

G DATA IT-Security-Trends 2021: Cyberattacken werden aggressiver, gezielter und intelligenter

Mit Malware-as-a-Service und Polyglotts führen Kriminelle komplexe Angriffe durch, die für Sicherheitslösungen nur schwer zu verteidigen sind

Bochum (Deutschland), 09. Dezember 2020

Cyberkriminelle arbeiten ebenfalls aus dem Homeoffice – jedenfalls nehmen die Angriffe nicht ab, sondern sogar zu. Unternehmen müssen sich auf immer raffiniertere Attacken einstellen. G DATA CyberDefense erklärt die IT-Security-Trends 2021.



„Die Corona-Krise hat uns deutlich vor Augen geführt, dass eine sichere IT-Infrastruktur so existenziell ist wie die Versorgung mit Strom oder Wasser. Leider nutzen auch Cyberkriminelle den aktuellen Digitalisierungsschub für sich aus und werden in Zukunft ihre Angriffsbemühungen verstärken. Dabei setzen sie auch auf automatisierte Attacken, um Netzwerke zu infiltrieren. Wer jetzt nicht in IT-Sicherheit investiert, der verspielt seine Digitalisierungsdividende leichtfertig“, sagt Andreas Lünig, Mitgründer und Vorstand von G DATA CyberDefense.

Komplexe Cyberangriffe mit Malware-as-a-Service und smarter Schadsoftware

Kriminelle Hacker suchen immer neue Tricks, um Netzwerke, PCs oder mobile Endgeräte zu kapern. Dabei setzen sie vermehrt Malware-Suiten ein, die verschiedene Arten von Schadsoftware wie etwa Keylogger, Information-Stealer und Ransomware miteinander kombinieren. Dafür müssen die Angreifer noch nicht einmal selbst die Software entwickeln, sondern bauen die Einzelteile lediglich zusammen. Die Bausteine erwerben sie dafür als Malware-as-a-Service in Untergrundforen. In diesem Vorgehen findet ein bestehender Trend seine logische Fortsetzung. Anwender, die Opfer einer solchen Attacke werden, verlieren auf einen Schlag ihre digitale Identität. Denn die Angreifer nutzen etwa die Logindaten weiter oder verkaufen sie selbst im Darknet. Und selbst wenn Opfer ein Lösegeld gezahlt haben, um die Veröffentlichung ihrer persönlichen Daten zu verhindern, ist dies kein Garant dafür, dass die Daten nicht trotzdem veröffentlicht werden.

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

Ein weiterer Trend: Cyberkriminelle kombinieren harmlose Dateien mit einer Malware, um Sicherheitslösungen auszuhebeln. Bei so genannten Polyglott-Angriffen verknüpfen die Angreifer beispielsweise eine ungefährliche exe-Datei mit einer böstigen jar-Datei. Gleichzeitig wird auch Malware smarter. Mit einfachen mathematischen Verfahren ermittelt die Schadsoftware den Finanzstatus des Opfers und passt die Lösegeldforderungen für verschlüsselte Daten individuell an. Als Indikatoren dienen etwa Bitcoin-Wallets oder die PC-Spielesammlung, die einen möglichen Aufschluss über die Finanzkraft des Opfers gibt.

Abzocke auf dem Smartphone

Auch Smartphones bleiben ein attraktives Ziel von Cyberkriminellen. Steigen wird die Gefahr durch sogenannte Fleeceware-Apps: Bei diesen Apps summieren sich nach kurzen kostenlosen Tests anschließende Monatsabonnements und In-App-Käufe auf Hunderte von Euros pro Jahr. Gerade diese In-App-Käufe sind dabei unerlässlich, um bestimmte App-Funktionen, optionale Erweiterungen oder Extras benutzen zu können. Besonders perfide: Durch aggressive Online-Werbung und gefälschte Fünf-Sterne-Bewertungen werden ahnungslose Nutzer überzeugt, die Apps zu installieren.

Im Bereich Mobile Security ist ein Umdenken erforderlich. Unternehmen werden im kommenden Jahr Angriffe auf die Smartphones der Mitarbeiter erleben, denn diese werden nicht mehr nur zur Kommunikation genutzt. Dank Homeoffice hat das Diensthandy eine größere Bedeutung gewonnen – über das reine Kommunikationsmittel hinaus: Als Teil der Sicherheitsarchitektur mit der Zwei-Faktor-Authentifizierung. Allerdings haben viele Firmen die Strategie noch nicht zu Ende gedacht. So müssen viele Verantwortliche noch klären, was passiert, wenn sich Mitarbeiter vom Zwei-Faktor-Verfahren ausperren, beispielsweise bei Diebstahl oder Verlust des Geräts. Grundsätzlich müssen sie neue Wege für das On- und Offboarding in Corona-Zeiten und darüber hinausfinden. Hier gilt es eine gute Mischung aus Sicherheit und Usability zu finden. Nur dann bringen moderne Sicherheitsverfahren für Firmen und Mitarbeiter einen Mehrwert.

Im Fadenkreuz der Angreifer: Mitarbeiter und mittelständische Firmen

Die Zahl der Angriffe auf kleine und mittelständische Unternehmen wird sich stark erhöhen. Diese glauben immer noch, dass ihre Netzwerke und Websites sicher sind, weil sie es nicht wert sind, gehackt zu werden. Das ist aber ein Irrglaube, denn kriminelle Hacker haben begriffen, dass diese Unternehmen ihnen auch die Möglichkeit bieten, schnelles Geld zu verdienen. Gerade kleine und mittelständische Unternehmen sollten sich intensiver mit dem Thema IT-Sicherheit befassen. Hinzu kommt: In immer stärker vernetzten Lieferketten bieten sie das Schlupfloch in der Cyberabwehr, um größere Firmen zu infiltrieren. Was vielen Unternehmen nicht bewusst ist: Angriffe finden heute zunehmend vollautomatisiert statt – etwa, wenn eine neue Schwachstelle veröffentlicht wird. Ein Unternehmen muss also gar nicht besonders ‘interessant’ sein, um am Ende infiziert zu werden. Dank der zunehmenden Arbeitsteilung krimineller Gruppen übernehmen einige die initiale Infektion und verkaufen den Zugang dann an andere Gruppen weiter. Diese spielt dann zum Beispiel eine Ransomware auf, um die Investition zu refinanzieren.

Phishing wird immer besser und reagiert in kurzen Zeiträumen auf aktuelle Ereignisse. Im kommenden Jahr ist damit zu rechnen, dass Nutzern statt potenzsteigernder Mittel oder Gesichtsmasken vermehrt Impfstoffe angeboten werden.

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

„Wir gehen davon aus, dass Kriminelle im kommenden Jahr versuchen werden, Nutzern den schnellen Zugang zu einer Corona-Impfung vorzugaukeln. Hier gilt es, nur auf die Informationen offizieller Stellen zu vertrauen und die angebotene Abkürzung kritisch zu hinterfragen“, sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense.

Phishing-Angriffe setzen zudem vermehrt auf bekannte Trust-Elemente, die den Nutzern Sicherheit vorgaukeln, wie etwa HTTPS-verschlüsselte Verbindungen zu Phishing-Seiten. Davon sollten Anwender sich aber nicht täuschen lassen. Denn ein grünes Schloss bedeutet nur, dass die Kommunikation mit der Webseite nicht abgehört werden kann – nicht, dass der Inhalt seriös ist.

Zum Durchschnaufen bleibt also auch im kommenden Jahr kaum Zeit. Doch mit einer Mischung aus der richtigen Sicherheitslösung und einer kritischen Aufmerksamkeit für IT-Sicherheitsfragen lassen sich viele IT-Sicherheitsprobleme auch in unsicheren Zeiten bewältigen.

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