Def'INSEEC
Pole Aerospace & Cybersecurity

Qu'est ce que la Cybersécurité ?

Interview de développeurs

Temps de lecture : 15min

INTRODUCTION:

La cybersécurité est, au même titre que l'aérospatial, un nouveau domaine aux enjeux encore peu connus de la société civile. Nouveau théâtre de conflits des forces étatiques, la cybersécurité recouvre de nombreux enjeux majeurs dans la gouvernance mondiale et dans la compétition internationale. Je vais alors tenter de simplifier sa définition à travers cet article.

L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) créée en 2009 définie la cybersécurité comme étant un "*Etat recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles*". Plus simplement, elle lutte contre la cybercriminalité via la cyberdéfense. Quelle est alors l'importance de la cybersécurité dans une société internationale ultra-connectée ?

Afin de comprendre cet univers, j'ai interrogé deux développeurs (aussi appelés analystes informaticiens), qui créent des logiciels et les mettent en oeuvre grâce au langage de programmation. Louis, développeur Web au sein d'une start up de big data franco-américaine et Mathieu développeur cette fois IOS (je ne vous présente plus cette entité qu'est Apple) nous présentent leurs métiers afin de comprendre ce que représente concrètement la cybersécurité par la programmation. Leurs noms de famille ne seront pas précisés afin de préserver leurs anonymats.

EN QUOI CONSISTE VOTRE MÉTIER DE DÉVELOPPEUR ?

Louis (développeur Web) : je développe un outil qui permet à l'équipe marketing de mieux cibler leurs clients et d'en acquérir de nouveaux . Le nom de cet outil est commun et s'appelle un *Costumer Data Plateform* (CDP). Plusieurs sont en train d'être créés et nous en faisons partie. Notre concurrent principal s'appelle *Segment*. Le but est de permettre aux équipes marketing de s'adresser aux bonnes personnes, aux bon moments, avec les bonnes données. En fait, on récupère les données de personnes qui naviguent sur Internet par exemple et s'ils arrivent sur ton site web c'est qu'ils sont intéressés. Il y a aussi une autre méthode, c'est la campagne *d'emailing*. Tu sais que si le potentiel client a cliqué sur le lien envoyé c'est qu'il est intéressé, ce qui montre que l'entreprise suscite un intérêt pour l'utilisateur en question. On peut aller un peu plus loin et permettre à nos clients de développer plein de manières d'activer ces mécanismes pour savoir ce qui suscite l'intérêt. Ca passe par des emails mais aussi par des outils marketing déjà existants sur Internet. C'est à dire qu'on développe des intégrations afin que cet outil fonctionne avec d'autres outils qui permet ensuite de centraliser les données chez *Hull*.

Mathieu (développeur IOS) : Ça fait 2 ans que je travaille dans une SS2I (on parle d'ESN depuis peu, c'est une boite qui emploi d'autres boites, un peu comme de la prestation de service) en tant que dévelopeur IOS et Android mais principalement IOS. J'ai travaillé sur différentes applications de start up et de grosses boites. Ça fait un an que je travaille pour Eurosport aujourd'hui, nous y refaisons l'application, en tout cas la partie IOS. Nous sommes sept à nous en occuper.

AVEZ-VOUS ACCÈS AUX DONNÉES DE VOS CLIENTS ?

Louis : Oui mais chacune de ces données sont réservées et encryptées pour chacun de nos clients. En fait, le cryptage des données fait que nous ne pouvons pas les lire mais à partir du moment où ces clients nous invitent dans leurs organisations ou dans leurs entreprises "virtuelles", nous pouvons avoir accès à ces données. On peut ensuite savoir ce qu'il faut mettre en place pour les aider à implanter notre système chez eux. C'est aussi notre devoir de ne pas divulguer ces données et de les conserver pour eux seulement. Seul les comptes administrateurs peuvent avoir accès aux données. Nous sommes chargé de mettre en place l'encryptage en suivant des standards d'encryptions qui permet ensuite une certification.

Mathieu : Nous gérons juste le chiffrage des appels que l'on passe à la base de données, aux API. Quand tu développes en général, tu as le *front end*, c'est la page que voit l'utilisateur et tu as la base de données où sont stockées les informations de ton ou tes utilisateurs. Entre les deux, comme ces deux choses ne communiquent pas directement, il y a une API qui interface ta base de données avec ton *front end*. Donc en général, je m'occupe du *front end*, je récupère de la data, je la chiffre et l'envoie ensuite à la base de données pour qu'elle la traite. Nous nous assurons que ces données ne soient pas interceptées et/ou modifiées. Le stockage de données est très encadré chez IOS (nous avons l'obligation de respecter le RGPD *(définit plus bas)*, demander à l'utilisateur qu'il accepte telle ou telle chose, etc), nous stockons quand nous créons des librairies pour de grands groupes comme Google qui va ensuite limiter les données qui vont être stockées ou non.

AVEZ-VOUS DÉJÀ ENTENDU PARLER DE CYBERSÉCURITÉ ? POURRIEZ-VOUS LA DÉFINIR ?

Louis : C'est la protection des données utilisateurs que ce soit dans l'aspect matériel : tu peux attaquer un ordinateur en te branchant dessus avec une clé USB en soutirant des données. Ou virtuel : tu peux attaquer des données en créant un malware par exemple ou en trouvant ce qu'on appelle une bague d'or dans les systèmes, c'est comme une faille qui te permet de te connecter en tant qu'administrateur pour accéder aux données. C'est par là que peut passer un hacker par exemple.

Mathieu : Pour moi ça touche à plusieurs aspects, en général quand je pense à cybersécurité je pense à tout ce qui est sécurité via tout ce qui est électronique donc tout ce qui est *hard ware* mais aussi *soft ware*, ca me fait penser à plein de chose comme l'encryption des données ou encore les portes dérobées dans les applications.

POUR UNE ENTREPRISE, QUELS SONT LES PLUS GROS RISQUES QUAND SA CYBERSÉCURITÉ N'EST PAS EFFICACE ?

Petite précision : La certification dont parle Louis est fournie par la fameuse ANSSI. Elle atteste de la robustesse d'un produit basé sur l'analyse de la conformité et des tests de pénétration réalisés par un évaluateur tiers sous l'autorité de l'ANSSI. Il existe deux types de certifications :

- La certification dite de ***"critères communs"*** : c'est une certification de haut niveau qui permet de s'assurer en tant qu'utilisateur de la conformité d'un produit à un cahier des charges ou à une spécification technique (on parle de "cible de sécurité"). Cette vérification se fait par un tiers dit "organisme certificateur" qui permet une confirmation indépendante et impartiale. En France, cette certification est décrite par le décret 2002-535 du 18 avril 2002 pour les produits et les systèmes de sécurité. Ces certifications sont reconnues à l'international. Cherche ce petit logo !
- La certification de ***sécurité de premier niveau (CSPN)*** est mise en place en 2008 par l'ANSSI et, consiste en des tests de "boites noires" en des temps et délais imposés. C'est une alternative à la première certification qui est bien plus onéreuse et longue et quand le niveau de confiance visé est moins élevé.

Le certificat ne s'applique pas aux nouvelles versions du produit. Mais parfois, certaines évolutions ne touchent pas à la sécurité du produit, le centre de certification propose alors une "continuité d'assurance". On parle aussi de surveillance du produit face aux nouvelles attaques mise en oeuvre où l'ANSSI surveille la vulnérabilité du produit et en informe son propriétaire. Si aucune de ces hypothèses n'est vérifiée, l'ANSSI entreprend alors la "Certification d'une nouvelle version d'un produit certifié" par une nouvelle évaluation. Clique sur ce lien si tu veux en savoir plus ! (https://www.ssi.gouv.fr/uploads/2018/01/certification_securite_produits_visa_securite_anssi.pdf)

Louis : J'en vois deux principales notamment une dans l'aspect marketing : si tu n'intègres pas des standards sur ta sécurité informatique, personne ne te fera confiance, tu n'auras aucun client et personne ne voudra entrer en contact avec toi. C'est rassurant quand tu as une certification qui prouve que tu intègres tel ou tel standard. La deuxième c'est qu'en tant qu'entreprise, tu peux perdre toutes tes données. Tout ce que tu as entrepris en termes de recherches et de projets peut se retrouver entre les mains de personnes malveillantes qui peuvent te demander des rançons contre tes données (ou encore des *ransomware*, c'est à dire un échange de données).

Mathieu : Ça peut aller très loin, par exemple, tu peux perdre des contrats dans une SS2I. Si tu travailles pour un client et que tu fais fuiter une clé d'un serveur qui a accès à des données, ça peut être utilisé à de mauvaises fins. Dans les entreprises, on se sert aussi beaucoup de service Cloud, (quand tu es développeur, tu as parfois besoin d'envoyer des mails de validation ou de confirmation). Pour avoir accès à ce Cloud il faut souscrire à un abonnement, on te donne alors des identifiants et si tu les perds, on peut s'en service pour faire du SPAM par exemple. Donc ça peut nous faire perdre des projets et des partenaires. On nous envoie souvent des formations sur la cybersécurité pour être à jour, ça rassure nos collaborateurs. On a aussi des audits de sécurité qui sont fait en général par nos clients.

EST-CE QUE VOUS PENSEZ QUE CEUX QUI NE SONT PAS DANS LE MILIEU DE LA PROGRAMMATION SE RENDENT COMPTE DE LA NÉCESSITÉ DE BIEN PROTÉGER LEURS APPAREILS CONNECTÉS ?

Louis : je ne pense pas parce que c'est quelque chose de complètement caché en fait ou au moins quelque chose qui va te demander beaucoup d'apprentissage. C'est loin d'être ce que tu vois dans les films, c'est plus qu'un terminal ou tu vois s'afficher plein de lettres et de chiffres. C'est assez complexe et mathématique et je pense que ce n'est pas non plus à la portée de tout le monde. En plus ça n'intéresse pas tout le monde non plus et ça rend les choses encore moins évidentes malheureusement. Pourtant il y a des sites web très sympa qui te permettent de t'y intéresser en te donnant des instructions de plus en plus dures, ce n'est pas forcement pour apprendre à coder mais au moins tu peux te familiariser avec la programmation (Let's go ! ! www.root-me.org/?lang=fr).

Mathieu : Non je ne pense pas, pas assez en tout cas. Sur les données bancaires j'ai l'impression que les gens essayent de faire plus attention mais ils ne se rendent pas compte qu'il y a tout un autre monde par rapport à leurs données en général. Quand on voit déjà les efforts considérables qu'on doit faire pour faire comprendre aux gens que le *phishing* existe, il y a des gens qui se font avoir par des mails qui sont horriblement mal fait. On les voit très vite quand on est dans l'informatique mais la plupart des gens ne les reconnaissent pas forcément. Ou des gens qui, quand ils entrent sur des sites rentrent des informations même sur Facebook ou autres sans forcément trop faire attention. Ils ne se rendent pas forcément compte des conséquences que ça peut engendrer. Par exemple TikTok récupère un nombre incroyable d'informations sur toi qui est juste absurde.

Des efforts sont fait dans ce sens-là, en tout cas dans le cadre de mon travail avec Apple et Google qui essayent vraiment de sensibiliser les gens à ça. Par exemple dans les dernières versions d'IOS, ils te préviennent quand une application que tu utilises saisie le contenu de ton presse-papier. Toutes les grosses applications se sont fait avoir par ça. Quand la nouvelle version est sortie, les gens se sont étonnés de savoir que des grosses applications comme LinkedIn pouvaient faire ça. Le *targetting* que les grosses applications sont capables de faire est incroyable, elles récupèrent l'intégralité de tes informations comme savoir où t'appuies, combien de temps tu passes à un endroit, qu'est ce qui t'intéresse... Ils ont même mis en place des algorithmes qui peuvent, même sans avoir accès à ta caméra mais juste avec ce que tu fais sur ton écran, savoir qu'elle partie du contenu t'es en train de regarder, qu'est ce qui t'intéresse et ensuite ils relient ces informations aux leurs.

Donc y a énormément d'informations qui sont récupérées sur toi et qui sont traitées d'une manière ou d'une autre. L'enjeu le plus important pour les entreprises c'est de récolter le plus de data possible parce qu'on est dans un monde où l'intelligence artificielle (IA) est facile à faire. Le plus compliqué dans l'IA c'est d'avoir la data nécessaire pour l'entrainer. Plus tu as de data et plus c'est facile de l'entrainer à reconnaître certaines choses et donc de mettre en place des pubs ciblées, de savoir ce que l'utilisateur a envie d'acheter, etc. Je pense qu'il n'y a pas du tout assez de gens au courant de ça. Il faudrait surtout que la data soit anonymisée mais beaucoup d'entreprises ne le font pas parce que ça permet de retracer les informations.

PARLONS UN PEU DE CYBER-ATTAQUES, EST CE QUE TU PEUX ME DÉFINIR CE QU'EST LE HACKING ?

Louis : La définition du mot cybersécurité est étroitement liée. C'est quand tu arrives à passer outre les précautions mises en place et que, manuellement, tu trouves un défaut dans cette sécurité pour parvenir à des fins diverses (rançon, espionnage, etc).

Mathieu : Je ne saurais pas vraiment le définir mais pour illustrer un peu la cyber-attaque la plus dangereuse selon moi, c'est une une cyber-attaque capable de vivre comme un virus. Vivre et se propager sur ton réseau wifi, Internet, et capable d'écouter et de voir tout ce que tu fais et par conséquent capable de récupérer les données que tu tapes sur ton écran ou lorsque tu parles et capable aussi les modifier. Par exemple tu es en train de payer quelque chose sur Internet, ça peut modifier ta page et t'envoyer une page de paiement pour un hackeur en Roumanie. Pour moi les plus dangereuses vont être celles qui s'attachent au nucléaire, à tout ce qui est électrique ou encore les hôpitaux.

Y A-T-IL UN ÉPISODE DE HACKING, OU PLUS GÉNÉRALEMENT DE CYBER-ATTAQUE, QUI VOUS A MARQUÉ ?

Louis : Au niveau des processeurs Intel (Il existe deux fournisseurs de processeurs, Intel ou AMD, Intel était l'un des plus utilisé à l'époque en 2018). Certaines personnes ont trouvé des failles pour atteindre la mémoire de ton ordinateur. La faille a été descellée par *Melt Down Inspector*. Intel s'est retrouvé débordé car tous les appareils qui avaient ce processeur ou un modèle plus ancien étaient infectés, ça concernait beaucoup d'appareils qui couraient le risque de se voir voler leurs données.

Mathieu : Tu as les attaques DDoS ("attaque par déni de service", ce sont des tentatives de surcharge d'un serveur en lui envoyant beaucoup plus de requêtes qu'il ne peut supporter). Ce sont les plus faciles à mettre en œuvre, n'importe qui peut le faire sur Internet avec un peu d'argent. Quand tu vas sur un site, tu envoies l'adresse du site à Google ou autre, qui t'affiche ensuite ta demande. Quand quelques personnes le font, le serveur supporte. Mais quand c'est six millions de personnes ça peut faire crasher le site et donc le faire redémarrer. Et ça c'est super facile à faire aujourd'hui surtout vu le nombre d'appareils connectés qu'on a maintenant qui sont très mal protégés. Donc tu as beaucoup de gens qui répandent des virus sur les appareils connectés et qui créent des *"réseaux de botnet"* qui vont pouvoir envoyer simultanément des demandes d'accès à une page et faire crasher le site. C'est déjà arrivé à de très gros services comme Netflix mais aussi au réseau de Playstation qui était HS pendant une journée entière... Et comme il y a de plus en plus d'objets connectés, ça devient de plus en plus compliqué. Le plus dangereux ça peut être de faire tomber des réseaux importants comme celui des hôpitaux qui essayent quand même de travailler le plus possible en réseau fermé mais cette possibilité reste quand même envisageable.

SELON VOUS, LA CYBERSÉCURITÉ EST-ELLE PLUS ACCESSIBLE QUE LE HACKING DE NOS JOURS ?

Louis : Je pense que maintenant il est plus simple de se protéger, un simple anti-virus c'est déjà assez protecteur. En termes de sécurité, l'information est très accessible. Il suffit d'aller sur Internet voir quelles sont les bonnes informations à prendre ou alors ce qu'il faut éviter et prendre les bonnes précautions : utiliser des générateurs de mots de passe, utiliser la double authentification ce qui permet d'assurer que ce soit toi qui autorises la connexion à un service. Alors que pour le hacking, il faut déjà savoir comment tout cela fonctionne derrière pour qu'ensuite tu puisses te connecter pour essayer de *bypass*.

Mathieu : Ce sera toujours apprendre à se protéger donc la cybersécurité est le plus accessible. À partir du moment où tu veux apprendre à hacker ou plutôt cyber-attaquer et que tu n'as aucune connaissance, tu devras passer par des services où tu vas payer très chère ou bien te faire arnaquer d'une manière ou d'une autre. Donc tu vas plutôt risquer d'attraper un virus en passant par des sites douteux. Pas mal de gens en sont conscients et c'est assez ancré dans les esprits.

POUR VOUS, QUEL EST L'APPAREIL LE PLUS MENACÉ ?

Louis : Je dirais que les mobiles s'en sortent bien parce qu'on peut contrôler un peu plus de chose. Pour moi ce sont plus les ordinateurs portables où tu peux lancer un navigateur internet. Ce qui m'énerve le plus c'est le *phishing*, en anglais on parle de SCAM, c'est une page qui apparait que tu ne peux pas quitter sans appuyer sur cette fenêtre type *"vous avez un problème sur votre ordinateur, contactez ce numéro"*. Quand tu appelles, quelqu'un répond et te donne des indications et finit par prendre le contrôle de ton ordinateur. Elle te demande ensuite de payer leur service et te voit entrer tes données bancaires pour ensuite te les voler. Ça arrive trop fréquemment et facilement parce qu'il n'y a pas assez sensibilisation sur le sujet .

Mathieu : Pour moi ce sont les petits appareils connectés qui ne coutent pas chère type smart home, ta lampe, ton interrupteur, ta prise connectée, toutes ces petites choses là parce qu'il y a peu de temps et d'argent qui sont mis dans le développement de ces appareils. C'est très mal protégé et ça accède à Internet au même titre que ton téléphone.

CONNAISSEZ-VOUS LA LÉGISLATION QUI ENCADRE LA RÉCOLTE ET LA PROTECTION DES DONNÉES ?

Louis : Je devrais, mais non pas vraiment... Dans le cadre de mon travail je m'assure toujours que les données soient le plus protégées possible, en tout cas soient le moins "extractables" mais je ne sais pas vraiment ce que la loi encadre ou non. En plus dans mon contrat il est précisé que je suis responsable et que je dois m'assurer qu'il n'y est aucune fuite de données.

Mathieu : C'est obligatoire maintenant en tout cas nous chez IOS nous n'avons pas le choix. Depuis les dernières versions d'IOS, Apple nous oblige à déclarer exactement les infos que nous récupérons, si nous insérons des pubs, de préciser si elles sont targettées ou non et d'autoriser l'utilisateur à ne pas accepter que les pubs soient targettées. Nous sommes obligés de détailler ce que nous faisons. Après il doit toujours y avoir des moyens de bypasser ça mais c'est quand même assez encadré.

Petite précision : C'est le ***RGPD*** qui encadre la récolte des données au sein de l'Union Européenne. Le RGPD (Règlement Général sur la Protection des Données) a été adopté par le Parlement Européen le 14 avril 2016. Il est applicable depuis 2018 dans tous les pays membres de l'Union Européenne. Il vise à renforcer les droits des citoyens européens et leurs donne plus de contrôle sur leurs données personnelles. Notamment, il permet aux citoyens d'obtenir leurs données sous une forme claire, accessible et compréhensible et d'en contrôler leurs utilisation (droit à l'oubli, droit à la portabilité, etc).

De plus, les mineurs font l'objet d'une protection particulière. Il vise également à simplifier les formalités pour les entreprises et leurs offre un cadre juridique unifié en leurs fournissant une boite à outils de conformité (code de conduite, certification). Enfin, le RGPD créé le Comité Européen de la Protection des données (CEPD) contribue à "l'application cohérente des règles en matière de protection des données au sein de l'Union Européenne et encourage la coopération entre autorités de l'UE chargée de la protection des données". Il peut rendre des avis contraignants notamment et prononcer des sanctions.

TROUVEZ-VOUS QUE CE QUE VOUS FAITES SUR INTERNET ET VOS ORDINATEURS EST BIEN ENCADRÉ ?

Louis : Tu peux faire beaucoup trop de choses selon moi. Même quand tu télécharges de la musique, le seul risque que tu prenais c'était un mail d'Hadopi. Mais à part Hadopi et la NASA qui nous observent je ne connais aucunes autres autorités censées contrôler ce qui se passe sur Internet.

Mathieu : Je pense que ce n'est pas assez encadré, parce que je vois que les seuls audits sont mandatés par les boites qui veulent être certaines qu'elles n'auront pas de problème plus tard mais ça s'arrête là. Je connais trop de gens dans des start-ups qui ne connaissent pas du tout le RGPD et qui pourtant récoltent beaucoup de données sur les utilisateurs. C'est super complexe de savoir quelle boite le fait ou non. Donc non je pense que c'est très mal contrôlé. Les grosses boites peuvent avoir des contrôles inopinés mais pour les petites boites il y a peu de chance que quelqu'un aille s'en inquiéter.

PENSEZ-VOUS QUE LE CONFINEMENT A UN EFFET SUR LA CYBERSÉCURITÉ DES INDIVIDUS ?

Louis : Je pense oui car certains business profitent de ce confinement, comme ils sont entièrement digitalisés, pour accumuler plus de clients et de données. Après c'est à eux que revient la responsabilité de les protéger donc ça peut être dangereux s'ils ne savent pas protéger correctement.

Mathieu : Je ne pense pas que les gens vont plus s'intéresser à ça pendant le confinement. Ils vont peut-être utiliser Internet davantage, on entend plus parler de chose comme Zoom qui s'est fait attraper pour le non-chiffrage de ses données mais ça s'arrête là. Concernant les gens que je connais, parents et famille, plus âgés en tout cas, je ne vois pas de regain d'intérêt soudain pour ces choses-là.

PEUX-TU ME DONNER TON AVIS SUR LA 5G ? POUR OU CONTRE ? LES RISQUES EXPOSÉS SONT-ILS RÉELS (VOL DE DONNÉES, ACCÈS À TA CAMÉRA, ETC) ?

Matthieu : Il y a ce débat tous les dix ans, c'est la fréquence à laquelle on change de standard et à chaque fois il y a ce débat de complotistes disant qu'on va avoir accès à tout. Mais la vérité c'est qu'il n'y a pas accès à plus de choses. Avec les nouvelles technologies, ça nous permettrait de faire avancer ces choses-là. La 5G nous permettra simplement d'avoir une plus grande vitesse et une meilleure qualité de débit, on pourra accéder plus rapidement aux choses.

Propos recueillis par Guillemette Jahn
Responsable du pôle Aerospace & Cybersecurity de l'association Def'INSEEC le 12/11/2020 et le 14/12/2020

Correctrices :

Anaëlle Le Lostec
Constance Alloy

Sitographie :

- https://www.ssi.gouv.fr/administration/glossaire/c/
- https://www.ssi.gouv.fr/uploads/2018/01/certification_securite_produits_visa_securite_anssi.pdf
- https://www.ssi.gouv.fr/administration/produits-certifies/cc/
- https://www.cnil.fr/fr/adoption-du-reglement-europeen-par-le-parlement-europeen-un-grand-pas-pour-la-protection-des-donnees
- https://edpb.europa.eu/about-edpb/about-edpb_fr

Suivez Def'INSEEC sur :

Def'INSEEC
Pole Aerospace & Cybersecurity