CASE STUDY

IT-Sicherheit auf Rezept

kohlpharma

Wenn die Nase läuft, die Wade zwickt oder ein wichtiges Medikament fehlt, geht man wie selbstverständlich zum Apotheker. Arzneimittel-Importeure wie kohlpharma sorgen dafür, dass der Patient dort die gewünschte Medizin sofort und preisgünstig erhält. Damit alles reibungslos läuft, bedarf es der perfekten Logistik – natürlich geschützt mit Sicherheitslösungen von ESET.

kohlpharma GmbH
www.kohlpharma.com

PRODUKT

ESET PROTECT Enterprise On-Premises*
ESET Server Security**
ESET Dynamic Threat Defense
ESET Detection & Response***

BRANCHE

Pharmabranche

FACHHÄNDLER

ttt-it AG

kohlpharma wurde 1979 gegründet und ist heute der marktführende Arzneimittel-Importeur in Europa. Das Unternehmen mit Sitz im saarländischen Merzig kauft Original-Markenarzneimittel namhafter Pharma-Hersteller in anderen EU-Ländern preisgünstig ein und importiert sie nach Deutschland. Patienten und Krankenkassen profitieren von den realisierten Einsparungen, Ärzte schonen ihr Budget und schaffen für sich und ihre Patienten Freiräume. Das Unternehmen beschäftigt 800 Mitarbeiter und beliefert sowohl Apotheken als auch deutsche Pharma-Großhändler.

*vormals: ESET Endpoint Protection Advanced | **vormals: ESET File Server | ***vormals: ESET Enterprise Inspector

UMFASSENDER ANFORDERUNGSKATALOG

Doch auch bei den Themen Industrie 4.0 und Vollautomatisierung ist der Arzneimittel-Importeur eines der führenden deutschen Unternehmen. Viele der notwendigen Arbeitsschritte wurden bereits teil- oder vollautomatisiert. Dadurch sind die Systeme auch potentielles Ziel von Cyberangriffen und bedürfen einer umfassenden Absicherung. kohlpharma suchte daher nach einer zukunftsweisenden IT-Securitylösung, die neben klassischem Malwareschutz auch ein Endpoint Detection und Response (EDR)-System umfassen sollte.

Projektleiter Johannes Zenner erarbeitete diesbezüglich eine ambitionierte Anforderungsmatrix aus wirtschaftlicher, funktioneller und administrativer Sicht. So schafften es lediglich drei Hersteller in die engere Auswahl. „ESET wurde uns von unserem Systemhaus ttt-it AG wärmstens ans Herz gelegt. Sehr gute Erkennungsraten, modernste Technologien sowie Empfehlungen von Gartner und AV-Comparatives – ESET brachte die perfekten Voraussetzungen mit“, erinnert sich Herr Zenner.

Alle potentiellen Lösungen nahm das Unternehmen aus Merzig intensiv unter die Lupe. In mehreren Testumgebungen mit geklonten Servern und Endpoints aus der Produktivumgebung konnte ESET überzeugen. „Der Kosten-Nutzen-Faktor von ESET war deutlich besser als bei anderen Mitbewerbern. Ausschlaggebend waren jedoch zwei weiche Faktoren. Das hohe Maß an Engagement sowie die offene und ehrliche Kommunikation ohne leere Versprechungen hat uns überzeugt“, bilanziert Stefan Pistorius, Gruppenleiter EDV Service und Administration.

ROLLOUT IN REKORDZEIT

In nur sechs Wochen wurde die ESET-Lösung „ESET PROTECT Enterprise On-Premises*“ mit ihren Komponenten ESET Endpoint Security, ESET File Server**, ESET Shared Local Cache und ESET PROTECT*** implementiert. In zwei weiteren Schritten erfolgte der Rollout von ESET Dynamic Threat Defense und ESET Detection & Response****. „Die gesamte Umstellung der 1.250 Seats auf ESET war von höchster Professionalität und harmonischer Zusammenarbeit aller Beteiligten geprägt. Das war beispielhaft“, freut sich Stephan Kapetanios von ttt-it AG. Systemhaus, Hersteller und Kunden arbeiteten während des gesamten Prozesses eng zusammen und konnten so selbst individuellste Anpassungen innerhalb kürzester Zeit umsetzen.

*vormals: ESET Endpoint Protection Advanced | **vormals: ESET Server Security | ***vormals: ESET PROTECT | ****vormals: ESET Detection & Response

„(...) sind übersichtlich, strukturiert aufgebaut, sehr performant und bieten eine Vielzahl an Möglichkeiten.“

Johannes Zenner,
Projektleiter bei kohlpharma

ENDPOINT DETECTION AND RESPONSE: DIE KÖNIGSDISZIPLIN DER IT-SECURITY FÜR KRITIS

„Unternehmen wie wir, die als Kritische Infrastruktur (KRITIS) eingestuft sind, müssen in der IT-Sicherheit mehr als eine Schippe drauflegen. Deshalb haben wir unsere bisherige Security-Architektur um ‚Endpoint Detection and Response' erweitert (EDR)", sagt Johannes Zenner. Dies bedeutet im Klartext: Weder darf auch nur eine Malware durchrutschen noch dürfen Schwachstellen im Netzwerk unentdeckt bzw. offen bleiben. Denn sollte die Logistik wegen eines Angriffs zum Erliegen kommen, drohen nicht nur finanzielle Verluste in Millionenhöhe – pro Tag. Viel schlimmer wiegt der Vertrauensverlust von Seiten der kohlpharma-Kunden und letztlich der Patienten. Dieser Schaden lässt sich kaum wiedergutmachen. Folglich setzt kohlpharma auf die beiden Lösungen ESET Dynamic Threat Defense und ESET Detection & Response*.

ESET DYNAMIC THREAT DEFENSE: EXTRA-SCHUTZ VOR INFIZIERTEN DATEIEN

Ein Netzwerk ist täglich mit Hunderten unbekannter Dateien konfrontiert. Einfache Dokumente und andere nicht ausführbare Dateien stellen dabei für etablierte Sicherheitslösungen meist kein Problem dar. Doch die Vollautomatisierung von Prozessen bei kohlpharma bringt es mit sich, dass auch viele ausführbare Files – beispielsweise für Aktualisierungen von einzelnen Rechnern oder Maschinen – von extern übermittelt werden. Dies kann natürlich höchst gefährlich sein, kann sich hinter der .exe doch Malware verbergen. Gleichzeitig ist die Ausführung für den reibungslosen Betriebsablauf zwingend notwendig. Die Lösung: Die Datei wird in einer Sandbox ausgeführt, um einschätzen zu können, was sie tut und worauf sie zugreift. Leider erfordert dies große Rechenressourcen und eine Vielzahl an Sandbox-Templates und war daher On-Premises nicht realisierbar.

Abhilfe schafft hier ESET Dynamic Threat Defense (EDTD) mit einer cloudbasierten Sandbox, um neue, bisher unbekannte Gefahren zu identifizieren. Damit ergänzt es die ESET Produkte zur Absicherung der kohlpharma-Endpoints um eine weitere Schutzschicht. Automatisch oder bei Bedarf auch manuell werden die Samples an das ESET-Rechenzentrum und deren Sandboxes geschickt. Diese bestehen aus verschiedensten Sensoren, die die statische Codeanalyse um Machine Learning, die Prüfung des Arbeitsspeichers und verhaltensbasierte Analysen erweitern. Im Vergleich zu den Endpoint-Lösungen nutzt EDTD damit ein weitaus größeres Spektrum an Technologien, um potentiell gefährliche Samples zu erkennen. Das Resultat wird anschließend zurückgespielt und

> *Eine komplexe IT-Sicherheitslösung muss einwandfrei funktionieren und dennoch einfach zu bedienen sein. Diesen Spagat schafft ESET vorbildlich.*

Stefan Pistorius,
Gruppenleiter EDV Service und Administration bei kohlpharma

infizierte Dateien bei Bedarf auch gleich gelöscht. Zusätzlich generiert EDTD ausführliche Berichte für die kohlpharma-Administratoren.

ESET DETECTION & RESPONSE* FINDET INTERNE SCHWACHSTELLEN

Doch auch das war Pistorius nicht genug: „Uns reicht es nicht, mit klassischen Malwarelösungen auf Angriffe zu reagieren. Wir wollen selbständig kontrollieren, wo sich Schwachstellen befinden und sie beseitigen". kohlpharma entschied sich daher, ESET Detection & Response* zum Einsatz zu bringen. ESETs Endpoint Detection and Response (EDR)-Tool sammelt Echtzeitdaten über Aktivitäten auf den verbundenen Endpoints und gleicht sie automatisch mit Regeln ab, die auf verdächtige Aktivitäten hindeuten. Die so gesammelten Informationen werden aufbereitet und in einem durchsuchbaren Format gespeichert. So entsteht eine per Drill-Down zugängliche Sammlung untypischer und verdächtiger Aktivitäten.

ESET Detection & Response* liefert zudem forensische Daten zu vergangenen Vorfällen und gibt Hinweise zu möglichen Gegenmaßnahmen. Selbst sogenannte Advanced Persistent Threats (APTs), die sich bereits im Netzwerk befinden, lassen sich so erfolgreich abwehren. ESET Detection & Response* vereint dazu die umfassenden Informationen aus allen ESET Erkennungstechnologien, u.a. Machine Learning.

EINFACHE BEDIENUNG ÜBER WEBKONSOLEN

Auf den ersten Blick sieht es aus, als sei die Kombination aus vielen verschiedenen Produkten und Technologien vor allem eines: kompliziert. Doch Johannes Zenner hat über die mitgelieferten ESET Webkonsolen jederzeit alles im Griff. Dreh- und Angelpunkt ist dabei ESET PROTECT**, worüber er alle Endpoints und Server zentral administriert. Für ESET Detection & Response* nutzt er eine zusätzliche Administrationskonsole. „Beide Tools erleichtern mir den Alltag enorm. Sie sind übersichtlich, strukturiert aufgebaut, sehr performant und bieten eine Vielzahl an Möglichkeiten", sagt der Projektleiter. „Wechselseitig werden die Daten automatisch synchronisiert – so bin ich immer auf dem aktuellen Stand. Und sollte es mal haken, kann ich auf aktuelle und umfangreiche Dokumentationen zurückgreifen".

Mit den eingesetzten ESET Sicherheitslösungen konnte

*vormals: ESET Enterprise Inspector | **vormals: ESET Security Management Center

kohlpharma den Schutz seiner Systeme auf ein völlig neues Niveau heben. Dabei ging es nicht nur um die bloße technische Lösung. Mindestens ebenso wichtig waren weiche Faktoren wie der persönliche Kontakt zwischen Kunde, Hersteller und Systemhaus sowie der umfassende und dauerhafte Service und Support. So kann kohlpharma sicher sein, auch im Krisenfall starke Partner an seiner Seite zu haben.

FALL

kohlpharma sucht eine neue IT-Sicherheitslösung, die den Anforderungen von KRITIS mehr als gerecht wird. Neben klassischem Malwareschutz sollen auch Endpoint Detection and Response Tools die eigene IT-Security verstärken.

LÖSUNG

Die professionelle Kombination aus ESET PROTECT Enterprise On-Premises*, ESET File Security, ESET Dynamic Threat Defense und ESET Detection & Response** sichert die komplexe Sicherheitsarchitektur erfolgreich vor Hackern und Cyberkriminellen.

BENEFIT

ESET liefert ganzheitliche IT-Lösungskonzepte aus einem Guss. Es wehrt Angriffe von außen zuverlässig ab und identifiziert interne Schwachstellen im Detail. Die hervorragende Bedienbarkeit über die ESET-Konsolen erleichtert den Administratoren die Arbeit.

*vormals: ESET Endpoint Protection Advanced | **vormals: ESET Enterprise Inspector