

IBM Security Report: Impfstoff-Lieferketten im Visier – Cyberattacken auf Gesundheits- und Energiesektor nehmen zu Erpressungstrojaner richten Millionenschäden an; auf Open-Source-Systeme spezialisierte Schadsoftware nimmt um 40 % zu und gefährdet Cloud-Plattformen

CAMBRIDGE, MA, 24. Februar 2021 – IBM hat heute den aktuellen [X-Force Threat Intelligence Index](#) vorgestellt. Die jährlich veröffentlichte Studie zur Cybersicherheit zeigt, wie Cyberkriminelle 2020 die sozioökonomischen und wirtschaftlichen Unsicherheiten durch die COVID-19-Pandemie ausgenutzt haben. Die IBM Security X-Force hat beobachtet, dass Angreifer für ihre Attacken zunehmend Unternehmen und Strukturen ins Visier nahmen, die für die COVID-19-Bekämpfung wichtig sind. Dazu gehörten beispielsweise Krankenhäuser, Medizinausrüster, Pharmamunternehmen und auch Energieversorger.

Laut den aktuellen Studienergebnissen haben sich Cyberangriffe auf Unternehmen der Gesundheits- und Energiebranche sowie das produzierende Gewerbe gegenüber dem Vorjahr verdoppelt. Die Angreifer zielten auf Unternehmen, die keine Ausfälle riskieren konnten, ohne medizinische Behandlungen oder kritische Lieferketten zu gefährden. Das produzierende Gewerbe und die Energiebranche gehören nun zu den am häufigsten angegriffenen Branchen, direkt nach der Finanz- und Versicherungswirtschaft. Zu dieser Entwicklung trug bei, dass Angreifer die im Vergleich zu 2019 um fast 50 % gestiegene Anzahl an entdeckten Schwachstellen in industriellen Steuerungssystemen (ICS) ausnutzten.

Für den X-Force Threat Intelligence Index wurden 150 Milliarden sicherheitsrelevante Ereignisse aus 130 Ländern ausgewertet. Zu den wichtigsten Erkenntnissen gehören:

- Europa rückte in den Fokus von Cyberkriminellen und liegt nun auf Platz 1 der attackierten Regionen: 31 % aller weltweit erfassten Angriffe fanden hier statt.
- Erpressungstrojaner waren mit 23 % die häufigste Angriffsmethode im Jahr 2020. Im Gesundheitssektor hat sich die Anzahl der Attacken durch Erpressungstrojaner sogar mehr als verdoppelt und beträgt nun 28 %.
- Im Mai 2020 kam es zu Angriffen auf einen international tätigen deutschen Konzern, der gemeinsam mit der öffentlichen Hand mit der Beschaffung medizinischer Schutzausrüstung gegen COVID-19 betraut war.
- Im Oktober 2020 entdeckte IBM X-Force eine Welle von Phishing-E-mails an Personen, Organisationen und internationalen Institutionen, die in die geplante Verteilung der COVID-19-Impfstoffe eingebunden waren. Hierzu gehörten auch internationale Institutionen mit Sitz in Deutschland, Italien, der Tschechischen Republik und weiteren europäischen Ländern.
- Cyberkriminelle nehmen verstärkt die Hybrid Cloud in den Fokus und setzen hierzu auf Linux-basierte

Schadsoftware, die auf verschiedenen Plattformen und Umgebungen laufen kann. Derartige Schadprogramme wurden im vergangenen Jahr bereits 40 % häufiger eingesetzt.

- Da Home Office und Onlineeinkäufe im vergangenen Jahr drastisch zugenommen haben, rückten Anbieter von Kollaborations-Werkzeugen wie Dropbox oder Microsoft und E-Commerce-Websites wie Amazon oder Paypal in den Fokus von Spoofing-Attacken. Beim Spoofing dringen die Angreifer über eine vorgetäuschte Identität ins Netzwerk ein, z.B. durch eine gefälschte Absenderadresse in E-Mails. Auch Adidas gehörte 2020 global erstmals zu den zehn meistgenutzten Markennamen für diese Art von Attacke.

Bei Interesse an weiteren Details und Studienergebnissen zum X-Force Threat Intelligence Index, lesen Sie bitte die [englischsprachige Originalmeldung](#). Die vollständige Studie finden Sie [hier](#).

Kontakt:

Barbara Jax

IBM Unternehmenskommunikation

Mobile: +43.664.618 7237

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