Verhindern von Malware-Ausbreitung in Datennetzen Quarantänisieren von Endgeräten

Jakob Döring, Lucas Schröder, Nils Trampel

In Datennetzen, in denen der Nutzer eigene Geräte mitbringen kann (BYOD), hat man als Admin nur beschränkte Möglichkeiten um die Sicherheit des Netzes und der Endgeräte sicherzustellen. Man kann keine Policies ausrollen, um regelmäßig Sicherheitsupdates einzuspielen; man weiß nichts darüber, ob die Nutzer Antivirussoftware - auch wenn der Gewinn derer nicht unumstritten ist - einsetzen, um mögliche Schädlinge zu beseitigen. Somit bleibt nur ein reaktiver sowie Blackbox-Ansatz: Isolation von Endgeräten mit ungewöhnlichem Verhalten, die möglicherweise Schadsoftware enthalten: Dies kann verhindern, dass zu einen benachbarte Geräte infiziert werden, und andererseits verdächtige Geräte nicht andersweitig genutzt werden, wie beispielsweise als Teil eines Botnetzes.

Ist die Isolation geschehen, muss zum einen der Nutzer über den Zustand seines Gerätes aufgeklärt und ebenso animiert werden, die nötigen Aufwände anzustrengen, um die Unschädlichkeit seines Gerätes zu beweisen, damit er die Isolation verlassen darf. Dafür ist vor allem die Bereitstellung von Antivirus-Software (inklusive aktueller Signaturen) sowie Updates für die Betriebssysteme von Nöten. Da eine komplette Netztrennung und Versorgung mit besagten Ressourcen nur über lokale Spiegel ohne Gerätemanagement extrem aufwändig und das Whitelisting von gewissen URLs über Verfahren wie transparente Proxies in Zeiten von *HTTPS/HSTS/CDNs* und co. nicht wirklich praktikabel ist, muss den Nutzern ein umfangreicher Netzzugriff gegeben werden. Um den Nutzer trotzdem zur Tätigkeit zu bewegen, wird im vorliegenden System nur für eine begrenzte Zeit Netzzugang zur Verfügung gestellt, nach dem dieser um Zeit beim Support bitten muss.

Im Vortrag wird ein im *Chemnitzer StudentenNetz (CSN)* eingesetztes System vorgestellt, welches aus einem speziell gefirewallten Netz besteht, in dem sich der Nutzer über ein Captive Portal für eine begrenzte Anzahl Versuche seinen Netzzugang temporär aktivieren darf. Für das Firewalling kommt hierbei die Eigenentwicklung *cpob*[1] zum Einsatz.

[1] https://github.com/camelusferus/cpob