Szenario:
Cyberangriff auf Elektrizitätswerke Rheingau AG

Allgemeine Lage

Die Elektrizitätswerke Rheingau AG (RAG) ist der kantonale Stromversorger des Kantons Rheingau. Die Firma betreibt das kantonale Elektrizitätsnetz, Kunden sind einerseits kleinere Lokalwerke, welche dann den Endkunden bedienen, oder aber grössere Stromkunden, welche von der RAG direkt beliefert werden. Seit fünf Jahren ist die RAG auch noch ins Geschäft als Internet-Provider und Hoster eingestiegen. Die RAG verwaltet als grösster Webhosting-Provider im Kanton Rheingau über 75'000 Domainnamen und unterhält eine der modernsten und stabilsten Infrastrukturen. Zu den Kunden zählen auch grosse, unter anderem Postfinance, HP und Migros (inklusive dem «Le Shop»-Internet-Bestell- und Lieferservice) oder die E-Mail-Server der Schweizerischen Nationalbank. Sie präsentieren sich auf Ihrer Website wie folgt:

Sie sind Verantwortliche/r für Unternehmenskommunikation bei der RAG und in dieser Funktion Teil der fünfköpfigen Geschäftsleitung, die auch den Kern-Krisenstab der Firma bildet.

Besondere Lage

Sie erhalten heute um 0908 Uhr einen Anruf, dass es einen Cyberangriff auf das Unternehmen gab. Verschiedene Kunden haben sich über Unregelmässigkeiten auf ihren Websites beklagt, u.a. dass sie keinen Zugang mehr hätten auf Ihre E-Mail-Accounts. Sie würden Fehlermeldungen erhalten, dass das Passwort nicht korrekt sei, obwohl sie sicher wären, dass das Passwort stimmen würde. Nach Gesprächen mit den technischen Verantwortlichen steht die Vermutung im Raum, dass die Angreifer offenbar Login-Daten von eigenen «Domainhost»-Mitarbeitern abgreifen und sich so Zugang zu Kundendaten verschaffen konnten. Was erbeutet wurde und in welchem Umfang Daten abgegriffen wurden, ist noch nicht bekannt. Es muss aber mit einem sehr umfangreichen Datenabfluss gerechnet werden, der auch sensible Bereiche tangieren könnte. Wenig später, um 0917 Uhr, erscheint auf den Computer ihrer Verwaltung eine Anonymous-Maske und darunter der folgende Text:

«Wir haben Euch. Solltet Ihr nicht bis heute Mittag die Summe von CHF 1.5 Millionen in Bitcoin an Empfängeradresse 3JKr1213uKtMbymvtxtuea5twTKgniEp2h geschickt haben, werdet Ihr weitere Überraschung erleben!»

Die Mitarbeiter/innen in der Verwaltung melden, dass Sie keinen Zugriff mehr auf ihre Sharedrives hätten.

Weitere Informationen stehen Ihnen zurzeit nicht zur Verfügung.

Aufgabe:

1.) Überlegen Sie das Wording der ersten Stunde
2.) Erstellen Sie eine Problemerfassung für den gesamten Krisenstab