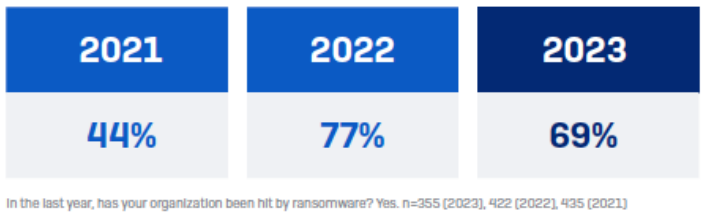
Ransomware im Einzelhandel:
Kostenexplosion trotz Angriffsrückgang

Sophos stellt die Ergebnisse des diesjährigen State of Ransomware in Retail Reports vor. Mit ambivalenten Ergebnissen:
Die Zahl der erfolgreichen Ransomware-Angriffe im Einzelhandel sinkt im Vergleich zum Vorjahr um acht Prozent, die Anzahl der Lösegeldzahlungen verringert sich um sechs Prozent, doch die Preise sind explodiert: Der Einzelhandel zahlt 10mal mehr Lösegeld als im letzten Jahr und 60 Prozent mehr als andere Branchen.

Cyberkriminalität ist eines der größten Risiken für Unternehmen aller Branchen. Dennoch sind Angriffsraten und daraus resultierende Schäden für Unternehmen je nach Branchensektor unterschiedlich. Das Cybersicherheitsunternehmen Sophos ist in einer weltweiten Studie der Frage nachgegangen, wie sich insbesondere die Cybergefahr der Ransomware im Bereich des Einzelhandels entwickelt hat und aktuell darstellt.

Erfreulicher Rückgang der Angriffsraten, Ransomware dennoch größte Gefahr
Die Rate der Ransomware-Angriffe im Einzelhandel ist von 77 % im Jahr 2022 auf 69 % im Jahr 2023 gesunken. Dies ist ein erfreulicher Rückgang. Die Tatsache aber, dass immer noch über zwei Drittel der Einzelhandelsunternehmen im letzten Jahr von Ransomware betroffen waren und trotz dieses Rückgangs die Rate im weltweiten Vergleich weiterhin über dem Durchschnitt liegt, macht diese Schadsoftware zum größten Cyber-Risiko, dem Einzelhandelsunternehmen heute ausgesetzt sind.



Sicherheitslücken als Haupteinfallstor
Ausgenutzte Sicherheitslücken (41%) waren die Ursache für die meisten Ransomware-Angriffe im Einzelhandel, gefolgt von kompromittierten Zugangsdaten (22 %). Phishing war die dritthäufigste Ursache mit 17 % der Vorfälle. Insgesamt gab fast ein Drittel der befragten Einzelhändler (32 %) an, dass E-Mails (bösartige E-Mails oder Phishing) die Ursache für den Angriff waren. Weltweit gehörte der Einzelhandel zu den Branchen, bei denen Ransomware-Angriffe am häufigsten über ausgenutzte Schwachstellen und Phishing durchgeführt wurden. Umgekehrt wurde die Verwendung kompromittierter Anmeldedaten als Ausgangspunkt für Ransomware-Angriffe im Einzelhandel am wenigsten von allen Branchen verzeichnet (gemeinsam mit IT, Telekommunikation und Technologie).

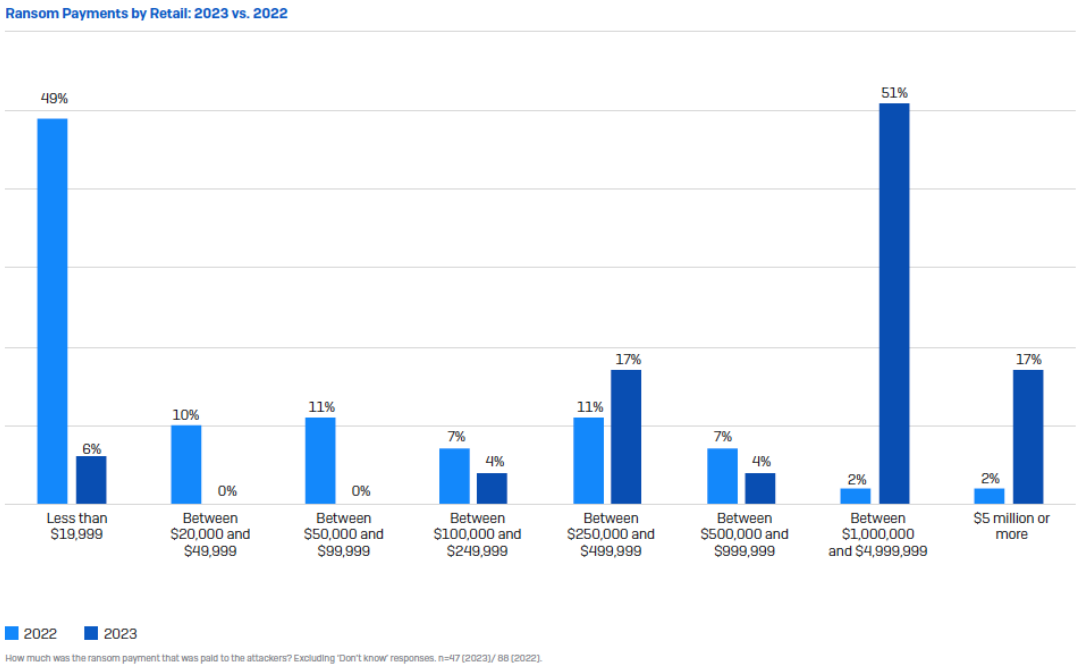
Einzelhandel zahlt 10mal mehr Lösegeld als im letzten Jahr und 60 Prozent mehr als andere Branchen
Auf globaler, branchenübergreifender Ebene ist die Bereitschaft zur Zahlung von Lösegeld zwar insgesamt auf dem Niveau der letztjährigen Studie, die Höhe der Zahlungen selbst hat sich jedoch mit einer Steigerung von $ 812.360 auf $ 1.542.330 (€ 1.389.639,33) im Vergleich zum Vorjahr fast verdoppelt. Im Einklang mit dem globalen Trend hat auch die durchschnittliche Lösegeldzahlung im Einzelhandel mit $ 2.458.481 (€ 2.215.226,60)

im Vergleich zum Vorjahr beträchtlich zugenommen: Sie lag mehr als 10mal höher als im Bericht von 2022 ($ 226.044 bzw. € 204.095,13).
Der Einzelhandel zahlt aber nicht nur mehr Lösegeld als im letzten Jahr, sondern auch mehr als viele andere Branchen: Die durchschnittlichen Lösegeldzahlungen im Einzelhandel waren fast 60 % höher als der branchenübergreifende globale Durchschnitt ($ 1.542.330 bzw. € 1.389.639,33) in der diesjährigen Studie.

	2022	2023
Cross-sector Average	$812,360 (mean) $76,500 (median)	$1,542,330 (mean) $400,000 (median)
Retail	$226,044 (mean) $20,000 (median)	$2,458,481 (mean) $3,000,000 (median)

How much was the ransom payment that was paid to the attackers? Excluding 'Don't know' responses and outliers.
Cross-sector: n=216 (2023)/ 965 (2022); Retail: n=47 (2023)/ 88 (2022).

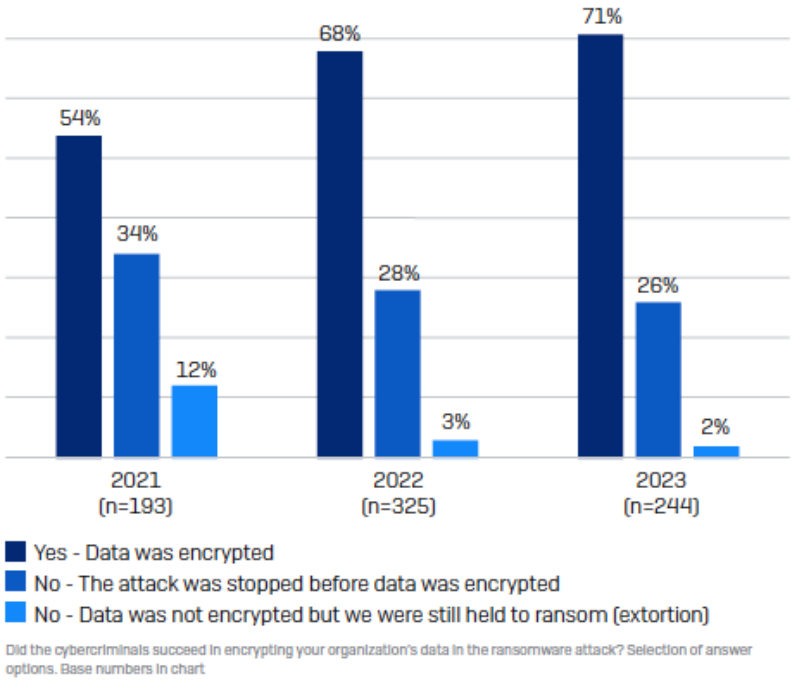
Auch der Anteil der Einzelhandelsunternehmen, die höhere Lösegelder zahlen, hat im Vergleich zur Studie aus dem Jahr 2022 zugenommen. Mehr als zwei Drittel der Einzelhandelsunternehmen (68 %) meldeten Zahlungen in Höhe von 1 Million US-Dollar oder mehr gegenüber rund 5 % im Vorjahr. Umgekehrt zahlten 6 % weniger als 100.000 US-Dollar, gegenüber 70 % im letztjährigen Bericht.



Versicherte Unternehmen mit hoher Bereitschaft zur Zahlung von Lösegeld
Im Gegensatz zu anderen Sektoren hatte der Versicherungsschutz nur einen geringen Einfluss auf die Wiederherstellungsrate im Einzelhandel. Allerdings hatte er einen erheblichen Einfluss auf die Bereitschaft das Lösegeld zu zahlen. Kurz gesagt: Einzelhandelsunternehmen mit einer eigenständigen Cyber-Versicherung waren eher bereit, Lösegeld zu zahlen, um Daten

wiederherzustellen, als solche mit einer Cyber-Versicherung als Teil einer umfassenderen Geschäftspolice sind oder Unternehmen, die überhaupt keine Versicherung haben.

Rate der Datenverschlüsselung im Einzelhandel zum dritten Mal in Folge gestiegen
Die Datenverschlüsselung im Einzelhandel hat weiter zugenommen, wobei der Bericht 2023 den höchsten Verschlüsselungsgrad seit drei Jahren aufweist. Dies spiegelt die immer professionelleren Fähigkeiten der Angreifer wider, die ihre Methoden stetig erneuern und verfeinern. Fast drei Viertel der Ransomware-Angriffe (71 %) im Einzelhandel führten zur Verschlüsselung von Daten, womit diese Zahl verglichen mit 68 % und 54 % in den beiden vorherigen Jahren weiter gestiegen ist. Die steigende Verschlüsselungsrate geht mit einer sinkenden Fähigkeit der Unternehmen einher, bei Angriffen rechtzeitig Abwehrmechanismen zu aktivieren. Nur einer von vier Angriffen (26 %) wird gestoppt, bevor die Daten verschlüsselt werden können. Ein eher besorgniserregender Trend.



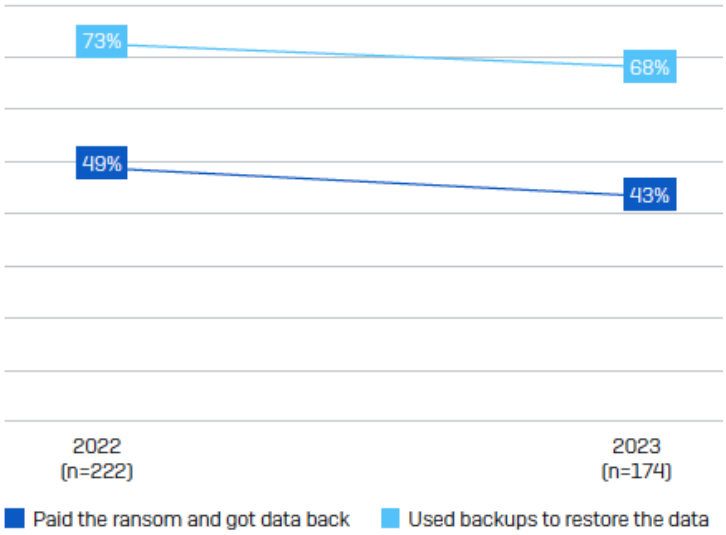
Dennoch steht der Einzelhandel insgesamt weltweit besser da als viele andere Branchen. Über alle Sektoren hinweg führten 76 % der Angriffe zu einer Datenverschlüsselung, und nur 21 % wurden gestoppt, bevor die Daten verschlüsselt wurden. Die höchste Häufigkeit der Datenverschlüsselung (92 %) wurde von Dienstleistungsunternehmen gemeldet.

Verschlüsselt und gestohlen
Bei 21 % der Angriffe im Einzelhandel, bei denen Daten verschlüsselt wurden, wurden auch Daten gestohlen. Dieser "Double-Dip"-Ansatz der Angreifer nimmt zu, da er die Möglichkeit Angriffe zu Geld zu machen, noch einmal erhöht. Die Drohung, gestohlene Daten öffentlich zu machen kann genutzt werden, um Zahlungen zu erpressen. Zudem lohnt sich für die Cyberkriminellen auch der Verkauf, die Daten sind heißbegehrte Handelsware m Darknet.

Durch die steigende Häufigkeit von Datendiebstählen wird es immer wichtiger, Angriffe rechtzeitig zu stoppen, bevor Informationen exfiltriert werden können.

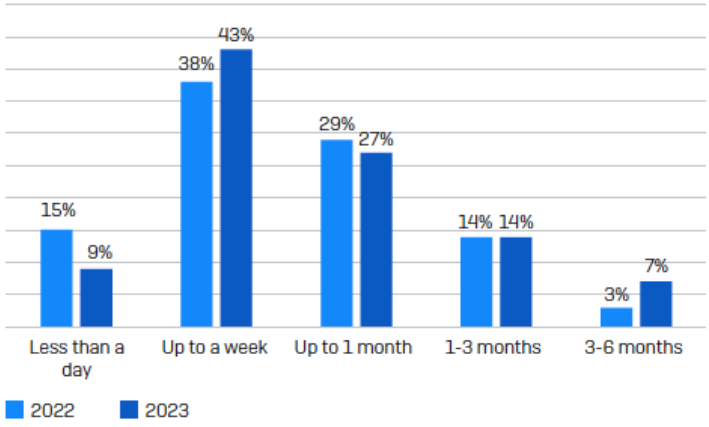
Datenrettungsrate im Einzelhandel hoch
97 % der Einzelhandelsunternehmen konnten ihre Daten nach einem Verschlüsselungsangriff wiederherstellen. 43 % der Einzelhandelsunternehmen gaben an, dafür Lösegeld gezahlt zu haben, mehr als zwei Drittel (68 %) verließen sich bei der Datenwiederherstellung auf Backups, was etwas weniger ist als der als der weltweite Durchschnitt von 46 % bzw. 70 %. 16 % der Befragten gaben an, mehrere Mittel zur Wiederherstellung verschlüsselter Daten einzusetzen.

Einsatz von Backups aber auch Anzahl der Lösegeldzahlungen rückläufig
Der Einsatz von Backups im Einzelhandel ging in der Umfrage von 2023 auf 68 % zurück von 73 % in der Umfrage von 2022. Dieser Rückgang bei der Nutzung von Backups entspricht dem globalen – eher besorgniserregenden – Trend, der einen Rückgang von 73 % im Jahr 2022 auf 70 % im Jahr 2023 verzeichnete. Was die Lösegeldzahlungen betrifft, so sank die Zahl der Lösegeldzahlungen im Einzelhandel von 49 % im Bericht von 2022 auf aktuelle 43 % im vorliegenden Bericht. Weltweit sind die Lösegeldzahlungen dagegen über alle Sektoren hinweg gleichblieben.



Wiederherstellungskosten im Einzelhandel etwas höher als im Branchendurchschnitt
Lösegeldzahlungen sind nur ein Element der Wiederherstellungskosten im Zusammenhang mit Ransomware. Ohne Berücksichtigung des gezahlten Lösegelds meldeten die Unternehmen weltweit einen Anstieg gegenüber dem Bericht von 2022. Auch die Wiederherstellungskosten für den Einzelhandel sind von $ 1.270.000 (€ 1.145.406,65) im Vorjahr auf $ 1.850.000 (€ 1.668.505,75) gestiegen – hiermit aber immer noch niedriger als die $1.970.000 (€ 1.776.802,10) aus dem Bericht für das Jahr 2021. Der Anstieg in diesem Jahr beruht möglicherweise auf den Herausforderungen des Sektors, die Datenverschlüsselungen bei Angriffen rechtzeitig zu stoppen. Außerdem kann die geringere Nutzung von Backups zur Wiederherstellung verschlüsselter Daten zu erhöhten Wiederherstellungskosten geführt haben.

Die Wiederherstellung von Daten dauert länger
Während die Zeit bis zur Wiederherstellung nach Ransomware-Angriffen im Einzelhandel weitgehend den Ergebnissen des Berichts von 2022 entspricht, ist der Prozentsatz derer, die sich in weniger als einem Tag erholen im Vergleich zum Vorjahr von 15 % auf 9 % gesunken Der Prozentsatz der Unternehmen, die mehr als einen Monat für die Wiederherstellung benötigten, stieg auf rund 21 % von rund 17 % im Vorjahr, was darauf hindeutet, dass die Erholung in diesem Sektor nun länger dauert.



How long did it take your organization to fully recover from the ransomware attack? 244 (in 2023) /325 (in 2022) retail organizations that were hit by ransomware.

Auswirkungen auf das Geschäft
82 % der Einzelhandelsunternehmen, die von Ransomware betroffen waren, gaben an, dass die Angriffe auch zu Geschäftseinbußen führten. Dies entspricht dem weltweiten Branchendurchschnitt von 84 %.

Für den Sektor des Einzelhandels wie auch für alle anderen Branchen stellt sich die entscheidende Frage, wie die Cyberkriminellen ins Unternehmen gelangen und welche Angriffstaktiken die größten Risiken für diese Branche birgt. Sophos rät Unternehmen, eine Reihe von Maßnahmen zur weiteren Stärkung ihrer Abwehrschilde zu ergreifen:

- Sicherheits-Tools, die vor den häufigsten Angriffsvektoren schützen, einschließlich Endpointschutz mit starken Anti-Exploit-Funktionen, um die Ausnutzung von Schwachstellen zu verhindern
- Zero Trust Network Access (ZTNA), um den Missbrauch kompromittierter Anmeldeinformationen zu vereiteln
- Adaptive Technologien, die automatisch auf Angriffe reagieren, die Angreifer stören und den Verteidigern Zeit verschaffen, um zu reagieren
- 24/7-Bedrohungserkennung, -untersuchung und -reaktion, entweder intern oder in Zusammenarbeit mit einem spezialisierten Managed Detection and Response (MDR)-Dienstleister
- Optimierung der Angriffsvorbereitung, einschließlich regelmäßiger Backups
- Üben der Wiederherstellung von Daten aus Backups und die Pflege eines aktuellen Reaktionsplans für Zwischenfälle
- Aufrechterhaltung einer guten Sicherheitshygiene, einschließlich rechtzeitiger Patchings sowie regelmäßige Überprüfung der Konfigurationen von Sicherheitstools

Über die Studie
Von Januar bis März befragte ein unabhängiges Marktforschungsinstitut im Auftrag von Sophos 3.000 Verantwortliche in der IT oder Cybersecurity in Unternehmen mit 100 bis 5.000 Angestellten, mindesten 10 Millionen Umsatz, in 14 Ländern. Darunter befanden sich 351 Einzelhandelsbetriebe, die Auskunft darüber gaben, wie sich die Situation der Cybersicherheit aus ihrer speziellen Sicht darstellt.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
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