Sophos Threat Report 2024: KMUs im Fadenkreuz

Diebstahl von Daten und Identitäten sind die größten Bedrohungen für kleine und mittelgroße Unternehmen. Fast 50 Prozent aller analysierten Schadsoftware-Fälle hatten es laut Sophos 2023 auf dieses Marktsegment abgesehen.

Weitere Ergebnisse des Sophos Threat Reports 2024:

- *90 Prozent aller Cyberangriffe beinhalten Daten- oder Identitätsdiebstahl*
- *Kompromittierung der Geschäftskommunikation auf dem Vormarsch*
- *Social Engineering steigt auf ein neues Level*

Wiesbaden, 12. März 2024 – Sophos stellt heute seinen neuen Threat Report: Cybercrime on Main Street vor. Schwerpunkt sind in diesem Jahr die größten Bedrohungen für kleine und mittlere Unternehmen (KMU).

Cyberkriminalität ist für Organisationen jeder Größenordnung eine Herausforderung, am härtesten und häufig unter dem Radar der Öffentlichkeit trifft sie jedoch kleine Unternehmen. Während Cyberangriffe auf Konzerne und Regierungsbehörden den Großteil der Berichterstattung ausmachen, sind kleine Unternehmen im Allgemeinen anfälliger und leiden proportional stärker unter den Folgen von Cyberangriffen. Ein Mangel an erfahrenem Sicherheitspersonal, unzureichende Investitionen in die Cybersicherheit und insgesamt geringere Budgets für Informationstechnologie tragen zu dieser Verwundbarkeit bei. Dabei sind KMUs keine Kleinigkeit. Nach Angaben der Weltbank sind mehr als 90 Prozent der Unternehmen weltweit kleine und mittlere Organisationen und sie stellen mehr als 50 Prozent der weltweiten Beschäftigung.

Keylogger, Spionagesoftware und Stealer bei 50 Prozent der Angriffe
Bei fast der Hälfte aller Angriffe auf KMUs kommen Keylogger, Spionagesoftware und sogenannte Stealers, also Schadsoftware zum Stehlen von Daten und Zugangsdaten, zum Einsatz. Cyberkriminelle nutzen diese entwendeten Informationen später für weitere Aktionen wie unautorisierten Fernzugriff, Erpressung oder das Installieren von Ransomware.

Der Sophos-Report analysiert des Weiteren sogenannte IABs, also Initial Access Brokers. Diese Kriminelle haben sich darauf spezialisiert, in Computer-Netzwerke einzubrechen. Der Report zeigt auf, dass Cyberkriminelle dabei das Dark Web nutzen, um ihre Dienstleistungen gezielt für KMU-Netzwerke anzubieten. Auch verkaufen sie direkt Sofortzugänge zu KMUs, die sie vorher bereits gehackt haben.

Cybercrime hat nur ein Ziel: Daten
Christopher Budd, Director Threat Research bei Sophos X-Ops, ordnet die Ergebnisse folgendermaßen ein: „Der Wert von Daten als Währung ist unter Cyberkriminellen exponentiell gewachsen und das gilt besonders für KMUs, da sie dazu tendieren, einen Service oder eine Applikation pro Funktion für die gesamte Organisation zu nutzen. Ein Beispiel: Angreifer setzen einen Infostealer auf einem Zielnetzwerk ein, um Zugangsdaten zu stehlen. Dabei fällt ihnen ein Passwort für die Rechnungssoftware des ganzen Unternehmens in die Hände. Sie könnten nun Zugang zu den Finanzdaten des Betriebes kommen und Gelder auf ihre eigenen Konten überweisen. Es gibt einen Grund dafür, dass 90 Prozent aller Cyberangriffe, die Sophos 2023 untersucht hat, in Daten- oder Identitätsdiebstahl verwickelt war – entweder durch Ransomware-Attacken, Datenerpressung, unautorisierten Remote-Zugang oder schlichtweg durch Datendiebstahl."

Ransomware bleibt größte Gefahr für KMUs, LockBit ist Nummer 1
Auch wenn die Zahl der Ransomware-Angriffe gegen KMUs gleichgeblieben ist, stellen diese doch die größte Cyberbedrohung für Unternehmen unter 500 Mitarbeitern dar. Laut des Sophos Incident Response-Teams, das bei akuten Überfällen eingreift, war LockBit die Ransomware-Gruppe mit dem größten Chaospotenzial. Akira und BlackCat folgen auf Platz 2 und 3. Auch Attacken älterer oder weniger bekannterer Ransomware, wie BitLocker oder Crytox kamen in letzter Zeit vor.

Remote-Verschlüsselung steigt um 62 Prozent
Der Report zeigt zudem, dass die Kriminellen ihre Strategie beibehalten, die Taktik für ihre Ransomware-Attacken immer wieder zu ändern, um erfolgreich zu bleiben. Das äußert sich aktuell durch ein vermehrtes Aufkommen von Verschlüsselungsaktivitäten per Fernzugriff sowie das gezielte Anvisieren von MSPs (Managed Service Providers) als Angriffsflächen-Multiplikator. Zwischen 2022 und 2023 stieg die Anzahl an Ransomware-Attacken mit Remote-Verschlüsselung um 62 Prozent. Das Sophos Managed Detection and Response-Team (MDR) reagierte zudem 2023 auf mehrere Fälle, in denen KMUs via Schwachstelle in Remote-Überwachungs- und Management-Software (RMM) ihres MSPs angegriffen wurden.

Social Engineering und Geschäftskommunikation: Angreifer werden penetrant
Speziell auf Unternehmen abzielende Scam-Emails, sogenanntes Business E-Mail Compromise (BEC), gehörten 2023 zu den zweithäufigsten Attacken nach Ransomware. Diese und weitere Social-Engineering-Angriffe beinhalten ein wachsendes Level an Raffinesse: Statt einfach nur eine E-Mail mit schädlichem Anhang zu senden, beschäftigen sich die Kriminellen nun näher mit ihrem Opfer und senden eine ganze Reihe an E-Mail-Nachrichten oder rufen sie sogar an. In dem Versuch, den klassischen Spam-Werkzeugen zu entgehen, experimentieren die Angreifer mittlerweile mit neuen Formaten für ihre schadhaften Inhalte, wie das Einbinden von Bildern mit Malware oder bösartige Anhänge in OneNote oder Archivformaten. In einem Fall deckte Sophos auf, dass die Betrüger ein PDF-Dokument mit einem verschwommenen, unlesbaren Thumbnail einer „Rechnung“ schickten. Der Download-Knopf beinhaltete dann einen Link zu einer schadhaften Webseite.

„Unser aktueller Report zeigt einmal mehr, dass es für KMUs nicht an Bedrohungen mangelt, und die Komplexität dieser Angriffe ist oft mit denen auf große Organisationen vergleichbar“, so Christopher Budd. „Denn während die zu erwartenden Lösegeld- oder Erpressungssummen geringer als bei einer größeren Organisation sind, gleichen die Kriminellen dieses ‚Manko‘ durch die Masse der Attacken und aufgrund der oftmals laxeren Cybersicherheitsvorkehrungen leicht wieder aus. Die Angreifer rechnen damit, dass kleinere Unternehmen weniger gut geschützt sind und keine modernen, hochentwickelten Tools zum Schutz ihrer Benutzer und Vermögenswerte einsetzen. Hierin liegt gleichzeitig auch der Schlüssel zum erfolgreichen Schutz: KMUs müssen diese Annahmen als falsch beweisen. Es gilt, die Mitarbeiter zu schulen, eine Multifaktor-Authentifizierung auf allen externen Ressourcen zu implementieren, Server und Netzwerkgeräte mit höchster Priorität zu patchen und gegebenfalls Managed Services in Anspruch zu nehmen. Unserer Erfahrung nach besteht der Hauptunterschied zwischen den Unternehmen, die am stärksten von Cyberangriffen betroffen waren, und denen, die am wenigsten darunter gelitten haben, in der Reaktionszeit. Sicherheitsexperten zu haben, die rund um die Uhr überwachen und reagieren, ist für eine wirksame Verteidigung im Jahr 2024 von entscheidender Bedeutung.“

Alle Details zu diesen Angriffen und weitere Informationen zum aktuellen Stand in Sachen Cyberkriminalität können im 2024 Sophos Threat Report: Cybercrime on Main Street nachgelesen werden.

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/
X/Twitter: @sophos_info

Über Sophos

Sophos ist ein weltweit führender und innovativer Anbieter von fortschrittlichen Cybersecurity-Lösungen, darunter Managed Detection and Response (MDR)- und Incident-Response-Dienste. Das Unternehmen bietet ein breites Portfolio an Endpoint-, Netzwerk-, E-Mail- und Cloud-Sicherheitstechnologien, das bei der Abwehr von Cyberangriffen unterstützt. Als einer der größten auf Cybersecurity spezialisierten Anbieter schützt Sophos mehr als 500.000 Unternehmen und mehr als 100 Millionen Anwender weltweit vor aktiven Angriffen, Ransomware, Phishing, Malware und vielem mehr.
Die Dienste und Produkte von Sophos werden über die cloudbasierte Management-Konsole Sophos Central verbunden und vom bereichsübergreifenden Threat-Intelligence-Expertenteam Sophos X-Ops unterstützt. Die Erkenntnisse von Sophos X-Ops erweitern das gesamte Sophos Adaptive Cybersecurity Ecosystem. Dazu gehört auch ein zentraler Datenspeicher, der eine Vielzahl offener APIs nutzt, die Kunden, Partnern, Entwicklern und anderen Anbietern von Cybersecurity und Informationstechnologie zur Verfügung stehen. Sophos bietet Cybersecurity-as-a-Service für Unternehmen an, die vollständig verwaltete, schlüsselfertige Sicherheitslösungen benötigen. Kunden können ihre Cybersecurity auch direkt mit der Security Operations Platform von Sophos verwalten oder einen hybriden Ansatz verfolgen, indem sie ihre internen Teams mit Sophos Services ergänzen, einschließlich Threat Hunting und Systemwiederherstellung.
Sophos vertreibt seine Produkte über Reseller und Managed Service Provider (MSPs) weltweit. Der Hauptsitz von Sophos befindet sich in Oxford, U.K.
Weitere Informationen unter: www.sophos.de

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