Case Study

BASE-IT FÜR SWIETELSKY AG

Base-IT Managed Service Security & Security Operations Center

DAS PROJEKT

AUSGANGSSITUATION

Die Swietelsky AG ist das drittgrößte Bauunternehmen Österreichs, verfügt über Niederlassungen in 19 Ländern und beschäftigt konzernweit rund 11.600 Mitarbeiter*innen (davon etwa 6.600 in Österreich).

Das Leistungsspektrum umfasst fünf Sparten (Hochbau, Tiefbau, Straßen- und Brückenbau, Bahnbau, Tunnelbau) und 16 Spezialkompetenzen. Im Wirtschaftsjahr 2020/21 hat SWIETELSKY eine Bauleistung von rund 3,1 Mrd. EUR erzielt.

Als einer der bedeutendsten Marktteilnehmer in der Baubranche verfügt das Unternehmen über eine große interne IT-Abteilung mit rund 70 Mitarbeiter*innen. IT-Infrastruktur, IT-Sicherheit und vieles mehr spielen eine entscheidende Rolle für den alltäglich störungsfreien Betrieb der tausenden Baustellen.

UNSERE ROLLE

Die IT-Sicherheit stellt in unserer heutigen Geschäftswelt eine zentrale Rolle dar. In einer modernen IT arbeiten Benutzer*innen mit zahlreichen digitalen Identitäten und einer großen Anzahl verschiedener Geräte (teilweise auch mit bring-your-own-devices). Des Weiteren arbeiten Benutzer*innen heutzutage sowohl im Büro als auch von unterwegs oder von zu Hause aus. Dabei greifen sie auch auf eine Vielzahl von Applikationen zu, die entweder lokal auf dem Rechenzentrum laufen, in einer Private oder Public Cloud sind, oder gar als Software-as-a-Service zur Verfügung gestellt werden. Wichtige und durchaus sensible Unternehmensinformationen werden nicht nur intern, sondern auch extern geteilt. Ziel dabei ist es immer, die eigenen Unternehmens-Ressourcen abzusichern und die komplexe Infrastruktur stets auf dem aktuellen Stand der Sicherheit zu halten.

base it

professional.
fast.
secure.

Case Study

DIE ZIELSETZUNG

Da wir seit vielen Jahren schon eine sehr intensive Partnerschaft mit SWIETELSKY pflegen und das Unternehmen bereits in vielen anderen IT-Projekten tatkräftigt unterstützt haben, hat uns SWIETELSKY beauftragt, ihre IT-Sicherheit mit Hilfe unseres **Managed Service Security & Security Operations Center** (nachfolgend „SOC“) aufzustocken.

Über 6500 User und rund 5000 Clients, weltweit im Einsatz, werden nun von uns verwaltet und vor möglichen Cyber-Angriffen geschützt. Außerdem unterstützen und erweitern wir SWIETELSKY´s eigenes SOC Team mit unserer 24x7 SOC Bereitschaft. Damit entlasten wir nicht nur wertvolle Ressourcen unseres Kunden, sondern ermöglichen damit auch einen störungsfreien und sicheren Betrieb, rund um die Uhr.

PROACTIVE OPERATIONS & SERVICING

Betreuung von Microsoft Security Lösungen auf Basis des gewählten Base-IT Managed Service Pakets, bei SWIETELSKY „Security Complete“

Reactive Alert Handling

Betreuung durch das Base-IT Security Operations Center

Forensic Analysis

Aufarbeitung von Incidents durch das Base-IT Security Experten*innen Team, um zukünftige Angriffe zu verhindern.

ZIELSETZUNG

SWIETELSKY hatte klare IT-Sicherheits-Anforderungen, denen wir mit einem ausgearbeiteten Sicherheitskonzept gerecht werden konnten. Die nachfolgenden Zielvorgaben haben wir in der Konzeptionierungsphase berücksichtigt und entsprechend umsetzt:

ONBOARDING VON MICROSOFT DEFENDER FOR ENDPOINT

Auch SWIETELSKY legt Wert auf schnelle Reaktionen bei Zwischenfällen, weshalb eine effiziente Weiterentwicklung von Endpoint Detection sowie der Response-Plattformen unumgänglich war. Microsoft Defender for Endpoint (nachfolgend „MDE“) stellt dabei als XDR Technologie (Extended Detection and Response) das dazu notwendige Tool dar. Mit Machine Learning, Big Data und Security Anomaly Detection genießt SWIETELSKY die Vorteile der Microsoft Cloud Lösung. SWIETELSKY hat mittels Microsoft Defender for Endpoint neben einer enormen Flexibilität auch ein Tool, welches nicht nur reaktiv handelt, sondern auch proaktiv. XDR Technologie analysiert Bedrohungen, priorisiert automatisch, und verfolgt/beseitigt diese, um SWIETELSKY vor Datenverlust oder anderen Sicherheitsbedrohungen zu schützen.

THREAT & VULNERABILITY MANAGEMENT

Eine der Anforderungen war es das Threat & Vulnerability Management auf Basis des MDE zu betreiben. Durch den daraus resultierenden wiederkehrenden Prozess ermöglicht SWIETELSKY einen störungsfreien Betrieb und eine IT-Sicherheit auf höchstem Niveau. Dabei evaluieren unsere Base-IT Experten regelmäßig vom MDE empfohlene Anpassungen, die dazu beitragen die Security Posture zu verbessern. Unsere Security-Experten prüfen vollumfänglich die Anwendbarkeit der empfohlenen Aktionen und stellen Chancen und Risiken gegenüber, um hier Potential zu identifizieren. Die Aktionen, die letztendlich einen Vorteil für unseren Kunden darstellen, werden in Abstimmung mit dem Cyber Security & Infrastructure Team von SWIETELSKY ausgerollt.

MICROSOFT SENTINEL ERWEITERUNG

Bereits im Frühjahr 2021 haben wir mit Microsoft Sentinel eine SIEM (Security Information & Event Management) und SOAR (Security Orchestration Automation Response) Lösung bei SWIETELSKY erfolgreich implementiert. Der Baukonzern legt allerdings großen Wert darauf, stets die aktuellste Technologie im Einsatz zu haben, weshalb wir den Auftrag erhalten haben, das Microsoft Sentinel entsprechend mit zusätzlichen Daten, Alarmierungen und Automatisierungen zu erweitern. Die Erweiterung erfolgt kontinuierlich und trägt wesentlich zur IT-Sicherheit bei.

DIE UMSETZUNG

UMSETZUNG

Die Umsetzung erfolgte mit dem Go-Live unseres Base-IT Managed Service Security & SOC Pakets. Das Proactive Operations & Servicing, das Reactive Alert Handling sowie die Forensic Analysis bedarf einer operativen Betriebsführung, die wir als Microsoft-Gold Partner und als Unternehmen mit mehr als 10 Jahren Erfahrung im Bereich IT-Security anbieten. Wir verstehen nämlich die IT-Security nicht als statisches Projekt, sondern als laufenden Prozess, welches ein operatives Servicing voraussetzt.

Jannis Langthaler [Consultant Modern Workplace & Security | Base-IT]

„Es ist eine Freude, die Swietelsky AG auf technisch höchstem Niveau zu begleiten und die Security Posture laufend zu verbessern. Außerdem finde ich es besonders spannend ein Unternehmen wie SWIETELSKY in diesen Umfang zu unterstützen und dadurch sehr vielfältige Erfahrungen zu sammeln. Überdies schätze ich die technische Kooperation und die intensive Zusammenarbeit mit SWIETELSKY´s IT-Personal! Die Partnerschaft mit SWIETELSKY ist in allen Aspekten eine sehr bereichernde Erfahrung."

SWIETELSKY hat sich nach umfassender Beratung für unser Security Complete Managed Service Security Paket entschieden und profitiert nun von einem vollumfassenden Leistungsspektrum. Dies umfasst unter anderem Azure AD Premium, Defender for Endpoint (Microsoft Defender for Endpoint), Defender for Identity (MDI), Defender for Office 365 (MDO), Azure Sentinel und vieles mehr.

 # 1 Step: Onboarding von Microsoft Defender for Endpoint

Nachdem sich SWIETELSKY für das Complete Paket entschieden hat, haben unsere Base-IT Experten das bestehende MDE Onboarding ausgebaut, damit auch alle weiteren Managed Service Security Dienstleistungen durchgeführt werden können. Somit sind sämtliche Clients und Server per XDR überwacht und geschützt!

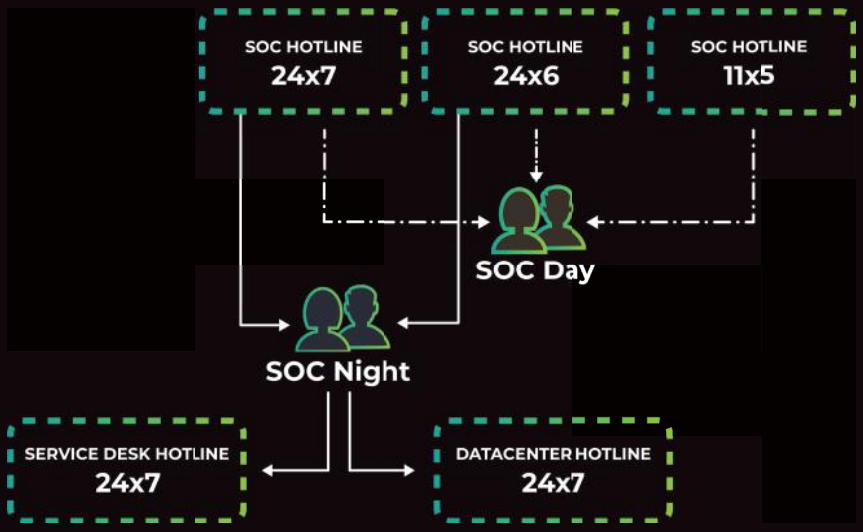
 # 2 Step: Managed Service Security & SOC

Mit dem laufenden Betrieb unseres Managed Service Security & SOC Pakets erfolgen ununterbrochen Implementierungen, die aus den Empfehlungen des Threat & Vulnerability Management resultieren. Außerdem erweitern unsere Base-IT Experten Microsoft Sentinel mit neuen Datenquellen und Automatisierungen von Workflows, damit die manuelle Abwicklung im Falle einer identifizierten Bedrohung durch automatisierte Funktionen des Systems übernommen wird. Microsoft stellt in diesem Bereich zahlreiche Templates zur Verfügung, doch unsere Base-IT Experten erstellen auch eigene Queries. Diese Queries entstehen reaktiv, wenn bestimmte Fälle eingetreten sind, sowie auch proaktiv, wenn bestimmte Threats vermutet werden und man diesen prophylaktisch entgegenwirken möchte.

DIE UMSETZUNG

base it
SECURITY COMPLETE & SOC

- Azure AD Premium P1
- Microsoft Defender AV
- Azure AD Premium 2
- Defender for Endpoint (MDE)
- Defender for Identity (MDI)
- Defender for Office 365 (MDO)
- Defender for Cloud Apps
- Defender for Cloud
- Azure Sentinel



Ein besonderer Aspekt dieses Projekts ist die Erweiterung des bestehenden SWIETELSKY SOC Team mit dem Base-IT SOC Team. Wie so viele Unternehmen, steht auch SWIETELSKY vor der Herausforderung entsprechend Ressourcen für das Thema IT-Sicherheit zu schaffen. Um diese Herausforderung zu meistern, hat SWIETELSKY sich dazu entschieden, das eigene SOC-Team mit unserem zu erweitern und profitiert dadurch von unserer IT-Security-Expertise. Damit werden Ressourcen freigespielt, Kosten gespart und um Reaktionszeiten außerhalb der normalen Bürozeiten (24x7) erweitert.

 # 3 Step: Weiterentwicklung von Defender for Office 365 (nachfolgend „MDO“)
Als Bestandteil des Managed Service Security Complete Pakets werden unsere Base-IT Experten auch demnächst den MDO weiterentwickeln und dieses Thema in die laufende Terminserie mit aufnehmen.

Gregor Dedl [Geschäftsführer | Base-IT]

„Der essentialste Part im Managed Service Security ist für uns die proaktive Betriebsführung der Security Lösungen und diese wissen wir nach jahrelanger Expertise zum Umsetzen und wir berücksichtigen dabei auch das reaktive Alert Handling sowie die forensische Analyse. Mit unserer Herangehensweise stärken wir die IT-Sicherheit von SWIETELSKY und sichern damit einen wesentlichen Wettbewerbsvorteil.“

FAZIT

IT-Sicherheit ist ein wesentlicher Bestandteil vieler erfolgreicher Geschäftsprozesse und Cyberkriminalität hat besonders während der Pandemie enorm zugenommen und stellt ein hohes Risiko für wirtschaftliche Abläufe dar. SWIETELSKY hat das erkannt und sieht die IT-Sicherheit weder als statisch noch als einmalig. Das Bauunternehmen hat sich für den sicheren Weg entschieden und uns, einen langjährigen und zuverlässigen IT-Partner, damit beauftragt, ihre IT-Sicherheit stets mit den aktuellsten Sicherheitsmaßnahmen zu erweitern und den laufenden Betrieb mit unserem Managed Service Security & SOC sicherzustellen.

Gemeinsam mit Matthias Klinski, Chief Information Security Officer bei SWIETELSKY, haben unsere Base-IT Experten Gregor Dedl, Christoph Moser, Christoph Reithmayr und Jannis Langthaler ein perfektes Zusammenspiel zwischen SWIETELSKY´s IT-Experten und unseren IT-Experten geschaffen und damit ein innovatives Managed Service Security & SOC Projekt umgesetzt.

Wir blicken auf eine überaus erfolgreiche Partnerschaft mit SWIETELSKY zurück, bedanken uns für die hervorragende und professionelle Zusammenarbeit und freuen uns weiterhin auf eine intensive Partnerschaft und viele spannende Projekte.

Matthias Klinski [Chief Information Security Officer | SWIETELSKY]

„Bei der Auswahl des Managed Security Operation Center Services waren für uns zwei Dinge entscheidend: State-of-the-Art Technologien und Transparenz im erbrachten Service. Der Managed Service Security der Base-IT vereint diese zwei Aspekte perfekt, indem die neuesten Microsoft Security Produkte gemeinsam durch uns Swietelskys sowie Experten der Base-IT betreut werden. Mit dieser Basis und dem daraus resultierenden kontinuierlichen voneinander lernen, sind wir bestens gewappnet um das „moving target" Cyber Security nachhaltig anzugehen."

FACTBOX

PROJEKTLAUFZEIT
Seit November 2021

BASE-IT CONSULTANT
Jannis Langthaler

ZIELSETZUNG
Onboarding des Base-IT Managed Service Security & Security Operations Center