



Verhindern von Windows Smartcard Logons für Administratoren und anderen Vertrauenspersonen

Smartcard Logon unter Microsoft Windows

Der zertifikatsbasierte Smartcard Logon unter Microsoft Windows erhöht die Sicherheit bez. Systemzugang, entlastet die Benutzer und den Helpdesk mit der Verwaltung von Passwörtern und bildet die Basis für Single Sign On.

Ist eine CA für Smartcard Logon im Active Directory konfiguriert, ist es nicht mehr möglich, bestimmten Benutzern oder Gruppen einen Logon mit einer Smartcard zu verbieten. Dies hat weitreichende Konsequenzen im Zusammenhang mit dem Sicherheitskonzept.

Risikofaktor CA Administrator - Identity theft

Bei einem Passwort basierten Logon hat der Benutzer das Geheimnis, nämlich das Passwort, in seinem Kopf gespeichert. Einem Angreifer ist es nicht möglich, ohne Social Engineering oder persönlichen Drohungen, das Passwort in Erfahrung zu bringen.

Anders verhält es sich unter Einsatz des zertifikatsbasierten Smartcard Logons. Ein CA Administrator hat immer die Möglichkeit, sich eine Smartcard eines bestimmten Benutzers auszugeben. Besonders problematisch ist dieser Sachverhalt, wenn der CA Administrator sich so höher privilegierte Rechte aneignet oder die Identität von Vertrauenspersonen (CxO, Personalwesen, Buchhaltung, etc.) annimmt.

Beim Ausstellungsprozess entgegnete man diesem Problem beispielsweise über die Sicherstellung

eines Vieraugenprinzips oder anderen organisatorischen Massnahmen. Diese sind jedoch aufwendig in der Umsetzung, unpraktisch und bieten keinen absoluten Schutz. Falls externe Zertifikate für den Smartcard Logon erlaubt werden, hat der Systemverantwortliche gar keinen Einfluss mehr auf den Ausgabeprozess der Zertifikate.

Zentraler Schutz durch Logon Shield

Mit dem Logon Shield von Keyon können gezielt Personen oder Gruppen vom Smartcard Logon ausgeschlossen werden. Die durch Logon Shield geschützten Benutzer können sich nur mit Username / Passwort am System anmelden. Einem CA Administrator ist es nicht mehr möglich, sich Identitäten so geschützter Benutzer anzueignen.

Logon Shield kann einfach installiert und konfiguriert werden und schützt so alle Systeme, die Zugang basierend auf dem Windows Smartcard Logon gewähren (inkl. Kerberos basierte Systemzugänge).

Logon Shield - Übersicht

- Zentrale Installation auf Windows Domain Controllern. Keine Installation auf Client Systemen.
- Einfache Konfiguration von Benutzern, Gruppen und erlaubten Zertifikatsklassen.
- Unterstützt Domain Hierarchien