



## Hauptziel von Ransomware und Datendiebstahl im Pandemiejahr 2020: Der Einzelhandel

*Einzelhandel in DACH zu 63 Prozent von Ransomware betroffen  
Gesamtkosten pro Angriff in DACH durchschnittlich 1,2 Millionen Euro*

**Wiesbaden, 10. August 2021** – Sophos hat detaillierte Ergebnisse einer weltweiten Umfrage mit dem Titel "[State of Ransomware in Retail](#)" veröffentlicht. Der neue Report beschreibt das Ausmaß sowie die Auswirkungen von Ransomware-Angriffen auf mittelständische Einzelhandelsunternehmen weltweit und im Vergleich zu Ländern und Regionen im Jahr 2020.

Ein Ergebnis ist, dass Einzelhandelsunternehmen während der COVID-19-Pandemie ein Hauptziel für Ransomware-Angriffe wurden; genau zu der Zeit, als viele erstmals in den Online-Handel eingestiegen sind. Die Ergebnisse zeigen auch, dass Einzelhändler besonders anfällig für einen wachsenden neuen Trend sind: reine Erpressungsangriffe, bei denen die Ransomware-Gangster keine Dateien verschlüsseln, sondern damit drohen, gestohlene Informationen online zu veröffentlichen, wenn kein Lösegeld gezahlt wird. Mit 12 Prozent weltweit (DACH 23 Prozent) waren mehr als eines von zehn Ransomware-Opfern im Einzelhandel davon betroffen, fast doppelt so viele wie der branchenübergreifende Durchschnitt von 7 Prozent weltweit (DACH 10 Prozent).

### Weitere wichtige Forschungsergebnisse sind:

- Gemeinsam mit dem Bildungswesen war der Einzelhandel am stärksten von Ransomware-Angriffen betroffen. 44 Prozent (DACH 63 Prozent) der Einzelhandelsunternehmen waren Opfer eines Angriffs im Vergleich zu 37 Prozent (DACH 48 Prozent) in allen Branchen.
- Die Gesamtkosten für die Behebung eines Ransomware-Angriffs im Einzelhandel betragen unter Berücksichtigung von Ausfallzeiten, Personalzeit, Gerätekosten, Netzwerkkosten, entgangenen Geschäftsmöglichkeiten, gezahltem Lösegeld etc. waren durchschnittlich 1,67 Millionen Euro (DACH 1,2 Millionen Euro) - verglichen mit einem branchenübergreifenden Durchschnitt von 1,57 Millionen Euro. (DACH 2,36 Millionen Euro)
- Mit 54 Prozent (DACH 50 Prozent) gaben über die Hälfte der von Ransomware betroffenen Einzelhandelsunternehmen an, dass es den Angreifern gelungen sei, ihre Daten zu verschlüsseln.
- Ein Drittel (32 Prozent weltweit; DACH 18 Prozent) der Einzelhandelsunternehmen, deren Daten verschlüsselt wurden, zahlten Lösegeld. Die durchschnittliche Lösegeldzahlung war weltweit 125.669 Euro. In DACH betrug die durchschnittliche Zahlung nur 9.210 Euro – der niedrigste Betrag überhaupt. Diejenigen, die zahlten, konnten jedoch im Durchschnitt nur zwei Drittel (67 Prozent weltweit; DACH 85 Prozent) ihrer Daten wiederherstellen; nur 9 Prozent weltweit erhielten alle verschlüsselten Daten zurück.

„Der Einzelhandel war schon immer ein attraktives Ziel für Cyberkriminelle, da er über komplexe und verteilte IT-Umgebungen verfügt, die eine Vielzahl von angeschlossenen POS-Geräten umfassen, eine relativ flüchtige und technisch nicht versierte Belegschaft beschäftigt und Zugang zu einer Vielzahl von persönlichen und finanziellen Kundendaten hat“, sagt Chester Wisniewski, Principal Research Scientist bei Sophos. „Die Auswirkungen der Pandemie führten zu zusätzlichen Sicherheitsherausforderungen, die Cyberkriminelle schnell auszunutzen wissen. Der vergleichsweise hohe Prozentsatz der Erpressungsangriffe auf der

Grundlage von Datendiebstahl im Einzelhandel ist nicht völlig überraschend. Dienstleistungsbranchen wie der Einzelhandel verfügen über Informationen, die oft strengen Datenschutzgesetzen unterliegen. Die Angreifer nutzen dann die Angst der Opfer vor den Folgen einer Datenpanne in Form von Geldstrafen und Schäden für den Ruf der Marke, den Umsatz und das Vertrauen der Kunden aus. Für IT-Manager im Einzelhandel gibt es jedoch nicht nur schlechte Nachrichten. Zwar führte die Pandemie für drei Viertel der Einzelhändler zu einer erhöhten Belastung der IT. Allerdings konnte dieser Sektor mit 77 Prozent (DACH 80 Prozent) am ehesten eine positive Bilanz in Bezug auf verbesserte Cybersicherheitsfähigkeiten und -kenntnisse ziehen.“

Um IT-Netzwerke im Einzelhandel vor Ransomware und anderen Cyberangriffen zu schützen, raten die Experten von Sophos, dass sich IT-Teams mit ihren Ressourcen auf drei kritische Bereiche konzentrieren: Aufbau einer stärkeren Abwehr gegen Cyberbedrohungen, Einführung von Sicherheitsschulungen für Benutzer, einschließlich Teilzeit- und Zeitarbeitskräften, und verstärkt in eine widerstandsfähige IT-Infrastruktur zu investieren.

### **Zur Studie**

Für die [“State of Ransomware in Retail“](#) Studie wurden 5.400 IT-Entscheider – darunter 345 IT-Manager im Einzelhandel – in 30 Ländern in Europa, Nord- und Südamerika, dem Asia-Pazifik-Raum, Zentralasien, dem Mittleren Osten und Afrika befragt.

[Der komplette englische Report kann hier heruntergeladen werden.](#)

### **Über Sophos**

Als ein weltweit führender Anbieter von Next-Generation-Cybersicherheit schützt Sophos mehr als 400.000 Unternehmen jeder Größe in über 150 Ländern vor den neuesten Cyberbedrohungen. Mit den SophosLabs und seinem globalen Team für Bedrohungs- und Datenanalyse schützen die Cloud- und KI-gestützten Sophos-Lösungen Endpoints (Laptops, Server und mobile Geräte) sowie Netzwerke vor sich ständig verändernden Cyberangriffen, einschließlich Ransomware, Malware, Exploits, Datenexfiltration, individuellen Hackervorstößen, Phishing und mehr. Die cloud-basierte Plattform Sophos Central integriert über APIs das gesamte Next Generation Sophos-Portfolio, von der Intercept X Endpoint-Lösung bis zur XG Firewall, in einem einzigen Synchronized-Security-System. Sophos treibt die Entwicklung zur Next Generation Cybersicherheit voran und setzt fortschrittliche Technologien, beispielsweise aus den Bereichen Cloud, Machine Learning, APIs, Automatisierung oder Managed Threat Response ein, um Unternehmen jeder Größe Schutz der Enterprise-Klasse zu bieten. Sophos vertreibt Produkte und Services exklusiv über einen globalen Channel mit mehr als 53.000 Partnern und Managed Service Providern (MSP). Sophos stellt seine innovativen, gewerblichen Technologien auch Privatanwendern via Sophos Home zur Verfügung. Das Unternehmen hat seinen Hauptsitz in Oxford, Großbritannien. Weitere Informationen unter [www.sophos.de](http://www.sophos.de).

### **Pressekontakt:**

Sophos  
Jörg Schindler, PR-Manager Central & Eastern Europe  
[joerg.schindler@sophos.com](mailto:joerg.schindler@sophos.com), +49-721-25516-263

TC Communications  
Arno Lücht, +49-8081-954619  
Thilo Christ, +49-8081-954617  
Ulrike Masztalerz, +49-30-55248198  
Ariane Wendt +49-172-4536839  
[sophos@tc-communications.de](mailto:sophos@tc-communications.de)