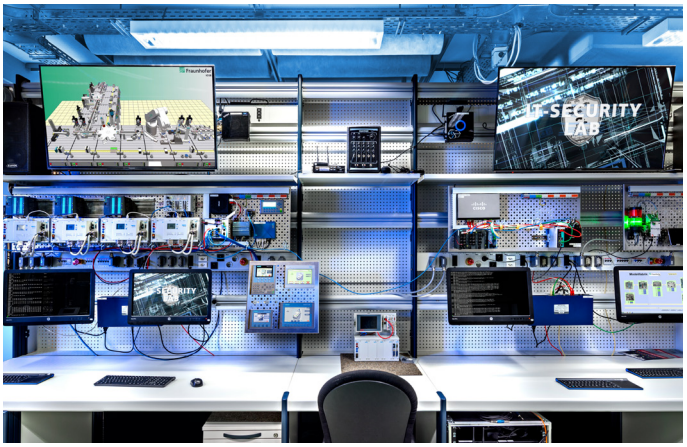
Überraschungsangriff auf die IT



Ausgangssituation

Das aus Sicherheitsgründen anonymisierte Unternehmen wurde Opfer eines professionell durchgeführten Verschlüsselungsangriffs mittels Ransomware, der die Geschäftsprozesse des Unternehmens vollständig zum Erliegen brachte. Der Notruf an eine staatliche Stelle erfolgte über das Handy des Geschäftsführers, da die gesamte Kommunikationsinfrastruktur zusammengebrochen war. Die auf Zulieferung von Daten angewiesene Produktion kam innerhalb von kurzer Zeit in erheblichem Umfang zum Erliegen. Die Angreifer haben sich höchstwahrscheinlich bereits im Vorfeld weitreichenden Zugang zum Netzwerk der Firma verschafft, was durch eine fehlende Segmentierung (logische Trennung in unterschiedliche Netzwerke) erheblich erleichtert wurde. So war es den Angreifern auch möglich, NAS- (Network Attached Storage) Systeme in den Auslieferungszustand zurück zu versetzen, was eine vollständige und unwiederbringliche Löschung der Backups zur Folge hatte.

Was ist die Lösung?

Das betroffene Unternehmen konnte mit Hilfe einer staatlichen Stelle, bei gleichzeitiger Unterstützung eines ausgewählten IT-Dienstleisters, den Angreifer im System isolieren und parallel eine neue Infrastruktur aufbauen. Nachdem zuerst die Kontaktaufnahme mit dem IT-Sicherheitsdienstleister sowie einem Fortbildungsdienstleister, der sich auf Informationssicherheit spezialisiert hat, erfolgt war, konnte zeitnah die Einführung eines Informationssicherheitsmanagementsystems (ISMS) nach der ISO 27001 etabliert werden. Parallel dazu wurden diverse Bausteinen aus dem IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI) implementiert. Nach Evaluierung eines erheblichern Schadens, hat sich das Unternehmen dazu entschieden, in Zukunft mehr Ressourcen in die Generierung eines adäquaten Sicherheitsniveaus zu investieren. Ein wichtiger Baustein war hierbei die Einbindung der Belegschaft bei der Umsetzung der Maßnahmen. Es musste ein Risikobewusstsein auf allen Ebenen geschaffen werden. Informationssicherheit soll künftig als wesentlicher Faktor in allen Geschäftsprozessen mitgedacht werden.
Die Implementierung der verschiedenen Sicherheitsmaßnahmen (ISO 27001, IT-Grundschutz, Fortbildungen, etc.) gestalteten sich grundsätzlich gut, da das Management die entsprechenden materiellen und administrativen Ressourcen bereitstellte.

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Mit dem IT-Grundschutzkompendium haben Unternehmen aus diversen ökonomischen Segmenten und unterschiedlicher Größen die Möglichkeit individuelle Maßnahmen umzusetzen.

Vorteile

Die durchgeführten Maßnahmen konnten das Risiko, erneut Opfer eines Angriffs zu werden, welcher einen Totalverlust als Folge hat, erheblich reduzieren. Außerdem konnte das Unternehmen durch eine gute Kommunikationskampagne das Vertrauen vieler Kunden, welche von dem Vorfall betroffen waren, zurückgewinnen.

Kurz und Knapp

Jedes Unternehmen kann zur Zielscheibe von Cyberangriffen werden. Wichtig sind eine Sensibilisierung der Mitarbeiter und die rechtzeitige Einführung von Sicherheitsmaßnahmen.
Eine wichtige Erkenntnis durch einen Vergleich mit anderen betroffenen mittelständischen Unternehmen ist, dass in vielen Fällen die Abhängigkeit von Geschäftsprozessen von der IT auch von Seiten der Geschäftsführung unterschätzt wird.

Haben auch Sie Ideen oder Fragen zur Digitalisierung, dann wenden Sie sich an uns!

Ihre Ansprechpartner

Mittelstand 4.0-Kompetenzzentrum Stuttgart

Jan Herrmann / Themenfeldleitung Gebäude
BWHM GmbH
Heilbronner Str. 43
70191 Stuttgart
jherrmann@handwerk-bw.de

David Ruge / Themenfeld IT-Sicherheit
FZI Forschungszentrum Informatik
Außenstelle Berlin
Friedrichstr. 60
10117 Berlin
ruge@fzi.de

Das Projekt Mittelstand 4.0-Kompetenzzentrum Stuttgart ist Teil des Förderschwerpunkts „Mittelstand-Digital – Strategien zur digitalen Transformation der Unternehmensprozesse“, der vom Bundesministerium für Wirtschaft und Energie (BMWi) initiiert wurde, um die Digitalisierung in kleinen und mittleren Unternehmen und im Handwerk voranzutreiben.
Weitere Informationen zum Förderschwerpunkt finden Sie unter **mittelstand-digital.de**
Alle Praxisbeispiele finden Sie unter **digitales-kompetenzzentrum-stuttgart.de/praxisinformationen/**

Impressum

Herausgeber und Redaktion
Mittelstand 4.0-Kompetenzzentrum Stuttgart c/o
Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO
Nobelstraße 12, 70569 Stuttgart
Bildnachweis: © Fraunhofer IOSB/indigo

Rechtsform
Das Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO ist eine rechtlich nicht selbstständige Einrichtung der Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.
Stand: Dezember 2019

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages