Data Leak Prevention

Autoren: Morris Tichy, Lukas Freudensprung

Inhaltsverzeichnis

1. Theorie

Data Leak Prevention (DLP) ist eine Technologie, die den unautorisierten Transfer von sensiblen Daten verhindert. DLP-Systeme überwachen den Datenverkehr und blockieren oder alarmieren, wenn sie sensible Daten erkennen. DLP-Systeme können auf verschiedenen Ebenen des OSI-Modells arbeiten, um Daten zu schützen. DLP-Systeme können auf der Anwendungsschicht arbeiten, um Daten in E-Mails oder Webseiten zu schützen.

2. Konfiguration Block Exe Datein

2.1. DLP

```bash
config dlp filepattern
    edit 3
        set name "case3-exe"
        config entries
            edit "exe"
                set filter-type type
                set file-type exe
            next
        end
    next
end
```

```bash
config dlp profile
    edit "profile-case3-type-size"
        config rule
            edit 1
                set proto http-get
                set filter-by none
                set file-type 3
                set action block
            next
            edit 2
                set proto http-get
                set filter-by none
                set file-size 500
                set action log-only
```

```
15              next
16          end
17      next
18  end
```

2.2. Firewall Policy

```bash
config firewall policy
    edit 9
        set dlp-profile "profile-case3-type-size"
    next
end
```

3. Überprüfung

Um zu überprüfen, ob die DLP-Konfiguration korrekt ist, geben Sie den folgenden Befehl ein:

```bash
show full-configuration dlp profile
```

Damit wir die Konfiguration der .exe Datei überprüfen können, wird putty.exe installiert. Wie man auf dem Screenshot sehen kann wird dieser blockiert.

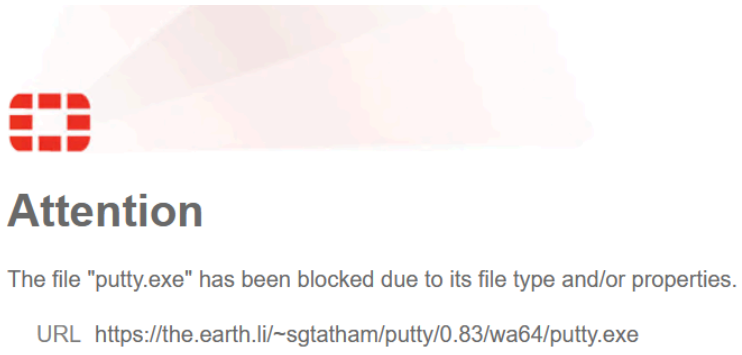

Abbildung 1: Blocked by FortiGate