PUBLIREPORTAGE

Branchen Insider

Microsoft® Office-Dateien und ihre «heutigen Gefahren»

Kindern bläut man ein, nie zu fremden Leuten ins Auto zu steigen. PC-Benutzende kennen alle die Warnung vor falschen E-Mails und Links. Aber täglich öffnen noch immer viele von uns Mails und Dateien oder Links, die nur dazu dienen, Schaden anzurichten.

Es gibt grundsätzlich zwei Methoden, wie Kriminelle in ein IT-System eindringen können: durch Sicherheitslücken in der Software oder die Benutzer. Dabei wissen wir: Öffne keine dubiosen E-Mail-Anhänge mit Dateien oder unbekannten Absendern! Unerwünschte Codes oder ein Virus lassen sich über ganz geläufige und vertraute Dateien ausbreiten, zum Beispiel über ein Word-Dokument, geöffnet im Posteingang von Outlook. Es ist an uns, besonders kritisch mit E-Mail-Anhängen umzugehen. Office-Dateien mit enthaltenen Makros können Schaden anrichten – denn fast jeder von uns nutzt Microsoft Office- Dokumente, bei der Arbeit und privat. Zwei der bekanntesten und häufigsten Methoden, Office-Dokumente zu missbrauchen, schauen wir hier an.

Emotet

Emotet ist quasi ein Super-Trojaner. Er infiziert nicht nur den ersten Computer, sondern verbreitet sich selbstständig über weitere Systeme. Die Schwachstelle kann bei einer Word-Datei(.doc) oder einer Excel-Datei(.xls) liegen.

Makros – die bösen und die guten

Ein Makro ist per Definition eine Folge von Anweisungen und Befehlen, die automatisch oder manuell gestartet werden, eingebettet in Word-, Excel-, PowerPoint-Dateien. Makros sind nicht per se schlecht. Makros können nützliche Werkzeuge am PC-Arbeitsplatz sein. Makros sind aber auch die effizienteste Methode für den Missbrauch von Office-Dokumenten. Es gilt «gute» Makros in der Unternehmung zu kennen und entsprechend zu zertifizieren.

Der Gefahr ins Auge sehen

Office-Dokumente sind bereits seit über zehn Jahren eine häufig genutzte Angriffsplattform. Die Anzahl Attacken hat jedoch in den letzten drei Jahren nochmals zugenommen. Eine Erklärung dafür könnte lauten, dass Browser-Exploits (also Angriffe direkt während dem Surfen im Internet) schwieriger geworden sind. Browser-Entwickler haben viel Arbeit in die Sicherheit ihrer Produkte gesteckt. OfficeCare beschäftigt sich seit über 20 Jahren mit der Automatisierung von Prozessen sowie mit der Effizienzsteigerung beim Arbeiten mit Microsoft® Office. Dabei haben wir Lösungen entwickelt. Viele dieser Applikationen enthalten Makros. Sind sie gefährlich? Nein, im Gegenteil: Sie sind ungefährlicher als jede normal gespeicherte Word-Datei mit der Endung doc. Denn sie sind als Office-Add-Ins bekannt und mit einem Zertifikat signiert und abgesichert.

Sich vor Makro-Angriffen schützen

Programm-Updates regelmässig ausführen I Globale Einstellungen im Trust Center von Office, nur zertifizierte Makros erlauben I Technische Einstellungen in Firewall/Virenschutz/etc. I Dateiablage mit «Altlasten» aufräumen I Mitarbeitende sensibilisieren und schulen I Alte Office-Formate beim Speichern vermeiden.

OfficeCare AG
Claudia Lüscher, Geschäftsleitung
032 675 06 66 I **officecare.ch**

OFFICE CARE AG
OFFICE CARE AG
Work smarter not harder