

G DATA IT-Security-Trends 2020: Neue Angriffsmuster und unaufmerksame Mitarbeiter gefährden die IT

Living-off-the-land-Angriffe nutzen Windows-Bordmittel für Infektionen

Bochum (Deutschland), 10. Dezember 2019

Mittelständische Unternehmen geraten noch stärker als bisher ins Visier von Cyberkriminellen. Gerade in der Supply-Chain mit Konzernen sind sie häufig das schwächste Glied der Kette. Das werden die Angreifer 2020 noch stärker als bisher ausnutzen und gezielt angreifen – auch mit neuen Methoden wie etwa Living-off-the-Land-Attacken. Und die Zahl der schädlichen Apps für Smartphones und Tablets erreicht 2019 einen neuen Rekord – Tendenz für 2020: steigend. Welche Gefahren im Jahr 2020 Unternehmen und Privatpersonen bedrohen, verraten die Experten von G DATA CyberDefense.



„Nachdem Kriminelle bei neuer Malware seit Jahren vor allem auf Masse gesetzt haben, sehen wir aktuell immer komplexer werdende Angriffsmuster, die nur mit einer intelligenten Verhaltensanalyse abgewehrt werden können“, sagt Andreas Lünig, Mitgründer und Vorstand von G DATA CyberDefense. Denn bei sogenannten Living-off-the-Land-Angriffen werden Angriffe mit Standard-Apps durchgeführt, die auf jedem Windows-System vorinstalliert sind. Lünig mahnt aber, nicht nur die technischen Gefahren zu sehen. „Die Zukunft ist bereits jetzt schon digital. IT-Sicherheit wird zu einem wesentlicher Erfolgsfaktor werden. Unternehmen müssen lernen, das zu verstehen, und dürfen dabei nicht den Menschen vergessen, der sich Gefahren bewusst sein muss. IT-Sicherheit beginnt nicht beim Endpoint, sondern bei uns Menschen, egal ob Geschäftsführer oder Mitarbeiter.“

Neue Angriffsmuster

Ein Trend im kommenden Jahr sind nach Meinung der Security-Experten von G DATA CyberDefense daher komplexer werdende Angriffsmuster. Bei sogenannten „Living-off-the-land-Attacken“ kombinieren Cyberkriminelle Windows-Bordmittel wie Powershell und Bitlocker mit einem bösartigen Skript, um damit einen Angriff ausführen. Sie spionieren dann beispielsweise Passwörter aus oder verschlüsseln wichtige Daten, um Lösegeld zu erpressen.

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

Um derartige Angriffsmuster überhaupt zu erkennen, braucht es eine Verhaltensüberwachung, die auch komplexe Prozesse zuverlässig als schadhaft identifizieren kann.

Das Geschäftsmodell Cybercrime floriert und wird weiterentwickelt: In Zukunft setzen die kriminellen Kollektive verstärkt auf Arbeitsteilung und Professionalisierung. Heißt: Während eine Gruppe sich darauf spezialisiert, in Unternehmensnetzwerke einzudringen, konzentriert sich ein anderes Team darauf, Daten aus dem Netzwerk zu exfiltrieren oder zu verschlüsseln. Die einen verdienen Geld, indem sie die Zugänge verkaufen, die anderen mit Lösegeldforderungen.

Der Mittelstand im Fadenkreuz

Der Mittelstand rückt noch stärker in den Fokus der Cyberkriminellen. Denn es fällt Kriminellen leichter, in deren Netzwerk einzudringen, weil die IT-Sicherheit immer wieder Lücken aufweist. Dabei sind sie häufig nicht einmal das primäre Ziel, sondern als Teil der Lieferkette das schwächste Glied, um einen großen Konzern zu infiltrieren. Hier sind alle Branchen gefordert, eigene IT-Sicherheitsstandards zu etablieren. Weiterhin problematisch ist, dass viele Unternehmen auf unsichere Methoden zur Fernwartung setzen, insbesondere auf das Remote-Desktop-Protokoll (RDP).

Riesigen Nachholbedarf hat insbesondere der Gesundheitssektor bei der ambulanten Gesundheitsversorgung. Es fehlt im Bereich der Praxis-IT an grundlegenden Sicherheitsstandards. Bei der Digitalisierung dieses Bereiches muss deutlich mehr Geld in die Cybersecurity gesteckt werden, um die Compliance-Anforderungen zu erfüllen und hohe Strafzahlungen zu vermeiden.

Menschen verhindern Cyberattacken

Spammails werden in Zukunft immer hochwertiger wie etwa Dynamite-Phishing. Diese sind nur schwer als schadhaft zu erkennen. Daher gilt mehr denn je das Motto: Erst denken, dann klicken. Wer gedankenlos oder aus reiner Neugierde auf einen möglichen Millionengewinn klickt, gefährdet die IT-Sicherheit. Sicherheitsbewusstsein ist nach wie vor die am meisten unterschätzte Maßnahme, um die gesamte sicherheitsrelevanten Verteidigungslandschaft auf ein höheres Niveau zu bringen. Hier müssen Unternehmen in Schulungsmaßnahmen für ihre Mitarbeiter investieren.

Mobile Geräte

Immer mehr Menschen nutzen Smartphones und Tablets als digitales Cockpit für ihren Alltag, etwa um ihr smartes Zuhause von unterwegs zu steuern. Und auch die Zahlungsdirektive PSD2 sorgt dafür, dass das Mobilgerät zunehmend für Onlinebanking mit Zwei-Faktor-Authentifizierung eingesetzt wird. Somit sind sie ein attraktives Ziel für Kriminelle. Dazu setzen diese insbesondere Adware ein, um Nutzer auszuspionieren und Daten zu sammeln.

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

Einen bedenklichen Trend beobachten die G DATA Experten im Bereich von Smartphones: Den Einsatz von Stalkerware. Stalkerware bietet die Möglichkeit, mittels kommerziell erhältlicher Schadsoftware in das Privatleben einer Person einzudringen und wird als Werkzeug für Missbrauch in Fällen von häuslicher Gewalt und Stalking eingesetzt. IT-Sicherheitsdienstleister und Opferschutzorganisationen arbeiten seit 2019 gemeinsam daran, den Schutz zu verbessern – und werden im Jahr 2020 weitere Initiativen starten. So engagiert sich G DATA im Kampf gegen gefährliche Apps wie etwa Stalkerware. Als Gründungsmitglied der „Coalition against Stalkerware“ setzt sich der deutsche IT-Sicherheitsspezialist dafür ein, Nutzer besser über potenzielle Risiken aufzuklären und arbeitet gemeinsam mit Opferschutzorganisationen, um auch nicht-technische Probleme im Zusammenhang mit Stalkerware anzugehen.

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