G DATA advanced analytics

Case Study

Mit Expertise für Incident Response die IT retten und wieder arbeitsfähig werden

Herausforderung

- Schnelle Wiederherstellung und Reinigung der Systeme nach einer Ransomware-Attacke
- Verbesserung des IT-Sicherheitsniveaus im Nachgang sicherstellen

Lösung

- Zusammenarbeit mit Incident-Response-Fachleuten von G DATA Advanced Analytics
- IT Security Consulting nach Wiederanlauf der IT-Infrastruktur, Vermeidung einer direkten Reinfektion und Erhöhung des Sicherheitsniveaus

Vorteile

- Kompetente Soforthilfe vor Ort
- Umfassendes Fachwissen im Bereich forensische Analyse und IT-Sicherheit
- Schnelle Wiederherstellung aller Systeme

Schramme

Branche:
Produzierendes Gewerbe

Umfang:
150 Mitarbeitende an Standorten in Deutschland und China

Standort:
Deggenhausertal, Deutschland
Yangzhou, China

Dank fachkundiger Hilfe von G DATA Advanced Analytics und einer fundierten IT-Sicherheitsstrategie konnte Magnetbau Schramme nach einer Ransomware-Attacke größere Schäden verhindern und war schnell wieder arbeitsfähig.

Ein schlecht gesicherter Rechner reicht Cyberkriminellen aus, um Schadsoftware ins Firmennetzwerk einzuschleusen. Diese Erfahrung musste auch Magnetbau Schramme machen. Allerdings hat das Unternehmen bereits zuvor viele Vorsichtsmaßnahmen ergriffen, sodass der Cyberangriff mit Hilfe von G DATA Advanced Analytics schnell abgewehrt werden konnte. Bei der Wiederherstellung der Systeme arbeiteten die Incident-Response-Fachleute Hand in Hand mit der IT von Magnetbau Schramme.

Der Alptraum begann bei Magnetbau Schramme an einem Montag, den 19. Juni 2019 um 22:19 Uhr. Das Ausmaß der Katastrophe offenbarte sich aber erst am Morgen des 20. Juni.

Eine Ransomware hatte das Netzwerk befallen und pro Stunde bis zu zehn Terabyte Daten verschlüsselt. Dienstag früh waren bereits 85 Prozent der Daten verschlüsselt. So konnten sich Mitarbeitende nicht mehr an ihrem Arbeitsrechner an- oder abmelden. Eine Datei mit einer E-Mail-Adresse und einer Lösegeldforderung im mittleren sechsstelligen Bereich sorgte für Gewissheit: Magnetbau Schramme war Opfer eines Cyberangriffs.

Seit mehr als 45 Jahren ist die Magnetbau Schramme GmbH, mit Sitz in Deutschland (Deggenhausertal) und China (Yangzhou), erfolgreich in der Entwicklung sowie Produktion von Elektromagneten, Ventilen, Sensoren und kundenspezifischen Aktuatoren etabliert. Seit Jahrzehnten haben Automobilzulieferer sowie viele Branchen der Industrie mit dem Familienunternehmen aus Baden-Württemberg eine zuverlässige Partnerschaft. Qualität und Service sind die höchsten Unternehmensziele. Daher setzt das Unternehmen auch auf eine leistungsfähige IT – in der Produktion und im Back-Office.

Retten, was zu retten ist

Diese IT war nach dem Angriff teilweise verschlüsselt und nicht mehr nutzbar. Der gesamte Verwaltungsbereich war betroffen, wo jetzt wieder zu Papier und Stift gegriffen wurde, um die Logistik etwa mit handausgefüllten Lieferscheinen am Laufen zu halten,

„In dieser Ausnahmesituation hat die Kooperation mit den Spezialisten sehr gut funktioniert. Wir haben eng zusammengearbeitet und schnell Lösungen gefunden.“

Marcello Ficht, Head of IT
Magnetbau Schramme GmbH & Co KG

Schnelle Hilfe dank Incident Response Retainer

denn die Produktion konnte annähernd störungsfrei weiterarbeiten. Das Unternehmen hatte sich bereits frühzeitig entschieden, eine umfangreiche IT-Sicherheitsstrategie zu realisieren.

„Hundertprozentige Sicherheit gibt es nicht“, sagt Marcello Ficht, Head of IT bei Magnetbau Schramme. *„Wir haben damit gerechnet, dass wir irgendwann Opfer eines Cyberangriffs werden und daher versucht, uns bestmöglich darauf vorzubereiten.“*

Dazu gehörte neben einer umfassenden Backup-Strategie die Segmentierung des Netzwerkes – eine weise Entscheidung, wie der aktuelle Notfall zeigte. Statt auf die Lösegeldforderung einzugehen, entschied das Familienunternehmen, die Incident-Response-Fachleute von G DATA Advanced Analytics zu beauftragen, um die Systeme von der Ransomware zu befreien, die IT-Infrastruktur wieder lauffähig zu machen und sicherzustellen, dass die Angreifer keinen Zugang mehr dazu haben. Beim Wiederherstellen und Desinfizieren der Systeme halfen zudem Mitarbeiter von Bechtle, die das Unternehmen als Systemhaus bei allen Fragen unterstützen.

Parallel dazu informierte Magnetbau Schramme den eigenen Datenschutzbeauftragten und den des Landes Baden-Württemberg und erstattete Anzeige beim Landeskriminalamt.

Den Angreifer aus dem Netz vertreiben

Im ersten Schritt mussten das Problem eingegrenzt, die genutzte Schadsoftware erkannt und weitere Werkzeuge der Angreifer identifiziert werden.

Gleichzeitig mussten die Fachleute den Tätern auf die Spur kommen, um zu klären, wie sie ins System eingedrungen waren und welche Schadsoftware die Systeme attackiert hatte. Es galt, die Lücke(n) zu schließen, um das Nachladen von weiterer Schadsoftware und das Abgreifen von Firmendaten zu verhindern.

Insgesamt wurden von den Angreifern rund 15 verschiedene Schadprogramme hochgeladen und aktiviert, darunter der Trojaner „Trickbot“ und die Verschlüsselungssoftware „Ryuk“. Umgehend passten die IT-Mitarbeitenden die Firewall an, um den Angreifer auszusperren und um weiteren Schaden zu verhindern.

Da fast alle unternehmenskritischen Daten in SAP gespeichert wurden und dieses System nicht vom Angriff betroffen war, konnten die Angreifer keine kritischen Daten kopieren und ableiten.

Mit speziell auf den vorliegenden Fall zugeschnittener Software identifizierten die Fachleute von G DATA Advanced Analytics lückenlos alle infizierten Systeme und waren in der Lage, diese vollständig zu bereinigen.

Sicher mit signierten Makros

In den allermeisten Fällen gibt es keinen Anlass dazu, in einem normalen Office-Dokument Makros zu verwenden.

Für die wenigen Fälle, in denen der Einsatz von Makros unabdingbar ist, sollte das Unternehmen ausschließlich signierte Makros verwenden und per Gruppenrichtlinie unsignierte Makros unternehmensweit deaktivieren.

So konnten Ausfallzeiten und Kosten einer kompletten Neuinstallation aller betroffenen Systeme vermieden werden.

Die Wiederherstellung der Daten ließ sich einfach bewerkstelligen, was an der funktionierenden Backup-Strategie des Unternehmens lag. Die Backups wurden getrennt vom Netzwerk vorgehalten, sodass die Incident-Response-Fachleute auf eine unverschlüsselte Datenbasis zugreifen konnten, um das Unternehmen schnellstmöglich wieder vollständig arbeitsfähig zu machen.

Eine unscheinbare Sicherheitslücke mit weitreichenden Folgen

Die forensische Analyse zeigte, dass sich bereits seit 2018 eine Schadsoftware gut versteckt im System eingenistet hatte. Über einen infizierten E-Mail-Anhang gelangte die Schadsoftware ins System und wurde von den Tätern über längere Zeit nicht aktiv genutzt.

Der eigentliche Einfallsvektor war nicht der Rechner, der durch den E-Mail-Anhang infiziert wurde, sondern ein Rechner zur Erfassung der Arbeitszeiten mit einer dauerhaften Verbindung zum Internet und erhöhten Rechten für eine Software. Diese erhöhten Rechte haben sich die Angreifer zu Nutze gemacht, um sich damit nahezu im gesamten Netzwerk von Magnetbau Schramme ungehindert bewegen zu können.

Dank der starken IT-Sicherheitsmaßnahmen und einer umfassenden Dokumentation gelang es den Incident-Response-Fachleuten, innerhalb von vier Tagen alle Systeme zu bereinigen und, wo nötig, neu aufzusetzen.

„In dieser Ausnahmesituation hat die Kooperation mit den Spezialisten sehr gut funktioniert“, sagt Marcello Ficht. *„Wir haben eng zusammengearbeitet und schnell Lösungen gefunden. Wichtig war auch eine genaue Analyse des Tathergangs, um die IT-Sicherheit zu verbessern.“*

Nach einem erfolgreichen Wiederanlauf der IT-Infrastruktur hat Magnetbau Schramme kontinuierlich, teils einfache, Maßnahmen umgesetzt, die zu einer signifikanten Verbesserung der IT-Sicherheit geführt haben. Dazu zählte die Implementierung von einem neuen Rechner zur Arbeitszeiterfassung ohne dauerhaften Internetzugang und erhöhten Rechten. Gleichzeitig wechselte das Familienunternehmen den Firewall-Anbieter, um das Sicherheitsniveau weiter zu erhöhen.

In Zukunft können nur noch eigene signierte Makros ausgeführt werden. Es wurden weitere Hürden eingebaut, um die vom regulären Netz separierten Backup-Server vor einer Infizierung durch Schadsoftware zu schützen.

„Dank der umgehenden Hilfe von G DATA Advanced Analytics und unserer guten IT-Sicherheitsstrategie konnten wir den Schaden schnell beheben und waren bald wieder handlungsfähig“, sagt Marcello Ficht. „Aufgrund der getrennten Netze konnte die Produktion annähernd ohne Einschränkung weiterarbeiten, sodass sich der finanzielle Schaden in Grenzen hielt.“

Neugierig, wie auch Sie Ihr IT-Sicherheitsniveau mit G DATA Advanced Analytics weiter erhöhen können? **Hier erfahren Sie mehr:**

gdata.de/business **info@gdata-adan.de** **0234 / 9762-820**

G DATA
advanced analytics