

WACKLER IMPLEMENTIERT IT-SICHERHEITSPAKET

Security Awareness, Monitoring und Incident Response als Managed Services sorgen für höchsten Schutz.



Modern Workplace
erleichtert die Arbeit
und schützt Daten und
Identitäten



SOC as a Service
überwacht und
schützt komplette
IT-Infrastruktur



Incident Response
über CDOC
der abtis erfüllt
NIS2-Richtlinie



Sensibilisierung
der User durch
Security-Awareness-
Maßnahmen

WACKLER
Spedition & Logistik

Die Spedition L. Wackler Wwe. Nachf. GmbH (Wackler) ist ein mittelständischer Logistikdienstleister für nationale und internationale Transportlösungen mit einer mehr als 150-jährigen Historie. Das umfangreiche Logistik-Portfolio des innovativen Familienunternehmens mit Hauptsitz in Göppingen bei Stuttgart, einer Niederlassung in Wilsdruff bei Dresden und einem Logistikzentrum in Uhingen reicht von Warehousing über Full-Service-Logistik bis zur E-Commerce-Lösung. Die Dachgesellschaft der Wackler GmbH ist die Schwarz-Gruppe.

MITARBEITENDE

> 500

PALETTENSTELLPLÄTZE

97.000

LINIENVERKEHRE/ TAG

> 114

01 — AUSGANGSLAGE

Sicherheitslücke muss geschlossen werden

Mit Personenverkehr, später Gütertransporten in geschlossenen Kastenwagen und vielen Pferden begann vor mehr als 150 Jahren die Firmengeschichte des Speditions- und Logistikunternehmens Wackler. Heute ist das Familienunternehmen Teil des Cargoline-Netzwerks, hat neben seinem Hauptsitz in Göppingen eine Niederlassung in Sachsen und ein Logistikzentrum in UHINGEN und transportiert, lagert und bewegt national wie international Waren jeder Art – von Stückgut bis Gefahrgut. Ein Angriff auf die IT-Infrastruktur des Unternehmens, der womöglich zu einer Vollverschlüsselung sämtlicher Daten und damit einem wochenlangen

Transportstillstand führen würde, wäre für Wackler eine Katastrophe. Die elfköpfige IT-Mannschaft des Logistikdienstleisters muss ein breites Spektrum an Themen abdecken und sieht sich als Sparringspartner für die Fachabteilungen. Die notwendigen Spezialkenntnisse für eine effiziente IT-Security können intern nicht abgedeckt werden. Schon gar nicht rund um die Uhr an sieben Tagen in der Woche und mit der Reaktionszeit, die ein derartiger Angriff bzw. dessen Prävention erfordern würden. Wackler war deshalb klar, dass diese wichtige Lücke nur mit Unterstützung eines externen Dienstleisters erfolgreich geschlossen werden kann.



„Einige Firmen in unserer Branche wurden in den vergangenen zwei Jahren Opfer von Hackerangriffen, die haben dann mit sehr starken Verlusten und Verdienstaussfällen arbeiten müssen und natürlich massivem Aufwand – wenn man mal die Summen hört, die so ein Angriff nach sich zieht, dann wird einem ganz schön blüherant.“

BERND WAGEGG
ABTEILUNGSLEITER IT-INFRASTRUKTUR
BEI WACKLER

02 — ANFORDERUNGEN

Zuverlässige personelle und fachliche Unterstützung benötigt

Wackler suchte also nach einem zuverlässigen und vertrauenswürdigen Partner, der die vollständige IT-Absicherung bei dem Speditions- und Logistikunternehmen übernimmt. Diese sollte auf drei Ebenen erfolgen: zunächst Transparenz über und die Sicherung der kompletten IT-Infrastruktur – Endgeräte, Server, Netzwerkgeräte, alles, was an Hardware vorhanden ist, zweitens der Schutz von Anwendungen, Daten und Identitäten – auch in der Cloud, und drittens die Sensibilisierung der Mitarbeitenden in Bezug auf verschiedene Varianten von Cyberangriffen und wie diese allein durch bewusstes menschliches Verhalten eingeschränkt werden können. Neben dem Expertenwissen im sich permanent rasant weiterentwickelnden Themenfeld IT-Security

benötigte Wackler insbesondere personell externe Unterstützung. Nur so konnte das Monitoring sämtlicher Systeme und proaktive Eingreifen in kritischen Situationen rund um die Uhr an 365 Tagen im Jahr abgedeckt werden. Zum Gesamtpaket gehörte für Wackler zudem die Einführung eines Modern Workplace, der die tägliche Arbeit und Zusammenarbeit der mehr als 400 Beschäftigten mit Zugang zum Wackler-Netzwerk erleichtern und absichern sollte – auch bei Zugriff von remote und zu jeder Tages- und Nachtzeit. Langfristig wollte Wackler damit ein deutlich höheres Sicherheitsniveau erreichen und gleichzeitig seinen Mitarbeitenden moderne Tools zur Verfügung stellen, die ihre Arbeit effizienter und angenehmer machen sollten.

Wackler entscheidet sich für umfassendes IT-Sicherheitspaket

In der Vergangenheit hatte Wackler bereits mehrfach erfolgreich mit abtis zusammengearbeitet. Der IT-Dienstleister hat beispielsweise die heterogene Netzwerkumgebung an den Wackler-Standorten Göppingen und Wilsdruff vereinheitlicht und die komplexe WLAN-Ausleuchtung im Hochregallager optimiert. Aufgrund der sehr guten Erfahrungen, die Wackler während dieser früheren Projekte bereits mit abtis gemacht hatte, entschied sich das Unternehmen auch für die Umsetzung des umfangreichen Security-Pakets wieder für die Experten aus

Pforzheim. Heute schützt abtis zuverlässig die Infrastruktur, Systeme und Daten bei Wackler vom Endpoint bis zur Cloud-Infrastruktur mit Azure Stack HCI, von den Firewalls bis zu Netzwerk und Domain Controllern. Dabei liefert der IT-Dienstleister nicht nur die komplette Hardware und dazugehörige Software aus einer Hand, sondern auch die Managed Services dazu, so dass die Wackler-IT von Wartung und Pflege der einzelnen Komponenten, aber beispielsweise auch aufwändigen Beschaffung und Verlängerung von Lizenzen befreit ist.

Monitoring und Incident-Response-Strategie mit SOC as a Service und abtis CDOC

Mit SOC as a Service (Security Operation Center) aus dem abtis Cyber Defense Operation Center (CDOC) überwacht abtis rund um die Uhr die komplette Wackler-Infrastruktur mit der bewährten Kombination aus Künstlicher Intelligenz wie Deep Instinct, Microsoft 365 E3 und Microsoft Defender Suite und dem hohen Sachverstand von Experten und Forensikern, die auf dem gesamten Globus verteilt sind. So werden nicht nur offensichtliche Angriffe erkannt und abgewehrt, sondern ebenso sämtliche Anomalien, untypisches Verhalten oder dergleichen nach einer zuvor definierten Alarmierungskette

gemeldet und entsprechend eskaliert. Eine derartige Incident-Response-Strategie ist auch Bestandteil der NIS2-Richtlinie, der Unternehmen der kritischen Infrastruktur wie Wackler unterliegen.

„Wir brauchen maximale Transparenz auf allen Systemen, die wir im Einsatz haben und die bekommen wir nur, wenn das Monitoring durchgängig und ganzheitlich erfolgt. Deshalb sehen wir die Kombination aus SOC as a Service und dem abtis CDOC als sinnvolles Gesamtkonzept“, erklärt Marc Fiegert, Bereichsleiter der IT-Abteilung bei Wackler.

Angenehmeres Arbeiten und Schutz von Daten und Identitäten mit dem Modern Workplace

Als weiterer Baustein des neuen Sicherheitskonzepts wurde mit der Einführung des Modern Workplace bei Wackler begonnen. Neben sämtlichen Tools, die das Arbeitsleben erleichtern, wie Microsoft Teams, Planner oder Loop als Teil von Microsoft 365, gehören auch die Umsetzung einer Multi-Faktor-Authentifizierung (MFA) und einer Lösung für Mobile Device Management (MDM) für mobile Endgeräte wie Firmen-Smartphones zum Modern Workplace.

In einem nächsten Schritt sollen sämtliche Daten, Endgeräte, Identitäten, Infrastruktur und Anwendungen nach dem Zero-Trust-Ansatz mit Azure Information Protection gesichert werden. Auch Network Access Control (NAC) soll im weiteren Projektverlauf umgesetzt werden, damit Endgeräte während der Authentifizierung auf Richtlinienkonformität geprüft werden können, also ob der Virens Scanner aktuell ist

oder das Client-Betriebssystem über den neuesten Sicherheits-Patch verfügt, bevor sie Zugang zum System erhalten. Auch der Modern Workplace wird an das CDOC der abtis angebunden und sämtliche Aktivitäten hinsichtlich verdächtiger Anomalien oder Angriffe entsprechend überwacht. Besonders angenehm für die interne IT bei Wackler ist, dass abtis sich nicht nur um die benötigte Hard- und Software kümmert, sondern auch um die entsprechenden Lizenzen. Tritt ein neuer Mitarbeiter in das Unternehmen ein, erhält er sofort Zugriff auf den Modern Workplace inkl. Office-Lizenz, Lizenz für Deep Instinct usw., ohne dass Wackler sich um den Erwerb oder – bei Austritt des Mitarbeiters aus dem Unternehmen – die Abmeldung der Lizenz kümmern muss. „Sonst wären wir permanent damit beschäftigt, separat verschiedene Lizenzen zu klicken – ein Verwaltungsaufwand, den man nicht betreiben möchte“, erklärt Wagegg.

Der Faktor Mensch

Bei allen technischen Möglichkeiten moderner Security-Lösungen darf der Mensch als potenzieller Risikofaktor nicht unterschätzt werden. In Zeiten von Deep-Fakes sind Phishing-Mails wahrscheinlich noch das kleinste Problem, wobei E-Mails noch immer das beliebteste Einfallstor für Hackerangriffe darstellen. Um zu verhindern, dass die eigenen Mitarbeitenden Cyber-Kriminellen unbeabsichtigt Zutritt zum Unternehmen verschaffen, ist Wackler eine Sensibilisierung und Schulung der Beschäftigten wichtig. abtis hat Wackler hier seinen Partner und Experten für Security Awareness KnowBe4 empfohlen.

Mit einer simulierten Phishing-Kampagne, die deutliche Lücken in der Erkennung der Gefahren offenbarte, wurde durch KnowBe4 zunächst eine Grundlage und Verständnis dafür geschaffen, dass einerseits Aufklärungsarbeit zu leisten ist und andererseits zunächst als lästig empfundene Zusatzaufwände – wie die Multi-Faktor-Authentifizierung – durchaus sinnvoll sind. Damit erfüllt Wackler einen weiteren Aspekt der besonders strengen Anforderungen der NIS2-Richtlinie, die ausdrücklich eine höhere Sensibilisierung im User-Verhalten vorsieht.

”

„Die Funktionen, die wir jetzt bei der abtis bekommen: SOC as a Service, CDOC und die Firewalls, die wir an jedem Standort ausgerollt haben, würden wir neben dem Tagesgeschäft nicht mal ansatzweise hinbekommen.“

MARC FIEGERT

BEREICHSL EITER IT-ABTEILUNG

BEI WACKLER

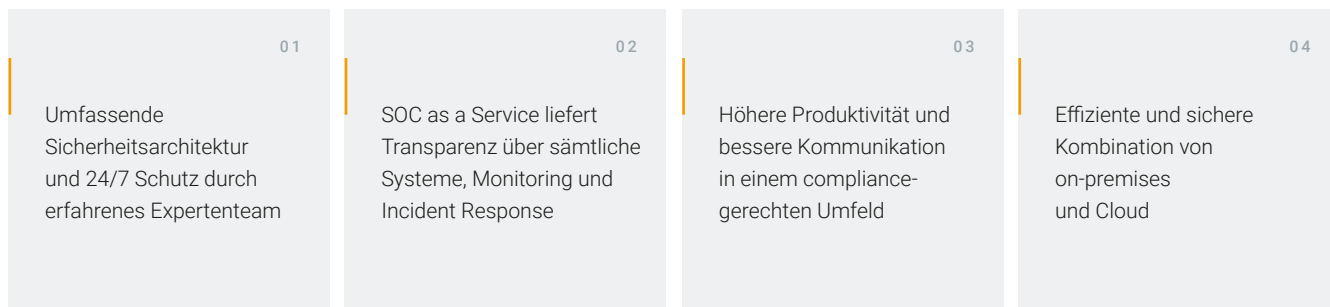


Mehr Sicherheit, mehr Features, weniger Zeitaufwand

In Summe ist bei Wackler jetzt eine umfassende Security-Strategie umgesetzt worden, die stets aktuell potentielle Gefahrenquellen auf verschiedenen Ebenen überwacht, absichert und damit die Bedrohungslage deutlich entschärft. Die Auslagerung verschiedener Services – insbesondere des Monitoring und Incident Response, aber auch der Support, die Wartung und Pflege der verschiedenen Komponenten – verschafft der internen IT Freiräume für das Tages- und Projektgeschäft, erklärt Marc Fiegert: „Durch die Auslagerung der verschiedenen Services haben wir definitiv eine Zeitersparnis – Beispiel Firewall: früher mussten wir uns intern darum kümmern, wenn etwas angepasst werden musste, und erst einmal die Zeit

dafür finden und das entsprechende Know-how auffrischen, heute macht man ein Ticket auf und es wird erledigt.“ Da abtis sämtliche gewünschte Komponenten – von der Hardware über die Software bis hin zu Managed Services – bereitstellt, ist sichergestellt, dass alle Tools optimal aufeinander abgestimmt und lizenziert sind. Ein weiterer Vorteil, alles aus einer Hand zu beziehen, liegt darin, dass bei auftretenden Problemen klar ist, an wen man sich wenden muss und ein Kompetenz- und Zuständigkeitsgerangel zwischen verschiedenen Dienstleistern gar nicht erst entsteht. Für die Zukunft plant das Unternehmen bereits weitere Investitionen in die Sicherheit sowie die Umsetzung von KI-Projekten mit Microsoft Copilot.

Umfassende Security für KRITIS-Unternehmen



„Uns war klar, dass wir da eine Lücke hatten, die wir jetzt geschlossen haben. Da wir alleine dazu nicht in der Lage gewesen wären, haben wir uns dafür Unterstützung von der abtis geholt. Das war genau die richtige Entscheidung.“

AUFGABE

- Absicherung sämtlicher Geräte, Systeme, Daten und Identitäten gegen Angriffe von außen
- Sensibilisierung der Mitarbeitenden
- Entlastung der internen IT durch abtis Managed Services

KONZEPT

- Umfassende Sicherheitsarchitektur inklusive Zero-Trust-Ansatz sowie vollständigem Monitoring und Incident Response
- Umsetzung von Vorgaben wie u.a. NIS2 und BSI-Grundschutz mit einer Kombination aus Technik und Services
- Zukunftsfähige Gesamtstrategie durch die Kombination von on-premises und Cloud

UNSERE LEISTUNG

- Security as a Service inklusive Bereitstellung benötigter Hardware und Software
- SOC as a Service mit dem abtis CDOC, 24/7 Monitoring und Incident Response
- Modern Workplace als Managed Service

ERGEBNIS

- Verlässlicher und stets aktueller Schutz sämtlicher Systeme, Geräte und Daten im Unternehmen
- Zukunftsgerichtetes Arbeiten mit Modern Workplace und sichere Cloud-Strategie
- Compliance mit rechtlichen Anforderungen wie der NIS2-Richtlinie

Nehmen Sie Kontakt mit uns auf.

 www.abtis.de
 +49 7231 4431 - 100
  vertrieb@abtis.de
 [/company/abtis-gmbh](https://www.linkedin.com/company/abtis-gmbh)

