

## **KRITIS-Anforderungen des Klinikums Osnabrück**

Mit Veröffentlichung des IT-Sicherheitsgesetzes<sup>1</sup> am 25.06.2015 hat der Gesetzgeber **Betreiber so genannter kritischer Infrastrukturen**<sup>2</sup> in die Pflicht genommen, sich den Herausforderungen zum Schutz dieser für das Allgemeinwohl wichtigen Einrichtungen im Kontext zunehmender Digitalisierung zu stellen. Dabei ist nicht nur die Sicherheit der IT-Systeme, sondern auch die Sicherheit der hiermit verarbeiteten Informationen von besonderer Bedeutung. Um diese zu schützen, bedarf es neben der Umsetzung technischer und organisatorischer Vorkehrungen auch eines bewussten Umgangs mit diesen Informationen. Der Schutz von Daten und Ressourcen, die Einhaltung von Maßnahmen zum Schutz vor Angriffen sowie - auch im Notfall - die Gewährleistung nachvollziehbarer Abläufe und Prozesse sowie schließlich die Einhaltung von Vertragsbeziehungen tragen dazu bei, die Aufrechterhaltung des gesellschaftlich etablierten Versorgungsniveaus zu gewährleisten.

Im Sektor Gesundheit repräsentiert die Branche „Medizinische Versorgung“ in den Krankenhäusern, d.h. die (voll-)stationäre Versorgung aus Sicht des Gesetzgebers die zentrale Dienstleistung des Sektors. Aufgabe der medizinischen Versorgung ist insbesondere die (Wieder-)Herstellung der Gesundheit der Bevölkerung. Die Perspektive des Gesetzgebers ist dabei der Schutz der Gesamtbevölkerung Deutschlands, so dass in Bezug auf die Anzahl betroffener Bürger vergleichsweise hohe Maßstäbe an das „Funktionieren des Allgemeinwesens“ geknüpft sind.

Das Klinikum Osnabrück, eine Krankenhausgesellschaft in kommunaler Trägerschaft, zählt zum Kreis der **Betreiber so genannter kritischer Infrastrukturen** („KRITIS“) und ist demnach dazu verpflichtet, zentrale Dienstleistungen – insbesondere die stationäre Versorgung von Patienten - auch in Zeiten sich ändernder Sicherheitsanforderungen, insbesondere mit Blick auf die wachsende Bedrohung durch Cyberkriminalität, dauerhaft und stabil erbringen zu können.

Da es dem Klinikum Osnabrück ein wichtiges Anliegen ist, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der betriebenen Kritischen Infrastrukturen maßgeblich sind, gelten diese Anforderungen auch für externe Lieferanten – wie beispielsweise IT-Dienstleister oder Hersteller von Medizintechnischen Geräten.

Vor diesem Hintergrund ist es insbesondere unerlässlich, sowohl Zugriffe auf Teile der IT-Infrastruktur des Klinikums Osnabrück, Fernzugriffe, Integration von Fremdsystemen und dem Umgang mit Daten verbindlich zu definieren.

Hierbei sind die folgenden Regelungen einzuhalten:

### **Zugriffe auf Teile der IT-Infrastruktur**

Der Zugriff auf Teile der IT-Infrastruktur des Klinikums Osnabrück birgt erhebliche Sicherheitsrisiken. Dabei ist es unerheblich, ob der externe Lieferant ein IT-System direkt mit der IT-Infrastruktur koppelt oder der Zugriff über zwischengeschaltete Netzwerke (wie z.B. dem Internet, Wireless LAN oder dem Telefonnetz) geschieht.

Für alle Varianten gelten die folgenden Regelungen:

- Zugriffe auf die IT sind im Vorfeld mit der IT-Abteilung abzustimmen. Sie dürfen ausschließlich über die speziell für diesen Zweck bereitgestellten Zugänge erfolgen.
- Wenn IT-Systeme des externen Lieferanten auf die IT des Klinikums Osnabrück zugreifen, müssen sie über grundlegende Sicherheitsmaßnahmen verfügen:

---

<sup>1</sup> [https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/it\\_sig\\_node.html](https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/it_sig_node.html)

<sup>2</sup> [https://www.bsi.bund.de/DE/Themen/KRITIS/kritis\\_node.html](https://www.bsi.bund.de/DE/Themen/KRITIS/kritis_node.html)

- Das IT-System muss ausreichend vor Malware gesichert sein. Bei IT-Systemen mit dem Betriebssystem Windows muss ein aktueller Virens Scanner eines namhaften Herstellers installiert sein. Dieser muss permanent im Speicher des Rechners aktiv sein und alle Lese- und Schreiboperationen auf Datenträger überwachen. Der Virens Scanner muss tagesaktuell mit den neuesten Virendefinitionen des Herstellers versorgt werden.
- Das Betriebssystem des IT-Systems muss in angemessenen Abständen (i.d.R. täglich) automatisch mit den neuesten Sicherheitsupdates des Herstellers versorgt werden.
- Auf dem System dürfen sich keine als „Hackertools“ bekannten Programme befinden.

Jeder Zugriff auf die nichtöffentliche IT-Infrastruktur muss das Prinzip der exklusiven Verbindung umsetzen: Sofern realisierbar sollten bei bestehender Verbindung mit der IT-Infrastruktur keine Verbindungen mit anderen Netzwerken möglich sein (z.B. dem Internet oder dem internen Netz des Dienstleisters).

### **Fernzugriffe**

Jegliche Formen des Fernzugriffs von außerhalb des Firmen-Netzwerks (drahtlos oder kabelgebunden, insbesondere über das Internet) bergen erhebliches Schadenspotential und sind unter allen Umständen mit der IT-Abteilung des Klinikums Osnabrück abzustimmen.

- Fernzugriffe werden nur gewährt, wenn dies für die Aufgabenerfüllung des externen Lieferanten unerlässlich ist.
- Zugangskennungen für die Nutzung der IT-Infrastruktur per Fernzugriff dürfen ausschließlich für die persönliche Nutzung eingesetzt werden. Die Zugangskennungen dürfen nicht an andere weitergegeben werden. Dies gilt auch für andere Mitarbeiter des externen Lieferanten.
- Fernzugriffe müssen auf die Systeme beschränkt sein, die für die Aufgabenerfüllung des externen Lieferanten unerlässlich sind.
- Sofern praktikabel sind Fernzugriffe je Sitzung durch einen Mitarbeiter des Klinikums Osnabrück zu initiieren bzw. freizugeben.
- IT-Systeme, die vom externen Lieferanten zum Fernzugriff genutzt werden, müssen durch gängige Schutzmechanismen gegen Schadcode abgesichert werden.
- Die IT-Abteilung des Klinikums Osnabrück kann (auch nachträglich) die Nutzung von Mehrfaktor-Authentifizierungen für die Nutzung von Fernzugriffen anordnen.
- Das eigenmächtige Einrichten eines Fernzugriffs ohne Genehmigung der IT-Abteilung ist untersagt und gilt als gravierender Verstoß gegen diese Vorgaben.

### **Integrieren von Fremdsystemen**

Als Fremdsystem werden alle Systeme bezeichnet, die sich über einen längeren Zeitraum hinweg in der IT-Infrastruktur des Klinikums Osnabrück befinden und von externen Lieferanten installiert, konfiguriert oder betreut werden.

Fremdsysteme können große Auswirkungen auf die Informationsverarbeitung haben (z.B. Störungen verursachen). Aus diesem Grund gelten hierfür die folgenden Regelungen:

- Bevor ein Fremdsystem in die IT-Infrastruktur des Klinikums Osnabrück integriert wird, muss dieses von der IT-Abteilung freigegeben werden.
- Der externe Lieferant muss jedes Fremdsystem dokumentieren. Hierzu stellt das Klinikum Osnabrück verbindliche Mindestvorgaben zur Verfügung (u.a. Systembeschreibung, Kommunikationswege, ...)
- Wird ein Fremdsystem von einem externen Lieferanten betreut, so hat dieser die Dokumentation des Systems aktuell zu halten.

Der externe Lieferant muss für jedes Fremdsystem ein Konzept vorlegen, wie das System aktuell gehalten wird und mit welchen Maßnahmen die Serverprozesse gegen Angriffe geschützt werden. Ein besonderer Schwerpunkt ist hierbei auf die Einhaltung des Stands der Technik zu legen, was u.a. eine inhaltliche Klärung von Fragestellungen wie Patch-Management, Malware-Schutz, Härtingsmaßnahmen, Kennwortverwaltung, Berechtigungen und Außerbetriebnahme nebst Aussonderung beinhaltet.

### **Umgang mit Daten des Klinikums Osnabrück**

Für den Umgang mit Daten des Klinikums Osnabrück gelten die folgenden Regelungen:

- Sofern möglich müssen die Daten des Klinikums Osnabrück in der eigenen IT-Infrastruktur verbleiben und dürfen nicht auf mobile Datenträger (USB-Sticks, Notebooks, Smartphones etc.) kopiert oder auf fremde IT-Systeme (Server, Cloud-Speicher, etc.) übertragen werden. Sollte sich dieses nicht realisieren lassen, sind sensible und personenbezogene Daten unbedingt verschlüsselt abzulegen.
- Die Verwendung von mobilen Datenträgern in der IT-Infrastruktur ist generell untersagt und muss durch die IT-Abteilung des Klinikums Osnabrück im Vorfeld explizit genehmigt werden.
- Jeder mobile Datenträger muss zeitnah vor Verwendung in der IT-Infrastruktur des Klinikums Osnabrück auf potenzielle Schadsoftware getestet werden.

Nachdem das Klinikum Osnabrück als KRITIS-Betreiber den „Stand der Technik“ einzuhalten hat, den es alle zwei Jahre gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) durch Prüfungen nachweisen gilt, übertragen sich auch diese Anforderungen auf den externen Lieferanten. Gleiches gilt es bei der Meldepflicht<sup>3</sup> zu berücksichtigen, bei der es gem. § 8b Abs. 4 Nr. 2 BSIg darum geht, erhebliche IT-Störung an das BSI zu melden.

Verfügen externe Lieferanten über Sicherheitszertifizierungen wie beispielsweise einem Zertifikat nach ISO/IEC 27001 ist dieses als klarer Vorteil anzusehen.

Stand: 16.01.2020

---

<sup>3</sup> [https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/Neuregelungen\\_KRITIS/Meldepflicht/meldepflicht\\_node.html](https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/Neuregelungen_KRITIS/Meldepflicht/meldepflicht_node.html)