

G DATA Bedrohungsreport: Angreifer nutzen Schwachstellen in öffentlich verfügbaren Diensten aus

Zahl abgewehrter Angriffe geht saisonal wegen Ferienzeit zurück

Bochum (Deutschland), 23. November 2021

Die Zahl der der abgewehrten Angriffsversuche ist im dritten Quartal 2021 weiter gesunken. Das zeigt der aktuelle Bedrohungsreport von G DATA CyberDefense. Ein Grund dafür: Die vermehrte Rückkehr von Angestellten ins Büro. Gleichzeitig nutzen Angreifer zurzeit verstärkt Schwachstellen in öffentlich verfügbaren Diensten aus, um Netzwerke zu kompromittieren.

Die Zahl der abgewehrten Cyberangriffe liegt im dritten Quartal 2021 wieder auf dem Niveau vor Beginn der Corona-Pandemie. Im Vergleich zum zweiten Quartal sank die Zahl um 28,7 Prozent. Die Gründe für den Rückgang: Traditionell ist in den Sommermonaten die Zahl der Angriffsversuche saisonal geringer als zu anderen Zeiten. Zudem trägt auch die Rückkehr von Mitarbeitenden in Unternehmen aus dem Homeoffice zur Normalität bei und führt zu sinkenden Zahlen. Gerade zu Beginn der Pandemie waren viele schlecht gesicherte Rechner im privaten Umfeld eine leichte Beute für Cyberkriminelle. Insgesamt sind die Zahlen im privaten Umfeld stärker zurückgegangen als bei Unternehmen. Innerhalb von drei Monaten sank die Zahl der abgewehrten Angriffssuche auf Consumer um mehr als 30 Prozent. Im Businessumfeld sank die Zahl um 22 Prozent.

G DATA CyberDefense AG
Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

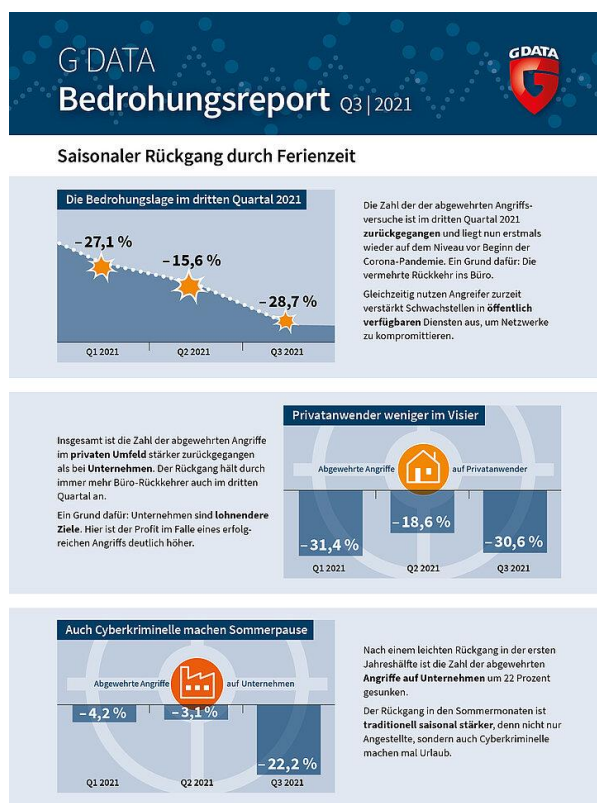
44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

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

Fax: +49 (0) 234 9762-299



„Wer angesichts der sinkenden Zahlen glaubt, dass das Risiko einer Cyberattacke gesunken ist, unterliegt einem Trugschluss. Aktuell verschaffen sich Angreifer vermehrt Zugang zu Unternehmen über ungesicherte Fernzugänge oder Schwachstellen in öffentlich verfügbaren Diensten, wie der Angriff der Hafnium-Gruppe über eine Schwachstelle in Exchange-Servern gezeigt hat. Um die IT-Sicherheit in Unternehmen zu verbessern, braucht es geschultes Personal sowie etablierte Prozesse. Hier müssen die Verantwortlichen schnell handeln. Sonst ist es nur noch eine Frage der Zeit, bis sie einem Angriff zum Opfer fallen“, sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense AG.

Coinminer: Gekommen, um zu bleiben

Die aktuellen Analysen zeigen für das dritte Quartal 2021 hohe Coinminer-Aktivitäten. Dabei nutzen Cyberkriminelle die Rechenleistung fremder Rechner, um insbesondere Monero zu generieren. Während kriminelle Eindringlinge damit Geld verdienen, müssen die Anwender die gestiegenen Stromkosten bezahlen und nutzen einen Rechner mit eingeschränkter Performance. Der finanzielle Schaden ist dann groß, wenn Kriminelle die Rechenkapazitäten von Unternehmen ausbeuten, indem sie Serverfarmer oder Cloud-Instanzen kompromittieren.

Malware: Alte Bekannte statt neuer Gefahren

Der aktuelle Bedrohungsreport zeigt: Angreifer setzen weiterhin auf etablierten Schadcode. Besonders aktiv waren sie damit zwischen Juni und August 2021 mit Malware - Glupteba, Agent Tesla und STOPRansomware –, die bereits seit mehreren Jahren aktiv ist. Diesen entwickeln die Cyberkriminellen stetig weiter und arbeiten zudem auch daran, den Schadcode vor Security-Lösungen zu verstecken. Dafür nutzen sie in der Regel sogenannte Packer, mit dem sie den schädlichen Kern unkenntlich machen. Mit automatisierten Tools schicken sie dabei fast im Sekundentakt neue Angriffswellen durch das Netz.

Rootkits: Totgesagte leben länger

Im Laufe dieses Jahres haben Cyberkriminelle wieder verstärkt Rootkits eingesetzt. Nach einigen Jahren erleben sie gerade eine Renaissance. Rootkits kommen zusätzlich zu Schadprogrammen wie Ransomware oder Droppern zu Einsatz und sorgen dafür, dass Malware oder Spionage-Programme möglichst lange unerkant auf dem System verbleiben oder kriminelle Gruppen aus der Ferne den Computer manipulieren können. Dabei haben sie weitreichende Rechte auf der Administrator-Ebene, sodass sie auf jede Funktion des Betriebssystems zugreifen können. Hinzu kommt: Rootkits können die meisten Spuren ihrer Existenz sehr gut verbergen.

„Angesichts der aktuellen Bedrohungslage benötigen Unternehmen zeitgemäße Schutztechnologien, um die trickreichen Angriffsversuche abzuwehren. Bei G Data nutzen wir unter anderem Machine-Learning-Technologien, um einen wirksamen proaktiven Schutz zu gewährleisten“, sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense AG.

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