Kracht wehrt Cyber-Angriff ab: Forensik-Team von Bechtle stellt IT wieder her.

Die Kracht GmbH in Werdohl ist ein führender deutscher Technologieanbieter für Pumpen, Fluidmessungen, Ventile, hydraulische Antriebe und kundenspezifische Systemlösungen. Rund 450 Mitarbeitende weltweit konstruieren, produzieren und vertreiben die Produkte. Im Februar 2022 attackierten Unbekannte das Unternehmen und brachten wichtige Systeme zum Stillstand. Mithilfe des Forensik-Teams von Bechtle, das sich auf Cyber-Angriffe und deren Behebung spezialisiert hat, war Kracht nach nur sieben Tagen wieder voll einsatzbereit. Bechtle sicherte dazu die Daten, erstellte ein forensisches Image und setzte das gesamte IT-System neu auf.

PROJEKTDATEN

- **Services**
  IT-Security
- **Branche**
  Fertigung/Prod. Gewerbe
- **Hersteller**
  Microsoft, Fujitsu, Sophos
- **Unternehmensgröße**
  > 450 Mitarbeitende

TECHNOLOGIE

- Cybereason
- Microsoft 365
- Fujitsu Server und Storage
- Sophos Intercept
- Sophos Firewall

UNSERE PARTNER

FUJITSU

Microsoft

SOPHOS

„Der Worst Case trat bei uns ein, als es Unbekannten gelang, die hohen Sicherheitsstandards unseres Unternehmens zu überwinden. Bechtle war mit seinem Forensik-Team sofort zur Stelle, handelte extrem bedacht und wusste, was zu tun war. So wurden keine übereilten Entscheidungen getroffen. Auf die Erpressung der Täter wollten wir nicht eingehen. Stattdessen setzte Bechtle mit uns gemeinsam innerhalb von nur sieben Tagen – und ebenso vielen Nachtschichten – das gesamte System neu auf. Das war wirklich beeindruckend.“ **Peter Schilg,** Leiter IT, Kracht GmbH

HERAUSFORDERUNG. Das mittelständische Familienunternehmen Kracht GmbH hat in über 100 Jahren viel erreicht. Vom Standort Werdohl aus treiben die Ingenieure des Maschinenbauers mit ihren Entwicklungen Innovationen voran und beeinflussen technische Revolutionen. Aus dem vollautomatischen Logistikzentrum und dem hochmodernen Maschinenpark werden hochwertige Technologien in den Bereichen Pumpen, Fluidmessungen, Ventile, hydraulische Antriebe und kundenspezifische Systemlösungen hergestellt und weltweit vertrieben. Die Basis dafür: ein stabiles und sicheres IT-System. Das jedoch wurde im Februar 2022 Ziel unbekannter Angreifer. Ihnen gelang es, die bestehenden hohen Sicherheitsstandards des Unternehmens zu überwinden, mit einer Verschlüsselungstechnologie wichtige Systeme zu blockieren und dadurch die Arbeit des Unternehmens zu verlangsamen. Die Täter forderten eine Kontaktaufnahme, um Geldforderungen zu übermitteln. Kracht ging darauf allerdings nicht ein, sondern kontaktierte umgehend den langjährigen IT-Partner Bechtle, um das Problem systematisch und überlegt, dabei aber auch schnell und effizient anzugehen.

LÖSUNG. Die Bechtle eigene Forensik-Abteilung hat sich auf derartige Angriffe spezialisiert. Zusammen mit einer von Bechtle binnen kürzester Zeit gebildeten Taskforce nahm das Forensik-Team noch am selben Morgen die Arbeit in den Räumlichkeiten von Kracht auf. Durch die langjährige Kundenbeziehung kannte Bechtle die IT-Infrastruktur und Kracht vertraute der Arbeit von Bechtle. Unnötige Unruhe oder ungenaues Arbeiten unter Druck kamen dadurch gar nicht erst auf. Das Forensik-Team handelte überlegt und sicherte zunächst die digitalen Spuren für die forensische Untersuchung. Der Zugangsweg der Cyber-Kriminellen war schnell identifiziert: Durch eine professionell aufgesetzte E-Mail hatten sie sich gezielt Zutritt zur Serverstruktur von Kracht verschafft. Um das IT-System von Kracht schnell wiederherzustellen, exportierte und sicherte das Forensik-Team von Bechtle alle relevanten Daten. Der Maschinenbauer war gut auf einen solchen Vorfall vorbereitet: Es gab ein aktuelles, gehärtetes Backup, auf das niemand von außen zugreifen konnte. Diese Backupdaten waren tagesaktuell und sauber. Bechtle hat jahrelange Erfahrung darin, verschlüsselte Systeme neu aufzubauen, und nutzt dazu einen internen Notfallplan. Kracht hatte bereits selbstständig alle Systeme vom Netz getrennt.

Bechtle schuf eine grüne Zone. In den sauberen, autarken Bereich wurden nur bereinigte und als gut befundene Daten wieder integriert. Bechtle sicherte dort die Exchange Postfächer, alle nicht verschlüsselten Daten und nach dem „Waschen" durch entsprechende Prüfverfahren und Sicherheitswerkzeuge auch die Nutzerdaten. Parallel arbeiteten die Fachkräfte am Neuaufbau der bestehenden Netzwerkinfrastruktur. Die zufällig einige Wochen zuvor bestellten neuen Server und Storage von Fujitsu waren bereits eingetroffen. Bechtle baute darauf die ESX Server von VMware und die Domänenstruktur neu auf, installierte Exchange und die Fileserver und zusammen mit Mitarbeitenden von Kracht konfigurierte das Team die Thin Clients über ein Master-Image neu. Mithilfe einer Kommunikationsmatrix ließ Bechtle nur noch Kommunikation der internen Netzwerkzonen über benötigte Ports zu. Die vor dem Angriff eingesetzte Sophos Firewall und Sophos Central konfigurierte Bechtle neu, passte das Regelwerk an und sicherte mit Cybereason die gesamte Umgebung zusätzlich neu ab. So kann Kracht jetzt potenzielle Risiken in Echtzeit erkennen und dagegen vorgehen. Nach nur sieben Tagen, die Kracht und Bechtle 24/7 daran arbeiteten, ging die neu aufgesetzte grüne Zone online. Es folgten die Neueinrichtung der Citrix Server für den digitalen Arbeitsplatz und deren Absicherung. Schließlich passte Bechtle noch die gesamte Microsoft 365-Umgebung den neuen Gegebenheiten an: Azure Connect, Exchange Hybrid, Intune und Conditional Access installierte Bechtle neu und band sie an die bestehende Serverstruktur an.

VORTEILE/NUTZEN. Nach dem Cyber-Angriff konnte Kracht dank Bechtle innerhalb weniger Tage die Arbeit mit einer sauberen IT-Infrastruktur in gewohnter Effizienz wieder aufnehmen. Innerbetrieblich hatte Bechtle dabei die gesamte IT von Kracht überprüft und stellte sie nach neuesten Standards optimiert und sicher auf. So ist der Maschinenbauer bestens vor krimineller Energie gegenüber der IT geschützt. Weiterhin wachsam ist Kracht dennoch, denn niemand ist – egal, wie hoch die Sicherheitsstandards auch sind – vor Cyber-Attacken gefeit. Mit passenden Tools wie Cybereason ist Kracht jetzt allerdings den Angreifern immer einen Schritt voraus.

Weitere Informationen:

bechtle.com

KRACHT®
FLUID TECHNOLOGY AND SYSTEMS

Die Kracht GmbH in Werdohl ist ein weltweit aktives mittelständisches Familienunternehmen mit rund 450 Mitarbeitenden. Neben dem vollautomatischen Logistikzentrum verfügt das mehr als 100 Jahre bestehende Unternehmen über einen hochmodernen Maschinenpark, in den fortlaufend investiert wird. Die Kernkompetenzen von Kracht liegen in der Entwicklung, Herstellung und im Vertrieb hochwertiger Technologien in den Bereichen Pumpen, Fluidmessungen, Ventile, hydraulische Antriebe und kundenspezifische Systemlösungen. Der hohe Qualitätsanspruch bildet dabei das Fundament für den Erfolg der breiten und tiefen Produktpalette. **kracht.eu**