Case Study

Stadtwerke Kamp-Lintfort: Mit Managed EDR zu mehr IT-Sicherheit

Herausforderung

- Einhaltung der KRITIS-Vorgaben
- Umsetzung der NIS-2-Direktive
- Umfassender Schutz vor Cyberattacken

Lösung

- G DATA 365 Managed Endpoint Detection and Response

Vorteile

- Erfahrener IT-Security-Spezialist aus Deutschland
- Rund-um-die-Uhr-Überwachung der IT-Systeme
- Sofortige Reaktion bei Störfällen

STADTWERKE KAMP-LINTFORT

Branche:
Kommunaler Versorger für Strom, Gas und Wasser

Umfang:
55 Mitarbeitende für 20.000 Kunden

Standort:
Kamp-Lintfort (Niederrhein)

Als KRITIS-Unternehmen müssen die Stadtwerke Kamp-Lintfort umfangreiche IT-Sicherheitsvorgaben erfüllen. Um den steigenden Anforderungen weiterhin gerecht zu werden, beschloss der Energieversorger, eine Managed-Endpoint-Detection-and-Response-Lösung einzusetzen. Bei der Wahl des passenden Anbieters entschieden sich die Verantwortlichen für ein deutsches Unternehmen: G DATA CyberDefense.

Die Stadtwerke Kamp-Lintfort versorgen am westlichen Rand des Ruhrgebiets mehr als 20.000 Haushalte und Firmen mit Strom, Wasser, Gas und Fernwärme. Mit mehr als 60 Mitarbeitenden zählt der kommunale Versorger zu den kleineren Stadtwerken. Gleichwohl gehört der Energieversorger als Betreiber der Gas- und Wasser-Netze zu KRITIS und muss diese entsprechend absichern. Die Systeme hat der Versorger so aufgebaut, dass bei einem Ausfall die Versorgung der Kunden trotzdem gewährleistet ist. „Angesichts des Ukraine-Kriegs haben wir uns schon frühzeitig die Frage gestellt, wie gut kritische Systeme vor Sabotage geschützt sind“, sagt Thomas Jansen, IT-Administrator der Stadtwerke Kamp-Lintfort. „Auch neue Vorgaben wie etwa die NIS-2-Direktive führen uns vor Augen, dass wir unsere Systeme besser absichern müssen.“

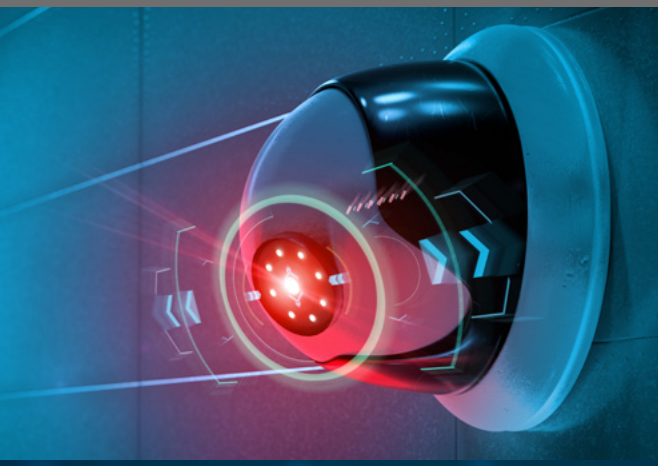
Zukunftsfähig aufstellen

Hinzu kam eine Prüfung der Systeme zur Angriffserkennung zum Jahresanfang – einer der zahlreichen Pflichten als KRITIS-Unternehmen. Die Untersuchung vom TÜV Süd zur Erfüllung einer Vorgabe des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ergab gute Hinweise, um das IT-Sicherheitsniveau der Stadtwerke zu verbessern. Daraufhin setzten sich die Verantwortlichen intensiv mit dem Thema auseinander und führten eine Bestandsaufnahme durch. Der Energieversorger setzte nicht nur eine Antivirenlösung von G DATA CyberDefense ein, sondern auch diverse Überwachungstools für die Systeme.

Aufgrund der mit NIS-2 weiter steigenden Anforderungen war klar, dass die Stadtwerke diese mit dem bestehenden Personal und der eingesetzten

„Die Lösung von G DATA hat uns geholfen, die Vorgaben aus der BSI-Prüfung bereits frühzeitig zu erfüllen und sehr weit umzusetzen."

Thomas Jansen
IT-Administrator der Stadtwerke Kamp-Lintfort



Managed Endpoint Detection & Response erkennt und stoppt Cyberangriffe

Endpoint Protection nicht erfüllen kann. Benötigt wurde ein Service, der eine frühzeitige Angriffserkennung Rund-um-die-Uhr ermöglicht. Daher fiel die Entscheidung auf eine gemanagte Security-Lösung. So lässt sich das IT-Sicherheitsniveau ohne eigenes Personal signifikant verbessern. Ein weiterer Grund für die Entscheidung: Für gute IT-Security sind spezifische Fähigkeiten und Erfahrung erforderlich. Das ist für eine IT-Abteilung mit vielfältigen Aufgaben sehr schwer herzustellen.

Im Fokus: Ein Partner aus Deutschland

Bei der Suche nach einer passenden Lösung ließen sich die Verantwortlichen auch vom IT-Systemhaus Bechtle beraten. Die Anforderungen waren schnell formuliert. Gesucht wurde eine Lösung, bei der IT-Security-Profis die Systeme der Stadtwerke Kamp-Lintfort 24/7 überwachen. Der Anbieter sollte seinen Standort idealerweise in Deutschland haben und auch ein deutschsprachiger Support stand weit oben auf der Prioritätenliste. „Einen Sicherheitsvorfall möchte ich nicht mit einem fremdsprachigen Support besprechen", begründet das Thomas Jansen. „Das Risiko von Missverständnissen ist zu hoch. Da fühle ich mich in meiner Muttersprache wohler." Darüber hinaus legte das Unternehmen großen Wert auf eine schnelle und einfache Meldekette, um bei Störungen umgehend benachrichtigt zu werden.

Da die Stadtwerke bereits mit G DATA zusammenarbeiten, empfahl Bechtle, G DATA 365 Managed Endpoint Detection and Response in Betracht zu ziehen. „Wir sind mit der eingesetzten Antiviren-Lösung von G DATA sehr zufrieden", erklärt Thomas Jansen. „In persönlichen Gesprächen haben die Security-Profis mit ihrer Kompetenz überzeugt. Da ist uns die Entscheidung leichtgefallen."

Stressfreier Rollout von Managed EDR

Die Implementierung von G DATA 365 Managed Endpoint Detection and Response lief problemlos ab. Vom Download der Software bis zur Installation auf den Clients waren nur kleine Anpassungen notwendig. Bis die Lösung auf allen Endpoints, die überwacht werden sollten, einsatzfähig war, gab es noch ein paar notwendige Angleichungen. G DATA reagierte hier sehr schnell und präsentierte innerhalb von einer Stunde eine gute Lösung.

Seit mehreren Monaten ist Managed EDR beim Energieversorger im Einsatz. Die Lösung geht nicht nur einen, sondern zwei Schritte weiter als klassische Virenschutzlösungen: Managed EDR nutzt Security-Technologien, ergänzt diese aber durch zusätzliche Sensoren (Detect) und ermöglicht eine Reaktion auf schädliche Aktionen (Respond).

Der entscheidende Unterschied sind die erfahrenen Security-Analysten von G DATA. Sie analysieren potenziell schädliche Vorgänge, schätzen diese ein und reagieren im Ernstfall umgehend. Dabei haben sie Zugriff auf alle relevanten Informationen, die nötig für eine Entscheidungsfindung sind. So können sie eine Cyberattacke bereits in der Anfangsphase stoppen und weitreichende Schäden verhindern. Zudem können Mitarbeitende von G DATA Systeme aus der Ferne abschalten, wenn gerade kein Angestellter der Stadtwerke vor Ort auf die Systeme zugreifen kann.

Die Erfahrungen aus den ersten Monaten sind durchweg positiv. „Die Lösung von G DATA hat uns geholfen, die Vorgaben aus der BSI-Prüfung bereits frühzeitig zu erfüllen und sehr weit umzusetzen", sagt Thomas Jansen. „Bei der IT-Sicherheit sind wir auf dem richtigen Weg. Es kommen sicherlich noch zusätzliche regulatorische Herausforderungen auf uns zu, aber mit Managed EDR haben wir eine gute Basis geschaffen."

Aufgrund der guten Erfahrung mit G DATA 365 Managed Endpoint Detection and Response haben die Stadtwerke eine weitere Dienstleistung von G DATA beauftragt: G DATA SecMon – ein zielgerichtetes Security Monitoring der IT-Infrastruktur.

Neugierig, wie auch Sie Ihr Unternehmen mit G DATA absichern können?
Hier erfahren Sie mehr:

gdata.de/business vertrieb@gdata.de 0234 / 9762-170

G DATA CyberDefense