Case Study

SCWP SCHINDHELM

BASE-IT FÜR SCWP - SAXINGER, CHALUPSKY & PARTNER RECHTSANWÄLTE GMBH (SCWP SCHINDHELM)

Implementierung E5 Security - Phase 2

DAS PROJEKT

AUSGANGSSITUATION

Saxinger, Chalupsky & Partner Rechtsanwälte GmbH ist bekannt für exzellente Beratung mit mehr als 230 Juristen an 27 Standorten weltweit.
In Österreich vertritt SCWP Schindhelm an den Standorten Linz, Graz, Wels und Wien mittelständische und große Unternehmen aus dem privaten und dem öffentlichen Sektor.

Immer neue Bedrohungsarten erfordern permanente Weiterentwicklung in der IT-Security. Nach erfolgreicher Implementierung der Security Phase 1 wollte SCWP Schindhelm ein weiteres Review um noch mehr Potenzial an Security-Themen auszuschöpfen und auch weiterhin bestmöglich abgesichert zu sein.

Weltweit sind 80 % der Angriffe auf gestohlene Passwörter zurückzuführen.
Deshalb beauftragten die IT-Experten von SCWP Schindhelm die Base-IT Consultants mit der Implementierung der Security Phase 2.

ZIELSETZUNG

In der Security Phase 2 sollten nun neue Features implementiert werden.
Auf die gesamte Anwaltskanzlei soll mithilfe unserer Base-IT Experten Self Service Password Reset, Conditional Access, Windows Hello for Business und Attack Surface Reduction Rules ausgerollt werden.

base it

professional.
fast.
secure.

SCWP SCHINDHELM

DIE UMSETZUNG

IMPLEMENTIERUNG

Durch den Einsatz von **Self-Service-Password-Reset (SSPR)** ist es möglich, dass die Passwörter von jedem User selbst, mittels alternativem Faktor zurückgesetzt werden können. Self-Service-Password-Reset beschleunigt die Problemlösung (Kennwort vergessen oder irrtümlich Zugang gesperrt) für die Mitarbeiterinnen und Mitarbeiter von SCWP Schindhelm und reduziert somit die eingehenden Tickets im Helpdesk.
Gemeinsam mit der Implementierung von **Windows Hello for Business** ist es möglich auch moderne Zwei-Faktor-Authentifizierungen mittels Face ID oder Touch ID zu verwenden.

Zusätzlich setzt die Anwaltskanzlei auf die Implementierung von **Conditional Access**. Dies gewährleistet, dass die Berechtigungen, welcher Client auf welche Daten zugreifen darf, auch von extern geregelt sind.

Um einen zusätzlichen Schutz der Zugänge sicher zu stellen, wurde **Windows Defender Credential Guard** installiert und erfolgreich eingerichtet.
Windows Defender Credential Guard schützt die Anmeldedaten direkt am Windwos 10 vor dem Auslesen. Damit können keine Pass-the-Hash-Angriffe mehr durchgeführt werden. Auch mögliche Social Engineering-Angreifer haben durch die von der Base-IT eingesetzte Technik beim SCWP-IT-Team keine Chance mehr.

Das implementierte **Azure Active Directory Identity Protection** Tool erkennt mittels Automatisierung, ob sich ein User an einem atypischen Ort anmeldet. Das bedeutet, dass ein User, der sich soeben in Linz angemeldet hat, sich nicht in den nächsten Stunden in Moskau anmelden kann.
Zusätzlich erkennt diese Anwendung, ob die Anmeldedaten (Credential) im Darknet zum Verkauf angeboten werden und fordert den User automatisiert auf, dass dieser sein Passwort ändert, bzw. eine Zwei-Faktor-Authentifizierung durchführt. Damit ist der Anmelde-Datensatz für den Angreifer unbrauchbar.

Aufgrund des weltweiten Anstiegs der Angriffe mittels Office Makro, PowerShell Skripte und in Adobe Reader Dateien versteckte Schadsoftware entschied sich die IT-Abteilung von SCWP Schindhelm, gemeinsam mit den Experten der Base-IT, zusätzlich die **Attack Surface Reduction Rules** zu implementieren.

Durch die Einrichtung und Definition dieser Angriffsregeln über **SCCM** bzw. **Microsoft Endpoint Manager** verhindern die IT-Experten, dass sich Dateien und Skripte automatisch ausführen und Schadsoftware heruntergeladen wird.
Das laufende Monitoring wird mittels **Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP)** durchgeführt, um schon proaktiv auf neue Sicherheitslücken und Bedrohungen vorbereitet zu sein.
Durch die im Hintergrund laufenden Analysen und Prozesse wird die Produktivität der Mitarbeiterinnen und Mitarbeiter von SCWP Schindhelm zu keiner Zeit beeinträchtigt oder gestört.

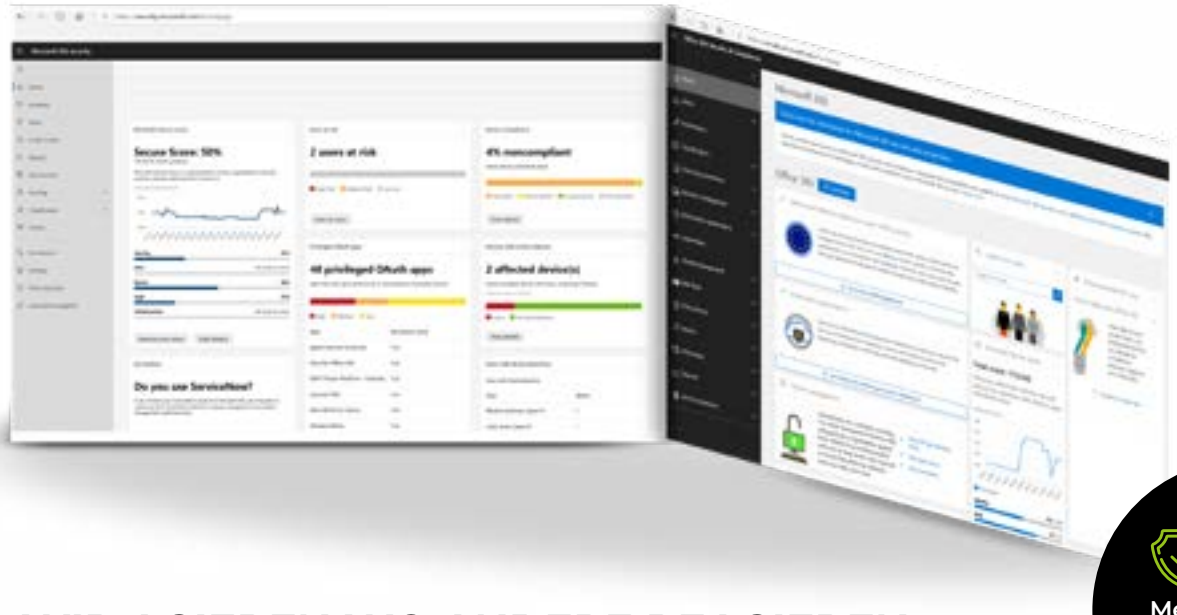
Bei IT-Sicherheit ist Zeit - Geld. Nutzen Sie unser Managed Service Security Angebot!

Diese von der Base-IT eingesetzte Technik ermöglicht nun einen noch sichereren Umgang mit den hochsensiblen Klienten-Daten. Damit diese Lösungen auch zu jeder Zeit reibungslos funktionieren, setzt SCWP Schindhelm auf das umfassende **Managed Service** Angebot der Base-IT. Somit ist das IT-System von SCWP Schindhelm weiterhin bestmöglich vor Attacken geschützt.

Case Study

SCWP SCHINDHELM

SECURE SCORE - VISUALISIERUNG DASHBOARD



Mehr zu unseren Angeboten zum Thema Security

WIR AGIEREN WO ANDERE REAGIEREN
IHRE IT-SICHERHEIT IST UNSER JOB

BASE-IT - ANSFELDEN & WIEN

FACTBOX

PROJEKTDAUER
2 Wochen

BASE-IT CONSULTANT
Spiesberger Robert

AUSGANGSSITUATION
mehr Potenzial, an Security-Themen auszuschöpfen

ZIELSETZUNG
neue Security-Features implementieren

base it

professional.
fast.
secure.