Keeper Security 2022 Cybersecurity Census Report: Deutsche Unternehmen sind nur unzureichend gegen die zunehmenden Cyberangriffe gewappnet und haben einen geringen Fokus auf die Sicherheit von Anmeldeinformationen

- Fast ein Viertel (24 %) der deutschen Unternehmen ist an jedem Arbeitstag etwa zwei Cyberangriffen ausgesetzt
- Identitäts- und Passwortdiebstahl ist eines der größten Risiken, aber nur 13 % der Befragten haben ein hochentwickeltes Regelwerk für die Sichtbarkeit und Kontrolle der Identitätssicherheit eingerichtet
- Nur ein Drittel (32 %) der Befragten gibt an, dass sie planen, in die Verwaltung von Passwörtern oder Infrastrukturgeheimnissen zu investieren
- 47 % der deutschen IT-Führungskräfte erwarten, dass die Gesamtzahl der Cyberangriffe und die Zahl der erfolgreichen Angriffe im nächsten Jahr steigen wird
- Mehr als die Hälfte (51 %) der deutschen IT-Leiter hat einen Cyberangriff auf ihr Unternehmen geheim gehalten

München, 6. Dezember 2022 – Cyberattacken treffen Unternehmen aller Größen und Branchen in ganz Deutschland, aber nur ein Bruchteil von ihnen ist darauf vorbereitet, sich dagegen zu verteidigen, so die neue Studie von Keeper Security. Der Cybersecurity Census Report 2022 zeigt, dass Unternehmen schwere organisatorische, finanzielle und rufschädigende Schäden erleiden. Obwohl die IT-Verantwortlichen davon ausgehen, dass sich dieser Ansturm im nächsten Jahr noch verstärken wird, ist nur eine Minderheit der Unternehmen auf die Bedrohungen vorbereitet.

Nach wie vor große Lücken bei der Sicherheit von Anmeldedaten
Die Identitätssicherheit stellt ein besonders großes Risiko dar, obwohl gestohlene und kompromittierte Anmeldedaten die häufigste Art und Weise sind, wie Cyberkriminelle in das Netzwerk eines Unternehmens eindringen. Überraschenderweise verfügen nur 13 % der Unternehmen in Deutschland über ein hochentwickeltes System zur Regelung des Systemzugangs. Noch bedenklicher ist, dass 31 % es den Mitarbeitern überlassen, ihre eigenen Passwörter festzulegen und der Zugang häufig gemeinsam genutzt wird. Dies scheint ein weltweites Problem zu sein. In Frankreich geben nur 18 % eine Anleitung für Passwörter, im Vereinigten Königreich sind es 21 %, und in den USA bestätigen 26 %, dass sie ein ausgefeiltes System haben.

„Wir sprechen seit Jahrzehnten über die Sicherheit von Passwörtern und Anmeldedaten und haben starke, einfach zu bedienende Lösungen auf dem Markt. Es ist enttäuschend, dass Unternehmen immer noch so sorglos mit dem Zugang zu ihren Netzwerken umgehen", sagt Rainer Enders, Vice President of Engineering bei Keeper Security. „Mindestens die Hälfte der Unternehmen in Deutschland, Frankreich, Großbritannien und den USA geben ihren Mitarbeitern einige Hinweise zu Passwörtern und zur Zugangsverwaltung. Viele stellen jedoch nicht sicher, dass diese Hinweise auch befolgt werden. Dies stellt ein völlig unnötiges und sehr hohes Risiko dar."

Die Zahl der Angriffe ist auf einem hohen Niveau
Der Bericht ergab, dass deutsche Unternehmen durchschnittlich 49 Cyberangriffe pro Jahr erleben - mehr als vier pro Monat. Fast ein Viertel (24 %) ist in einem einzigen Jahr mehr als 251 Angriffen ausgesetzt und 14 % erleben mehr als 500 Angriffe pro Jahr. IT-Leiter befürchten, dass die Häufigkeit der Angriffe zunehmen wird. 81 % erwarten, dass sowohl die Gesamtzahl der Angriffe als auch die Zahl der erfolgreichen Angriffe im nächsten Jahr steigen wird.

Zum Vergleich mit anderen europäischen und weltweiten Regionen: Im Vereinigten Königreich sind Unternehmen im Durchschnitt mit 44 Cyberangriffen konfrontiert, in Frankreich mit 48 und in den USA mit 42 Cyberangriffen pro Jahr.

Cyberangriffe fügen Unternehmen erheblichen Schaden zu
Erfolgreiche Cyberangriffe haben das Potenzial, Unternehmen jeder Größe zum Stillstand zu bringen. Mindestens 40 % der Befragten halten ihr Unternehmen für sehr gut vorbereitet, um sich gegen solche Angriffe zu verteidigen. In den USA (64 %) und in Frankreich (42 %) halten sich die Unternehmen sogar noch besser vorbereitet, während im Vereinigten Königreich nur 26 % dieses Verteidigungsniveau bestätigen.

- Etwa ein Drittel (31 %) der Opfer eines Cyberangriffs berichtet über eine Unterbrechung des Handels, z. B. der Fähigkeit, Geschäftsvorgänge auszuführen, im Vergleich zu 32 % in Frankreich, 35 % im Vereinigten Königreich und 23 % in den USA.
- Nur 25 % der deutschen Unternehmen haben aufgrund eines Angriffs einen Imageschaden erlitten, während 34 % im Vereinigten Königreich, 25 % in Frankreich und 28 % in den USA damit konfrontiert waren.
- Auf die Frage nach den finanziellen Auswirkungen eines Cyberangriffs lag die häufigste Antwort in Deutschland zwischen 10.000 und 49.999 Euro. In Großbritannien lag diese Zahl bei 100.000 bis 499.999 Pfund und in den USA bei 50.000 bis 99.999 US-Dollar.

Investitionen und Tools für die Cybersicherheit
Die Zunahme von Hybrid- und Remote-Arbeitsplätzen vergrößert die Kluft zwischen dem, was für die Sicherheit von Unternehmen notwendig ist, und dem, was zur Verfügung steht – wobei fehlende Investitionen in die Cybersicherheit Unternehmen ungeschützt lassen.

Die Sichtbarkeit von Systembenutzern sowie die Stärke von Passwörtern und Berechtigungen sind Grundvoraussetzungen, unabhängig von der Größe des Unternehmens oder der Branche. Doch IT-Führungskräfte geben zu, dass es ihren technischen Systemen an wesentlichen Tools mangelt:

- 42 % der deutschen Befragten vermissen einen Manager für IT-Geheimnisse wie API-Schlüssel, Datenbankpasswörter und Zugangsdaten
- 84% der Befragten sind besorgt über die Gefahren von hart kodierten Anmeldedaten, d.h. die direkte Einbettung von Authentifizierungsdaten wie Benutzer-IDs und Passwörtern in den Quellcode
- 47 % haben keinen Verbindungsmanager, um den Fernzugriff auf privilegierte Infrastrukturen zu verwalten.

„Die Cybersicherheitslandschaft ist komplex, mit sich ständig ändernden Risiken und wechselnden Prioritäten, die es zu verwalten gilt. Die Studie zeigt jedoch, dass Unternehmen mehr tun könnten und sollten", so Darren Guccione, CEO und Mitbegründer von Keeper Security. „Während viele Unternehmen über zukünftige Investitionen nachdenken, sehen sie sich durch steigende externe Bedrohungen und die Anforderungen, die durch bestehende Schwachstellen entstehen, überfordert."

Cybersecurity in der Unternehmenskultur
Trotz Budgetverpflichtungen und einer Priorisierung der Cybersicherheit durch die Unternehmensleitung geben die IT-Verantwortlichen selbst einen beunruhigenden Mangel an Transparenz bei der Meldung von Cyberangriffen zu. Mehr als die Hälfte (51 %) der deutschen IT-Führungskräfte geben an, dass sie von einem Cyberangriff Kenntnis hatten und diesen nicht an eine zuständige Behörde gemeldet haben. Darüber hinaus sind 78 %

der IT-Fachleute besorgt über einen Angriff innerhalb ihrer eigenen Organisation. Diese Zahlen sollten für Unternehmensleiter ein Warnsignal sein, denn ohne eine Kultur des Vertrauens, der Verantwortlichkeit und der Reaktionsfähigkeit wird die Cyberkriminalität weiterhin wachsen.

Guccione fasst zusammen: „Obwohl deutsche Unternehmen einige Schritte unternommen haben, um der Cybersicherheit Priorität einzuräumen, gibt es nach wie vor deutliche Lücken. Umfang und Tempo der Bedrohungen für Unternehmen nehmen zu und die Verantwortlichen können es sich nicht leisten, zu warten. Unternehmen und IT-Führungskräfte müssen sich nicht nur zur Cybersicherheit bekennen, sondern auch danach handeln. Sie müssen erkennen, wie sich Arbeitsumgebungen entwickelt haben und neue Wege einschlagen, um ihre Mitarbeiter, ihre Daten und ihren Lebensunterhalt zu schützen."

Der Cybersecurity Census Report 2022 steht zum Download bereit unter:
https://www.keepersecurity.com/de_DE/german-cybersecurity-census-report-2022/

Über Keeper Security Inc.
Keeper Security verändert die Art und Weise, wie Menschen und Organisationen auf der ganzen Welt ihre Passwörter, Geheimnisse und vertraulichen Informationen schützen. Die benutzerfreundliche Cybersecurity-Plattform von Keeper basiert auf der Grundlage von Zero-Trust- und Zero-Knowledge-Sicherheit, um jeden Benutzer und jedes Gerät zu schützen. Die Lösung ist in wenigen Minuten einsatzbereit und lässt sich nahtlos in die Systemumgebung integrieren, um Datenschutzverletzungen zu verhindern, Helpdesk-Kosten zu senken und die Einhaltung von Vorschriften zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelpersonen und Tausenden von Unternehmen auf der ganzen Welt und ist der führende Anbieter von erstklassigem Passwortmanagement, Geheimnismanagement, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging. Schützen Sie, was wichtig ist, auf KeeperSecurity.com.

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@eskenzipr.com