L'UNION SOCIALE POUR L'HABITAT
Les Hlm, habiter mieux, bien vivre ensemble

Circulaire n°73/16
Note d'information

27 juillet 2016
Destinataires :
Tous les organismes Hlm
N/Réf. : FP/ML/AF/bs

Le Délégué général

Recrudescence des escroqueries aux faux ordres de virements internationaux dans les organismes Hlm

Madame, Monsieur le Président,
Madame, Monsieur le Directeur général,

Un organisme Hlm du Nord de la France vient d'être victime d'une escroquerie financière de très grande ampleur, du fait de faux ordres de virements, entraînant une perte financière importante

Dans ces conditions, je tiens à vous alerter à nouveau sur les risques encourus par les organismes Hlm, face à ces escroqueries qui sont malheureusement encore très répandues, bien que leur scénario soit parfaitement connu et les moyens pour s'en prémunir identifiés depuis plusieurs années. L'Office Central de Répression de la Grande Délinquance Financière indique que ces escroqueries ont généré, pour les sociétés implantées en France et/ou leurs filiales domiciliées sur l'Union européenne, un préjudice global d'environ 430 millions d'euros, pour des tentatives portant sur plus de 800 millions d'euros. Vous trouverez en annexe la note de sensibilisation diffusée par ce service de la Police Judiciaire.

J'insiste sur le fait que, contrairement à certaines idées reçues considérant que les grandes entreprises seraient les principales cibles de ces escroqueries, les entreprises de toute taille sont visées, et en particulier celles qui gèrent des paiements unitaires de sommes très élevées, comme par exemple pour les opérations de construction engagées par les organismes Hlm.

A titre d'illustration du caractère très réel de ces menaces pour les organismes Hlm, je vous invite à prendre connaissance des témoignages qui ont été apportés, au cours d'une journée du Club Habsis sur la sécurité et la cybercriminalité en octobre 2015.

Ils décrivent de façon très détaillée les tentatives d'escroquerie, dont leurs organismes ont été victimes ainsi que les mesures opérationnelles d'amélioration de la sécurité de leurs procédures financières et informatiques internes qu'ils ont mises en œuvre pour se prémunir de ces risques pour l'avenir. Ces mesures portent principalement sur la mise en place et le contrôle des habilitations et des modalités de passation des virements bancaires, en interne comme en lien avec les banques, de modification des RIB dans les progiciels avec l'instauration systématique de contre-appels, la formation des agents d'accueil téléphonique, mais aussi l'audit de la sécurité des systèmes d'information.

Il est également indispensable d'assurer la sensibilisation régulière des collaborateurs concernés (comptables, trésoriers, responsables de programmes, informaticiens) aux questions de sécurité financière, au respect des procédures et à la vigilance.

Je vous invite donc à la plus grande vigilance et à prendre, si nécessaire, les mesures complémentaires dans vos organismes afin de faire échouer ces tentatives d'escroqueries.

Je vous prie d'agréer, Madame, Monsieur le Président, Madame, Monsieur le Directeur général, l'expression de ma considération distinguée.

Frédéric Paul

Contact :
Antoine Ferré
Directeur
Mission Numérique Hlm
antoine.ferre@union-habitat.org

Documents disponibles :
Circulaire 37/15 de 2015 sur les risques de fraudes financières pour les organismes Hlm
Fiche réflexe de l'OCRGDF : « Prévention des escroqueries aux faux virements internationaux » (FOVI)
Réseau n°106 publié par Habsis – Sécurité de l'information et des données personnelles

Annexe :

1/ Pour un OPH : témoignage de Christian Harcouët, secrétaire général du Groupe Valophis, président d'Habsis

Valophis a fait l'objet d'une tentative d'escroquerie au président en 2013. Via un appel téléphonique au standard, l'escroc a réussi à être mis en contact avec une personne de la comptabilité. Il lui a demandé de faire une opération financière nécessaire au « sauvetage de l'entreprise ». Il a obtenu son silence en arguant que les difficultés dont il fallait sortir seraient précisément dues aux agissements de sa hiérarchie. Un faux avocat est entré dans le jeu et a communiqué des coordonnées d'un compte bancaire à Hong-Kong où devait être virée une somme de l'ordre du million d'Euros. L'ordre de virement a été passé, suite à quoi la personne concernée a pris conscience de la réalité des faits. Elle est venue en rendre compte au secrétaire général, qui faisait au même moment l'objet d'un contre-appel de la banque. Les fonds ont donc pu être bloqués. Auparavant, la banque avait pourtant déjà avisé l'organisme de ce type d'escroquerie, et ses salariés en avaient été informés.

Une autre tentative d'escroquerie a eu lieu sur une opération de construction. Un appel téléphonique a permis à un escroc de se rapprocher du service de comptabilité qui gère les situations de travaux. Se faisant passer pour le représentant d'une entreprise qui intervenait sur un chantier en cours, il a prétendu que celle-ci avait changé de banque pour envoyer ensuite un RIB, par mail. Deux virements ont été ainsi effectués, jusqu'à ce que l'entreprise s'inquiète de ne recevoir aucun règlement. Par chance, les fonds ont pu être récupérés à travers le système bancaire : ils n'avaient pas quitté le compte vers lequel ils avaient été détournés, compte qui s'est avéré contenir environ dix fois la somme dont l'organisme avait été lésé, servant sans doute à d'autres malversations. Dans ce cas, on notera que les procédures internes de l'organisme n'avaient pas été correctement suivies.

Dans l'un et l'autre cas, si des catastrophes financières ont pu être évitées, les retentissements qu'ils ont eu chez les personnes qui s'étaient faites manipuler ont été très profonds, et n'ont pas été non plus négligeables auprès de leurs équipes. Ce point ne doit pas être sous-estimé.

Les escroqueries sont un sujet que l'on répugne souvent à évoquer. Il faut au contraire souligner qu'un des premiers moyens de les prévenir est d'en parler. A le faire, on s'aperçoit d'ailleurs que la chose est plus fréquente que l'on ne croit. Il s'agit parfois de tentatives si grossières qu'elles peuvent en devenir presque comiques : tentative d'usurpation d'identité par téléphone, mais avec une voix qui ne colle vraiment pas, ou par mail, avec la bonne signature et la bonne adresse, mais avec une orthographe et un style aventureux. D'autres actes malveillants sont plus sérieux. Se faisant passer pour un membre de la DSI, on demande à un salarié son mot de passe, on en aurait besoin « pour prendre la main »… Une demande de rançon est faite après blocage du SI ou de certaines applications par un virus qui y a été introduit via un mail… L'imagination des escrocs semble ne pas connaitre de limites, quant au hacking, il peut toujours avoir des conséquences financières.

a. Adapter les procédures

Pour réduire les risques, les procédures ont été fortement centralisées. Lors du passage d'un marché, un correspondant est identifié chez le fournisseur et ses coordonnées sont saisies dans l'ERP. Des demandes de modifications ultérieures (changement de RIB…) feront obligatoirement l'objet de contre-appels auprès de lui. Ces contre-appels ne peuvent être effectués que par deux personnes parmi la vingtaine que compte l'équipe comptable. Ces deux personnes sont également les seules habilitées à créer des fournisseurs dans le SI (saisie de leurs coordonnées bancaires, etc.). Quant aux paiements, ceux-ci sont désormais effectués par voie électronique afin de les sécuriser. Ce système conduit à impliquer les responsables de programmes qui passent les marchés en construction, en réhabilitation ou en exploitation : ce sont eux qui collectent l'identité des correspondants financiers des entreprises.

Le succès nécessite de sensibiliser les équipes, ne serait-ce que du fait que les tentatives d'escroquerie évoluent. Pour maintenir la vigilance, le principe d'une réunion tous les six mois a été retenu. Ce sont d'abord les équipes comptables qui y ont été invitées. Mais si elles sont en première ligne, avec la DSI, il est envisagé d'étendre le mouvement à l'ensemble de l'entreprise de manière à ce que tout le monde devienne sensible à ce type de situation. Devant un événement suspect, une demande étrange qui peut être agressive, ou au contraire trop cordiale, le réflexe doit être de ne pas rester dans l'isolement mais au contraire d'échanger avec ses collègues et ses responsables. Les salariés sont devenus bien plus vigilants -la tentative d'un escroc qui se parait de la dignité institutionnelle de la Dgfip a pu être ainsi brisée dans l'œuf- et l'information, que l'on pourrait considérer comme un impératif pour l'employeur, est effective.

b. Un audit

Par ailleurs, les tentatives plus ou moins artisanales qui s'étaient produites ont amené à s'interroger sur d'autres, qui pourraient davantage s'appuyer sur la technologie. Un audit des systèmes d'information a donc été lancé. Son premier résultat a été de montrer que les sites internet de l'organisme n'avaient pas fait l'objet d'intrusions. Mais son but était aussi de voir si les dispositifs de sécurité en place étaient satisfaisants et de déterminer comment les optimiser.

L'attention s'est porté sur l'exposition via l'internet, le vecteur par lequel les intrusions sont les plus aisées. Il s'agissait d'identifier les capacités de rebondir vers l'ERP pour un attaquant qui prendrait le contrôle d'un serveur, quelles seraient les informations auxquelles il pourrait accéder et sur lesquelles il pourrait intervenir.

Il s'agissait également d'examiner la sécurité physique : il n'est pas très difficile de pénétrer par effraction dans un certain nombre d'espaces d'accueil des locataires (loges). Quelles conséquences cela peut-il avoir ? Quant au système de vidéo-protection, s'il n'est pas intégré au système de gestion, il en est proche. Quels risques cela présentait-il ? Quel est le niveau de sécurité des réseaux wi-fi ? Et, concernant cette fois les salariés de l'entreprise dotés de tels ou tels droits d'accès, que se passe-t-il, au regard de la loi informatique et libertés ?

Les résultats de cet audit ont été relativement satisfaisants. Les mesures qu'il a préconisées ont été mise en œuvre. Il a notamment conduit à la publication de tableaux de bord qui permettent de sensibiliser l'ensemble des salariés aux menaces. Ils font par exemple apparaitre que les firewalls ont rejeté 469 000 flux en août dernier, mois d'intense activité : ce nombre n'atteignait que 390 000 en juillet. L'ordre de grandeur des virus qui ont réussi à passer, pour être ensuite bloqués sur les postes des utilisateurs, n'est pas le même : ils se comptent seulement en centaines.

2/ Pour une ESH : Témoignage de Willy Freulon, directeur administratif et financier et système d'information de Vallogis

Un 31 octobre, la veille d'un jour férié, en milieu d'après-midi, le directeur administratif et financier a reçu un appel téléphonique de son banquier qui voulait lui parler d'un ordre de virement étonnant par son montant, 2 M€, comme par sa destination : la République Populaire de Chine. Un peu plus tard, une personne de la comptabilité est venue le trouver pour lui dire qu'elle pensait avoir été victime d'un escroc. Il était 16h20 alors que l'heure de départ des virements est fixée à 16h30.

Le virement bloqué, et la décision de déposer plainte une fois prise, encore restera-t-il à identifier le service compétent auprès duquel le faire, ce qui amènera aux alentours de 20h. Ce dépôt de plainte aura lieu en présence du directeur, ce qui s'avèrera utile : le débriefing est alors complet et les informations détaillées. Le directeur apprend ainsi que des copies d'écrans de tous les comptes bancaires sont dans les mains escrocs. Mais si les particuliers disposent d'un service 24/7 pour faire opposition sur leur compte, rien de tel n'existent pour les entreprises, il faut attendre la fin du week-end, que le management, comme la victime, peuvent

passer à se rejouer le film, dont le scénario a duré toute une journée au cours de laquelle la victime a réussi à masquer son stress.

L'appel de l'escroc est arrivé à l'accueil où l'on n'a rien trouvé à redire à ce que « le président » passe par son intermédiaire, ni à le mettre en relation avec la personne qu'il souhaitait. Cela amène à s'interroger sur le rapport qu'entretiennent les salariés par rapport à « l'autorité ». L'injonction « président » semble affranchir de toutes les procédures établies. Que ce « président » prétende ensuite « l'entreprise en danger » et déploie un décor où règnent des « avocats d'affaire » et finance internationale finit de rendre le cocktail toxique.

Exposé au cours du conseil d'administration qui suit, l'incident entraine des réactions variées. Pour les uns, c'est un peu gros, on pourrait quand même faire attention. Mais certains témoignent qu'ils ont eu affaire à plusieurs reprises à de tels incidents. D'autres attirent l'attention sur les répercussions qui peuvent se produire auprès des salariés impliqués. Quant au dernier, bien au fait du procédé, il rapporte qu'un de ses comptables a fait l'objet de menaces sur ses enfants dont les établissements scolaires étaient connus des escrocs. A en parler, il devient clair en tous cas que ce type de faits n'a rien d'exceptionnel, même s'il a un caractère de tabou, jusque pour le banquier qui, lorsqu'on le fera parler, expliquera qu'il s'agit, de fait, d'événements relativement fréquent. Les organismes HLM apparaitraient d'ailleurs moins portés que d'autres entreprises à prendre les mesures nécessaires pour faire face à ce nouvel environnement, mais sans que cela ne conduise pour autant ledit banquier à les y sensibiliser.

En abordant la question, le comité de direction s'est pour sa part remis en cause : plusieurs directeurs étaient au courant de tentatives de fraudes dans d'autres organismes, malgré quoi le sujet n'avait jamais été abordé dans cette enceinte. Il est alors apparu que le sujet méritait un projet d'entreprise, non pas seulement un audit limité aux process de comptabilité et de trésorerie.

Une formation a été organisée, réunissant le comité de direction, les managers, les comptables et les trésoriers. On y apprendra au moins que la fraude peut être externe, mais aussi interne, et que l'on peut mettre le curseur de la sécurité où l'on veut. Il est par exemple possible de mettre en place des systèmes très complexes et totalement blindés, mais qui nécessiteront des moyens matériels et humains à la hauteur et compliqueront les process.

Actions

La première action a concerné la formation des Accueils. Ils se sont vu rappeler quel était leur rôle, ils ont été sensibilisés au risque de fraude et à la nécessité d'une vigilance particulière durant les congés et aux veilles de week-end ou de jours fériés. Non sans résultat : deux tentatives de fraude ont été déjouées dès l'Accueil peu de temps après.

La trésorerie doit pour sa part respecter les process. Son rôle n'est pas de débloquer des situations urgentes ou de dépanner ceux qui sont en retard. En cas de doute, elle doit effectuer un contre-appel ou exercer un devoir d'alerte auprès de sa hiérarchie. En cas d'appel d'un administrateur ou d'un président, elle doit y mettre immédiatement fin, pour le rappeler aussitôt sur sa ligne directe. De leur côté, les directeurs doivent cesser de demander des paiements en urgence et de générer ainsi du stress. Chaque personne est acteur dans la lutte contre la fraude.

Plusieurs process ont été améliorés. Il est par exemple devenu impossible de faire des copies d'écran des comptes. Les informations bancaires ne sont plus accessibles par tous les comptables. Le nombre de personnes susceptibles de saisir des RIB a été lui aussi restreint. Leur modification donne systématiquement lieu à des contre-appels.

Les rapprochements sont par ailleurs effectués très rapidement, ce qui permet par exemple de lutter contre une tendance aux prélèvements frauduleux qui s'est récemment développée : des abonnements téléphoniques, ou autres, étant ainsi souscrits en communiquant les coordonnées de l'organisme. La rapidité

des rapprochements permet de bloquer ces prélèvements. La base RIB, qui contient notamment ceux des salariés, est auditée deux fois par an.

La signature des paiements doit s'accompagner de vérifications aléatoires, ou systématiques lorsque les montants sont significatifs. Elle a donc été retirée aux administrateurs qui avaient historiquement accès aux moyens de paiement mais sans avoir les moyens d'effectuer les vérifications voulues.

Cette démarche a également conduit à mettre en place pour les paiements une solution Saas fonctionnant sous le protocole EBICS TS (*), Exabanque Ce protocole permet d'envoyer des ordres de paiement sécurisées à l'ensemble des banques, avec des règles d'habilitation générales, non plus banque par banque, et avec des fonctionnalités qui facilitent les rapprochements comptables, les prévisions bancaires, et autres. Seul inconvénient : le temps nécessaire à la mise en place, à la gestion des contrats auprès des banques et à la validation des certificats. Mais c'est aussi l'occasion de remettre à plat un certain nombre de paramètres avec elles : les banques, elles non plus, ne sont pas là pour dépanner, et l'on attend d'elles qu'elles respectent les process voulus.

(*) EBICS : Electronic Banking Internet Communication Standard