Cyberkrieg: Hacker gegen die Demokratie

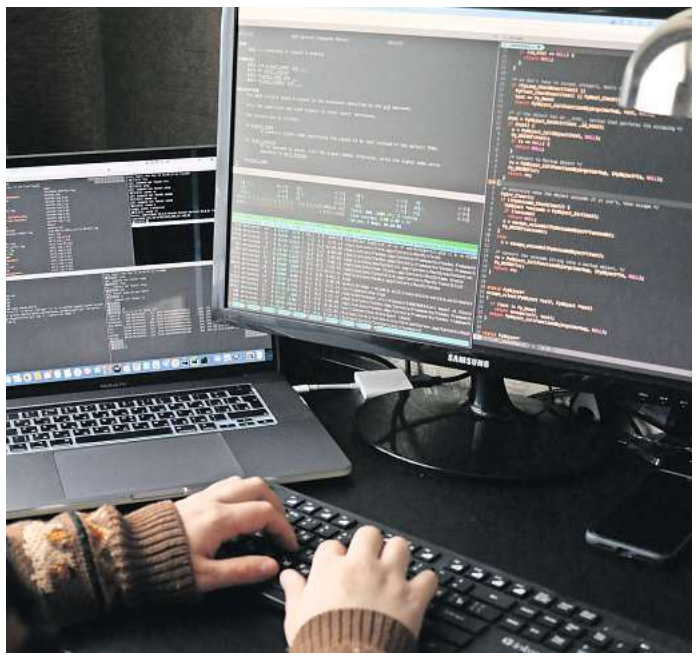
Wahlmanipulationen oder Fake News – Hackergruppen greifen westliche Gesellschaften immer stärker an

VON FELIX HUESMANN

Kriminelle Hackergruppen verwenden häufiger KI-Anwendungen, der Krieg in Gaza sorgt für neue Cyberangriffe, und im Jahr 2024 ist weltweit mit einer Zunahme von Wahlbeeinflussungsversuchen durch Russland, China und den Iran zu rechnen. Das sind einige der wichtigsten Erkenntnisse vom Crowdstrike Global Threat Report. Crowdstrike ist eines der weltweit führenden Cybersicherheitsunternehmen und war in der Vergangenheit an der Untersuchung spektakulärer Cyberangriffe auf Unternehmen, aber auch auf die Demokratische Partei in den USA beteiligt.

Das sind die zentralen Erkenntnisse des Reports:

Kriminelle Gruppen: Crowdstrike fasst die von dem Unternehmen beobachteten Cyberkriminalitätsaktivitäten im „Crowdstrike eCrime Index" zusammen. Der Wert dieses Index ist demnach im Jahr 2023 um 67 Prozent angestiegen. Besonders in der Zeit zwischen Juni und August habe es einen rapiden Anstieg von Cyberkriminalität gegeben, vor allem durch DDoS-Attacken und sogenanntes Big-Game-Hunting. Unter DDoS-Attacken versteht man automatisierte Massenzugriffe auf einen Server, mit dem Ziel, ihn zu überlasten und somit außer Gefecht zu setzen. Beim Big-Game-Hunting – der digitalen Großwildjagd – greifen kriminelle Gruppen lukrative Ziele an, oft, um hohe Lösegeldsummen zu erpressen.



Hackergruppen sorgen nach Angaben der Experten von Crowdstrike für immer mehr Cyberangriffe. SYMBOLFOTO: MIKHAIL FESENKO/UNSPLASH

Schnelle Angreifer: Cyberkriminelle professionalisieren sich zunehmend und benötigen immer weniger Zeit, um in die Systeme ihrer Opfer einzudringen. Die durchschnittliche Zeit zwischen dem Beginn eines Angriffs und der erfolgreichen Infektion eines Computersystems ist laut Crowdstrike-Angaben im vergangenen Jahr von zuvor 84 auf nur noch 62 Minuten gesunken. Je schneller so ein Angriff erfolgt, desto weniger Zeit bleibt den Verteidigern, ihn abzuwehren und die Schäden und Kosten zu minimieren.

Angriffe auf die Cloud: Immer mehr Unternehmensdaten liegen mittlerweile nicht mehr auf lokalen Festplatten, sondern in der Cloud. Dementsprechend richtet sich auch ein steigender Anteil ausgeklügelter Cyberangriffe gegen Cloud-Dienstleistungen. Fälle, in denen Angreifer erfolgreich in Cloud-Umgebungen eingedrungen sind, haben Crowdstrike zufolge 2023 um 75 Prozent gegenüber dem Vorjahr zugenommen. Solche dürften demnach im Jahr 2024 noch weiter zunehmen.

Russland, China und Iran: Russland, China und den Iran sieht Crowdstrike weiterhin als wichtigste staatliche Akteure in der globalen Cyberkriminalität an. Russische und mit Russland verbundene Akteure hätten insbesondere im Zusammenhang mit dem russischen Angriffskrieg gegen die Ukraine ein hohes Aktivitätsniveau aufrechterhalten, heißt es im Global Threat Report. Dadurch seien Spionageaktivitäten, Störaktionen und Informationsoperationen russischer Nachrichtendienste unterstützt worden. Chinesische Akteure, fasst Crowdstrike zusammen, gingen in einem unvergleichlichen Tempo, gut getarnt und in großem Stil vor, um gezielt Daten zur nachrichtendienstlichen Überwachung zu sammeln und geistiges Eigentum zu stehlen. Iranische staatliche Akteure und dem Iran nahestehende Gruppen und „Hacktivisten" aus dem Nahen Osten hätten ihre Aktivitäten 2023 vor allem auf den Konflikt zwischen Israel und der Hamas ausgerichtet.

Gazakrieg befeuert Cyberangriffe: Auf den terroristischen Angriff der Hamas auf Israel und den anschließenden Krieg Israels gegen die Hamas im Gazastreifen folgte auch eine Reihe von Cyberangriffen durch propalästinensische und Hamas-nahe Hacker auf Israel und verbündete Staaten. Teilweise seien Angriffe auf Israel von „Faketivisten" ausgegangen; Angreifern, die sich als propalästinensische Aktivisten tarnen, bei denen es sich aber eigentlich um staatliche oder staatsnahe iranische Akteure handelt.

Künstliche Intelligenz: Generative Künstliche Intelligenz hat im vergangenen Jahr besonders in Form von Diensten wie ChatGPT immer stärker Eingang in den Lebens- und Arbeitsalltag vieler Menschen gefunden. Das gilt auch für Cyberkriminelle und staatliche Angreifer. Generative KI habe die Möglichkeiten von Cyberangriffen „demokratisiert", schreiben die Experten von Crowdstrike. Die Einstiegshürden für die Cyberkriminalität seien damit auch für weniger raffinierte Akteure niedriger. KI könne Angreifern dabei helfen, ihre Angriffe zu planen und durchzuführen und dafür einen passenden Schadcode zu erstellen. Außerdem könne generative KI die Effizienz und Effektivität digitaler Angriffe steigern.

Gefahr der Wahlmanipulation: Mit KI-unterstützten Einflussoperationen und Cyberangriffen sei 2024 auch im Zusammenhang mit Wahlen zu rechnen, warnt Crowdstrike. In 55 Ländern weltweit fänden in diesem Jahr Wahlen auf nationaler Ebene statt. Darunter sind die Europawahlen und die US-Präsidentschaftswahlen. „Das Potenzial des Jahres 2024, die Geopolitik rund um den Globus für die nähere Zukunft zu verändern, wird Angreifern wahrscheinlich zahlreiche Gelegenheiten und einen beträchtlichen strategischen Anreiz bieten, Einrichtungen ins Visier zu nehmen, die an Wahlprozessen beteiligt sind", so die Crowdstrike-Experten.