SOPHOS

Cybersecurity-Report 2023: Der Business Impact von Cyberangriffen

Ergebnisse einer unabhängigen Befragung von 3.000 IT-/Cybersecurity-Entscheidern aus 14 Ländern im Januar und Februar 2023.

Sophos-Whitepaper, April 2023

Vorgehensweise

Um die tatsächlichen Auswirkungen der Cybersecurity auf Unternehmen im Jahr 2023 zu beleuchten, hat Sophos eine unabhängige Befragung von 3.000 IT-/Cybersecurity-Entscheidern in 14 Ländern in Auftrag gegeben. An der Umfrage nahmen Unternehmen und Einrichtungen mit 100 bis 5.000 Mitarbeitern teil. Die Umfrage wurde von Vanson Bourne zwischen Januar und Februar 2023 durchgeführt.

3.000
IT-Entscheider

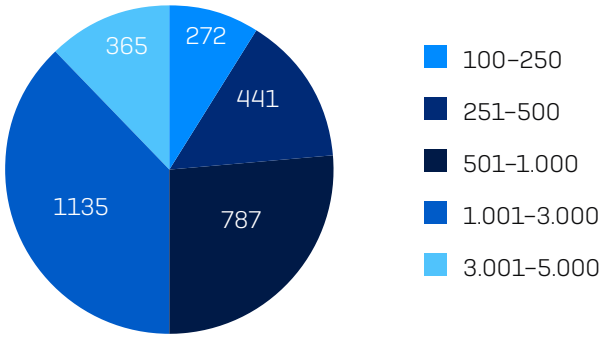
100-5.000
Mitarbeiter

14
Länder

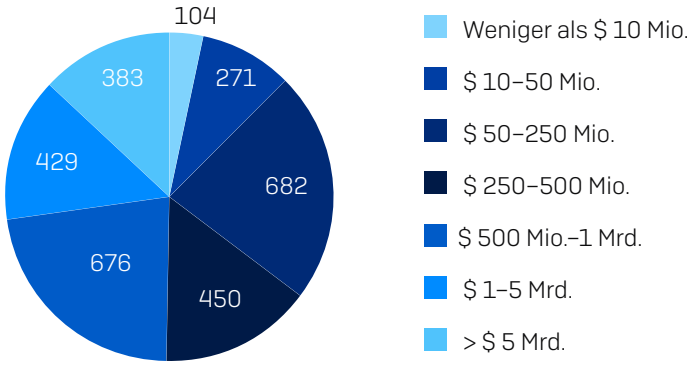
< $10 Mio.–$ 5 Mrd. +
Jahresumsatz

Jan/Feb 23
Befragung durchgeführt

Befragte nach Unternehmensgröße (Mitarbeiterzahl)



Befragte nach Unternehmensgröße (Jahresumsatz)



Befragte nach Land

LAND	ANZAHL DER BEFRAGTEN	LAND	ANZAHL DER BEFRAGTEN
Vereinigte Staaten	500	Vereinigtes Königreich	200
Deutschland	300	Südafrika	200
Indien	300	Frankreich	150
Japan	300	Spanien	150
Australien	200	Österreich	100
Brasilien	200	Singapur	100
Italien	200	Schweiz	100

Zusammenfassung

Situation: Unternehmen können mit der Geschwindigkeit der Angreifer nicht mithalten

Wie aus der Umfrage hervorgeht, bewegen sich Angreifer in einer anderen Geschwindigkeit als Unternehmen mit Ihren IT-Teams. Dank Automatisierung, Cybercrime-as-a-Service-Modellen, Identitätstäuschung und ihrer Anpassungsfähigkeit können Cyberkriminelle eine Vielzahl an großangelegten, komplexen Angriffen immer schneller durchführen. 94 % der Umfrageteilnehmer waren im vergangenen Jahr von Cyberangriffen betroffen. Daher sollten Unternehmen jeder Größe davon ausgehen, dass sie auch im Jahr 2023 im Visier von Angreifern stehen.

Aufgrund des Fachkräftemangels, einer Flut von Warnmeldungen und der zeitaufwändigen Reaktion auf Vorfälle sind Unternehmen nicht mehr in der Lage, mit den Angreifern Schritt zu halten. Die Bedrohungserkennung und -reaktion gestalten sich für die meisten Unternehmen schwierig. Für 93 % der befragten Unternehmen stellen auch grundlegende Sicherheitsaufgaben eine Herausforderung dar.

Die Analyse von Sicherheitswarnungen wird für viele Unternehmen zum Problem. Im Schnitt wird nur knapp die Hälfte (48 %) aller Warnmeldungen daraufhin untersucht, ob es sich um Anzeichen für bösartige Aktivitäten handelt. Zudem fällt es den meisten Unternehmen schwer, die zu untersuchenden Warnmeldungen/Ereignisse zu ermitteln (71 %) sowie zu priorisieren (71 %). Der gesamte Prozess der Erkennung, Analyse und Reaktion auf Warnmeldungen dauert bei Unternehmen mit 100 bis 3.000 Mitarbeitern durchschnittlich 9 Stunden, bei Unternehmen mit 3.001 bis 5.000 Mitarbeitern sogar bis zu 15 Stunden.

Im operativen Bereich mangelt es den Unternehmen an Vertrauen in ihre Prozesse, wobei die Fehlkonfiguration von Sicherheitstools im Jahr 2023 als das größte Sicherheitsrisiko wahrgenommen wird. Mehr als die Hälfte (52 %) der IT-Experten räumt ein, dass sie nicht mehr in der Lage ist, den zunehmend komplexen Cyberangriffen ohne Unterstützung von außen Herr zu werden. Bei kleinen Unternehmen (100–250 Mitarbeiter) liegt der prozentuale Anteil sogar bei 64 %.

Business Impact: Die Situation hat finanzielle, betriebliche und personelle Konsequenzen

Der Geschwindigkeitsvorsprung von Angreifern hat beträchtliche Auswirkungen auf das gesamte Unternehmen. Die direkten finanziellen Folgen eines Cybervorfalls sind beträchtlich: Die durchschnittlichen Kosten für die Bereinigung eines Ransomware-Angriffs belaufen sich in kleineren und mittleren Unternehmen auf 1,4 Mio. US-Dollar.[1] Bereinigungskosten sind jedoch nur ein Teil des Problems.

Die Kapazitäten für die Umsetzung von IT-Programmen werden eingeschränkt. So geben 55 % der befragten Unternehmen an, dass der mit Cyberbedrohungen verbundene Zeitaufwand die Arbeit des IT-Teams an anderen Projekten beeinträchtigt. Die Dringlichkeit und Unvorhersehbarkeit erforderlicher Cybersecurity-Maßnahmen bremsen andere Projekte aus: 64 % der befragten Unternehmen würden sich wünschen, dass IT-Teams mehr Zeit für strategische Projekte statt für fieberhafte Akutmaßnahmen aufwenden könnten.

Darüber hinaus sind die Analyse und Behebung von Sicherheitswarnmeldungen mit einem erheblichen finanziellen und personellen Aufwand verbunden.

Zudem ist die Situation sehr belastend für die Mitarbeiter. 57 % der IT-Experten geben an, dass die Sorge, das Unternehmen könnte von einem Cyberangriff betroffen sein, ihnen manchmal schlaflose Nächte bereite. Bei Unternehmen mit 3.001 bis 5.000 Mitarbeitern sind es sogar 65 %. Auch die Kosten, die mit der Anwerbung, Schulung und Bindung von Fachpersonal einhergehen, sind für Unternehmen eine Herausforderung.

1 The State of Ransomware 2022, Sophos

Empfehlung: Beschleunigen Sie Ihre Abwehr und überholen Sie die Angreifer

Unternehmen benötigen eine umfassende, klare Strategie, um Angreifer im Jahr 2023 im Cybersecurity-Wettlauf zu überholen. Zunächst müssen Unternehmen skalierbare Prozesse für die Reaktion auf Vorfälle einführen. Dabei gilt es, die Angriffsfläche zu reduzieren und die Anzahl der Warnungen, die Maßnahmen erfordern, zu minimieren. Spezielle Incident-Response-Services helfen dabei, Reaktionszeiten zu optimieren.

Als Nächstes müssen sie eine adaptive Abwehr umsetzen, die sich automatisch an die jeweilige Situation anpasst. So werden die Angreifer ausgebremst. Dies wiederum verschafft Security-Teams Zeit, auf Bedrohungen zu reagieren.

Schließlich gilt es, Technologien und menschliches Know-how zu kombinieren, um noch schneller und effizienter reagieren zu können. So verschaffen sich Unternehmen einen Geschwindigkeitsvorsprung.

Ein wesentlicher Erfolgsfaktor ist dabei die Zusammenarbeit mit externen Spezialisten. Das Gros der Unternehmen setzt auch bereits auf ein hybrides Cybersecurity-Konzept. 94 % arbeiten mit externen Spezialisten zusammen, um ihre Cybersicherheit zu skalieren. Da Angreifer zunehmend professionell vorgehen, wird die Zusammenarbeit mit Bedrohungsspezialisten immer wichtiger.

Wichtigste Erkenntnisse

94 % der Unternehmen waren im vergangenen Jahr von Cyberangriffen betroffen

Datenexfiltration gilt als zentrales Sicherheitsproblem in 2023

93 % der Unternehmen erachten grundlegende Sicherheitsaufgaben als Herausforderung

48 % aller Sicherheitswarnungen werden analysiert

15 Stunden beträgt die durchschnittliche Reaktionszeit auf Warnmeldungen in Unternehmen mit 3.001–5.000 Mitarbeitern

Fehlkonfiguration von Sicherheitstools wird als das größte Sicherheitsrisiko in 2023 wahrgenommen

52 % können komplexe Cyberbedrohungen nicht selbst bewältigen

55 % geben an, dass der mit Cyberbedrohungen verbundene Zeitaufwand die Arbeit des IT-Teams an anderen Projekten beeinträchtigt

64 % der befragten Unternehmen würden sich wünschen, dass IT-Teams mehr Zeit für strategische Projekte statt für fieberhafte Akutmaßnahmen aufwenden könnten

57 % der IT-Experten bereitet die Sorge, das Unternehmen könnte von einem Cyberangriff betroffen sein, schlaflose Nächte

Cyberbedrohungen 2023: Reale Erfahrungen aus erster Hand

Hauptsorgen in der Cybersecurity in 2023

99 % der IT-Experten befürchten, dass ihr Unternehmen in 2023 von Cyberbedrohungen betroffen sein könnte. Datenexfiltration (Diebstahl durch externe Angreifer) führt die Liste der Bedrohungen an, die IT-Experten als eine ihrer Hauptsorgen einstufen, gefolgt von Phishing (einschließlich Spear-Phishing). Ransomware steht an dritter Stelle.

Diese drei Bedrohungen sind häufig miteinander verknüpft: Angriffe gehen nicht selten von einer Phishing-E-Mail aus und führen zu Datenexfiltration und Ransomware.

CYBERBEDROHUNG	BEFRAGTE, FÜR DIE DIES EINE HAUPTSORGE IST
Datenexfiltration (Diebstahl durch externe Angreifer)	41 %
Phishing (inkl. Spear-Phishing)	40 %
Ransomware	35 %
Cyber-Erpressung	33 %
Denial-of-Service-Angriffe (DDoS)	32 %
Business Email Compromise	31 %
Aktive Angreifer (manuelles Hacking)	30 %
Mobilgeräte-Malware	30 %
Cryptominer	22 %
Wiper	16 %
Sonstige Produkte	0 %
Ich mache mir keine Sorgen darüber, dass mein Unternehmen in 2023 von Cyberbedrohungen betroffen sein könnte	1 %
Unsicher	0 %

Welche Cyberbedrohungen stufen Sie in 2023 als Hauptsorge für Ihr Unternehmen ein? (Anzahl=3.000)

Großangelegte Hackerangriffe sind an der Tagesordnung

Die Hauptsorgen von IT-Entscheidern spiegeln die Realität wider: 94 % aller Unternehmen verzeichneten im vergangenen Jahr mindestens einen Cyberangriff. Ransomware war die Angriffsart, die am häufigsten genannt wurde, doch Cyberkriminelle führen eine Vielzahl verschiedenster Angriffe aus. In ihrem Ausmaß und ihrer Komplexität stellen Cyberangriffe Unternehmen vor immer größere Herausforderungen.

Hinter diesen Zahlen verbirgt sich eine zunehmende Kommerzialisierung der Cyberkriminalität. Das Geschäftsmodell „Cybercrime-as-a-Service" („Access-as-a-Service", „Phishing-as-a-Service", „Scamming-as-a-Service" usw.) boomt. Diese Entwicklung erleichtert den Einstieg in die Cyberkriminalität. [Mehr zu diesem Thema erfahren Sie im Sophos Threat Report 2023.]

Cyberangriffe ohne Ransomware und prozentualer Anteil der betroffenen Unternehmen

27 %	**27 %**	**26 %**
Schad-E-Mails	Phishing (inkl. Spear-Phishing)	Datenexfiltration (nach Angreifer)
24 %	**24 %**	**21 %**
Cyber-Erpressung	Business Email Compromise	Mobilgeräte-Malware
18 %	**24 %**	**14 %**
CryptoMining	Denial of Service (DDoS)	Wiper

Aktive Angreifer gehören mittlerweile zum Alltag

23 %
waren im letzten Jahr Opfer eines aktiven Angriffs

30 %
zählen aktive Angreifer zu ihren Hauptsorgen in der Cybersecurity in 2023

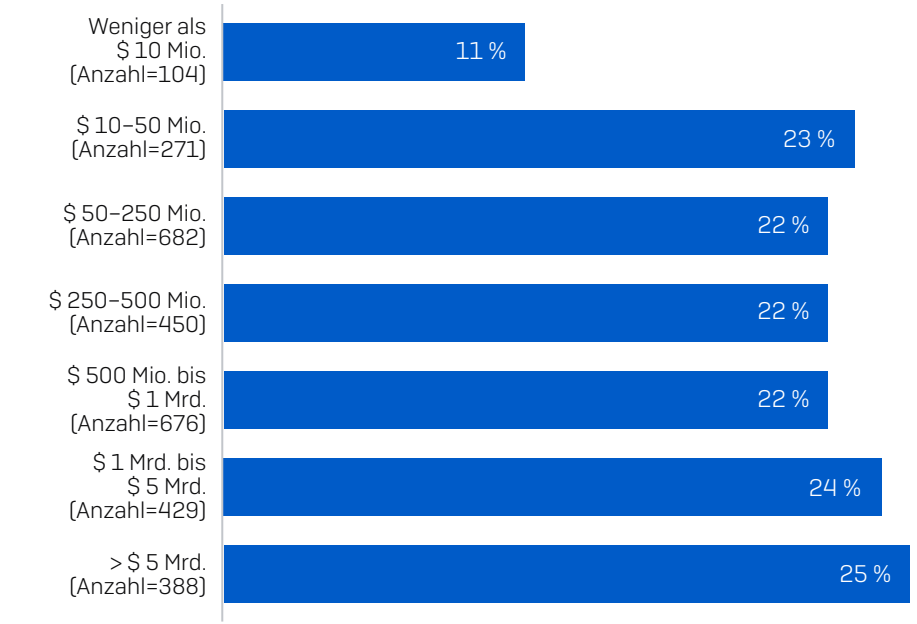
Aktive Angreifer passen ihre Techniken, Taktiken und Prozesse (TTPs) in Echtzeit an Abwehrmaßnahmen von Sicherheitstechnologien und Bedrohungsexperten an, um unerkannt zu bleiben. Diese manuellen Angriffe führen oft zu verheerenden Ransomware-Angriffen und Sicherheitsvorfällen und lassen sich nur sehr schwer stoppen.

23 % der Unternehmen waren im vergangenen Jahr Opfer von einem aktiven Angriff. Das Angriffsaufkommen war bei Unternehmen aller Größen relativ gleich hoch und variierte lediglich um zwei Prozentpunkte.

Interessanterweise meldeten nur 11 % der Unternehmen mit einem Jahresumsatz von weniger als 10 Millionen US-Dollar aktive Angriffe. Möglicherweise ist dies ein Indiz dafür, dass sich aktive Angreifer bewusst auf besonders lukrative Ziele konzentrieren. Die Erkennung aktiver Angreifer erfordert fundiertes Expertenwissen. Zudem ist die tatsächliche Zahl der Vorfälle aller Wahrscheinlichkeit nach höher.

Mit Hinblick auf die potenziell verheerenden Auswirkungen dieser Angriffe geben 30 % der Befragten an, dass sie aktive Angreifer als eine der besorgniserregendsten Cyberbedrohungen in 2023 einstufen.

Aktive Angriffe nach Umsatz

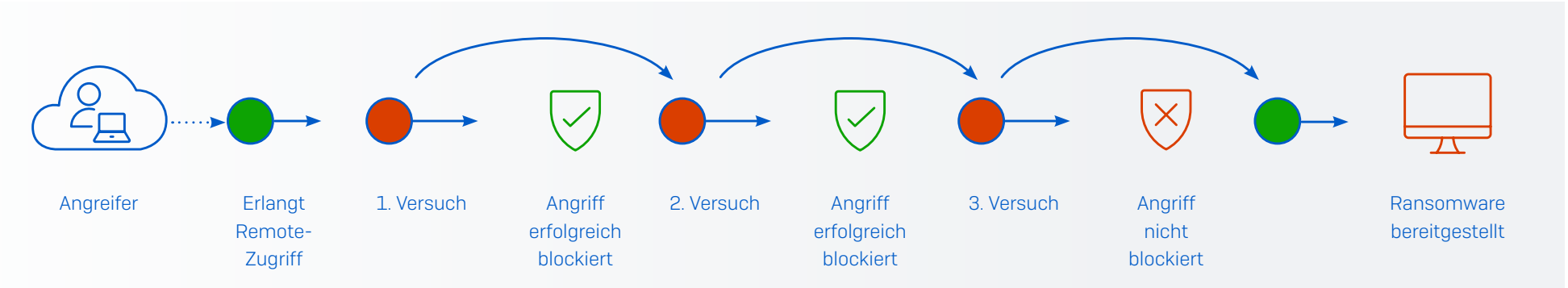


War Ihr Unternehmen im letzten Jahr von einem oder mehreren Cyberangriffen betroffen? Ja – von aktiven Angreifern (manuellem Hacking)

Aktive Angreifer verstehen

Aktive Angreifer stellen die Cyberabwehr-Teams vor eine schwer lösbare Aufgabe: Es reicht nicht aus, sie einfach nur zu blockieren. Diese versierten, hartnäckigen Bedrohungsakteure bedienen sich unterschiedlicher Techniken, Taktiken und Prozesse und verfolgen dabei unter anderem folgende Ziele:

- Ausnutzen von Sicherheitslücken (gestohlene Zugangsdaten, ungepatchte Schwachstellen und Fehlkonfigurationen von Sicherheitstools), um die Unternehmensabwehr zu überlisten und sich lateral im Netzwerk zu bewegen
- Zweckentfremden legitimer IT-Tools, um keine Erkennungen auszulösen
- Anpassen ihrer Angriffe in Echtzeit an Sicherheitskontrollen und Ausweichen auf neue Techniken, bis sie ihre Ziele erreichen



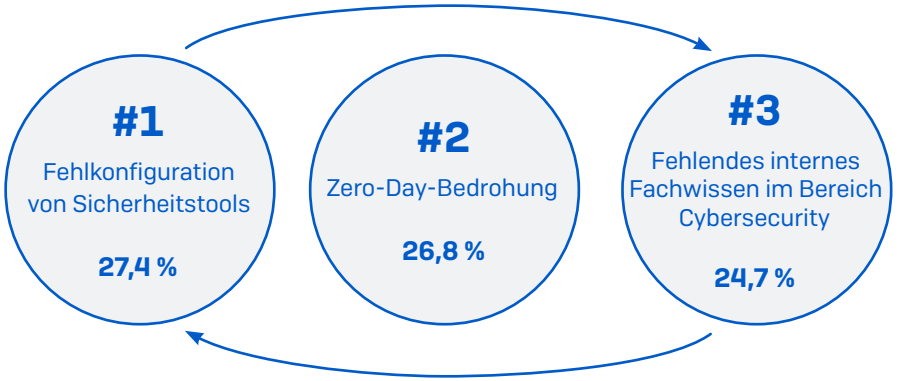
Cybersecurity 2023: Die Situation im Bereich Cyberabwehr

Größte Cyberrisiken

Die Fehlkonfigurationen von Sicherheitskontrollen (z. B. Endpoint- oder Firewall-Lösung) wird besonders häufig als Sicherheitsrisiko eingestuft: 27,4 % der Unternehmen zählen sie zu den drei größten Risiken. Sicherheitskontrollen müssen immer korrekt konfiguriert und bereitgestellt werden, denn Angreifer können Lücken in der Abwehr eines Unternehmens sofort ausnutzen.

Zero-Day-Angriffe, d. h. Angriffe, die bisher unbekannte Schwachstellen oder Softwarefehler ausnutzen, stehen an zweiter Stelle. 26,8 % stufen sie als eines der drei größten Sicherheitsrisiken ein. Auf dem dritten Platz (25 %) liegt fehlendes internes Fachwissen im Bereich Cybersecurity.

Es besteht ein direkter Zusammenhang zwischen mangelndem Know-how und der Fehlkonfiguration von Sicherheitstools: Wenn Unternehmen nicht die Zeit, das Know-how und die Erfahrung haben, Sicherheitskontrollen richtig zu konfigurieren, entstehen Lücken in der Abwehr.



CYBERSECURITY-RISIKO	EINSTUFUNG ALS EINE DER DREI HAUPTSORGEN IN PROZENT
Fehlkonfigurationen von Sicherheitskontrollen (z. B. Endpoint- oder Firewall-Lösung)	27 %
Zero-Day-Bedrohungen (Bedrohung, die sich einer bisher unbekannten Angriffstechnik bedient).	27 %
Fehlendes internes Fachwissen im Bereich Cybersecurity	25 %
Gestohlene Zugangsdaten und Anmeldeinformationen	24 %
Ungeschützte Geräte (einschl. unbekannter Geräte)	24 %
Mangel an Cybersecurity-Tools	23 %
Ungepatchte Sicherheitslücken	22 %
Remote-Zugriff von Benutzern	20 %
Unsichere WLANs	20 %
Interne Benutzer (versehentlich)	18 %
Partner/Lieferkette	18 %
Remote-Access-Tools	18 %
Interne Benutzer (absichtlich)	17 %
IoT-Geräte	17 %
Sonstige Produkte	0 %
Nichts davon stellt ein Cybersecurity-Risiko für mein Unternehmen dar	0 %
Unsicher	0 %

Wer/was sind Ihrer Meinung die drei größten Cybersecurity-Risiken für Ihr Unternehmen? Kombination von Antworten auf den Rängen 1–3 (Anzahl=3.000)

Unterschiedlicher Umgang mit Warnmeldungen

Unternehmen untersuchen **48 % aller Sicherheitswarnungen** auf Anzeichen schädlicher Aktivitäten

Eine der Herausforderungen, mit der Unternehmen zu kämpfen haben, ist die Frage, welchen Warnmeldungen sie nachgehen sollen und wie sie ihre begrenzten Ressourcen optimal einsetzen können.

Im Schnitt wird knapp die Hälfte (48 %) aller Sicherheitswarnungen daraufhin untersucht, ob es sich um Anzeichen schädlicher Aktivitäten handelt. Bei Unternehmen mit 3.001 bis 5.000 Mitarbeitern sind es 54 %. Bei der Vorgehensweise lassen sich jedoch signifikante Diskrepanzen feststellen: 16 % der Unternehmen untersuchen mehr als drei Viertel aller Warnmeldungen (davon gehen 5 % allen Warnmeldungen nach) und 18 % untersuchen ein Viertel oder weniger.

Im Branchenvergleich gehen Bundesbehörden prozentual den wenigsten Warnmeldungen nach (39 %) (Anzahl=89), Unternehmen aus dem Energie-, Öl/Gas- und Versorgungssektor den meisten (55 %) (Anzahl=69).

Kosten für die Erkennung, Analyse und Reaktion

Die durchschnittliche Reaktionszeit auf Warnmeldungen beträgt in Unternehmen mit 100–3.000 Mitarbeitern 9 Stunden, bei Unternehmen mit 3.001 bis 5.000 Mitarbeitern sogar bis zu 15 Stunden. Vermutlich ist dies auf die komplexeren Betriebsumgebungen zurückzuführen.

Im Branchenvergleich zeigen sich beträchtliche Unterschiede. Produktions- und Fertigungsunternehmen benötigen mit 15 Stunden und Energie-, Öl/Gas- und Versorgungsunternehmen mit 18 Stunden mehr als doppelt so lange wie Unternehmen in den Bereichen IT, Technologie und Telekommunikation (6,75 Stunden).

Dabei werden bei den meisten Warnmeldungen jedoch keine Reaktionsmaßnahmen ergriffen. Sicherheitstechnologien blockieren die meisten Angriffe proaktiv. Dabei wird ein Teil der Warnmeldungen klassifiziert und analysiert. Je nach Vorfall variieren die ergriffenen Reaktionsmaßnahmen stark: vom Löschen einer Phishing-E-Mail aus dem Posteingang von Mitarbeitern bis hin zur Wiederherstellung einer gesamten Serverfarm.

Durchschnittliche Reaktionszeit auf Warnmeldungen

AKTIVITÄT	100–3.000 MITARBEITER (Anzahl=2.460)	3.001–5.000 MITARBEITER (Anzahl=350)	IT, TECHNOLOGIE UND TELEKOMMUNIKATION (Anzahl=98)	FERTIGUNG UND PRODUKTION (Anzahl=331)	ENERGIE, ÖL/GAS UND VERSORGUNGSUNTERNEHMEN (Anzahl=66)
Erkennung	3 Stunden	3 Stunden	1,5 Stunden	3 Stunden	6 Stunden
Analyse	3 Stunden	6 Stunden	2,25 Stunden	6 Stunden	6 Stunden
Reaktion	3 Stunden	6 Stunden	3 Stunden	6 Stunden	6 Stunden
Gesamt	**9 Stunden**	**15 Stunden**	**6,75 Stunden**	**15 Stunden**	**18 Stunden**

Wie viel Zeit benötigt Ihr Unternehmen, um einen potenziellen Vorfall zu erkennen, zu analysieren und gegebenenfalls zu beheben? (Anzahl=2.812 Unternehmen, die Warnmeldungen intern analysieren)

Fehlendes Fachwissen im Bereich Cybersecurity

Wie bereits erwähnt, betrachten IT-Experten fehlendes internes Fachwissen im Bereich Cybersecurity als eines der größten Sicherheitsrisiken im Jahr 2023. So erachtet die Mehrheit der befragten Unternehmen grundlegende Sicherheitsaufgaben als Herausforderung. 93 % stufen mindestens eine der folgenden Aktivitäten als schwierig ein:

- Ermitteln relevanter Signale (für 71 % schwierig)
- Priorisieren der zu untersuchenden Signale/Warnmeldungen (für 71 % schwierig)
- Erfassen ausreichender Daten, um festzustellen, ob ein Signal schädlich oder harmlos ist (für 71 % schwierig)
- Zeitnahe Reaktion auf relevante Warnmeldungen oder Vorfälle (für 71 % schwierig)
- Ermitteln der Ursache eines Vorfalls (für 75 % schwierig)
- Detaillierte Protokollierung der Analyse (für 68 % schwierig)

Insbesondere die Analyse der Ursache von Vorfällen gestaltet sich für viele Unternehmen (75 %) problematisch.

Unternehmen mit dem geringsten Jahresumsatz (unter 10 Millionen US-Dollar) empfinden Sicherheitsaufgaben am ehesten als Herausforderung, gefolgt von Unternehmen mit dem höchsten Umsatz (5 Milliarden US-Dollar und mehr). Unternehmen an beiden Enden des Spektrums werden mit unterschiedlichen Problemen konfrontiert. In größeren Organisationen spielen komplexere Systeme und Umgebungen wahrscheinlich eine größere Rolle.

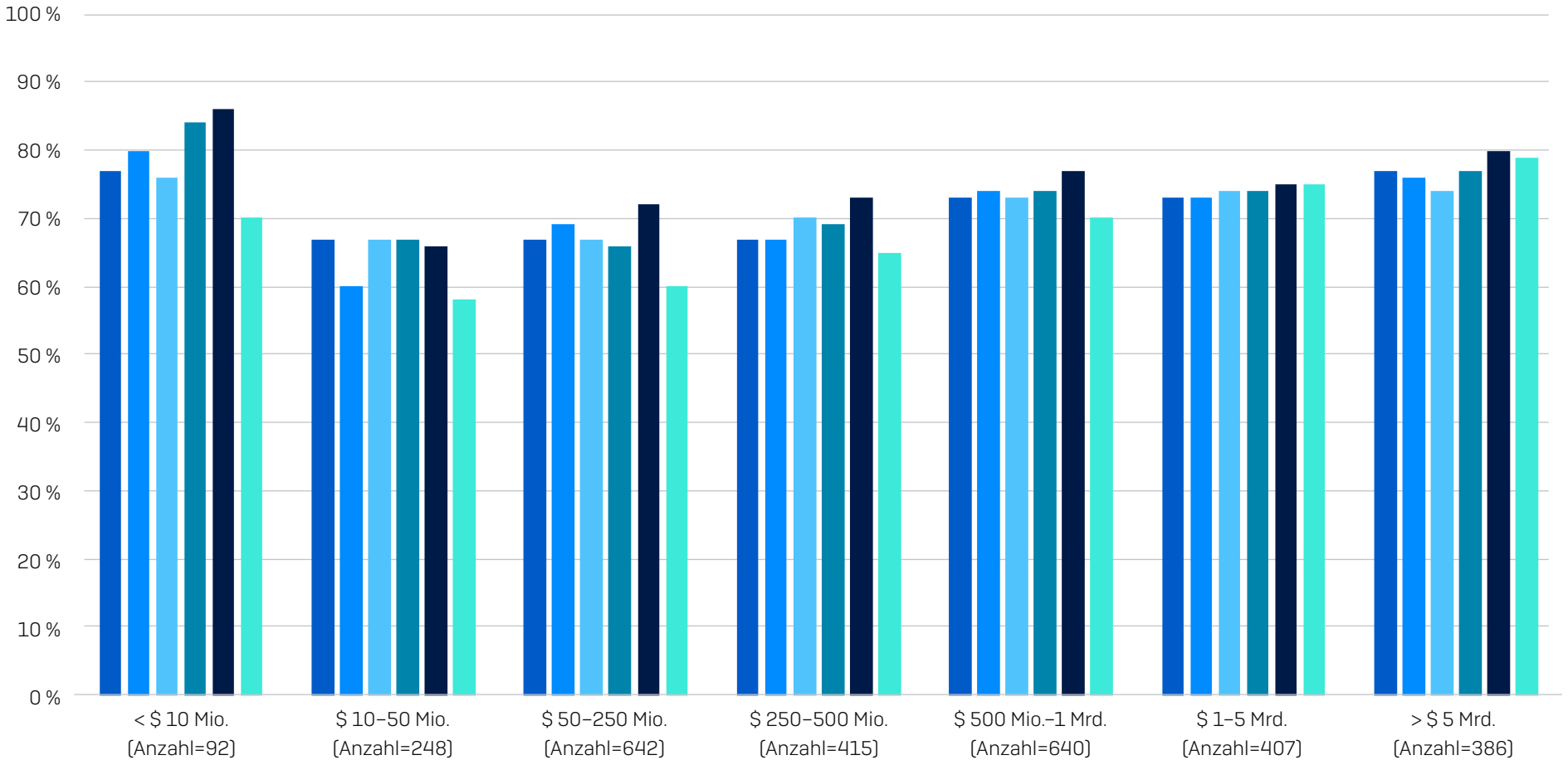
Das fehlende Fachwissen führt zu einem Dominoeffekt: Die Analyse von Warnmeldungen dauert länger, dadurch fehlen dem Team Kapazitäten, was wiederum das Risiko erhöht.

93 %
erachten Sicherheitsaufgaben als Herausforderung

75 %
können die Vorfallursache nur schwer ermitteln

71 %
wissen nicht, welche Warnungen sie untersuchen sollen

Unternehmen, die Sicherheitsaufgaben als schwierig einstufen, nach Umsatz



Unternehmen, die die Analyse verdächtiger Warnmeldungen als sehr schwierig oder relativ schwierig einstufen (Anzahl=2.812 Befragte, die Sicherheitswarnungen intern untersuchen)

- Ermitteln relevanter Signale und Warnmeldungen, die untersucht werden müssen
- Priorisieren der zu untersuchenden Signale/Warnmeldungen
- Erfassen ausreichender Daten, um festzustellen, ob ein Signal schädlich oder harmlos ist
- Ermitteln der Ursache eines Vorfalls, d. h. des Ablaufs des Angriffs
- Zeitnahe Reaktion auf relevante Warnmeldungen oder Vorfälle
- Detaillierte Protokollierung der Analyse

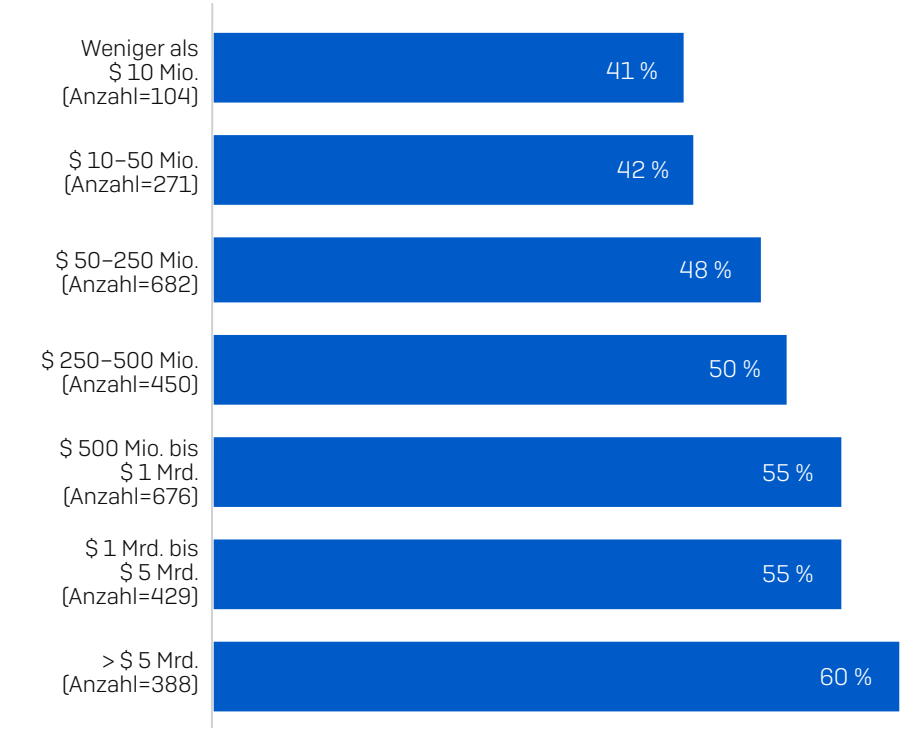
Angreifer auf der Überholspur

52 %
geben an, komplexe Cyberbedrohungen nicht selbst bewältigen zu können

Mehr als die Hälfte (52 %) der IT-Experten räumt ein, dass sie nicht mehr in der Lage ist, den zunehmend komplexen Cyberangriffen ohne Unterstützung von außen Herr zu werden. Bei kleinen Unternehmen (100–250 Mitarbeiter) liegt der prozentuale Anteil sogar bei 64 %.

Je höher der Unternehmensumsatz, desto größer die Wahrscheinlichkeit, dass interne Teams nicht mithalten können. Grund hierfür ist vermutlich, dass in Unternehmen mit hohem Umsatz die Cybersecurity-Umgebungen komplexer sein dürften. Dies erklärt auch die größere Bereitschaft dieser Unternehmen, spezialisierte Cybersecurity Services in Anspruch zu nehmen. Und eventuell ist es auch ein Zeichen dafür, dass in diesen Unternehmen mehr Bewusstsein über die Bedrohungslage und die Herausforderungen bei der Abwehr komplexer Bedrohungen vorhanden ist.

Unternehmen können komplexe Cyberangriffe nicht mehr selbst bewältigen



Inwieweit stimmen Sie der folgenden Aussage zu oder nicht zu? Unser Unternehmen kann komplexe Cyberbedrohungen nicht selbst bewältigen. Ich stimme voll und ganz zu, ich stimme eher zu (Anzahl der erhaltenen Antworten jeweils in Klammer)

Der Business Impact

Auswirkung auf die Umsetzung von IT-Programmen

64 %
würden sich wünschen, dass IT-Teams mehr Zeit für strategische Projekte statt für fieberhafte Akutmaßnahmen aufwenden könnten

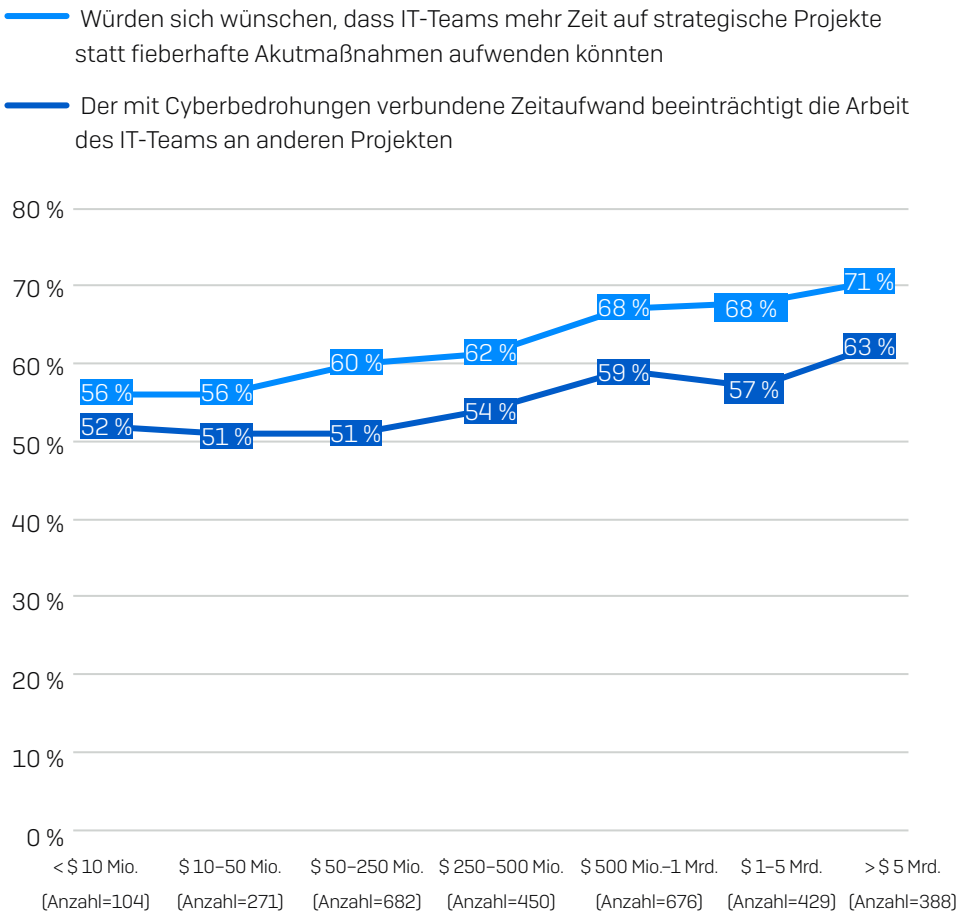
55 %
geben an, dass der mit Cyberbedrohungen verbundene Zeitaufwand die Arbeit des IT-Teams an anderen Projekten beeinträchtigt

Für 60 % der Unternehmen sind Cybersecurity und die IT im Allgemeinen eng verknüpft. Bei 52 % ist die Cybersecurity-Abteilung Teil des IT-Teams. Bei 8 % hingegen verwaltet die IT-Abteilung die Cybersecurity. In den übrigen 40 % sind die Cybersecurity-Abteilung und die IT-Abteilung voneinander getrennt. Der für die Cybersicherheit erforderliche Zeit- und Arbeitsaufwand wirkt sich sehr stark auf die IT aus.

Mehr als die Hälfte (55 %) der Unternehmen gibt an, dass der mit Cyberbedrohungen verbundene Zeitaufwand die Arbeit des IT-Teams an anderen Projekten beeinträchtigt. Hiervon sind Unternehmen mit dem höchsten Jahresumsatz am stärksten betroffen.

Die Dringlichkeit und Unvorhersehbarkeit der Cyberabwehr-Aktivitäten bremsen andere Projekte aus: Im Schnitt würden sich 64 % der befragten Unternehmen wünschen, dass IT-Teams mehr Zeit auf strategische Projekte statt fieberhafte Akutmaßnahmen aufwenden könnten. Je höher der Jahresumsatz, umso drastischer sind auch die Auswirkungen auf die Umsetzung von IT-Projekten.

Cybersecurity schränkt die Umsetzung von IT-Programmen ein



Inwieweit stimmen Sie der Aussage zu oder nicht zu? Der mit Cyberbedrohungen verbundene Zeitaufwand beeinträchtigt die Arbeit des IT-Teams an anderen Projekten. Ich würde mir wünschen, dass die IT mehr Zeit auf strategische Projekte statt fieberhafte Akutmaßnahmen aufwenden könnte (Anzahl der erhaltenen Antworten jeweils in Klammer)

Finanzielle Auswirkungen

Die komplexe Bedrohungslage hat für Unternehmen mehrere finanzielle Auswirkungen. Großer finanzieller Schaden entsteht bei einem schwerwiegenden Cyberangriff. Laut dem Ransomware-Report 2022 von Sophos kostet die Bereinigung eines Ransomware-Angriffs durchschnittlich 1,4 Mio. US-Dollar.

Doch die finanziellen Auswirkungen im Bereich Cybersecurity beschränken sich nicht auf die Bereinigungskosten bei Cyberangriffen. Betrachtet man das durchschnittliche Jahresgehalt eines Cybersecurity-Spezialisten (ca. 100.000 Dollar), ergeben sich daraus erhebliche Kosten für die Analyse von Warnmeldungen. Zwar variieren Gehälter je nach Region, doch sind die finanziellen Auswirkungen der oft langwierigen Analyseprozesse generell beträchtlich.

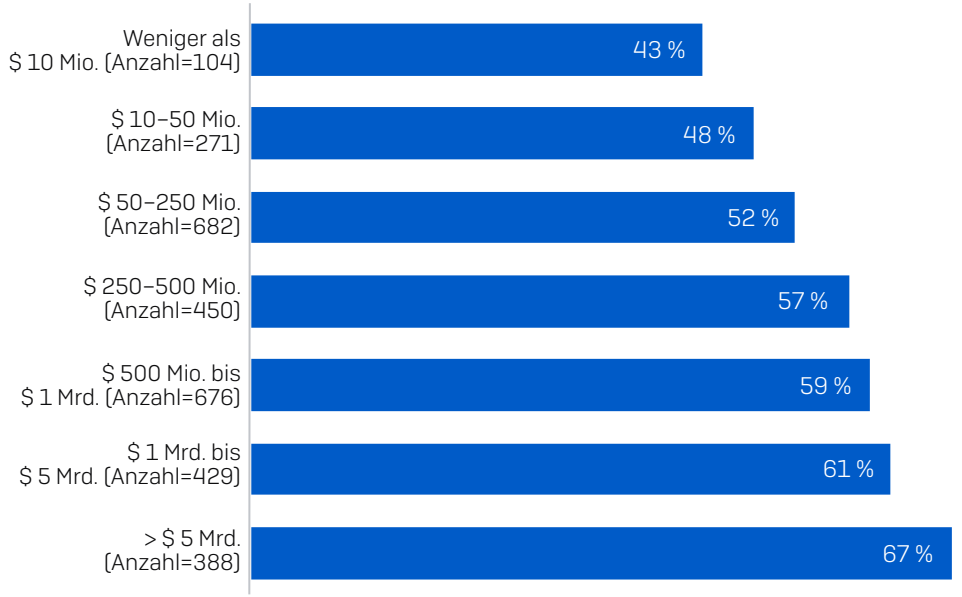
Auswirkungen auf das Team

57 % der IT-Experten geben an, dass die Sorge, das Unternehmen könnte von einem Cyberangriff betroffen sein, ihnen manchmal schlaflose Nächte bereitet. In Anbetracht der hohen Kosten, die mit der Anwerbung und Bindung von Fachpersonal einhergehen, ist dies ein Grund zur Besorgnis, sowohl aus sozialer als auch aus wirtschaftlicher Sicht. Auch lässt sich daraus schließen, dass Unternehmen ihren Sicherheitstools nicht uneingeschränkt vertrauen.

Viele Cybersecurity-Experten leiden an Burnout. Die Flut an Warnmeldungen und eine hohe Arbeitsbelastung bedeuten enormen Stress für die IT. Überlastete Teams verpassen wichtige Signale leichter, was den Druck noch erhöht. Früher oder später ist die Belastung für die Belegschaft zu groß.

Je größer das Unternehmen, desto eher bereitet die Cybersecurity Mitarbeitern schlaflose Nächte: Bei Unternehmen mit einem Jahresumsatz von weniger als 10 Mio. US-Dollar liegt der prozentuale Anteil bei 43 %, bei Unternehmen mit einem Jahresumsatz von mindestens 5 Mrd. US-Dollar immerhin bei 67 %.

Prozentsatz der Befragten, denen die Sorge, das Unternehmen könnte von einem Cyberangriff betroffen sein, schlaflose Nächte bereitet



Inwieweit stimmen Sie der Aussage zu oder nicht zu? Die Sorge, das Unternehmen könnte von einem Cyberangriff betroffen sein, bereitet mir schlaflose Nächte (Anzahl der erhaltenen Antworten jeweils in Klammer)

Empfehlungen

Das Problem lässt sich mit einem einfachen Drei-Stufen-Plan in den Griff bekommen: Einführen eines skalierbaren Reaktionsprozesses für schnellere Reaktionszeiten; Ausbremsen der Angreifer mit adaptiven Abwehrmechanismen; Erzeugen eines positiven Kreislaufs für besseren Schutz bei niedrigeren Kosten.

Um moderne, komplexe Angriffe zu stoppen, müssen Unternehmen die Effizienz ihrer Abwehr (ihre „Schutzschilde") optimieren. Kontextsensitive Technologien bieten dabei zusätzlichen Schutz. Außerdem müssen sie das Zeitfenster, das ihnen Abwehrmaßnahmen eröffnen, für die Ursachenanalyse durch Experten nutzen.

Starke Schutzschilde

Die Qualität Ihrer Cybersecurity-Technologien ist von entscheidender Bedeutung. Sicherheitskontrollen sollten:

- **Die Abwehr optimieren** und so viele Bedrohungen am Anfang der Angriffskette wie möglich erkennen und stoppen. So minimieren Sie die Risiken für Ihr Unternehmen und Ihre Sicherheitsexperten können sich auf weniger Erkennungen konzentrieren.
- **Risiken minimieren** durch korrekte Nutzung und Konfiguration von Sicherheitstools.
- **Angreifer stören**. Technologien, die Angriffsverhalten automatisch erkennen und unterbrechen, verschaffen dem IT-Team Zeit, den Vorfall zu stoppen.

Abwehr optimieren

Stoppen Sie Angriffe so früh wie möglich, um Schäden bei einem Vorfall zu minimieren

Risiken minimieren

Schließen Sie Sicherheitslücken, damit Angreifer keine Chance haben

Angreifer stören

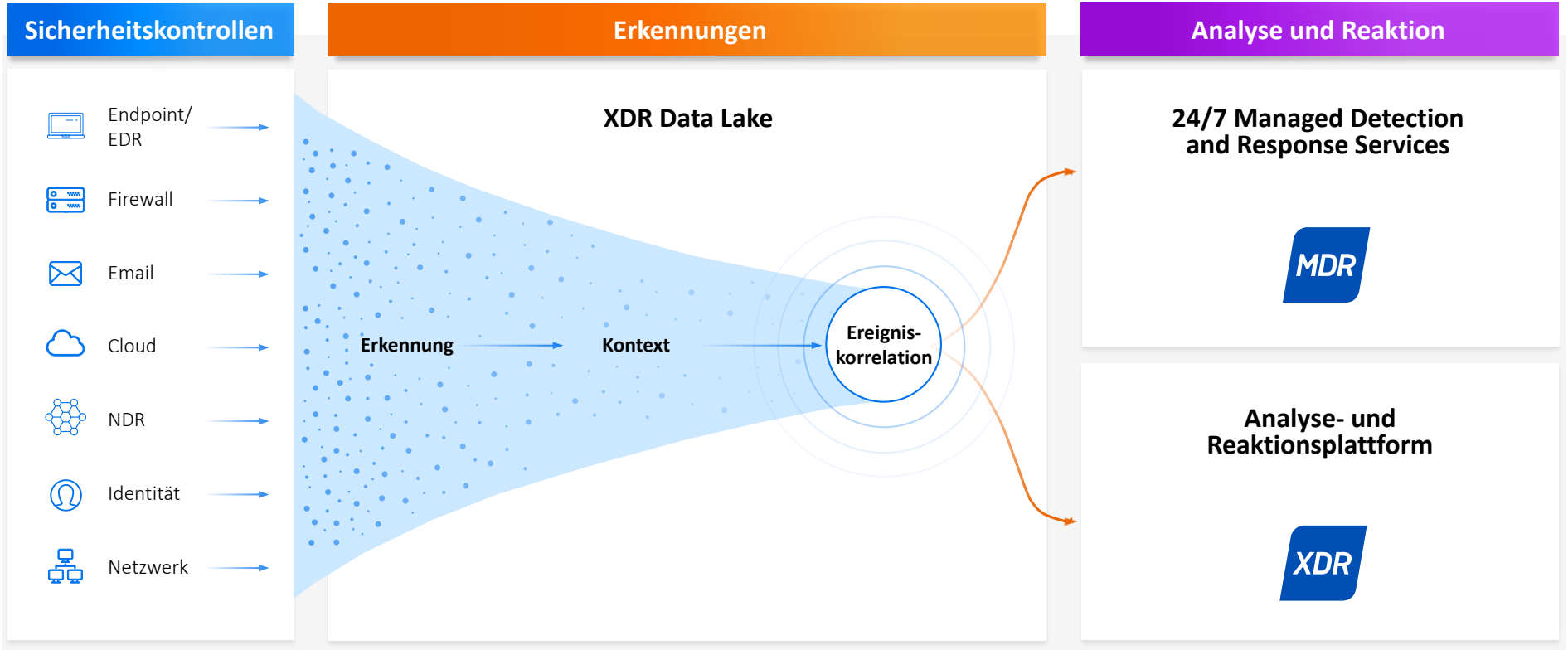
Verschaffen Sie IT-Teams Zeit für die Reaktion auf komplexe, manuelle Angriffe

Ursachenbekämpfung mittels Expertise und Technologie

Schutzschilde verschaffen Experten wertvolle Zeit, um Vorfälle zu analysieren und zu stoppen. Und dennoch garantieren sie keine unfehlbare Abwehr. Eine zeitnahe, fundierte Ursachenanalyse bleibt unerlässlich.

Wie unsere Recherche zeigt, verlassen sich nicht alle Angreifer auf den gleichen Angriffsvektor. Durch die Nutzung von Telemetriedaten vorhandener Sicherheitslösungen aus der gesamten Umgebung sind IT-Teams schneller in der Lage, Bedrohungen zu erkennen und darauf zu reagieren. Gleichzeitig wird der Return on Investment vorhandener Lösungen gesteigert.

Das Aufspüren bösartiger Aktivitäten in der Flut an Warnmeldungen gleicht oft der sprichwörtlichen Suche nach der Nadel im Heuhaufen oder sogar im Nadelhaufen. Eine XDR-Plattform (Extended Detection and Response) liefert kontextbezogene Erkenntnisse zu Signalen und korreliert zusammenhängende Warnmeldungen. So kann sich die IT schnell auf das Wesentliche konzentrieren. Die interne IT-Abteilung kann Analyse und Reaktion mit einer XDR-Plattform durchführen. Alternativ können Unternehmen einen spezialisierten MDR-Service (Managed Detection and Response) mit der Erkennung, Analyse und Reaktion beauftragen.



Schnellere Abwehr

Wenn sich ein Schwungrad erst einmal mit hoher Geschwindigkeit dreht, möchte es sich weiter drehen. Je mehr Kraft das Schwungrad antreibt, desto schneller dreht es sich. Durch die Kombination menschlicher Expertise und Schutztechnologien beschleunigen Unternehmen ihr Cybersecurity-Schwungrad. Mit umfassenden Sicherheitskontrollen bewältigen Unternehmen die Flut an Warnmeldungen. So können sie sich auf die Abwehr von Angriffen und die Optimierung ihres Sicherheitsstatus konzentrieren. Dies sorgt wiederum für effizientere Sicherheitskontrollen. Ein positiver Kreislauf wird in Gang gesetzt.

Einführung notwendiger Kontrollen und Services

Wie aus der Umfrage hervorgeht, plant das Gros der Unternehmen, in den nächsten 12 Monaten Lösungen für die Bedrohungserkennung und -reaktion einzuführen. Mehr als drei Viertel (78 %) planen, im nächsten Jahr Endpoint Detection and Response (EDR) und/oder Extended Detection and Response (XDR) zu implementieren.

Die Analyse und Abwehr komplexer Cyberbedrohungen erfordert fundiertes Know-how. Mindestens fünf oder sechs Experten sollten sich rund um die Uhr mit dieser Aufgabe befassen. Da fehlendes internes Fachwissen im Bereich Cybersecurity zu den größten Cyberrisiken im Jahr 2023 zählt, nehmen viele Unternehmen externe Services in Anspruch: 44 % der Unternehmen planen, in den nächsten 12 Monaten einen MDR-Anbieter (Managed Detection and Response) hinzuzuziehen.

Anteil der Unternehmen, die in den nächsten 12 Monaten Detection-and-Response-Lösungen einführen möchten

78 %	44 %
EDR/XDR	MDR

Cybersecurity-Lösungen von Sophos

Sophos bietet Services und Technologien, mit denen Unternehmen ihre Abwehr beschleunigen und Angreifer überholen können. Wir schützen mehr als 550.000 Unternehmen und Einrichtungen vor modernsten Bedrohungen. Sophos MDR ist der Managed-Detection-and-Response-Service, dem weltweit die meisten Kunden vertrauen.

Stärkster Schutz von Anfang an

Unsere Endpoint/EDR-, Firewall-, E-Mail- und Cloud-Lösungen bremsen Angreifer aus und verschaffen Sicherheitsexperten Zeit und wichtige Einblicke:

- **Abwehr optimieren:** Sophos-Lösungen blockieren automatisch 99,98 % der Bedrohungen. So können sich Analysten besser auf Vorfälle konzentrieren, die menschliches Eingreifen erfordern, und Risiken werden minimiert.
- **Risiken minimieren:** Vom ersten Tag an werden automatisch die optimalen Schutzeinstellungen angewendet, um Sicherheitslücken zu schließen. Integrierte Kontosicherheitsprüfungen zeigen fehlende Software und Konfigurationsprobleme auf, die vermeidbare Vorfälle nach sich ziehen können.
- **Angreifer stören:** Die Adaptive Active Adversary Protection verschärft die Sicherheit automatisch, wenn ein manueller Endpoint-Angriff erkannt wird. Dies verschafft Sicherheitsexperten wertvolle Zeit für die Vorfallsreaktion.

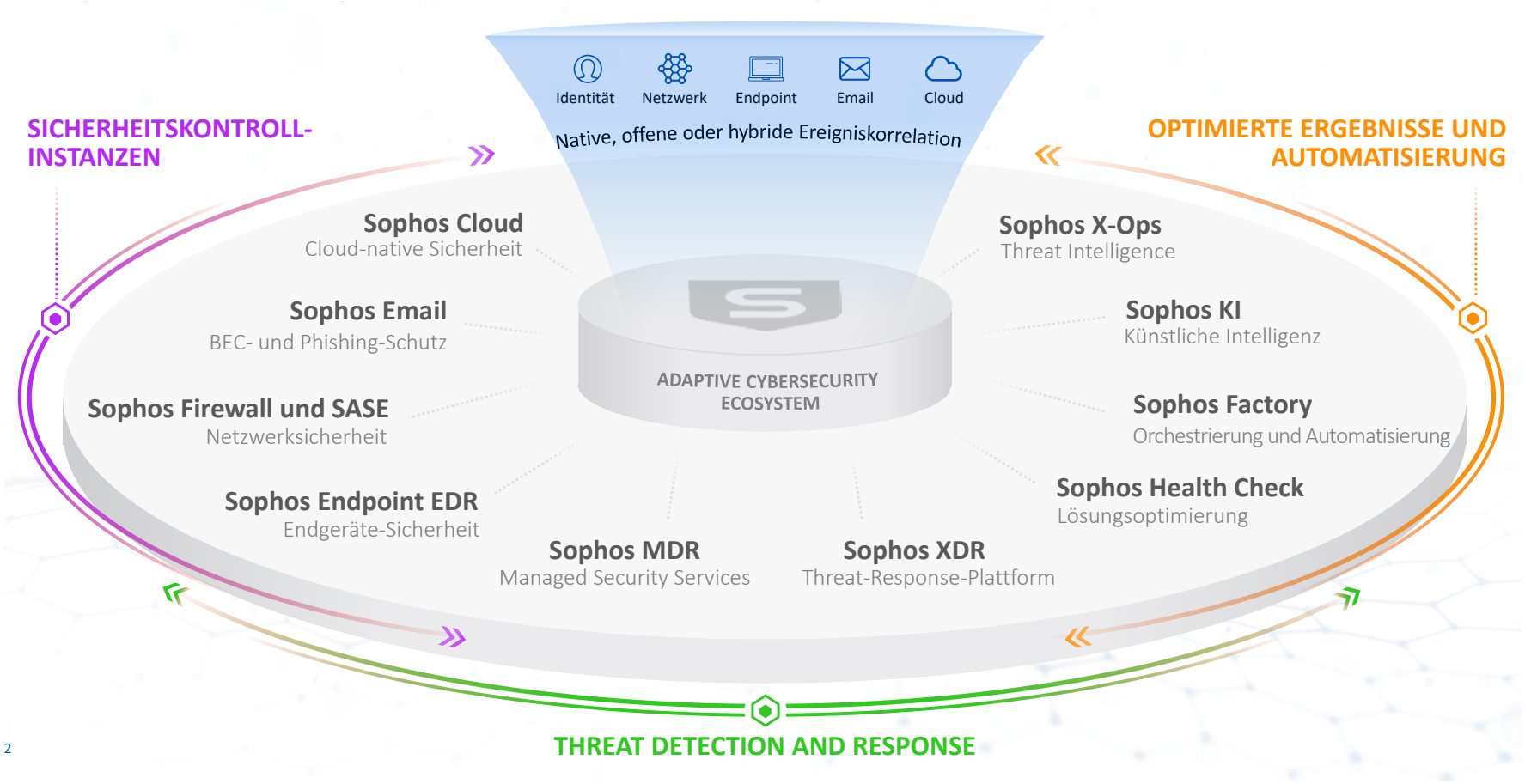
Optimierte Erkennung, Analyse und Reaktion

Je mehr Einblicke IT-Teams haben, desto schneller können sie reagieren. Dank der Integration von Telemetriedaten von Sicherheitstools anderer Hersteller und Sophos-Lösungen nutzt Sophos Erkennungen aus der gesamten Sicherheitsumgebung und beschleunigt so die Bedrohungserkennung und -reaktion. Unsere Kunden steigern gleichzeitig den Return on Investment vorhandener Lösungen.

Sophos MDR verfügt über die kollektive Erfahrung von über 500 Experten, die für Kunden 24/7/365 proaktiv Angriffe aufspüren, analysieren und Reaktionsmaßnahmen ergreifen. Im Schnitt beheben die MDR-Experten von Sophos Vorfälle in nur 38 Minuten – deutlich schneller als interne Teams. Alternativ können Unternehmen Angriffe mit den umfassenden EDR-Funktionen der Sophos-XDR-Plattform direkt untersuchen und stoppen oder mit dem Sophos-MDR-Team zusammenarbeiten.

Sophos hilft Unternehmen und Einrichtungen jeder Größe dabei, ihre Abwehr zu beschleunigen und modernsten Bedrohungen einen Schritt voraus zu bleiben. Weitere Informationen erhalten Sie unter www.sophos.de.

Optimaler Cyberschutz – mit Sophos



2023-03-29 (WP-NP)

SOPHOS