Case Study Baden-Baden:

DTS Managed Detection & Response für die Stadt Baden-Baden

Als kommunale Behörde verantwortet die Stadtverwaltung Baden-Baden eine Vielzahl komplexer Aufgaben. Das Spektrum reicht weit über generelle Bürgerdienste, z. B. Personalausweise, Pässe, KFZ- und Führerscheinstelle, hinaus. So zählen etwa auch die Bereiche Planen und Bauen, Denkmalpflege, Pflege der Grünflächen oder Kultureinrichtungen zum Aufgabengebiet. Längst versteht sich die Stadtverwaltung als Service-Anbieter für die 57.000 Bürger sowie die ortsansässigen Unternehmen und Geschäfte. Um allen Anforderungen zeitnah und professionell begegnen zu können, zählt eine moderne IT-Infrastruktur genauso zu den selbst gesetzten Zielen wie ein wirtschaftlicher Umgang mit den IT-Mitteln.

Doch auch die modernsten IT-Infrastrukturen und Lösungen sind rund um die Uhr gefährdet durch eine sich ständig ändernde Bedrohungslage. Cyberkriminelle entwickeln fortwährend neue Methoden für Datendiebstahl, -missbrauch und -manipulation. Für Behörden, Unternehmen und sonstige Organisationen wird es gleichzeitig immer aufwendiger, ihre IT vollumfassend zu schützen. Aus diesem Grund sah sich auch die Stadt Baden-Baden dazu veranlasst, die eigene Strategie zur Verbesserung der Informationssicherheit anzupassen.

Um auf derartige Gefahren reagieren zu können, sind 24/7 neue Technologien, Prozesse und Fachwissen erforderlich. Darum besteht die wahrscheinlich größte Herausforderung darin, dass viele Organisationen

„Das DTS MDR wurde nahtlos bei uns integriert. Nun wird ein deutlich besserer Überblick der sicherheitsrelevanten Ereignisse gewährleistet. Die Zusammenhänge, Auswertungen und die 24/7-Nachverfolgung der Security-Events, über vernetzte Komponenten und Services hinweg, führen zu einer maßgeblichen Erhöhung des gesamten IT-Sicherheitsstandards."

„Das Projekt wurde DTS-seitig partnerschaftlich und unter Einbeziehung des Herstellers professionell und effizient durchgeführt. DTS konnte zudem wirtschaftlich punkten."

BADEN BADEN

BRANCHE:
Öffentliche Verwaltung

HERAUSFORDERUNG:
- Massiv gestiegene Bedrohungslage im Bereich der Cyber Security
- Auf Technologie basierende Analyse & Reaktion
- Anbindung sicherheitsrelevanter Infrastruktur-Komponenten an ein SOC
- Anforderung an einen Katastrophenfall-Support

LÖSUNG:
- DTS Managed Detection & Response (MDR) Service
- DTS Security Operations Center
- Palo Alto Networks Cortex XDR

ERGEBNISSE:
- Deutlich besserer Überblick über sicherheitsrelevante Ereignisse
- 24/7/365 Managed Detection, Überwachung & Reaktion
- Maßgebliche Erhöhung des gesamten IT-Sicherheitsstandards

PARTNER:
DTS Systeme GmbH

nicht die Möglichkeit haben, ein hochqualifiziertes 24/7/365 Team aufzubauen und zu betreiben, welches eine adäquate Bedrohungserkennung und -reaktion gewährleisten kann. Das ist teuer und zeitaufwendig. Mit dem DTS Managed Detection and Response (MDR) ermöglichen wir der Stadt Baden-Baden den idealen Service.

Das DTS MDR nutzt die einzigartige Technologie von Palo Alto Networks Cortex XDR als wesentlichen Bestandteil. Mit Cortex XDR stoppen wir neuartige Angriffe mit der branchenweit ersten offenen und KI-basierten Extended Detection and Response Plattform, die alle Endpunkt-, Netzwerk- und Cloud-Daten berücksichtigt. Sie bietet nicht nur die Möglichkeit als Endpoint Detection and Response (EDR) Lösung einen Prevention First Ansatz auf dem Endpoint auszuführen, sie sammelt zeitgleich wertvolle Informationen, um zielgerichtete Angriffe zu erkennen.

Unsere langjährige, strategische Partnerschaft mit Palo Alto Networks ermöglicht es uns, die führende Technologie durch besondere Services zu veredeln. Wir bieten eine Kombination aus hochqualifiziertem Fachwissen und erstklassiger Technologie zur schnellen Erkennung dynamischer Bedrohungen im gesamten IT-Ökosystem. Der DTS MDR Service ermöglicht hierfür eine 24/7/365 Bedrohungsüberwachung und -abwehr, welche von unseren Security Operations Center (SOC) Experten durchgeführt wird. Diese effektive Kombination aus Technologie und aktiver Überwachung gewährleistet eine schnelle Erkennung und sofortige Gegenmaßnahmen.

Highlights des DTS MDR:
- 24/7/365 Managed Detection & Response, inkl. SOC mit zertifiziertem Fachpersonal
- Automatisierte, proaktive, kontinuierliche Analyse & Reaktion
- Ursachenanalyse, Prozesseingrenzung & -behebung
- Erkennung von Bedrohungen auf Basis führender Threat Intelligence Plattformen
- Digitale, forensische Untersuchungen

Die größten Herausforderungen bei der Wahl möglicher Lösungen bzw. Services lagen darin, die wirklich beste Endpoint Security für sämtliche Clients und Server, ebenso wie die ideale Anbindung sicherheitsrelevanter Infrastruktur-Komponenten an ein SOC zu gewährleisten. Natürlich sollten auch Synergieeffekte unter Berücksichtigung von Kompatibilitätsaspekten genutzt werden. Gleichzeitig galt es aber das passende Preis-Leistungs-Verhältnis abzuwägen, vor allem mit Berücksichtigung der genauen Anforderung an einen verfügbaren Support im Katastrophenfall.

Da bereits teilweise Palo Alto Networks Lösungen im Einsatz waren, konnte sich DTS, inkl. Cortex XDR und dem eigenen SOC, nahtlos in die bestehende Struktur integrieren. Zusätzlich wusste DTS auch wirtschaftlich zu überzeugen. Das Ergebnis ist ein deutlich besserer Überblick der sicherheitsrelevanten Ereignisse. Zusammenhänge, Auswertungen und die 24/7-Nachverfolgung der Security-Events, über vernetzte Komponenten und Services hinweg, führten zu einer maßgeblichen Erhöhung des gesamten IT-Sicherheitsstandards. Das Projekt wurde partnerschaftlich und unter Einbeziehung des Herstellers professionell und effizient durchgeführt. Die Umstellung und Einführung nahmen sogar deutlich weniger Zeit und Aufwand in Anspruch als zunächst angedacht, der geplante Kostenrahmen wurde problemlos eingehalten.