IBM DACH Newsroom

IBM X-Force Report: Europa verzeichnete 2023 weltweit die meisten Cyberattacken

• 32 % aller im Jahr 2023 verzeichneten Angriffe erfolgten in Europa; Großbritannien (27 %), Deutschland (15 %) und Dänemark (14 %) sind die am häufigsten angegriffenen Länder in der Region

• Die Fertigungsindustrie war mit 28 % aller Vorfälle die am häufigsten angegriffene Industriebranche in Europa

• Die größten Schwachstellen für europäische Unternehmen sind Benutzeridentitäten und E-Mails, wobei der Missbrauch gültiger Konten (30 %) und Phishing (30 %) den Großteil der Angriffe ausmachten

• 74 % der Cyberattacken in der Europäischen Union zielten im Jahr 2023 auf kritische Infrastrukturen ab

CAMBRIDGE, Mass., 21. Februar 2024 – IBM hat heute den 2024 X-Force Threat Intelligence Index veröffentlicht, der Europa als die weltweit am häufigsten angegriffene Region identifiziert. Anhand der Ergebnisse des Berichts sieht IBM X-Force eine sich abzeichnende ‚Krise der Identitäten' in Europa und weltweit, da Cyberkriminelle verstärkt Nutzeridentitäten zur Kompromittierung von Unternehmen missbrauchen. Laut IBM X-Force, der Abteilung für offensive und defensive Sicherheitsdienstleistungen von IBM Consulting, gab es im Jahr 2023 weltweit mehr Möglichkeiten für Cyberkriminelle, sich über gültige Konten in Unternehmensnetzwerke einzuloggen anstatt diese zu hacken – diese Taktik ist somit eine bevorzugte Vorgehensweise für Angreifer. Dies gilt auch für Europa, wo die Verwendung gültiger Konten durch Cyberkriminelle als Mittel zur Kompromittierung von Unternehmen im Vergleich zum Vorjahr um 66 % gestiegen ist.

Der X-Force Threat Intelligence Index basiert auf Erkenntnissen und Beobachtungen aus der Überwachung von über 150 Milliarden Sicherheitsereignissen pro Tag in mehr als 130 Ländern. Darüber hinaus werden Daten aus mehreren Quellen innerhalb von IBM erfasst und analysiert, einschließlich IBM X-Force Threat Intelligence, Incident Response, X-Force Red, IBM Managed Security Services sowie Daten von Red Hat Insights und Intezer, die zum Bericht 2024 beigetragen haben.

Der Bericht 2024 enthält unter anderem folgende Ergebnisse für Europa und Deutschland:

- Im Jahr 2023 war Europa mit 32 % der von X-Force bearbeiteten Vorfälle die am stärksten von Cyberangriffen betroffene Region, vor Nordamerika (26 %), Asien und Pazifik (23 %), Lateinamerika (12 %) sowie dem Nahen Osten und Afrika (7 %). Im Jahr 2023 verzeichnete X-Force die höchste Anzahl von Vorfällen in Europa im Vergleich zu den Vorjahren, mit einem Anstieg von 31 % gegenüber dem Vorjahr.
- Malware war mit 44 % der europäischen Vorfälle die am häufigsten beobachtete Ursache. Außerdem gab es in Europa mit 26 % der Angriffe die meisten verzeichneten Ransomware-Angriffe weltweit, was mitverantwortlich für Europas Ranking im Jahr 2023 ist.
- Die drei wichtigsten Auswirkungen auf europäische Unternehmen waren das Abgreifen von Anmeldeinformationen - Credential Harvesting - (28 %), Erpressung (24 %) und Datenlecks (16 %).
- Die Fertigungsindustrie war die am häufigsten angegriffene Industrie in Europa (28 %), gefolgt von professionellen Dienstleistungen und Dienstleistungen für Unternehmen und Verbraucher (25 %), Finanzdienstleistungen (16 %) und dem Energiesektor (14 %).
- In Deutschland zielten 39 % der Angriffe auf Einrichtungen des Gesundheitswesens ab, während 23 % der Angriffe auf die Fertigungsindustrie und Finanzinstitute ausgerichtet waren.
- Auf globaler Ebene verzeichnete Europa den höchsten Prozentsatz an Vorfällen im Energiesektor (43 % aller weltweit erfassten Vorfälle) sowie in der Finanz- und Versicherungsbranche (37 %).

Einige der globalen Highlights und Ergebnisse des Berichts 2024 sind:

- **Angriffe auf kritische Infrastrukturen machen „Fauxpas“ der Industrie sichtbar.** Bei fast 85 % der Angriffe auf kritische Sektoren hätte die Kompromittierung mithilfe von Patches, Multi-Faktor-Authentifizierung oder dem Least Privilege Prinzip - dem Einschränken von Benutzer Accounts - verhindert werden können. Dies zeigt, dass die von der Sicherheitsbranche seit jeher als „Basissicherheit“ bezeichnete Sicherheit schwieriger zu erreichen ist als behauptet.
- **Ransomware-Gruppen stellen auf ein schlankeres Geschäftsmodell um.** Ransomware-Angriffe auf Unternehmen sind im vergangenen Jahr um fast 12 % zurückgegangen, da sich größere Unternehmen gegen eine Zahlung und Entschlüsselung zugunsten des Wiederaufbaus ihrer Infrastruktur entschieden haben. Da dieser wachsende Widerstand wahrscheinlich die Umsatzerwartungen der Angreifer aus verschlüsselungsbasierter Erpressung beeinflusst, ist zu beobachten, dass die zuvor auf Ransomware spezialisierten Gruppierungen zunehmend zu Infostealern werden.
- **Kein Gewinn durch Angriffe auf generative KI - noch nicht.** Laut X-Force-Analyse ist davon auszugehen, dass, sobald eine einzelne generative KI-Technologie einen Marktanteil von 50 % erreicht oder sich der Markt auf drei oder weniger Technologien konsolidiert, Angriffe im großen Stil gegen diese Plattformen erfolgen werden.

„Wenngleich ‚Sicherheitsgrundlagen‘ nicht so viel Aufsehen erregen wie ‚KI-gesteuerte Angriffe‘, so bleibt doch festzuhalten, dass das größte Sicherheitsproblem von Unternehmen auf die grundlegenden und bekannten

Probleme hinausläuft – und nicht auf die neuen und unbekannten“, so Charles Henderson, Global Managing Partner, IBM Consulting und Leiter von IBM X-Force. „Identität wird wieder und wieder für Angriffe auf Unternehmen missbraucht – ein Problem, das sich noch verschärfen wird, wenn Angreifer in KI investieren, um diese Taktik zu optimieren.“

Globale 'Krise der Identitäten' wird sich weiter verschärfen

Gültige Konten zu missbrauchen, ist für Cyberkriminelle der Weg des geringsten Widerstands, da heute Milliarden von kompromittierten Anmeldedaten im Dark Web zugänglich sind. Im Jahr 2023 beobachtete X-Force, dass Angreifer zunehmend in Maßnahmen zur Erlangung von Nutzeridentitäten investierten – mit einem 266 % Anstieg bei Infostealing-Malware, die darauf ausgelegt ist, persönliche Informationen wie E-Mails, Anmeldedaten für soziale Medien und Messaging-Apps, Bankdaten, Krypto-Wallet-Daten und mehr zu stehlen.

Dieser „leichte Einstieg“ für Angreifer ist weitaus schwieriger zu entdecken und erfordert kostspielige Maßnahmen von Unternehmen. Laut X-Force waren größere Vorfälle, die von Angreifern durch die Nutzung gültiger Konten verursacht wurden, mit fast 200 % komplexeren Reaktionsmaßnahmen der Sicherheitsteams verbunden als der durchschnittliche Vorfall – wobei Sicherheitsverantwortliche zwischen legitimen und bösartigen Benutzeraktivitäten im Netzwerk unterscheiden müssen. In der Tat stellte der IBM 2023 Cost of a Data Breach Report fest, dass bei Sicherheitsverletzungen, die durch gestohlene oder kompromittierte Zugangsdaten verursacht wurden, rund 11 Monate für die Erkennung und Wiederherstellung benötigt wurden – die längste Reaktionszeit im Vergleich zu jedem anderen Infizierungsvektor.

Dieser umfangreiche Zugriff auf die Online-Aktivitäten von Nutzern wurde deutlich, als das FBI und die europäischen Strafverfolgungsbehörden im April 2023 ein globales Forum für Cyberkriminalität ausschalteten, das die Anmeldedaten von mehr als 80 Millionen Nutzerkonten sammelte. Identitätsbasierte Angriffe werden wahrscheinlich weiter zunehmen, da Angreifer generative KI nutzen werden, um ihre Angriffe zu optimieren. Bereits im Jahr 2023 beobachtete X-Force über 800.000 Beiträge zu KI und GPT in Dark-Web-Foren, was bestätigt, dass diese Innovationen die Aufmerksamkeit und das Interesse von Cyberkriminellen geweckt haben.

Angreifer „loggen“ sich in kritische Infrastruktur-Netzwerke ein

Weltweit richteten sich fast 70 % der Angriffe, zu denen X-Force zur Hilfe gerufen wurde, gegen Unternehmen mit kritischen Infrastrukturen – ein alarmierendes Ergebnis, das verdeutlicht, dass Cyberkriminelle auf die Notwendigkeit der Verfügbarkeit dieser hochwertigen Ziele setzen, um ihre eigenen Ziele zu erreichen. Dieser Sektor machte 74 % der Vorfälle in der EU aus.

Fast 85 % der Angriffe, auf die X-Force in diesem Bereich reagierte, wurden durch die Ausnutzung von öffentlichen Anwendungen, Phishing-E-Mails und die Nutzung von gültigen Konten verursacht. Letzteres stellt ein erhöhtes Risiko für den Sektor dar, wobei nach Angaben des DHS CISA die Mehrheit der erfolgreichen Angriffe auf Regierungsbehörden, Unternehmen mit kritischer Infrastruktur und staatliche Regierungsstellen im Jahre 2022 die Verwendung gültiger Konten beinhaltete. Dies unterstreicht die Notwendigkeit, dass diese Unternehmen häufiger Belastungstests für ihre Umgebungen durchführen müssen, um potenzielle Risiken zu erkennen und Pläne zur Reaktion auf Vorfälle zu entwickeln.

Generative KI – die nächste große Herausforderung für die Sicherheit

Damit Cyberkriminelle einen Gewinn aus ihren Kampagnen ziehen können, müssen die Technologien, auf die sie abzielen, in den meisten Unternehmen weltweit vertreten sein. Gleichermaßen wie die technologischen Voraussetzungen in der Vergangenheit cyberkriminelle Aktivitäten begünstigt haben – wie beispielsweise Ransomware und die Marktdominanz von Windows Server, BEC-Betrug und die Dominanz von Microsoft 365 oder Kryptojacking und die Konsolidierung des Infrastructure-as-a-Service-Marktes – wird sich dieses Muster höchstwahrscheinlich auf KI ausweiten.

X-Force geht davon aus, dass eine generative KI-Marktdominanz, bei der eine einzelne Technologie einen Marktanteil von 50 % erreicht oder sich der Markt auf drei oder weniger Technologien konsolidiert, den Ausschlag für die Attraktivität von KI als Angriffsfläche geben und weitere Investitionen von Cyberkriminellen in neue Tools auslösen könnte. Obwohl sich die generative KI derzeit in der Phase vor der Massenvermarktung befindet, ist es unerlässlich, dass Unternehmen ihre KI-Modelle sichern, bevor Cyberkriminelle ihre Aktivitäten ausweiten. Unternehmen sollten auch erkennen, dass ihre vorhandene zugrunde liegende Infrastruktur ein Gateway zu ihren KI-Modellen ist, das keine neuen Taktiken von Angreifern erfordert, um es zu attackieren. Dies unterstreicht die Notwendigkeit eines ganzheitlichen Ansatzes für Sicherheit im Zeitalter generativer KI, wie im IBM Framework for Securing Generative AI beschrieben.

Weitere Ressourcen

- Laden Sie eine Kopie **des 2024 X-Force Threat Intelligence Index** herunter.
- Weitere Informationen zu den wichtigsten Ergebnissen des Berichts finden Sie in diesem **IBM Security Intelligence** Blog.
- Registrieren Sie sich für das Webseminar zum **2024 IBM X-Force Threat Intelligence** am Donnerstag, den 21. März um 09:00 Uhr (ET).
- Setzen Sie sich mit dem **IBM X-Force Team** in Verbindung, um eine persönliche Einschätzung der Ergebnisse zu erhalten.

Kontakt für Journalisten:

Barbara Jax

IBM Unternehmenskommunikation

barbara.jax@at.ibm.com
