

IBM X-Force-Report: Ransomware-Angriffe und mangelnde Passworthygiene sind die größten Herausforderungen für die IT-Security

Falsch konfigurierte Systeme und Cloud-Server erklären 85 Prozent der gestohlenen Datensätze

CAMBRIDGE, MA und Ehningen - 11. Februar 2020 - Der aktuelle IBM X-Force Threat Intelligence Index 2020 von IBM Security macht die Wichtigkeit des IT Grundschutzes in Form von Passworthygiene und Cloud-Security für Unternehmen und Privatpersonen deutlich:

- **Mangelnde IT-Sicherheit hat 2019 zu einem neuen Rekord von mehr als 8,5 Milliarden gestohlener Datensätze geführt, was einem Anstieg von 200 Prozent gegenüber dem Vorjahr gleichkommt.**
- **Gestohlene Zugangsdaten und nicht gepatchte Schwachstellen werden zu einem immer größeren Problem für die IT-Sicherheit.**
- **Schwachstellen und Patches: Hacker lernen aus den Fehlern der IT-Security.**

Die Ergebnisse des aktuellen [IBM X-Force Threat Intelligence Index 2020](#) zeigen, wie sich die Techniken von Cyberkriminellen entwickelt haben, nachdem sie jahrzehntelang auf Milliarden von Firmen- und Personendaten sowie Hunderttausende von Softwarefehlern zugreifen konnten.

Kriminelle nutzen beim ersten Eindringen vermehrt gestohlene Zugangsdaten und bekannte Software-Schwachstellen. Und obwohl aktuell 150.000 Schwachstellen bekannt sind, patchen Unternehmen immer noch nicht so konsequent und schnell, wie sie sollten.

Dies führte 2019 dazu, dass 30 Prozent der Vorfälle auf das Scannen und Ausnutzen von Schwachstellen zurückzuführen sind – 2018 waren es nur 8 Prozent. Bekannte Schwachstellen von Microsoft sind dabei am häufigsten ausgenutzt worden. Europa ist nach den USA und Asien auf Platz drei der am häufigsten angegriffenen Regionen und wurde 2019 den IBM Spam-Forschern zufolge hauptsächlich von direkt finanziell motivierten Cyberkriminellen ins Visier genommen.

Weitere Ergebnisse des IBM X-Force Threat Intelligence Index 2020:

- Cyberangriffe mit Lösegeldforderungen stiegen 2019 weltweit deutlich an: Im 4. Quartal 2019 um 67 Prozent im Vergleich zum 4. Quartal des Vorjahres.
- Passwörter – das offene Geheimnis: Mangelnde Passworthygiene gibt Angreifern Zugriff auf noch mehr Zugangsdaten, den sie in 29 Prozent der Fälle auch nutzen. Laut einer kürzlich von IBM gesponserten [EMA-Studie](#) verwenden 39 Prozent der Mitarbeiter dasselbe Passwort für mehrere Konten und 28 Prozent setzen diese nicht systematisch zurück. Dieses Verhalten sowie die Menge an gestohlenen Zugangsdaten im Dark Web helfen Cyberkriminellen dabei, Angriffe zu skalieren.
- Die Cloud muss sicher sein – Von den mehr als 8,5 Milliarden Datensätzen, die 2019 gestohlen wurden, gehen sieben Milliarden oder mehr als 85 Prozent auf falsch konfigurierte Cloud-Server und andere falsch konfigurierte Systeme zurück.

- Ein Phish namens Google: Phishing bleibt mit 31 Prozent der Spitzenreiter unter den Erstinfektionsvektoren, hat aber im Vergleich zum Vorjahr abgenommen. Angreifer nutzen nun vielmehr das Konsumentenvertrauen in Technologiemarken aus: Google (39 Prozent), YouTube (17 Prozent) und Apple (15 Prozent) führen die Top 10 der Markennamen an, die bei Phishing-Versuchen eingesetzt werden.

Laut IBM X-Force macht die häufige Wiederverwendung von Passwörtern diese Marken potenziell zur Zielscheibe. Dazu ergab die [IBM-Studie Future of Identity Study](#), dass 41 Prozent der Millennials dasselbe Kennwort mehrmals wiederverwenden, während die Generation Z im Durchschnitt nur fünf Kennwörter verwendet, was auf eine höhere Wiederverwendungsrate hinweist.

- Ransomware nimmt zu und hat ein neues Ziel: Banken. 7,5 Milliarden US-Dollar haben Ransomware-Angriffe Unternehmen im letzten Jahr gekostet. Bankentrojaner machten hierbei über 50 Prozent des neuartigen Malware-Codes aus. Einer der aktivsten Bankentrojaner 2019 war TrickBot.

- Keine Branche bleibt von Cyberangriffen verschont. Kommunale und öffentliche Einrichtungen stehen im Epizentrum dieser Angriffe. Veraltete Technologien und eine dezentralisierte Infrastruktur machen es Cyberkriminellen einfach.

Weitere Informationen entnehmen Sie bitte der US-amerikanischen Original-Meldung:

<https://newsroom.ibm.com/2020-02-11-IBM-X-Force-Stolen-Credentials-and-Vulnerabilities-Weaponized-Against-Businesses-in-2019>

Der neue Bericht von IBM enthält Daten, die das X-Force-Security-Team 2019 erhoben hat, um Informationen über die globale Bedrohungslandschaft zu liefern und Sicherheitsexperten über die für ihr Unternehmen wichtigsten Bedrohungen zu informieren. Um eine Kopie des IBM X-Force Threat Index 2019 herunterzuladen, besuchen Sie bitte: <https://ibm.biz/downloadxforcethreatindex>

Über IBM Security: IBM Security bietet eines der fortschrittlichsten und integriertesten Portfolios an Produkten und Dienstleistungen für die Unternehmenssicherheit. Das Portfolio, das von der weltweit agierenden IBM X-Force®-Forschung unterstützt wird, ermöglicht es Unternehmen, Risiken effektiv zu managen und sich gegen neue Bedrohungen zu schützen. IBM betreibt eine der weltweit breitesten Forschungs-, Entwicklungs- und Serviceorganisationen für Sicherheit, überwacht 70 Milliarden Sicherheitsereignisse pro Tag in mehr als 130 Ländern und hält weltweit mehr als 10.000 Sicherheitspatente. Weitere Informationen finden Sie unter www.ibm.com/security, folgen Sie [@IBMSecurity](#) auf Twitter oder besuchen Sie den IBM Security Intelligence blog.

Kontaktinformation

Annette Fassnacht

Presse- und Öffentlichkeitsarbeit, IBM Deutschland

Mobile: +49 (0)160 90105052

E-Mail: annettefassnacht@de.ibm.com

<https://de.newsroom.ibm.com/announcements?item=122564>