Le Monténégro à la merci des cyberattaques

Monitor (Monténégro) | Par Dragan Lučić | mardi 22 novembre 2022

Trois mois après la série de cyberattaques qui ont paralysé le pays, le Monténégro se rend à l'évidence : sans investissements, ni personnel, ni infrastructures, assurer la sécurité informatique est mission quasi impossible. Ce n'est pourtant pas la première fois que le pays est visé.

Traduit par Jasna Tatar Anđelić (article original)

Cet automne, le Monténégro rejoindra la base de données du Centre d'études stratégiques et internationales (CSIS) relatives aux cyberattaques, aux côtés notamment de l'Albanie et des États-Unis. Fin août, une bonne partie du pays est passée en mode offline, suite à une attaque informatique d'ampleur qui a ciblé de nombreux sites et serveurs institutionnels. Depuis, peu d'informations ont été communiquées concernant l'identité des hackers et l'ampleur de l'attaque. La seule certitude est que le Monténégro n'a pas assez de moyens ni de compétences pour prévenir d'autres intrusions.

Dans un communiqué publié une semaine après les faits, l'Agence monténégrine pour la sécurité nationale a accusé les services russes, estimant avoir localisé sur son territoire la source d'une opération qui n'avait encore jamais été tentée auparavant. Selon le média en ligne ITpro, spécialisé dans les questions de cybersécurité, les hackers du groupe Cuba ransomware auraient revendiqué être en possession de milliers de fichiers issus du site du Parlement monténégrin, dont des documents financiers, fiscaux et des données personnelles. Le groupe, poursuivi par le FBI, a pour habitude de « cibler les entreprises des secteurs financier, gouvernemental, de la santé et des technologies de l'information en utilisant le logiciel malveillant Hancitor pour accéder aux systèmes Windows. » Une fois les identifiants récupérés et les données copiées, les hackers utilisent des logiciels d'extorsion et exigent d'importantes sommes d'argent en échange de la restitution des données sensibles.

Vagues de cyberattaques dans la région

Le ministre de l'Administration publique Maraš Dukaj a confirmé l'identification du groupe de hackers tout en reconnaissant que certains documents visés étaient en accès libre sur le site du Parlement. Le Monténégro n'est pas le seul pays des Balkans récemment visé. Une semaine avant, la Slovénie a également subi la plus grande cyberattaque jamais connue, tandis qu'en Moldavie, 80 systèmes d'information, de plateformes et de portails publics ont aussi été ciblés début septembre dans le but de « rendre les ressources d'information de l'État indisponibles ».

Le ministère russe des Affaires étrangères a balayé les accusations d'un revers de main, accusant Podgorica de « chercher à anéantir les relations avec la Russie ». Au Monténégro, les experts s'interrogent sur la faiblesse des politiques mises en œuvre pour protéger la sécurité informatique. Le manque de financements et de prise de conscience de l'importance d'investir dans la cybersécurité aux plus hauts niveaux de l'État ont été reconnus comme les principales causes d'échec. Podgorica n'a pas tiré les leçons des attaques menées ces dix dernières années. De 2017 à juin 2021, 2609 cyberattaques sur des adresses web monténégrines ont en effet été enregistrées, avec une augmentation notable d'année en année.

En cause, selon un document rédigé par le ministère pour la période 2022-2026, l'absence de budget prévu et le manque de ressources humaines, financières et techniques. Seule une trentaine d'employés sont habilités à traiter les questions de cybersécurité pour l'ensemble des institutions gouvernementales, tandis qu'environ 1% des 55 000 employés de l'administration publique ont suivi une formation sur le sujet. Le gouvernement promet de porter ce nombre à 15% d'ici 2026. « La simple utilisation par les employés des ministères de services de messagerie tels que Yahoo représente un risque énorme, car les données échangées ne sont plus protégées par l'institution », note Marko Lakić, expert juridique en matière de cybercriminalité.

À cela s'ajoutent les fréquents changements structurels dûs à l'instabilité politique et la fuite des ressources humaines hautement qualifiées. « La plupart des jeunes programmeurs préfèrent travailler dans des entreprises privées où les conditions, les salaires et les perspectives d'évolutions de carrières sont nettement plus élevés que dans la fonction publique », souligne le rapport.

Suite aux cyberattaques, les États-Unis, la France et la Grande-Bretagne ont proposé leur aide au Monténégro, mais la question d'une solution à long terme reste en suspens. Le Conseil national de sécurité milite pour la création d'une Agence de cybersécurité, reste à voir si ces demandes seront prises en compte par le prochain gouvernement.

P.-S.

Cet article est publié avec le soutien de la fondation Heinrich Böll Paris.