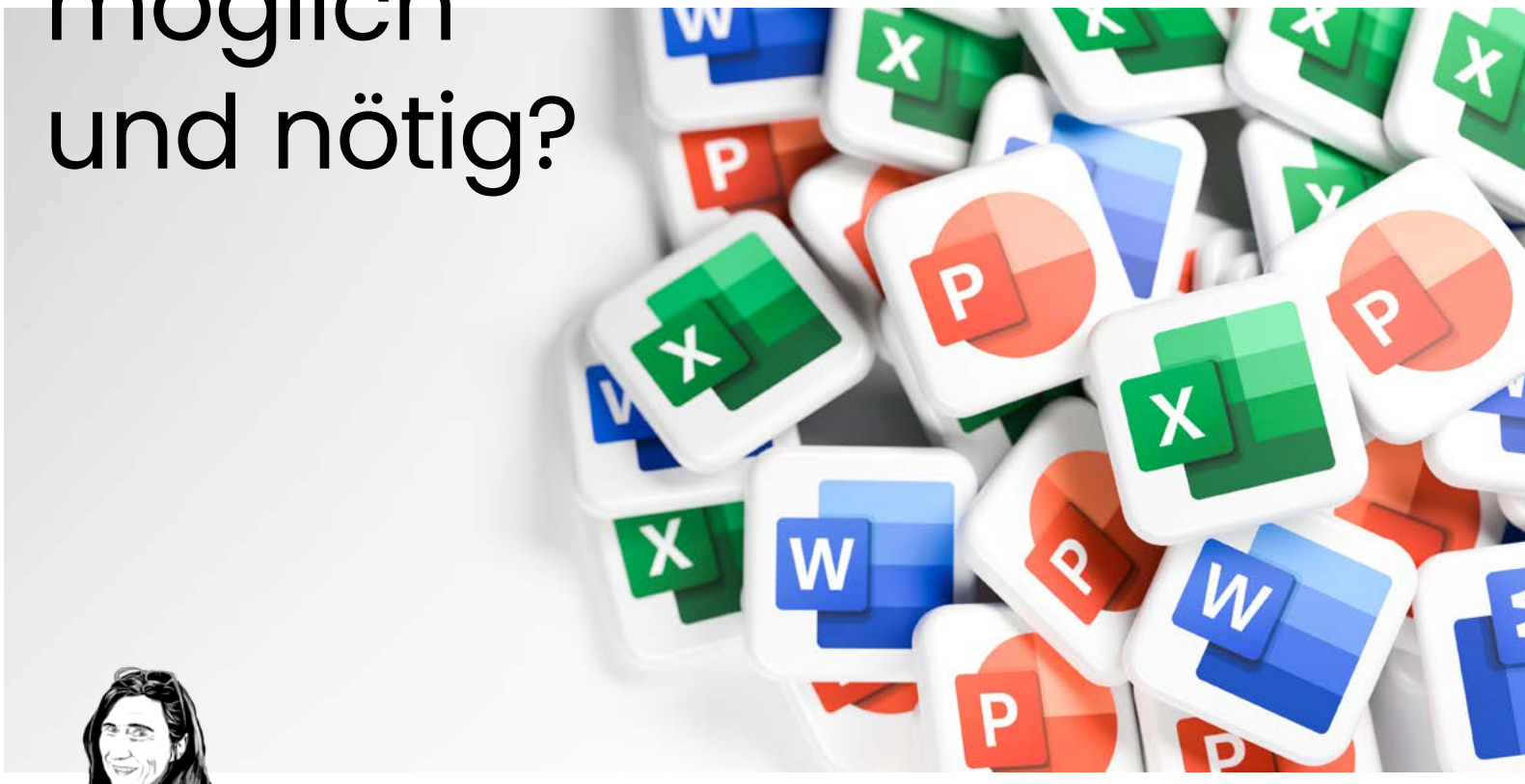
Risk-Management mit Office-Dateien – möglich und nötig?



Claudia Lüscher OfficeCare AG

Kindern bläut man ein, nie zu fremden Leuten ins Auto zu steigen. PC-Benutzende kennen alle die Warnungen vor falschen E-Mails und Links – so könnte man zumindest meinen. Aber täglich öffnen noch immer viele PC-Nutzerinnen und -Nutzer E-Mails und Dateien oder klicken auf Links, die nur dazu dienen, Schaden anzurichten. Sie öffnen damit Cyber-Kriminellen Tür und Tor. Die Folgen sind unterschiedlich: Im besten Fall passiert gar nichts. Im schlimmsten Fall führen Produktionsausfälle zu Schäden in Millionenhöhe. Nur: Wo ist jetzt die Verbindung zu Office-Dateien, zu einem harmlosen Word-Dokument oder einer Excel-Tabelle?

In den Medien lesen wir immer wieder von Phishing-Mails, Trojanern, Virenangriffen, Sicherheitslücken in PC-Systemen und regelrechten Cyberangriffen auf ganze Systeme. Es gibt grundsätzlich zwei Methoden, wie Kriminelle in ein IT-System eindringen können: durch Sicherheitslücken in der Software oder durch die Benutzer. Dabei wissen wir: Öffne keine dubiosen E-Mail-Anhänge mit ungewöhnlichen Dateiendungen oder unbekannten Absendern!

Ein unerwünschter Code oder eben ein Virus lässt sich über ganz geläufige und vertraute Dateien ausbreiten, z. B. über ein Word-Dokument, geöffnet im Posteingang von Outlook. Am Ende aller Schutzbemühungen (Firewall, Spam-Abwehr, Virenscanner, Sicherheitseinstellungen, Warnmeldungen) steht der Mensch, sozusagen die «Last Line of Defense». Es ist an uns, besonders kritisch mit E-Mail-Anhängen umzugehen. Fast jeder von uns nutzt Microsoft-Office-Dokumente, bei der Arbeit und privat. Auch Cyberkriminelle wissen, dass viele von uns so gut wie jedes Dokument öffnen, oft auch bei unbekannten Absendern. Drei der bekanntesten und häufigsten Methoden, Office-Dokumente zu missbrauchen, schauen wir hier an.

Emotet und wie man sich vor ihm schützt

Emotet ist quasi ein Super-Trojaner. Er infiziert nicht nur den ersten Computer, bei dem er ankommt, sondern verbreitet sich selbständig über weitere Systeme. Die Schwachstelle liegt oft bei einer Worddatei mit der Endung .doc. Dieses Format wurde mit der Einführung von Microsoft® Office 2010 abgelöst. Wir stellen immer wieder fest, dass viele PC-User ihre Word-Dokumente im alten Format abspeichern. Warum? Wohl hauptsächlich im Unwissen über die Gefahren von Makroviren und auch nach dem Prinzip «es ging ja immer so». Ein Klick auf das «Speichern»-Symbol ist schneller als zwei Klicks auf «Datei» und «Speichern unter» und die Auswahl des Formats .docx.

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 usw. Sie sind nicht per se schlecht oder gehören gar zur Gruppe Schadsoftware, im Gegenteil. Makros können nützliche Werkzeuge am PC-Arbeitsplatz sein. Makros sind aber auch die effizienteste Methode für den Missbrauch von Office-Dokumenten. Hat die Benutzerin Makros z.B. im Word aktiviert, können sie beim Öffnen eines Dokuments sofort gestartet und der Schadcode auf dem PC ausgeführt und/oder verbreitet werden. Setzt man die Makros hingegen auf «deaktiviert», erscheint ein Pop-up-Fenster mit verschiedenen Warnhinweisen. Ausserdem enthält die neue Endung von Office-Dateien ein «m» für «Makro» (.docm, xlsm, pptm).

«80 Prozent der Schweizer Unternehmen rechnen mit einem Cybervorfall in den nächsten 12 Monaten.

Besonders fürchten sie sich vor Ransomware und vor zielgerichteten Cyberattacken mit Lösegeldforderung.»

Microsoft® Formel-Editor

Mathematische Formeln lassen sich in Office-Dokumente mittels Microsoft® Formel-Editor, z.B. in ein Word-Dokument, einbetten. Seine Schwachstellen können von infizierten Word-Dateien zum Einschleusen von Viren genutzt werden. So geschehen in einem prominenten Fall in Deutschland, nachdem ein per E-Mail verschicktes infiziertes Word-Dokument geöffnet worden war.

Seien Sie kritisch!

Office-Dokumente sind bereits seit über zehn Jahren eine häufig genutzte Angriffsplattform. Die Anzahl dokumentbasierter Attacken hat jedoch in den letzten drei Jahren nochmals enorm zugenommen. Eine Erklärung dafür könnte lauten, dass Browser-Exploits (also Angriffe direkt während des Surfens im Internet) schwieriger geworden sind. Browser-Entwickler haben viel Arbeit in die Sicherheit ihrer Produkte gesteckt. Umso entscheidender ist es, dass Unternehmen und wir als Userinnen und User bei der täglichen Arbeit am PC sehr aufmerksam und kritisch sind! Denn die Auswirkungen solcher Cyber-Angriffe werden immer schlimmer.

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, die heute als Standardprodukte auf dem Markt sind. Viele dieser Applikationen enthalten Makros. Sind sie gefährlich? Nein, im Gegenteil: Sie sind ungefährlicher als jede normal gespeicherte Office-Datei. Denn sie sind als Office-AddIn bekannt und mit einem Zertifikat abgesichert.

Risk-Management mit Office-Dateien: möglich und nötig?

Unsere Erfahrung sagt ganz klar Ja! Die Vergangenheit hat gezeigt, dass es viele Unternehmen, auch in der Schweiz, eiskalt erwischt hat und der Schaden zum Teil immens ist. Für den optimalen Schutz ist die Kombination von technischen und organisatorischen Massnahmen entscheidend. Aktuell ist leider der Trend festzustellen, dass der Schwarze Peter vermehrt den Benutzern zugeschoben wird. Beim Umgang mit Makros fehlt es diesen aber oft an Fachwissen. Gerne helfen wir weiter und geben Ihnen auf Anfrage Referenzkunden bekannt. Wir übernehmen die Projektleitungen und/oder die konkreten Ausführungen, das Abarbeiten der unterschiedlichen Prozesse bis hin zur Analyse von Makros sowie die Schulung und verständliche Information für Ihre Mitarbeitenden.

Begrifflichkeiten

Emotet
Emotet ist eine Familie von Computer-Schadprogrammen für Windows-Systeme in Form von Makroviren, die per E-Mail versendet werden. Öffnet ein Empfänger die Anlage bzw. den Anhang einer solchen E-Mail, werden Module mit Schadfunktionen nachgeladen und ausgeführt. Seit Ende 2018 ist Emotet auch in der Lage, Inhalte aus E-Mails auszulesen. Die betroffenen Empfänger erhalten nun E-Mails mit authentisch aussehenden Inhalten von Absendern, mit denen sie zuvor in Kontakt standen. Auch sensibilisierte Nutzer werden zum Öffnen des schädlichen Dateianhangs oder eines Links verleitet. Seit Ende Januar 2022 beobachten Sicherheitsforscher wieder eine starke Zunahme von Spam-Mails aus dem Emotet-Botnetz.
Quelle: Wikipedia 2022

Makros
Makros werden direkt in der Microsoft® Office-Datei gespeichert und sind auf den ersten Blick beim Öffnen nicht sichtbar. Clever aufgebaute Makros können dem Benutzer das Arbeiten am PC massiv erleichtern. Sie fassen gewisse Arbeitsschritte zusammen oder führen z.B. per Knopfdruck aufwendige Reportaufbereitung aus.
Quelle: Wikipedia 2022

Nationales Zentrum für Cybersicherheit (NCSC) der Schweiz
Das Kompetenzzentrum des Bundes für Cybersicherheit ist erste Anlaufstelle für Wirtschaft, Behörden und Bevölkerung bei Cyberfragen. Seit rund einem Jahr nimmt es freiwillige Meldungen über Cybervorfälle entgegen, analysiert diese und gibt den Meldenden Hilfestellungen für das weitere Vorgehen. Von der Öffentlichkeit meist unbemerkt werden Schweizer Unternehmen gehackt, erpresst und die «erbeuteten» Daten im Darknet gehandelt.
Quelle: www.ncsc.ch

Tipp

Wie kann ich mich gegen Makro-Angriffe schützen?

1. **Programm-Updates regelmässig ausführen**
   Aktivieren der automatischen Update-Funktion.

2. **Einstellungen im Trust Center von Office**
   Bei Einstellungen «Nur zertifizierte Makros zulassen» wählen; oder Makros dürfen nur aus vertrauenswürdigen Quellen geöffnet werden.

3. **Technische Einstellungen in Firewall, Virenschutz usw.**
   Diverse Optionen sind im Hintergrund möglich, sodass Office-Dateien mit Makros kaum noch ausgeführt werden können. Diese Einstellungen werden in den Systemrichtlinien und Policies der Unternehmung festgelegt.

4. **Mitarbeiter sensibilisieren und schulen**
   Regelmässige Schulungen und Informationen zum Thema Sicherheit mit Office-Dateien und E-Mail-Anhängen.

5. **Alte Office-Formate beim Speichern vermeiden**
   Das Dateiformat lässt Dateien mit und ohne Makro zu.

Dateiendung	Beschreibung
doc / xls / ppt	können Makros enthalten
docx / xslx / pptx	x – beinhaltet keine Makros
docm / xlsm / pptm	m – können Makros enthalten (in der Regel, da die Endung M dafür steht)
xlsb	b – können Makros enthalten (enthält ausführbar Binärdateien)

6. **Sichere Zukunft mit Makro-Dateien: Signieren, zertifizieren**
   Zertifikat installieren und effektive Makro-Dateien für Word, Excel, PowerPoint usw. von einer vertrauenswürdigen Stelle in der Unternehmung zertifizieren lassen. Doppelter Praxisnutzen: Makro ist sicher, Makro ist bekannt.
   Praxistipp: Wer AddIns in Microsoft Office entwickelt und verkauft, verfügt heute in aller Regel über ein solches Zertifikat oder hat die Möglichkeit, das Unternehmenszertifikat des Kunden zu nutzen.

7. **Altlasten von Makro-Dateien auf den File-Ablagen entfernen**
   OfficeCare hat ein Script entwickelt, das File-Ablagen scannt und potenziell gefährliche alte Dateien sowie Makro-Dateien für eine spätere Bearbeitung listet und automatisiert abarbeitet. Dies kann ein Löschprozess aller alten Dateien (älter 20 Jahre «no use») oder die Umwandlung zu makrofreien PDF-Dateien sein.