

Ransomware-Angriff bei der GWG Wohnungsbaugesellschaft: Cybercrime kommt in der Mitte der Gesellschaft an

Bochum (Deutschland), 19 November 2020

Wie gestern bekannt wurde, ist die Münchener GWG Wohnungsbaugesellschaft Opfer eines Ransomware-Angriffs geworden. Ein Großteil der IT-Systeme und Daten des Unternehmens ist betroffen, sogar Backup-Server und anderweitige Datensicherungen wurden im Zuge des Angriffs verschlüsselt. Wie immer bei solchen Attacken gaben die Hacker an, die Daten nur nach Zahlung eines Lösegelds wieder zu entschlüsseln.



Vorfälle wie diese treten immer wieder auf und insbesondere die derzeitige Krisensituation mit all ihren Folgen hat für ein Ansteigen sämtlicher Arten von Cyber-Angriffen gesorgt. Viele Organisationen haben zwecks Risikominimierung ihre Belegschaft ins Homeoffice geschickt. Die Folge: Die alltägliche Kommunikation zwischen Kollegen findet nicht mehr in der gewohnten Form statt. Dies nutzen Kriminelle gezielt aus und setzen auf raffinierte Social-Engineering-Methoden, um ihre Opfer zu unüberlegten Handlungen zu bringen, etwa auf einen Link in einer Mail zu klicken oder vertrauliche Daten herauszugeben.

Die [aktuelle Bedrohungsanalyse](#) von G DATA CyberDefense zeigt: Die Anzahl der abgewehrten Cyber-Angriffe hat sich in Folge der Krise vom zweiten zum dritten Quartal hin fast verdoppelt. Die Konsequenzen einer erfolgreichen Attacke können, wie im aktuellen Fall, für betroffene Organisationen verheerend sein. In einer Welt, in der immer mehr Lebensbereiche digitalisiert werden und vom Internet aus erreichbar sind, stellen Cyber-Angriffe eine unmittelbare Gefahr dar.

„Der aktuelle Vorfall bei der Wohnungsbaugesellschaft zeigt: Cybercrime kommt der Lebenswelt der Menschen immer näher. Wenn immer mehr Geräte, wie etwa Heizungssteuerungen, für Effizienzgewinne an das Internet angeschlossen werden steigt zugleich das Risiko für erfolgreiche Angriffe. Bereits im Jahr 2016 fiel in einer Wohnanlage in Finnland mitten im Winter für mehrere Tage die Heizung aus, nachdem ein Denial-of-Service-Angriff die Steuerungsanlage lahmlegte. IT-Sicherheit ist eine gesamtgesellschaftliche Aufgabe, bei der alle handelnden Akteure Verantwortung übernehmen müssen“, sagt Hauke Gierow, Head of Corporate Communications bei G DATA CyberDefense.

G DATA CyberDefense AG Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299

Um auch in Krisenzeiten weiterhin den normalen Geschäftsbetrieb gewährleisten zu können, müssen Unternehmen der IT-Sicherheit der ihr angemessene Bedeutung beimessen. Zum einen gilt es, aktuelle Antiviren-Lösungen zu nutzen und sämtliche Geräte und Applikationen jederzeit auf dem neuesten Stand zu halten. Zum anderen müssen Mitarbeiter hinreichend über die Gefahren aufgeklärt sein, die im Zuge der Arbeit von zuhause auf sie zukommen können. Einfache Ratgeber und Merkzettel können einen ersten Schritt darstellen. Um Mitarbeiter jedoch ausreichend auf die Gefahren durch Social Engineering vorzubereiten, sollten Unternehmen sich mit dem Thema Cyber Awareness-Trainings auseinandersetzen. Durch regelmäßige (Online-)Schulungen können Risiken effektiv verringert werden – und die Geschäftsleitung sehen ihr eigenes Unternehmen nicht als Opfer eines Angriffs in der Zeitung.

Weitere Informationen zu diesen Themen und wie sich Unternehmen schützen können, gibt es unter: <https://www.gdata.de/tipps-tricks/arbeiten-im-homeoffice>

G DATA CyberDefense AG
Unternehmenskommunikation

G DATA CyberDefense AG

G DATA Campus

Königsallee 178

44799 Bochum

www.gdata.de

E-Mail: presse@gdata.de

Tel.: +49 (0) 234 9762-239

Fax: +49 (0) 234 9762-299