Incident report

Unavailability of messaging platforms

Thursday 17/08 – 8h56pm

Sunday 20/08 - 11h45pm

On **Thursday 17/08 at 8:56pm**, the registrar ENOM, hosting **the domain name ex10.biz**, decided to **suspend the domain name** because of suspicion of phishing. At IKOULA, this domain name is used to support the **Exchange and Zimbra messaging systems**.

The IKOULA teams immediately launched an **internal audit of the implicated servers**, to check the existence of this phishing. However, the investigations produced **no conclusive results**, as no suspicious redirection attempts were identified, and the information provided by ENOM did not confirm any phishing activity either.

This was followed by **dozens of urgent requests** from the IKOULA teams **to ask ENOM to remove** the suspension of the domain name, but **without any effect over the whole weekend** (despite dozens of tickets, emails, calls to support and other direct contacts with ENOM staff around the world). The incident was not resolved until **Sunday 20/08 at 11.45pm**, when the ENOM teams returned. However, they did not officially notify the IKOULA teams until Monday 21/08 at 5.58pm.

Following this incident, IKOULA is awaiting an incident report from ENOM concerning the causes of this "**false positive**" on the ex10.biz domain name.

IKOULA's teams have begun to work on **securing the messaging platform** so that this type of incident does not occur again in the future. We'll be sure to keep you informed of progress soon.

The IKOULA Teams