Cyberkriminalität wird für Produktionsbetriebe noch teurer

Sophos stellt die Ergebnisse des aktuellen State of Ransomware Reports für die verarbeitende Industrie vor. Es ist keine Entspannung in Sicht: Angriffe werden häufiger und raffinierter, zugleich steigen die Lösegeldforderungen und die Wiederherstellung nach einem Angriff dauert immer länger.

Cyberkriminalität ist eines der größten, geschäftsschädigenden Risiken für Unternehmen aller Branchen. Doch es gibt durchaus Unterschiede zwischen den diversen Marktsegmenten. Wie sich die Gefahr durch Cybergangster aktuell auf das produzierende Gewerbe auswirkt, hat das Cybersicherheitsunternehmen Sophos in einer weltweiten Studie festgestellt.

Beunruhigende Stagnation
Die vermeintlich gute Nachricht ist, dass der Anteil der produzierenden Unternehmen, die mit Ransomware attackiert wurden, nur wenig gestiegen ist. 56 Prozent wurden im letzten Jahr angegriffen. Im Vergleich: ein Jahr zuvor waren es 55 Prozent. Zwar gibt es Branchen und Sektoren, die deutlich mehr betroffen sind – der Durchschnitt über alle Branchen liegt bei 66 Prozent – allerdings gibt es wenig Grund zum Aufatmen, wenn mehr als jedes zweite Unternehmen von den Cyberkriminellen ins Visier genommen wird.

2021	2022	2023
36%	55%	56%

In the last year, has your organization been hit by ransomware? Yes. n=363 (2023), 419 (2022), 438 (2021)

Viele Einfallstore
Für die produzierende Industrie stellt sich die entscheidende Frage, wie die Cyberkriminellen ins Unternehmen gelangen und welche Angriffstaktiken die größten Risiken für diese Branche birgt. Die gute Nachricht zuerst: In der Rangliste der Angriffstaktiken haben produzierende Unternehmen die potenziell ausnutzbaren Schwachstellen mit nur 24 Prozent vergleichsweise gut im Griff. Über alle Branchen hinweg ist diese Angriffstaktik mit 36 Prozent deutlich höher. Eine größere Herausforderung mit 27 Prozent scheint die Branche mit der Sicherheit von Nutzerdaten und Passwörtern zu haben, die Cyberkriminelle stehlen, um sich Zugang zur IT-Infrastruktur zu verschaffen.

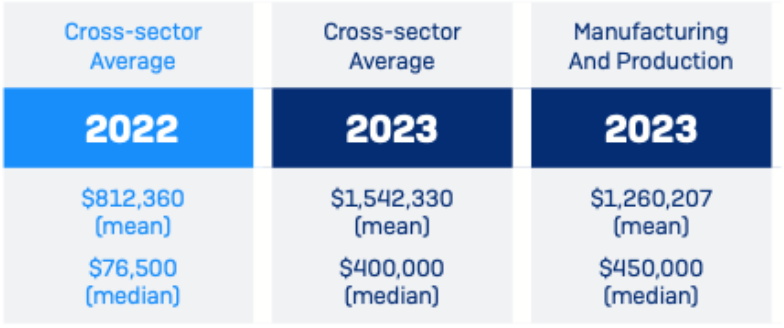
	MANUFACTURING AND PRODUCTION	CROSS-SECTOR AVERAGE
Exploited vulnerability	24%	36%
Compromised credentials	27%	29%
Malicious email	21%	18%
Phishing	20%	13%
Brute force attack	5%	3%
Download	2%	1%

Besonderen Nachholbedarf hat das produzierende Gewerbe laut Studie mit 20 Prozent bei der Abwehr von Phishing-Angriffen. Da der branchenübergreifende Durchschnitt lediglich 13 Prozent beträgt, liegt die Vermutung nahe, dass sich andere Sektoren besser um die Schulung ihrer Mitarbeiter in dieser Hinsicht kümmern.

Angriffe mit Folgen

Ein Angriff auf ein Unternehmen bedeutend nicht zwingend, dass die Cyberkriminellen Erfolg damit haben, ihre Ransomware zum Einsatz zu bringen und Lösegeld fordern. Der Trend für die produzierende Industrie zeigt jedoch deutlich, dass die Cyberkriminellen bei ihren Angriffen und den eingesetzten Technologien kräftig aufgerüstet haben. In der aktuellen Studie sind 68 Prozent der Angriffe „erfolgreich“ und nur 27 Prozent konnten rechtzeitig entdeckt und gestoppt werden. Im Vergleichszeitraum ein Jahr zuvor schafften es die Cyberkriminellen bei 57 Prozent ihrer Angriffe, die Daten zu verschlüsseln und 38 Prozent konnten verhindert werden. Erschwerend kommt die „Double-Dip“-Taktik der Cyberkriminellen hinzu. Hierbei werden die Daten zudem gestohlen, bevor sie verschlüsselt werden – eine Methode, die das Lösegeld und die Bereitwilligkeit zu bezahlen in die Höhe treiben, da auch Unternehmen, die die Daten wiederherstellen können, noch mit Veröffentlichung erpresst werden können.

Die unmittelbaren Auswirkungen auf die Lösegeldforderungen sind in der Studie deutlich nachvollziehbar. Der mittlere Durchschnitt der geforderten Lösegeldsumme liegt in der produzierenden Branche bei $ 1.260.207 (€ 1.156.289). Das ist nur etwas niedriger als der Durchschnitt über alle Branchen hinweg mit $ 1.542.330 (€ 1.415.148). Zum Vergleich, ein Jahr zuvor lag der allgemeine Durchschnitt deutlich niedriger bei $ 812.360 (€ 745.372).



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); Manufacturing: n=25 (2023)/ 38)(2022). Manufacturing has low base numbers so the findings should be considered indicative.

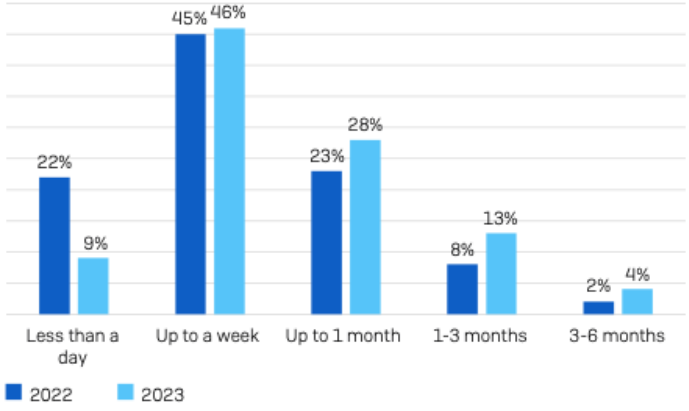
Teure Wiederherstellung der Systeme

Ein Angriff auf ein Unternehmen kann nicht nur dann teuer werden, wenn sich das Unternehmen dazu durchringt, die Lösegeldsumme zu bezahlen, sondern auch durch die zusätzlichen Folgekosten bei der Wiederherstellung der Systeme. Abgesehen davon, dass nach einer Bezahlung des Lösegelds nicht garantiert ist, dass sich alle Daten wiederherstellen lassen, kostet das Instandsetzen viel Zeit und Geld. Zusätzlich zum Lösegeld musste das produzierende Gewerbe durchschnittlich $ 1.080.000 (€ 990.942) in die Wiederherstellung (im Jahr zuvor waren es durchschnittlich $1.230.000 (€ 1.128.573)) investieren. Damit verdoppelt die Wiederherstellung die Gesamtsumme inklusive Lösegeld nahezu. Mit den Wiederherstellungskosten kommt die Produzierende Industrie trotz der hohen Summe vergleichsweise glimpflich davon. Beispielsweise im Transportwesen werden durchschnittlich $ 3.540.000 (€ 3.248.088) benötigt.

Entscheidender Faktor Zeit

Die Summen für das Lösegeld und die Wiederherstellung stellen viele Unternehmen aller Branchen vor große Herausforderungen. Diese werden durch die benötigte Zeit, bis die Systeme wieder laufen und das Unternehmen betriebsfähig ist, noch einmal deutlich komplexer und teilweise existenzgefährdend. Denn ein Unternehmen, das stillsteht, verliert

jede Stunde und jeden Tag viel Geld und erleidet zusätzlich einen Image- und Reputationsverlust im Markt – bei Partnern und Kunden.
Die größte Varianz der aktuellen Studie zu den Ergebnissen des Vorjahres ist der Prozentsatz produzierenden Unternehmen, die sich in weniger als einem Tag von einer Cyberattacke erholen konnten Dieser Prozentsatz ist deutlich auf 9 Prozent gesunken (gegenüber 22 Prozent in der letzten Umfrage). Gleichzeitig ist der Prozentsatz der Unternehmen, die mehr als einen Monat für die Wiederherstellung benötigten, auf 17 Prozent gestiegen, verglichen mit 10 Prozent ein Jahr zuvor. Dies deutet darauf hin, dass der Aufwand für die Wiederherstellung des Geschäftsbetriebs in diesem Sektor insgesamt größer geworden ist.



How long did it take your organization to fully recover from the ransomware attack? 205(in 2023) /230 (in 2022) manufacturing and production organizations that were hit by ransomware.

Beliebtes Ziel: Lieferketten
Ransomware ist die meistverbreitete Bedrohung mit dem Ziel, Geld zu machen. Allerdings sollten sich Unternehmen im Klaren darüber sein, dass Ransomware stets die letzte Stufe eines erfolgreichen Angriffs ist, zu dem auch Informationsdiebstahl, Downloader-Trojaner, Cryptominer und viele andere Bedrohungen gehören.
„Eine besondere Rolle nehmen die vermehrten Angriffe auf die Lieferkette ein. Diese Attacken scheinen auf dem Vormarsch zu sein“, erklärt John Shier, Field CTO Commercial bei Sophos. „Kompromittierungen der Lieferkette sind für Cyberkriminelle sehr attraktiv, da sie ihnen Zugang zu mehreren Opfern auf einmal verschaffen können. Solange die Cyberkriminellen hiermit Geld erbeuten können, werden diese Angriffe für sie effektiv sein und weitergehen. Unternehmen sollten daher nicht nur sicherstellen, dass sie gegen direkte Angriffe gewappnet, sondern auch in der Lage sind, Angriffe von vertrauenswürdigen Partnern abzuwehren.“

Robuste Security aus Mensch und Maschine im Team
Für Unternehmen aller Branchen ist es wichtig, robuste Security-Ökosysteme zu implementieren. Da bei komplexen Bedrohungen eine rein maschinelle und verhaltensbasierte Erkennung und Beseitigung von Angriffen oft nicht mehr ausreicht, sollten die technologischen Lösungen mit Künstlicher Intelligenz oder anomaliebasierter automatischer Reaktion durch hoch spezialisierte MDR-Teams (Managed Detection and Response) aus IT-Sicherheitsprofis ergänzt werden. MDR-Services kombinieren technische Security-Lösungen mit einem Expertenteam, das auf Prävention, Früherkennung und Schadensbeseitigung spezialisiert ist. Dieses Team ergreift Maßnahmen, um nicht nur die klassischen Cyberbedrohungen, sondern vor allem die immer besser getarnten Schleichfahrten der Kriminellen im Netzwerk zu eliminieren.

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 363 Produktionsbetriebe, 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