klopfer
datennetzwerk gmbh

Makro-Sicherheit im Unternehmen

Wie viele Bäume hat der Wald?

klopfer datennetzwerk gmbh
Dr. René Devantier
rd@klopfer.com
Oktober 2019

Worum handelt es sich bei einem Makro?

Ein Makro ist eine Stück Programmcode, das in einem MS-Office Dokument eingebettet ist. Makros erledigen viele nützliche Dinge im täglichen Arbeitsablauf. Die Programmierung erfolgt in VBA (Visual Basic for Application) und ist Dank der Verfügbarkeit von MS Office an nahezu jeden Arbeitsplatz gegeben. Daher erfreuen sich Makros großer Beliebtheit.

Dies ist auch Erstellern von Schadcode bekannt, die Makros zur Verbreitung nutzen und Unternehmen seit Jahrzehnten zum Handeln zwingen.
Stellvertretend seien an dieser Stelle aktuelle Emotet-Ereignisse[1] genannt:

- 02.10.2019: Mutmaßlicher Emotet-Befall: Trojaner wütet in Berliner Kammergericht[2]
- 10.09.2019: Neue Emotet-Welle legt Neustädter Stadtverwaltung lahm[3]
- 13.05.2019: Trojaner-Befall: Emotet bei Heise[4]

Auf der einen Seite sind Makros sehr nützlich, auf der anderen Seite aber potenziell hoch gefährlich. Der einfache Ansatz, Makros komplett zu verbieten, ist nur selten eine Option!

Warum findet der Virenscanner den Schadcode nicht?

Aufgrund der Vielzahl von Virensignaturen kann nicht jede Bedrohung zeitnah erkannt werden kann. Modernste Anti-Malware Techniken wie Sand Boxing, ASR (attack surface reduction), AMSI (Antimalware Scan Interface), … lassen sich wiederum umgehen und aushebeln. In der Kombination mit Massen-Emails (Dynamit-Phishing) oder auch gezielten Attacken (Spear-Phishing) steht nicht die Frage **ob, sondern nur wann etwas passiert.**

Was kann getan werden?

Bezüglich Office-Makros kann etwas *Entscheidendes* getan werden. Etwas, das möglicherweise zu lange übersehen wurde. Vielleicht darum, weil man es als zu aufwendig betrachtet hat, weil es zu komplex erschien und man sich daher nicht die Zeit genommen hat, mit dem Thema auseinanderzusetzen.

> *Haben wir den Wald vor lauter Bäumen nicht gesehen?*

Das Stichwort heißt: **Codesignatur.**
Das bedeutet, dass (verbunden mit einer Richtlinie) auf allen Rechnern nur noch von der IT zertifizierte Makros zugelassen werden.

Die Umsetzung des Verfahrens ist weder hochkomplex noch mit zusätzlichen Investitionen verbunden. Wenn man auf Makrofunktionalitäten im Unternehmen nicht verzichten kann, besteht aus unserer Sicht kaum eine Alternative als entsprechende Richtlinien umzusetzen.

Sie haben Fragen, wie dies technisch / organisatorisch erfolgen kann?
Auf der nächsten Seite haben wir für Sie eine kleine **FAQ** bereitgestellt.

Sollten noch Fragen offen sein, sprechen Sie uns einfach an!

FAQ – Was bedeutet Makrosignatur für mein Unternehmen?

Ich benötige eine mehrstufige PKI (public key infrastructure)?

Nein! Für die Codesignatur ist dies keinesfalls erforderlich.
Wenn eine PKI bereits vorhanden ist, kann sie natürlich benutzt werden. Sie ist aber keine notwendige Voraussetzung.

Ich benötige also ein kostenpflichtiges externes Zertifikat einer anerkannten CA?

Nein! Für die Codesignatur reicht prinzipiell ein **kostenloses** selbstsigniertes Zertifikat.

Also bedarf es eines beträchtlichen Knowhows zu Fragen rund um X509-Zertifikate, Authenticode, Zeitstempel, Schlüssellänge, Crypto-Serviceprovider, Hash-Algorithmen etc.?

Nein! Diese Fragen müssen nicht erschöpfend beantwortet werden. Folgen wir einfach den best-practice Empfehlungen. Die Erstellung / Beschaffung eines geeigneten Zertifikates für Codesignatur kann in weniger als 5 Minuten erledigt werden. Hierbei unterstützen wir Sie.

Die Signierung von Makros ist sehr aufwendig. Muss nicht jedes Makro einzeln mit einem Zertifikat versehen werden, was eine Vielzahl von Zertifikaten nach sich zieht?

Nein! Die Signierung von Makros kann im Batch erfolgen. Wir empfehlen eine zentrale Stelle in der IT. Ebenso empfehlen wir die Verwendung *eines* einheitlichen Zertifikates. Dies kann durch ein einziges Skript erfolgen. Prinzipiell ist es egal, ob es sich um ein Makro, hundert oder gar tausende Makros handelt.
Unvermeidlicher Aufwand entsteht eher in der Organisation des Prozesses: Einsammeln aller im Unternehmen befindlichen Makros und Wiederverteilung nach der Signierung.

Kann man die Richtlinien zur Ausführung signierter Makros per GPO umsetzen?

Ja. Die Richtlinienumsetzung erfolgt mittels GPO (group policy objects).

Das ist ja sehr einfach?!

Ja und Nein. Die Erstellung der GPO und das Verteilen ist in der Tat sehr einfach und unterscheidet sich kaum von anderen Richtlinien. Was aber nicht so einfach ist, ist die Bestimmung der korrekten Einstellungen innerhalb der GPO. Denn Fragen zu vertrauenswürdigen Ordnern, Dokumenten und Zonen etc. sollten dabei berücksichtigt werden. Hier existieren Abhängigkeiten, die bis hin zu SMB-Dateifreigaben reichen und im Vorfeld geplant werden sollten.

Ist die Makrosignatur auch in Ihrem eigenen Unternehmen aktiv?

Ja. Makrosignatur und Richtlinien sind bei der Firma klopfer datennetzwerk gmbh seit Juli 2019 aktiv. Wir konnten keine Probleme in unseren Geschäftsabläufen feststellen.

Gibt es offizielle Empfehlungen, das Verfahren umzusetzen?

Ja. Das BSI hat z.B. entsprechende Empfehlungen [5] am 19.06.2019 veröffentlicht.
Auch von Microsoft existiert eine entsprechende Handlungsrichtlinie[6]

Wie viele Bäume hat der Wald?

Einen. Die überraschende Antwort auf diese Frage findet sich hier: Pando-Baum[7] . Es lassen sich zwar viele einzelne Stämme zählen, dennoch handelt es sich um einen Organismus. Manchmal sind ganz nahe liegende Dinge nicht unbedingt auf den ersten Blick ersichtlich.

Quellen:

[1] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Emotet-Warnung_230919.html
[2] https://www.heise.de/newsticker/meldung/Mutmasslicher-Emotet-Befall-Trojaner-wuetet-in-Berliner-Kammergericht-4544747.html
[3] https://www.heise.de/security/meldung/Ransomware-Neue-Emotet-Welle-legt-Neustaedter-Stadtverwaltung-lahm-4518819.html
[4] https://www.heise.de/ct/artikel/Trojaner-Befall-Emotet-bei-Heise-4437807.html
[5] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Empfehlungen_Microsoft_190619.html
[6] https://docs.microsoft.com/en-us/DeployOffice/security/plan-security-settings-for-vba-macros-in-office
[7] https://de.wikipedia.org/wiki/Pando_(Baum)