

G DATA IT-Security-Trends 2022: Künstliche Intelligenz macht Cyberattacken gefährlicher

Angriffe auf Lieferketten nehmen weiter zu und verursachen große finanzielle Schäden.

Bochum (Deutschland), 18. November 2021

Cyberkriminalität steigt auch 2022 weiter an. Angreifer nutzen dabei konsequent jede Schwachstelle aus. Um ihre Ziele zu erreichen, setzen sie auf Multi-Ransomware-Angriffe und verwenden Künstliche Intelligenz, mit der sie besseren Schadcode herstellen. Auch die mögliche Integration von Android-Apps in Windows 11 bietet Kriminellen eine neue Angriffsfläche.

Der Trend der steigenden Cyberkriminalität wird auch 2022 anhalten. Angreifer nehmen insbesondere Unternehmen ins Visier, um maximalen Profit zu erzielen. Dabei gehen sie arbeitsteilig vor und verfeinern ihre Methoden. Ein Trend in den kommenden Jahren: Die Angreifer missbrauchen legale Tools für ihre Zwecke, wie etwa Malware-Programmierung via Codex. Eine Künstliche Intelligenz, die Sprache in verschiedene Programmiersprachen, wie Python, JavaScript oder PHP umwandelt. Codex macht Programmieren einfacher und schneller und reduziert die Fehler im Code. Davon profitieren nun auch Malware-Autoren, die auf diesem Weg Schadsoftware schneller und besser schreiben können. Gleichzeitig nutzen die Angreifer neue Sprachen für Schadsoftware, wie etwa Kotlin oder Swift. Neue Prinzipien und Features erleichtern den Cyberkriminellen die Arbeit.



„Kriminelle müssen ihre Strategien anpassen, weil es heute nicht mehr ausreicht, Schadcode mit Packern vor Security-Software zu verstecken. Schadcode in neuen Programmiersprachen lässt sich manchmal schwerer analysieren, weil am Anfang die Unterstützung durch spezielle Analyse-Tools fehlt. Aber das ist nur eine Frage der Zeit. Das bekannte Katz-und-Maus-Spiel zwischen kriminellen Hackern und Verteidigern setzt sich also fort“, sagt Karsten Hahn, Malware Analyst bei G DATA CyberDefense AG.

Ransomware on Steroids

Aber nicht nur neue Angriffsmöglichkeiten bedrohen die Netzwerke in Unternehmen, Organisationen und Kommunen, sondern auch die

G DATA CyberDefense AG
Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299

Pressemitteilung

Weiterentwicklung bestehender und profitabler Angriffsvektoren. Daher ist von mehr Multi-Ransomware-Angriffen auszugehen. Dabei kombinieren die Kriminellen mehrere Angriffsvektoren: Sie leiten Daten aus dem Unternehmen ab, verschlüsseln die Daten im Netzwerk und führen einen DDoS-Angriff auf die Website des Unternehmens aus. Anschließend erpressen sie nicht nur das Unternehmen, sondern auch die Kunden und drohen bei Nicht-Bezahlen mit der Veröffentlichung persönlicher Daten. Darüber hinaus passen Angreifer ihre Ziele an, um den Druck auf ihre Opfer zu erhöhen. Daher werden sie in Zukunft nicht mehr ausschließlich die Infrastruktur eines Unternehmens angreifen, sondern auch miteinander vernetzte Produkte – von Fahrzeugen über Spielekonsolen bis hin zu Küchengeräten oder vernetzten Industrieanlagen. Ein weiterer Trend: Insbesondere Betreiber kritischer Infrastrukturen rücken verstärkt ins Visier, denn sie haben einen großen und wertvollen Datenschatz.

„Das IT-Sicherheitsniveau in Unternehmen hängt unmittelbar mit dem gesamten Level der IT zusammen. Je professioneller ein Unternehmen aufgestellt ist, desto höher ist hier die Sicherheit. Kleine und mittelständische Unternehmen haben erheblichen Nachholbedarf. Dafür müssen sie Budget freimachen und entweder fachkundiges Personal einstellen oder mit externen Dienstleistern zusammenarbeiten“, sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense AG.

Windows 11: Zutritt durch die Android-Hintertür

Mit der möglichen Integration von Android-Apps in Windows 11 eröffnet Microsoft nicht nur Anwender*innen neue Möglichkeiten, um etwa Spiele künftig auf einem großen Monitor anstelle des Smartphone-Screens zu spielen. Auch für Cyberkriminelle ergeben sich neue Wege, Windows-Rechner anzugreifen und Schadcode in Systeme einzuschleusen. Hier sind auch Unternehmen beziehungsweise die IT-Administratoren gefordert, wenn eine Bring-your-own-device-Policy die dienstliche Nutzung privater Android-Geräte erlaubt. Gegenwärtig kämpfen Entwickler mobiler Malware noch mit einer Reihe praktischer Probleme, wie etwa Genehmigungsverfahren in App-Stores. Allerdings lässt sich mobile Malware als Update für ein beliebtes Softwarepaket tarnen und infiziert so Smartphones, weil viele Menschen unachtsam sind und nicht auf Warnhinweise achten.

Mittelstand im Fadenkreuz

2021 hat bereits gezeigt, dass Cyberkriminelle verstärkt Lieferketten attackieren, um Unternehmen zu infiltrieren. Dieser Trend wird sich nicht nur fortsetzen, sondern auch verstärken. Dabei rücken insbesondere kleine und mittelständische Unternehmen in den Fokus, weil diese dem Thema IT-Sicherheit immer noch nicht die notwendige Aufmerksamkeit widmen. Sie sind häufig das schwächste Glied in der Kette und bieten Angreifern das Einfallstor, um auch größere Organisationen zu infiltrieren.



G DATA CyberDefense AG Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299