Citation : de Mittelwihr C., 2016. Cybersécurité paroissiale. *Nouveaux eCrits scientifiques*, NeCs_01-2016, p. 1-6.

http://paleopolis.rediris.es/NeCs/NeCs_01-2016/

Cybersécurité paroissiale

Christian de Mittelwihr

Webmestre et webdesigner (CdM Créations)
cdemittelwihr@free.fr

Résumé

La grande majorité des paroisses protestantes française n'ont pas encore de visibilité sur le Web et ce retard est préjudiciable, notamment pour la jeune génération, dans le partage de la foi et la communication. Aujourd'hui, l'accès paroissial à Internet doit être managé avec professionnalisme à cause des mesures de cybersécurité à imposer aux échanges et à la protection des données au sein d'une paroisse. Les règles d'une protection de base sont fournies en ce qui concerne la protection des ordinateurs, celle des échanges de courriel. Une attention particulière est accordée aux adresses avec ou sans IP et les risques encourus dans ce dernier cas. Un paragraphe porte sur les sites web. En conclusion, on en arrive à penser que ce sont les structures ecclésiales et leur non-évolution qui marquent l'absence de paroisses de l'Eglise Protestante Unie sur le web.

La grande majorité des paroisses protestantes françaises[1] ne dispose pas encore de site web, ceci est regrettable pour celles dans les zones touristiques. Certes souvent, il y a une page mélangeant paroisse et site national de l'Eglise Protestante Unie. Ni téléphone, ni adresse email, mais on est face à une machine qui dit transmettre votre message. Combien restés sans réponse ? Aux pages blanches, on trouve un numéro de téléphone. Ce retard est préjudiciable, notamment pour la jeune génération, dans le partage de la foi, la communication (évangélisation disait-on dans le temps) envers les autres, du besoin d'ouvrir au-delà du cercle très fermé de la paroisse. L'effort aurait dû être fait en 2000. Les pasteurs présents sur le Web reconnaissent tous combien Internet est un formidable relais de la parole protestante et du partage spirituel dans le cadre paroissial. Pourtant, plus de 15 ans plus tard Internet reste une timide vitrine presque vide. « *Un site doit être à l'image d'une communauté et le reflet d'un vécu dans la vie réelle.* » comme le souligne Fanny Bijaoui (2013) dans *Réforme*.

Aujourd'hui, l'accès paroissial à Internet doit être managé avec professionnalisme, car il n'y a de plus de place à l'amateurisme. En plus, du rapide développement des techniques informatiques, basées sur des logiciels professionnels, incluant la protection des échanges et des accès, et un ensemble de lois, souvent contraignantes, comme celles sur la propriété intellectuelle, se sont déployées de nouvelles pratiques destructrices dans le cyberespace (cybercriminalité, espionnage à visée politique, économique, religieuses, attaques contre les infrastructures à des fins de sabotage).

Emanant de groupes ou d'individus, les cyberattaques se jouent des frontières et des distances ; elles sont anonymes, et peuvent être réalisées relativement facilement, à bas coût et à très faible risque pour l'attaquant. Elles visent à mettre en péril le bon fonctionnement des systèmes d'information et de communication (SIC) utilisés ou mise en œuvre par les citoyens, les associations, les entreprises et les administrations. Une paroisse est une association cultuelle avec des employés, au moins un pasteur, et à ce titre devrait s'inscrire dans un contexte professionnel ; celui-ci devrait relever des obligations et responsabilités du conseil presbytéral.

La cybersécurité recouvre l'ensemble des mesures de sécurité susceptibles d'être prises pour se défendre contre ces attaques. L'augmentation spectaculaire du niveau de sophistication et d'intensité des cyberattaques a conduit ces dernières années la plupart des pays développés à renforcer leur résilience et à

[1] Celles de l'Eglise Protestante Unie, formée de l'Eglise Réformée de France (calviniste) et de l'Eglise Luthérienne de France (Paris et Montbéliard). Voir aussi note 6.

adopter des stratégies nationales de cybersécurité, ce qui est le cas des pays européens et de l'UE.

Il s'agit d'être vigilant et de se sécuriser sans paranoïa, et aussi ses correspondants. On ignore souvent que mettre autrui en danger est puni par la loi que nul n'est sensé ignorer. Il n'en apparaît pas moins que nombre de paroisses semblent ignorer le b.a.-ba, car accéder à Internet demande un minimum de précautions et de connaissance ce que nombre de paroisse méconnaisse totalement. Or, c'est de la responsabilité du Conseil presbytéral de se doter des compétences pour garantir un accès sécurisé à Internet et maintenir un site web. Quelques conseils de base pourraient ne pas être inutiles : c'est le but recherché ici.

La vraie menace, c'est le vol de données, car les celles-ci, notamment personnelles, qui ont désormais une valeur marchande, sont au cœur du problème. Et elles peuvent coûter d'autant plus cher à la paroisse que la règlementation européenne est très stricte sur leur vol. Aujourd'hui non seulement il faut bloquer les intrusions, mais aussi de plus en plus se concentrer sur leur détection.

Cybersécurité des ordinateurs [2]

La plateforme utilisée (Windows, Lunix, MacOS X) sur un ordinateur induit les consignes de sécurité à employer :

- Un bon code d'accès personnel (8-12 caractères alphanumériques) à son ordinateur, idem pour la wifi – un ordinateur n'a pas besoin d'être connecté 24/24 à la wifi et on oublie souvent la liaison Ethernet. Sur toute plateforme.
- Un paramétrage efficace du (ou des) firewall(s) et du modem Internet /wifi.
- Un paramétrage efficace de ses navigateurs : les meilleurs représentant environ 80% des utilisateurs sont Firefox, Safari, Chrome. A éviter Internet Explorer qui ne fonctionne que sur PC. Pour toute plateforme.
- Un Antivirus efficace :
  - Avec Windows (sur PC ou Mac [3]) : un antivirus est obligatoire. D'après des études récentes, un tel PC non protégé et relié à Internet a une durée de survie d'environ 5-6 minutes avant d'être infesté !
  - Avec Unix (Linux sur PC ; MacOs X sur Mac), il y a de faibles risques. Notamment le système MacOs est auto-immune, néanmoins il est facile d'installer un anti-virus, généralement gratuit là où le même est payant sur PC.

Si les seuls ordinateurs sont évoqués ici, il faut évidemment prendre en compte de la même façon les tablettes et les smartphones. L'usage professionnel de ces derniers nécessite une protection en cas de vol.

Cybersécurité en courriel

Le choix des adresses électroniques pour garantir la cybersécurité des échanges reste ignoré de la plupart des paroissiens et peut entraîner des conséquences dramatiques dans les relations au sein d'une paroisse, comme entre correspondants privés. Une adresse peut être une faille grave dans un réseau de correspondants et mettre en danger toute une paroisse.

Il existe deux types d'adresse, celle(s) fournie(s) par le FAI (Fournisseur d'Accès à Internet) et celle demandée à un fournisseur de *freemail* (gratuit, anonyme et sans accès direct à Internet, donc qui nécessite un FAI) :

1 – Adresse(s) du FAI :

Pour accéder à internet, il faut un FAI qui est généralement aussi celui pour le téléphone fixe ou mobile (Orange, Free, SFR, Bouygues, etc. et leurs adresses annexes [4]). Ce FAI vous propose d'avoir des adresses multiples, selon vos besoins et activités. Personnellement, j'en ai 8 et mon épouse 4 : avantage, elles sont gérées ensemble par le même *mailer* (logiciel de email), dans notre cas sur des ordinateurs distincts. A chacun d'avoir son paramétrage du mailer adapté à son usage.

Il y a souvent confusion entre une adresse personnelle et une adresse professionnelle, cela vaut pour tous les responsables au sein d'une paroisse, à commencer par le pasteur, car il faut inclure le secret de la confession.

Ces adresses sont sécurisées par le FAI mais chacune nécessite un excellent code d'accès (8-12 caractères alphanumériques), évidemment distinct pour chacune de vos adresses. Elle sont

[2] Les ordinateurs de la paroisse et ceux privés correspondants avec la paroisse et leurs membres.

[3] Faut-il rappeler que les Mac peuvent aussi travailler sous Windows… depuis des décennies !

[4] Par exemple, Free, outre @free, gère aussi infonie, aliceadsl, libertysurf, worldonline, teamtiscali, etc. Orange est aussi Wanadoo.

généralement enregistrés et sécurisés sans avoir à l'indiquer à chaque usage, selon le paramétrage que vous avez imposé à votre ordinateur.

Les messages doivent être stockés de manière sécurisée soit sur le serveur du FAI, soit dans votre ordinateur – à noter qu'un vol n'est jamais exclu et si les données sont accessibles elles peuvent mettre autrui en danger. Les parades existent. Vous fermez bien la porte à clé en partant !

Cette adresse possède un IP (Internet Protocol) qui est un numéro d'identification attribué de façon permanente ou provisoire par le FAI à chaque appareil connecté à un réseau informatique utilisant l'Internet Protocol. L'adresse IP est à la base du système d'acheminement (le routage) des messages sur Internet : elle identifie l'envoyeur d'un message (en tout cas son ordinateur). Ces données sont facilement contrôler en ouvrant présentation > message > *en-têtes longs* (selon votre logiciel, ici *Mail* sur Mac). Il faut aussi remarquer que des liens douteux dans un message se vérifier en cliquant sur *contenu brut*, selon la même chaîne que ci-dessus, ce qui évite d'ouvrir le lien ce qui peut s'avérer hasardeux.

Comme exemple, l'en-tête long d'un message d'un pasteur à Marseille :

De : xx <xxx@free.fr>
Objet : **Rép : mise à jour**
Date : 10 juin 2016 14:26:05 HAEC
À : yyy <yyy@free.fr>

Return-Path: <xxx@free.fr>
Delivered-To: yyy@free.fr
Received: from smtp3-g21.free.fr (mx28-g26.priv.proxad.net [172.20.243.98]) by toaster1-g26 (Postfix) with ESMTP id 6101660579 for <yyy@free.fr>; Fri, 10 Jun 2016 14:26:07 +0200 (CEST)
Received: from smtp3-g21.free.fr ([**212.27.42.3**]) by mx1-g20.free.fr (MXproxy) with ESMTPS for yyy@free.fr (version=TLSv1/SSLv3 cipher=AES256-GCM-SHA384 bits=256); Fri, 10 Jun 2016 14:26:10 +0200 (CEST)
Received: from [192.168.0.8] (unknown [**82.234.219.24**]) by smtp3-g21.free.fr (Postfix) with ESMTPS id 23D4F13F8B2 for <yyy@free.fr>; Fri, 10 Jun 2016 12:28:46 +0200 (CEST)
X-Proxad-Sc: state=HAM score=0
X-Proxad-Cause: (null)
Content-Type: text/plain; charset=utf-8
Mime-Version: 1.0 (Mac OS X Mail 9.3 \(3124\))
In-Reply-To: <7A26E487-1856-4ADE-8179-06DD41B2A6E2@free.fr>
Content-Transfer-Encoding: quoted-printable
Message-Id: <0D3C5E62-0BC8-425D-B42F-8C8B704BC7FC@free.fr>
References: <CB8ECA04-F73E-4D38-A4E0-122C79693320@free.fr> <EA7B70FA-BA15-4BD3-88FC-A8165779BD08@free.fr> <7A26E487-1856-4ADE-8179-06DD41B2A6E2@free.fr>
X-Mailer: Apple Mail (2.3124)

Nota : les données en rouge se contrôle sur le web avec un moteur de recherche.
Adresse IP: **212.27.42.3** = PTR enregistrement de ressource: smtp3-g21.free.fr - Organisation: Free SAS - FAI: Free - Pays: France
82.234.219.24 est une Free box située à fer13-2 (Marseille). L'ordinateur est un mac et le mailer est Apple Mail

Je peux correspondre en toute confiance avec xxx dont le message correspond bien au nom de l'adresse email de l'envoyeur et à son identité.

Toutes les paroisses disposent d'un FAI : il est donc de la responsabilité du conseil presbytéral d'imposer des adresses du FAI pour un usage « professionnel » dans et hors paroisse. Il convient aussi d'éviter des adresses nominatives dans une association afin de garantir une continuité même en cas de changements de responsables ou de pasteur. Cela ne signifie pas qu'il ne puisse y avoir des adresses personnelles du FAI. C'est de la gestion au sein de la paroisse en ayant en permanence un regard sur la cybersécurité et ses évolutions.

Il est aisé de changer un mot de passe d'une adresse en cas de changement.

Ci-dessous, un exemple de l'en-tête long d'un freemail.

De : xxx <xxx@gmail.com>
Objet : **Demande**
Date : 8 juin 2016 10:35:11 HAEC
À : yyy <yyy@free.fr>

Return-Path: <xxx@gmail.com>
Delivered-To: free.fr-yyy@free.fr
Received: (qmail 7639 invoked from network); 8 Jun 2016 08:35:13 -0000
Received: from mx22-g26.free.fr (HELO mail-oi0-f68.google.com) (212.27.42.84) by mrelay4-g25.free.fr with SMTP; 8 Jun 2016 08:35:13 -0000
Received: from mail-oi0-f68.google.com ([**209.85.218.68**]) by mx1-g20.free.fr (MXproxy) with ESMTPS for yyy@free.fr (version=TLSv1/SSLv3 cipher=AES128-GCM-SHA256 bits=128); Wed, 8 Jun 2016 10:35:13 +0200 (CEST)
Received: by mail-oi0-f68.google.com with SMTP id x204so232036oia.0 for <yyy@free.fr>; Wed, 08 Jun 2016 01:35:13 -0700 (PDT)
Received: by 10.157.13.167 with HTTP; Wed, 8 Jun 2016 01:35:11 -0700 (PDT)
X-Proxad-Sc: state=HAM score=0
Dkim-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=20120113; h=mime-version:from:date:message-id:subject:to; bh=0TbKYd3R4Rjw10SFs/qp9dgp1OMGVyP+MVrGjZJVzil=; b=u51tnQElVZVO7EVtJzT0lE0aR7+R9R2Czfju+riasfcZHXj7WbMaYbi084KYgnbpNe hjzII576lUN5h317/5iSZoEKK8sfZxRQsPiPzldObnxYdhj7OOElz7nbb+K3n7a3O8kW ++I1iDNy90BTRTBQpO/a7tm0a1ugPE01mqP42rm2o/1iSHsprg1IIAceZ8rxmzfkrHkF pDaF9wuUhz4JQf2tFECUbV2uGUz0S1M/xKjcUz+lJEFEihYFafvd+a3fZ5q4LMAIw/my k//v4imwffun1SdlCrQl2tJTquh1TOa3gwLfflgdHAZ1KI6RUBZ22UO7vyzzD4m1aPv1 NbSg==
X-Google-Dkim-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=1e100.net; s=20130820; h=x-gm-message-state:mime-version:from:date:message-id:subject:to; bh=0TbKYd3R4Rjw10SFs/qp9dgp1OMGVyP+MVrGjZJVzil=; b=MljpybAaNZdHSl4w3/A9gU7XWb/OSGgmQY4Rx4Szk2vLnP3pfTC48ULS3/p5JaerFs OCuxKeB3V6TllWYG3gopc+l0OCid3UqA++VtvoPDrcE8Y5WvbQ2Bl+M5v0V1LXjEPjKv WuoQl6Y2/lMrMMQFLQ/+79hZANBXtu2wvB8M6sIhNN4u7xpc+K6r69hiNG0mPJxlky3J CoKkoFhAb1flh3ME1oMlaCeWsVHm9en37/VjDOAnz/NGUSZE8odRlmZwaPpJiv42FDxw HWKdSoyZ+/GURjcRipdAvKKAL98t/J61+/zt095pGrmhj5VGpNEON2cE7iM5mH5ohSXX GbPA==
X-Gm-Message-State: ALyK8tI6CUZOlanKHXIJkNcUcTnemgRBWSnO7tQJTiBTLH1lg6jSfRCe4IlPSwYGjpn/+2nbbz+gAngHCX3MKw==
X-Received: by 10.202.86.148 with SMTP id k142mr1736469oib.54.1465374911957; Wed, 08 Jun 2016 01:35:11 -0700 (PDT)
Mime-Version: 1.0
Message-Id: <CAMi-Fp7RxTP+MkZJH=7CP-YjwESt4M_QVfC-_aVoazQwtDoqLw@mail.gmail.com>
Content-Type: multipart/mixed; boundary=001a113d78f61759f70534c02f50

The organization for IP address 209.85.218.68 *is Google in United States.*

Ceci est la seule identité connue – donc impossible de savoir qui se cache derrière xxx@gmail.com - xxx pouvant être une personne supposée connue ou un hacker qui en profitera pour vous attacher un fichier pouvant rançonner, détruire votre ordinateur ou y installer un logiciel espion.

2 – Adresse(s) *freemail*:

Les adresses *freemail* sont des adresses anonymes sans IP, dissimulant l'identité de l'envoyeur qui peut être un hacker ayant piraté l'adresse de l'exemple xxx@gmail.com donné ci-dessous. Les freemail habituels sont Hotmail, Yahoo et dérivés, gmail et dérivés, laposte.net, live.fr, AOL… toutes ces adresses sont susceptibles de se faire hacker avec l'ensemble des données contenu sur le serveur qu'il est impossible d'effacer, car tout est enregistré à l'insu du plein gré de celui qui possède l'adresse – généralement selon des algorithmes – ce qui génèrent facilement ensuite des spams [5]. Les messages électroniques (sauf cryptés) peuvent être lu à chaque nœud et bien sûr par le propriétaire du freemail ici Google ainsi que par les services secrets des pays traversés. A noter

[5] xxx@gmail.com en fait profiter tous ses correspondants et lui-même par son adresse free connue de Google. Supprimé tout échange avec des freemail et votre nombre de spam va chuter.

en quelques fractions de seconde.

Pour des protestants plus que frileux et franchement attardés vis-à-vis d'internet, le comble est l'usage de messages freemail permettant à la moitié de la Terre de les lire. Amusant, car quand j'ai demandé de connaître le nom des paroissiens vivant à proximité de mon domicile pour une réunion de quartier – le secret du fichier paroissial m'a été opposé ! Peut-être Google le sait ?

Enfin, posez-vous la question *est-ce que vous répondriez à une lettre anonyme* et la réponse est non, mais sur Internet cela devient oui !

Quand un hacker met la main sur une adresse, il en prend le contrôle total : accède à la boîte-aux-lettres et en refuse l'accès, lit l'ensemble du contenu (messages, adresses,…). Dans un tel cas, il est indispensable de prévenir immédiatement tous ses correspondants, à condition d'avoir une sauvegarde de toutes leurs adresses ! Ceci explique que les adresses *freemail* sont de plus en plus refusées par cybersécurité. Si une entreprise possède une telle adresse, passez au large, l'arnaque n'est pas loin. Alors quand c'est l'adresse d'un pasteur !!

La règle d'or est de ne JAMAIS ouvrir un fichier joint à un tel message et de mettre à la poubelle message et pièce jointe ! Reste ensuite à chacun de prendre ses responsabilités.

Pour revenir aux échanges paroissiaux, nul pasteur, ni responsable presbytéral ne peut et ne doit accepter de mettre en danger – un danger certain – les paroissiens. Sauf à être irresponsable et punissable par la loi.

Cybersécurité des sites Web

Les sites web paroissiaux sont soumis à des règles strictes de sécurité, à commencer par un login hyper protecteur. Leur suivi devrait être assumé par des webmestres confirmés. Cela se trouvent souvent parmi la génération Y, mais il faut savoir convaincre, ce qui n'est pas facile au sein de paroisses qui n'ont su prendre le virage Internet en 2000 !

Un site web n'est pas une simple vitrine, mais un véritable moyen de communication à condition de respecter les règles et spécificités du Web. C'est un lieu de rencontre et de dialogue pour peu qu'il y ait une bonne adresse email et une réponse immédiate - sous 24 h – ce qui est rare chez les protestants, et encore heureux quand il y a une réponse. Moi même, mes enfants et petits-enfants ont eu des expériences douloureuses, loin de la convivialité chrétienne. Cela vaut aussi pour bien des structures adjacentes comme le mouvement des Eclaireurs et Eclaireuses Unionistes de France – largement anonyme ! Incompréhensible pour une jeunesse ayant pourtant toujours un smartphone à la main.

On ne peut mettre des adresses *freemail* sur un site Web pour correspondre dans la paroisse et pourtant nombre de responsables en ont, hérités de leur jeune époque ? Mais le monde a bien changé depuis. Peu imagine les risques et la virulence de cyber-attaques. Quand une survient, il est trop tard. J'en ai malheureusement quelques exemples à conter.

Conclusion

La présence sur les réseaux sociaux d'une paroisse ou groupe de paroisses devrait faire l'objet d'un débat circonstancié en assemblée générale, peut-être même à chacune. En effet, certains documents mis en ligne ne vont pas sans poser des questions, y compris des autorisations de publier et de la propriété des photographies. Pour une association, avoir une présence sur un réseau est surtout un appel vers son propre site web, avec des liens vers les pages d'actualité.

Si certains pensent que l'outil Internet correspond à la conception de l'église dans le protestantisme, au service de la foi de chacun, il n'est guère au centre du développement religieux des paroisses de l'Eglise Protestante Unie, qui ne veulent à se mettre hors-murs dans Internet. En 1999-2000, avec le développement naissant de l'Internet grand public et de ses outils numériques encore méconnus des paroissiens, avec plusieurs pasteurs, nous avions proposé un projet qui échoua à cause du changement de divers responsables et de pasteurs, de l'incompréhension des conseils presbytéraux face à ce nouvel outil, de l'envie de certains membres, sans compétence, de vouloir se l'approprier.

La raison principale est liée à la non-évolution des structures ecclésiales au tournant du XXIe siècle et les freins consécutifs à la cooptation des membres dirigeants, limitant toute ouverture, vécue comme une perte de pouvoir personnel. L'expression de la foi se fait chez les huguenots en cercles très fermés, ne sont-ils pas à l'origine de la loi sur la laïcité [6] rejetant la religion dans la sphère privée. L'altérité ne s'accepte que dans la

[6] Au contraire des luthériens alsaciens et mosellans qui sont de la Confession d'Augsbourg, dont je suis, né dans une région française sous Concordat napoléonien de 1801, non soumis à la loi de 1905, et où la religion s'affiche jusque dans la déclaration d'impôts.

stricte limite admise dans une paroisse. Heureusement il y a des exceptions.

Et pourtant, il n'est que temps, tant le retard est énorme, que l'usage d'internet devienne le quotidien des paroisses ou un ensemble de paroisses, que ce développement fasse l'objet d'un suivi par une petite commission de paroissiens spécialistes (des vrais) assurant aussi la cybersécurité et des modalités à mettre en œuvre. Car les solutions sont connues, simples à mettre en œuvre à condition d'avoir l'humilité et la foi d'accepter d'évoluer, ce qui est du devoir de tout chrétien.

Quelques références et liens

Bergounhoux J., 2015. Etude : Les salariés trop confiants quant à la cybersécurité dans leur entreprise. http://www.usine-digitale.fr/article/etude-les-salaries-trop-confiants-quant-a-la-cybersecurite-dans-leur-entreprise.N336115

Bijaoui F., 2013. L'Église protestante unie sur Internet. *Réforme*, http://reforme.net/node/51816/publi-pdf.

Cottin J. & J. N. Bazin, 2003. Vers un christianisme virtuel ? Enjeux et défis d'Internet. Labor et Fides, Genève, 145 p.

Emig C. C., 2012. Alsace entre guerres et paix. *In* : Faire la guerre, faire la paix : approches sémantiques et ambiguïtés terminolo-giques. *Actes des Congrès des Sociétés historiques et scientifiques*, Éd. Comité des Travaux Historiques et Scientifiques, Paris, p. 195-207.

Emig C. C., 2013. Les publications des sociétés savantes françaises face à Internet. *Nouveaux eCrits scientifiques*, NeCs_02-2013, p. 1-5. http://paleopolis.rediris.es/NeCs/NeCs_02-2013/

Entreprises et cybersécurité à l'horizon 2020 - Synthèse de l'étude menée en 2013-2014 par le CIGREF associé à Futuribles International, 4 p. http://www.cigref.fr/wp/wp-content/uploads/2015/02/Futuribles-CIGREF-Entreprises-cybersecurite.pdf.

Esteral Consulting, 2011. Etude sur la cyberdéfense et la cybersécurité au sein des institutions européennes. Délégation aux Affaires Stratégiques, Ministère de la Défense, Paris, 38 p. http://www.defense.gouv.fr/content/download/149570/1496328/file/Cyberd%C3%A9fense%20et%20cybers%C3%A9curit%C3%A9%20au%20sein%20des%20institutions%20de%20l/'UE.pdf

La France et la cybersécurité, 2014. http://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/defense-et-securite/cybersecurite/

Lallement P., 2014. Cyber-Sécurité et PME : perception du risques, pratiques, besoins. p. 1-15, https://www.cecyf.fr/wp-content/uploads/2014/04/Etude-PME.pdf

Pernot M., 2016. Protestantisme et internet. https://oratoiredulouvre.fr/articles/protestantisme-et-internet.php. Consulté le 12 juin 2016.

Rapport Steria, 2014. Etude sur la cybersécurité des entreprises européennes. http://www.cil.cnrs.fr/CIL/spip.php?article2102

Serra J., La cybersécurité reste une problématique sous estimée dans les entreprises. http://riskattitude.net/la-cybersecurite-reste-une-problematique-sous-estimee-dans-les-entreprises/ 6 p.

Stener C., 2016. Dictionnaire politique d'internet et du numérique: Les cent enjeux de la société numérique. Books on Demand, Paris, 548 p.