Mitarbeitende schüren das Risiko einer Cyberattacke

15.07.2026, 10:24 | IT, New Media & Software

Pressemitteilung von: *Press'n'Relations GmbH*

Eine aktuelle Erhebung von WatchGuard Technologies zeigt, dass das Verhalten der Belegschaft von kleinen und mittelständischen Unternehmen (KMU) mit erheblichen und oft verborgenen Cybersicherheitsrisiken einhergeht. Laut dem Cybersecurity Hygiene Report 2026 geben 64 Prozent der Befragten zu, nicht autorisierte KI-Tools für ihre Arbeit zu nutzen. Das Problem der „Schatten-KI" wird damit offensichtlich: Da viele Unternehmen keine Kenntnisse darüber haben, welche KI-Werkzeuge im eigenen Geschäftsalltag tatsächlich zum Einsatz kommen, stehen sie auch den damit einhergehenden Gefahren blind gegenüber. Gleichzeitig gibt es hinsichtlich anderer, vielerorts gängiger Gewohnheiten am Arbeitsplatz keine Entwarnung: 76 Prozent der Mitarbeitenden verwenden Passwörter mehrfach, 70 Prozent nutzen öffentliches WLAN für die Arbeit und 50 Prozent greifen ohne VPN-Schutz auf Unternehmensressourcen zu. Das Risiko von Identitätsdiebstahl, Datenabfang und unbefugtem Zugriff ist somit allgegenwärtig.

„Unternehmen investieren zwar in Sicherheitslösungen, doch vielen fehlt es nach wie vor an Einblick in die tatsächlichen Arbeitsabläufe ihrer Mitarbeiterschaft", so Marc Laliberte, Director of Security Operations bei WatchGuard. „Alltägliche Verhaltensweisen – von der Nutzung künstlicher Intelligenz bis hin zum verbesserungswürdigen Umgang mit Passwörtern – bergen Risiken, für deren Bewältigung herkömmliche Kontrollmechanismen nicht ausgelegt sind."

Wachsende Transparenzlücken mit zunehmender Verbreitung von KI
KI-Tools für den Privatgebrauch bilden inzwischen eine ganz eigene Kategorie im Hinblick auf die vielfältigen geschäftlichen Sicherheitsrisiken. Nur wenige Unternehmen haben bisher mit einem verbindlichen Governance-Ansatz darauf reagiert. Wie im Bericht dargelegt, glauben weniger als 30 Prozent der Befragten, dass ihr Unternehmen über eine genaue Bestandsaufnahme der intern eingesetzten Software verfügt. Fast 40 Prozent gehen davon aus, dass ihr Arbeitgeber nicht genau weiß, welche Anwendungen die Belegschaft wie nutzt.

Dieser Mangel an Steuerung – einschließlich organisatorischer Vorgaben hinsichtlich zugelassener Tools und einer Konkretisierung, welche Informationen überhaupt weitergegeben werden dürfen – schafft einen gefährlichen blinden Fleck für IT- und Cybersicherheitsteams.

Etablierte Gewohnheiten als weitere sicherheitsrelevante Herausforderung
Abgesehen von „Schatten-KI" untergraben auch andere, weit verbreitete Verhaltensweisen die Sicherheitsmaßnahmen von Unternehmen und eröffnen Hackern zusätzliche Angriffsmöglichkeiten:

- 76 Prozent der Befragten geben zu, für mehrere Konten dasselbe Passwort zu verwenden. Das bedeutet, dass

bereits ein einziger kompromittierter Zugangsdatensatz ein Unternehmen anfällig für Kontoübernahmen, laterale Bewegungen und umfangreichen Datendiebstahl über mehrere Systeme, Plattformen und Anwendungen hinweg macht. Darüber hinaus gaben 30 Prozent der Befragten an, ihre Passwörter an andere weiterzugeben.

- 70 Prozent nutzen im Geschäftsalltag öffentliches WLAN, während 50 Prozent ohne VPN-Schutz auf Unternehmensressourcen zugreifen. Dies vergrößert die Angriffsfläche eines Unternehmens erheblich und erhöht das Risiko von Datendiebstahl, Missbrauch von Zugangsinformationen und unbefugtem Netzwerkzugriff. Bedrohungen wie beispielsweise Man-in-the-Middle-Angriffe zielen genau auf solche ungesicherten Verbindungen ab.
- 55 Prozent nutzen ihre Arbeitsgeräte ebenso für private Zwecke. Damit wächst die Gefahr im Rahmen von Malware-Infektionen, Phishing-Angriffen und Zugriffen auf Anwendungen oder Websites, bei denen Sicherheitskontrollen des Unternehmens gezielt umgangen werden. Der Wechsel zu Hybrid- und Remote-Arbeit hat die Grenzen zwischen Privat- und Berufsleben verwischt und Angreifern neue Chancen eröffnet, Unternehmensdaten zu kompromittieren. Für Sicherheitsteams wird es dadurch immer schwieriger, Risiken wirksam zu mindern.

Mit MSP-Unterstützung dem Security-Anspruch standhalten
Zunehmender Produktivitätsdruck, sich wandelnde Arbeitsumgebungen und die rasante Einführung neuer Technologien führen zu riskantem Verhalten in der gesamten Belegschaft. Hier können Managed Service Provider (MSP) Stärke beweisen und kleinen und mittleren Unternehmen dabei helfen, Lücken in der Cybersicherheitshygiene zu schließen, bevor diese zu schwerwiegenden Vorfällen führen.

„Die Erkenntnisse der Umfrage verdeutlichen einen grundsätzlichen Wandel in Bezug auf Cybersicherheitsrisiken. Da Unternehmen neue Technologien einführen und dezentrales Arbeiten fördern, wird insbesondere der Umgang mit menschlichem Verhalten zu einer zentralen Anforderung“, so Laliberte. „Für MSP bietet sich hier die Chance, über die Technologie hinaus in neue Bereiche der Wertschöpfung vorzudringen – mit Fokus auf eine transparente Darstellung von Nutzerrisiken, Richtlinien-Governance und die kontinuierliche Sensibilisierung für Sicherheitsfragen.“

WatchGuard empfiehlt kleinen und mittleren Unternehmen sowie MSP-Partnern, sich auf sechs praktische Maßnahmen zu konzentrieren: die Durchsetzung einer flächendeckenden Nutzung von Passwort-Managern und Multifaktor-Authentifizierung (MFA), die gezielte Identifikation der unbefugten Nutzung oder des Einsatzes von „Schatten-KI“, die Festlegung klarer Richtlinien zur zulässigen Nutzung von KI, die Ausweitung des Schutzes über das Büro hinaus durch VPN und Zero-Trust-Ansätze sowie die Durchführung kontinuierlicher Sicherheitsschulungen bei gleichzeitiger Erfassung von Kennzahlen zu menschlichen Risiken neben technischen Indikatoren.

Der vollständige „Cybersecurity Hygiene Report 2026“ ist online verfügbar: https://www.watchguard.com/de/wgrd-resource-center/2026-cyber-hygiene-report

Methodik
Die Ergebnisse basieren auf einer im April 2026 durchgeführten unabhängigen Online-Umfrage unter 684 Mitarbeitenden auf Seiten kleiner und mittelständischer Unternehmen (50–500 Mitarbeiter) in den USA, Großbritannien, Deutschland, Frankreich, Spanien, Australien, Mexiko und Brasilien. Alle Prozentangaben spiegeln das von den Mitarbeitenden selbst angegebene Verhalten wider.

Press'n'Relations GmbH

Magirus-Deutz-Straße 14
89077 Ulm
Deutschland

RebeccaHorn

rh@press-n-relations.de

press-n-relations.com

Portrait

WatchGuard Technologies ist ein weltweit führender Anbieter von einheitlichen Cybersicherheitslösungen, die speziell für Managed Service Provider entwickelt wurden. Mit seiner Unified Security Platform® sorgt WatchGuard für umfassende Sicherheit und verbindet die Produkte für Netzwerksicherheit, Endpoint Security sowie zur Absicherung von Identitäten mit KI- und Zero-Trust-Technologien für einen starken, skalierbaren Schutz. Mithilfe von Funktionen wie „Cloud Detection and Response“ (CloudDR) unterstützt WatchGuard Unternehmen nicht zuletzt dabei, Schatten-IT und die unbefugte Nutzung von KI-Anwendungen zu erkennen und zu durchdringen – für einen besseren Überblick über neu auftretende Risiken in Cloud-Umgebungen.

Mehr als 25.000 Security-Reseller bzw. Managed Service Provider und über 1,5 Millionen Kunden weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau. Dabei hilft WatchGuard Partnern, schnell zu wachsen, operative Hindernisse zu beseitigen und starke Ergebnisse zu erzielen – alles aus einer Hand und ohne zusätzliche Konsolen oder Komplexität. Neben der Zentrale in Seattle im US-Bundesstaat Washington verfügt WatchGuard über Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum.

Aktuelle Informationen, Aktionen und Updates finden Sie auch auf X, Facebook oder LinkedIn. Der deutschsprachige Unternehmensblog beleuchtet zudem regelmäßig aktuelle Trendthemen im Umfeld von IT-Sicherheit. Reinschauen lohnt sich. Oder Sie abonnieren den „443 – Security Simplified“-Podcast über das WatchGuard Cybersecurity Hub bzw. wo immer Sie Ihre Lieblings-Podcasts finden.

Pressekontakt

WatchGuard Technologies GmbHDr. Alfred-Herrhausen-Allee 26
47228 Duisburg
Deutschland

PaulMoll (Senior Field Marketing Manager Central Europe)

paul.moll@watchguard.com

www.watchguard.com/de

News-ID: 1318150 • Views: 75 (Stand: 27.07.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1318150/Mitarbeitende-schueren-das-Risiko-einer-Cyberattacke.html