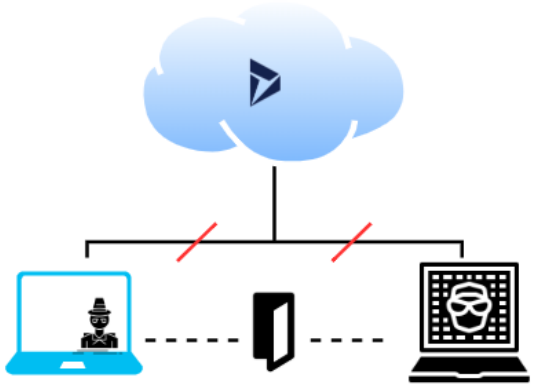
Technische Berufsschule Zürich TBZ

Höhere Fachschule
Sihlquai 101
8090 Zürich

Client Security

Diplomand: Ives Schneider
Klasse: ITSE17a
Schulexperte: Hanspeter Kramer
Firmenexperte: Simon Andres
Firma: Winterhalter + Fenner AG

Ives Schneider



bitwarden

Verteidigen, wo angegriffen wird

Entwendete Geräte und kompromittierte Administrationskonten können leicht verwendet werden, um in fortgeschrittenen Angriffen die Rechte weiter zu erhöhen. Durch sogenanntes «lateral movement» kann der Standpunkt weiter im Netzwerk gefestigt werden.

In der Arbeit - Client Security, wurden mehrere Massnahmen definiert und umgesetzt, um die Sicherheit auf den Endgeräten zu erhöhen.

Passwortmanagement in Container

Unternehmen befinden sich in einer prekären Situation ihren Mitarbeitern eine gute Passworthygiene beizubringen. Allzu oft werden Logins aufgeschrieben, geteilt und im Klartext abgespeichert. Teilweise fahrlässiger Umgang mit sensiblen Daten, hat so manchen Betrieb in schwierige Sachlagen gebracht.

Anhand bestimmten Geschäftsanforderungen wurden mehrere On-Premises Lösungen evaluiert. Bitwarden stellte sich als zutreffende Passwortmanagement Lösung, welche allen diesen Anforderungen gerecht wurde, heraus. Die Implementation geschah in einer Container-Umgebung, wobei ein Synchronisierungsdienst täglich die Zuteilung der Richtlinien direkt über das Bitwarden-Management übernimmt.

Technische Berufsschule Zürich TBZ

Höhere Fachschule
Sihlquai 101
8090 Zürich

Conditional Access bringt Schutz

Der Wechsel zum cloudbasierten ERP erfordert eine andere Sichtweise der IT-Sicherheit. Da die Buchhaltung bis hin zum Lagermanagement global erreichbar wird, besteht kein Zweifel, dass auch Drittpersonen dies nicht entgeht. Conditional Access, welche vertraute IP-Bereiche definiert, erhöht den Schutz vor unbekannten Endpunkten durch eine starke Multifaktor-Authentifizierung.

LAPS

„Local Administrator Passwort Solution“ soll Bewegungen innerhalb Netzwerke durch ein infiziertes System erschweren. Passwörter jedes eingebauten Administrators sind einzigartig und werden zentral verwaltet. Der automatisierte ständige Wechsel der Zugangsdaten schützt vor einfacheren Angriffen auf restliche Systeme.

Lock the Disks - Bitlocker

Entwendete Geräte können leicht mit einem externen Betriebssystem gestartet und sensible Daten extrahiert werden. Bei einer Bitlocker Implementation, welche TPM als abgesicherte Grundlage für die Aufbewahrung der Hashwerte für Entschlüsselungen nutzt, finden auch gestohlene Geräte keinen Nutzen für weitere Angriffe.

Windows Hello for Business

Ein immer höherer Sicherheitsstandard ruft nach alternativen Methoden, um eine Identität zu beweisen. Passwörter allein genügen nicht mehr diese zweifelsfrei verifizieren zu können. Sie sind schwer zu merken und können leicht von dritten für weitere Angriffe verwendet werden. Benutzer, Geräte sowie eine initiale Multifaktor-Authentifizierung stellt Identitätsaspekte priorisierter gegenüber Passwörtern hin. Biometrische Faktoren helfen dabei, auch die letzten Bedenken zu beseitigen.