Un « leader européen » des données de santé licencie un lanceur d'alerte pour « faute grave »

Il avait fait patcher l'AP-HP

59 • 49

INTERNET 26 MIN

Par Jean-Marc Manach
Le vendredi 2 octobre 2020 à 16:53

Signaler une erreur

En plein confinement, alors que l'AP-HP avait été victime d'une cyberattaque, un employé de Dedalus France – « *leader européen en matière de solutions logicielles de Santé* » – alertait les autorités pour faire colmater une faille importante en urgence. Licencié « pour faute grave », il nous raconte son histoire.

Moins d'une semaine après le début du confinement, L'Express **révélait** que l'Assistance publique – Hôpitaux de Paris (AP-HP) avait été la cible d'une attaque informatique nécessitant de « *couper momentanément* », le dimanche 22 mars, l'accès externe aux mails et à des outils de télétravail.

Le Parisien **rappelait** que dès janvier, Guillaume Poupard, patron de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), l'avait prophétisé : « *les attaquants n'ont pas d'éthique donc ils seraient capables d'attaquer les CHU au moment d'une crise quand nous avons besoin d'eux pour être sûr de récupérer une rançon* ».

qu'administrateur, à plus de 150 infrastructures médicales, AP-HP comprise.

Il tenta d'abord d'alerter le directeur de la technologie et le PDG italien de son employeur qui, du fait de la pandémie, avaient d'autres priorités. Il contacta alors un haut responsable de la sécurité informatique du gouvernement qui, ayant assisté à l'attaque de l'AP-HP, prit la mesure du problème. Il demanda à Dedalus France de colmater la brèche en urgence. Dans la foulée, l'entreprise licenciait le lanceur d'alerte, « *pour faute grave* ».

L'enchaînement des faits, et l'incompréhension manifeste entre le développeur et son employeur, sont un cas d'école. Non seulement parce qu'il s'agit d'une entreprise traitant des données de santé – et donc sensibles – mais également parce que, quatre ans après l'adoption du RGPD, il ne devrait plus être possible de minorer à ce point les questions de cybersécurité. Surtout au regard du statut de l'entreprise.

Passée en quelques années de TPE à celui de multinationale cotée en bourse, ses process qualité en termes de sécurité informatique ne semblent pas avoir évolué en conséquence.

« Le premier fournisseur de logiciels de santé en Europe »

Pour comprendre cette histoire, il faut remonter **à 1998**, lorsque le dirigeant d'un laboratoire d'analyse médicale demandait à son fils, étudiant en informatique, de développer un intranet pour informatiser le traitement de ses dossiers, et « *faciliter leur démarche Qualité* ».

Deux ans plus tard, en 2000, ils créaient Netika, pour commercialiser leur logiciel auprès d'autres labos. En 2015, Netika se **présentait** comme « *leader sur le marché français des logiciels de qualité pour les laboratoires d'analyses médicales* ». Cette année-là, 2 500 établissements de santé publics et privés (dont l'AP-HP) **utilisaient** les outils de l'entreprise, qui se targuait alors d'occuper 60 % du marché de la biologie médicale.

En 2017, elle équipait 2 800 établissements, employait près de 70 personnes et revendiquait un chiffre d'affaires de 6 millions d'euros. Elle était **rachetée** près de 10 millions par Medasys, qui se présentait alors comme « *principal éditeur et intégrateur français de logiciels médicaux pour établissements de santé, publics et privés* », et **revendiquait** « *plus de 44 % de parts de marché en France sur le segment des grands établissements CHU/CHR* ».

Créée en 1980, Medasys avait déjà procédé à ce type d'« *opérations de croissance externe* ». En 2009, elle avait ainsi repris l'activité « *Systèmes d'Information Hospitaliers* » de Thales, et acquis Mega-Bus, l'un des trois principaux éditeurs de logiciels de gestion pour les laboratoires privés d'analyses médicales en France.

Depuis 2016, Medasys a par ailleurs pour actionnaire majoritaire le groupe Dedalus Italia, « *leader en informatique de Santé, (et) l'un des leaders européens en matière de solutions logicielles de Santé* », comptant 1 700 collaborateurs et présent dans 25 pays. En mars 2019, Medasys et ses filiales (Netika, DL Santé, Dedalus C&G, Mexys, Medasys Africa, Medhealth Maroc, Medasys Japan) **changeaient** de nom pour devenir Dedalus France.

Une fuite de 4 Go de données, une autre de 1 400 emails...

Autodidacte, Arnaud D. (nous avons, à sa demande, pseudonymisé son nom) était recruté en avril 2018 par Netika en tant que développeur web « **full stack** ». Passionné de cybersécurité, il identifia assez rapidement plusieurs failles dans les logiciels et systèmes d'information de l'entreprise, puis des autres sociétés rachetées par Medasys, qu'il transmettait logiquement et régulièrement à ses supérieurs.

Une fuite de 4 Go de données sur un serveur et une autre de 1 400 emails de clients, accessibles depuis Internet et sans mot de passe dans les deux cas. Plusieurs failles de sécurité logicielles, aussi. Arnaud D. n'avait pas été recruté pour identifier les brèches de sécurité affectant les logiciels commercialisés par son employeur. Ses supérieurs n'en reconnurent pas moins, initialement, son expertise en la matière.

En mars 2019, à sa demande, Dedalus France prit ainsi en charge son déplacement aux **GS Days**, « *journées francophones de la sécurité* ». En novembre, il était de nouveau autorisé par sa hiérarchie à assister au Forum International de la Cybersécurité (**FIC**), « *l'événement de référence en Europe en matière de sécurité et de confiance numérique* ». Dans les deux cas, Dedalus lui demanda, en contrepartie, de rédiger une note afin de résumer ce qu'il y aurait appris, et ce qui pourrait concerner ou être utile à son employeur.

« J'ai accès à des comptes rendus médicaux qui ne sont pas les miens ! »

Dans le compte-rendu qu'il nous a transmis, Arnaud D. soulignait d'entrée que « *l'un des principaux vecteurs d'attaque sont les interfaces Web (intranet, portail applicatif...)* [qui] *représente 33 % des attaques d'entreprises* [en] *2019. C'est un choix idéal car les applications Web sont accessibles depuis partout dans le monde et les technologies et leurs vulnérabilités sont largement connues* ».

En mai, deux particuliers alertaient l'entreprise au sujet d'une faille de sécurité affectant **LaboConnect**, un logiciel de Dedalus France permettant de consulter les résultats de ses examens de biologie. Tous deux professionnels de la sécurité informatique, ils venaient en effet de découvrir que « *LaboConnect permet à n'importe quel utilisateur connecté d'accéder à l'ensemble des ordonnances ainsi qu'aux résultats hébergés sur la plateforme* », comme l'expliquait l'un d'entre eux, dans un e-mail que nous avons pu consulter.

À l'image de ce que nous avions **découvert** l'an passé sur le serveur de l'assurance maladie, les dossiers médicaux des autres patients étaient en effet accessibles en modifiant l'identifiant présent dans l'URL de consultation des examens médicaux.

- **N'importe qui pouvait lire les courriers d'Ameli**

« *En voulant récupérer mes résultats d'analyse en ligne via votre site,* déplorait l'autre utilisateur, *j'ai remarqué qu'il s'agissait d'un fichier PDF dont l'URL est : https://laboconnect.com/[...]&docId=XXXXXX. Problème : en remplaçant XXXXXX par à peu près n'importe quel nombre, j'ai accès à des comptes rendus qui ne sont pas les miens, comportant des données médicales sensibles !* ».

qu'il effectue un « *test de sécurité* ». Arnaud D. l'a alors réalisé et nous l'a transmis. Il y relevait quatre failles « *importantes* ».

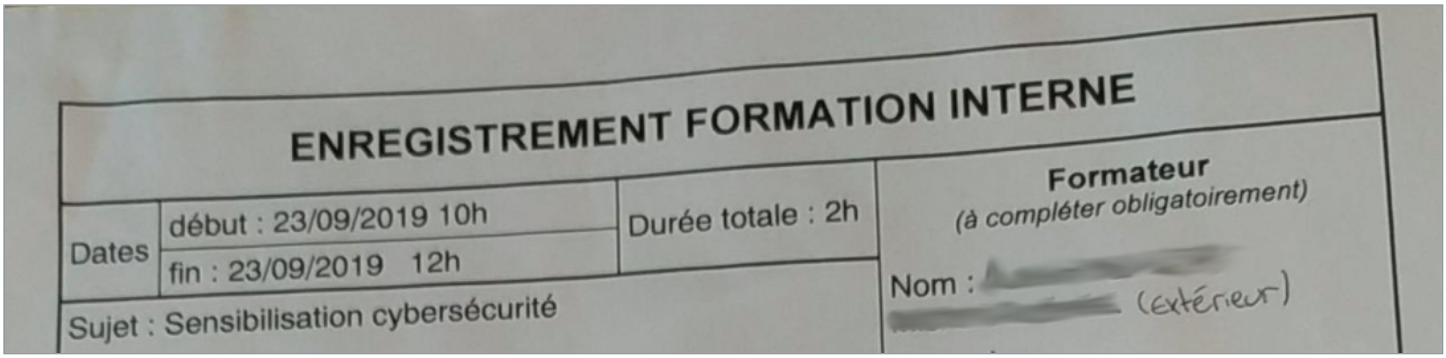
« J'ai pu accéder à tous les mdp par défaut »

En juin 2019, Arnaud D. découvrait que le wiki de l'intranet de l'entreprise était accessible à n'importe qui, y compris depuis l'extérieur. Si les articles n'étaient accessibles qu'aux seules personnes connectées, « *tout le monde peut créer un compte et accéder à absolument tout le contenu* », comme il l'expliquait alors par mail à ses supérieurs.

« *J'ai testé en créant le compte "test" et "bidule" et j'ai pu accéder à tous les articles qui contiennent beaucoup d'informations très sensibles (et les modifier), mdp par défaut, adresse ip, configuration VPN… Il faudrait limiter les accès assez rapidement* ». Dans la foulée, la création de compte avait été bloquée.

Il découvrait également que n'importe qui pouvait accéder à l'extranet, depuis le web, en utilisant « *test:test* » comme identifiants. Ce qui permettait notamment d'accéder aux tickets ouverts par les hôpitaux et laboratoires clients de Dedalus, où figuraient entre autres leurs identifiants et mots de passe de téléadministration TeamViewer.

En septembre, il faisait venir un responsable de l'ANSSI pour une « *formation interne* » de « *sensibilisation (à la) cybersécurité* » à dix de ses collègues, dont huit supérieurs hiérarchiques. Sur la feuille d'émargement, que nous avons pu consulter, Arnaud D. était présenté comme « *formateur* », aux côtés du responsable de l'ANSSI.


ENREGISTREMENT FORMATION INTERNE

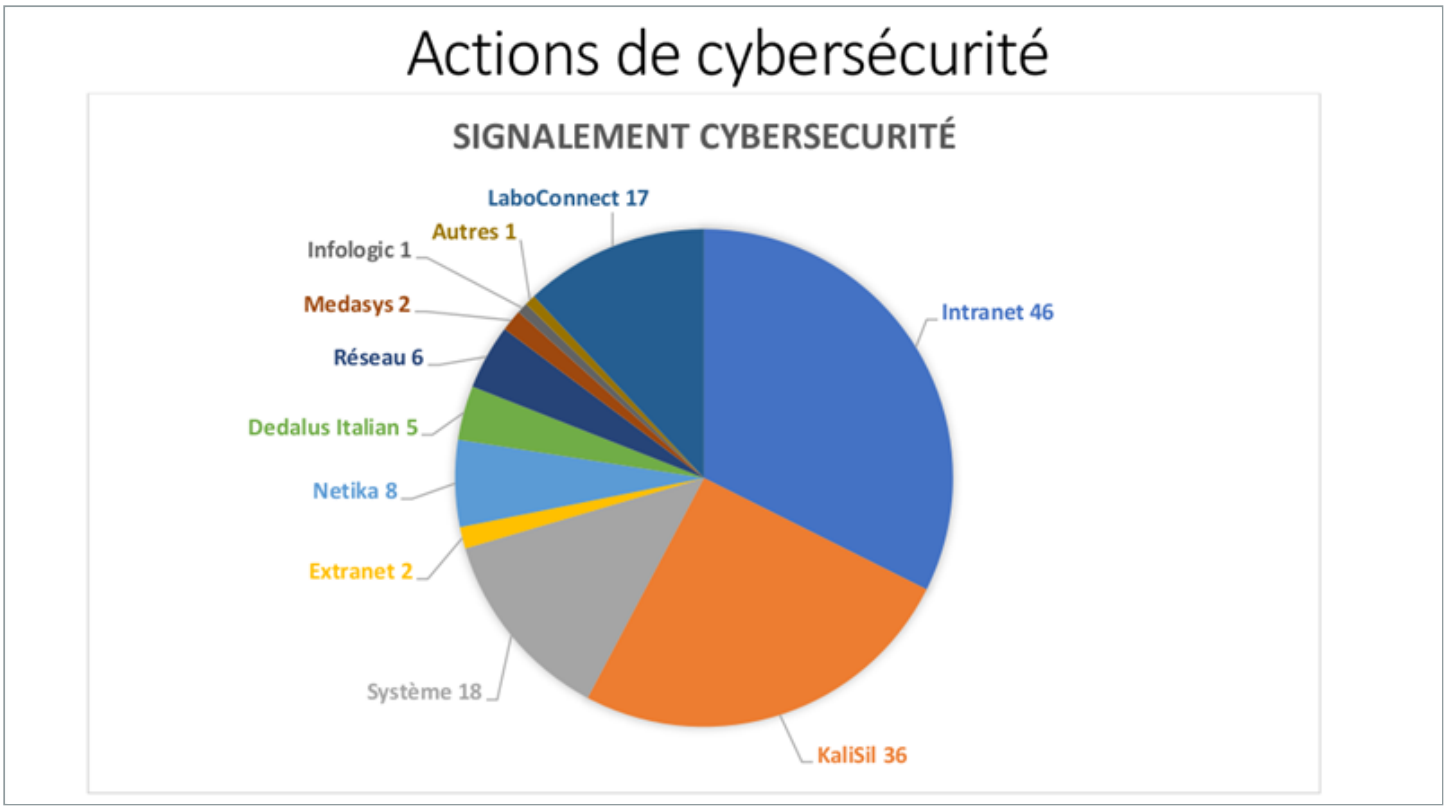
Dates	début : 23/09/2019 10h fin : 23/09/2019 12h	Durée totale : 2h	Formateur (à compléter obligatoirement) Nom : [redacted] (extérieur)
Sujet : Sensibilisation cybersécurité			

« N'importe qui peut accéder à toutes les données de nos clients »

Cherchant à faire reconnaître et valoriser ses compétences et son expertise en la matière, Arnaud D. écrivait à la DRH, en novembre 2019, afin de bénéficier d'une évolution salariale et de faire figurer « *un titre de sécurité informatique sur ma fiche de poste 2020, ainsi qu'une rémunération reflétant mon niveau d'expertise* ».

Dans un email qu'il nous a transmis, il listait à ce titre les 142 « *actions (et) signalements de cybersécurité* » qu'il avait effectué depuis son recrutement, un an et demi plus tôt. Au-delà du test de LaboConnect diligenté à la demande du DG, il détaillait également celui de leur CRM Intranet, qui avait mis en évidence « *de gros problèmes de sécurité pouvant compromettre notre sécurité et celle de nos*

Il rappelait que « *mon manager a reconnu mes compétences en sécurité informatique et m'a octroyé deux jours par mois pour effectuer de l'amélioration continue en sécurité informatique* ».



En décembre, il alertait sa hiérarchie : « *n'importe qui peut recopier le code source du nouvel extranet* », qui était accessible sur le web. « *Heureusement que je l'ai vu, si une personne avait eu accès au code source il aurait pu récupérer les identifiants d'accès à l'API de l'intranet et accéder à toutes les données de nos clients* ».

Début janvier, il les alertait de nouveau au sujet de trois autres vulnérabilités. La première permettait, à partir de quelques mots clefs sur Google, de retrouver « *une grande partie des serveurs de résultats de* [ses] *clients* ». La seconde d'accéder, sur ces serveurs, à des répertoires non protégés.

La troisième de s'y connecter, en root, grâce au « *mot de passe par défaut* » largement documenté dans leurs procédures internes. « *Connu par tous* », il figurait sur le wiki qui avait longtemps été accessible depuis le web et qu'il venait, quelques mois plus tôt, de protéger. Or, ce mot de passe, non content d'être « *constitué de six consonnes en minuscules* », n'avait en outre pas été modifié entre temps.

« Deux ans maintenant que je corrige des failles critiques »

Mi-janvier 2020, il venait aux nouvelles de sa demande d'évolution vers un poste de « ***pentester*** », arguant du fait que « *le CTO a confirmé que je devais mettre à profit mes compétences de sécurité avec le RSSI* » (responsable de la sécurité des systèmes d'information). Il soulignait qu'il venait de lui signaler une « *fuite de 4 giga-octets de données* » et une autre « *de 1 400 emails de clients* », toutes deux sur des serveurs accessibles sans mot de passe.

cybersécurité de manière reconnue, cela fait déjà presque deux ans maintenant que je corrige des failles critiques. La sécurité informatique est quelque chose de très important aujourd'hui dans le domaine de la santé, en tant que leader européen nous sommes une cible évidente ».

En réponse, la DRH rappelait lui avoir déjà expliqué, lors de leur entretien de décembre, que : « *le RSSI venait d'être nommé (deux jours auparavant), je t'ai donc indiqué qu'il lui fallait prendre la pleine mesure de sa mission puis identifier les besoins pour la mener à bien* », et qu'« *il était bien trop tôt* » pour valider sa demande d'évolution.

Elle le remerciait pour ce qu'il avait fait jusque là en termes de sécurité, mais ne l'invitait pas moins à : « *te concentrer sur les objectifs définis par ton manager, et te canaliser sur les sujets sur lesquels tu es attendu* ».

« Ça les dérangeait que je pointe du doigt ce qui n'allait pas »

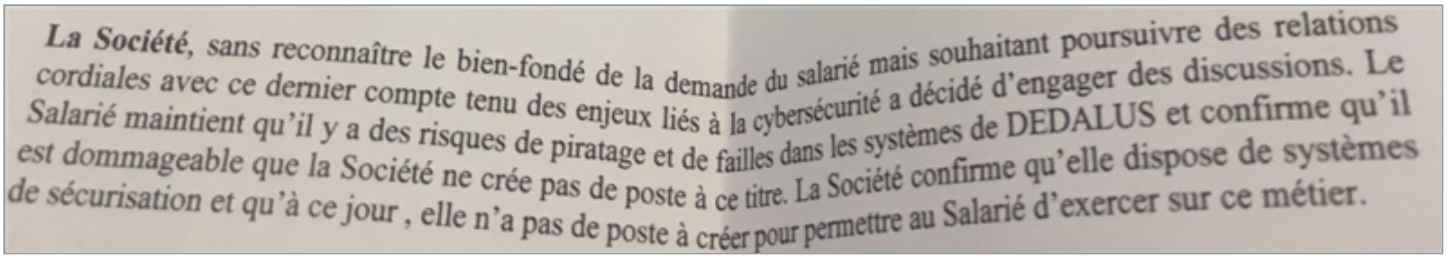
Après avoir été rappelé à l'ordre par l'un de ses N+1 de sorte qu'il se concentre sur son travail « *plus assidument* », qu'il respecte le pointage de son emploi du temps, et cesse donc de traquer les failles de sécurité, Arnaud D. faisait une nouvelle découverte, début février. Dedalus venait de nouveau de racheter une entreprise.

Au vu du nombre de failles qu'il avait précédemment identifiées, Arnaud D. chercha à s'assurer qu'elle ne pâtissait pas, elle aussi, de tels problèmes de sécurité. Découvrant là encore des serveurs non protégés, il alerta aussitôt sa hiérarchie, en mettant le PDG et le RSSI (notamment) en copie.

Fin février, dépité de voir que ses « *alertes* » en interne, n'étaient pas écoutées, il envoyait au CTO italien de Dedalus le fichier Excel où il avait répertorié l'essentiel de ses découvertes. Sur 78 failles de sécurité, 65 étaient exploitables depuis le web. 20 avaient été corrigées, 20 étaient estampillées « à faire », 38 ne l'avaient donc toujours pas été.

Ce mail fut la goutte d'eau. Dedalus lui proposa en effet dans la foulée de signer un protocole transactionnel au motif, explique Arnaud D., que « *ça les dérangeait que je pointe du doigt ce qui n'allait pas, car la sécurité n'est pas mon job de "développeur" et ce n'est pas le focus de la direction* ».

Dans son article 1, le protocole précisait que « *le salarié maintient qu'il y a des risques de piratage et de failles dans les systèmes Dedalus et confirme qu'il est dommageable que la société ne crée pas de poste à ce titre. La société confirme qu'elle dispose de systèmes de sécurisation et qu'à ce jour, elle n'a pas de poste à créer pour permettre au salarié d'exercer sur ce métier* ».



La Société, sans reconnaître le bien-fondé de la demande du salarié mais souhaitant poursuivre des relations cordiales avec ce dernier compte tenu des enjeux liés à la cybersécurité a décidé d'engager des discussions. Le Salarié maintient qu'il y a des risques de piratage et de failles dans les systèmes de DEDALUS et confirme qu'il est dommageable que la Société ne crée pas de poste à ce titre. La Société confirme qu'elle dispose de systèmes de sécurisation et qu'à ce jour , elle n'a pas de poste à créer pour permettre au Salarié d'exercer sur ce métier.

Début mars, il prenait attache avec un haut responsable gouvernemental en charge de la cybersécurité qu'il avait rencontré lors d'un salon l'an passé afin de lui exposer la situation. Se présentant comme un « *lanceur d'alerte* », il lui expliqua : « *en tant que réserviste cyberdéfense, je suis totalement abasourdi* » par les réponses des responsables. Il demanda s'il pouvait être mis en relation avec « *une personne au sein du gouvernement pour faire comprendre à la direction* [de Dedalus, ndlr] *l'importance de la cybersécurité* ».

Ce dernier le renvoya à un haut fonctionnaire de défense et de sécurité (HFDS), responsable de la cybersécurité au sein d'un ministère, qui répondit au lanceur d'alerte qu'il allait demander à ses équipes de vérifier, et qu'il protégerait son anonymat. Le 16 mars, du fait du confinement et du peu de perspectives d'embauche, Arnaud D. préféra finalement dénoncer le protocole transactionnel.

Le 22 mars, il découvrit que l'AP-HP faisait l'objet d'une cyber-attaque. Puis que l'AP-HP figurait au nombre des clients de Dedalus et que plusieurs de ses serveurs étaient répertoriés sur **shodan.io**, le moteur de recherche des appareils connectés. Or, la clef privée (.rsa) permettant d'obtenir un accès root à l'ensemble des autres serveurs de son employeur se trouvait dans une sauvegarde inopportunément accessible sur l'intranet (non protégé) de l'entreprise, ainsi que sur un autre serveur de Netika à l'étranger.

« Un peu plus de 150 structures vulnérables »

Arnaud D. téléchargea, depuis son poste de travail et donc sans chercher à se cacher, la clef privée utilisée pour accéder aux serveurs de Dedalus, afin de vérifier si c'était la même que celle qu'il avait trouvée via shodan. Elle n'avait pas été changée, l'ensemble des serveurs de Dedalus étaient donc à haut risque.

En urgence, il tenta d'alerter le CTO et le PDG italien du groupe, en vain : du fait du confinement, ils avaient d'autres urgences et problèmes à régler. Arnaud D. recontacta donc le haut fonctionnaire avec qui il avait échangé. Comme le narre sa notification de « *licenciement pour faute grave* », le DG de Dedalus France fut de fait contacté dans la foulée par « *le Pôle Cybersécurité du gouvernement* », de sorte de colmater la brèche, en urgence.

Dans un courrier qu'il lui a adressé (et que nous reproduisons, anonymisé), le haut fonctionnaire – qui n'a pas répondu à nos questions – confirme que « *c'est uniquement après avoir alerté ses supérieurs sans succès qu'il a décidé de lancer l'alerte* », mais également qu'au-delà du serveur de l'AP-HP affecté, « *une autre recherche nous a permis d'identifier un peu plus de 150 structures vulnerables* ».

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE

SERVICE DU HAUT FONCTIONNAIRE DE DEFENSE ET DE SECURITE
(HFDS)

Fonctionnaire de sécurité des systèmes d'information

Paris, le 02mai 2020

Le fonctionnaire de sécurité des systèmes d'information

Je soussigné , fonctionnaire de sécurité des systèmes d'information avoir été alerté par monsieur employé du groupe Dedalus (Éditeur de logiciel de santé) le 25 mars 2020.

Il nous a indiqué que c'est uniquement après avoir alerté ses supérieurs sans succès, qu'il a décidé de lancer cette alerte. Il nous a simplement alerté sur le fait que des laboratoires étaient potentiellement exposés à une vulnérabilité permettant d'accéder à leurs systèmes d'information avec le plus haut privilège d'exploitation et ainsi de s'en rendre maître.

. En pleine crise COVID-19, nous avons immédiatement investigué sur cette éventuelle vulnérabilité.

Une simple recherche internet nous a permis de trouver un accès à un intranet ouvert, utilisé par la société Dedalus, permettant de récupérer la clef privée donnant accès aux serveurs mis en place dans différents laboratoires. Une autre recherche, nous a ainsi permis d'identifier (à commencer par le CHU d'Angers) un peu plus de 150 structures vulnérables.

Le 26 mars, après avoir repris contact avec pour lui indiquer que j'allais prendre attache avec sa direction en préservant son anonymat comme lanceur d'alerte, j'ai personnellement alerté le groupe Dedalus le jour même. Il leur a été donné les éléments récupérés ainsi que la liste des structures concernées. Le groupe Dedalus a fait le nécessaire pour sécuriser ces accès et proposé une nouvelle version du logiciel. Nous avons eu un retour concernant cette montée de versions par la société Française d'informatique de laboratoire le 02 avril 2020.

« Un acte de "non-assistance à personne en danger" »

Dedalus n'en a pas moins décidé, depuis, de le mettre à pied à titre conservatoire puis de le licencier « *pour faute grave* ». Son attestation de licenciement, que nous avons pu consulter, détaille trois raisons.

D'une part : « *malgré nos demandes de vous conformer à votre contrat de travail en restant focalisé sur le métier et les missions pour lesquels nous vous avons recruté, vous n'aviez d'autre souhait que d'être affecté sur une activité en Cybersécurité* ».

l'entreprise ». Et ce, alors même que ces managers ont « *instamment demandé de consacrer 100 % de votre temps de travail à développer conformément à la mission pour laquelle vous avez été recrutée* » (nous avons laissé les fautes telles que présentes dans son attestation).

Enfin, pour ne pas avoir informé son entreprise au préalable. Dans le compte-rendu de son entretien préalable à sa mise à pied à titre conservatoire, il explique que faute d'avoir « *été pris au sérieux lors de ses précédentes alertes, il voulait donc informer des personnes "plus hautes" dans la hiérarchie* ». Ce pour quoi il avait d'abord tenté de contacter le CTO et le PDG italiens du groupe avant d'alerter, au vu de l'état d'urgence, le haut fonctionnaire.

Dedalus lui reproche enfin d'avoir « *délibérément fait une fausse déclaration sur* [sa] *réelle activité, ce qui dans une période de télétravail est intolérable puisque cette dernière bafoue le principe même de confiance et du principe de loyauté, base de la relation de travail* ». Arnaud D. avait en effet téléchargé la clef privée sur le réseau interne, « *entre 11h40 et 11h48* », alors même qu'il avait déclaré sur la feuille de pointage avoir effectué, de 9h50 à 12h, les tâches qui lui avaient été assignées.

«*Lors de l'entretien,* précise la notification de licenciement*, vous nous avez déclaré que pour vous, la recherche de cette potentielle faille était un acte de bienveillance considérant que vos managers n'appréciaient pas à sa juste valeur le risque que vous remontiez, ce qui était assimilable à un acte de "non-assistance à personne en danger", pour reprendre vos termes* ». Des arguments qui « *ne nous ont pas permis d'envisager une autre décision que de vous notifier votre licenciement pour faute grave* ».

« Seuls les tickets portant sur les fonctionnalités qui rapportent de l'argent sont traités »

Sous couvert d'anonymat, un autre ex-salarié témoigne :

> « *Dès qu'il y a des problèmes de sécurité, ils ne nous disent rien, les développements sont mis en "privé" pour que ça ne s'affiche pas chez le client et qu'ils apprennent l'existence de failles, mais personne ne les traite. Au boulot ils font tout pour qu'on en sache le moins.*
>
> *Ils font pas forcément les mises à jour, travaillent avec de vieilles technologies, à l'ancienne. À chaque fois qu'on propose des améliorations techniques ou de sécurité, on nous répond que c'est pas ça qui paie, alors qu'ils ont des contrats de maintenance.*
>
> *Et seuls les tickets portant sur les fonctionnalités qui rapportent de l'argent sont traités. Et même quand des failles sont corrigées, c'est pas déployé. Les nouveaux clients bénéficient de la mise à jour, mais pas les anciens* ».

« Il serait dommage de chercher à ternir l'image du groupe »

Notre enquête nous a par ailleurs permis de découvrir que, quatre mois après que Dedalus ait pourtant été invité à corriger la faille de sécurité que le lanceur d'alerte avait identifié, une clef privée (.rsa) était encore accessible cet été sur un autre serveur non sécurisé.

à d'autres problèmes de sécurité pouvant concerner des données de santé.

Contactée, Dedalus n'a pas voulu répondre à nos questions détaillées et circonstanciées (que vous trouverez plus bas) sur l'absence de RSSI ou de procédure de protection des lanceurs d'alerte notamment, préférant botter en touche, et nous accuser de « *chercher à ternir l'image* » du groupe :

> *« Dans un contexte sanitaire aussi grave, les enjeux de notre Groupe demeurent d'accompagner au mieux nos clients et, bien évidemment, de renforcer leur confiance. La place de la sécurité ne cesse de s'accroître et nous y sommes particulièrement attentifs. Nous sommes également bien entendu à l'écoute des conseils et recommandations que nous pouvons recevoir, qu'ils émanent de sources internes ou externes.*
>
> *Concernant Monsieur D., les motifs de la rupture du contrat de travail n'ont pas de lien avec une situation ou un rôle de lanceur d'alerte. Lorsque nous avons décidé de mettre un terme à notre collaboration, nous avons pris cette décision sur la base de faits précis. Il s'agit d'éléments confidentiels sur lesquels nous ne pouvons échanger avec vous. Monsieur D. a saisi le Conseil de Prud'hommes, comme le droit le lui permet, et cette instance jugera en fait et en droit du bien-fondé de ce licenciement.*
>
> *Nos équipes et notre entreprise ont été extrêmement mobilisées dans le cadre de la crise du COVID et il serait dommage de chercher à ternir, à partir d'un fait extrait de son contexte, l'image d'un Groupe dont la principale et unique mission est de fournir les meilleures solutions dans un domaine aussi sensible que la Santé ; environnement particulièrement encadré et certifié par différentes normes réglementaires, dans lesquelles nous évoluons depuis de nombreuses années. »*

La manière dont Dedalus semble avoir géré les problèmes de sécurité de ses filiales est d'autant plus incompréhensible que, non contente de se présenter comme « *leader européen en matière de solutions logicielles de Santé* », elle est également devenue un mastodonte financier, bien loin de la petite entreprise familiale qui avait initialement embauché Arnaud D.

En l'espace de trois ans seulement, elle est en effet passée du statut de PME de 70 salariés à celui de filiale d'un **groupe mondial** de plus de 5 500 collaborateurs, « *dont environ 2 000 uniquement dans la R&D* », générant « *plus de 700 millions d'euros de chiffre d'affaires* », mais sans pour autant que les moyens et process, en termes de cybersécurité, ne suivent cette hypercroissance.

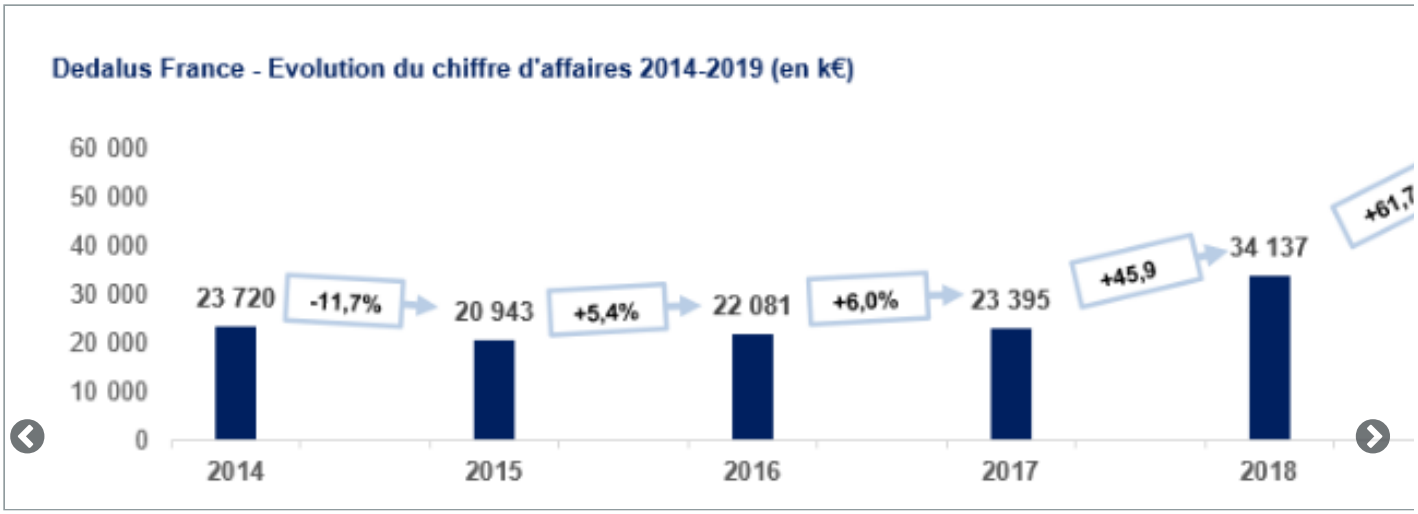
+136 % de chiffre d'affaires

Cotée en bourse au **Compartiment C** (qui réunit les entreprises dont la capitalisation boursière est inférieure à 150 millions d'euros) d'Euronext Paris, l'entreprise qui avait racheté Netika, Medasys, **annonçait** un chiffre d'affaires de 18 millions d'euros en 2017, et de 29,4 millions en 2019, ses effectifs passant de 146 à 259 employés.

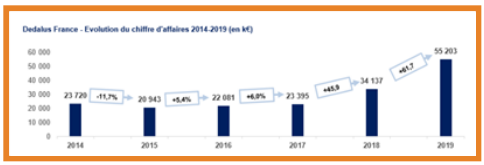
À l'occasion d'une offre publique d'achat (OPA) simplifiée **lancée** fin juin par Dedalus Italia – actionnaire majoritaire de Medasys – en prévision d'une fusion absorption d'Agfa France par Dedalus France, on apprenait par ailleurs qu'en incluant ses filiales, le chiffre d'affaires de Dedalus France était passé de 23,4 à 55,2 millions d'euros.

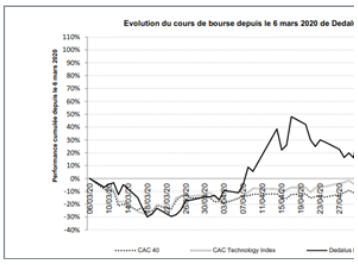
octobre 2018, des sociétés DL Santé et Infologic-Santé (leader en France dans les solutions d'anatomopathologie et de génétique), ainsi que par l'entrée dans le Groupe, en juillet 2019, de la société WEB100T (société d'édition de logiciels de gestion médico-administrative et médicale dédiés aux établissements de santé principalement privés) ».

Pour autant, le **cours** de son action a régulièrement baissé depuis son introduction en Bourse fin 1998 :



CA de Dedalus France





« Un objectif clair : asseoir notre réputation en tant qu'"entreprise citoyenne" »

Sur son **site web**, le groupe Dedalus se présentait en juin comme « *le premier fournisseur de logiciels de santé et de diagnostic en Europe et l'un des plus importants au monde* », employant plus de 3 400 collaborateurs « *hautement qualifiés* », et disposant de « *la plus grande équipe de logiciels de R&D du secteur en Europe avec plus de 1 100 personnes* », travaillant pour « *plus de 5 000 hôpitaux et 4 800 laboratoires à travers le monde* ».

américaine **DXC Technology**, faisant de Dedalus « *un acteur mondial dans le domaine des solutions logicielles hospitalières et diagnostiques* ».

Une acquisition qualifiée de « *pas décisif vers la consolidation du marché européen et mondial* » par **Ardian** (ex-AXA Private Equity). Cette société française de capital-investissement, qui avait **acquis** 60 % de Dedalus en 2016, en détient aujourd'hui 75 %. « *Avec 100 milliards de dollars gérés et/ou conseillés en Europe, en Amérique et en Asie* », et plus de 150 entreprises **en portefeuille**, Ardian est l'« *un des leaders mondiaux de l'investissement privé* ».

Sa présidente, **Dominique Senequier**, **figure** depuis plusieurs années dans le top 20 du classement de Forbes des femmes les plus puissantes du monde. Sur LinkedIn, Dedalus France **précise** prévoir d'« *investir en R&D plus de 80 millions d'euros sur les cinq prochaines années* », afin de répondre « *à un objectif premier : positionner le patient au cœur du Système d'Information Clinique* ».

En mai dernier, elle **employait** « *400 collaborateurs* », et explique sur son **site web** que son métier est de permettre aux établissements d'« *optimiser et de fiabiliser les processus médicaux dans une logique de sécurité patient, de performance et de maîtrise des coûts* ».

Sa page « ***démarche qualité*** » précise que « *nos solutions répondent sur l'ensemble des points exigés par la norme, à savoir : traçabilité, confidentialité, sécurité, intégrité, interopérabilité, disponibilité* ». Mais également, en terme de responsabilité sociétale de l'entreprise, que « *la mise en place de politiques responsables nous permet de cibler un objectif clair : asseoir notre réputation en tant qu'"entreprise citoyenne"* ».

Vers une saisine du Défenseur des droits

Faute de réponse, difficile de savoir si Dedalus a, à ce jour, mis en œuvre la procédure de protection des lanceurs d'alerte. Une protection pourtant prévue par la loi dite **Sapin II** de 2016 « *relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique* ».

Elle dispose notamment qu'« *un lanceur d'alerte est une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi (…) une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance* ». Mais également que « *tout salarié ayant signalé une alerte, dans le respect des conditions prévues par la loi, ne pourra faire l'objet d'une procédure de licenciement* » dès lors que « *le signalement d'une alerte est porté à la connaissance du supérieur hiérarchique, direct ou indirect, de l'employeur ou d'un référent désigné par celui-ci* », comme Arnaud D. dit l'avoir fait.

La loi précise en outre qu'« *en l'absence de diligences de la personne destinataire de l'alerte mentionnée (…), celui-ci est adressé à l'autorité judiciaire, à l'autorité administrative ou aux ordres professionnels. En dernier ressort, à défaut de traitement par l'un des organismes mentionnés au deuxième alinéa du présent I dans un délai de trois mois, le signalement peut être rendu public* ». Ce que Arnaud D. dit avoir précisément respecté et mis en œuvre.

On ne sait si Dedalus a mis en place les « *procédures appropriées de recueil des signalements émis par les membres de leur personnel ou par des collaborateurs extérieurs et occasionnels sont établies par les personnes morales de droit public ou de droit privé d'au moins cinquante salariés* » instaurées par cette loi.

aimerait toujours pouvoir évoluer vers la cybersécurité.

Voici la liste des questions que nous avions posées à Dedalus :

- "Leader en informatique de Santé", Netika/Medasys/Dedalus sont censés aborder "by design" et "by default" les questions de sécurité et de confidentialité des données informatisées (au vu de la loi informatique et libertés, du RGPD, ainsi que du caractère particulièrement sensible des données de santé que vous traitez); pourquoi avoir attendu décembre 2019 pour nommer un RSSI @Netika/Medasys ?

- Qui y était, préalablement, en charge des questions de cybersécurité ?

- Comment expliquez-vous que ses supérieurs aient par la suite, en début d'année, demandé à Arnaud D. d'arrêter de chercher d'éventuels problèmes de cybersécurité dans vos systèmes, infrastructures et logiciels, alors qu'il avait pourtant et préalablement réussi à identifier (et dûment notifié à sa hiérarchie) plus d'une centaine de failles avérées ou potentielles ?

- Avez-vous mis en place un dispositif de protection des lanceurs d'alerte, comme le prévoit la loi dite "**Sapin 2**" ?

- Pourquoi n'avez-vous pas accordé le statut de "lanceur d'alerte" à Arnaud D. alors que vous avez bel et bien corrigé la faille de sécurité que le CERT de l'ANSSI avait estimée suffisamment grave pour vous la notifier et vous demander de la corriger dans la foulée ?

- Quelles mesures avez-vous prises depuis que le pôle cybersécurité du gouvernement vous ait alerté du fait que cette clef privée .rsa était accessible sur un serveur non protégé ?

- Avez-vous pu déterminer si la faille de sécurité avait été exploitée ? Et l'avez-vous **notifié à la CNIL** ?

- Comment expliquez-vous que, 3 mois après, une autre clef privée .rsa était elle aussi toujours accessible, ainsi qu'un répertoire non protégé, sur un autre serveur, en juillet dernier (ce que nous avions alors notifié au CERT de l'ANSSI, qui nous a dans la foulée confirmé vous avoir alerté à ce sujet, la faille ayant de fait été corrigée immédiatement après) ?

- Quels sont les moyens, procédures et dispositifs mis en place par Dedalus pour vérifier que les enjeux et problèmes de cybersécurité et de protection des données personnelles sont dûment pris en compte par les (nombreuses) entreprises qu'elle acquiert (et a acquises ces dernières années) ?

Si vous voulez témoigner ou me contacter de façon sécurisée (voire anonyme), le mode d'emploi **se trouve par là**.

59 commentaires

KP2 - 02/10/20 à 17:19:53 **#1**

Hé bé... Je sens que les Prud'hommes vont se régaler avec cette histoire.

Y'a beaucoup trop de cas de soit-disant "lanceurs d'alertes" qui ne sont en fait que des glands qui cherchent à se victimiser. Mais là, je crois qu'on a un beau cas réel et documenté d'un gars qui a vraiment fait un boulot de lanceur d'alerte dans les règles et qui s'est fait jeter pour ça.
Dans une boite de softs médicaux en plus.

J'espère que ce groupe se fera secouer les pruneaux et qu'il sera condamné a verser un beau chèque à Arnaud D

Idiogène - 02/10/20 à 17:24:50 **#2**

Le questionnaire en bas de page fait plaisir.

darkjack - 02/10/20 à 17:25:02 **#3**

Franchement, faut avoir du courage pour être lanceur d'alerte...

Obidoub - 02/10/20 à 17:25:42 **#4**

Merci pour l'article.
Il ne reste pas beaucoup d'autres solutions que d'afficher ces entreprises sans éthique.
Pas besoin de chercher des complots, les actions sont commises sans se cacher: t'es lanceur d'alerte, au mieux tu es licencié, au pire traîné en justice...

Buffort - 02/10/20 à 17:27:44 **#5**

> **darkjack a écrit :**
>
> Franchement, faut avoir du courage pour être lanceur d'alerte...

Ouai, et pas qu'un peu !

Je viens d'apprendre qu'il existait une Maison des Lanceurs d'Alerte. Je trouve que c'est une excellente idée, c'est ... rassurant, de mon point de vue.

Idiogène - 02/10/20 à 17:31:11 **#6**

darkjack - 02/10/20 à 17:31:55 **#7**

Buffort Ah cool, connaissais pas. C'est une super initiative!

Et j'ai l'impression que l'auteur de l'article est chaud bouillant sur le sujet
"Si vous voulez témoigner ou me contacter de façon sécurisée (voire anonyme), le mode d'emploi se trouve par là "

Merci Jean-Marc pour cet article et vive les lanceurs d'alertes!

Sheepux - 02/10/20 à 17:35:27 **#8**

KP2 pas forcément simple. Si la personne n'a pas travaillé sur son travail c'est en effet une faute grave (après rappels à l'ordre via un blâme).
Par contre lancer une alerte sans "piétiner" sur son travail aurait été sans problème (la lettre de licenciement joue sur cela).

David_L - 02/10/20 à 17:38:59 **#9**

darkjack C'est précisé à chaque fin d'article de JMM ;)

Le_CuLtO - 02/10/20 à 17:45:05 **#10**

darkjack Franchement, quand t'es développeur en 2020, tu peux te permettre sereinement ce genre de choses. Le mec met son cv sur internet et reçoit 1 coup de fil toutes les 5min.

Il n'est plus possible de commenter cette actualité.

« ‹ **Page 1 / 6** › »