



Case Study GETEC:

G+E GETEC Holding GmbH geht mit DTS in die nächste Generation der IT-Security

GETEC ist einer der führenden Energieversorger und Contracting-Spezialisten für Industrie und Wohnungswirtschaft in Deutschland und Europa. Das Werteverprechen von GETEC lautet: „Wir haben die Energie für mehr“. Dieses Leitbild gilt für über 1.400 Mitarbeiter an rund 30 Standorten. Dabei versteht sich GETEC als Partner für smarte, effiziente und grüne Energielösungen.

Branchenweit werden die Herausforderungen hinsichtlich zielgerichteter Cyberbedrohungen immer größer. Herkömmliche IT-Lösungen können den modernen Anforderungen kaum noch Stand halten und selbst präventive Ansätze sind oft nicht mehr ausreichend. In diesem Zusammenhang ist auch der Schutz vor neuartigen Threats nicht mehr allein mit klassischem, signaturbasiertem Virenschutz realisierbar.

GETEC war auf der Suche nach einem innovativen Ansatz, der eine Detect & Response Lösung in Verbindung mit einem verhaltensbasierten Malwareschutz bietet. Dies war der nächste, logische und notwendige Schritt im Ausbau der Widerstandsfähigkeit der GETEC IT-Systeme. Dabei musste mit einem möglichst geringen Aufwand eine ausreichend große Wirkung erzielt werden. Durch eine Partnerempfehlung von unserem langjährigen IT-Security-Partner Palo Alto Networks, kam schließlich eine Zusammenarbeit mit der DTS Systeme zustande. Betreut vom DTS Account Manager

„Die DTS bietet im gesamten IT-Lifecycle eine sehr gute Betreuung.“

Thomas Heinemann, Information Security Officer,
 G+E GETEC Holding GmbH



GETEC

BRANCHE:

Energie

DIE HERAUSFORDERUNG:

- Steigende Anforderungen im Bereich IT-Sicherheit
- Gefahr durch neuartige Cyberbedrohungen
- Hohe Wirkung mit wenig Aufwand

DIE LÖSUNG:

- Cortex XDR als innovative Cybersecurity
- Detect & Response anstatt signaturbasierter Erkennung

ERGEBNISSE:

- Schutz vor modernen, zielgerichteten, bisher unbekanntem Cyberangriffen
- Deutlich bessere Detection & wesentlich kürzere Erkennungs- sowie Reaktionszeit
- Tiefgehende Transparenz im gesamten Netzwerk & an den Endpunkten

PARTNER:

DTS Systeme GmbH

Mehdi Assaad, wurden zunächst Palo Alto Networks Next-Generation Firewalls in die IT-Infrastruktur von GETEC integriert. Nach erfolgreicher Umsetzung wurde die Implementierung der Detect & Response Lösung „Cortex XDR Pro“ umgesetzt.

Angesichts der zunehmend automatisierten und komplexen Angriffe setzen die Security-Experten dabei in der Regel auf einen mehrstufigen Ansatz und kombinieren leistungsfähige Analyse- und Erkennungstechnologien. Das Ziel, zielgerichtete Angriffe effizient erkennen und verhindern zu können, kann jedoch nur erreicht werden, wenn diese Technologien sich gegenseitig unterstützen und die Einrichtung konsistenter Schutzmaßnahmen in der gesamten Unternehmensumgebung durchgesetzt wird. Mit einer derart integrierten Infrastruktur können Sie das Sicherheitsniveau Ihres Unternehmens kontinuierlich heben und Angriffe auf koordinierte Weise abwehren.

Cortex XDR ist die effizienteste Lösung, um automatisiert zielgerichtete, bisher unbekannte Bedrohungen zu erkennen und zu stoppen. Dies gilt für das gesamte Netzwerk bis hin zum einzelnen Endpunkt. Es hilft Unternehmen jeder Größenordnung die durchschnittliche Zeit zur Erkennung und Reaktion auf Cyberangriffe zu minimieren. Dazu identifiziert Cortex XDR jeden Schritt eines Angriffs, indem Daten aus nötigen Datenquellen in Verhaltensanalysen und maschinelles Lernen einbezogen werden, um Bedrohungen zuverlässiger zu erkennen. Aufbauend auf dem bereits mit DTS durchgeführten Next Generation Firewall Projekt konnte mit der Endpoint Protection von Cortex XDR und best practices von DTS verbesserter Schutz bei GETEC implementiert werden. Die geschaffene Transparenz in der Infrastruktur sowie dem Verhalten der User und Assets bietet hierbei wesentliche Mehrwerte im Kampf gegen die Cyberkriminalität.

Auf Wunsch ist DTS für seine Kunden rund um die Uhr im Einsatz und ermöglicht zudem bedarfsgerechte Managed Services. Das beinhaltet z. B. den Betrieb von Security-Plattformen, Health Checks oder Managed Detection & Response Services durch unser eigenes Security Operations Center (SOC). So unterstützen wir unsere Kunden als Security Service Provider auch auf der Datenbasis von Cortex XDR. Dies erspart unseren Kunden wertvolle Zeit, die Konzentration auf wesentliche Geschäftsprozesse im betrieblichen Ablauf und das Profitieren von der langjährigen Erfahrung der DTS in den Bereichen Design, Integration, Betrieb von ganzheitlichen Sicherheitsplattformen sowie Analyse und Bewertung von Security-Alarmen.

GETEC berichtet von ausgesprochen guten Erfahrungen mit DTS hinsichtlich Beratung, Einführung und Support. Die problemlose, direkte Integration der Firewalls hat die Entscheidung für Cortex XDR stark beeinflusst, da so die gesetzten Herausforderungen gut umgesetzt werden konnten. Der Cortex XDR Agent hat bereits deutlich mehr Malware im System erkannt und entfernt, als es die vorherige Lösung vermochte. Mit Cortex XDR konnte GETEC eine tiefgehende Transparenz in ihren Netzen und Systemen gewinnen. Threats werden frühzeitig erkannt und eingedämmt. Die Herausforderung mit geringem Aufwand eine hohe Wirkung zu erzielen wurde vollständig erfüllt.