Cybersecurity Report

# Bedrohung auf Rekordniveau

**[14.03.2024] Der aktuelle Cybersecurity Report von Trend Micro zeigt, dass Angriffe auf IT-Systeme immer raffinierter werden. Deutschland gehört zu den am stärksten betroffenen Ländern, insbesondere im Bereich Ransomware. Im Fokus der Angreifer stehen staatliche Einrichtungen und Kritische Infrastrukturen.**

2023 war ein Rekordjahr für Cyber-Bedrohungen. Der Cybersecurity-Spezialist Trend Micro stellte in seinem jährlichen Sicherheitsbericht fest, dass seine Systeme mehr als 161 Milliarden schädliche Aktivitäten erkannt und blockiert haben. Seit 2019 habe sich die Zahl der Bedrohungen fast verdreifacht, was die wachsende Bedrohung durch Cyber-Kriminalität unterstreiche, heißt es in einer Pressemitteilung. Besonders alarmierend sei die Entwicklung in Deutschland, das weltweit zu den am stärksten von Malware und Ransomware betroffenen Ländern zählt.

## Cloud-Umgebungen im Auge behalten

„Cyber-Kriminelle greifen immer gezielter an und entwickeln ihre Ransomware-Taktiken weiter“, erklärt Richard Werner, IT-Sicherheitsexperte bei Trend Micro. Er betont, dass Unternehmen ihre Cloud-Umgebungen besonders im Auge behalten sollten, da diese zu den Hauptzielen der Angriffe gehören. Regierungseinrichtungen und Kritische Infrastrukturen wie das Gesundheitswesen und die Energieversorgung standen 2023 besonders im Fokus der Angreifer. Der Trend Micro Report zeigt, dass der Finanzsektor weltweit am häufigsten von Ransomware-Angriffen betroffen war, gefolgt von Regierungseinrichtungen und dem Technologiesektor. In Deutschland waren das Gesundheitswesen und das produzierende Gewerbe besonders betroffen.

## Cyber-Kriminelle setzen auf Qualität statt Quantität

Während die Gesamtzahl der geblockten Bedrohungen gestiegen ist, verzeichnen die Experten einen Rückgang bei der Erkennung von E-Mails und Websites. Stattdessen steigt die Zahl der blockierten schädlichen Dateien, was darauf hindeutet, dass Cyber-Kriminelle zunehmend auf Qualität statt Quantität setzen und sich auf bestimmte Opfergruppen konzentrieren. Sicherheitsexperte Richard Werner mahnt, dass Unternehmen und Behörden ihre Sicherheitskonzepte an die veränderte Bedrohungslage anpassen müssen. „Eine rasche und ganzheitliche Angriffserkennung über alle Vektoren der IT-Umgebung hinweg ist unabdingbar“, sagt er und weist auf die Bedeutung eines kontinuierlichen Cyber-Risiko-Managements hin, wie es die kommende NIS2-Richtlinie vorschreibt.

(al)

• Trend Micro 2023 Annual Cybersecurity Report (in englischer Sprache)

Stichwörter: Innere Sicherheit, IT-Sicherheit, Trend Micro, Cyber Security, IT-Sicherheit