Update 17. August 2026

Technischer Sicherheitsvorfall im Juli 2026 am IDOS

Im Juli 2026 erfolgte ein Angriff auf eine Netzwerkkomponente des IDOS, über die **versucht wurde, auf interne Systeme zuzugreifen**.

Sowohl die unmittelbar nach der Entdeckung des Vorfalls gemeinsam mit externen IT-Sicherheitsspezialisten begonnenen Analysen als auch die Überarbeitung der Absicherung der gesamten IT-Infrastruktur des IDOS dauern an. Die betroffene Netzwerkkomponente, die als Einfallstor identifiziert wurde, ist inzwischen **vollständig erneuert**.

Die seit der Stellungnahme vom 6. August 2026 fortgeführten Analysen bestätigen, dass alle dem Angriff zuzuordnenden Zugriffsversuche auf interne Systeme gescheitert sind, es gibt weiterhin **keine Hinweise auf Kompromittierung, auf einen Zugriff auf gespeicherte Daten oder auf einen Datenabfluss. Es wurden keine Daten verschlüsselt durch Ransomware.**

E-Mails und Erreichbarkeit des IDOS

Die E-Mail und Dokumenten-Systeme des Instituts sind weiterhin vom Netzwerk getrennt.

***E-Mails**, die seit dem 27. Juli 2026 an uns gesendet wurden**, erreichen uns weiterhin nicht**. Sie werden nicht zwischengespeichert und werden nach einigen Tagen mit einem Hinweis auf die Nichterreichbarkeit an die Absender*innen zurückgesendet.*

*Alternativ erreichen Sie uns **telefonisch.***

Gemeinsam mit unseren externen IT-Sicherheitsspezialisten arbeiten wir mit Hochdruck am Wiederaufbau der IT-Infrastruktur, um eine sichere und zuverlässige Wiederherstellung zu gewährleisten. Dieser Prozess nimmt jedoch noch etwas Zeit in Anspruch.

Ziel ist es **bis Freitag, 21. August 2026** wieder **per E-Mail erreichbar** zu sein. Sobald dies der Fall ist, informieren wir Sie umgehend und aktualisieren diesen Beitrag.

Vielen Dank für Ihr Verständnis.

Prof. Dr. Anna-Katharina Hornidge, Dr. Axel Berger, Margret Heyen

Update 17 August 2026

Technical security incident at IDOS in July 2026

In July 2026, an attack was carried out on a network component belonging to IDOS, through which an **attempt was made to gain access to internal systems**.

Both the investigations, which began immediately after the incident was discovered in collaboration with external IT security specialists, and the review of the security measures for IDOS entire IT infrastructure are ongoing. The affected network component, which was identified as the point of entry, **has since been completely replaced**.

The analyses, which have continued since the Statement of 6 August, confirm that all attempts to access internal systems attributable to the attack have failed; there is still **no evidence of a breach, of access to stored data or of a data leak. No data has been encrypted by ransomware.**

Emails and IDOS availability

The Institute's email and document systems remain disconnected from the network.

***Emails** sent to us **since 27 July 2026** are still **not reaching us**. They are **not temporarily stored** and are returned to the senders after a few days with a message stating that the address is unreachable.*

*Alternatively, you can contact us **by telephone**.*

Together with our external IT security specialists, we are working flat out to rebuild our IT infrastructure to ensure a secure and reliable recovery. However, this process will still take some time.

Our aim is to be reachable by **email** again **by Friday, 21 August 2026**. As soon as this is the case, we will inform you immediately and update this post.

Thank you very much for your understanding.

Prof. Dr. Anna-Katharina Hornidge, Dr. Axel Berger, Margret Heyen