



KOMMUNIKATION VON SICHERHEITSVORFÄLLEN

INFORMATIONEN ZUR VORBEREITUNG DER EXTERNEN KOMMUNIKATION
IM KRISENFALL

Version 1.1 vom: 12.09.2024

Management Summary

Im Falle eines Sicherheitsvorfalls sollten Sie auf eine vorbereitete Kommunikationsstrategie zurückgreifen können, um nicht unter Zeitdruck eventuell fehlerbehaftete Meldungen für die Öffentlichkeit verfassen zu müssen. Die Kommunikation mit Presse, Bürgern und Mitarbeitern sollte rechtzeitig erfolgen können und die Inhalte sollten gezielt und mit angemessener Präzision bedacht sein. Ziel einer vorbereiteten Kommunikationsstrategie ist es weiterhin, Reputationsschädigung und Spekulationen zu vermeiden.

🔗 Planung Ihrer Kommunikationsstrategie

Diese LSI-Info soll Ihnen helfen, eine geeignete Kommunikationsstrategie bei IT-Sicherheitsvorfällen für die Information der Öffentlichkeit vorzubereiten. Gesetzliche Meldepflichten und Meldewege sind separat zu betrachten. Bei Ihren Vorüberlegungen sollten Sie folgende Aspekte berücksichtigen, um den Informationsfluss zu steuern:

- Wer ist auskunftsberechtigt gegenüber externen Stellen und Presse?
- Was sind geeignete Kanäle für die Information der Öffentlichkeit (z.B. Pressemitteilung, Homepage Ihrer Gemeinde, falls vorhanden Social Media Account Ihrer Gemeinde)

Im Folgenden finden Sie grundlegende Textbausteine, die Sie für die Ausarbeitung von Vorlagen gerne verwenden können. Sie beziehen sich auf drei Kommunikationsanlässe:

- Information der Öffentlichkeit über die Beeinträchtigung der Verfügbarkeit
- Information der Mitarbeiter
- Aufklärung mit Pressearbeit nach erfolgter Analyse und Problembehebung

🔗 Basis-Schemata für externe Kommunikation über eigene Kanäle und Pressemitteilungen

Zu einem professionellen Krisenmanagement gehört es, die betroffenen Bürger möglichst zeitnah über die Beeinträchtigung der von Ihrer Gemeinde angebotenen Dienste zu informieren.

Folgende Informationen sollten Sie in die externe Kommunikation aufnehmen:

- Bis wann wird die Verwaltung der Gemeinde voraussichtlich nicht erreichbar sein?
- Betrifft der Ausfall die gesamte Verwaltung und damit alle Dienste oder nur bestimmte Verfahren (Dienste) oder bestimmte Kanäle (z.B. Mail)?
- Wer ist Ansprechpartner für externe Anfragen (z.B. von der Presse)?
- Wann / Wie ist eine weitere Information der Öffentlichkeit geplant?

Sie sollten vermeiden, unsichere und vage Informationen in die erste Meldung aufzunehmen, wenn sich das vermeiden lässt, um Spekulationen vorzubeugen. Namen von Angreifer-Gruppen sollten nicht in die Meldung mit genannt werden.



Beispiel:

Aufgrund einer Störung der IT-Systeme der GEMEINDE MUSTER, sind wir für unsere Bürger und andere Stellen voraussichtlich bis TAG X nicht erreichbar / nur telefonisch erreichbar. Wir arbeiten mit Hochdruck an der Analyse der Ursachen und der Problembehebung.

Ansprechpartner:
Fr. Musterfrau
Tel. 0888/123-123

Optional:
Weitere Informationen werden wir im Laufe des nächsten Arbeitstages veröffentlichen und einen öffentlichen Informationstermin / Pressekonferenz festsetzen / Pressemitteilung veröffentlichen. Bis dahin bitten wir auf Rückfragen zu verzichten bis Analyse und Problembehebung abgeschlossen sind.

Bei Teilausfall sollten zusätzlich folgende Punkte berücksichtigt werden:

- o Welche Dienste sind betroffen? Wie lange werden diese voraussichtlich ausfallen? (ggf. nur Mail/Website betroffen, ggf. nur bestimmte Verfahren betroffen)
- o Welche Dienste werden noch über welchen Kanal angeboten? Z.B. Bürger-Hotline

Beispiel für Meldung auf der Homepage:

AKTUELLES

Bürgermeister@Mustergemeinde - 25.7.2019

Achtung: Am Freitag, den 26.7.2019 bleibt das Rathaus geschlossen. Auch eine telefonische Erreichbarkeit ist nicht gegeben.

Wie kann eine interne Information an Mitarbeiter aussehen?

Betreff: Dringend - Bitte unverzüglich lesen!

Liebe Kolleginnen und Kollegen,

sicherlich haben Sie schon mitbekommen, dass wir ein IT-Problem haben. Wir gehen aktuell von einer Bedrohung durch Schadcode aus.

Presse und Öffentlichkeit haben wir über die Störung unserer IT-Systeme informiert und auch auf unserer Homepage wird darauf hingewiesen. Sollten Anfragen der Presse oder Öffentlichkeit an Sie gerichtet werden, geben Sie keine Auskunft, sondern verweisen Sie bitte an Hr./Fr. XY.

Bitte folgen Sie den Anweisungen des Informationssicherheitsbeauftragten.

Weitere Informationen erhalten Sie im Verlauf des Tages von Ihrer direkten Führungskraft.

Beispiel für Pressemitteilung nach erfolgreicher Bereinigung

Kernaussagen sollten sein:

- Information zur Art des Vorfalls – was ereignete sich wann.

Beispiel:

Am 30.6.2019 ging eine gefälschte Bewerbungsmail auf eine offene Stelle in unserer Gemeinde ein. Diese enthielt im Anhang den Trojaner GandCrab 5.2. Der Trojaner hat Teile der Dateien auf einem Rechner und einem Server verschlüsselt.

- Aktueller Status – Ursache gefunden und Problem behoben

Das Problem ist mittlerweile behoben. Mit Hilfe unseres IT-Dienstleisters konnte der Trojaner lokalisiert, typisiert, isoliert und entfernt werden. Nicht befallene Rechner wurden unverzüglich heruntergefahren und nach Entfernung des Trojaners vom befallenen System zur Sicherheit nochmals überprüft. Die verschlüsselten Dateien konnten durch das Einspielen einer gespiegelten Sicherung rekonstruiert werden.

IT-Sicherheitsvorfälle mit Verbindung zum Bayerischen Behördennetz sind an das LSI zu melden unter: <https://lsi.bybn.de/sicherheitsvorfall/index.php>

KONTAKT

Weitere Informationen finden Sie unter:

<https://lsi.bayern.de/kommunen/>

Für Unterlagen und Beratung wenden Sie sich bitte per E-Mail an:

Beratung-Kommunen@lsi.bayern.de.

Gerne ist das kommunale Beratungsteam auch telefonisch unter 0911 21549-523 für Sie erreichbar.

Landesamt für Sicherheit in der Informationstechnik – Leitfaden A#04 Kommunikation von Sicherheitsvorfällen (Stand: 12.09.2024)

Verwendungshinweis: Dieses Dokument darf nur in unveränderter Form unter eindeutiger Angabe der Quelle und des Sachstands verbreitet werden.