ikoula
HÉBERGEUR DEPUIS 1998

Rapport d'incident

Indisponibilité des plateformes de messagerie

Jeudi 17/08 – 20h56

Dimanche 20/08 - 23h45

Le **jeudi 17/08 à 20h56**, le registrar ENOM, chez qui le **nom de domaine ex10.biz** est enregistré, décide de **suspendre le nom de domaine** pour suspicion de phishing. Ce nom de domaine supporte chez IKOULA les deux systèmes de messagerie **Exchange** et **Zimbra**.

Les équipes IKOULA lancent immédiatement un **audit interne des serveurs concernés**, afin de vérifier l'existence de ce phishing. Or, les vérifications ne donnent **aucun résultat probant**, aucune tentative de redirection suspecte n'ayant été identifiée, et les éléments fournis par ENOM ne permettant pas de confirmer une quelconque activité de phishing.

S'en suivent alors des **dizaines de sollicitations** en urgence de la part des équipes IKOULA afin de demander la levée de la suspension du nom de domaine **auprès d'ENOM**, mais **sans aucun effet sur l'ensemble du week-end** (en dépit de dizaines de tickets, emails, appels au support et autres contacts directs auprès de personnel ENOM à travers le monde). La **levée** ne se fera que le **dimanche 20/08 à 23h45**, au retour des équipes ENOM qui cependant, ne feront un retour officiel aux équipes IKOULA que le lundi 21/08 à 17h58.

Suite à cet incident, IKOULA est en attente d'un rapport d'incident de la part d'ENOM concernant les causes ayant provoqué ce « **faux positif** » sur le nom de domaine ex10.biz.

Les équipes ont, quant à elles, engagé des **travaux de sécurisation de la plateforme** de messagerie afin de ne plus rencontrer ce type d'incident à l'avenir. Nous ne manquerons pas de vous tenir informé des avancées prochainement.

Les équipes IKOULA