**Vorlagen für die Kommunikation zu einem Ransomware-Angriff**

**Phase 1: Information über den Cyberangriff**

**Interne Kommunikation**

Sehr geehrte / Liebe (NAME)

Am (TAG/DATUM) wurde die Unternehmung/Organisation (NAME) Opfer eines Ransomware-Angriffes, bei welchem die Systeme verschlüsselt wurden. Der zuständige IT-Dienstleister hat nach Absprache mit der Kantonspolizei die Systeme gemäss Notfallplan kontrolliert heruntergefahren. Wir haben alle notwendigen technischen Massnahmen zum Schutz der IT-Infrastruktur eingeleitet und mit der Wiederherstellung der Systeme begonnen.

Die Wiederherstellung der IT-Systeme wird mehrere Tage in Anspruch nehmen. Dies bedeutet auch, dass Sie in den nächsten Tagen keinen oder nur begrenzten Zugriff auf die Systeme der Unternehmung/Organisation haben. Dies hat möglicherweise Auswirkungen auf die Ausübung Ihrer Arbeitstätigkeit. Ihre Vorgesetzten werden sich mit Ihnen absprechen und organisieren. Aus gegebenem Anlass bitten wir Sie zudem, nicht auf (PORTAL/APPLIKATION) zuzugreifen.

Wir bedauern den Vorfall sehr und werden Sie weiterhin über/auf (KOMMUNIKATIONSKANAL) auf dem Laufenden halten. Bei Fragen können Sie sich jederzeit an (NAME/MAIL oder TEL) wenden. Leiten Sie bitte allfällige Medienanfragen an (PERSON/E-MAIL) weiter und beantworten Sie die Anfrage nicht selber. Herzlichen Dank für Ihre Mithilfe.

**Externe Kommunikation**

***Titel: Cyber-Angriff auf die Unternehmung/Organisation (NAME)***

**Die Unternehmung/Organisation (NAME) wurde am XX.YY.20XX Opfer eines Cyber-Angriffes. Der Vorfall wurde am (DATUM) entdeckt. Massnahmen, um den Angriff abzuwehren und einzugrenzen wurden umgehend ergriffen. Der Vorfall wurde dem Bundesamt für Cybersicherheit (BACS) gemeldet. Zudem hat die Unternehmung/Organisation bei der Kantonspolizei Strafanzeige erstattet. Im Rahmen dieses Angriffs kam es zu einer Verschlüsselung der Daten.**

*Ort, Datum –* Bei einem Angriff auf die IT-Systeme der Unternehmung/Organisation (NAME) am XX.YY.20XX blockierten die Angreifer den Zugang zu mehreren Systemen und forderten ein Lösegeld. Der zuständige IT-Dienstleister hat in Absprache mit der Kantonspolizei die nötigen technischen Massnahmen zum Schutz der IT-Infrastruktur eingeleitet und mit der Wiederherstellung der Systeme begonnen. Aufgrund des Vorfalles ist der Zugriff auf die Webseite derzeit und in den kommenden Tagen nicht oder nur teilweise gewährleistet.

Die Unternehmung/Organisation (NAME) geht auf die Lösegeldforderung nicht ein. Derzeit steht noch nicht fest, ob und in welchem Ausmass möglicherweise sensible Daten kompromittiert und gestohlen wurden. Aufgrund der aktuell laufenden Untersuchungen kann sich die Unternehmung/Organisation (NAME) nicht weiter zum Fall äussern. Betroffene Kunden werden direkt informiert, damit diese ihrerseits allfällig notwendige Massnahmen ergreifen können.

Die Unternehmung/Organisation (NAME) bedauert den Vorfall und die verbundenen Unannehmlichkeiten sehr.

Die Unternehmung/Organisation wird über neue Erkenntnisse informieren und eine Aktualisierung auf (URL) veröffentlichen.

Ansprechperson für Medien

Vorname Name, Funktion, Abteilung, Telefon, E-Mail-Adresse