we run your business

Cyberangriff auf BER

ein weiterer Weckruf für Unternehmen!

Vor wenigen Tagen wurde der Flughafen Berlin-Brandenburg (BER) Opfer eines schweren Cyberangriffs, der erhebliche Störungen in der Passagier- und Gepäckabfertigung verursachte. Der Angriff richtete sich nicht direkt gegen den Flughafen selbst, sondern gegen einen externen IT-Dienstleister: Collins Aerospace. Das betroffene System modulierte zentrale Abläufe wie Check-in, Boarding und Gepäckaufgabe über eine Plattform, die von mehreren Flughäfen in Europa genutzt wird.

Was ist genau passiert?

- Am Freitagabend kam es zu einer Infektion mit **Ransomware**, wodurch Daten und Systeme verschlüsselt wurden.
- Dadurch fielen wichtige elektronische Systeme bei mehreren Flughäfen aus, darunter Berlin, Brüssel, Dublin und London-Heathrow.
- Die Reaktion bestand teilweise darin, auf manuelle Prozesse zurückzugreifen: Papierlisten, Stift, händische Gepäcketiketten etc.
- Fluggesellschaften und der Flughafenbetrieb standen wegen der Einschränkungen deutlich unter Druck. Warteschlangen, verspätete Flüge, Flugausfälle, erhebliche Verzögerungen: insbesondere bei Rückflügen, z. B. nach dem Berlin Marathon.
- Noch Tage nach dem Angriff waren Systeme nicht vollständig wiederhergestellt. Es kann mehrere Tage dauern, bis ein „normales“ Funktionieren erwartet wird.

Welche Probleme sind besonders deutlich geworden?

1. **Abhängigkeit von Dritt-Dienstleistern und vernetzten Systemen,**
   Dass ein Ausfall bei einem externen Anbieter so weitreichende Folgen haben kann, zeigt, wie kritisch Dienstleister in der Kette sind. Wenn zentrale Systeme über einen solchen Anbieter laufen, kann ein Fehler oder Angriff der gesamten Kette zum Problem machen.
2. **Unzureichende Redundanz und Notfallprozesse**
   Zwar wurde auf manuelle Verfahren umgestellt, doch ist offenbar nicht alles vorbereitet: Die Prozesse sind langsamer, ineffizient und belasten Personal und Infrastruktur stark. Die fehlende oder unzureichende Automatisierung von Backup-Systemen oder alternativen Abläufen wurde offenkundig.
3. **Kommunikation mit den Betroffenen**
   Passagiere litten und äußerten Frust über mangelnde Informationen, verspätete Flüge, unklare Zeitpläne. In Krisenfällen ist transparente, klare und selbstkritische Kommunikation essenziell, um Vertrauen zu erhalten.
4. **Gesetzliche und regulatorische Rahmenwerke**
   Es wird auf die kommende Umsetzung der europäischen **NIS-2-Richtlinie** verwiesen. Diese soll Mindeststandards festlegen, Meldepflichten schaffen und organisatorische und technische Sicherheitsmaßnahmen verbindlicher machen.

Warum Resilienz so wichtig ist – und was darunter zu verstehen ist

Resilienz heißt in diesem Zusammenhang nicht nur, ein System gegen Angriffe abzusichern, sondern so vorbereitet zu sein, dass Dienste auch dann weiterlaufen können, wenn der Zugriff auf zentrale Systeme gestört oder verloren ist. Im Einzelnen beinhaltet das:

- **Technische Resilienz**
  - Redundante Systeme (Backup-Hardware, alternative Kommunikationswege)
  - Segmentierung: Damit nicht alle Systeme gleichzeitig betroffen sind
  - Sichere, isolierte Notfallpläne für den Fall, dass digitale Systeme ausfallen
- **Organisationale Resilienz**
  - Ein klarer Krisenstab mit Verantwortlichkeiten
  - Gut geübte manuelle Verfahren, die im Notfall sofort greifen
  - Schulung des Personals → nicht nur das reguläre Handling, auch der Krisenmodus
- **Regulatorische Resilienz**
  - Gesetzliche Mindestanforderungen, wie durch NIS-2, um Sicherheit und Meldungspflichten zu standardisieren
  - Audits und Kontrollen, damit Anforderungen eingehalten werden
  - Verantwortlichkeiten auch bei Dienstleistern festlegen
- **Kommunikative Resilienz**
  - Transparente Informationspolitik gegenüber Reisenden und Öffentlichkeit
  - Frühzeitige Warnhinweise, Tipps (z. B. früh anreisen, online einchecken)
  - Rückmeldungen zum Status.

Was sollte passieren – Lehren und Empfehlungen

Unternehmen und kritische Infrastrukturen wie Flughäfen müssen Cybersicherheit als festen Bestandteil ihrer Organisationsstruktur verankern. Das bedeutet konkret:

- **Einführung von Managementsystemen**: Informationssicherheits-Managementsysteme (ISMS) nach ISO 27001 oder dem BSI-Grundschutz schaffen verbindliche Rahmenwerke für den Schutz kritischer Systeme und Daten. Ergänzend dazu stellt ein Business Continuity Management System (BCMS) sicher, dass der Betrieb auch bei massiven Störungen fortgeführt werden kann.
- **Vertragliche Absicherung gegenüber Dienstleistern**: Verträge mit IT-Dienstleistern sollten nicht nur Service Levels, sondern auch klare Vorgaben zur Einhaltung von ISMS- und BSI-Grundschutz-Standards enthalten. So wird die Abhängigkeit von Dritten beherrschbarer und Sicherheitslücken entlang der Lieferkette minimiert.
- **Regelmäßige Audits und Notfallübungen**: Gezielte Tests, Simulationen von Cyberangriffen und Penetrationstests überprüfen die Wirksamkeit der implementierten Sicherheits- und Resilienz Maßnahmen. Notfallübungen helfen, Personal und Prozesse auf den Ernstfall vorzubereiten.
- **Technische und organisatorische Resilienz Maßnahmen**: Dazu zählen segmentierte Netzwerke, redundante Systeme sowie Notfallhandbücher und Offline-Verfahren für kritische Prozesse. In Verbindung mit einem BCMS lassen sich Auswirkungen von Angriffen begrenzen.
- **Frühzeitige Erkennung und Monitoring**: Systeme zur Angriffserkennung und kontinuierlichen Überwachung helfen, Bedrohungen frühzeitig abzuwehren und Schadensausmaß zu reduzieren.
- **Zusammenarbeit mit Behörden**: Eine enge Verzahnung mit Sicherheitsbehörden, CERTs und branchenspezifischen Sicherheitsorganisationen sorgt für Informationsaustausch, schnellere Reaktionszeiten und verbindliche Mindeststandards.

Fazit

Der Cyberangriff auf den Flughafenbetrieb zeigt eindrücklich, dass **digitale Sicherheit und Resilienz zentrale Managementaufgaben** sind. Unternehmen, die auf hochgradig vernetzte Systeme setzen, müssen Cybersicherheit strategisch verankern – nicht als technisches Projekt, sondern als dauerhaften Prozess.

Ein ISMS nach ISO 27001 oder BSI-Grundschutz schafft dabei eine strukturierte Grundlage, während ein BCMS die Handlungsfähigkeit im Krisenfall sicherstellt. Beide Systeme ergänzen sich und machen Organisationen widerstandsfähiger gegen Angriffe und Störungen.

Die Lehre aus diesem Vorfall ist eindeutig: **IT-Sicherheit, Cybersicherheit und Business Continuity dürfen nicht isoliert betrachtet, sondern müssen integriert umgesetzt und regelmäßig überprüft werden.** Nur so können Flughäfen, Unternehmen und Dienstleister gewährleisten, dass ihre Systeme auch unter Angriffsdruck stabil bleiben – und das Vertrauen von Kunden, Partnern und Öffentlichkeit erhalten bleibt.

we run your business

Quellen

Reuters - EU agency confirms ransomware attack behind airport disruptions

T-Online - Cyberattacke trifft europäische Flughäfen

FAZ - Cyberangriff auf europäische Flughäfen – auch BER betroffen

FAZ - Verzögerungen am BER auch am Sonntag

DLF - Cyberangriff auf Flughafen-Dienstleister – auch BER betroffen