SOPHOS
Cybersecurity evolved.

IT-Security Teams im Jahr 2021 und in der Zukunft

Ergebnisse einer Umfrage unter 5.400 IT-Managern aus 30 Ländern

Sophos-Whitepaper. Juni 2021

In fast allen Unternehmen spielten IT-Security-Teams eine zentrale Rolle bei der Bewältigung der Pandemie. Trotz der COVID-19-Beschränkungen trugen IT-Abteilungen in aller Welt mit ihrem Engagement und unermüdlichen Einsatz entscheidend dazu bei, dass Unternehmen ihren Betrieb unterbrechungsfrei fortsetzen konnten. Einige Beispiele: Die IT unterstützte den Bildungssektor bei der Bereitstellung von digitalem Unterricht, ermöglichte dem Einzelhandel den Umstieg auf Online-Shops und sorgte dafür, dass öffentliche Einrichtungen weiterhin systemrelevante Dienstleistungen anbieten konnten.

Dieser Report, der auf dem direkten Feedback von 5.400 IT-Managern in 30 Ländern basiert, beleuchtet die Lage von IT-Abteilungen in den letzten 12 Monaten. Der Bericht zeigt Veränderungen auf, mit denen die IT-Teams 2020 konfrontiert waren, und geht auch auf die entsprechenden Folgen für die IT ein – insbesondere im Hinblick auf das Thema Cybersecurity. Zudem bietet der Report Ausblicke auf die Zukunft von IT-Security-Abteilungen und zeigt deren Erwartungen für die nächsten fünf Jahre. Außerdem erfahren Sie, wie Sie schon heute Ihre IT-Organisation von morgen aufbauen können.

Wichtigste Erkenntnisse

Veränderungen im Arbeitsalltag von IT-Teams in 2020

- **Höhere Arbeitsbelastung der IT- und Cybersecurity-Teams:** 63 % der befragten Unternehmen verzeichneten ein höheres Arbeitspensum der IT im Allgemeinen, 69 % eine höhere Arbeitsauslastung der IT-Security im Speziellen
- **Mehr Cyberangriffe:** 61 % meldeten einen Anstieg der Cyberangriffe auf ihr Unternehmen
- **Verbesserung der Cybersecurity-Kompetenzen in IT-Abteilungen:** 70 % gaben an, dass sie ihre Kompetenz und ihr Know-how im Bereich Cybersecurity im Verlauf der Pandemie verbessern konnten
- **Größerer Zusammenhalt im Team:** 52 % berichteten, dass die Moral im Team im vergangenen Jahr gestärkt wurde. Dies trifft insbesondere auf Unternehmen zu, die von Ransomware betroffen waren (60 % ggü. 47 % bei Unternehmen, die keine Ransomware-Angriffe verzeichneten)

Die aktuelle Lage

- **IT-Abteilungen benötigen Unterstützung bei der Abwehr komplexer Angriffe:** 54 % können komplexe Cyberangriffe eigenen Angaben zufolge nicht selbst bewältigen
- **IT-Abteilungen fühlen sich für die Herausforderungen der Zukunft gut gerüstet:** 82 % sind der Meinung, dass sie über die nötigen Tools und die Expertise zur umfassenden Analyse verdächtiger Aktivitäten verfügen

Die IT-Abteilung der Zukunft

- **IT-Security-Abteilungen werden größer**
  - 68 % der befragten Unternehmen gehen davon aus, dass ihre interne IT-Security-Abteilung bis 2023 wachsen wird, 76 % rechnen mit einem Personalanstieg bis 2026
  - 56 % prognostizieren einen Anstieg an externen IT-Security-Kräften bis 2023, 64 % bis 2026.
- **Künstliche Intelligenz spielt bei Security-Strategien der Zukunft eine zentrale Rolle**
  - 92 % gehen davon aus, dass KI künftig zur Bewältigung der steigenden Anzahl und/oder der zunehmenden Komplexität von Bedrohungen eingesetzt wird

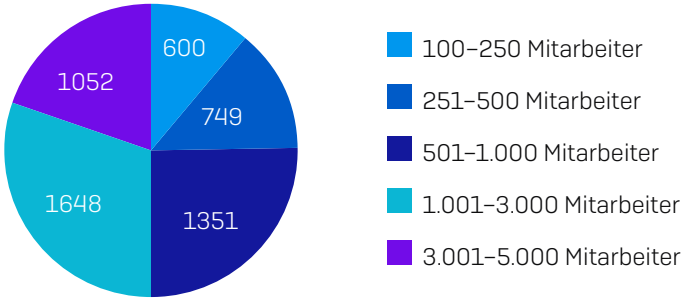
Über die Studie

Sophos hat eine unabhängige Befragung zum Thema Ransomware in Auftrag gegeben, die vom Marktforschungsinstitut Vanson Bourne zwischen Januar und Februar 2021 durchgeführt wurde. Im Rahmen dieser Studie wurden 5.400 IT-Manager in 30 Ländern zu ihren Erfahrungen mit Ransomware befragt.

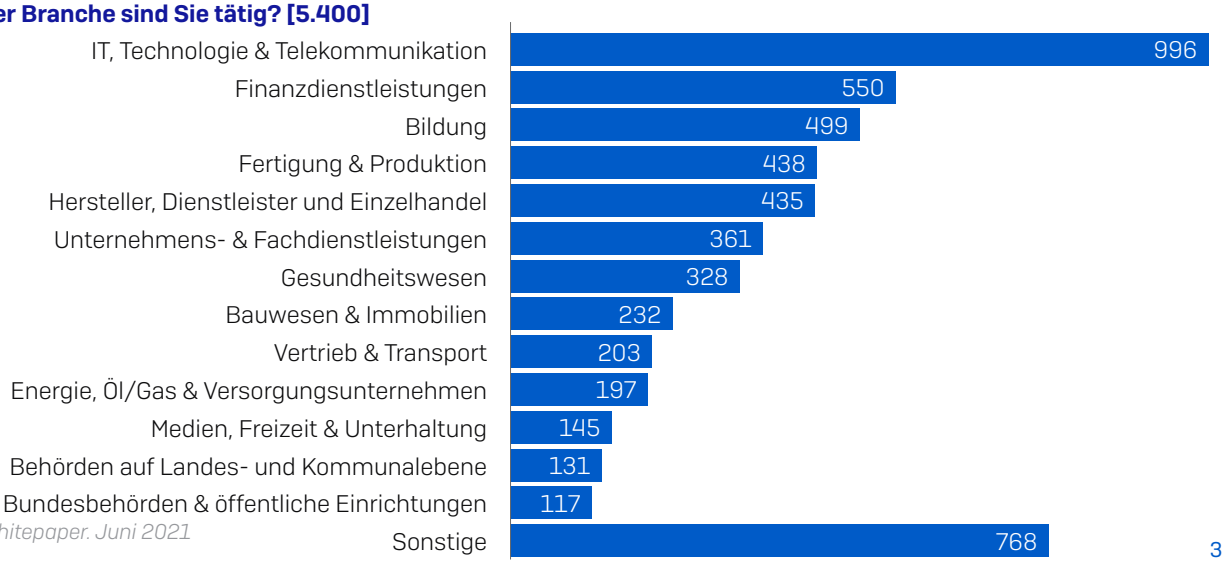
Land	# Umfrageteilnehmer	Land	# Umfrageteilnehmer	Land	# Umfrageteilnehmer
Australien	250	Indien	300	Saudi-Arabien	100
Österreich	100	Israel	100	Singapur	150
Belgien	100	Italien	200	Südafrika	200
Brasilien	200	Japan	300	Spanien	150
Kanada	200	Malaysia	150	Schweden	100
Chile	200	Mexiko	200	Schweiz	100
Kolumbien	200	Niederlande	150	Türkei	100
Tschechische Republik	100	Nigeria	100	VAE	100
Frankreich	200	Philippinen	150	Vereinigtes Königreich	300
Deutschland	300	Polen	100	USA	500

Die Umfrageteilnehmer stammten zu 50 % aus Unternehmen mit 100 bis 1.000 Mitarbeitern und zu 50 % aus Unternehmen mit 1.001 bis 5.000 Mitarbeitern. Zudem repräsentieren die befragten Unternehmen einen breiten Querschnitt unterschiedlicher Branchen.

Wie viele Mitarbeiter beschäftigt Ihr Unternehmen weltweit? [5.400]



In welcher Branche sind Sie tätig? [5.400]



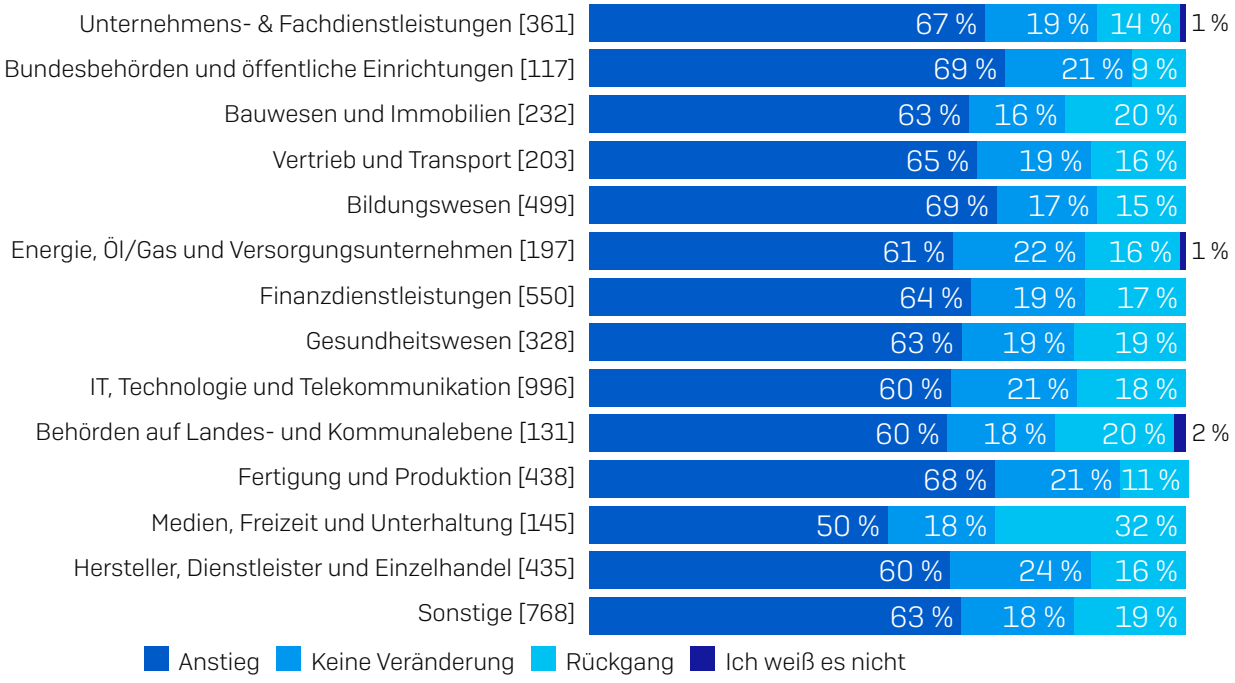
2020: Ein Jahr des Wandels

2020 stellte uns alle vor völlig neue Herausforderungen. IT-Teams sorgten an vorderster Front dafür, dass Unternehmen ihre Arbeitsabläufe an die neuen Gegebenheiten in der Pandemie anpassen konnten. Es ist kaum verwunderlich, dass sich dies signifikant auf die Arbeitslast der Belegschaft auswirkte.

Die IT hatte viel zu tun

IT-Abteilungen waren in 2020 enorm ausgelastet: 63 % der IT-Manager gaben an, dass die Arbeitslast der IT (ohne Berücksichtigung der IT-Security) im Laufe des Jahres 2020 zunahm. Nur 17 % verzeichneten weniger Arbeit. Insbesondere Umfrageteilnehmer aus der Türkei (84 %), Österreich (81 %) und den USA (75 %) meldeten ein höheres Arbeitsaufkommen.

Wie entwickelte sich die Auslastung der IT-Abteilung (ohne Berücksichtigung der IT-Security) im Laufe des Jahres 2020?



Im Laufe des Jahres 2020 gab es bei der Arbeitsauslastung unserer IT (ohne Berücksichtigung der IT-Security) einen Anstieg/einen Rückgang/keine Veränderung [Basiszahlen im Diagramm], nach Branche bzw. Sektor

Im Branchenvergleich zeigt sich, dass IT-Teams in **Bundesbehörden und öffentlichen Einrichtungen** sowie im **Bildungssektor** besonders ausgelastet waren: 69 % der Umfrageteilnehmer verzeichneten ein höheres Arbeitspensum, was aller Wahrscheinlichkeit nach auf die zentrale Rolle der Behörden und Bildungseinrichtungen bei der Reaktion auf die Pandemie zurückzuführen ist. In der Branche **Medien, Freizeit und Unterhaltung** sank die Arbeitslast hingegen bei 32 % der Befragten, da ihre Dienstleistungen während der Pandemie teilweise Einschränkungen unterlagen.

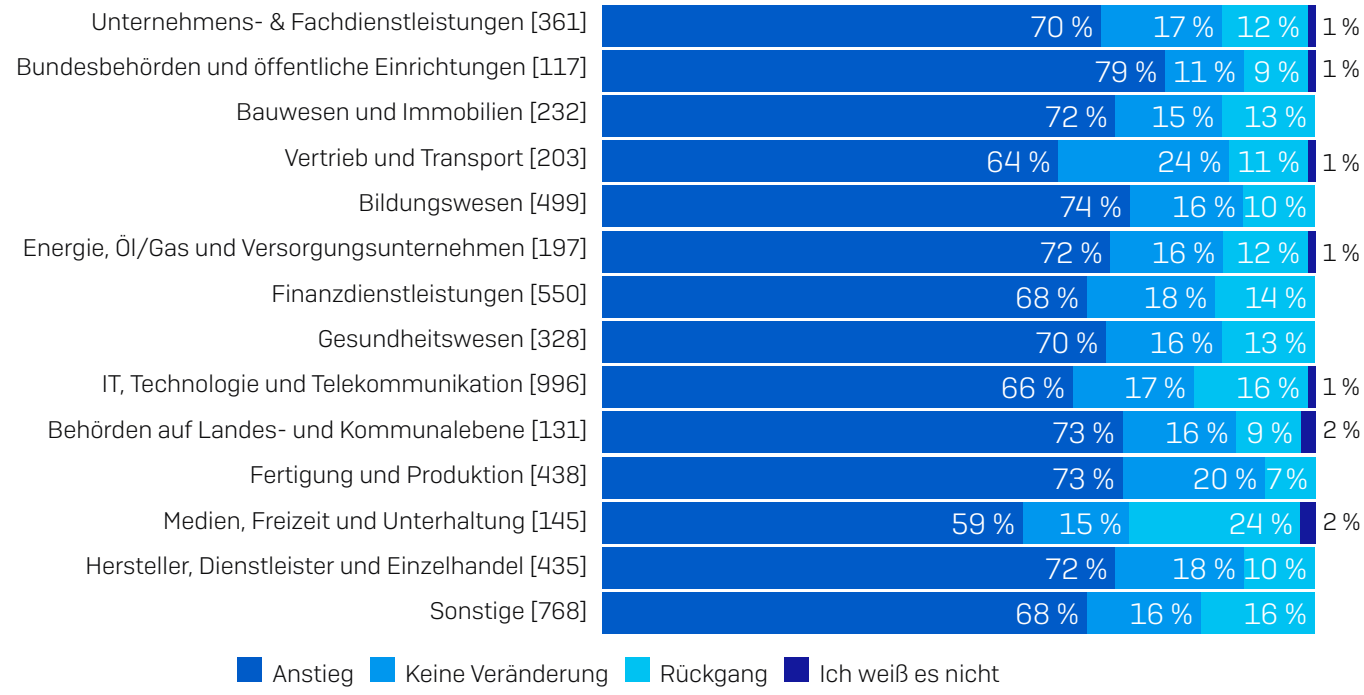
... und die IT-Security hatte noch mehr zu tun

Wie entwickelte sich die Auslastung der IT-Security-Abteilung im Laufe des Jahres 2020?

Im Laufe des Jahres 2020 gab es bei der Arbeitsauslastung unserer IT-Security einen Anstieg/einen Rückgang/keine Veränderung [5.400] (ohne Berücksichtigung der Antwortoption „Ich weiß es nicht“)

Bei 69 % der befragten Unternehmen nahm die Arbeitsauslastung der IT-Security im Vergleich zum Vorjahr zu, bei 13 % ab und 17 % stellten keine Unterschiede fest. Die Türkei (82 %) meldete auch hier den höchsten Anstieg, gefolgt von Schweden (80 %), Israel und Brasilien (jeweils 78 %). Einen Rückgang des Security-Arbeitsaufkommens beobachteten vor allem Unternehmen in den Vereinigten Arabischen Emiraten (26 %), der Schweiz (22 %), Nigeria und den Philippinen (jeweils 19 %).

Wie entwickelte sich die Auslastung der IT-Security-Abteilung im Laufe des Jahres 2020?



Im Laufe des Jahres 2020 gab es bei der Arbeitsauslastung unserer IT-Security einen Anstieg/einen Rückgang/keine Veränderung [Basiszahlen im Diagramm], nach Branche

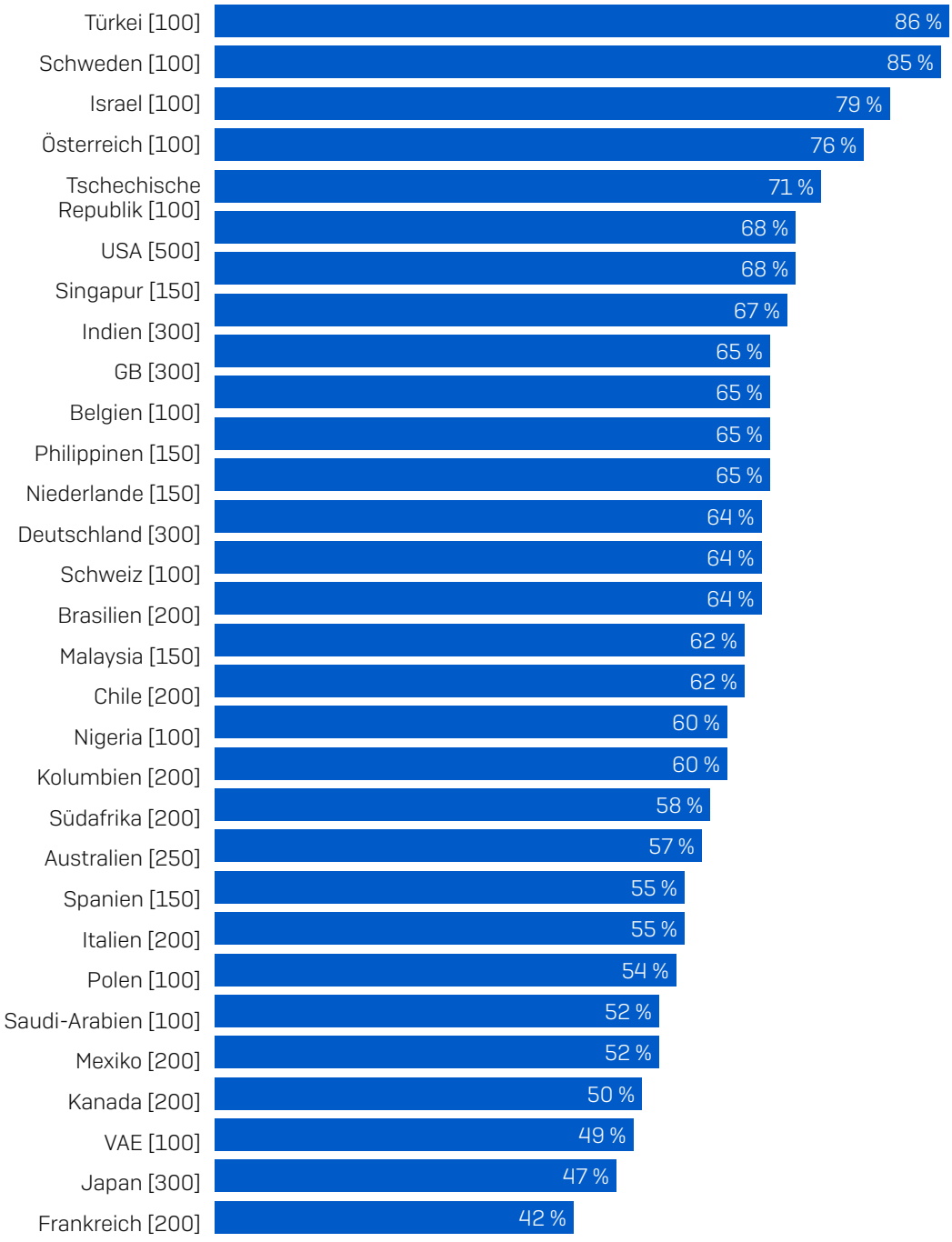
Im Branchenvergleich zeichnet sich auch hier wieder der gleiche Trend ab: Am häufigsten meldeten IT-Manager aus **Bundesbehörden und öffentlichen Einrichtungen** (79 %) sowie dem **Bildungssektor** (74 %) eine höhere Arbeitsauslastung im Bereich Cybersecurity im Laufe des letzten Jahres. Bei Unternehmen im Bereich **Medien, Freizeit und Unterhaltung** ging das Arbeitsaufkommen hingegen mitunter zurück (24 %). Auch diese Ergebnisse lassen sich wahrscheinlich darauf zurückführen, dass diese Sektoren besonders stark von der Pandemie betroffen waren – wenn auch auf sehr unterschiedliche Weise.

Mehr Cyberangriffe

Die höhere Arbeitsbelastung im Bereich Cybersecurity im Laufe des Jahres 2020 erklärt sich teilweise durch ein erhöhtes Angriffsaufkommen: Mehr als sechs von zehn (61 %) der befragten Unternehmen beobachteten im vergangenen Jahr steigende Cyberangriffszahlen. Lediglich 19 % verzeichneten weniger Angriffe.

Der Anstieg zieht sich durch alle Branchen. Lediglich 16 Prozentpunkte trennen die Sektoren bzw. Branchen, die die höchste **(Bundesbehörden und öffentliche Einrichtungen)** bzw. die geringste Zunahme beobachteten **(IT, Technologie und Telekommunikation** und **Medien, Freizeit und Unterhaltung)** (74 % ggü. 58 %).

Prozentualer Anteil der Unternehmen, die im Laufe des Jahres 2020 mehr Cyberangriffe feststellten



Im Laufe des Jahres 2020 stieg die Anzahl der Cyberangriffe [Basiszahlen im Diagramm], wobei einige Antwortmöglichkeiten übersprungen wurden, nach Land

Betrachten wir die Daten jedoch im Ländervergleich, zeigen sich größere Diskrepanzen: So verzeichneten etwa mehr als doppelt so viele Unternehmen in der Türkei (86 %) Angriffe im Vergleich zu den befragten Unternehmen in Frankreich (42 %). Darüber hinaus beobachteten zudem insbesondere schwedische (85 %), israelische (79 %) sowie österreichische (76 %) Unternehmen steigende Angriffszahlen im Laufe des Jahres 2020. In Frankreich, Japan und den Vereinigten Arabischen Emiraten ging die Anzahl der Angriffe hingegen bei weniger als der Hälfte der befragten Unternehmen zurück.

Angriffe lassen sich immer schwerer stoppen

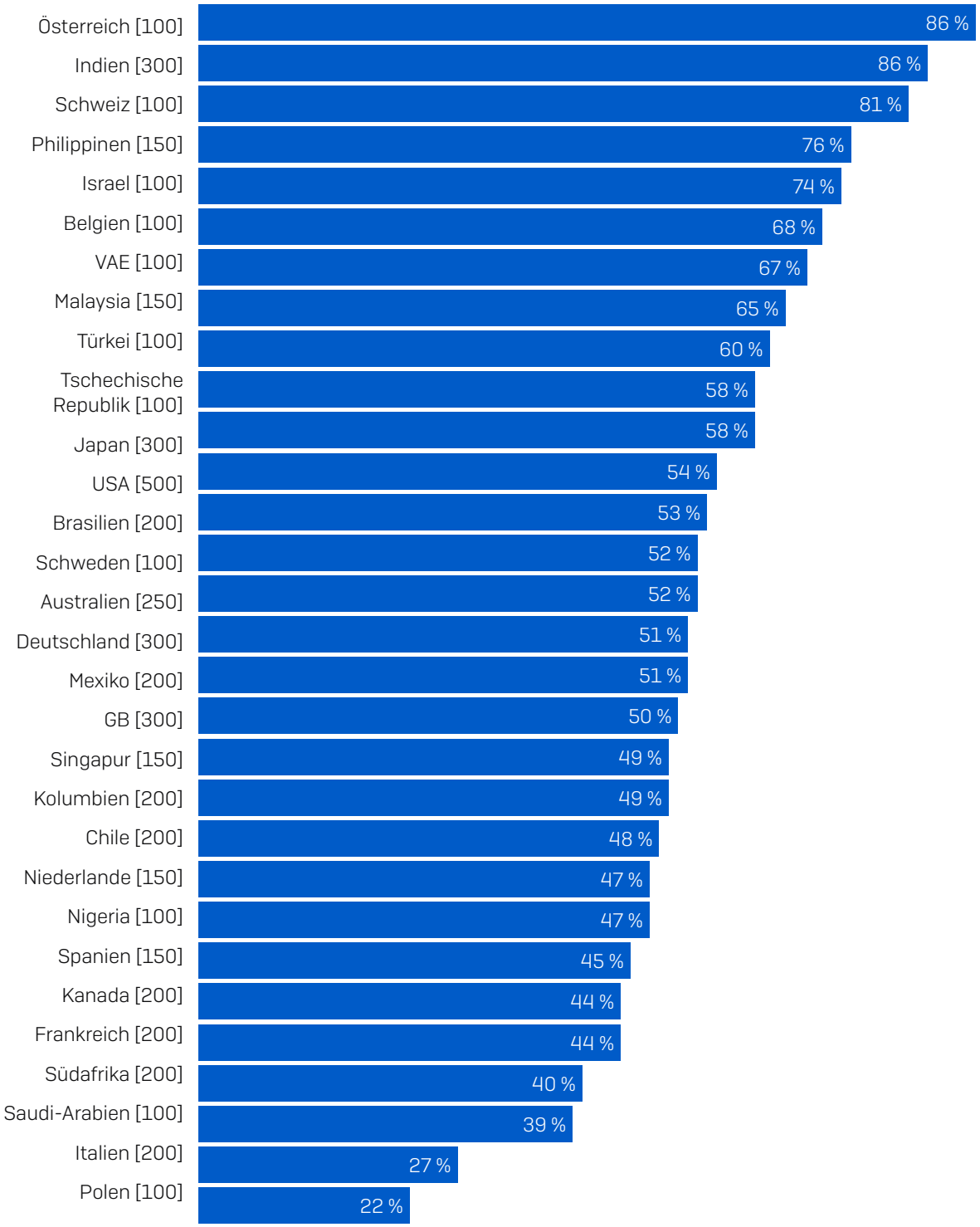
Cyberkriminelle greifen bei komplexen, mehrphasigen Angriffen auf immer neue Taktiken, Techniken und Prozesse (TTPs) zurück. Die Abwehr dieser Angriffe ist kein leichtes Unterfangen: Mehr als die Hälfte (54 %) der befragten Unternehmen können komplexe Angriffe nach eigenen Angaben nicht mehr selbst bewältigen.

können komplexe Cyberangriffe eigenen Angaben zufolge nicht selbst bewältigen

In der Branche **Unternehmens- und Fachdienstleistungen** fühlen sich sogar ganze 63 % der Umfrageteilnehmer mit der Abwehr komplexer Angriffe überfordert, gefolgt von den **Bundesbehörden und öffentlichen Einrichtungen** (62 %) und dem **Gesundheitswesen** (60 %). Dagegen sehen sich vor allem Unternehmen aus dem Bereich **Bauwesen und Immobilien** sowie **Behörden auf Landes- und Kommunalebene** (47 %) dieser Aufgabe gewachsen. Die Umfrageergebnisse der Behörden auf Landes- und Kommunalebene überraschen: Denn wie aus unserem Ransomware-Report 2021 hervorgeht, besteht bei diesem Sektor die größte Wahrscheinlichkeit für eine Datenverschlüsselung im Zuge eines Ransomware-Angriffs.

Im Ländervergleich lassen sich signifikante Unterschiede bei der Sicherheit im Umgang mit komplexen Angriffen feststellen.

Unternehmen, die komplexe Cyberangriffe eigenen Angaben zufolge nicht selbst bewältigen können



Unternehmen, die komplexe Cyberangriffe eigenen Angaben zufolge nicht selbst bewältigen können [Basiszahlen im Diagramm], wobei einige Antwortmöglichkeiten übersprungen wurden, nach Land

Insbesondere Unternehmen in Österreich und Indien (86 %) sahen sich häufig nicht in der Lage, komplexe Angriffe selbst abzuwehren, gefolgt von der Schweiz (81 %), den Philippinen (76 %) und Israel (74 %).

Schon allein das Bewusstsein, dass Bedrohungen komplex sind und Unternehmen Unterstützung durch externe Experten benötigen, ist ein wichtiger Schritt bei der Abwehr moderner Cyberangriffe. Unsere SophosLabs- und Sophos Managed Threat Response-Experten verzeichnen einen signifikanten Anstieg an Cyberangriffen, bei denen verstärkt auf eine Kombination aus Automatisierung und manuellem Hacking gesetzt wird. Die Bekämpfung solcher komplexen Angriffe erfordert fundiertes Cybersecurity-Know-how. Für Unternehmen ist es daher entscheidend zu erkennen, wann sie Cybersecurity-Aufgaben an externe Experten auslagern sollten.

Vergleichsweise wenige polnische (22 %) und italienische (27 %) Unternehmen fühlen sich hingegen mit der Abwehr komplexer Angriffe überfordert. Möglicherweise erklärt sich die Sicherheit im Umgang mit der steigenden Angriffszahl durch die Investition in qualifiziertes Fachpersonal und Weiterbildungsmaßnahmen. Es kann jedoch auch sein, dass Unternehmen die Gefahr mitunter unterschätzen. Da Cyberkriminelle kontinuierlich an ihren Angriffsstrategien feilen, ist es für Unternehmen äußerst wichtig, die zur Abwehr benötigte Expertise realistisch einzuschätzen.

Längere Reaktionszeiten

Angesichts der höheren Arbeitsauslastung im Laufe des Jahres 2020 sowie der Herausforderungen bei der Umstellung auf die neuen Arbeitsmodelle in der Pandemie überrascht es wohl kaum, dass die Reaktionszeiten auf IT-Fälle bei der Mehrheit (61 %) der befragten Unternehmen anstiegen. 20 % meldeten in diesem Zeitraum kürzere Reaktionszeiten. 19 % konnten dagegen keine Unterschiede feststellen.

Entwicklung der Reaktionszeit auf IT-Fälle im Laufe des Jahres 2020

Im Laufe des Jahres 2020 wurde die Reaktionszeit bei IT-Fällen länger/kürzer unverändert [5.400] (ohne Berücksichtigung der Antwortoption „Ich weiß es nicht")

Vor allem im **Bildungssektor** stiegen die Reaktionszeiten (65 %). Da die pandemiebedingte Umstellung auf digitalen Unterricht für IT-Abteilungen im Bildungssektor in vielen Ländern mit einem enormen Arbeitsaufwand verbunden war, ließen sich Tickets nicht mehr so schnell beantworten.

In der Branche **Medien, Freizeit und Unterhaltung** meldete dagegen knapp ein Drittel (32 %) der befragten Unternehmen schnellere Reaktionszeiten. Auch hier spielt die Pandemie mit Sicherheit eine entscheidende Rolle: IT-Teams waren weniger ausgelastet und konnten somit schneller reagieren.

Auswirkungen des Jahres 2020 auf IT-Abteilungen

Doch es gibt nicht nur schlechte Nachrichten. Die aktuelle Lage der befragten IT-Teams stimmt durchaus positiv. 70 % der IT-Manager gaben an, dass ihre Teams ihre Expertise im Bereich Cybersecurity im Laufe des Jahres 2020 erweitern konnten. Bei lediglich 12 % war das Gegenteil der Fall.

Cybersecurity-Kompetenzen und -Know-how konnten im Laufe des Jahres 2020 erweitert werden

Im Laufe des Jahres 2020 nahm unsere Fähigkeit, Cybersecurity-Kompetenzen und -Know-how zu erweitern, zu/ab/blieb unverändert [5.400] (ohne Berücksichtigung der Antwortoption „Ich weiß es nicht")
Aufgrund der Rundung liegt die Gesamtsumme der Ergebnisse nicht bei 100 %

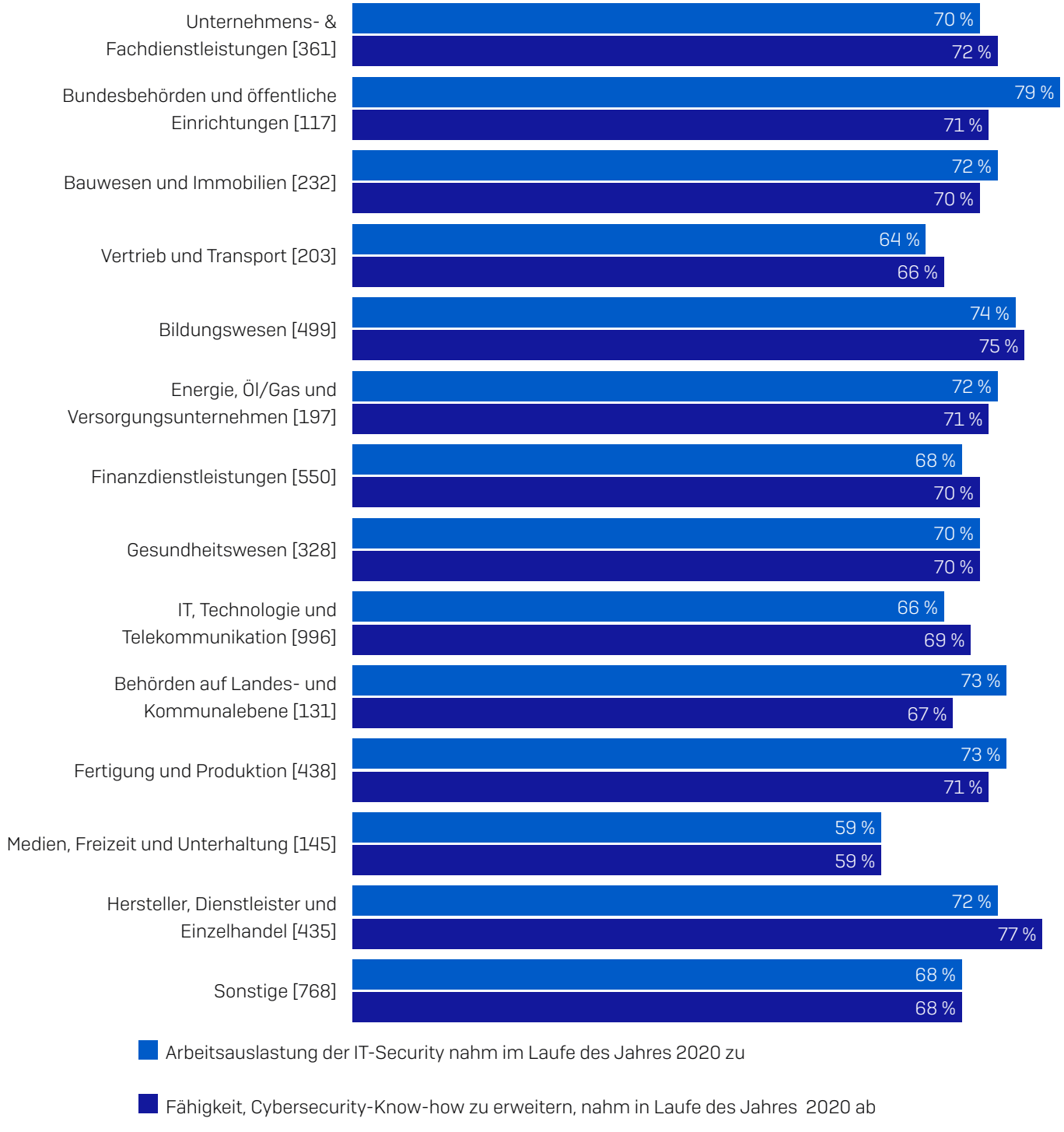
Interessanterweise variierten die Erfahrungen in mehreren, besonders schwer von der Pandemie betroffenen Branchen bzw. Sektoren:

- Vor allem IT-Abteilungen im **Einzelhandel** (77 %) gewannen Cybersecurity-Know-how dazu. Wahrscheinlich brachte der Umstieg auf den Online-Handel aufgrund des Lockdowns neue Herausforderungen und Chancen für IT-Teams in dieser Branche mit sich.
- An zweiter Stelle der Unternehmen, die ihre Kompetenzen im Bereich IT-Security steigern konnten, lag der **Bildungssektor** mit 75 %. Auch dieser Bereich vollzog im vergangenen Jahr einen dramatischen Wandel. Zwar stellte der Umstieg auf digitalen Unterricht die IT vor enorme Herausforderungen, er eröffnete jedoch gleichzeitig auch neue Lernmöglichkeiten.
- Mit 59 % entfiel der geringste prozentuale Anteil der Unternehmen, die ihr Cybersecurity-Know-how steigern konnten, auf den Bereich **Medien, Freizeit und Unterhaltung**. Da das Arbeitsaufkommen in dieser Branche in der IT im Allgemeinen und der IT-Security im Speziellen auch am meisten zurückging, waren die Lernmöglichkeiten aller Wahrscheinlichkeit nach entsprechend begrenzt.

Die höhere Arbeitsauslastung führte zu mehr Know-how

Insgesamt belegen die Daten einen klaren Zusammenhang zwischen dem höheren Arbeitsaufkommen im Bereich Cybersecurity und einer Verbesserung des Cybersecurity-Know-hows – ein Trend, der sich durch alle Branchen zieht.

Höhere Cybersecurity-Arbeitsauslastung und Verbesserung der Cybersecurity-Expertise



Im Laufe des Jahres 2020 nahm die Arbeitsauslastung unserer IT-Security zu/Im Laufe des Jahres 2020 konnten wir unsere Expertise im Bereich Cybersecurity erweitern [Basiszahlen im Diagramm], nach Branche

84 % der Umfrageteilnehmer, die im Laufe des Jahres 2020 mehr Cybersecurity-Aufgaben übernehmen mussten, konnten ihre Kompetenzen und ihr Know-how in diesem Bereich ausbauen. Gleiches gilt für mehr als acht von zehn (82 %) Unternehmen, die ein höheres Angriffsaufkommen verzeichneten. Das ergibt Sinn: Eine größere Arbeitsbelastung und mehr Cyberangriffe erhöhen zwar den Druck auf die IT, eröffnen aber gleichzeitig auch neue Lernmöglichkeiten.

Die Bewältigung der Herausforderungen stärkte die Teammoral

Mehr als die Hälfte der befragten IT-Manager (52 %) gab an, dass sich die Moral in ihrem Team im Laufe des Jahres 2020 verbesserte. Bei 26 % sank die Moral im Team dagegen und bei 22 % blieb sie unverändert.

Entwicklung der Moral in IT-Abteilungen im Laufe des Jahres 2020

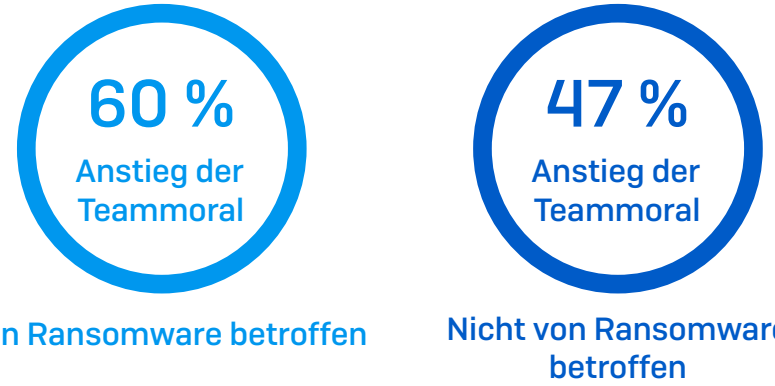
Im Laufe des Jahres 2020 gab es bei der Moral in unserem Team einen Anstieg/eine Abnahme/keine Veränderung [5.400] (ohne Berücksichtigung der Antwortoption „Ich weiß es nicht")

Im Ländervergleich wirkte sich die Pandemie vor allem in der Türkei (75 %), Österreich (71 %), Indien und Südafrika (jeweils 69 %) positiv auf die Moral im Team aus. Im Gegensatz dazu konnten vergleichsweise wenige IT-Manager in Israel (26 %), Frankreich (31 %), Italien (33 %) und Polen (36 %) einen Anstieg der Moral in ihrem Team feststellen.

Wie Sie vielleicht bemerkt haben, wurden mehrere dieser Länder bereits in anderen Abschnitten erwähnt. Die Türkei und Österreich, die den höchsten Anteil an Unternehmen aufwiesen, bei denen sich die Moral im Team verbesserte, zählten auch zu den vier Ländern, die am häufigsten einen Anstieg an Cyberangriffen meldeten. Frankreich, das Land mit dem zweitniedrigsten Anteil an Unternehmen, die eine Verbesserung der Moral in der IT-Abteilung feststellten, verzeichnete den geringsten Anstieg an Cyberangriffen. Der Zusammenhang zwischen Cyberangriffen auf Unternehmen und der Entwicklung der Teammoral zählt zu den bemerkenswertesten Ergebnissen unserer Umfrage.

Ein weiterer Beleg für diese Korrelation: Bei 60 % der befragten Unternehmen, die im vergangenen Jahr Opfer von Ransomware waren, stieg die Moral im Team (ggü. 47 % bei Unternehmen, die nicht von Ransomware betroffen waren).

Entwicklung der Moral in IT-Abteilungen im Laufe des Jahres 2020

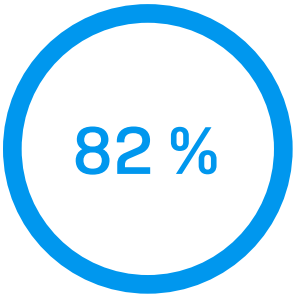


Im Laufe des Jahres 2020 gab es bei der Moral unserer Mitarbeiter einen Anstieg/eine Abnahme/keine Veränderung [5.400], wobei einige Antwortmöglichkeiten übersprungen wurden, nach Unternehmen, die im vergangenen Jahr von Ransomware betroffen waren

Dieser Zusammenhang ist aller Wahrscheinlichkeit nach auf mehrere Faktoren zurückzuführen. Herausforderungen – in diesem Fall Cyberangriffe – können den Zusammenhalt und die Moral im Team stärken, da alle Mitarbeiter an einem Strang ziehen und das gleiche Ziel verfolgen. Zudem wirkt sich die Erfahrung, das eigene Unternehmen im Kampf gegen zunehmende Cyberangriffe unterstützen zu können, positiv auf die Belegschaft aus. Den signifikantesten Anstieg der Moral in der IT meldeten das **Bildungs-** (58 %) sowie das **Gesundheitswesen** (57 %) – beide Bereiche traf die Pandemie besonders schwer.

Möglicherweise erhielt die IT aufgrund ihrer zentralen Rolle bei der Sicherstellung der Business Continuity im Verlauf der Pandemie auch mehr Anerkennung, was sich wiederum positiv auf die Moral im Team auswirken kann. Wenn das Engagement der IT bisher noch keine Anerkennung gefunden hat, ist jetzt der richtige Zeitpunkt, IT-Teams für ihren Einsatz zu würdigen.

IT-Abteilungen fühlen sich für die Herausforderungen der Zukunft gut gerüstet



sind der Meinung, dass sie über die nötigen Tools und die Expertise zur umfassenden Analyse verdächtiger Aktivitäten verfügen

Umfrageteilnehmer, die nach eigenen Angaben über die erforderliche Expertise und die nötigen Tools zur umfassenden Analyse verdächtiger Aktivitäten verfügen [5.400], wobei einige Antwortmöglichkeiten übersprungen wurden

Angesichts der höheren Arbeitsbelastung sowie der hohen Anzahl an Cyberangriffen im Jahr 2020 stimmt es positiv, dass 82 % der befragten IT-Manager angaben, über die erforderliche Expertise und die nötigen Tools zur umfassenden Analyse verdächtiger Aktivitäten in ihrem Unternehmen zu verfügen. Während der Pandemie konnten IT-Teams ihre Kompetenz und ihr Know-how erweitern und sind daher für die Herausforderungen der Zukunft gut gerüstet. Damit IT-Abteilungen auch in Zukunft mit dem kontinuierlichen Wandel der Bedrohungslandschaft Schritt halten können, müssen Unternehmen weiter in Tools und Weiterbildungsmaßnahmen investieren.

Wenn wir die Antworten jedoch im Branchenvergleich betrachten, stechen **Bundesbehörden und öffentliche Einrichtungen** (67 %) sowie **Behörden auf Landes- und Kommunalebene** (64 %) hervor. Behörden waren weltweit besonders schwer von der Pandemie betroffen. So mussten sie zum einen weiterhin systemrelevante Dienstleistungen anbieten und zum anderen Bürger und Unternehmen zusätzlich unterstützen. Dabei sind finanzielle Mittel im öffentlichen Sektor jedoch in vielen Ländern knapp bemessen, was sich auch wiederum in den begrenzten Ressourcen niederschlägt. Da Ransomware-Akteure Regierungsbehörden vermehrt ins Visier nehmen, sind die nötige Kompetenz sowie die erforderlichen Ressourcen zur effektiven Analyse verdächtiger Aktivitäten in diesem Bereich unerlässlich.

Die Zukunft von IT-Security-Abteilungen

Wie wir bereits gesehen haben, war 2020 ein sehr schwieriges Jahr für die IT. IT-Abteilungen meisterten die neuen Herausforderungen jedoch mit Bravour, was sich positiv auf ihre Kompetenzen und ihre Moral auswirkte. Die Erfahrungen der Pandemie sowie die Veränderungen in der IT im Allgemeinen (z. B. flexiblere Homeoffice-Arbeitsmodelle, Cloud-Nutzung) haben einen direkten Einfluss auf die Gestaltung von IT-Security-Abteilungen der Zukunft.

IT-Security-Abteilungen werden zügig wachsen

Angesichts der erhöhten Auslastung von IT-Abteilungen rechnen die befragten Unternehmen mit einem starken Anstieg an internem und externem IT-Security-Personal in den nächsten zwei Jahren:

- 68 % gehen davon aus, dass sie in den nächsten zwei Jahren mehr interne IT-Fachkräfte einstellen. 76 % rechnen mit einem Personalanstieg im Laufe der nächsten fünf Jahre
- 56 % prognostizieren einen Anstieg an externen IT-Security-Kräften in den nächsten zwei Jahren, 64 % in den nächsten fünf Jahren
- Lediglich 8 % erwarten einen Rückgang des internen Personals in den nächsten fünf Jahren

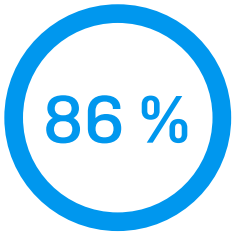
IT-Security-Ressourcen	Erwartete Änderungen	Bis 2023	Bis 2026
Internes IT-Security-Personal	Anstieg	68 %	76 %
	Rückgang	11 %	8 %
Externes IT-Security-Personal	Anstieg	56 %	64 %
	Rückgang	14 %	10 %

Wie wird sich der Umfang Ihrer IT-Security-Abteilung bis 2023 und 2026 Ihrer Meinung nach ändern? [5.400], wobei einige Antwortmöglichkeiten übersprungen wurden

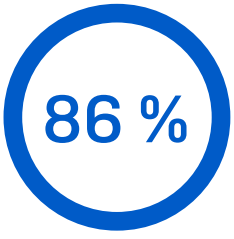
Interessanterweise geht das verstärkte Outsourcing nicht zu Lasten der internen Belegschaft. So rechnet fast die Hälfte (46 %) der befragten Unternehmen damit, bis 2023 sowohl mehr interne als auch mehr externe IT-Security-Fachkräfte zu beschäftigen. 55 % prognostizieren einen Anstieg bis zum Jahr 2026.

Insgesamt erwarten 77 % der befragten Unternehmen einen Anstieg in mindestens einem Bereich (interne oder externe IT-Security-Fachkräfte) in den nächsten zwei und 85 % in den nächsten fünf Jahren.

Zentraler Faktor: Künstliche Intelligenz



gehen davon aus, dass KI die Abwehr der steigenden Anzahl an Bedrohungen erleichtert



gehen davon aus, dass KI die Abwehr zunehmend komplexer Bedrohungen unterstützt

Unternehmen, die davon ausgehen, dass KI-Technologien die Bewältigung der steigenden Anzahl und/oder zunehmenden Komplexität von Bedrohungen unterstützen können [5.400], wobei einige Antwortmöglichkeiten übersprungen wurden

Fast alle IT-Abteilungen messen künstlicher Intelligenz eine wichtige Rolle bei der Abwehr rasant ansteigender und zunehmend komplexer Cyberbedrohungen bei. 86 % gehen davon aus, dass KI-Technologien die Bewältigung der steigenden Anzahl an Bedrohungen erleichtern können. Genauso viele Unternehmen rechnen damit, dass KI die Abwehr zunehmend komplexer Bedrohungen unterstützen kann. Dabei wählten 92 % mindestens eine der beiden Optionen aus.

Bauen Sie jetzt Ihre IT-Abteilung der Zukunft auf

Beginnen Sie schon heute mit dem Aufbau Ihres IT-Teams von morgen. Nutzen Sie die direkte Erfahrung von IT-Managern in aller Welt, um wesentliche Weichenstellungen für eine erfolgreiche, zukunftsgerichtete Cybersecurity vorzunehmen. Auf Basis der Umfrageergebnisse haben wir die folgenden fünf Tipps für Sie ausgearbeitet:

1. Entlasten Sie Ihre IT durch geeignete Tools und Strategien

Die Arbeitsauslastung von IT-Security-Abteilungen sowie der IT im Allgemeinen nahm im vergangenen Jahr eindeutig zu. Mit Tools und Strategien zur Entlastung der IT-Security schaffen Sie Kapazitäten und Ressourcen für andere Aufgaben.

- **Automatisierung.** Automatisieren Sie aufwändige Routineaufgaben, damit sich die IT auf Strategieprojekte konzentrieren kann. Keine Frage: Maschinen reagieren schneller als Menschen. Automatisierung minimiert folglich sowohl Reaktionszeiten als auch das Angriffsrisiko.
- **Konsolidierung.** Verwalten Sie alle Ihre Cybersecurity-Lösungen über eine zentrale Konsole, um den täglichen Verwaltungsaufwand auf ein Minimum zu reduzieren. So muss Ihre IT nicht mehr zwischen verschiedenen Konsolen jonglieren, Daten aus unterschiedlichen Quellen korrelieren oder Security-Lösungen in separaten System verwalten – und spart wertvolle Zeit und Ressourcen. Durch die Konsolidierung Ihrer IT-Security senken Sie zudem Ihre Kosten beim Anbieter-Management.
- **Integration.** Entscheiden Sie sich für integrierte Lösungen, die perfekt aufeinander abgestimmt sind. Auf diese Weise lassen sich Aufgaben besser automatisieren. Außerdem können Sie so problemlos produktübergreifende Analysen durchführen und erhalten deutlich mehr Einblick in Ihren Sicherheitsstatus.

2. Investieren Sie in Tools und Weiterbildung, damit Ihre IT auf dem neuesten Stand ist

Im vergangenen Jahr konnten sich IT-Teams viele neue Kompetenzen aneignen. Unternehmen sollten daher in Tools und Weiterbildung investieren, damit IT-Teams ihre neue Expertise nutzen und weiter ausbauen können. Diese Ressourcen unterstützen Sie zudem bei der Rekrutierung qualifizierter Bewerber.

3. Setzen Sie auf interne und externe IT-Experten

Mehr als die Hälfte der befragten IT-Manager können komplexe Cyberbedrohungen bereits nicht mehr selbst bewältigen. Kombinieren Sie das fundierte Cybersecurity-Know-how externer Partner mit den umfassenden Unternehmenskenntnissen und der Expertise Ihrer internen IT. So können Sie schneller und besser auf Veränderungen reagieren, da Ihnen die besten Ressourcen für jede Situation zur Verfügung stehen. Ein idealer Security-Partner ergänzt die Kompetenzen und Kapazitäten Ihrer internen IT-Abteilung perfekt und passt sich flexibel an Ihre Betriebsabläufe an.

4. Gewinnen Sie die besten Bewerber aus aller Welt für sich

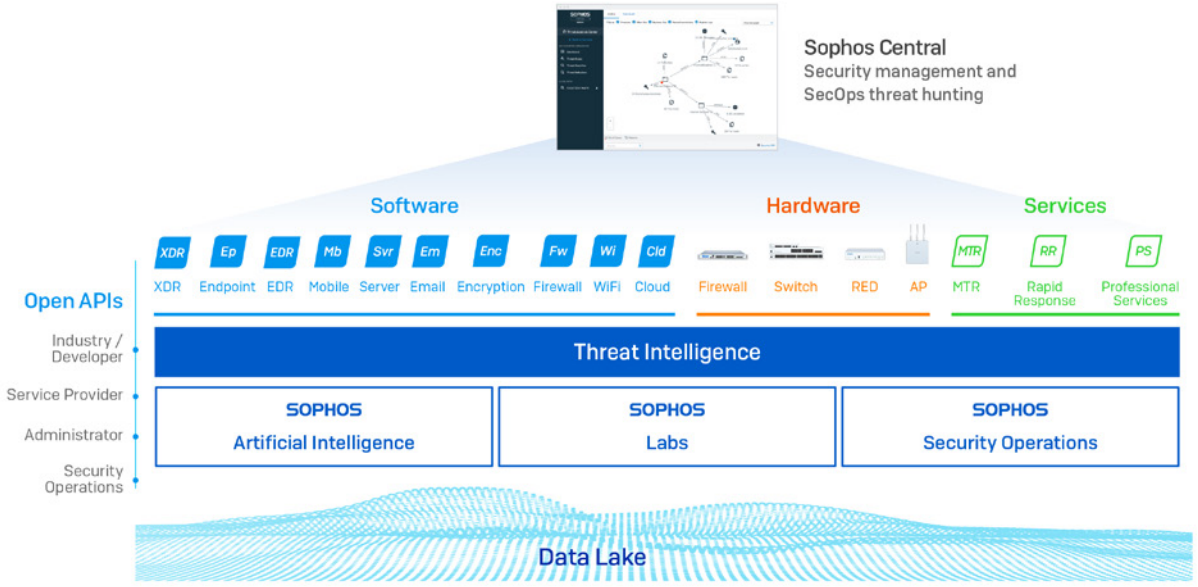
Da viele Unternehmen eine Erweiterung ihrer IT-Abteilung planen, wird der Wettbewerb um qualifiziertes Personal immer intensiver. Eine Investition in innovative Technologien, die sich von überall verwalten lassen, erleichtert Ihnen den Aufbau Ihres Talentpools. Denn wie die Pandemie gezeigt hat, lassen sich heutzutage fast alle IT-Aufgaben bei Bedarf auch remote durchführen. Außerdem locken Sie mit erstklassigen Tools die besten Bewerber an.

5. Stärken Sie das Know-how Ihrer internen Fachkräfte

Schon jetzt herrscht ein Mangel an qualifizierten Cybersecurity-Experten. Halten Sie deshalb nicht nur nach neuen Mitarbeitern Ausschau, sondern stärken Sie auch die Expertise und das Know-how Ihrer bereits vorhandenen internen Fachkräfte mit In-House-Angeboten und praktischen Trainings im Job. Das Bild vom über die Tastatur gebeugten Computer-Nerd im Hoodie mag ein Klischee sein. Doch es zeigt auch, dass viele Cybersecurity-Spezialisten ihr Know-how nicht über die klassischen Karrierepfade erworben haben.

Wie Sophos helfen kann

Sophos unterstützt IT-Abteilungen in über 500.000 Unternehmen und 150 Ländern bei der Abwehr von Cyberbedrohungen.



Sophos Adaptive Cybersecurity Ecosystem (ACE)

- Wir bieten ein umfassendes Portfolio an **Next-Gen-Technologien** mit der Power von **künstlicher Intelligenz.** Unsere Produkte sind perfekt aufeinander abgestimmt, automatisieren manuelle Aufgaben und minimieren das Bedrohungsrisiko. Wir nennen diese leistungsstarke Kombination Synchronized Security. Kunden, die unseren Endpoint- und Firewall-Schutz nutzen, verzeichnen regelmäßig um mindestens 50 % geringere IT-Verwaltungskosten und weniger Sicherheitsvorfälle.
- Mit **Sophos Extended Detection and Response (XDR)** und **Sophos Endpoint Detection and Response (EDR)** erkennt und beseitigt Ihre IT Bedrohungen und Sicherheitsprobleme schnell und einfach. Sophos EDR ist die erste speziell für Sicherheitsanalysten und IT-Administratoren entwickelte EDR-Lösung, mit der IT-Teams fundiertes Expertenwissen entwickeln – ohne zusätzliches Personal.
- Die Next-Gen-Produkte von Sophos werden über unsere webbasierte Security-Plattform **Sophos Central** verwaltet. Mit ihr können Sie Ihre Sophos-Lösungen von überall aus steuern und müssen sich bei der Suche nach dem besten IT-Security-Personal nicht auf bestimmte Regionen beschränken.
- Mit **Sophos Managed Threat Response (MTR)** und **Sophos Rapid Response** stehen Ihrer IT unsere Rundum-Service-Teams zur Seite, die Bedrohungen aktiv bekämpfen und gezielte Reaktionsmaßnahmen ergreifen. Dabei kontrollieren Sie, wie und wann potenzielle Vorfälle eskaliert werden und welche Maßnahmen wir ggf. einleiten sollen.
- Unsere Schutzlösungen basieren auf der kollektiven Threat Intelligence aus den **SophosLabs, den Sophos Security Operations,** der **Sophos KI** sowie dem **Sophos Data Lake.**
- Dank **offener APIs** profitieren unsere Kunden von den Erkenntnissen und Telemetriedaten unserer Partner in aller Welt.

Sie möchten mehr über unsere Lösungen und darüber erfahren, wie wir Ihre IT unterstützen können? Besuchen Sie unsere Website oder wenden Sie sich an einen Sophos-Ansprechpartner.

Sie möchten mehr über unsere Lösungen und darüber erfahren, wie wir Ihre IT unterstützen können? Besuchen Sie unsere Website oder wenden Sie sich an einen Sophos-Ansprechpartner.

Sophos bietet branchenführende Cybersecurity-Lösungen für Unternehmen jeder Größe und schützt Kunden in Echtzeit vor komplexen Bedrohungen, wie Malware, Ransomware und Phishing. Bewährte Next-Gen-Funktionen mit der Power von Machine Learning und künstlicher Intelligenz sichern Unternehmensdaten effektiv.

2021-05-20 (WP-NP)

SOPHOS