Windows Hardening mit Microsoft Applocker

Studiengang: MAS | Vertiefung: MAS Information Technology

Im Jahr 2018 wurden mehr als die Hälfte der gemeldeten Cyber-Angriffe durch Malware-Infektionen verursacht. Ein paar unachtsame Klicks eines Benutzers reichen schon, um ganze Endgeräte zu kompromittieren und einem Angreifer Türen zu öffnen, der dann Daten verschlüsseln und dadurch unbrauchbar machen kann. Um die Benutzer und die Infrastruktur zukünftig besser schützen zu können, sind technische Massnahmen zur Applikationskontrolle unerlässlich.

Ausgangslage

Die Mobiliar betreibt eine moderne Client Infrastruktur mit mehreren Tausend Windows Clients und einer zentralen Softwareverteilung, über welche zahlreiche Softwarepakete verwaltet werden. Für sehr selten und dediziert genutzte Applikationen, wird teilweise auf den Paketierungsprozess verzichtet und die entsprechende Applikation nach einer internen Freigabe mit lokalen Administratorenrechte direkt auf dem betroffenen Client installiert. Administratorenrechte werden nur für einen sehr beschränkten Zeitraum sowie mit Begründung bewilligt. Durch dieses Vorgehen soll sichergestellt werden, dass keine ungewollten Applikationen auf den Clients installiert werden. Das Ausführen von Programmdateien sowie portablen Applikationen auf Wechseldatenträgern, ist jedoch auch ohne Administratorenrechte möglich. Diese Tatsache macht es möglich, dass ein Benutzer ihm untergeschobene Ransomware ausführen kann und alle Daten, auf denen er berechtigt ist, unabsichtlich verschlüsselt werden.

Vorgehen

In einer ersten Phase wurden die Grundlagen und die nötigen Hintergrundinformationen über die Bedrohungslage erarbeitet und ausgewertet. Durch einen weiteren Arbeitsschritt wurden die bisherigen Prozesse und technischen Massnahmen zur Applikationskontrolle untersucht und zusammengetragen. Daraufhin wurde in einer nächsten Phase ein Konzept erarbeitet, welches die Möglichkeiten und Grenzen der Einführung von Microsoft Applocker in die bestehende Infrastruktur der Mobiliar beschreibt und die nötigen Umsetzungsempfehlungen liefert. Das erstellte Konzept sowie die darin aufgezeigten Empfehlungen wurden anschliessend in einer dritten Phase in Form eines Proof of Concept überprüft und mit den gewonnenen Erkenntnissen ergänzt.

Resultat

Das zentrale Ergebnis der Arbeit ist ein Konzept zur Einführung von Microsoft Applocker in die bestehende Infrastruktur der Mobiliar. Es konnte ein sauberer Durchstich von der Erstellung der Gruppenrichtlinie bis hin zur Sammlung der Windows Events und der Auswertung von blockierten Applikationen erzielt und entsprechend dokumentiert werden. Wie erwartet wird der Audit Modus eine zentrale Rolle spielen, um in einer ersten Phase das Baselining zu ermöglichen. Durch die Aktivierung des Audit Modus werden keine Applikationen blockiert. Beim Start einer Applikation wird allerdings überprüft, ob die Applikation gemäss den aktuellen Applocker Regeln ausgeführt werden darf oder allenfalls blockiert werden müsste. Diese Information wird in einem Windows Event protokolliert. Die entsprechenden Windows Events werden im bestehenden Security Information and Event Management (SIEM) System gesammelt und ausgewertet. Der technische Aufbau wurde bereits im Proof of Concept aufgebaut und kann für die produktive Einführung direkt übernommen werden. Zusätzlich wurden die notwendigen Prozesse im Konzept beschrieben und die zu involvierenden Stellen aufgezeigt.

Schlussbetrachtung

Das erstellte Konzept konnte durch das durchgeführte Proof of Concept erfolgreich validiert werden. Die darin beschriebenen Vorgehensschritte sind sowohl aus technischer wie auch aus organisatorischer Sicht anwendbar und liefern eine solide Grundlage für die anstehende produktive Einführung. Nach Abschluss der Master Thesis wird die produktive Einführung vorbereitet. Geplant ist, dass in einer ersten Phase der Audit Modus bei einer grösseren Gruppe von Endgeräten aktiviert wird. Die daraus gewonnenen Events sollen dann für ein erstes Baselining genutzt werden.

Dominique Guyer