mFIN-CERT.tg

Les 5 erreurs de cybersécurité qui exposent les institutions de microfinance

Par Maklawe HADATOKI
Analyste Cybersécurité & Lead CTI departement

Les investigations CTI permettent d'identifier des tendances récurrentes dans les incidents et expositions affectant les organisations financières. Dans le secteur de la microfinance, certaines faiblesses reviennent régulièrement et peuvent faciliter la compromission de comptes ou l'exploitation d'infrastructures exposées.

Erreur N°1 - Ne pas surveiller les identifiants compromis
Une organisation peut disposer de contrôles de sécurité efficaces tout en ignorant qu'un compte utilisateur apparaît dans une fuite provenant d'un poste compromis. La surveillance des données compromises permet d'identifier rapidement les comptes à risque et de déclencher une réinitialisation ou une investigation.

Erreur N°2 - Réutiliser les mots de passe
La réutilisation d'un même mot de passe entre plusieurs services augmente considérablement l'impact d'une fuite. Un identifiant récupéré sur une plateforme peut être testé sur une autre. L'utilisation de mots de passe uniques, d'un gestionnaire de mots de passe et de l'authentification multifacteur réduit fortement ce risque.

Erreur N°3 - Négliger les actifs exposés sur Internet
Les domaines, sous-domaines, interfaces d'administration, services de gestion et composants logiciels exposés doivent être inventoriés et surveillés. Une exposition non maîtrisée facilite la reconnaissance et peut permettre à un attaquant d'identifier des composants vulnérables ou mal configurés.

Erreur N°4 - Considérer le phishing comme un simple problème utilisateur
Le phishing doit être traité comme un risque technique et opérationnel. Les campagnes modernes sont souvent personnalisées et peuvent s'appuyer sur des informations publiques ou issues de précédentes compromissions.
La protection doit combiner sensibilisation, filtrage, MFA, analyse des messages et détection des connexions anormales.

Erreur N°5 - Ne pas intégrer la CTI aux opérations de sécurité
Une veille ponctuelle ne suffit pas. Les renseignements issus des fuites, des infrastructures malveillantes et des campagnes en cours doivent être intégrés dans les processus SOC et de gestion des incidents. La CTI devient réellement utile lorsqu'elle entraîne une action : blocage, investigation, réinitialisation, notification, takedown ou renforcement d'un contrôle.

Les cinq erreurs sont différentes mais étroitement liées. Une institution peut réduire son exposition en combinant visibilité sur ses actifs, surveillance des compromissions, MFA, gestion des identités, sensibilisation et intégration des renseignements CTI dans les opérations.