LE TEMPS

INFORMATIQUE ABONNÉ

Quand une importante société de sécurité informatique à Genève se fait elle-même pirater

Banques privées, services de l'Etat, enquêtes judiciaires: plus de 200 entités romandes ont recouru à un prestataire de services informatiques dont nombre de données confidentielles se sont retrouvées sur le darknet

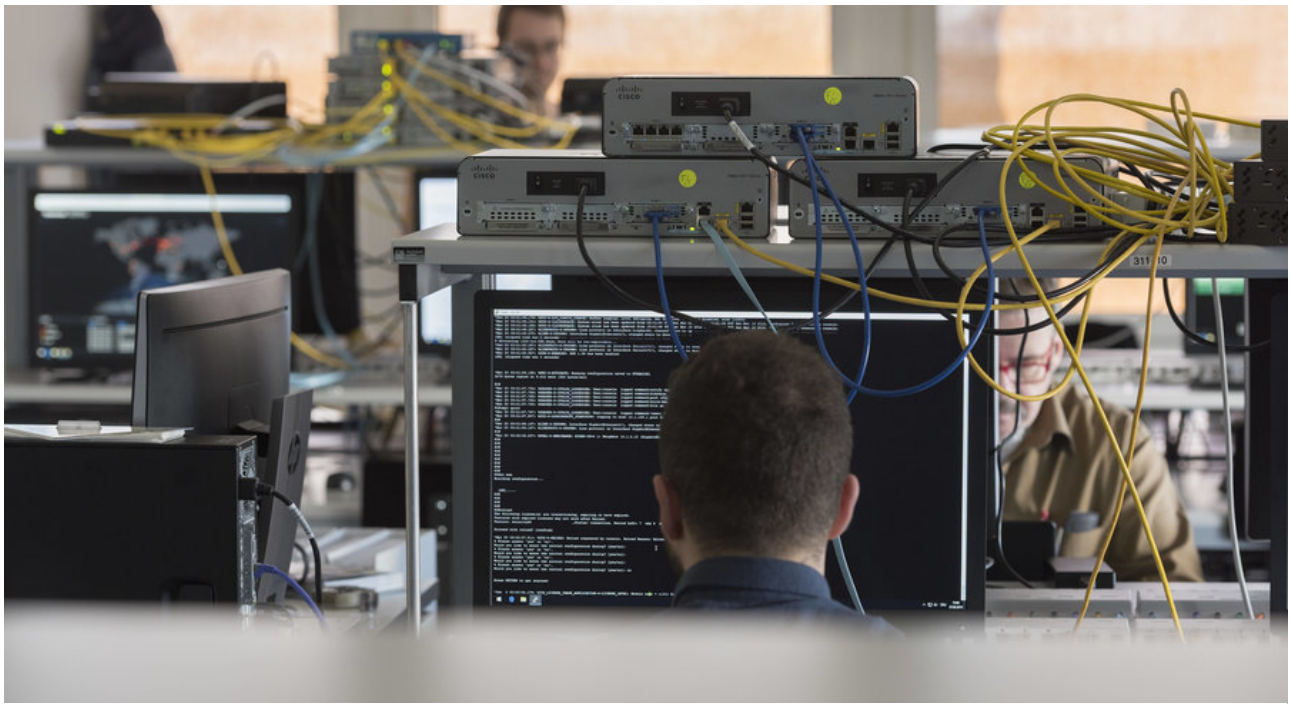

Image d'illustration. Cursus de bachelor «Sécurité de l'information et cybersécurité» à la Haute Ecole spécialisée de Lucerne. 27 février 2019, Rotkreuz. — © Christian Beutler/Keystone

Fanny Noghero

Publié mardi 26 juillet 2022 à 15:01
Modifié mercredi 27 juillet 2022 à 07:22

Le dimanche 24 juillet en fin d'après-midi, 64 967 documents confidentiels sont apparus sur le darknet. Ils proviennent du piratage d'une entreprise genevoise prestataire de services informatiques. On y découvre notamment la liste de ses clients, présents ou passés: des institutions publiques telles que la Chancellerie d'Etat de Genève, l'Hospice général, les HUG, l'aéroport de Genève ou encore des banques privées parmi les plus prestigieuses. S'y ajoutent des institutions vaudoises, des multinationales ainsi que des cabinets d'avocats et fiduciaires des deux cantons. Ces documents datent de 2000 à 2022.

Clients pas informés

Contactée lundi midi, l'entreprise informatique semblait découvrir qu'elle avait été piratée. Plus tard dans la journée, son directeur a indiqué au *Temps* n'avoir aucune déclaration à faire à ce sujet, et qu'il ne parlait «qu'avec la police». A noter qu'aucun des clients de ce prestataire que nous avons contactés n'ont été informés que des documents les concernant étaient accessibles en ligne.

«Même si la loi sur la protection des données (LPD) ne formule pas de manière explicite une obligation d'informer les personnes concernées lors d'une fuite de données, l'article 4 alinéa 2 LPD est interprété de la manière suivante: tout traitement de données doit être effectué conformément au principe de la bonne foi, ce qui implique une obligation de transparence. L'obligation d'informer existe en particulier lorsqu'il y a un risque pour les personnes concernées – ce qui semble être le cas ici –, afin qu'elles puissent prendre des mesures pour se protéger», précise Silvia Böhlen, spécialiste en communication du préposé fédéral à la protection des données et à la transparence.

Et Sébastien Fanti, avocat et préposé à la protection des données du canton du Valais, de compléter: «En revanche, dans le cadre contractuel, le prestataire est tenu d'informer son mandant afin de lui éviter des dommages. Dans le cas présent, si une des banques concernées devait subir des attaques consécutives à la mise en ligne de ces données, elle pourrait se retourner contre la société informatique qui ne l'aurait pas mise en garde.» Et l'avocat de souligner que les établissements bancaires sont tenus par la Finma, le surveillant de la finance suisse, d'annoncer immédiatement tout événement important du point de vue de la surveillance.

Demande de rançon émise

Ces dizaines de milliers de documents ont d'abord été mis aux enchères sur le darknet dimanche matin par un groupe de hackers utilisant le *ransomware** d'origine russe LockBit3.0. Une demande de rançon a été émise, et comme elle n'a apparemment pas été payée, les documents se sont retrouvés en ligne en fin d'après-midi.

Dans un des fichiers que *Le Temps* a pu consulter – une réponse à un cabinet d'avocat qui a mandaté cette entreprise informatique afin d'examiner certaines pièces dans le cadre d'une procédure pénale toujours en cours –, on trouve une description de la société piratée: «Spécialisée depuis 1998 dans l'installation de systèmes de sécurité, firewalls, messageries protégées et réseaux sécurisés. Consultée régulièrement pour des audits de sécurité et d'intrusion. Responsable de la mise en place de centres de secours en cas de catastrophe ou d'attaques informatiques.»

Données pas protégées

Et pourtant, parmi les documents piratés se trouvent des échanges en clair par e-mail contenant les données techniques des serveurs installés dans certaines entreprises, ainsi que les mots de passe pour s'y connecter. «Une hérésie, s'étrangle un spécialiste de la sécurité informatique. Pour des gens qui font des audits de sécurité, c'est d'un grand amateurisme, j'ai rarement vu pareille bêtise.»

Parmi les documents mis en ligne on retrouve encore des contrats, des rapports d'intervention, des pièces d'identité, des permis d'établissement, des extraits de casiers judiciaires, des attestations de poursuites, des CV avec photos, les données bancaires des clients, des adresses e-mail et des numéros de téléphone privés. D'autres éléments particulièrement sensibles émanant de la justice vaudoise, portant sur le décès d'un adolescent, sont également accessibles, sans être cryptés ou protégés par un mot de passe. Le prestataire avait été mandaté pour analyser le contenu du téléphone de la victime.

En ce qui concerne les HUG, aucune donnée sur des patients ne figure dans la liste, il s'agit plutôt de détails techniques sur le réseau informatique de l'hôpital.