IBM DACH Newsroom

Report der IBM X-Force zeigt: Die Fertigungsindustrie war 2021 aufgrund der Lieferketten-Problematik am stärksten von Cyberangriffen betroffen

• Asien-Pazifik ist mittlerweile die am meisten von Cyberangriffen betroffene Region, gefolgt von Europa auf dem zweiten Platz

• Die durchschnittliche Lebensdauer von Ransomware-Gruppen beträgt 17 Monate

• Vishing verdreifacht die Phishing-Klickrate

CAMBRIDGE, Mass., 23. Februar, 2022 - IBM Security veröffentlicht heute seinen jährlichen X-ForceThreat Intelligence Index. Dieser zeigt, dass der Einsatz von Ransomware und das Ausnutzen von Sicherheitslücken Unternehmen und ihren globalen Lieferketten im Jahr 2021 am meisten gefährdet haben. Die Fertigungsindustrie war hierbei mit 23 % aller Angriffe die weltweit am stärksten betroffene Branche. In Europa betrug der Wert 25 % und in Deutschland sogar 31 %. Phishing war im vergangenen Jahr allgemein die häufigste Ursache für Cyberangriffe. Die IBM Security X-Force beobachtete zudem einen 33-prozentigen Anstieg von Angriffen, die Schwachstellen in ungepatchter Software ausnutzten. Dieses Einfallstor nutzten weltweit 44 % aller Ransomware-Attacken im Jahr 2021, um ihre Angriffe auszuführen – mehr als jede andere Angriffsmethode. In Europa nutzten sogar 46 % aller Ransomware-Attacken diesen Weg, um in Unternehmen einzudringen. Die Länder in Europa mit den meisten verzeichneten Angriffen waren das Vereinigte Königreich, Italien und Deutschland.

Der Report erläutert, wie Ransomware-Angreifer im Jahr 2021 versuchten, globale Lieferketten mit Angriffen auf die Fertigungsindustrie zu unterbrechen. Absoluter Spitzenreiter in Sachen Ransomware war bis dato die Finanzdienstleistungs- und Versicherungsindustrie. Dass nun die Fertigungsindustrie mit 23 % der Angriffe an die Spitze rückte hat folgenden Grund: Angreifer setzten auf den Dominoeffekt, den Störungen bei Fertigungsunternehmen auf ihre nachgelagerten Lieferketten haben würden, um sie zur Zahlung des Lösegelds zu zwingen. Alarmierende 47 % der Angriffe auf Fertigungsunternehmen zielten auf IT-Schwachstellen ab, die die betroffenen Unternehmen noch nicht behoben hatten oder nicht beheben konnten. Das macht deutlich, dass Unternehmen dem Schwachstellenmanagement Priorität einräumen müssen.

Der IBM Security X-Force Threat Intelligence Index 2022 zeigt neue Trends und Angriffsmuster auf, die IBM Security beobachtet und analysiert hat. Die Daten stammen aus Milliarden von Datenpunkten, die von Netzwerk- und Endpunkt-Erkennungsgeräten, Incident-Response-Einsätzen, Phishing-Kit-Tracking und mehr stammen – einschließlich der Daten von Intezer.

Die wichtigsten Erkenntnisse im diesjährigen Report

- **Ransomware-Gruppen trotzen Takedowns.** Ransomware war auch im Jahr 2021 die am häufigsten beobachtete Angriffsmethode. Die Ransomware-Gruppen zeigten dabei trotz des Anstiegs der Ransomware-Takedowns keine Anzeichen für Schwäche. Laut dem Bericht beträgt die durchschnittliche Lebensdauer einer Ransomware-Gruppe bis zur Ausschaltung oder Neuaufstellung 17 Monate.

- **IT-Sicherheitslücken sind die größte Achillesferse von Unternehmen.** Der X-Force Report zeigt, dass ungepatchte IT-Schwachstellen bei Unternehmen in Europa, Asien sowie dem Mittleren Osten und Afrika im Jahr 2021 Ziel von etwa 50 % der Angriffe waren. Das zeigt, dass das Patchen von Schwachstellen das größte Problem in den Unternehmen ist.

- **Frühe Warnzeichen für eine Cyber-Krise in der Cloud.** Cyberkriminelle bereiten sich darauf vor, Cloud-Umgebungen ins Visier zu nehmen. Der Report zeigt einen 146-prozentigen Anstieg von neuem Linux-Ransomware-Code. Zudem nehmen die Angreifer verstärkt Docker ins Visier. Das macht es möglicherweise für mehr Cyberkriminelle einfacher, Cloud-Umgebungen für böswillige Zwecke zu nutzen.

„Cyberkriminelle sind normalerweise hinter Geld her. Mit Ransomware sind sie nun auf der Jagd nach Druckmitteln“, sagt Charles Henderson, Leiter von IBM X-Force. „Unternehmen sollten erkennen, dass Sicherheitslücken eines ihrer zentralen Probleme sind – denn Ransomware-Gruppen nutzen diese zu ihrem Vorteil. Dies ist eine nicht-binäre Herausforderung. Die Angriffsfläche wird immer größer. Anstatt also davon auszugehen, dass alle Schwachstellen in ihrer Umgebung gepatcht sind, sollten Unternehmen davon ausgehen, dass sie kompromittiert sind, und ihr Schwachstellenmanagement mit einer Zero-Trust-Strategie verbessern.“

Die „Neun Leben“ von Ransomware-Gruppen

Als Reaktion auf die jüngst verstärkte Ransomware-Bekämpfung durch die Strafverfolgungsbehörden aktivieren Ransomware-Gruppen möglicherweise ihre eigenen Disaster Recovery-Pläne. Die Analyse von X-Force zeigt, dass die durchschnittliche Lebensdauer einer Ransomware-Gruppe bis zur Stilllegung oder Neuformierung 17 Monate beträgt. Die Gruppe REvil zum Beispiel, die für 37 % aller Ransomware-Angriffe im Jahr 2021 verantwortlich war, bestand sogar vier Jahre lang und stellte sich immer wieder neu auf. Das deutet auf die Wahrscheinlichkeit hin, dass sie wieder auftaucht, obwohl sie Mitte 2021 durch eine internationale Polizeioperation ausgeschaltet wurde.

Strafverfolgungsbehörden können die Ransomware-Angreifer nicht nur aufhalten. Sie belasten sie durch die Verfolgung auch mit den Kosten, die für die Finanzierung ihrer Neuaufstellung oder den Wiederaufbau ihrer Infrastruktur erforderlich sind. Da sich das Spielfeld ändert, ist es wichtig, dass Unternehmen ihre Infrastruktur modernisieren und ihre Daten in einer gut geschützten IT-Umgebung unterbringen – sei es vor Ort oder in einer Cloud. Dies hilft Unternehmen dabei, ihre Workloads zu verwalten, zu kontrollieren und zu schützen und Angreifern die Arbeit zu erschweren, indem sie es aufwändiger machen, auf kritische Daten in hybriden Cloud-Umgebungen zuzugreifen.

Schwachstellen können zu einer existenziellen Krise werden

Der X-Force Report unterstreicht die rekordverdächtige Zahl der im Jahr 2021 aufgedeckten Schwachstellen. Die Sicherheitslücken in industriellen Steuerungssystemen sind dabei im Vergleich zum Vorjahr um 50 % gestiegen. Obwohl in den letzten zehn Jahren mehr als 146.000 Schwachstellen aufgedeckt wurden, haben Unternehmen erst in den letzten Jahren ihre digitale Entwicklung beschleunigt – vor allem aufgrund der Pandemie. Das deutet darauf hin, dass die Herausforderung des Schwachstellenmanagements ihren Höhepunkt noch nicht erreicht hat.

Gleichzeitig wird das Ausnutzen von Schwachstellen als Angriffsmethode immer beliebter. X-Force beobachtete einen Anstieg von 33 % gegenüber dem Vorjahr, wobei die beiden 2021 am häufigsten ausgenutzten Schwachstellen in weit verbreiteten Unternehmensanwendungen (Microsoft Exchange, Apache Log4J Library) zu finden waren. Die Herausforderung für Unternehmen, Schwachstellen zu managen, könnte sich weiter verschärfen, da digitale Infrastrukturen expandieren und Unternehmen mit Audit- und Wartungsanforderungen überfordert sein können. Das unterstreicht, wie wichtig es für Unternehmen ist, grundsätzlich von einer Kompromittierung auszugehen und eine Zero-Trust-Strategie anzuwenden, um ihre Architektur zu schützen.

Angreifer zielen auf Gemeinsamkeiten zwischen den Clouds

Im Jahr 2021 beobachtete X-Force, dass Angreifer zunehmend Container wie Docker ins Visier nehmen – lautRedHat die bei weitem dominierende Container Laufzeitumgebung. Angreifer haben erkannt, dass Container in Unternehmen mittlerweile weit verbreitet sind. Daher suchen sie verstärkt nach Möglichkeiten, ihren ROI mit Malware zu maximieren, die plattformübergreifend ist und als Sprungbrett zu anderen Komponenten der Infrastruktur ihrer Opfer genutzt werden kann.

Der Bericht warnt auch davor, dass Angreifer weiterhin in neue, bisher unbeobachtete Linux-Malware investieren. Die von Intezer bereitgestellten Daten zeigen bei Linux-Ransomware mit neuem Code einen Anstieg um 146 %. Die Angreifer suchen weiterhin nach Möglichkeiten, ihre Aktivitäten mit Hilfe von Cloud-Umgebungen zu skalieren. Daher müssen sich Unternehmen darauf konzentrieren, ihre hybriden Infrastrukturen besser zu analysieren und zu verstehen. Hybride Cloud-Umgebungen, die auf Interoperabilität und offenen Standards beruhen, können Unternehmen dabei helfen, blinde Flecken zu erkennen und Sicherheitsmaßnahmen zu beschleunigen und zu automatisieren.

Weitere Ergebnisse des Berichts für 2022 sind:

- **Die meisten Attacken treffen Asien –** Mit mehr als einem von vier Angriffen, die IBM 2021 weltweit beobachtet hat, gab es in Asien im vergangenen Jahr mehr Cyberangriffe als in jeder anderen Region. Finanzdienstleister und Fertigungsunternehmen waren zusammen von fast
  60 % der Angriffe in Asien betroffen. Europa ist weltweit die am zweithäufigsten angegriffene Region. Hier wurden im Jahr 2021 26 % aller Zwischenfälle verzeichnet, im Jahr 2020 waren es noch 31 %.

- **Telefonanarufe machen Phishing erfolgreicher –** Phishing war 2021 die häufigste Ursache von Cyberangriffen. Bei den

Penetrationstests von X-Force Red verdreifachte sich die Klickrate in den Phishing-Kampagnen, wenn sie mit Telefonanrufen kombiniert wurde.

Den kompletten IBM Security X-Force Threat Intelligence Index 2022 finden Siehier.

Außerdem interessant:

- Melden Sie sich hier für das IBM Security X-Force Threat Intelligence Index-Webinar 2022 am Donnerstag, 3. März 2022 um 11:00 Uhr ET an.
- Lesen Sie einen Blog-Beitrag der Autoren des Berichts, um mehr über drei der wichtigsten Ergebnisse des Berichts zu erfahren, auf dem IBM Security Intelligence Blog.

Über IBM Security
IBM Security bietet eines der fortschrittlichsten und am besten integrierten Portfolios an Sicherheitsprodukten und -services für Unternehmen. Das Portfolio, das von der weltweit anerkannten IBM Security X-Force-Forschung unterstützt wird, ermöglicht es Unternehmen, Risiken effektiv zu verwalten und sich gegen neue Bedrohungen zu schützen. IBM betreibt eine der weltweit umfangreichsten Organisationen für Sicherheitsforschung, -entwicklung und -bereitstellung, überwacht täglich mehr als 150 Milliarden Sicherheitsereignisse in mehr als 130 Ländern und hat weltweit mehr als 10.000 Sicherheitspatente erteilt bekommen. Weitere Informationen finden Sie unter www.ibm.com/security, folgen Sie @IBMSecurity auf Twitter oder besuchen Sie den IBM Security Intelligence Blog.

IBM Pressekontakt:
Kerstin Pehl
Unternehmenskommunikation IBM DACH
Tel: +49-176-10185348
E-Mail: kerstin.pehl@de.ibm.com

Additional assets available online: Photos

https://de.newsroom.ibm.com/2022-02-23-IBM-X-Force-Threat-Intelligence-Index-2022