# *Handlungsempfehlung zur Microsoft Advisory ADV190023 - LDAP Security*

***Was wird seitens Microsoft geändert?***

Microsoft hat angekündigt, mit einem Patch im 2. Halbjahr 2020 die Signierung / Verschlüsselung von LDAP-Anfragen zu erzwingen. Dieser Patch wird ausgerollt, um mögliche Angriffe mittels Auslesen oder Umleiten dieser unverschlüsselten Daten zu verhindern. Eine Absicherung des Protokolls ist unbedingt notwendig, da über LDAP beispielsweise Benutzer-Kennwörter zurückgesetzt oder gar Domänen-Administratoren berechtigt werden.
Zusätzlich wurden bereits am 10.03.2020 Windows-Updates veröffentlicht, welche einer vereinfachten Überwachung der LDAP-Anfragen dienen.

***Welche Auswirkungen kann das auf Ihre Infrastruktur haben?***

Mit dieser Änderung würden alle nicht signierten und unverschlüsselten LDAP-Anfragen abgelehnt. Dies kann nicht nur ein Multifunktionsgerät sein, welches das Adressbuch per LDAP ausliest, sondern sehr häufig auch diverse unternehmenskritische Anwendungen (wie z.B. ERP-Systeme, Krankenhaus-Informationssysteme, VoIP-Telefonanlagen, Webproxies, etc.).

***Was sollte nun unternommen werden?***

Unsere Active Directory- sowie Security-Experten empfehlen zunächst eine detaillierte Analyse Ihrer Infrastruktur mit anschließender Erstellung eines Aktionsplans, um bereits im Voraus alle Systeme auf signierte / verschlüsselte LDAP-Anfragen umzustellen. Dies würde folgendermaßen ablaufen:

1. Prüfung der aktuellen LDAP-Konfiguration
2. Installation der Windows-Updates (März) auf den Domänen-Controllern
3. Aktivierung der Überwachung auf den Domänen-Controllern
4. Detaillierte Analyse der nicht-signierten / unverschlüsselten LDAP-Anfragen
5. Erstellung eines Aktionsplans zur Umstellung auf LDAP-Signing / -Encryption
6. Individuelle Besprechung und Umsetzung des Aktionsplans

Bitte kontaktieren Sie zur Umsetzung unseren Support per E-Mail (support@k-is.com) oder telefonisch (Deutschland: +49 271 31370-30 (Siegen) oder +49 6761 9321-55 (Simmern) | Schweiz: +41-55-536-1020) und vereinbaren einen zeitnahen Termin. Der Aufwand ist immer individuell abhängig von Ihrer Infrastruktur und den auflaufenden LDAP-Anfragen.

Verfasst von Robin Faust