IBM DACH Newsroom

IBM-Report: Auch 2022 kam bei den meisten Cyberattacken Ransomware zum Einsatz

Fertigungsindustrie ist die am häufigsten erpresste Branche – weltweit und in Deutschland; E-Mail-Thread-Hijacking-Versuche nehmen zu; Zeit bis zur Lösegeldübergabe verkürzt sich von Monaten auf Tage

ARMONK, NY; Ehningen -- 22. Februar, 2023 -- IBM Security hat heute seinen jährlichen **X-Force Threat Intelligence Index** veröffentlicht. Es wurde festgestellt, dass der Anteil von Vorfällen mit Ransomware an den registrierten IT-Sicherheitsvorfällen im Jahr 2022 weltweit nur geringfügig (um vier Prozentpunkte) zurückgegangen ist. IT-Sicherheitsexperten waren jedoch erfolgreicher darin, Attacken durch Ransomware zu erkennen und zu verhindern. Trotzdem waren Angreifer weiterhin innovativ: Der Bericht zeigt, dass die durchschnittliche Zeit bis zum Abschluss eines Ransomware-Angriffs von zwei Monaten auf weniger als vier Tage gesunken ist.

Laut dem Bericht von 2023 haben sich Backdoors, die Fernzugriff auf Systeme ermöglichen, im letzten Jahr zur bevorzugten Angriffsmethode der Cyberkriminellen entwickelt. Ungefähr 67 Prozent dieser Backdoor-Fälle bezogen sich auf Versuche Ransomware zu installieren, bei denen Sicherheitsteams in der Lage waren, die Backdoor rechtzeitig zu erkennen, bevor die Ransomware installiert wurde. Der Anstieg der Backdoor-Nutzung kann teilweise auf ihren hohen Marktwert zurückgeführt werden. X-Force beobachtete, dass die kriminellen Akteure bestehende Backdoor-Zugänge für bis zu 10.000 US-Dollar verkaufen können. Gestohlene Kreditkartendaten werden im Vergleich dazu heute für weniger als 10 US-Dollar pro Karte verkauft.

Das Ausnutzen von Backdoors war auch in Deutschland eine der drei häufigsten Angriffsmethoden. Die beiden anderen waren die Kompromittierung von geschäftlichen E-Mails (Business E-Mail Compromise) sowie das Kapern von E-Mail-Konversationen (E-Mail-Thread-Hijacking). Europaweit rangierten Backdoors mit 21 Prozent

der registrierten Fälle, Verschlüsselungstrojaner (11 Prozent) und das Ausnutzen von Fernzugriffs-Tools (10 Prozent) an der Spitze. Nach dem Überfall Russlands auf die Ukraine stieg das Ausnutzen von Backdoors in Europa signifikant an. Insgesamt war das Vereinigte Königreich mit 43 Prozent aller beobachteten Fälle das am häufigsten angegriffene Land in Europa. Deutschland lag mit 14 Prozent auf dem zweiten Platz, Portugal mit 9 Prozent auf dem dritten.

Der IBM Security X-Force Threat Intelligence-Index erfasst fortlaufend die neuen und bestehenden IT-Security-Trends und Angriffsmuster – aus Milliarden von Datenpunkten von Netzwerk und Endgeräten, Incident Response Einsätzen und anderen Quellen.

„Die Verlagerung hin zur Erkennung von Cyberangriffen und zur rechtzeitigen Reaktion hat es den Verteidigern ermöglicht, Angreifer früher in der Angriffskette abzufangen. Damit konnten sie die weitere Verbreitung von Ransomware zumindest vorübergehend eindämmen", sagte Charles Henderson, Leiter der IBM Security X-Force. „Aber es ist nur eine Frage der Zeit, bevor das heutige Backdoor-Problem die Ransomware-Krise von morgen wird. Angreifer finden immer neue Wege, um der Erkennung zu entgehen. Gute Verteidigung ist nicht mehr genug. Um das endlose Wettrennen mit Angreifern zu beenden, müssen Unternehmen eine proaktive, bedrohungsbezogene Sicherheitsstrategie verfolgen.“

Zu den wichtigsten Ergebnissen des X-Force Threat Intelligence Index 2023 gehören:

- **Erpressung: Die beliebteste Methode der Angreifer**. Die häufigste Auswirkung von Cyberattacken im Jahr 2022 war Erpressung. Hierzu wurden in erster Linie Ransomware oder die Kompromittierung von geschäftlichen E-Mails genutzt. Europa war die wichtigste Zielregion für diese Art von Taten. 44 Prozent der beobachteten Erpressungsfälle fanden hier statt, da Bedrohungsakteure die aktuellen geopolitischen Spannungen ausnutzten. In Deutschland war Erpressung die wichtigste Auswirkung der von X-Force behobenen Vorfälle.
- **Cyberkriminelle nutzen E-Mail-Konversation als Angriffsmittel**. Das sogenannte Thread-Hijacking verzeichnete im Jahr 2022 einen deutlichen Anstieg. Angreifer nutzten kompromittierte E-Mail-Konten, um sich im laufenden Mailverkehr einzuklinken, dann als ursprüngliche Teilnehmer auszugeben und als diese zu antworten. X-Force verzeichnete einen Anstieg der monatlichen Versuche um 100 Prozent im Vergleich zu den Daten aus dem Jahr 2021.
- **Altbekannte Exploits, die immer noch funktionieren.** Der Anteil der bekannten Exploits im Vergleich zu den Schwachstellen sank von 2018 bis 2022 um 10 Prozentpunkte. Das liegt aber daran, dass die Anzahl der insgesamt bekannten Schwachstellen ein weiteres Allzeithoch erreichte. Die Zahlen des aktuellen Reports zeigen, dass ältere Schadprogramme wie WannaCry und Conficker weiterhin existieren und sich verbreiten konnten.

Erpressungsdruck auf Fertigungsindustrie steigt

Cyberkriminelle zielen häufig auf die anfälligsten Branchen, Unternehmen und Regionen mit Erpressungsmaschen ab. Sie wenden dann hohen psychologischen Druck an, um Opfer zur Zahlung zu zwingen. Die Fertigungsindustrie war die am meisten erpresste Branche im Jahr 2022, und das bereits das zweite Jahr in Folge. In Deutschland war sie mit ca. 25 Prozent der beobachteten Fälle die mit am stärksten betroffene Branche. Der Grund: Fertigungsunternehmen sind angesichts der extrem geringen Ausfalltoleranz in den laufenden Produktionsprozessen ein attraktives Ziel für Erpressung.

Ransomware ist eine bekannte Erpressungsmethode, aber die Angreifer suchen immer neue Wege, zum Ziel zu kommen. Eine ihrer neuesten Strategien besteht darin, mitbetroffene Opfer wie zum Beispiel Kunden und Geschäftspartner über gestohlene Daten zu informieren. Durch die Einbindung dieser Mitgeschädigten erhöhen die Erpresser den Druck auf die betroffene Organisation. Die Kriminellen werden auch weiterhin mit solchen Taktiken experimentieren, um die potenziellen Kosten und psychologischen Auswirkungen eines Cyberangriffs zu erhöhen. Daher ist es wichtig, dass Unternehmen über vorbereitete Reaktionspläne verfügen, die auch die Auswirkungen eines Angriffs auf mitbetroffene, externe Opfer wie Kunden und Geschäftspartner berücksichtigen.

Thread-Hijacking im Aufwärtstrend

Die Zahl der registrierten Fälle von E-Mail-Thread-Hijacking ist im letzten Jahr stark angestiegen. Die monatlichen Hijacking-Versuche haben sich im Vergleich zu den Daten aus 2021 verdoppelt. Im Laufe des letzten Jahres stellte X-Force fest, dass Angreifer diese Taktik verwendet haben, um Emotet, Qakbot und IcedID zu verbreiten - Schadsoftware, die häufig zu Ransomware-Infektionen führt. Thread-Hijacking gehörte auch in Deutschland gemeinsam mit Backdoors und dem Kompromittieren von Geschäftsmails zu den drei am häufigsten registrierten Angiffsarten. Alle drei wurden hier von der X-Force gleich häufig beobachtet.

Da Phishing die Hauptursache für Cyberangriffe im letzten Jahr war und Thread-Hijacking stark anstieg, ist es klar, dass Angreifer das Vertrauen in E-Mails ausnutzen. Unternehmen sollten Mitarbeiter auf Thread-Hijacking aufmerksam machen, um das Risiko zu verringern, dass sie zu Opfern werden.

Mind the GAP: Exploit R&D (Forschung und Entwicklung) hinkt der Entwicklung von Schwachstellen hinterher

Das Verhältnis von bekannten Exploits zu Schwachstellen ist seit 2018 um zehn Prozentpunkte zurückgegangen. Cyberkriminelle haben mittlerweile Zugriff auf mehr als 78.000 bekannte Exploits. Ältere, noch nicht gepatchte Schwachstellen sind leicht auszunutzen und ein gefährliches Einfallstor in IT-Systeme: Selbst mehr als fünf Jahren stellen die Sicherheitslücken, die zu Infektionen mit WannaCry führten, immer noch eine erhebliche Bedrohung dar. X-Force hat seit April 2022 einen 800% Anstieg des WannaCry-Ransomware-Datenverkehrs in Telemetriedaten festgestellt. Die fortlaufende Nutzung älterer Exploits macht deutlich, dass Unternehmen ihre Programme für das Schwachstellenmanagement optimieren und weiterentwickeln müssen. Dazu gehört auch, dass sie ein besseres Verständnis ihrer Angreifbarkeit entwickeln und Patches risikobasiert priorisieren müssen.

Weitere Ergebnisse des Berichts 2023 umfassen:

- **Phisher verlieren Interesse an Kreditkartendaten.** Die Anzahl der Cyberkriminellen, die auf Kreditkarteninformationen in Phishing-Kits abzielen, sank in einem Jahr um 52 Prozent. Das weist darauf hin, dass Angreifer personenbezogene Daten wie Namen, E-Mails und Privatadressen priorisieren, die zu einem höheren Preis im Dark Web verkauft oder für weitere Zwecke verwendet werden können.
- **Nord-Amerika Hauptziel von Angriffen im Energiesektor.** Die Energiebranche bleibt weiterhin die am vierthäufigsten attackierte Industrie im vergangenen Jahr. Die globale Sicherheitslage wirkte sich hier auf einen bereits turbulenten globalen Energiehandel aus. Auf die nordamerikanischen Energieunternehmen entfielen 46 Prozent aller im letzten Jahr insgesamt beobachteten Angriffe auf Energieunternehmen. Das

entspricht einem Anstieg von 25 Prozent gegenüber 2021.

- **Europa erlebt einen Anstieg der Angriffe.** Europa war mit 28 Prozent aller erfassten Angriffe die weltweit am zweithäufigsten betroffene Region und verzeichnete einen Anstieg um 4 Prozentpunkte gegenüber den Zahlen von 2021. Unternehmen für professionelle, geschäftliche und Verbraucherdienstleistungen sowie Finanz- und Versicherungsunternehmen wurden hier am häufigsten angegriffen. An zweiter Stelle steht das verarbeitende Gewerbe mit 12 % der Fälle, an dritter Stelle die Energie- und Gesundheitsbranche mit 10 %.

Der Bericht enthält Daten, die IBM im Jahr 2022 global erfasste, um Informationen zur globalen IT-Bedrohungslage bereitzustellen. Er informiert die Sicherheitscommunity über die Bedrohungen, die für ihre Unternehmen am relevantesten sind. Sie können eine Kopie des neuesten IBM Security X-Force Threat Intelligence Index für 2023 hier herunterladen.

Zusätzliche Quellen

- Weitere Informationen zu den wichtigsten Ergebnissen des Berichts finden Sie in diesem IBM Security Intelligence-Blog.
- Melden Sie sich für das IBM Security X-Force Threat Intelligence Index-Webseminar 2023 am Donnerstag, 2. März 2023, um 17:00 Uhr hier an.
- Planen Sie eine Beratung mit IBM Security X-Force

Informationen zu IBM Security

IBM Security schützt die weltweit größten Unternehmen und Behörden mit einem integrierten Portfolio von Sicherheitsprodukten und -services, das dynamische KI- und Automatisierungsfunktionen bietet. Das Portfolio, das von der weltweit bekannten IBM Security X-Force®-Forschung unterstützt wird, ermöglicht es Unternehmen, Bedrohungen vorherzusagen, Daten während der Übertragung zu schützen und schnell und präzise zu reagieren, ohne geschäftliche Innovation zu behindern. Sicherheitsexperten weltweit, Tausende von Unternehmen vertrauen IBM als Partner bei der Bewertung, Strategie, Implementierung und Verwaltung von Sicherheitstransformationen. IBM betreibt eine der weltweit größten Organisationen für Sicherheitsforschung, -entwicklung und -bereitstellung, überwacht mehr als 150 Milliarden Sicherheitsereignisse pro Tag in mehr als 130 Ländern und hat weltweit mehr als 10.000 Sicherheitspatente erhalten.

Kontakt für Journalisten:

Barbara Jax

IBM Unternehmenskommunikation

e-mail: barbara.jax@at.ibm.com

Mobile: +43.664.618 7237
