Schutz von Identitäten in Microsoft Infrastrukturen

Studiengang: MAS Information Technology

Der bisherige Ansatz der Abschottung und des kompletten Schutzes ist hinfällig und nicht mehr zeitgemäss. Der heute zielführende Grundgedanke muss sein, einen Angriff zu erwarten und die aktuelle Vorgehensweise der Gegner zu verstehen und aufdecken zu können. 63% der Angriffe beginnen mit der Kompromittierung eines Benutzerkontos und sind aufgrund schwacher Passwörter oft erfolgreich. Ein Umdenken bei der Verwendung von Identitäten muss daher unbedingt stattfinden.

Ausgangslage

Viele Firmen setzen für die zentrale Benutzerverwaltung, Authentifizierung und Autorisierung das Microsoft Active Directory ein. Es ermöglicht dem Benutzer ein Single Sign-on Erlebnis und die Anmeldung über die Protokolle Kerberos und NTLM. Die Benutzer können in Standarduser, Administratoren und Dienstkonten für Applikationen unterteilt werden. Der Schutz dieser Benutzer bestand bisher lediglich aus Massnahmen in der Netzwerksicherheit und auch die Überwachung war nur mangelhaft auf die Erkennung von Angriffen und Missbrauch ausgelegt.

Risikoanalyse

In der Studie wird die These geklärt, ob Identitäten einfach und nachhaltig geschützt werden können. Aufgrund der weitreichenden Privilegien sind Administratoren besonders lohnende Ziele für Credential Diebstahl. Es handelt sich dabei um eine Technik, bei der ein Angreifer die Anmeldeinformationen eines Benutzers von einem kompromittierten Computer erlangt und sich mit diesen Credentials authentifiziert und im Netzwerk bewegt. Ist ein Angreifer drinnen, kann er sich mit dieser Methode über das gesamte Netzwerk ausbreiten. Es wurden aber noch mehr Risiken dokumentiert, welche von organisatorischen Regelungen, Prozessen, technischen Schwachstellen und unzureichender Überwachung ausgehen.

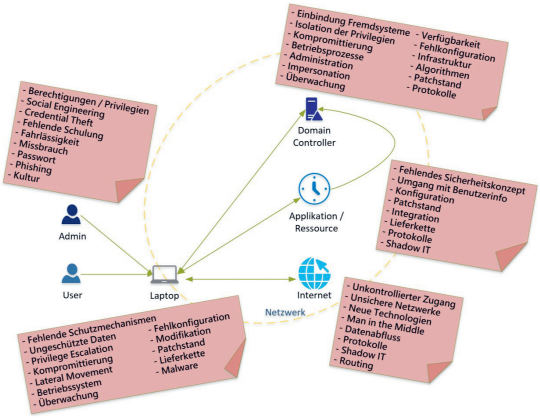
Massnahmen

Im Hinblick auf die Gefahren wird versucht die Ursachenszenarien, also weshalb eine Gefahr auftritt, zu mindern. Es geht dabei um den Schutz von Identitäten, Applikationen sowie Daten, Infrastruktur und Geräten. Dazu wurden rund 50 Massnahmen definiert, welche von der Isolation der Privilegien über Sensibilisierung der Betroffenen bis zu technischen Massnahmen reichen. Auch die neuen Möglichkeiten durch die Cloud haben sich als sehr erfolgsversprechend herausgestellt.

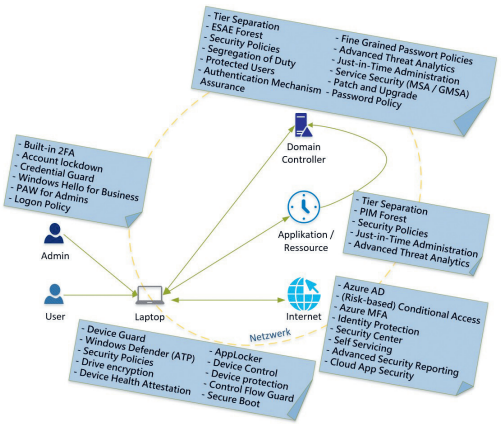
Fazit

Die Studie und der Proof of Concept beweisen die These, dass eine effiziente und nachhaltige Sicherheitsstrategie mit standardmässig integrierten und eigenständigen technischen Lösungen vom Hersteller Microsoft möglich ist. Als Voraussetzung für Cyber Security müssen sich jedoch alle bewusst sein, dass jeder ein Ziel ist und man sich nicht gegen alles verteidigen kann. Die Unternehmen unterscheiden sich nur darin, ob sie bereits kompromittiert sind oder eine Kompromittierung erst noch vor sich haben (assume breach). Die Thematik muss also von oberster Stelle aufgegriffen und vorangetrieben werden. Nur so kann etwas bewirkt werden.

Dominik Kessler



Übersicht der Risiken



Übersicht der Massnahmen