Umfassende 24/7-IT-Security mit SOCaaS

Dank FortiGuard SOCaaS profitiert das Unternehmen Götz Elektro AG von Cybersecurity auf Enterprise-Niveau – zu KMU-Konditionen.

Beim Elektrobetrieb Götz Elektro ist es vor einiger Zeit zu einer Ransomware-Attacke gekommen. Dabei gelang es den Angreifern, wichtige Daten zu verschlüsseln. Betroffen waren allerdings nur die produktiv genutzten Daten. Das Backup in der Cloud konnte von den Angreifern nicht verschlüsselt werden.

Damit es bei Götz Elektro nie mehr zu einem erfolgreichen Cyberangriff kommen kann, setzt der neue ICT-Partner Tessera ICT auf die Managed-Security-Service-Lösung FortiGuard SOC as a Service (SOCaaS) von Fortinet. Diese sorgt für die zeitnahe Erkennung, Analyse und Abwehr von Bedrohungen.

Höchste IT-Sicherheit ist für Götz Elektro essenziell, denn das Unternehmen ist vollständig digitalisiert.

Zunehmende Risiken

Bekanntermassen entwickelt sich die Cyberbedrohungslage rasant. Vor diesem Hintergrund genügt es nicht mehr, auf Cyberangriffe zu reagieren – vielmehr müssen entsprechende Attacken möglichst sofort erkannt werden, idealerweise noch, bevor sie ihre zerstörerische Wirkung entfalten können. Rolf Neff, ICT-Spezialist bei Tessera ICT, bringt es auf den Punkt: «Heute muss man präventiv unterwegs sein. Nur wenn wir Bedrohungen früh erkennen, können wir verhindern, dass es wieder zu erfolgreichen Angriffen kommt.» Demnach ist es laut Neff wichtig, dafür zu sorgen, dass Angriffe wirksam und rund um die Uhr abgewehrt werden. «Dies setzt eine kontinuierliche Überwachung des gesamten Netzwerks voraus – besonders dann, wenn in einem Unternehmen wie bei Götz Elektro auch webbasierte Dienste und SaaS-Anwendungen genutzt werden.»

KMU-taugliche Cybersecurity-Lösung auf Enterprise-Niveau

Kontinuierliches Monitoring und automatisierte Bedrohungserkennung rund um die Uhr während 365 Tagen im Jahr, wie sie in Grossunternehmen von einem Security Operations Center (SOC) geleistet werden, sind weder von einem KMU-Betrieb noch von einem lokalen IT-Dienstleister ohne übermässigen Aufwand zu stemmen – von den Kosten ganz zu schweigen. Doch dank der Managed-Security-Service-Lösung FortiGuard SOC as a Service (SOCaaS) von Fortinet können sowohl das betroffene Unternehmen als auch sein IT-Partner von entsprechenden Services des renommierten Cybersecurity-Anbieters Fortinet profitieren.

Security Operations Center fast ohne Eigenaufwand

FortiGuard SOCaaS ist ein schlüsselfertiger, cloudbasierter Managed Security Service, mit dem sich Sicherheitsbedrohungen im Netzwerk rasch und konsequent feststellen lassen. Der Dienst basiert auf der Fortinet Security Fabric, die in eine zentral verwaltete SOC-Plattform eingebettet ist und Log-Daten rund um die Uhr überwacht und analysiert – dies unterstützt durch Machine Learning und künstliche Intelligenz. Wird eine Sicherheitsbedrohung festgestellt, informiert Fortinet je nach Bedarf schnellstmöglich den Endkunden oder dessen IT-Partner und liefert eine auf die Situation abgestimmte Handlungsempfehlung.

Der SOC-Dienst erstellt zudem regelmässige Berichte über Warnmeldungen, Benachrichtigungen, neu erfasste Geräte im Netz, Statusänderungen und Tickets, die über das Serviceportal generiert und gemeldet wurden. Nachdem ein Sicherheitsvorfall klassifiziert und bestätigt wurde, eröffnet der Dienst ein Security Incident Ticket und erstattet je nach Schweregrad des Vorfalls in abgestuften Intervallen Meldungen per E-Mail und im Fall kritischer Vorfälle auch per Telefon.

Über das entsprechende Serviceportal, das wahlweise vom Kunden oder vom IT-Partner genutzt werden kann, stehen auch die SOC-Analysten von Fortinet für Interaktionen zur Verfügung. Im Fall von Götz Elektro übernehmen die Spezialisten von Tessera ICT die Kommunikation mit dem SOC-Dienst – seitens Götz Elektro fällt praktisch kein Aufwand an.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58 I 5430 Wettingen
Tel. 056 437 60 60 I info@boll.ch I boll.ch