

Addictions en série

Gouvernements européens, il est temps de chasser le colon Microsoft

Une enquête réalisée par un consortium de neuf journalistes européens met à jour les risques qui dérivent de la dépendance des gouvernements à Microsoft — aucun n'est indemne...

Même si çà et là des efforts sont notés pour migrer vers des solutions *open source* voire libres, l'adversaire est impitoyable et utilise un arsenal bien rodé.

Combien faudra-t-il encore de telles enquêtes pour provoquer une prise de conscience et pour que les décisions nécessaires soient prises et mises en œuvre ?



Traducteurs : PasDePanique, Paul, dominix, Asta, Luc, MO, lyn., Jérochat, simon, LP, Opsylac, Paul, Hello, Mika + 5 anonymes

L'addiction de l'Europe à Microsoft, un énorme risque pour la sécurité

Nous vous proposons ici une traduction de l'article paru dans *Der Tagesspiegel*, qui correspond à une partie de l'enquête menée par neuf journalistes européens dans leurs pays respectifs sur les relations entre Microsoft et les institutions publiques, chacun traitant de la situation particulière dans son pays (voir les différents articles déjà publiés ici). L'hebdomadaire *Marianne* a publié l'article de de Leila Minano dans son édition du 19 mai sur la situation française, intitulé Microsoft : menace sur la sécurité de l'État.

Le 13 mai 2017

par Crina Boros, Wojciech Ciesla, Elisa Simantke, Ingeborg Eliassen, Leila Minano, Nikolas Leontopoulos, Maria Maggiore, Paulo Pena et Harald Schumann



Le Parlement européen de Strasbourg - Photo par Frédéric Chateaux (CC BY-SA 2.0)

Le 12 mai 2017, des hackers ont frappé plus d'une centaine de pays à l'aide d'un outil volé à la NSA, en ciblant des vulnérabilités des logiciels Microsoft. Les attaques ont infecté uniquement des appareils fonctionnant avec le système d'exploitation Windows. Parmi les victimes, on compte plusieurs organismes publics, par exemple les hôpitaux du NHS (National Health Service, Service national de santé) au Royaume-Uni. Investigate Europe a passé des mois à enquêter sur l'extrême dépendance des pays européens envers Microsoft et les risques que cela implique pour la sécurité. Lisez notre enquête complète.

Nota bene : cet article est une traduction de la version anglaise d'un billet d'Investigate Europe publiée le 13 mai 2017. Pour savoir dans quelles publications de presse, pays et langues le billet est disponible, veuillez consulter cette page.

En général, lorsque le conseil municipal de Munich se réunit, ça n'intéresse pas grand-monde en dehors du périmètre de la ville. Mais en ce jour de février, tout est différent. Dans le grand hall du magnifique hôtel de ville néogothique, tous les sièges réservés à la presse et aux spectateurs sont occupés. Ceux qui n'ont pas trouvé de place se tiennent debout dans les allées. Des membres du conseil rapportent qu'ils ont reçu des courriels et des demandes de médias en provenance de toute l'Allemagne et de toute l'Europe.

Et pourtant l'événement semble purement technique. Pendant dix ans, des experts ont travaillé à migrer le système informatique de la ville vers des logiciels libres et ouverts. Les coûteux logiciels de l'entreprise américaine Microsoft ne sont désormais plus utilisés qu'exceptionnellement. Cela n'a pas seulement permis à la ville d'économiser plusieurs millions d'euros de frais de licences, mais a aussi rendu le système plus sûr - « un franc succès », ainsi que l'annonçaient en 2014 les responsables politiques de la ville. Mais, aujourd'hui, le maire, Dieter Reiter, et sa grande coalition rassemblant le Parti Social-Démocrate (SPD), de centre-gauche, et l'Union Chrétienne Sociale (CSU), de centre-droit, souhaitent ramener chez Microsoft les 24 000 ordinateurs de la ville.

Les débats sont animés. M Reiter et ses sympathisants ne réussissent pas à donner d'arguments convaincants - ni à dire combien pourrait coûter la transition. La décision est donc reportée. Le chef du groupe parlementaire des Verts, Florian Roth, est agacé : « Cela ne semble être rien de plus qu'un jeu de pouvoir politique, dit-il, mais un jeu à haut risque ». Il ajoute en guise

d'avertissement : « Voulons-nous vraiment rendre notre administration éternellement dépendante du monopole de l'américain Microsoft ? »

Dans toute l'Europe, les systèmes informatiques des administrations publiques reposent sur les programmes de Microsoft

Le problème n'est absolument pas exagéré et ne se limite pas à Munich. Dans l'Europe entière, de la Finlande au Portugal, de l'Irlande à la Grèce, les technologies informatiques dans les administrations publiques reposent sur les programmes de l'éditeur de logiciels états-unien. Et puisque les systèmes numériques continuent à grandir et à prendre de plus en plus d'importance, les États deviennent de plus en plus dépendants de cette unique entreprise. La Commission européenne a même admis qu'elle était « concrètement captive de Microsoft ».

Quelles sont les conséquences de ce *lock-in*, comme on l'appelle dans le jargon technique, qui nous attache à un seul fournisseur ? Et comment les gouvernements peuvent-ils gérer cela ? L'équipe de journalistes d'Investigate Europe s'est lancée pendant trois mois dans une mission d'exploration pour établir des faits et interviewer des économistes, des responsables informatiques, des experts en sécurité et des politiciens dans douze pays européens, ainsi qu'à la Commission et au Parlement européens. Les résultats sont inquiétants.

La dépendance des États envers Microsoft :

- engendre des coûts en hausse constante et bloque le progrès technique au sein des autorités publiques ;
- contourne systématiquement les lois européennes en matière de passation des marchés et de règles de concurrence ;
- introduit une influence politique étouffante de la part de cette entreprise ;
- crée pour les systèmes informatiques étatiques, ainsi que pour les données de leurs citoyens, un grand risque technique et de sécurité politique.

Microsoft n'a souhaité répondre à aucune des questions d'Investigate Europe sur ces sujets. Et les personnels qui travaillent au sein des services informatiques des

administrations savent pourquoi.

« De nombreuses administrations publiques sont tellement dépendantes de cet unique fournisseur qu'elles n'ont plus aucune liberté quand il s'agit de choisir un logiciel. Cela signifie que les États européens risquent de perdre le contrôle sur leurs propres infrastructures informatiques », avertit l'ingénieur informaticien et avocat Martin Schallbruch. Jusqu'à 2016, il était directeur du département des nouvelles technologies et de la cybersécurité au ministère de l'Intérieur fédéral allemand. Schallbruch n'est que trop familier de cette situation précaire. Si on voulait écarter ce danger et « basculer vers une architecture numérique indépendante, cela demanderait d'énormes investissements », déclare ce responsable informatique expérimenté, qui mène désormais des recherches au sein de l'école de commerce de Berlin ESMT.

Le problème n'est pas seulement grave, il est aussi complexe. Au cœur des enjeux se trouve le modèle économique de Microsoft. Le géant des logiciels, basé à Redmond dans l'État de Washington aux États-Unis, vend ses logiciels, en particulier le système d'exploitation Windows et les programmes de bureautique tels que Word, Excel, Powerpoint et Outlook, en tant que produits sous licence. Dans le métier, on qualifie ce type de logiciel de « propriétaire », ce qui signifie qu'il interdit à tout concurrent d'utiliser ses propres logiciels pour interpréter correctement les données encodées par les programmes de Microsoft. Concrètement, ce seront, par exemple, des titres, des tableaux ou des dates dont les données de mise en forme ou en page seront modifiées ou perdues.

C'est là la clé du monopole global de Microsoft - un business de rêve aussi ! Année après année, ce sont ainsi quelques 50 milliards de dollars que la multinationale empoche sous la forme de redevances de licences qui ne couvrent rien d'autre que la distribution de copies de ses programmes. Et parce que vos collègues, vos relations commerciales ou personnelles utilisent des fichiers Microsoft, cela paraît logique de faire de même, même si cela engage des frais, encore et toujours. La plupart des utilisateurs d'ordinateurs Apple, eux aussi, continuent d'acheter la suite Microsoft Office.

Les autorités administratives à la merci de

Microsoft

Les administrateurs des services informatiques de l'État sont parfaitement avertis de cet état de fait. Cette monoculture présente de sérieux désavantages. Dans d'autres secteurs, le développement logiciel adhère depuis longtemps à un principe complètement différent. Google ou Siemens, par exemple, travaillent en priorité avec des programmes dits *open source*, en d'autres termes des programmes dont le code est partagé librement. Dans ce cadre, n'importe quel programmeur ou entreprise peut utiliser le code, à la condition que le dernier arrivé mette chaque amélioration qu'il apporte au code à la disposition de tous. Cela signifie que les entreprises ne peuvent pas gagner d'argent en vendant ce genre de logiciel. Mais, dans le même temps, elles bénéficient du travail des programmeurs du monde entier sans avoir à les rémunérer.

Quels que soient les produits, de la centrale électrique à l'appareil de radiographie, Siemens a besoin d'un ensemble étendu de logiciels. « Or, 90 % d'entre eux réalisent des tâches de pure routine », explique Karsten Gerloff, informaticien du service concerné au sein de l'entreprise. « Pour cela, nous utilisons bien sûr des solutions *open source* ». L'entreprise utilise du « code propriétaire » uniquement pour des fonctionnalités précises, propres aux machines de Siemens. Si tous les logiciels devaient être mis au point par des équipes de l'entreprise, « ce sont 1 000 programmeurs de plus que nous devrions employer et nous ne serions plus compétitifs », indique M. Gerloff.

Le recours à la créativité d'une masse de cerveaux de par le monde engendre une dynamique bien plus forte que celui qui serait restreint aux seuls cerveaux d'une entreprise. C'est pourquoi « l'*open source* est maintenant la norme dans le domaine scientifique et économique » pour Matthias Kirschner, président de la *Free Software Foundation Europe* (FSFE), qui plaide pour une plus grande autonomie dans l'usage des technologies de l'information. Cela s'applique autant aux smartphones qu'aux superordinateurs, systèmes de commande des machines ou serveurs web. L'ancien modèle du monopole ne concerne plus que les logiciels d'ordinateurs de bureau et les suites bureautiques.

Il n'en reste pas moins que les administrations publiques s'appuient toujours sur ce vieux monopole, et pas uniquement pour la bureautique. Il existe des milliers d'applications dont seules les autorités ont l'usage. Qu'il s'agisse d'augmenter les impôts, de payer les retraites ou de calculer le coût de la collecte des déchets,

que ce soit dans la police, à la sécurité sociale ou dans les services de l'urbanisme, pour quasiment chaque service que rend l'État, il existe un logiciel opérationnel spécifiquement conçu pour cette tâche. Or, parce que le système d'exploitation Windows est utilisé partout, la plupart de ces « applications spécifiques » reposent sur ce système, mettant les autorités à la merci de son éditeur.

On a vu jusqu'où cela pouvait aller quand, à la fin de l'année 2014, Microsoft a cessé de fournir des mises à jour de sécurité pour Windows XP. Du jour au lendemain, des services publics partout en Europe se sont vus contraints de souscrire des contrats de service onéreux avec Microsoft afin de s'assurer que l'entreprise continuerait de colmater les failles de sécurité de son vieux système d'exploitation. Le gouvernement britannique a ainsi déboursé 6,5 millions de livres afin de disposer d'une année supplémentaire pour migrer ses ordinateurs vers Windows 7. Les Pays-Bas, ainsi que les länder allemands de Basse-Saxe et de Berlin, ont, eux aussi, payé plusieurs millions d'euros pour disposer d'un délai. « Il s'est passé la même chose dans toute l'Europe », confirme un expert de la Commission européenne. Et cela risque de se reproduire, vu que dans trois ans, c'en sera terminé des mises à jour de Windows 7.

La Commission européenne n'écoute pas ses propres experts

Dans le même temps, les États prennent du retard à cause du verrouillage de Microsoft. « Il n'existe pas de preuves formelles de ceci actuellement, mais il est logique de supposer que la dépendance envers un fournisseur unique ralentit le progrès technique dans le secteur public », prévient Dietmar Harhoff, directeur de l'institut Max-Planck pour l'innovation et la concurrence à Munich. Par exemple, si les municipalités pouvaient développer leurs centaines d'applications dédiées sur la base de programmes *open source*, chaque innovation pourrait être immédiatement utilisée par les services d'autres villes sans coût supplémentaire. « Ce potentiel est énorme pour le secteur public », selon D. Harhoff.

Dès 2012, la Commission européenne avait, par conséquent, lancé un programme au nom évocateur : « Contre le verrouillage ». L'idée était que les futurs appels d'offres publics portant sur l'achat de technologies informatiques et de logiciels ne comporteraient plus la mention explicite de noms d'entreprises et de

technologies « propriétaires » de ces dernières. À la place, les administrations publiques devaient s'astreindre à demander le recours à des « normes ouvertes » accessibles à l'ensemble des fabricants et éditeurs logiciels. Ce faisant, le monopole de Microsoft disparaîtrait au fil du temps dans la mesure où les problèmes de compatibilité ne se poseraient plus : les fichiers pourraient être lus par des logiciels concurrents, et cela sans perte de données. Si tous les services administratifs publics utilisaient les mêmes formats ouverts, on économiserait le prix des licences. « Les normes ouvertes créent de la concurrence, mènent à l'innovation et font économiser de l'argent », expliquait la commissaire à la Concurrence d'alors, Nellie Kroes. Selon ses experts, « le manque de concurrence » dans le secteur informatique et télécoms « coûte à lui seul 1,1 milliards d'euros par an au secteur public ».

Mais l'inertie des bureaucrates de l'État a eu raison des bonnes intentions, et l'initiative n'a abouti à rien. Pourtant, la législation européenne définit désormais des règles précises. Les administrations publiques nationales sont tenues de passer par des appels d'offres européens pour toute commande dont le montant excède 135 000 euros. Pour les autres organismes publics, cette règle s'applique pour des montants supérieurs à 209 000 euros. Quand ils achètent des logiciels standards pour leurs administrations, les gouvernements des États membres, comme un seul homme, passent outre la loi en vigueur et privilégient le fournisseur habituel Microsoft.

La mise en concurrence remplacée par de curieuses procédures

Une curieuse façon de procéder. Sans passer d'appel d'offres publics, les administrations négocient des réductions avec l'entreprise états-unienne et concluent des contrats-cadres sur cette base. Tous les groupements publics peuvent ensuite en profiter. Dans les offres ultérieures, ils cherchent uniquement des revendeurs qui leur vendront des licences Microsoft selon ces conditions. Il n'y a *de facto* aucune concurrence pour ces contrats publics.

En Allemagne aussi. En 2015, le ministère de l'Intérieur a convenu de nouvelles « conditions contractuelles » avec la filiale irlandaise de Microsoft, d'où la firme conduit ses affaires européennes pour optimiser ses impôts. Les rabais identifiés dans le nouvel accord peuvent être utilisés par tous les pouvoirs publics, du

ministère fédéral jusqu'à la petite municipalité. La ville de Dortmund a ainsi passé un appel d'offres, par exemple pour trouver un « distributeur pour le contrat BMI de licences Microsoft en volume ».

« C'est comme si l'État publiait une offre pour acheter des voitures, mais uniquement de revendeurs Volkswagen », se moque l'avocat néerlandais Matthieu Paapst, dont le doctorat à l'Université de Groningen a porté sur l'achat de logiciels dans le secteur public. Sa conclusion : « Se fournir en produits Microsoft, pour une administration publique, sans passer d'appel d'offres ouverts, viole la législation européenne en vigueur ». En vérité, selon l'avocat, la Commission européenne devrait engager des poursuites contre ce phénomène. L'unique raison pour laquelle elle s'en garde bien, c'est qu'elle n'applique pas elle-même les recommandations.

En effet, la Commission européenne a un contrat exclusif avec Microsoft, valable pour toutes les institutions de l'UE - elle ignore de ce fait les recommandations de ses propres experts. C'est aussi « parfaitement légal » se défend Gertrud Ingestad, qui est responsable de la Direction générale pour l'Informatique (DG Digit), dans une interview à Investigate Europe. Il n'y aurait « pas d'autres possibilités » de garantir la continuité du travail de l'Union européenne. Et, dans ce cas, la législation permet explicitement le recours à une « procédure de négociation » non publique. Mais ce n'est pas exact : cette exception est explicitement valable « seulement quand il n'existe pas d'alternative raisonnable ou de solution de remplacement », selon l'article 32 du livret de recommandations de l'UE. Et c'est justement ce que la Directrice générale G. Ingestad et ses collègues ne peuvent pas prouver. Il existe des alternatives viables.

Le général italien Camillo Sileo, par exemple, a beaucoup à dire sur ce sujet. Ce militaire, qui travaille au ministère de la Défense, à Rome, reçoit dans une petite bibliothèque. Là, un sourire aux lèvres, d'une voix douce, il parle de son projet comme d'une affaire mineure. Pourtant, il est à la tête d'une opération peu commune, voire révolutionnaire, l'opération « Libre Défense ». Son objectif est de migrer les quelques 100 000 ordinateurs de l'armée italienne vers des logiciels *open source*. « Nous avons constaté que les deux types de logiciels sont capables de satisfaire de la même façon nos besoins », explique le général. « Voyez par vous-même », dit-il en montrant à l'écran la première page d'une étude récente du ministère. « Ici, vous avez un fichier Microsoft Word », dit-il avant de cliquer, « Et, ici, la version *open source* LibreOffice. Le logo, le titre, la structure, tout est

là. Aucune différence, » dit-il, radieux. «La migration permettra une économie de 28 millions d'euros d'ici 2020 », a prévu le général. Par temps de crise en Italie, l'armée, elle aussi, doit faire des économies.

Le fait est que si la migration s'est déroulée sans accroc jusqu'ici, c'est grâce à une solide planification, selon le général. Le logiciel libre de remplacement peut satisfaire tous les besoins, mais il se manipule différemment et les utilisateurs doivent donc être formés. Pour cela, des volontaires de l'association « LibreItalia » ont formé des personnels de tous les services de l'armée devenus à leur tour formateurs et conseillers pour former leurs collègues. Ainsi, il y aura bientôt assez d'experts dans tous les services de l'armée. « Bien communiquer est un préalable à la réussite du projet », précise le général Sileo. « Si les gens comprennent l'objectif du changement, ils sont capables de surmonter toutes leurs résistances mentales ». Il n'a pas encore été décidé si l'armée migrera aussi son système d'exploitation un jour, pour être totalement indépendante de Microsoft, mais la question sera examinée de très près », accorde le général Sileo.

La gendarmerie nationale française, l'une des deux forces de police nationales, a déjà mené à bien une opération de migration démarrée dès 2005. Aujourd'hui, 72 000 ordinateurs de la gendarmerie nationale sont équipés d'une version particularisée du système d'exploitation Linux, avec LibreOffice comme application principale. La gendarmerie affirme que l'économie réalisée depuis le début du projet s'élevait en 2014 à quelques 20 millions d'euros. Précisons que jusqu'à cette année-là, la migration s'était déroulée pratiquement dans le secret. « La migration vers Linux pourrait être vue par Microsoft comme une menace de son monopole », peut-on lire dans une note interne obtenue par Investigate Europe. Cela aurait pu « déclencher des actions visant à discréditer cette politique de la gendarmerie ». C'est pour cette raison que la migration s'est effectuée « sans publicité » jusqu'au moment où le processus est devenu irréversible.

Les institutions mettent la pression sur ceux qui se désengagent

Ces précautions étaient fondées. Encore aujourd'hui, 12 ans après le lancement du projet, la direction de la gendarmerie est sous « pression permanente » pour faire marche arrière, rapporte un membre de l'équipe du département

Informatique et Télécom du ministère de l'Intérieur à Paris, qui ne souhaite pas être nommé de peur de représailles. « Chaque jour de fonctionnement du système est une gifle pour notre administration qui maintient que seul Microsoft fonctionne correctement » dit-il.

Le bras de fer entre le ministère de tutelle et les partisans de Linux au sein de la gendarmerie est confirmé par une lettre du ministre, d'avril 2016, qu'Investigate Europe a eue entre les mains. Dans cette lettre, le ministre demande aux fonctionnaires responsables de la gendarmerie un retour définitif et intégral à Windows - prescription dont la direction de la police n'a pas tenu compte jusqu'à présent. Interrogé sur la question, un porte-parole faisait savoir « avec regret » qu'il était dans « l'incapacité de fournir une explication ». En parallèle, cependant, il écrivait de façon clairement subversive que la migration vers le logiciel libre « se passait en douceur et pour longtemps ». « Nous avons choisi Linux parce que le rapport coût/bénéfice est meilleur et, au final, nous gagnons en indépendance».

Ce conflit est caractéristique de ce que vivent partout les pionniers d'une émancipation vis-à-vis du monopole. Partout en Europe, il y a eu et il y a des centaines d'administrations et de municipalités qui ont migré ou tentent de migrer vers des logiciels *open source* : que ce soit l'administration des retraites de l'État en Suède, les écoles de Jaworzno en Pologne, les services municipaux de la ville de Rome, l'arrondissement de Camden à Londres, la grande ville de Nantes en France, le gouvernement de la communauté autonome d'Estrémadure en Espagne ou encore la ville de Vieira do Minho au Portugal. Ces projets sont à ce jour autant d'îlots perdus dans l'océan Microsoft. Pour cette raison, nombreux sont ceux qui subissent régulièrement des pressions pour rentrer dans le rang, parce que les produits et les lobbyistes de Microsoft sont omniprésents et peuvent créer de nouveaux ennuis.

Des lobbyistes à l'œuvre au sein des ministères

Dans le différend concernant l'administration municipale de Munich, ce qui se passe en coulisses est aussi un élément à prendre en considération. Dans cette ville, le maire centre-gauche SPD a besoin des voix du centre-droit CSU. Or, ce dernier est étroitement lié à l'entreprise étasunienne. Dorothee Belz, par exemple, vice-présidente chez Microsoft Europe jusqu'en 2015, fait partie du comité exécutif du conseil économique du parti conservateur.

Des épisodes identiques « d'allers-retours » se constatent partout en Europe. En Italie, un ancien directeur chez Microsoft pilote aujourd'hui la « transformation numérique » des affaires de la ville de Milan. Au Portugal, c'est un cadre de Microsoft qui a organisé la campagne pour l'élection du président conservateur. Plus de six cadres et directeurs ont des liens étroits avec des ministres et des politiciens. Dans le même temps, des techniciens de Microsoft travaillent directement dans les services informatiques des administrations. Au moins cinq d'entre eux possèdent une adresse électronique qui les identifie comme s'ils faisaient partie du personnel administratif, ce qui leur permet de « faire leur travail de lobbying pour Microsoft à l'intérieur de l'administration », affirme un fonctionnaire à Investigate Europe. En Allemagne aussi, l'accès aux ordinateurs du gouvernement est largement ouvert. Il existe plusieurs milliers d'experts dans les centres informatiques du gouvernement, y compris des personnels de Microsoft et ses partenaires, indique l'ex-responsable informatique du gouvernement fédéral, Martin Schallbruch.

Microsoft peut également instrumentaliser sans restriction les écoles et les universités à des fins marketing. Les écoliers et les enseignants reçoivent en général les produits Microsoft gratuitement, de sorte que les enfants grandissent sans rien connaître d'autre. La stratégie veut qu'après leurs études ils payeront des frais de licence pendant le reste de leur existence. « Une telle méthode est un classique du modèle « crack », utilisé dans le trafic de drogue », explique Rufus Pollock du Centre pour la propriété Intellectuelle et les lois de l'information (CIPIL) à l'Université de Cambridge. Les produits sont gratuits jusqu'à ce que les utilisateurs soient rendus accros.

Cela démontre que les gouvernements européens approuvent tacitement leur propre dépendance envers Microsoft. Ainsi que le formule Anna Strezyńska, ministre polonaise du numérique : « Oui, nous sommes dépendants, mais je pense que c'est raisonnable ».

Cela signifie aussi que ces décideurs exposent leurs pays et leurs citoyens à d'innombrables risques de sécurité, tant techniques que politiques.

Ce n'est pas un hasard si les attaques informatiques majeures qui, ces dernières années, ont pris pour cible des institutions de l'État comme le Bundestag allemand ou encore la Commission et le Parlement européens, ont systématiquement exploité des failles de sécurité des logiciels Microsoft. La suite bureautique de Microsoft, notamment, et les fichiers qu'elle permet de créer, sont

une des portes d'entrée privilégiée par les hackers, selon le rapport 2011 du Bureau fédéral allemand pour la Sécurité des technologies de l'information (BSI). D'après ce rapport, la moitié des attaques ciblées avait pour origine des documents infectés de type Microsoft, tels les fichiers « .docx », dans lesquels les hackers avaient dissimulé leur logiciel malveillant. « La particulière complexité de ces fichiers facilite la tâche des hackers », affirment les experts du BSI. Ces fichiers contiennent bien plus de code que nécessaire, ne serait-ce que pour empêcher d'autres logiciels de les lire facilement. « Ce constat est toujours d'actualité, confirme Joachim Wagner, porte-parole du BSI. Le format des fichiers Microsoft est bien plus complexe que celui des logiciels *open source*, ce qui augmente d'autant la « surface d'attaque » de la cible pour les hackers ».

Italo Vignoli, un des experts qui travaillent sur le logiciel libre LibreOffice, l'a testé pour Investigate Europe avec un simple texte de 5 500 caractères. Sous la version courante de Microsoft Word, le code du fichier couvre 390 pages. Par comparaison, le format libre OpenDocumentText ne fait que onze pages.

Les programmes de Microsoft sont confus et vulnérables

La particulière vulnérabilité des logiciels de bureautique de Microsoft se voit au nombre de failles de sécurité. « Aux États-Unis, le National Institute for Standards and Technology (NIST, Institut national des normes et de la technologie) a repéré 188 nouvelles failles dans la suite Microsoft Office au cours des trois années précédant le mois d'avril 2017. Les trois quarts de ces failles font partie de la catégorie des failles les plus graves. Sur la même période, on n'a découvert que onze failles dans LibreOffice. D'après M. Vignoli, cela n'a rien à voir avec le fait que LibreOffice est moins répandu. Simplement, malgré tous leurs efforts, même les meilleurs experts n'ont pu dénicher d'autres failles dans LibreOffice.

Cela n'a rien de surprenant. N'importe quel utilisateur chevronné peut contrôler le code source de LibreOffice. Pour l'un des meilleurs experts européens, Michael Waidner, directeur de l'institut Fraunhofer pour la sécurité des technologies de l'information, c'est la clef de voûte : « Si l'Union européenne ou un État entend vraiment préserver sa souveraineté, il doit être en mesure de vérifier que ses matériels informatiques et ses logiciels font bien ce qu'ils sont censés faire et rien d'autre, explique-t-il. Cela ne revient pas à dire que l'Europe doit devenir

autonome. « Mais nous devons faire en sorte que nos experts aient accès à toute l'information requise pour tester les logiciels là où la sécurité est en jeu. Il est essentiel d'avoir accès au code source », exige l'expert. Sans cela, affirme-t-il, il ne peut y avoir de « souveraineté numérique ».

Or, c'est précisément ce que Microsoft refuse de fournir. L'entreprise a créé un « centre de la transparence », à Bruxelles, où les représentants gouvernementaux sont invités à inspecter le code source. Mais le BSI allemand juge la proposition insuffisante. « Microsoft doit satisfaire à un éventail complet de prérequis techniques pour créer un climat de confiance », a expliqué le BSI au magazine spécialisé *C't*. Or Microsoft n'autorise même pas les experts à conserver leurs notes écrites et exige la signature d'un accord de non-divulgaration, a confirmé un expert de la BSI à Investigate Europe.

Même si une inspection du code était possible, les conclusions en seraient probablement obsolètes dès la mise à jour suivante. En outre, le risque que représentent les produits Microsoft n'est pas seulement technique, il est aussi politique.

Déclasser l'Europe au rang de colonie numérique

L'entreprise est soumise aux lois des États-Unis. Cela signifie qu'à tout moment l'administration de ce pays peut la forcer à collaborer afin d'accéder aux données des citoyens et des pouvoirs publics d'autres pays. Pour satisfaire cet objectif, il existe ce qu'on appelle « la lettre du renseignement » dans la loi américaine, autorisant des tribunaux secrets à délivrer de telles instructions, avec obligation de se taire sous peine de poursuites légales. Les révélations de l'ancien agent Edward Snowden ont montré que les services de renseignement américain font un usage démesuré de leurs pouvoirs. Les documents qu'il a publiés révèlent que Microsoft coopère étroitement avec les services secrets de la NSA.

Un document de la NSA du 8 mars 2013 explique avec force détails que Microsoft a ouvert aux autorités américaines l'accès à ses services dans le nuage (*cloud*), autrement dit aux dispositifs de stockage de données auxquels recourent un nombre grandissant d'organisations privées, mais aussi publiques, qui confient ainsi à un prestataire externe leurs données informatiques par souci d'économiser sur les coûts de leur informatique interne. Les documents de Snowden ont aussi révélé que la NSA utilise une cyber-arme, Regin, en collaboration avec ses partenaires britanniques pour espionner la Commission et le Parlement

européens via une faille de sécurité du programme Windows.

Wikileaks a publié des documents secrets qui prouvent que ce n'était pas un cas isolé. Ils montrent que la CIA a même développé un véritable arsenal de logiciels malveillants (*malwares*) ciblant exclusivement les logiciels de Windows. La NSA n'est pas en reste, un de ses outils exploitant, ainsi que l'a révélé récemment le groupe de hackers Shadow Brokers, quatre failles de sécurité du système d'exploitation Windows inconnues jusqu'alors (vulnérabilités Jour Zéro).

De fait, l'utilisation de produits Microsoft par les institutions de l'État « n'est plus compatible avec un État de droit », affirme le juriste et député Vert du Parlement européen Jan Philipp Albrecht. Beaucoup le considèrent comme le père de la loi européenne sur la protection des données. Albrecht précise qu'il y a pléthore de données individuelles stockées dans des ordinateurs appartenant à l'État, tels les montants acquittés pour les impôts, l'état de santé, les fichiers de police et les données sociales. « Cependant, les institutions ne peuvent garantir la confidentialité de ces données tant qu'elles travaillent avec des logiciels dont elles n'ont pas le contrôle », prévient Albrecht. Il va falloir changer cela, sous peine de « transformer l'Europe en une colonie numérique ».

M. Albrecht n'est pas le seul à exprimer ce genre d'opinion. En 2014, après les révélations d'E. Snowden, une grande majorité du Parlement européen appelait les États membres de l'UE à s'unir pour « développer des compétences-clés autonomes dans le domaine des technologies de l'information », qui devraient « être basées sur des standards ouverts et des logiciels *open source* », de manière à pouvoir « être testées ».

Un an plus tard, le Parlement nouvellement élu appelait à nouveau à l'adoption d'« une stratégie européenne pour l'indépendance du secteur des technologies de l'information ». Il indiquait aussi comment cela pouvait être acté : il est important d'établir « un code source publiquement accessible comme critère de sélection obligatoire dans toutes les procédures d'attribution des technologies de l'information du secteur public », ainsi que le préconisait l'expert en sécurité Michael Waidner.

Si l'open source devenait la norme obligatoire pour le développement logiciel, « les acteurs européens deviendraient immédiatement

compétitifs ».

Si cela se faisait, M. Albrecht pense qu'il y aurait un effet sur les technologies de l'information « semblable à celui du projet Airbus ». De la même manière que l'Europe s'est autrefois affranchie de Boeing, elle pourrait s'affranchir aujourd'hui de sa dépendance à Microsoft, et cela pour un coût bien moindre, pense-t-il ; si l'*open source* devenait la norme obligatoire pour le développement logiciel, « les acteurs européens deviendraient immédiatement compétitifs, affirme Albrecht. Après tout, ajoute-t-il, les solutions alternatives sont développées depuis longtemps ».

Pourtant, aujourd'hui encore, les gouvernements européens s'avèrent incapables de chiffrer le montant du tribut versé au « seigneur » des licences de Redmond, aux États-Unis. De la Norvège au Portugal, la réponse des administrations compétentes aux demandes d'information d'Investigate Europe a invariablement été qu'il n'existe pas de statistiques en la matière. En Allemagne, le bureau des achats du ministère fédéral de l'Intérieur a précisé ne pouvoir fournir qu'une « estimation » des dépenses en licences Microsoft des autorités fédérales. Dix semaines après la demande, le bureau n'était toujours pas en mesure de fournir ces données.

Pierre Audoin Consultants, société spécialisée dans l'analyse des marchés IT, estime que, globalement, en Europe, Microsoft a tiré près de 2 milliards d'euros de revenus de ses opérations avec le secteur public pour l'exercice fiscal 2015-16. Cela voudrait dire que ce sont au moins 20 milliards d'euros de recettes fiscales européennes qui partent vers l'entreprise étasunienne tous les dix ans, assurément assez pour que l'Europe développe sa propre industrie du logiciel.

Jusqu'à présent, les dirigeants européens ne veulent rien entendre d'un « projet Airbus » pour le secteur des technologies de l'information. Andrus Ansip, commissaire européen au marché unique du numérique ne veut même pas en parler. Son directeur de cabinet, Roberto Viola, botte en touche en déclarant que ce n'est pas là leur principal souci

Les entreprises américaines de l'Internet, de leur côté, n'ont pas besoin d'un dessin. Que se soit Facebook, Google ou Amazon, leurs infrastructures informatiques fonctionnent exclusivement avec des logiciels libres à en croire leurs porte-paroles. C'est le seul moyen qu'elles ont de se protéger. C'est bien

aussi l'intention des dirigeants chinois, qui ont commencé à se libérer du monopole de Microsoft après le scandale de la NSA.

Sous l'égide de l'Académie nationale d'ingénierie chinoise, un système d'exploitation ouvert, Neokylin, a été développé, accompagné de sa suite bureautique. L'opération de « déwindowsisation », comme l'appelle le professeur Ni Guangang, chef du projet, concernera au premier chef les secteurs les plus sensibles en termes de sécurité. C'est pourquoi l'usage de programmes libres/ouverts est en train de devenir obligatoire pour les militaires, l'administration d'État et le secteur financier. L'opération devrait se terminer en 2020.

La Chine prend le chemin de l'indépendance. Que fait l'Europe pendant ce temps-là ?



photo par Leonid Mamachenkov (CC BY 2.0)

Cet article est une traduction de la version anglaise d'un billet d'Investigate Europe publiée le 13 mai 2017. Pour savoir dans quelles publications de presse, pays et langues le billet est disponible, veuillez consulter la page suivante.