NACHRICHTEN AG

10. Juni 2025

Hackerangriff auf Arcona: Hotels in Rostock und Rügen betroffen!

Hotelgruppe Arcona in Rostock Ziel eines Cyberangriffs durch die Hackergruppe Akira; IT-Sicherheitsfirma untersucht Vorfall.

Rostock, Deutschland - Die Hotelgruppe Arcona hat einen schwerwiegenden Hackerangriff öffentlich gemacht, der mehrere ihrer Einrichtungen in Mitleidenschaft gezogen hat. Betroffen sind drei Hotels, darunter das Vju und Koopmanns auf Rügen sowie das Hotel Elephant in Weimar, sowie die zentrale Verwaltung in Rostock. Dieser Vorfall wurde am 23. Mai 2025 ausgetragen, als die kriminelle Cyber-Gruppe Akira in die Systeme eindrang. Experten von der IT-Sicherheitsfirma ResponseOne haben den Vorfall mittlerweile untersucht, um die genauen Umstände zu klären.

Die Ursachen des Angriffs sind besorgniserregend, denn die Angreifer konnten aufgrund fehlerhafter Netztrennung zwischen

den Unternehmensstandorten ungehindert agieren. Es bleibt jedoch unklar, wie genau Akira in die Systeme eindringen konnte. Laut dem Landeskriminalamt wird dieser Angriff als Teil einer größeren Bedrohung im digitalen Raum analysiert.

Akira: Eine wachsende Bedrohung

Akira ist seit 2023 im Darknet aktiv und hat sich schnell einen Namen gemacht, indem sie Erpressersoftware einsetzt, um Unternehmen unter Druck zu setzen. Im Falle von Arcona wurde berichtet, dass Daten gestohlen wurden; die genaue Art dieser Daten ist jedoch noch unbekannt. Akira hat eine Nähe zu Russland und wird als eine der fünf gefährlichsten Hacker-Gruppen weltweit angesehen, mit über 60 erfolgreichen Angriffen auf kleine und mittelgroße Unternehmen.

Ziele solcher Angriffe sind nicht nur Finanzdaten, sondern auch kritische Informationen, die in der heutigen digitalen Welt von hohem Wert sind. Arcona-Chef Alexander Winter äußerte sein Bedauern über diesen Vorfall und das mögliche Ausmaß des Datenabflusses. Die Bedrohung durch Cyberangriffe hat sich mittlerweile als die größte Gefahr für Unternehmen in Deutschland etabliert, wie die Allianz Risk Barometer 2025 feststellt.

Cyberangriffe: Eine Zunahme der Bedrohung

Cyberkriminelle, wie die Gruppe Akira, agieren häufig ähnlich wie Unternehmen und nutzen ein Geschäftsmodell namens Ransom as a Service (RaaS). Dies bedeutet, dass sie sich auf den Datenschutz und die Systeme von Unternehmen spezialisiert haben, um durch gezielte Angriffe erhebliche Summe zu erpressen. Berichten zufolge könnte das geforderte Lösegeld für den Angriff auf Arcona in die Hunderttausende gehen, obwohl keine offiziellen Angaben diesbezüglich vorliegen.

Die Herausforderungen für Unternehmen wie Arcona, sich gegen solche Angriffe zu wappnen, sind enorm. Sicherheitsteams kämpfen damit, ihre IT-Systeme zu schützen, da Angreifer oft nur eine Schwachstelle ausnutzen müssen. Die Einführung von Multi-Faktor-Authentifizierung (MFA) und die Implementierung effektiver Sicherheitsstrategien sind entscheidend, um solche Vorfälle zu verhindern. Zudem ist eine Schulung des Sicherheitsbewusstseins innerhalb der Belegschaft erforderlich, da menschliche Fehler oft zu Sicherheitsverletzungen führen.

Obwohl Arcona und andere Unternehmen derzeit Maßnahmen zur Schadensbegrenzung ergreifen, bleibt die Frage offen, wie die Gefahren im Cyberraum langfristig eingedämmt werden können. Die Zeit wird zeigen, wie sich die Lage entwickelt und welche weiteren Maßnahmen ergriffen werden müssen, um das Vertrauen in digitale Geschäftsprozesse zurückzugewinnen.

Die aktuellen Entwicklungen unterstreichen die Dringlichkeit, in Cybersicherheit zu investieren, insbesondere in einer Zeit, in der Cybervorfälle die größte Bedrohung für Unternehmen darstellen.

Details	
Vorfall	Cyberkriminalität
Ursache	Hackerangriff
Ort	Rostock, Deutschland
Quellen	• **www.mopo.de** • **www1.wdr.de** • **www.computerweekly.com**