MacroMilter: Wie ein Admin zum Entwickler wurde

Das Jahr 2015 – eine E-Mail-Welle mit Malware-Office-Dokumenten im Anhang rollt über Deutschland. Die Dokumente enthalten Malware zu Infizierung der Clients mit Ransomware. Das große Problem hierbei ist, dass tausende dieser E-Mails tatsächlich erfolgreich in die Postfächer zugestellt und anschließend von den Clients geöffnet werden.

Das BSI reagiert daraufhin mit der Empfehlung, schnellstmöglich das Zustellen von Macro-Dokumenten an E-Mailservern zu unterbinden, da die aktuellen Virenscanner, bedingt durch die große Anzahl an unterschiedlichen Malware-Samples, diese nicht als Schadprogramme erkennen können. Problematisch umzusetzen wird diese Empfehlung jedoch wenn in einem Geschäftsprozess ein Macro-Dokument via Mail versendet werden muss. Aus dieser Problematik heraus entstand der MacroMilter. Die Idee dahinter ist, den Malware-Code dynamisch auf abnormale Merkmale hin zu untersuchen und so potentielle Malware zu erkennen.

Der Vortrag soll einen Einblick in die Idee einer alternativen Erkennung geben, speziell für den Fall, wenn eine generelle Deaktivierung von Macros in Dokumenten nicht möglich ist. Ebenso werden Themen wie die Analyse und Bestimmung von Malware angesprochen, die eine fundamentale Rolle in der Entwicklung des Milters spielen. Der MacroMilter ist in Python geschrieben und wurde insbesondere für die Postfix-Milter-Schnittstelle entwickelt. Durch seine einfache Installation ist sowohl ein nachträgliches Einbinden, als auch ein Parallelbetrieb mit herkömmlichen Anti-Viren-Filter in einer schon existierenden Postfix-Umgebung leicht umzusetzen. Die Live-Demo mit Messdaten einer produktiven Umgebung während des Vortrags wird das Vorgehen und die Wirkungsweise des Milters anschaulich machen.

Über die Funktionsweise und technische Umsetzung hinaus, wird im Vortrag auch die Entwicklung einer Idee eines Administrators und Nicht-Entwicklers bis hin zur Entstehung des ersten Open-Source-Projektes aufgezeigt; denn jeder fängt mal an. Ein wesentlicher, nicht außer Acht zu lassender Bestandteil, sind hierbei auch die anfänglichen Probleme und Hürden, die solch ein Projekt ohne Vorkenntnisse mit sich geführt hat.

Jeder der sich für diese Thematiken interessiert ist willkommen, egal ob mit oder ohne Postfix- oder Python-Kenntnisse. Im Anschluss an die Präsentation des Milters ist noch eine kleine Feedback-Runde geplant, wobei gerne auch Meinungen oder Ideen zum Thema ausgetauscht werden können.

Quellen und weitere Informationen:

- MacroMilter Projekt mit weiteren Infos: `https://github.com/sbidy/MacroMilter`
- Ransomware: Bedrohungslage, Prävention & Reaktion: `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf`
- OLEVBA Analyse: `https://www.decalage.info/`
- Postfix-Milter-Schnittelle: `http://www.postfix.org/MILTER_README.html`