Ein (kleiner) Schritt in die richtige Richtung: Office-Makros aus dem Internet werden standardmäßig blockiert

Microsoft will Änderung der Sicherheitseinstellungen in Office vornehmen, bei der Makrocode aus dem Internet nun standardmäßig abgeschaltet werden soll. Sophos nimmt diese Ankündigung unter die Lupe.

Endlich eine gute Nachricht: Microsoft kündigte eine Änderung der Sicherheitseinstellungen in Office an, bei der Makrocode aus dem Internet nun standardmäßig abgeschaltet werden soll.

Historisch gesehen ist dieser Schritt (längst) überfällig. Denn tatsächlich waren Makroviren schon ein Problem, bevor die Office-Anwendungen zu einer Suite von Tools mit einer gemeinsamen Makro-Codiersprache namens VBA (Visual Basic for Applications) zusammengeführt wurden. Doch was bedeutet dieser Schritt aus Redmond wirklich und was bringt es aus Sicht der Sicherheit für die Benutzer:innen?

Eine (über-)lange Historie
Bereits vor 1997 verfügte Microsoft Word beispielsweise über eine eigene Skriptsprache namens WordBasic (mit dem späteren VBA nicht kompatibel), die von Malware-Akteuren in großem Umfang für die Programmierung selbstladender Computerviren missbraucht wurde. Als dann später die standardisierte und leistungsfähigere Skriptsprache im Zusammenhang mit Office zum Einsatz kam, stürzten sich die Cyberkrimiinellen darauf wie der Teufel auf eine arme Seele.

Aus Sicht des Softwareanbieters waren die Skripte ein gut gemeinter Ansatz, denn wenn ein Office-Dokument ein eingebettetes Makro enthielt, dessen Name mit einer der Office-Menüoptionen übereinstimmte, wurde dieses Makro automatisch ausgelöst, sobald jemand auf den entsprechenden Menüpunkt klickte. Auf diese Weise konnten Unternehmen das Verhalten ihrer Office-Anwendungen leicht an ihre eigenen Arbeitsabläufe anpassen, was enorm praktisch war. Sicherheitstechnisch sind Makros aber ein nicht unerhebliches Problem. Etwa ereignisbasierte Makros, wie Auto_Open, wurden automatisch ausgelöst, sobald der Nutzer das Dokument nur j“ansah“. Ein Segen für einen Malware-Autor, der eine Dokumentendatei mit einer Falle versehen wollte. Denn um bei jedem Aufruf des Dokuments ein eingebettetes Virus auszulösen, waren keine speziellen Hacking- oder Programmierkenntnisse notwendig.
Ein zusätzlicher Teil des Problems bestand auch darin, dass die große Mehrheit der Benutzer:innen die VBA eigentlich gar nicht brauchten, sie aber dennoch gezwungen waren, es zu installieren und standardmäßig zu aktivieren.

Jahrelang hat die Cybersicherheitsbranche Microsoft gedrängt, die Standardeinstellungen von Office so zu ändern, dass bei der Installation die VBA-Funktionalität deaktiviert werden kann oder auf Wunsch sogar überhaupt nicht installiert wird. Die Antwort aus Redmond war immer „Nein“.

Steter Tropfen
Letzten Endes hat sich auch Microsoft dem Thema Cybersicherheit angenommen und kontinuierlich Änderungen am VBA-Ökosystem vorgenommen. Diese haben dazu beigetragen, die „freie Bahn“ der Virenschreiber in den späten 1990er Jahren einzudämmen.

Beispiele sind etwa die einfachere und schnellere Erkennung, ob es sich bei einer Datei um ein reines Dokument handelt, wodurch schnell zwischen Dokumentobjekten, die überhaupt keine Makros enthalten und Vorlagendateien mit Makrocode, unterschieden werden konnte. Allerdings hat dies die Makro-Malware im Allgemeinen nicht verhindert. So nützlich die Funktion auch ist, dass Makros erst dann ausgeführt werden, wenn sie zugelassen werden, die Cyberkriminellen haben gelernt, auch diese Hürde zu umgehen.
Eine weitere Variante der Eindämmung sollen Einstellungen in den Gruppenrichtlinien für strengere Makrokontrollen in Unternehmensnetzwerken darstellen. Damit können Administratoren beispielsweise Makros in Office-Dateien, die von außerhalb des Netzwerks stammen, vollständig blockieren. Damit können Benutzer:innen die Ausführung von Makros in Dateien, die sie per E-Mail erhalten oder aus dem Internet heruntergeladen haben, nicht per Mausklick aktivieren. Diese hilfreiche Einstellung ist jedoch derzeit standardmäßig deaktiviert.

Bestenfalls ein Teilsieg über VBA-Malware
Die jüngste Ankündigung ist auf den ersten Blick daher erfreulich. Allerdings bedeutet das standardmäßige Blockieren von Makros nur einen kleinen Sicherheitsschritt für Office-Benutzer, denn:

- VBA wird weiterhin in vollem Umfang unterstützt, und es ist weiterhin möglich, Dokumente per E-Mail oder im Browser zu speichern und sie dann lokal so zu öffnen, dass eingebettete Makros zulässig sind. Es ist also damit zu rechnen, dass Cyberkriminelle Wege finden, diese Hürde zu umgehen.
- diese Änderungen werden die älteren Office-Versionen erst in einigen Monaten, vielleicht sogar Jahren, erreichen. Selbst die aktuelle Version wird das standardmäßige Blockieren von Makros frühestens im Januar 2023 enthalten. Änderungsdaten für Office 2021 und früher wurden noch nicht einmal bekannt gegeben.
- Mobile und Mac-Benutzer werden diese Änderung überhaupt nicht erhalten.
- es sind nicht alle Office-Komponenten enthalten. Offenbar werden nur Access, Excel, PowerPoint, Visio und Word diese neue Einstellung erhalten. Obwohl diese Dateitypen den Großteil der Angriffe abdecken, wäre es besser, wenn diese Makro-Blockierfunktion für alle Microsoft-Produkte gelten würde.

Zum detaillierten Bericht über Makrocodes in Microsoft Office vom Sophos Security-Spezialisten Paul Ducklin geht es hier: https://nakedsecurity.sophos.com/2022/02/08/at-last-office-macros-from-the-internet-to-be-blocked-by-default/

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de