LogOnWatch - die geschützte Microsoft-Anmeldung

Das Problem:

Jedes handelsübliche Anmeldeverfahren an Microsoft Betriebssysteme, das eine Tastatur-zur Eingabe benötigt und dafür keine Spezialhardware einsetzt, setzt auf Infrastrukturen des Betriebssystems wie Message bzw. Keyboard Queue, die für alle laufenden Anwendungen öffentlich zugänglich sind und ist daher sehr leicht mitgelesen werden können. Eine Sicherheit gegen Wiedereinspielen bieten diese nicht.
Der auf der BlackHat 2014 in LasVegas [1]von Karsten Nohl und Jakob Lell vorgestellte Angriff „BadUSB" ist einer von vielen Angriffsvektoren in diesem Zusammenhang. Keylogger in Hardware und Software stellen weitere Bedrohungen dar. Auch die über lange Jahre ungepatcht enthaltene Schwachstelle der Kerberos-Implementierung motivierten Großunternehmen mit erweitertem Sicherheitsbedarf über verfeinerte Anmeldeverfahren nachzudenken

1 K. Nohl, J. Lell: BadUSB - On Accessories that Turn Evil Bad, URL: http://www.blackhat.com/us-14/briefings.html#badusb-on-accessories-that-turn-evil (04.12.2014)

Die Lösung:

Zentrale Steuerung:

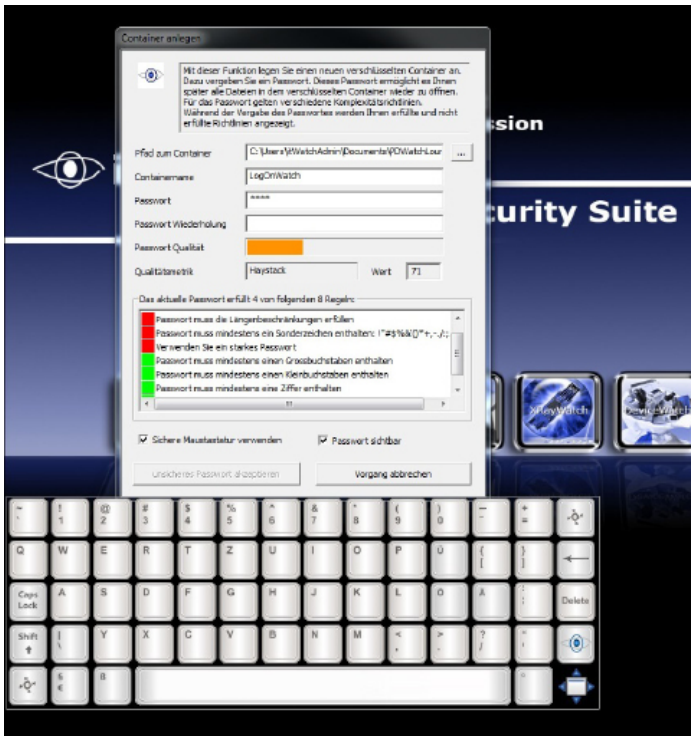
- wer sich auf welchem Rechner mit welchem Anmeldeverfahren anmelden darf / muss.

Zentral definierbare Passwortkomplexitätsregeln:

- farbig und grafisch für den Benutzer visualisiert, mit einem individuell steuerbaren Wörterbuch verbotener Passworte

Zentral definierbare Benutzer/Gruppenabhängige Wahl der Passworteingabe:

- Eine sichere von itWatch entwickelte Maustastatur, die gegen Wiedereinspielen und Abhören geschützt ist – auch die Aufzeichnung der Mausbewegung gibt keinen Hinweis auf das verwendete Passwort
- Der Einsatz einer bestimmten Tatstatur, z.B. mit verschlüsselten Transport der Tasteninformation



Zentraler Überblick:

- über alle im Unternehmen registrierten Anmeldeverfahren und deren Installations / Verwendungsort – inkl. Schutz bzw. Alerting beim Versuch neue Anmeldeverfahren einzuschleusen
- wer sich wo mit welchem Anmeldeverfahren und welchem Ergebnis angemeldet hat
- Einbindung von allen Fremdverfahren inkl. Chipkartenanmeldung

Automatische Nachforderung einer Anmeldung

- mit einem höherwertigen Anmeldeverfahren, wenn die verfügbaren Rechte bezogen auf das bestehende Anmeldeverfahren nicht ausreichen und prinzipiell aber mehr Rechte für diesen Account verfügbar wären
- höherwertige „Re-Anmeldung" kann auch nur auf einzelne Anwendungen bezogen werden, so dass beispielsweise nicht alle Anwendungen auf digitale Signaturen einer Smart-Card oder eines Soft-Zertifikates zugreifen können

Zusätzliche Bindung an Besitz und Wissen

- Mit einem Webinterface können berechtigte Administratoren bestimmte Peripheriegeräte inklusive deren Seriennummern personalisieren und so bereits bestehende Devices kostengünstig zu einer Anmeldung mit „Besitz und Wissen" heranziehen

FSLOW-190327