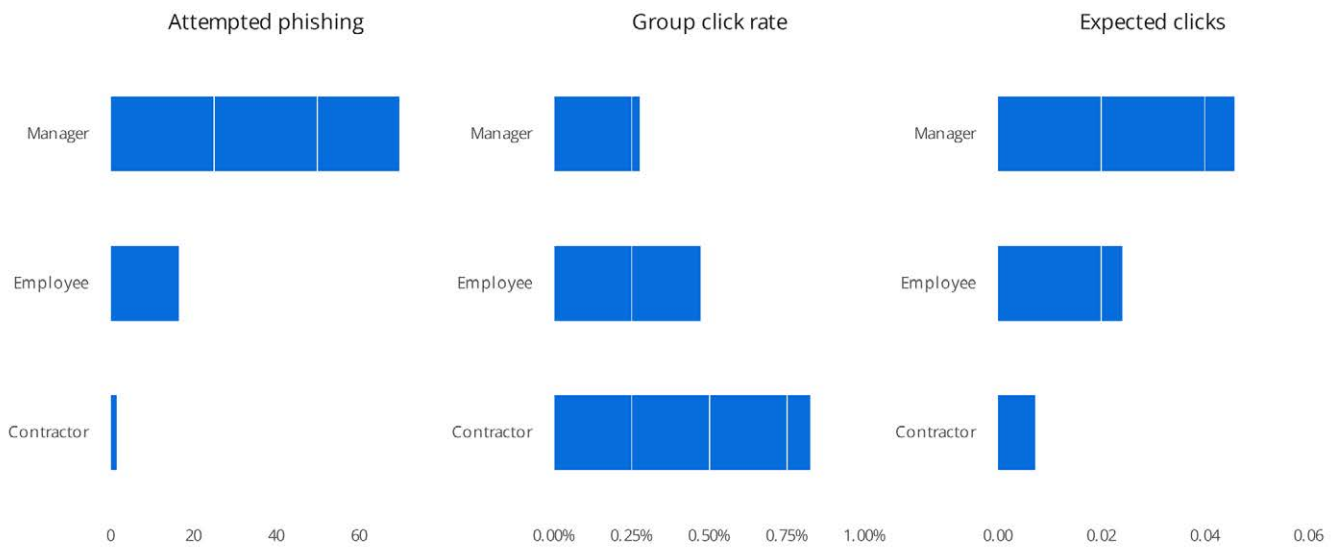
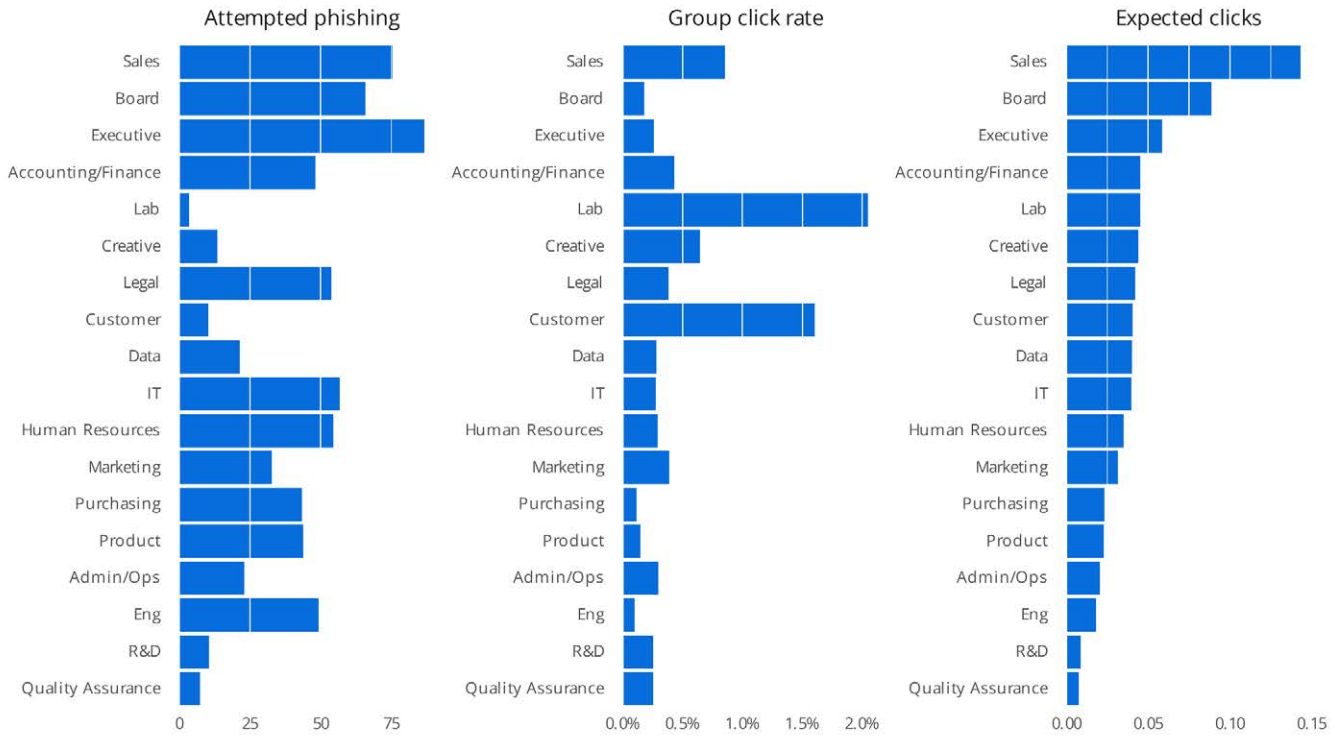


Abbildung 18 betrachtet risikobehaftete Rollen detaillierter, indem verschiedene organisatorische Abteilungen oder Funktionen miteinander verglichen werden. Basierend auf der vorherigen Grafik ist es nicht überraschend, dass Führungskräfte die meisten Phishing-E-Mails erhalten. Doch auch der Vertrieb und der Vorstand stehen in dieser Hinsicht nicht weit zurück. All diese Rollen sind häufig öffentlich sichtbar, was sie auf den Radar der Phisher bringt. Obwohl diese Rollen tendenziell niedrige bis durchschnittliche Klickraten aufweisen, übersteigt die Wahrscheinlichkeit, dass sie erfolgreich gephisht werden, die aller anderen.

Laborangestellte sind ein hervorragendes Beispiel für die Unterscheidung zwischen „zielgerichtet“ und „getäuscht“. Sie erhalten die wenigsten Phishing-E-Mails, klicken jedoch am wahrscheinlichsten darauf. Kunden zeigen ein ähnliches Muster. Dies macht sie zu idealen Kandidaten für gut gestaltete Schulungen oder Phishing-Simulationen, um die Klickraten zu senken und ihr gesamtes Risikoprofil zu verringern.

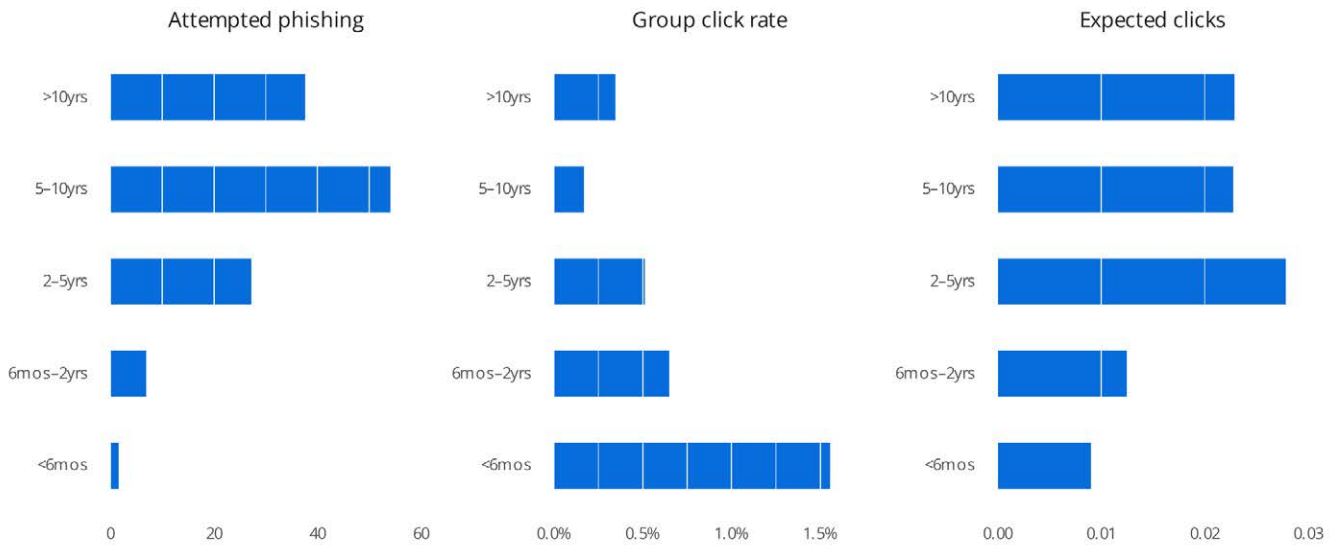
Abbildung 18: Vergleich der Phishing-Risiko-Metriken zwischen Abteilungen



Zu guter Letzt wollen wir uns ansehen, wie die Betriebszugehörigkeit das Risikoprofil eines Mitarbeiters beeinflusst. Die kurze Version lautet: Je länger man im Unternehmen ist, desto häufiger wird man Ziel von Phishing-Angriffen. Das hängt wahrscheinlich damit zusammen, dass Firmen-E-Mail-Adressen mit der Zeit immer mehr in die Kontaktlisten von Cyberkriminellen aufgenommen werden.

Die Klickraten zeigen einen gegenteiligen Trend: Die neuesten Mitarbeitenden lassen sich am leichtesten täuschen. In Bezug auf erfolgreiche Angriffe scheint eine Betriebszugehörigkeit von zwei Jahren ein Wendepunkt zu sein, ab dem das erwartete Risiko sich verdoppelt. Wie bei Managern liegt dies an der erhöhten Zielgerichtetheit gegenüber erfahreneren Mitarbeitenden, wobei jedoch mehr Schulungen das Risiko wahrscheinlich nicht ausgleichen können.

Abbildung 19: Vergleich der Phishing-Risiko-Metriken nach Betriebszugehörigkeit beim aktuellen Arbeitgeber



ZUSAM-MENFAS SUNG

Cybersicherheit geht nicht mehr nur darum, externe Sicherheitslücken zu verhindern, sondern auch die Risiken zu managen, die von innen kommen. Indem sie das Human Risk verstehen und mindern, können

Trotz des „Cyber"-Präfixes beginnt und endet Cybersicherheit mit den Menschen. Menschliches Verhalten bleibt eine bedeutende Schwachstelle, selbst in den sichersten Umgebungen. Die Daten verdeutlichen, dass fast die Hälfte der Mitarbeitenden riskante Verhaltensweisen zeigt, die ihre Organisationen Phishing, Malware und anderen Cyberbedrohungen aussetzen. Dieses anhaltende Human Risk stellt eine Herausforderung für Cybersicherheitsverantwortliche dar, bietet aber gleichzeitig auch eine Gelegenheit. Cybersicherheitsverantwortliche müssen daher einen proaktiven, menschenzentrierten Ansatz zur Risikominderung verfolgen. Dies erfordert, über grundlegende Bewusstseinsschulungen hinauszugehen und den Fokus auf Verhaltensänderungen durch gezielte, kontinuierliche Weiterbildung und Verstärkung zu legen. Wie in der Mimecast-Studie gezeigt, konzentrieren sich wiederholte riskante Verhaltensweisen oft auf einen kleinen Prozentsatz von Mitarbeitenden. Diese kleine Gruppe ist für die Mehrheit der Sicherheitsvorfälle verantwortlich.

Gezielte Maßnahmen für diese hochriskanten Nutzer sind entscheidend.

Cybersicherheits-verantwortliche sollten einen datengestützten Ansatz implementieren, um diese Personen zu identifizieren, zu erreichen und zu schulen.

Dies beinhaltet:

1

Nutzung von risikospezifischen Schulungen und Maßnahmen

Nutzung von Verhaltensanalytik, um gezielte Schulungen für Mitarbeitende mit wiederholten riskanten Verhaltensweisen anzubieten, insbesondere für Führungskräfte und Vertriebsteams.

2

Erhöhung der Risiko-Sichtbarkeit

Die nutzerbasierte Risikoanalyse sollte mehr umfassen als nur Phishing-Simulationen. Diskrepanzen in den Simulationen können deren Effektivität verringern. Es sollte auch andere verhaltensbasierte Daten in die Bewertung des Human Risk einfließen.

3

Entwickle rollenbasierte Schutzmaßnahmen

Da bestimmte Rollen (z. B. Führungskräfte, Vertrieb, Vorstandsmitglieder) stärker ins Visier genommen werden, sollten zusätzliche Schutz- und Überwachungsebenen für diese Personen eingesetzt werden. Dazu gehört auch, ihre Exposition in öffentlich sichtbaren Situationen zu verringern.

4

Ein ganzheitliches Frame-work für Human Risk Management

Sicherheitstechnologien sollten mit einer menschenzentrierten Strategie kombiniert werden, die kontinuierliche Beteiligung und Verantwortung fördert. Mimecast's KI-gestützte Human Risk Management Plattform zeigt, wie Technologie die Sichtbarkeit erhöhen und Maßnahmen zur Risikominderung unterstützen kann.

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.

www.mimecast.com

Über Cyentia Institute

Das Cyentia Institute ist ein Forschungs- und Datenanalyseunternehmen, das darauf abzielt, das Wissen und die Praxis der Cybersicherheit voranzutreiben. Cyentia verfolgt dieses Ziel durch datengestützte Studien wie diese und ein wachsendes Portfolio an Analyse-Dienstleistungen.

www.cyentia.com