

Angriffsszenarien auf etablierte Netzwerkprotokolle

EternalBlue und WannaCry

EternalBlue ist eine Schwachstelle in der Windows-Implementation des SMB-Protokolls, das zum *File-sharing* innerhalb eines Netzwerkes genutzt wird. Der SMB-Server läuft auf Windows mit Systemrechten, und ist daher ein gutes Ziel für Angreifer, die Zugriff auf einen Rechner erlangen wollen.

WannaCry ist ein sog. **Ransomware**, der ältere Versionen von u.a. Windows 7, 8.1, 10 und Vista angegriffen hat. Er nutzt die EternalBlue-Schwachstelle, um ein System zu infizieren. WannaCry wird als ein sog. *Ransomware* (dt. *Lösegeld-Wurm*) bezeichnet, da er ein System hybrid verschlüsselt und sich selbstständig weiterverbreitet.

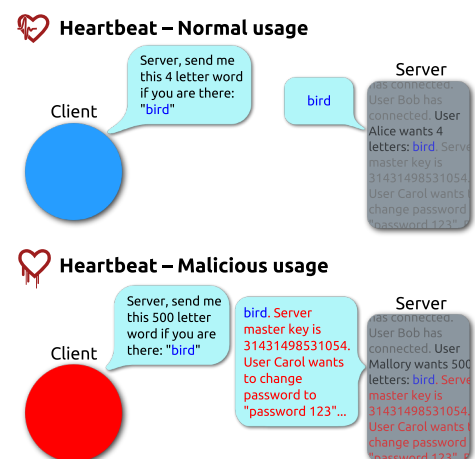
→ Das BSI, Verbraucherzentrum und Microsoft raten **gegen** die Zahlung!

OpenSSL und Heartbleed

OpenSSL ist eine sehr weit verbreitete Bibliothek für C/C++, die es erleichtern soll, in Programmen **SSL** bzw. **TLS** zu nutzen, was man für **HTTPS** benötigt. Unter anderem nutzen **Apache HTTPD** und **NGINX**, zwei der am weitesten verbreiteten Engines, wenn das HTTPS-Modul aktiv ist, OpenSSL standardmäßig.

Dem Server wird eine Zeichenkette (im Beispiel: "bird") und die dazugehörige Länge (im Beispiel: 4), die der Server zurücksenden soll bzw. zurücksendet.

Allerdings überschreibt die **angegebene Länge** die **eigentliche Länge** wenn sie nicht übereinstimmen (im Beispiel: "bird", eigentlich: 4, angegeben: 500)




Prävention

▼ Als End-Nutzer

- Installiere Apps nur aus vertrauenswürdigen Quellen
(z.B. aus vorinstallierten App-Stores)
- Halte deine Systeme immer möglichst auf dem neusten Stand
- Setze möglichst auf Open-Source-Software (= "OSS"/"FOSS")
aber: auch OSS kann gravierende Fehler haben!

▼ Als Entwickler

- Nutze **Kommentare** und **Dokumentiere** deinen Code
- Halte dich an die **Standards** der Programmiersprache
- Nutze Versions-kontrollsysteme (z.B. **Git**)
- Wenn dein Code Fehler hat nutze **Rubber Duck Debugging**

Die Präsentation, das Handout selbst, die Seminararbeit und Quellen findest du unter:  github.com/akb1154/seminararbeit

▼ System-rechte

Zugriffsrechte mit denen das System selbst arbeitet. In Windows sind System-rechte höher gestellt als Administrator-rechte.

→ Windows selbst kann `C:\Windows\System32` löschen, aber ein Administrator (bzw. normaler Nutzer) können dies Nicht.

Sie sind vergleichbar mit dem `root` - Nutzer auf *macOS* bzw. *Linux**