GRADION
scaling business

FERTIGUNG · CYBERSECURITY

Ein britischer Möbelhersteller wehrt einen aktiven Cyberangriff ab und lässt seine gesamte IT-Infrastruktur von Gradion auf Schwachstellen prüfen und absichern

Aktive Cyberangriffe abgewehrt, sämtliche Schwachstellen in der IT-Infrastruktur identifiziert und ohne Datenverlust geschlossen.

KUNDE	VON	STATUS
Britischer Möbelhersteller	**Gradion**	**Laufend**

Kundenkontext

Ein etablierter britischer Hersteller von Gartenmöbeln und industriellen Werkbänken aus Holz bedient sowohl den privaten als auch den gewerblichen Markt. Für den laufenden Betrieb ist das Unternehmen auf digitale Auftragsverwaltung, Kundendatensysteme und eine funktionierende IT-Infrastruktur angewiesen.

Die Herausforderung

Zum Zeitpunkt der Beauftragung war der Hersteller mit aktiven Cyberangriffen konfrontiert. Bedrohungsakteure hatten versucht, interne Daten zu stehlen, Bestelldatensätze zu manipulieren und die IT-Infrastruktur zu sabotieren. Unklar war, ob diese Versuche bereits erfolgreich gewesen waren oder ob es bereits zu einem Sicherheitsvorfall gekommen war. Es brauchte Klarheit: Waren Daten kompromittiert, Bestell- oder Zahlungsdatensätze verändert worden, oder war die Infrastruktur noch unberührt? Gleichzeitig mussten sämtliche ausnutzbaren Schwachstellen identifiziert und geschlossen werden, bevor die Angreifer zurückkehren oder ihre Angriffe ausweiten konnten. Für einen Hersteller reichen die Folgen eines erfolgreichen Angriffs über den Datenverlust hinaus: Manipulierte Bestellungen stören die Produktionsplanung und die Kundenbeziehungen, eine sabotierte IT-Infrastruktur kann den Betrieb zum Stillstand bringen. Gefragt waren deshalb sowohl die Eindämmung des akuten Vorfalls als auch eine dauerhafte Verbesserung der Sicherheit.

Der Ansatz

Gradion begann mit einer sofortigen Reaktion auf den Vorfall: einer schnellen Bewertung der aktiven Bedrohungslage, um festzustellen, was angegriffen worden war, welche Methoden die Angreifer eingesetzt hatten und ob es zu einem Sicherheitsvorfall gekommen war. Im Anschluss folgte ein vollständiger Penetrationstest mit Schwachstellenanalyse der gesamten IT-Infrastruktur und der geschäftskritischen Systeme des Herstellers - darunter die Plattform zur Auftragsverwaltung, die Kundendatenumgebung sowie die IT-Systeme, die die Angreifer zuvor ausgekundschaftet hatten. Alle dabei entdeckten Schwachstellen und Fehlkonfigurationen, die die Angriffsversuche ermöglicht hatten, wurden behoben. Ergänzend setzte Gradion umfassende Maßnahmen zur Absicherung der Infrastruktur um, um die Angriffsfläche zu verringern und die Widerstandsfähigkeit des Herstellers gegenüber künftigen Bedrohungen zu stärken.

Ergebnisse

Die Untersuchung bestätigte: Die Angreifer waren nicht in das System eingedrungen. Es wurden keine Daten entwendet, keine Datensätze verändert und kein dauerhafter Zugriff eingerichtet - eine forensische Untersuchung des Vorfalls bestätigte, dass es zu keinem Datenverlust kam. Der Fertigungsbetrieb lief während des gesamten Einsatzes ohne Unterbrechung weiter. Sämtliche kritischen Schwachstellen, die der Penetrationstest aufgedeckt hatte, wurden geschlossen, und die umgesetzten Sicherheitshärtungsmaßnahmen verringerten die Angriffsfläche in der gesamten IT-Infrastruktur. Insgesamt ist der Hersteller künftigen Angriffsversuchen dadurch deutlich besser gewachsen. Eine Stellungnahme eines Vertreters des Unternehmens kann auf Anfrage bereitgestellt werden; der Einsatz war zum Zeitpunkt der Beschreibung noch laufend.

Leistungen & Methodik

Leistung
Reaktion auf Cybervorfälle
Penetrationstests
Schwachstellenanalyse und -behebung
Sicherheitshärtung
Forensische Vorfalluntersuchung
Überprüfung der IT-Infrastruktursicherheit

Eingesetzte Methodik

- Vollumfängliche Penetrationstest-Methodik
- Schwachstellenscans der IT-Infrastruktur
- Sicherheitsbewertung der Bestell- und Datensysteme
- Sicherheitshärtung und Behebung von Fehlkonfigurationen

Engagement-Modell: Sicherheitseinsatz mit Vorfallreaktion und Behebung.

GRADION
scaling business

Aktive Bedrohung, offene Fragen? Gradion schafft Klarheit und schließt Sicherheitslücken.

Sprechen Sie mit unseren Sicherheitsexperten über Ihre IT-Infrastruktur.

23
Jahre Erfahrung

ISO
27001 · Gradion Pte. Ltd.

3
Regionen: DACH, SEA, Afrika

Kontakt: sales@gradion.com

bsi. ISO/IEC 27001 Information Security Management

Gradion Pte. Ltd. (Singapur) ist ISO/IEC 27001-zertifiziert · Zertifikat-Nr. IS 824945