Theater im Cyber-Angriff:
Das Krisenmanagement der Staatstheater Stuttgart

kulturBdigital-Konferenz am 2.11.2020

Referent: Marc-Oliver Hendriks, Geschäftsführender Intendant der Württembergischen Staatstheater Stuttgart

IT

- **Anzahl IT-User:** ca. 800
- **Anzahl Server** (incl. virtueller Server): ca. 50
- **Anzahl Spezialsoftware** (ohne Bühnentechnik): ca. 20 u.a. für Kartenverkauf, ERP-System, Theaterdisposition, CAD Werkstätten, Kostümverwaltung, Lohnabrechnung für Gäste, Zeiterfassung, Grafik, Internetdienste, Gebäude
- **Internetanbindung:** als nachgeordnete Einrichtung des MWK über das Wissenschaftsnetz + Landesnetz BW für Personalverwaltung /Gehaltszahlungen
- **IT- Sicherheit:** Überprüfung BSI-Grundschutz und Penetrationstests durch externe IT-Dienstleister

Krisenmanagement beim IT-Sicherheitsvorfall

IT-Sicherheitsvorfall Ende März 2019 mit IT-Ausfall, während dem dennoch der Produktions- und Spielbetrieb aufrecht erhalten wurde.

Zentrale Elemente des Krisenmanagements waren:

- Umsetzung Meldepflichten
- Einbindung externer Unterstützung
- Etablierung eines Krisenstabs
- Kommunikation nach Innen und Außen
- Aufrechterhalten des Theaterbetriebs durch Notbetriebe
- Gesteuerte Wiederinbetriebnahme mit Priorisierung.

Telefonische Meldungen des IT-Sicherheitsvorfalls unmittelbar nach Feststellung (Tag 0):

- Zentrale Ansprechstellen Cybercrime der Länder und des Bundes (ZAC) → polizeiliche Ermittlung
- Ansprechpartner zuständige Ministerien und CISO des Landes BW
- CERT BITBW und CERT Uni Stuttgart
- Mündliche Meldung Datenpanne beim LfDI BW (Tag +2)

Hinzuziehung externer Experten:

- IT-Spezialexperten für Analyse und Behebung (Tag 0)
- Spezialist der Wirtschaftsprüfer für Beratung bei Notfall- und Business-Continuity-Management (Tag +1)

Einrichtung eines Krisenstabs

- Einrichtung eines Krisenstabs ab Tag +1
- 2 x täglich Sitzung
- Geschützter Lageraum („situation room“)
- Visualisierung von relevanten Informationen
- Protokollierung jeder Sitzung
- Kommunikation des Krisenstabs mit der Polizei

Ermittlung der Risiken und kritischen Pfade durch den Krisenstab

- Abschätzung der Risiken (sehr hoch, hoch, mittel, gering) durch den IT-Ausfall für den Spielbetrieb, Planungsdaten, Finanzsteuerung, Einhalten von Rechtsvorschriften, Infrastruktur, Sicherheit.
- Gespräche mit Verantwortlichen in Sparten, Direktionen und Abteilungen zur Erhebung der Auswirkungen des IT-Ausfalls auf den Betrieb und den Zeitpunkten, wann diese kritisch werden.
- Zusammenstellung der konkreten Auswirkungen auf den Betrieb in einem Lagebericht.
- Grundlage für Priorisierung bei der Wiederinbetriebnahme

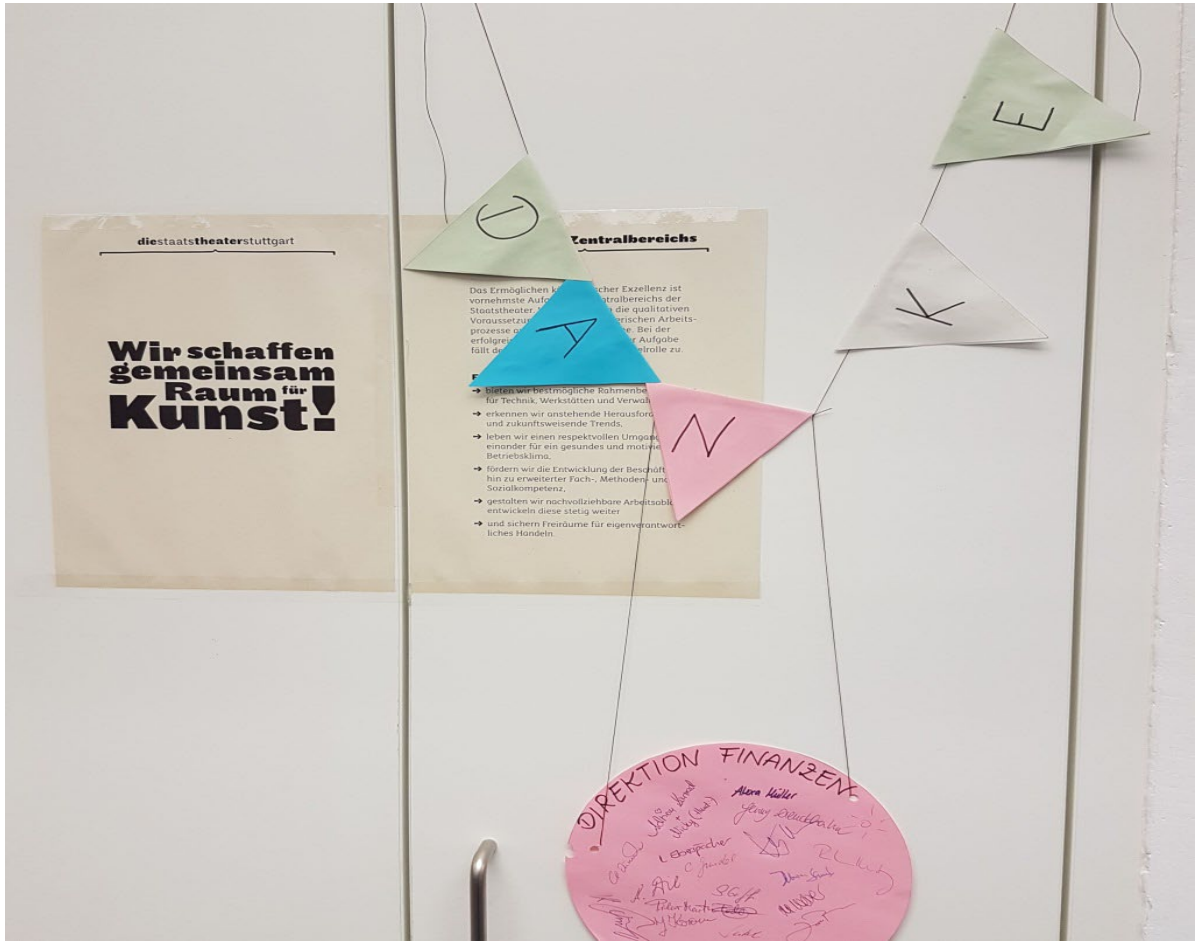
Interne Kommunikation des Krisenstabs

- Tägliche Besprechungen des Geschäftsführenden Intendanten und des Krisenstabs mit Spartenvertretern und Direktoren.
- Information des Geschäftsführenden Intendanten auf Mitarbeiterversammlungen, per Aushang und durch den Krisenstab beim Wiederanlaufen der IT per E-Mail.
- Vorortgespräche in den Arbeitsbereichen.

Interne Kommunikation ohne IT und E-Mail

- Interne Kommunikation nur persönlich oder per Telefon, sehr viel mehr persönliche Kontakte, positive Rückmeldung von Mitarbeiter/innen.
- Starker Zusammenhalt, die Krise gemeinsam zu meistern.

Krisenmanagement / IT-Abteilung



- Ausnahmezustand für die IT-Abteilung mit einer extrem hohen zeitlichen Belastung.
- Kontakt zur IT-Abteilung lief nur über Krisenstab.
- IT-Abteilung bekam von Mitarbeiter/innen im Haus positive Unterstützung, z.B. gebackene Kuchen.
- Abgeltung in Überstunden.

Kommunikation mit Stakeholder

- Rechtsträger (MWK, Verwaltungsrat und IM)
  - nur durch Geschäftsführenden Intendanten
- Kunden
  - Handreichung der Abteilungsleitung für Mitarbeiter/innen des Karten- und Abonnementverkaufs sowie des Besucherservice
  - Hinweis auf Kontakt zu Datenschutzbeauftragter
- Presse
  - nur durch Geschäftsführenden Intendanten und Direktor strategische Kommunikation in Abstimmung mit dem Rechtsträger
- Lieferanten
  - Über Zentralen Einkauf, FIBU und Ansprechpartner im Haus

Ein paar praktische Empfehlungen für ein IT-Notfall-Management

- Ermitteln Sie die kritischen Geschäftsprozesse und Ressourcen ihrer Organisation(„Kronjuwelen“).
- Regeln Sie Verantwortlichkeiten, Pläne und Verhaltensregeln möglichst in einem Notfallplan.
- Legen Sie fest, wer den Krisenstab bilden und welche Aufgaben und Befugnisse er haben soll.
- Krisenmanagement muss Chefsache sein.
- Klären Sie ab, wer im Falle eines IT-Notfalls informiert und eingebunden werden muss (Kontaktliste).

- Klären Sie ab, welche Einrichtung/Stelle ihres Rechtsträgers sie bei einem IT-Sicherheitsvorfall/Cyber-Angriffs fachlich unterstützen wird.
- Klären Sie ab, welche externe Experten im Fall eines IT-Sicherheitsvorfalls/ Cyber-Angriffs für die Analyse, forensische Beweissicherung und Wiederinbetriebnahme in Frage kommen bzw. beauftragt werden können. Soweit möglich, schließen Sie einen Rahmenvertrag ab.
- Schulen Sie die Mitarbeiter. Wichtig ist die Erfahrung von langjährigen Mitarbeitern, wie Prozesse manuell ohne IT praktisch umgesetzt werden können.

Ein paar praktische Empfehlungen bei einem IT-Sicherheitsvorfall/Cyberangriff (Krisenfall)

- Melden Sie den IT-Sicherheitsvorfall/Cyberangriff umgehend den erforderlichen Stellen, u.a. ZAC, LfD
- Ziehen Sie so schnell wie möglich externe Experten für die Analyse, forensische Beweissicherung und Wiederinbetriebnahme hinzu.
- Berufen Sie den Krisenstab ein und schaffen Sie einen geschützten Lageraum („situation room“).
- Versuchen Sie mit mobilen Geräten und Telefonlisten erreichbar und arbeitsfähig zu sein.
- Protokollieren Sie jede Sitzung des Krisenstabs.
- Steuern Sie die Wiederinbetriebnahme mit Priorisierung.

- Stimmen Sie die Krisenkommunikation mit ihrem Rechtsträger ab.
- Informieren Sie innerhalb der Organisation gestuft (Leitungsebene und Mitarbeiter/innen)
- Betrachten Sie das Notfall- / Business-Continuity-Management als gemeinsame Anstrengung aller Mitarbeiter/innen den Betrieb der Organisation auch im Krisenfall (manuell) aufrechtzuerhalten.
- Schützen Sie und unterstützen Sie die IT-Mitarbeiter/innen, die wochenlang „rund um die Uhr“ arbeiten müssen.
- Nehmen Sie keine internen „Schuldzuweisungen“ vor. Die gemeinsame Krisenbewältigung hat Vorrang.