



# Kundenreferenz Naturkundemuseum

Wiederaufbau der IT-Infrastruktur nach Hackerangriff  
mit erhöhten Sicherheitsanforderungen.

# Das Unternehmen Naturkundemuseum

Das Museum für Naturkunde Berlin (*auch Naturkundemuseum Berlin*) ist das größte Naturkundemuseum in Deutschland. Die Bestände umfassen mehr als 30 Millionen Objekte. Das Museum agiert mit dem Aufgabendreiklang von Sammeln, Forschen und Vermitteln als Schnittstelle zwischen Wissenschaft und Gesellschaft. Das Museum für Naturkunde stattete zu diesem Zeitpunkt seine rund 450 Mitarbeiter/-innen mit 600 – 700 Endgeräten aus.

## Überblick

Die **Projektanforderungen** umfassten die schnelle Entwicklung einer neuen IT-Infrastruktur nach einem Hackerangriff. Die alte und neue IT-Umgebung mussten entkoppelt und unter hohen Sicherheitsanforderungen zusammengeführt werden. Hohe Sicherheitsstandards wurden eingeführt, um zukünftigen Angriffen standzuhalten, wobei der Einsatz von M365 zur Gewährleistung von Sicherheit und Skalierbarkeit vorgesehen war.

Der **Projekterfolg** beruhte auf der zügigen Wiederherstellung der Arbeitsprozesse und dem Neuaufbau der IT-Infrastruktur unter Zeitdruck. Dabei wurden die Sicherheitsanforderungen erhöht, eine flexible Endgeräteverwaltung implementiert und die IT-Supportkosten um etwa 30 % gesenkt.





## Die Herausforderung

Das Museum für Naturkunde Berlin ist Mitte Oktober 2023 Opfer eines gezielten Hackerangriffs geworden. Davon betroffen waren weite Teile der digitalen Infrastruktur. Ein interner Krisenstab arbeitete gemeinsam mit mehreren Forensik-Dienstleistern an der Bereinigung.

Gleichzeitig galt es, einen schnellen Wiederaufbau der Infrastruktur zu ermöglichen, um die wichtigsten Dienste des Museums zu gewährleisten und im Anschluss eine Bereitstellung der Systeme zügig sicherzustellen.

### **Schnelle Wiederherstellung der IT-Infrastruktur nach dem Hackerangriff**

Die größte Herausforderung bestand darin, unter erheblichem Zeitdruck ein Konzept zu entwickeln, das die wichtigsten Schritte zur schnellen Wiederaufnahme der Arbeit definierte und gleichzeitig die Sicherheitsanforderungen erhöhte.

### **Erhöhte Sicherheitsstandards zur Abwehr zukünftiger Angriffe**

Dabei war es essenziell, die alte Infrastruktur vollständig von der neu zu errichtenden IT-Umgebung zu entkoppeln, um eine erneute Kompromittierung zu verhindern. Die Infrastruktur des Museums für Naturkunde Berlin ist aufgrund der Vielzahl von Archivsammlungen besonders umfangreich und komplex. Es war notwendig, zahlreiche Infrastrukturdienste wie Exchange- und Active-Directory zu berücksichtigen und weitere kritische Dienste zu identifizieren. Nachdem die wichtigsten Dienste eingerichtet waren, sollten schrittweise weitere wichtige Komponenten bereitgestellt werden.

Die JAEMACOM GmbH wurde als IT-Infrastrukturpartner des Landes Berlin beauftragt. Dank der Expertise in der strategischen Beratung und Umsetzung zu Microsoft 365 und dem bestehenden Vertrauen erhielt die JAEMACOM GmbH den Auftrag, kurzfristig ein Wiederaufbauplan des IT-Betriebes auszuarbeiten und umzusetzen.

# Lösung und Projektverlauf

## Identifikation und Priorisierung der Systeme

Im ersten Schritt wurden gemeinsam mit den internen Mitarbeitern des Museums die prioritären Systeme identifiziert und mögliche Lösungen erarbeitet. Die Situation bot die Gelegenheit, auf Microsoft 365 umzustellen und in die Cloud zu migrieren, wodurch das Museum von Vorteilen wie erhöhter Sicherheit, Skalierbarkeit und globaler Verfügbarkeit profitieren konnte.

## Umstellung auf Microsoft 365 und Cloud-Migration

Im Zuge der Einführung von Exchange Online und der Synchronisation der Benutzerkonten mit Microsoft Entra ID in die Cloud wurden zusätzliche Sicherheitsmaßnahmen wie die Multi-Faktor-Authentifizierung implementiert. Dieser Prozess ermöglicht es, initial eine neue Domainstruktur aufzubauen, E-Mail-Dienste automatisiert über PowerShell in die Cloud zu migrieren und zeitnah Microsoft Teams als Kommunikationsplattform bereitzustellen. Um eine gute Einführung in das Arbeiten mit Microsoft Teams zu ermöglichen, wurden für die Mitarbeiter/-innen des Museums Schulungen in englischer und deutscher Sprache angeboten.

Damit das Museum seine bestehende Identitätsinfrastruktur in Azure nutzen und andere Clouddienste anbinden kann, wurde Entra Domain Services eingerichtet. So können die üblichen Active-Directory-Dienste direkt als verwalteter Cloud-Service genutzt werden.



## Sicherheitsmaßnahmen und Implementierung

Um Sicherheit und Benutzerzugriff effektiv zu verwalten, kam ein robustes, cloudbasiertes Identitäts- und Zugriffsmanagement zum Einsatz. Mit der Implementierung von Microsoft Intune wurde zunächst ein Mindestmaß an Endgeräteverwaltungskomponenten eingerichtet, die später weiter ausgebaut werden sollen.

Nach dem erfolgreichen Wiederaufbau und der Wiederaufnahme des Betriebes wurden weitere Sicherheitsmaßnahmen im M365-Mandanten des Museums für Naturkunde implementiert, darunter Microsoft Entra Conditional Access und Microsoft Entra Privileged Identity Management. Je nach individuell bewertetem Risiko eines Anmeldevorgangs wurden zusätzliche Identitätsprüfungen vorgenommen, um unautorisierte Zugriffe zu blockieren. Die Zuweisung erhöhter Berechtigungen erfolgt nach dem „Least-Privilege“-Prinzip, angepasst an den aktuellen Bedarf und zeitlich begrenzt.



## Vorteile auf einen Blick

- Schnelle Wiederherstellung der IT-Infrastruktur nach dem Hackerangriff
- Erhöhte Sicherheitsstandards zur Abwehr zukünftiger Angriffe
- Umstieg auf Microsoft 365 für verbesserte Sicherheit und Skalierbarkeit
- Flexible Endgeräteverwaltung durch Microsoft Intune
- Reduzierung der IT-Supportkosten um ca. 30 %
- Effiziente Verwaltung von Benutzerzugriffen durch cloudbasiertes Identitätsmanagement

## Das Ergebnis

Als IT-Infrastrukturpartner des Museums konnte die JAEMACOM GmbH innerhalb von zwei Wochen einen Plan für die Wiederherstellung des IT-Betriebes vorstellen und durchgehend unterstützen.

Durch die bereitgestellten Ressourcen der JAEMACOM GmbH konnte innerhalb von sehr kurzer Zeit das Active-Directory aufgebaut und ein erster Betrieb mit E-Mails zur Verfügung gestellt werden.

### Vorteile der Cloud-Migration

Der Umstieg auf Microsoft 365 und die Migration in die Cloud boten dem Museum zahlreiche Vorteile, darunter erhöhte Sicherheit, bessere Skalierbarkeit und eine erhöhte Ausfallsicherheit. Die Einführung von Exchange Online in Verbindung mit Microsoft Entra ID und der Synchronisation der Benutzerkonten ermöglichte die Nutzung von Multi-Faktor-Authentifizierung, wodurch die Sicherheit zusätzlich um ein Vielfaches erhöht wurde.

### Verbesserte Sicherheit und Kostenreduktion

Ein cloudbasiertes Identitäts- und Zugriffsmanagement gewährleistete dabei eine effektive Verwaltung von Sicherheit und Benutzerzugriff. Die Implementierung von Microsoft Intune ermöglichte es, die Endgeräte zentral zu verwalten und somit die Sicherheit jederzeit zu gewährleisten.

Neben der schnellen Wiederherstellung des IT-Betriebes, bei einer maßgeblichen Erhöhung der Sicherheitsanforderungen und einer ersten flexiblen Endgeräteverwaltung, konnten die IT-Supportkosten um ca. 30 % gesenkt werden.



## **JAEMACOM GmbH**

Rigaer Straße 44  
10247 Berlin

Germany

Tel.: +49 30 233292 333

Mail: [info@jaemacom.de](mailto:info@jaemacom.de)

[www.jaemacom.de](http://www.jaemacom.de)

