Bedrohungen und Massnahmen bei Microsoft Active Directory Systemen

Studiengang: MAS Cyber Security

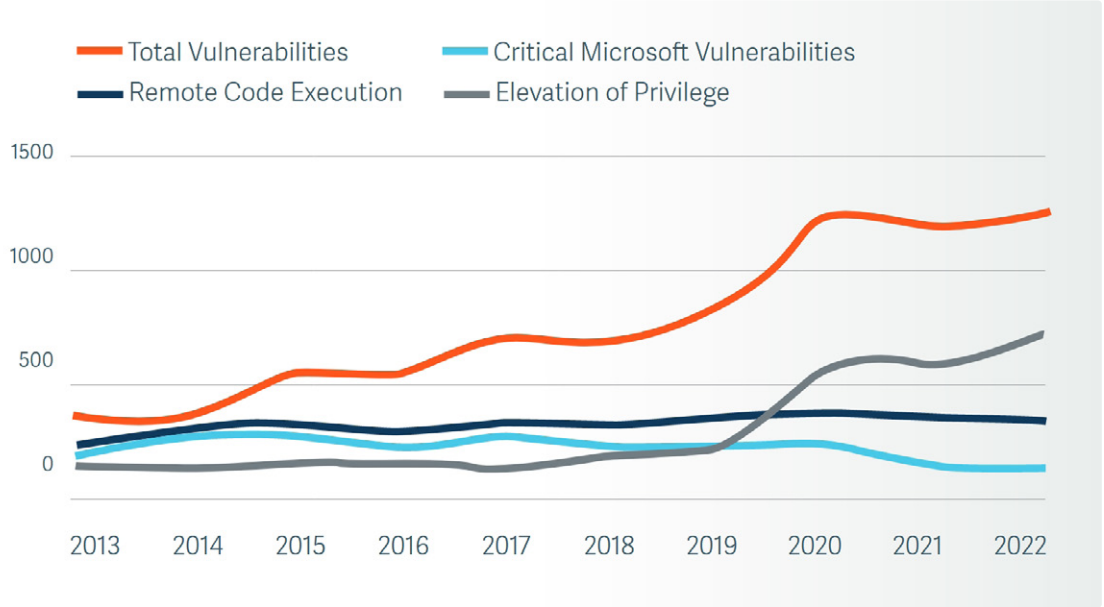
Jede IT-Infrastruktur benötigt einen Identity Provider, welcher die Identitäten bereitstellt, die Authentifizierung und Autorisierung durchführt. Weltweit wird dies vorwiegend mit dem Microsoft Active Directory Domain Service realisiert. Im Rahmen dieser Master-Thesis wird eruiert, mit welcher Technik und Vorgehensweise Angriffe erfolgen und mit welchen Massnahmen eine Mitigation erzielt wird.

Ausgangslage
Das Active Directory hat eine bedeutende Rolle in IT-Infrastrukturen und gerät gerade deswegen oft ins Visier von Angreifern. Ein kompromittiertes Active Directory verschafft weitreichende Zugriffe auf unternehmenskritische Daten. Die Gewährleistung der Informationssicherheit in solchen Systemen hängt oft von einer korrekten und sicheren Konfiguration ab. Fehlerhafte oder veraltete Konfigurationen können erheblichen Sicherheitslücken öffnen und somit verschiedene Bedrohungsvektoren schaffen. Besonders in den letzten Jahren haben die Angriffe auf die Elevation of Privilege, welche sich sowohl in horizontaler als auch in vertikaler Bewegung auswirkt, signifikant zugenommen.

Zielsetzung
Das Ziel dieser Arbeit besteht darin, verschiedene Angriffsstrategien darzulegen. Insbesondere ist der Fokus auf die Vorgehensweise und Technik eines Angriffs aufzuzeigen. Darüber hinaus hebt diese Arbeit nicht nur die Bedrohungen hervor, sondern zeigt mitigierende Massnahmen auf. Diese sollen dabei helfen Risiken, die mit solchen Angriffen einhergehen, zu minimieren und das Sicherheitsniveau zu erhöhen. Es sind Lösungsansätze für den Lesenden bereitzustellen.

Ausblick
Die Erkenntnis aus dieser Arbeit liefert nicht nur einen wertvollen Beitrag zur Bereinigung von Sicherheitslücken, sondern auch eine Awareness für weiterführende Sicherheitsanalysen. Sicherheit kann nicht durch einmaliges Handeln verbessert werden, sondern ist ein fortlaufender Prozess.

Marc Furtwängler



A Snapshot of Microsoft Across the Decade (2013 – 2022) @BeyondTrust