SAFELY ENABLING BUSINESS

Incident-Response-Einsatz

# Firefighting bei Metabo

**Stillstand: Nach einem Ransomwareangriff im Juni war bei Werkzeughersteller Metabo die gesamte IT-Infrastruktur ausgefallen. Zeit, für das Notfall-Incident-Response-Team von SecureLink Germany in Aktion zu treten. Durch strategisches Firefighting konnten die kritischen Systeme schnell wiederhergestellt werden.**

## Zentralnervensystem lahmgelegt

Die Metabowerke GmbH mit Stammsitz im baden-württembergischen Nürtingen ist ein Hersteller von Elektrowerkzeugen. Das Unternehmen hat 23 Vertriebsgesellschaften und mehr als 100 Importeure. Weltweit arbeiten 1.800 Menschen für Metabo. Metabo hat im Jahr 2015 einen Umsatz von 408 Millionen Euro erwirtschaftet.

Produktion, Warenmanagement und Vertrieb sind auf dem Stand der Technik – was bedeutet: sie sind vollautomatisiert und IT gestützt.

Nachdem am Dienstag, dem 27. Juni 2017 die Ransomware **NotPetya** in die Systeme von Metabo eingeschleust wurde, infizierte die Malware in kürzester Zeit mehr als 1.000 Arbeitsplatzrechner und 350 Server und verursachte einen Ausfall der gesamten Informations- und Kommunikationstechnik.

## Einsatz für die Incident Response Truppe

SecureLink wurde als deutscher Incident-Response-Dienstleister für den Sicherheitsvorfall als externe Beratungsfirma zum Firefighting hinzugezogen. Die Sicherheitsexperten von SecureLink wurden gegen 18:00 Uhr informiert und waren bereits wenig später vor Ort.

Das Ziel des Incident Response Auftrages war es, die wichtigsten Systeme schnell wieder online zu bringen sowie sie vor einer sofortigen Neuinfektion zu schützen.

Zur Wiederherstellung der Produktion mussten die Systeme so schnell wie möglich mit einem effektiven Wiederherstellungskonzept wieder in einen ordnungsgemäßen Betrieb überführt werden.

Eine besondere Herausforderung hierbei waren die, bei Produktionsunternehmen üblichen, unterschiedlichen Systemlandschaften und proprietären Spezialanwendungen.

Mit der Unterstützung von SecureLink gelang es nach einer intensiven Woche, viele zentrale Systeme wiederherzustellen. Durch das von SecureLink ausgearbeitete Konzept wurde das Risiko einer erneuten Infektion minimiert. Mit Cylance Protect konnte zusätzlich sichergestellt werden, dass die kritischen Zielsysteme jetzt exzellent vor Angriffen geschützt sind.

metabo®
PROFESSIONAL POWER TOOL SOLUTIONS

**Kunde:** Metabowerke GmbH

**Branche:** Herstellung von Elektrowerkzeugen

**Leistungen:**

- Sofortiger Einsatz eines qualifizierten Incident Response-Teams
- Analyse und Eindämmung des Angriffes
- Immunisierung der Systeme gegen Neuinfektion
- Ausrollen von nachhaltigen Schutzmaßnahmen für die kritische Infrastruktur des Kunden zum besseren Schutz vor künftigen Angriffen
- Kontrollierte Wiederherstellung der kritischen Systeme

### Das sagt der Kunde:

*» In unserem Fall war die Herausforderung nicht allein Disaster Recovery. Vielmehr ging es auch um wirkungsvollen Schutz vor Reinfizierung.*

*Ich war beeindruckt, wie schnell und präzise das Incident Response Team den Angriffsvektor identifizieren und geeignete nachhaltige Vorsorgemaßnahmen implementieren konnte. Dank ihrer professionellen und vielseitigen Unterstützung waren wir in kürzester Zeit wieder produktiv. «*

*Thomas Rinas, Leiter IT Metabowerke GmbH*

Erfahren Sie mehr unter:
www.securelink.de/services/securerespond

# Erfolgsfaktor Response Team

Das Recruiting von Sicherheitsexperten stellt neben Mehrschichtbetrieb und Fluktuation für die meisten Organisationen eine echte Herausforderung dar. Top qualifizierte Analysten sind für den Betrieb eines CDCs und die Zusammenstellung von Firefighting Teams essentiell.

Solche Spezialteams können im Falle eines Cyber Incidents umfassende Soforthilfe leisten. Je nach Zustand des Systems kann so die Produktivität wiederhergestellt werden. Dabei wird auch Wert auf Nachhaltigkeit gelegt: die Analyse des Angriffes gibt Aufschluss über Schwachpunkte. So können die Experten nicht nur akute Abhilfe schaffen sondern auch nachhaltig das Risiko von Folgeangriffen reduzieren.

## Lösungsansatz

Unsere Experten erhalten ihr Know-how aus einer umfangreichen Ausbildung, permanentem Training und aus der täglichen Bearbeitung von Sicherheitsvorfällen. Sie kennen neueste Tools und Technologien, können auf eingespielte Prozesse zurückgreifen und sind für jede Herausforderung bestens gerüstet.

**Was unsere Experten mitbringen:**

- SANS Zertifizierungen
- Schnelle Reaktionszeit
- Expertenkenntnisse und Erfahrung in Pentesting, Threat Hunting und Incident Response
- Expertise in der Analyse und Eindämmung von Cyberangriffen
- Einbeziehung branchen-/ firmenspezifischer Spezialanwendungen

## Ergebnisse

Mit der Unterstützung von SecureLink gelang es, nach einer intensiven Woche viele zentrale Systeme wiederherzustellen. Durch das von SecureLink ausgearbeitete Konzept wurde das Risiko einer erneuten Infektion minimiert. Mit Cylance Protect konnte zusätzlich sichergestellt werden, dass die kritischen Zielsysteme in Zukunft vor Angriffen wesentlich besser geschützt sind.

**Diese Leistungen wurden erbracht:**

- Kontrollierte Wiederherstellung der kritischen Systeme in kürzester Zeit
- Analyse der Malware
- Ausrollen von Updates auf die Systemlandschaft
- Upgrade der Sicherheit: Ausrollen von Cylance Protect auf die kritische Infrastruktur


SecureLink Germany GmbH • Paul-Gerhardt-Allee 24 • 81245 München • info@de.securelink.net • +49(0) 89 2000148 00
www.securelink.de

SecureLink is the market leading provider of cyber security in Europe.