

# MEHR SICHERHEIT FÜR JEDES UNTERNEHMEN

Ein Leitfaden für Unternehmen jeder Größe

# HOMEOFFICE UND SICHERHEIT

Die Arbeit im Homeoffice war bei Arbeitnehmerinnen und Arbeitnehmern beliebt, lange bevor sie zur Pflicht wurde. Umfragen vor der Pandemie ergaben, dass 98 % der Arbeitnehmerinnen und Arbeitnehmer gerne dauerhaft die Möglichkeit hätten, auch von zu Hause aus zu arbeiten.<sup>1</sup>

Die Pandemie hat Wunsch und Wirklichkeit einander angenähert. Vor der Pandemie arbeiteten vergleichsweise wenige Menschen in Deutschland im Homeoffice: Zwar hatten 56 % der Arbeitnehmerinnen und Arbeitnehmer die technischen Möglichkeiten, um von zu Hause aus zu arbeiten, aber nur etwa die Hälfte davon arbeitete tatsächlich im Homeoffice. Ab März 2020 stieg die Zahl derer, die von zu Hause aus arbeiten, von knapp 30 % auf über 66 % – und damit um mehr als das Doppelte gegenüber Vorpandemiezeiten.

Unter diesen veränderten Bedingungen geht mit Online-Meeting, dem Austausch von Dokumenten, Zusammenarbeit und Datenübermittlung ein erhöhtes Risiko einher. Ganz zu schweigen von dem sprunghaften Anstieg der Anzahl an Endgeräte, durch die jetzt Daten fließen, von veralteten Desktop-Computern über Tablets bis hin zu Smartphones. Für die Sicherheit bedeutet das neue dezentrale Arbeiten:



# HOMEOFFICE UND SICHERHEIT



## 1. DAS HOMEOFFICE IST DAS NEUE LIEBLINGSZIEL FÜR CYBERKRIMINALITÄT

Die Cybersicherheit im Homeoffice ist geringer als in Firmennetzwerken und auf von Unternehmen zur Verfügung gestellten Endgeräten. Das liegt u. a. daran, dass im Homeoffice persönliche Wi-Fi-Verbindungen, private mobile Endgeräte und private Apps genutzt werden und sich die Internetnutzung der Mitarbeitenden nur schwer kontrollieren und überwachen lässt. Ihr Unternehmensnetzwerk wurde wahrscheinlich nicht für das Arbeiten im Homeoffice eingerichtet, sodass Ihnen vielleicht noch immer die richtigen Sicherheitsprotokolle fehlen.

## 2. DATENSCHUTZ IST WEITERHIN WICHTIG

Je digitaler Unternehmen arbeiten, desto attraktiver werden sie für Hackerinnen und Hackern, die bei weniger gut geschützten Heimnetzwerken leichtes Spiel haben und sich Zugang zu Daten verschaffen. Auch Großkonzerne kämpfen mit diesen Herausforderungen. Kleine und mittlere Unternehmen stehen bei ähnlichen Risikofaktoren, aber geringeren Ressourcen vor besonderen Problemen.

Unter dem Strich zeigen sich erhebliche Sicherheitsmängel:

- **Starker Anstieg bei Cybersicherheitsvorfällen:** 61 % der Unternehmen haben im Jahr 2019 Vorfälle gemeldet.<sup>2</sup>
- **Zu wenige moderne Sicherheitsmaßnahmen:** Nur 8 % aller weltweiten Administratoren in Microsoft 365 sind durch Multi-Faktor-Authentifizierung (MFA) geschützt.<sup>3</sup>

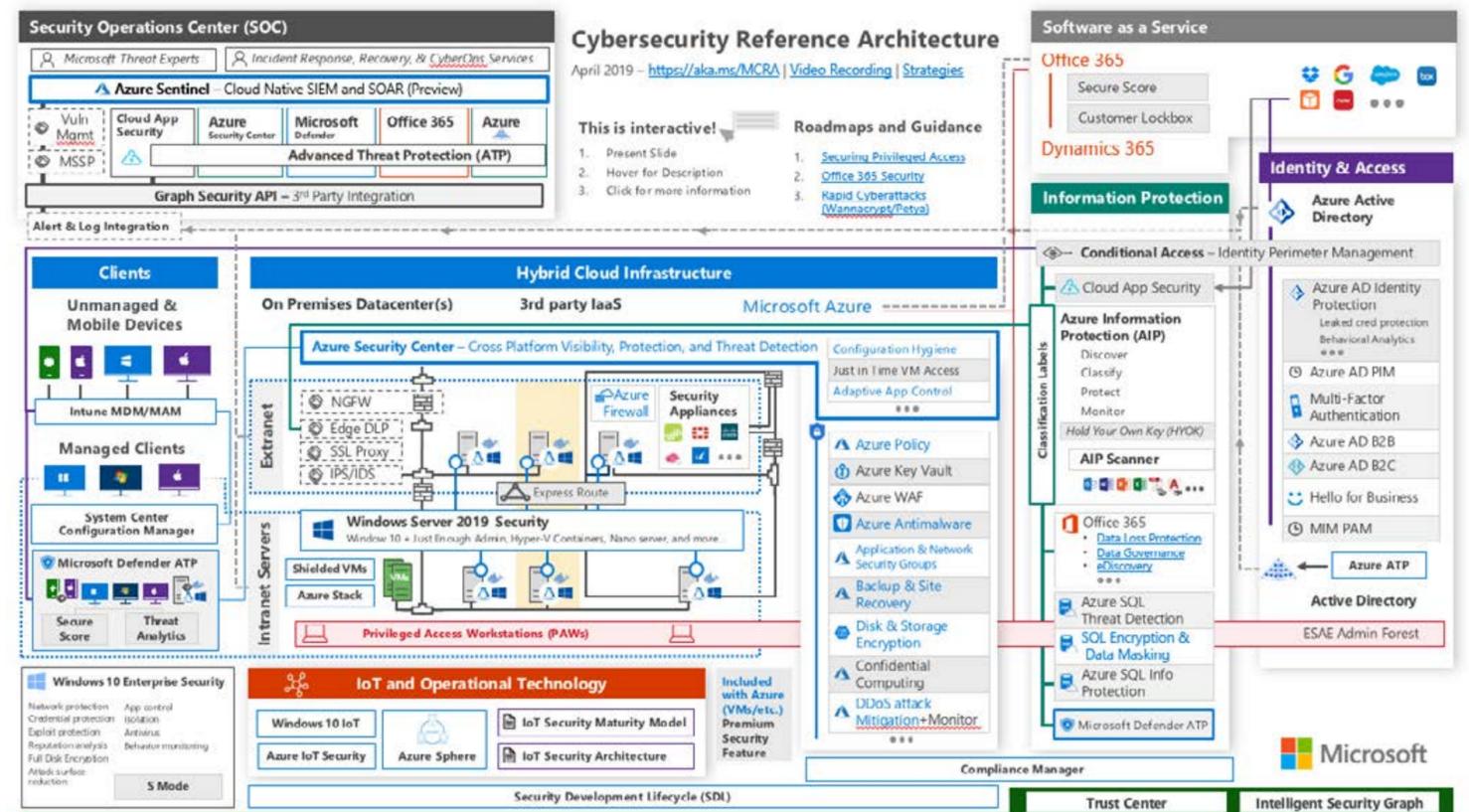
Wenn dokumentiert und verwaltet, senken diese Faktoren das Sicherheitsrisiko von Microsoft Tenants deutlich auf durchschnittlich 32/539.<sup>4</sup> Das geht aber noch besser! In diesem E-Book erfahren Sie, mit welchen Methoden Conexxos den Grad der Sicherheit von kleinen und mittleren Unternehmen um das Vier- bis Fünffache erhöhen kann.

# PROBLEM CYBERSICHERHEIT UND IHRE HERAUSFORDERUNGEN FÜR KLEINE UNTERNEHMEN

Zu viele kleine und mittlere Unternehmen sind den Anforderungen, die Homeoffice-Arbeit, Geschäftswachstum und sich ständig wandelnde Cyberrisiken mit sich bringen, nicht gewachsen. Nahezu unmöglich scheint es, die wachsenden Sicherheitsanforderungen kosteneffektiv zu erfüllen. Schließlich benötigt man zur Überwachung und Instandhaltung von guten Sicherheitslösungen Lizenzen, Personal, Instrumente und Ressourcen. Ganz zu schweigen von der Anforderung, eine reibungslos funktionierende Arbeitsumgebung zu schaffen und aufrechtzuerhalten, in der Sicherheit, Datenschutz und Privatsphäre gewahrt bleiben und in der auch die Freude an der Arbeit nicht zu kurz kommt. Die Messlatte liegt hoch! Und selbst wenn Unternehmen das alles können, ist die Verwaltung messbarer Sicherheit mit Microsoft 365 mitunter komplex und teuer.

Dazu kommt bei kleinen und mittleren Unternehmen:

- mangelndes internes Wissen zum Thema Cybersicherheit,
- Fachkräftemangel im Bereich Sicherheitstechnik, selbst wenn genügend Ressourcen vorhanden sind, um solche Fachkräfte einzustellen
- hohe Fixkosten für die Umsetzung und Überwachung von Sicherheitslösungen



*Glauben Sie keinem, der Ihnen weismachen will, dass Cybersicherheit für kleine und mittlere Unternehmen nicht komplex ist.*

# WAS IST EINE SICHERHEITSBEWERTUNG UND WAS BRINGT SIE?

Mit einer Sicherheitsbewertung können Sie Ihren Sicherheitsstatus regelmäßig genau unter die Lupe nehmen. Durch Quantifizierung einzelner Sicherheitsaspekte erhalten Sie einen nachvollziehbaren, detaillierten Überblick über Ihren aktuellen Sicherheitsstatus. Der Sicherheitsbericht gibt Ihnen z. B. Auskunft über:

- ✓ den Gesamtstatus Ihrer Sicherheitseinstellungen und durchgeführte Änderungen
- ✓ Ihre App-, Cloud- und Exchange-Einstellungen
- ✓ den Status Ihrer IOS-App-Schutzrichtlinien
- ✓ Ihren Sicherheitsstatus (in übersichtlicher Form)
- ✓ Anti-Virus-Maßnahmen, z. B. Postfachrichtlinien
- ✓ mobile Postfachrichtlinien
- ✓ SharePoint- und OneDrive-Sicherheitseinstellungen
- ✓ alle Gerätebeschränkungen in Windows 10
- ✓ Lizenzen, Benutzer und Gruppen
- ✓ eine Sicherheitsbewertung mit Protokollen und Vergleichen

# MEHR SICHERHEIT IN DREI SCHRITTEN

Wir von Conexxos haben einen Prozess entwickelt, der drei Schritte umfasst und für Unternehmen jeder Größe schnell und einfach anwendbar ist

## 1. Analyse Ihres Tenants

Mit Conexxos können Sie Ihr Tenant auf Schwachstellen überprüfen. So erhalten Sie eine Bewertung Ihres allgemeinen Sicherheitsstatus sowie ausführliche Ergebnisse und Empfehlungen zur Erhöhung Ihrer Sicherheit.

## 2. Einrichtung eines individuellen Sicherheitsdienst

Auf der Grundlage der Ergebnisse der Sicherheitsbewertung richten Sie mit nur einem Klick ein Managed-Security-Tool ein, das die richtigen Sicherheitseinstellungen vornehmen und anwenden kann. So konfigurieren Sie Ihr Microsoft Tenant automatisch im Sinne höchster Sicherheit. Das alles bietet Ihnen unsere Sicherheitslösung Managed Security 365 – fast ohne Aufwand für Sie!

## 3. Überwachen Sie Ihre Sicherheitseinstellungen

Sobald Managed Security 365 (in einem sehr schnellen Verfahren) eingerichtet ist, wird Ihr Tenant konsequent überwacht und werden Ihre Sicherheitseinstellungen laufend überprüft. Ändert oder löscht ein/e BenutzerIn unbefugt die festgelegten Sicherheitseinstellungen, korrigiert das Sicherheitstool diese falschen Einstellungen automatisch. Eine Lösung wie Managed Security 365 entwickelt sich ständig und passt sich an aktuelle Bedrohungen und Sicherheitslagen an. Dadurch sind Sie vor neuen Risiken geschützt, ohne Ressourcen zu deren Ermittlung oder Bekämpfung abstellen zu müssen.



## DANK MANAGED SECURITY 365 KONNTEN UNTERNEHMEN:

- ✓ Analyse- und Planungszeiten um 50 % reduzieren
- ✓ Implementierungs- und Bereitstellungsprozesse um das Zehnfache beschleunigen
- ✓ Überwachungs- und Einsatzzeiten um 80 % senken
- ✓ die Einführung neuer Sicherheitsmaßnahmen um 300 % erhöhen

# MESSBAR MEHR SICHERHEIT FÜR UNTERNEHMEN ALS SERVICE



Sicherheit ist wahrscheinlich nicht das Kerngeschäft Ihres Unternehmens, und vermutlich nicht einmal ein Bereich, für den Sie mehr Ressourcen und Geld aufwenden möchten als unbedingt nötig. Hier kommt Conexxos ins Spiel! Mit einem Partner wie uns erhalten Sie die Sicherheit und die messbaren Ergebnisse, wie sie sonst nur den ganz großen Unternehmen vorbehalten sind – aber zu geringeren Kosten. Der ideale Sicherheitspartner sollte:

## **Mehr als Sicherheitsmaßnahmen bieten, damit die digitale Transformation gelingt**

Transformation hat viele Gesichter. Ihr Partner sollte Sie dabei unterstützen, flexible und skalierbare Lösungen für die digitale Transformation Ihres Unternehmens zu entwickeln. Wir bei Conexxos bewerten Ihre aktuelle Situation und stimmen unsere Lösungen auf Ihre Infrastruktur, Ihr Budget, die Größe Ihres Unternehmens und Ihr Team ab. So können Sie die Produktivität Ihrer Mitarbeitenden durch nahtlose Zusammenarbeit sicher skalieren und verbessern.

## **Ihnen ein virtuelles Team für Cybersicherheit zur Seite stellen**

Große Unternehmen haben Teams für Cybersicherheit, die über die Zeit und die Ressourcen verfügen, um Cyberrisiken einen Schritt voraus zu sein. Ihre Mitarbeitenden haben all das vermutlich nicht. Kein Problem: Conexxos bietet kosteneffektive Lösungen. Wir investieren fortwährend in modernste Technologie

und Tools, um sicherzustellen, dass unsere Sicherheitslösungen auf dem neusten Stand sind und bewährten Praktiken entsprechen – damit IT-Kosten kein Problem mehr für Sie sind. Wir schützen Ihr Unternehmen, indem wir unsere Lösungen von Microsoft-SpezialistInnen entwickeln lassen, sie ständig aktualisieren und an neue Bedrohungen anpassen.

## **Sie zuverlässig und lückenlos vor Datenverlust schützen**

Unsere Sicherheitsüberwachung funktioniert rund um die Uhr und schützt Sie so vor Datenverlust, finanziellen Schäden- und Imageschäden. Wir ermitteln kontinuierlich und proaktiv Risiken und liefern Ihnen Sicherheitsberichte und -bewertungen zum Sicherheitsstatus Ihres Unternehmens.

## **Mühe los alle Ihre regulatorischen und Compliance-Anforderungen erfüllen**

Managed Security 365 unterstützt Sie bei der Erfüllung gesetzlicher Anforderungen wie der DSGVO. Dank automatisierter Einführung von bewährten Sicherheitsverfahren, kontinuierlicher Überwachung, automatischer Fehlerkorrektur sowie Funktionen für Berichterstattung und E-Mail-Archivierung wird Ihr Compliance-Management deutlich vereinfacht.

# SO FINDEN SIE IHREN PARTNER FÜR MANAGED SECURITY

1

Ist Ihr Partner in der Lage, regelmäßig und ausführlich Bericht zu erstatten über den Sicherheitsstatus von:

- |   |                                     |
|---|-------------------------------------|
| <input type="checkbox"/> Microsoft Office 365 | <input type="checkbox"/> Exchange   |
| <input type="checkbox"/> Teams                | <input type="checkbox"/> SharePoint |
| <input type="checkbox"/> AzureAD?             |                                     |

2

Bietet er Ihnen umfassenden Geräteschutz und die Endpunktverwaltung für Geräte, die folgende Systeme nutzen:

- |   |                                      |
|---|--------------------------------------|
| <input type="checkbox"/> Microsoft Endpoint Manager | <input type="checkbox"/> Android     |
| <input type="checkbox"/> IOS                        | <input type="checkbox"/> Windows 10? |

3

Bietet er Ihnen Lösungen für das Identity- und Access-Management und Features zur Unterstützung von: Azure Active Directory und Azure Active Directory Extended Audit Logs?

- Ja  Nein

4

Bietet er Ihnen eine Übersicht der Sicherheitsbewertungen für verschiedene Benutzerkonten, sodass alle Sicherheitsbewertungen an einem Ort zusammengeführt werden?

- Ja  Nein

5

Bieten er Ihnen alles, was Sie brauchen, um eine skalierbare und wiederholbare automatisierte Sicherheitspraxis einzurichten?

- Ja  Nein

# JETZT UPGRADE FÜR MEHR MESSBARE CYBERSICHERHEIT HOLEN

Das Team von Conexxos macht Cybersicherheit für Ihr Unternehmen nicht nur messbar, sondern auch verwalt- und bezahlbar. Kontaktieren Sie uns und erfahren Sie, wie auch Sie sich mehr Sicherheit, Effizienz und Agilität holen können.

Machen Sie den nächsten Schritt