maz
KOMMUNIKATION

Szenario:
Cyberangriff auf Elektrizitätswerke Rheingau AG

Lageentwicklung

Die Abklärungen der technischen Abteilung haben Folgendes ergeben:

Die Vermutung hat sich bestätigt, dass die Angreifer Login-Daten von ihren Mitarbeitern abgreifen und sich so Zugang zu den Kundendaten verschaffen konnten. Wie Ihre Security herausgefunden hat, ist es den Angreifern gelungen, einen Software-Keylogger einzuschleusen. Dieser Trojaner war in eine Bilddatei eingebaut, die von einem gefälschten E-Mail-Account der Event-Agentur, welche vor einer Woche Ihr Teamfest organisiert hatte, an ihre Mitarbeiter/innen verschickt worden war. – Mit anderen Worten: Die Täter mussten über interne Abläufe Bescheid gewusst haben: Das Teamfest war ein interner Anlass für das Team und (wenige) externe Partner.

Über diesen Zugangsweg haben die Angreifer die die verschiedensten SQL-Datenbanken, welche Domainhost betreibt, Zugriff.

Unklar ist, ob es den Hackern gelungen ist, sämtliche Mitarbeiter-Logindaten zu entwenden oder nur die Daten von einzelnen Mitarbeiter/innen. Das ist deshalb von Relevanz, weil insbesondere die Administratoren nicht alle Dienste betreuen, sondern nach verschiedenen Arbeitsgebieten aufgeteilt sind: Die für E-Mail-Dienste beispielsweise sind andere Mitarbeiter/innen zuständig als für die gehosteten Webseiten.

Klar ist, dass persönliche Kundendaten wie Namen, verschlüsselte Passwörter, Adressen, E-Mail-Adressen, Geburtstage und Telefonnummern abgegriffen worden sind, die aus der zentralen Kundenverwaltung stammen, auf die praktisch alle Administrator/innen Zugriff haben. Mit Sicherheit betroffen sind auch die E-Mail-Dienste. Allerdings sind bei den E-Mail-Diensten die Login-Daten für jeden Kunden in einer eigenen SQL-Datenbank gespeichert. Und gegenwärtig ist noch nicht klar, ob alle diese Datenbanken abgegriffen wurden oder nur einzelne.

Wie viele Kunden betroffen sind, ist damit also noch unklar. Ebenso, ob sich die Angreifer Zugang zu den Webhosting-Services verschaffen konnten. – Falls ja, könnte nicht ausgeschlossen werden, dass sie dort Zugangsdaten zu Verwaltungsinstrumenten für online-Shops erbeuten konnten. Mit diesen Daten könnten sie beispielsweise Zahlungen in online-Stores auf ihre eigenen Bankkonten umleiten.

Die IT ist gegenwärtig der Meinung, dass die Hacker aufgrund der gewählten Angriffsmethode auf die Elektrizitätsleitstelle der RAG keinen Zugriff haben dürfte. – Würde es den Hackern allerdings gelingen, in die Systeme der Leitstelle einzudringen, könnten Sie dort die verschiedenen Schaltungen der Elektrizitätsleitungen manipulieren und letzten dem ganzen Kanton Rheingau ein Blackout bescheren.

Durch die verschiedenen betroffenen Kundinnen und Kunden haben unterdessen auch die Medien von den Schwierigkeiten der RAG Kenntnis erhalten. Sie haben verschiedene schriftliche Anfragen erhalten und das SCHWEIZER FERNSEHEN möchte für SCHWEIZ AKTUELL einen Beitrag realisieren.

Aufgabe:

1. Überlegen Sie, inwiefern die neue Entwicklung Einfluss auf Ihre Handlungen/Botschaften hat. Müssen Sie Ihr Wording ändern? Falls ja, was schlagen Sie dem Krisenstab vor?
2. Ihr Verwaltungsratspräsident, Nationalrat Hans Schlüter, möchte testen, ob Sie ausreichend gute Antworten auf kritische Medienfragen hätten und bittet Sie, eine Nasty Questions List zu erstellen und ein Probe-Interview durchzuspielen.