IBM DACH Newsroom

# Neuer IBM X-Force Sicherheitsreport: Anzahl gestohlener Datensätze in 2017 gesunken - Cyberkriminelle fokussieren sich auf Ransomware

**Menschliches Versagen ist für zwei Drittel aller kompromittierten Datensätze verantwortlich, ebenso für den Rekordanstieg bei falsch konfigurierten Cloud-Infrastrukturen von 424 Prozen**

**Cambridge, MA, USA - 04 Apr 2018:  IBM (NYSE: IBM) Security gibt die Ergebnisse des X-Force Threat Intelligence Index 2018 bekannt: Im vergangenen Jahr sank die Anzahl kompromittierter Datensätze um fast 25 Prozent, da Cyberkriminelle den Schwerpunkt auf Ransomware-Angriffe verlagerten. Letztes Jahr wurden allerdings immer noch mehr als 2,9 Milliarden Datensätze gehackt, gegenüber 4 Milliarden im Jahr 2016. Während die Anzahl der gehackten Datensätze damit noch immer signifikant war, dominierte 2017 das Phänomen Ransomware, da Angriffe wie WannaCry, NotPetya und Bad Rabbit versuchten, Chaos über mehrere Branchen hinweg zu stiften.** Andere wichtigen Studienergebnisse beinhalten einen historischen 424-prozentigen Anstieg bei Hacks im Zusammenhang mit falsch konfigurierter Cloud-Infrastruktur, hauptsächlich aufgrund menschlicher Fehler. Auch war die Finanzbranche erneut mit den meisten erfolgreichen Angriffen Spitzenreiter unter den Angriffszielen: 27 Prozent aller Angriffe zielten auf den Bankensektor.

Der IBM X-Force Threat Intelligence-Index umfasst Erkenntnisse und Beobachtungen aus Daten, die über Hunderte von Millionen von geschützten Endpunkten und Servern in nahezu 100 Ländern analysiert wurden. IBM X-Force unterhält Tausende von Spam-Traps auf der ganzen Welt und überwacht täglich Millionen von Spam- und Phishingangriffen. Dabei werden Milliarden von Webseiten und Bildern analysiert, um betrügerische Aktivitäten und Missbrauch zu erkennen.

"Obwohl die Anzahl von Hacks ein Anzeichen für die Aktivitäten von Cyberkriminellen sind, erzählen sie nicht die ganze Geschichte von 2017 aus Security-Perspektive", sagt Caleb Barlow, Vice President Threat Intelligence von IBM Security. "Letztes Jahr hatten Kriminelle einen klaren Fokus darauf, Daten durch Ransomware-Angriffe zu verschlüsseln. Diese Angriffe werden nicht anhand der Anzahl gestohlener Datensätze gemessen, sondern stellen sich für Unternehmen als noch kostspieliger dar gegenüber traditionellen Datenhacks: Die Fähigkeit, diese Angriffe zu antizipieren und dagegen vorbereitet zu sein, wird von entscheidender Bedeutung sein, da Cyberkriminelle ihre Taktiken dahin weiterentwickeln werden, wo sie sich als am lukrativsten erweisen. "

## Ransomware-Angriffe üben Druck auf Incident-Response aus

Ransomware-Angriffe wie WannaCry, NotPetya und Bad Rabbit sorgten im Jahr 2017 nicht nur für Schlagzeilen, sondern brachten auch ganze Betriebe zum Erliegen, als Cyberkriminelle kritische Infrastrukturen unter anderem im Gesundheitswesen, im Transportwesen und in der Logistik übernahmen und zeitweilig sperren konnten. Insgesamt haben Ransomware-Vorfälle Unternehmen im Jahr 2017 mehr als 8 Milliarden Dollar gekostet, als Cyberkriminelle Angriffe starteten, bei denen es darum ging, kritische Daten zu sperren, anstatt gespeicherte Datensätze zu kompromittieren.

Dieser Trend führt zu einem erhöhten Druck auf Unternehmen, mit Reaktionsstrategien angemessener darauf vorbereitet zu sein, um die Auswirkungen eines Angriffs besser begrenzen zu können. Eine IBM Security-Studie aus dem letzten Jahr hat herausgefunden, dass eine langsame Reaktion die Kosten eines Angriffs negativ

beeinflussen kann, da Vorfälle, die mehr als 30 Tage dauerten, eine siebenstellige Summe mehr kosten können als diejenigen, die in kürzerer Zeit abgefangen werden können.

**Menschliches Versagen bleibt das schwache Glied in der Sicherheitskette**

Im Jahr 2017 nutzten Cyberkriminelle weiterhin menschliche Fehler und Irrtümer bei Infrastrukturkonfigurationen, um Angriffe zu starten. Tatsächlich zeigt der Bericht, dass unbeabsichtigte Aktivitäten wie eine falsch konfigurierte Cloud-Infrastruktur für 70 Prozent der kompromittierten Datensätze verantwortlich waren. Auch werden Cyberkriminelle zunehmend auf die Existenz von falsch konfigurierten Cloud-Servern aufmerksam. Eine Folge: 2017 gab es einen sehr starken Anstieg (424 Prozent) in Bezug auf kompromittierte Datensätze, die durch Fehlkonfigurationen in Cloud-Servern exponiert wurden.

Neben falsch konfigurierten Clouds machten Einzelpersonen, die über Phishing-Attacken gehackt wurden, ein Drittel der Vorfälle im Thema menschliches Versagen aus, die 2017 zu einem Sicherheitsvorfall führten. Dazu gehört das Klicken auf einen Link oder das Öffnen eines Anhangs mit bösartigem Code, der von einer von Cyberkriminellen gestarteten Spam-Kampagne geteilt wird . Der Bericht kommt zu dem Ergebnis, dass sich Cyberkriminelle im Jahr 2017 stark auf das Necurs-Botnetz verlassen haben, um in einigen Fällen Millionen von Spam-Nachrichten über einen Zeitraum von nur wenigen Tagen zu verteilen. In einem zweitägigen Zeitraum im August beobachtete die IBM X-Force-Studie beispielsweise, dass vier separate Necurs-Kampagnen 22 Millionen E-Mails spammten.

**Cyberkriminelle erfolgreich bei der Jagd auf Bankkunden**

In den vergangenen Jahren war die Finanzbranche von Cyberkriminellen mit am stärksten betroffen. Im Jahr 2017 fiel sie auf den dritten Platz in Bezug auf Anzahl der Angriffe (17 Prozent) - hinter der Informations- und Kommunikationstechnologie (33 Prozent) und der Fertigung (18 Prozent) -erlebte jedoch die meisten Sicherheitsvorfälle (27 Prozent), die einer weiteren Untersuchung bedurften.

Weil Finanzdienstleister stark in Cybersicherheitstechnologien zum Schutz ihrer Organisationen investiert haben, konzentrieren sich Cyberkriminelle nun darauf, Banking-Trojaner gezielt gegen Endverbraucher und Bankkunden einzusetzen.

Im IBM X-Force Threat Intelligence Index-Bericht wird beispielsweise festgestellt, dass der Gozi-Banking-Trojaner (und seine Varianten) im Jahr 2017 die am häufigsten verwendete Malware in der Bankbranche war. Die Gozi-Malware richtet sich speziell an Endkunden, da sie anfängliche Banking-Anmeldebildschirme mit Eingabeaufforderungen für Verbraucher zur Eingabe anderer persönlicher Informationen vortäuscht, die dann direkt mit dem Angreifer geteilt werden.

Der Einsatz von Gozi, von dem angenommen wird, dass er von einer äußerst erfahrenen Gruppe von Cyberkriminellen betrieben wird, zeigt, dass das organisierte Verbrechen alle anderen Klassen von Akteuren in der Betrugsszene mit finanzieller Malware überholt hat.

Der neue IBM Bericht enthält Daten, die das X-Force-Security-Team zwischen dem 1. Januar 2017 und dem 31. Dezember 2017 gesammelt hat, um aufschlussreiche Informationen über die globale Bedrohungslandschaft zu liefern und Sicherheitsexperten über die Bedrohungen zu informieren, die für ihre Organisationen am

relevantesten sind. Um eine Kopie des IBM X-Force Threat Index 2018 herunterzuladen, besuchen Sie bitte: https://www.ibm.com/account/reg/us/signup?formid=urx-31271

Tip: Melden Sie sich am Donnerstag, den 5. April um 11:00 Uhr EDT (=17h CET) https://bit.ly/2E2KYSb für das IBM X-Force Threat Index-Webinar an.
Weitere Informationen: ibm.com/security

## Kontaktinformation

**Hans Rehm**

IBM Kommunikation 0171-5566940 hansrehm@de.ibm.com

---

https://de.newsroom.ibm.com/2018-04-04-Neuer-IBM-X-Force-Sicherheitsreport-Anzahl-gestohlener-Datensatze-in-2017-gesunken-Cyberkriminelle-fokussieren-sich-auf-Ransomware