Accès refusé aux vulnérabilités d'une application informatique

Pauline Meyer, le 18 juillet 2022

La sécurité publique s'oppose à la divulgation de rapport(s) de tests de sécurité sur les vulnérabilités d'une plateforme servant au traitement de demandes de permis de construire et de dossiers de construction (art. 16 al. 2 let. b LInfo).

Arrêt du Tribunal fédéral 1C_235/2021 du 17 mars 2022

Un individu requiert auprès de la Centrale des autorisations en matière de construction vaudoise (CAMAC) la communication du ou des rapport(s) d'audit de sécurité depuis 2015 concernant l'application ACTIS, qui est une application de saisie, de traitement et de suivi des demandes de permis de construire et des dossiers de construction. Un document portant sur des tests d'intrusion dans l'application est identifié par la Direction générale du numérique et des systèmes d'information (DGNSI), laquelle refuse d'accorder au requérant l'accès au document. Ce document consiste en un rapport de tests de sécurité portant sur les vulnérabilités de la plateforme ACTIS, les manières d'exploiter ces failles et les actions pour y remédier. Compte tenu de la sensibilité informatique de ces informatiques, la DGNSI estime que la sécurité publique s'oppose, en tant qu'intérêt public prépondérant, à la communication de ce document.

La Cour de droit administratif et public du canton de Vaud (CDAP) confirme cette décision (arrêt de la Cour de droit administratif et public (CDAP) du Tribunal cantonal du Canton de Vaud, 30 mars 2021, GE.2020.0217), dans la mesure où le document requis contient des informations engendrant un risque accru de piratage.

Le requérant conteste cette décision auprès du Tribunal fédéral, se plaignant d'une application arbitraire du droit cantonal, plus spécifiquement en lien avec l'art. 16 al. 2 let. b de la Loi vaudoise du 24 septembre 2002 sur l'information(LInfo).

Il n'est pas contesté que la DGNSI est un organe de l'État soumis au principe de transparence en vertu de l'art. 2 al. 1 LInfo et que le document requis constitue un document officiel tel que compris à l'art. 9 LInfo. Les art. 16 s. LInfo fixent les limites au droit à l'information.

Le document requis consiste en une présentation PowerPoint d'une cinquantaine de pages présentant notamment le nombre de vulnérabilités identifiées sur la plateforme ACTIS, les

risques liés à chacune d'entre elles ainsi que l'effort et le temps estimés pour y remédier. Les informations contenues présentent donc un caractère sensible, puisqu'elles identifient les vulnérabilités du système et la manière de les exploiter. Le TF estime que ces informations peuvent permettre de faciliter des piratages informatiques susceptibles de causer un risque important à la sécurité publique. Selon lui, elles peuvent servir à perturber les procédures en matière de construction sur une large échelle ainsi que compromettre la confidentialité et l'intégrité de données pouvant être qualifiées de sensibles.

Le document ne permet pas de distinguer entre les vulnérabilités auxquelles il a pu être remédié et celles qui sont toujours d'actualité. Pour pouvoir répondre à cette question, il faudrait, selon le TF, procéder à une nouvelle interpellation de la DGNSI. De toute manière, notre haute Cour estime que les informations concernant tant les vulnérabilités corrigées que les vulnérabilités pendantes pourraient engendrer un risque de piratage.

Sur cette base, le TF confirme que l'information requise ne peut être fournie en vertu de l'intérêt prépondérant que constitue la sécurité publique (art. 16 al. 2 let. b LInfo), conclut que l'arrêt de l'instance inférieure n'est pas arbitraire et rejette le recours.

La conclusion à laquelle aboutit le TF nous paraît raisonnable. Sa motivation quant à l'admission de l'intérêt public prépondérant, naturellement plus expéditive que celle de la CDAP, mérite d'être approfondie. Comme relevé par la DGNSI et confirmé par la CDAP et le TF, la divulgation au public de vulnérabilités est susceptible d'engendrer un risque important pour la sécurité publique, qu'il s'agisse de vulnérabilités corrigées ou non. Cette allégation coule de source pour les vulnérabilités auxquelles il n'a pas encore été possible de remédier, moins pour les vulnérabilités corrigées.

La divulgation de précisions sur des vulnérabilités déjà réparées est également susceptible d'engendrer un risque pour la sécurité publique. Les vulnérabilités, même corrigées, communiquent des informations utiles pour des acteurs malveillants portant sur le système et l'application en question. En outre, il n'en va pas uniquement de l'application ACTIS dans la mesure où, compte tenu de l'interconnexion aujourd'hui reconnue entre les différents systèmes, les précisions sur les vulnérabilités trouvées (et éventuellement réparées) sur cette plateforme pourraient servir de porte ouverte pour ACTIS comme pour d'autres applications et systèmes connexes. Finalement, les informations fournies par les vulnérabilités réparées permettraient à des acteurs malveillants de découvrir et exploiter d'autres vulnérabilités, dans la mesure où des vulnérabilités distinctes peuvent présenter des similarités.

L'intérêt public que constitue la sécurité publique est donc admis à juste titre comme un inté-

rêt primant celui de la transparence dans le cas d'espèce.

Proposition de citation : Pauline MEYER, Accès refusé aux vulnérabilités d'une application informatique, 18 juillet 2022 *in* www.swissprivacy.law/157