österreichische
bundestheater

Empfehlung zur Informationssicherheit für Kulturbetriebe

Überblick und Checkliste

Autor: Markus Huber

17.10.2024

Inhalt und Ziel dieser Präsentation

- Überblick über Ziele und Nutzen der Informationssicherheit für Kulturbetriebe
- Überblick über die Gefährdungs-/Problempotentiale
- Überblick über den Aufbau der Informationssicherheit
- Auflistung und Priorisierung möglicher Maßnahmen zur Sicherstellung der Informationssicherheit

Disclaimer:
Diese Präsentation enthält keine vollständige Aufstellung notwendiger Maßnahmen zur Informationssicherheit sowie zu deren Ausgestaltung. Die Beurteilung und Umsetzung notwendiger Maßnahmen muss durch jede Organisation auf Basis einer Risikobeurteilung und unternehmerischer Rahmenbedingungen getroffen werden.

Ziele der Informationssicherheit

Ziel der Informationssicherheit ist

- der Schutz der Daten vor unberechtigtem Zugriff und Missbrauch
- der Schutz der Daten vor unbefugter oder fehlerhafter Veränderung
- der Schutz vor Daten vor Verlust
- die Sicherstellung der Verfügbarkeit der Daten für zugriffsberechtigte Personen

Daraus lassen sich folgende zentrale Schutzziele ableiten

- Sicherstellung der **Verfügbarkeit** von Daten
- Sicherstellung der **Vertraulichkeit** der Daten
- Sicherstellung der **Integrität** (Korrektheit) der Daten

Nutzen der Informationssicherheit

Der **Nutzen der Sicherstellung der Informationssicherheit für einen Kulturbetrieb** ist

- Sicherstellung der Vertriebstätigkeiten und des Kartenverkaufs (Online, Kassa, Apps, …)
- Sicherstellung der Marketingtätigkeiten (Webauftritt, externe Plattformen, …)
- Sicherstellung des Ausstellungs-/Spielbetriebs (Zutrittskontrolle, Infosysteme, Ausstellungs-/Bühnentechnik, Gebäudetechnik, Alarmanlagen, Brandschutz, …)
- Sicherstellung der Nutzbarkeit/Aufbewahrung der eigenen Digitalisatesammlung (intern/extern/Kulturpool/Europeana)
- Sicherstellung der Back-Office- und Verwaltungstätigkeiten (Buchhaltung, Lohnverrechnung, Ausstellungsplanung, Spielplanung, Inventarverwaltung, …)
- Vermeidung von Reputationsverlusten (Lösegeldzahlungen infolge Kryptotrojaner, Datenschutzverletzungen, missbräuchliche Verwendung der angebotenen Plattformen, ….)
- ein wesentlicher Beitrag zur Einhaltung gesetzlicher Vorgaben (DSGVO, Urheberrecht, …)

Überblick über die Gefährdungs-/Problempotentiale

Cybergefahren

- Schadsoftware (Viren, Trojaner, …)
- Phishing/Identitätsdiebstahl
- DDoS-Attacken
- unbefugtes Eindringen in IT-Systeme
- Social Engineering

Gefahren bei IT-Systemen

- Ausfall von HW/SW
- Fehlfunktionen von HW/SW
- Netzwerkausfälle
- Ausfall von IT-Serviceprovidern oder IT-Systemlieferanten
- …

Anwendungsgefahren

- fehlerhafte Zugriffsberechtigungen
- missbräuchliche Systemnutzung
- Verlust von IT-Geräten/Datenträgern
- Diebstahl von IT-Geräten/Datenträgern
- …

Infrastrukturgefahren

- Stromausfall
- Feuer, Wassereinbruch
- Überhitzung in IT-Räumen
- Verschmutzung, Staub, Korrosion in IT-Räumen
- unbefugtes Eindringen
- …

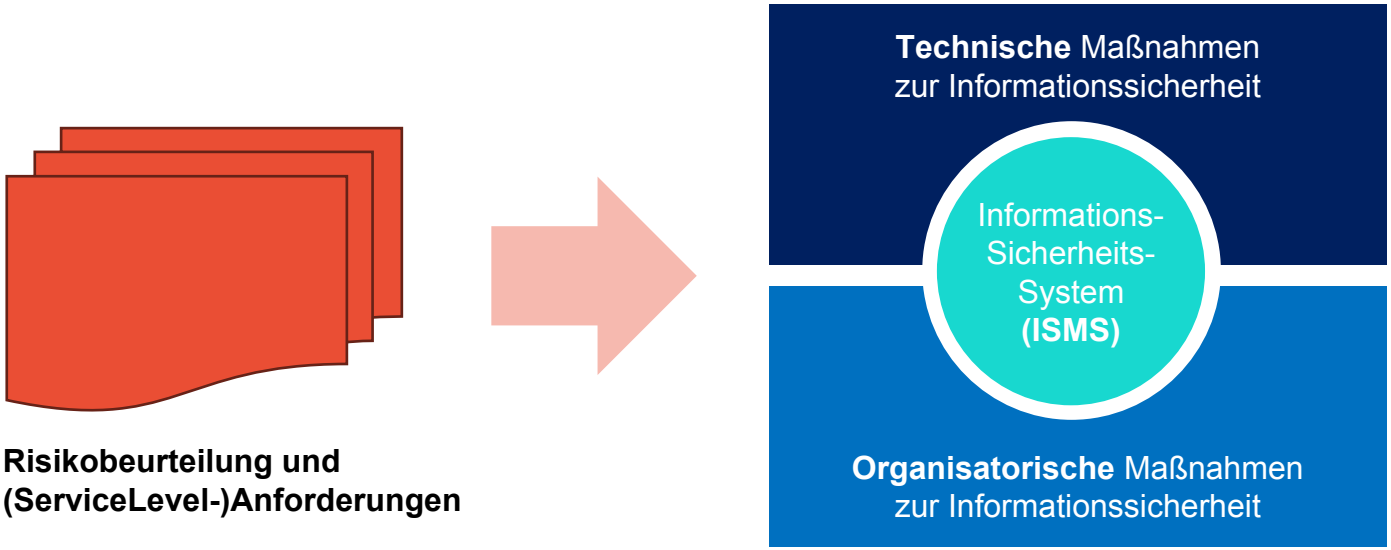
Wahrscheinlichkeit von Cyberangriffen

Veränderung der Angriffsarten	Wert	Veränderung gegenüber 2023
Abhören der Kommunikation (Man-in-the-Middle-Angriff)	26 %	0 %
Advanced Persistent Threats (APTs)	38 %	12 %
Business-E-Mail-Compromise, CEO-/CFO-Fraud	80 %	-9 %
Cloud-Fehlkonfiguration	36 %	-10 %
Datendiebstahl (Data Breach)	32 %	-30 %
Deepfake (Audio, Images, Video)	35 %	119 %
Denial-of-Service-Attacken (DoS)	54 %	-41 %
Identitätsdiebstahl	45 %	-24 %
Insider Threat	22 %	29 %
Malware (E-Mail-Anhang)	86 %	-10 %
Mis-/Desinformation	54 %	erstmals 2024 abgefragt
Mobile Malware	34 %	-13 %
OT-Kompromittierung (Industrial Control System)	8 %	-11 %
Passwortdiebstahl	47 %	0 %
Ransomware/Erpressung	24 %	-27 %
Social Engineering	62 %	9 %
(Spear-)Phishingattacke (E-Mail-Link)	87 %	-13 %
Spoofing	52 %	0 %
Supply-Chain-Angriff (Lieferkette)	46 %	18 %

Quelle: KPMG/KSÖ (04/2024): Cybersecurity in Österreich/Sicherheitsforum digitale Wirtschaft Österreich

… im Jahr 2024 haben Cyberangriffe wieder einen neuen Höchsstand erreicht!

Überblick über den Aufbau der Informationssicherheit



- **risikobasierter Ansatz** → grundlegende Risikoerstbetrachtung ist als Basis notwendig
- **ISMS** definiert Verfahren und Regeln zur Steuerung, Kontrolle, Aufrechterhaltung und laufender Verbesserung der Informationssicherheit (ISO 27001, BSI-Grundschutz, ...)
- **pragmatischer Ansatz für ISMS** besonders bei kleineren Organisationen notwendig!
- **Technische und organisatorische Maßnahmen (TOMs)** dienen zur Umsetzung der Informationssicherheit

Grundlegende Maßnahmen zur Informationssicherheit

- **klares Bekenntnis des Unternehmens zur Bedeutung der Informationssicherheit (TopDown)!!!!**
- klare Zuständigkeit der Verantwortung für Informationssicherheit
- KnowHow-Aufbau zur Informationssicherheit
- Sicherstellung der notwendigen Ressourcen / Budgetmittel
- Outsourcing (von Teilen) der IT-Sicherheitsmaßnahmen + Nutzung von standardisierten (cloudbasierten) IT-Services zur IT-Security zumeist unbedingt notwendig!

Legende:
!! notwendig
! empfohlen
o optional

TOMs zur Sicherstellung der Verfügbarkeit (1)

- ☐ !! Dokumentation und Überwachung (Monitoring) aller (wesentlichen) IT-Systemkomponenten (zur Früherkennung von Problemen und zur Fehlersuche)
- ☐ !! Sicherstellung der Herstellerunterstützung bei (wesentlichen) IT-System-komponenten (Wartungsvereinbarungen, Updates, Austausch, Ersatzteile, …)
- ☐ !! Datensicherung (räumlich getrennt, zumindest täglich, mehrere Generationen)
- ☐ !! Unterbrechungsfreie Stromversorgung (USV, zur geordneten Abschaltung)
- ☐ !! Definition des Vorgehens zur Wiederherstellung und zum Wiederanlaufs der IT-Systeme und regelmäßige Prüfung der Wiederherstellung
- ☐ !! Aufstellung der zentralen Hardwarekomponenten in geeigneten, klimatisierten (Rechner)räumen (Temperatur, Luftfeuchtigkeit, …) mit adäquatem Brandschutz
- ☐ !! Integrationstests vor dem Einsatz neuer Software-Versionen (auf Testsystemen)
- ☐ !! *bei Systemoutsourcing/Cloudservices: Vereinbarung von angemessenen Servicelevels (Performance, Verfügbarkeit, …) inkl. Nachweiserbringung und Pönalvereinbarungen*

Legende:
!! notwendig
! empfohlen
o optional

TOMs zur Sicherstellung der Verfügbarkeit (2)

- ☐ ! redundante Gestaltung zentraler Hardwarekomponenten/Ausfallssysteme (Applikationsserver, DB-Server, WebServer, Nameserver, Storage, Router, ...)
- ☐ ! DDoS-Schutz (gegen Distributed Denial of Service-Attacken)
- ☐ O örtlich getrennter Ausweich-Rechnerraum
- ☐ O redundante Internet-Anbindungen (unterschiedliche I-Provider)
- ☐ O Notstromversorgung (Generator) und/oder alternative Stromanbindung
- ☐ O Vereinbarung einer (notariellen) System-/Sourcecodehinterlegung (inkl. Dokumentation und Nutzungsvereinbarung) für wesentliche Softwarekomponenten als Vorsorge für eine Insolvenz des Herstellers
- ☐ O *bei Systemoutsourcing/Cloudservices: lokale Datensicherung der extern verarbeiteten Daten*

Legende:
!! notwendig
! empfohlen
o optional

TOMs zur Sicherstellung der Vertraulichkeit (1)

… aufbauend auf den TOMs zur Verfügbarkeit

Schwerpunkt „technische Absicherung der Systeme“:

- ☐ !! laufendes Einspielen von Security-Patches
- ☐ !! laufend aktualisierter Virenschutz (Server + Endgeräte)
- ☐ !! serverseitiger Mailschutz (Prüfung auf Viren, Spam/Phishing, Sandboxing, ….)
- ☐ !! Blockieren gefährlicher Internetinhalte
- ☐ !! professionelle/hochwertige (mehrstufige) Firewalls
- ☐ !! Sicherstellung einer verschlüsselten Datenübertragung mit Dritten (insbesonders Outsourcing-Partnern) oder für externe Zugriffe (VPN, SSL, …)
- ☐ !! Sicherstellung einer abgesicherten Fernwartung von Dritten (kein direkter Zugriff)
- ☐ !! Einsatz eines NAC (Network Access Control) zum Schutz von unauthorisierten Zugriffen/Endgeräten
- ☐ !! Trennung in internes WLAN und Gäste-WLAN

Legende:
!! notwendig
! empfohlen
o optional

TOMs zur Sicherstellung der Vertraulichkeit (2)

- ☐ **!!** Tools zur Deaktivierung von Endgeräten im Verlustfall/bei Diebstahl (MDM, …)
- ☐ **!!** (physischer) Zutrittsschutz zu wesentlichen Hardwarekomponenten/Rechnerräumen
- ☐ **!** EDR/XDR(Endpoint Detection and Response)-Schutz (Server + Endgeräte; ua. zur Abwehr von Ransomware)
- ☐ **!** Zusammenfassung von IT-Systemen, die aus dem Internet erreichbar sind, in einer DMZ (demilitarisierten Zone) und Absicherung zu den internen Systemen (Firewall)
- ☐ **!** Einrichtung eines systemübergreifenden Security-Monitorings (ggf. mit automatisierten Maßnahmen infolge von Sicherheitsverletzungen)
- ☐ **!** physische Trennung der Backupmedien vom Netzwerk (AirGap, entfernbare Medien)
- ☐ **!** *bei Systemoutsourcing/Cloudservices: Verschlüsselung der gespeicherten Daten*
- ☐ **o** Secure-DNS (ua. zum Blockieren von Netzwerkverbindungen von Angreifern)
- ☐ **o** Durchführung einer Netzwerksegmentierung (zB. bei mehreren Standorten) und Absicherung der Segmente zueinander um Angriffen isolieren zu können
- ☐ **o** DLP (DataLeak-Prevention) für sensible (zB.: urheberrechtlich geschützte) Inhalte

Legende:
!! notwendig
! empfohlen
o optional

TOMs zur Sicherstellung der Vertraulichkeit (3)

Schwerpunkt „Zugriffschutz“:

- ☐ **!!** rollenbasierte Berechtigungssysteme/vergabe
- ☐ **!!** Festlegung und Umsetzung notwendiger IT-Maßnahmen bei Onboarding / Offboarding / Funktionswechsel (Berechtigungsänderungen, Geräteübergaben, …)
- ☐ **!!** Passwort-Policy zur Sicherstellung „sicherer“ Passwörter
- ☐ **!!** Multifaktorauthentifizierung für Zugriffe von externen Netzwerken
- ☐ **!** besonderer Schutz privilegierter User-Accounts/Systemadministrator:innen (MFA, keine direkten Adminzugriffe, …)
- ☐ **!** Überwachung/Logging von Systemadministrationstätigkeiten
- ☐ **o** erweiterte Überwachung von System-Logins (Darknet-Monitoring, Aktivitätsanalyse, …)
- ☐ **o** zentrales Identity-Management/Berechtigungssystem

Legende:
!! notwendig
! empfohlen
o optional

TOMs zur Sicherstellung der Vertraulichkeit (4)

weitere Schutzmaßnahmen:

- ☐ **!!** Definition des Vorgehens bei IT-Sicherheitsverletzungen (inkl. Zuständigkeiten, Meldeverfahren/möglichkeiten und Kommunikation)
- ☐ **!!** Festlegung und Einführung von Verfahren für die Meldung von Geräteverlusten/Diebstahl
- ☐ **!!** *bei Systemoutsourcing/Cloudservices: Vereinbarung der notwendigen IT-Sicherheitsmaßnahmen inkl. Nachweiserbringung und Pönalvereinbarungen*
- ☐ **!** IT-Sicherheitsrichtlinien für Anwender:innen (Handlungsvorgaben/empfehlungen)
- ☐ **!** IT-Security-Awareness-Ausbildung für Anwender:innen (zur Sensibilisierung)
- ☐ **!** regelmäßige Security-Überprüfungen/Audits (Pentesting, Blackbox-Tests, Gesamtaudits, …)
- ☐ **o** regelmäßige Audits/Prüfung aller Systemberechtigungen

Legende:
!! notwendig
! empfohlen
o optional

TOMs zur Sicherstellung der Integrität

… aufbauend auf den TOMs zur Verfügbarkeit + Vertraulichkeit

- ☐ **!!** Datenprüfung nach Versionsumstellungen und Vorsorge durch Rollback-Szenarien (zum etwaig notwendigen Zurückgehen auf die Vorversion)
- ☐ **!** Funktionstests vor dem Einsatz neuer Software-Versionen (auf Testsystemen)
- ☐ **o** Logging/Versionierung von Datenänderungen

Querschnittsmaßnahmen zur Informationssicherheit

- Planung und Dokumentation aller Systemänderungen im Rahmen eines durchgängigen Änderungsmanagements (ChangeManagement)
- durchgängige Dokumentation von Verletzungen der Informationssicherheit und der Abwehr/Bewältigungsmaßnahmen
- Integration der Informationssicherheitsmaßnahmen im BusinessContinuity-/Notfallmanagement des Unternehmens
  - BusinessContinuity-Management definiert ua. die Vermeidung und Bewältigung von Störungen in Hinblick auf die Geschäftstätigkeit (gesamtheitlich!)
  - Notfallmanagement umfasst die Bewältigung von schweren Störungen/Katastrophen
  - inkl. interner und externer Kommunikation
- Berücksichtigung der Anforderungen zur Informationssicherheit bei der Auswahl neuer IT-Systeme oder IT-Serviceprovider/Lieferanten
- Berücksichtigung von „Security by Design“ bei der Eigenentwicklung von Software
- Abschluss einer Cyberversicherung ist eine Möglichkeit zur Überwalzung des Schadensrisikos