Application mobile pour la prévention des risques cyber

Cahier des charges

Projet de

Michel Nguyen
Thierry Ralainarivo

Etudiants en master de mathématiques à Paris VIII

Février 2021

Contexte

Dans une période de crise sanitaire où la nécessité d'organiser de la communication à distance est de plus en plus exigée, le risque de cyberattaque prend une place prépondérante dans notre société devenue hyper connectée.

En effet, des grandes entreprises subissent des cyberattaques quotidiennement, mettant en péril leur bon fonctionnement. Les petites et moyennes entreprises sont aussi dans le viseur, d'où le besoin d'une défense cyber solide.

Ainsi, il nous faut se protéger contre des cyberattaques potentielles qui pourraient être dévastateur contre des groupes de mieux en mieux organisés dans le vol de données.

Pour cela, le Gouvernement français décide de mener un dispositif expérimental, en lien avec le ministère de l'Intérieur, qui vise à mieux s'adapter aux nouvelles technologies. Ce dispositif est incarné par la création d'une application mobile gratuite qui doit être un outil puissant face aux risques cyber en complément de son site préventif contre les risques cyber[1].

Cette application doit être rapide d'utilisation, simple à manipuler et pratique à utiliser. Concrètement, d'une part, toutes les données du site du gouvernement sont transposées à l'application. D'autre part, de nouvelles fonctionnalités sont ajoutées pour garantir une efficacité maximale : possibilité de contacter via visioconférence des experts de la cybersécurité (ce sont des fonctionnaires ou salariés), s'alerter en cas de cyberattaque et réponse dans les plus brefs délais du ministère de l'Intérieur, suivre un cours en ligne qui enseigne les bonnes pratiques à avoir en entreprise.

Objectifs de l'application mobile

La création d'une applications s'inscrit dans une modernisation de l'Etat pour répondre aux nouveaux usages de la société. Le téléphone portable est un bien possédé par de nombreuses personnes de toutes catégories sociales. En particulier, il peut constituer un outil de travail. Récemment, le Gouvernement français lance sa première application mobile gratuite « Tous AntiCovid » qui connait un certain succès (plus de 10 millions

[1] https://www.gouvernement.fr/risques/risques-cyber

d'utilisateurs). Il s'agit d'un outil qui réunit : informations sur la crise sanitaire, possibilité de se déclarer cas covid et recevoir une alerte en cas de contact covid. Il est donc cohérent de lancer un nouveau dispositif expérimental concernant les risques cyber car les cyberattaques prennent de plus en plus de poids au fil des années. Inspiré de l'application « Tous AntiCovid », l'application se veut simple d'utilisation et doit constituer un guide contre la menace cyber.

Dans un premier temps, le déploiement sera à l'échelle régionale puis nationale.

L'application a deux objectifs. D'une part, l'intention d'informer et de prévenir les risques cyber. Puis d'enseigner les bons gestes en entreprise à adopter. D'autre part, la volonté de renforcer la défense des entreprises en cas de cyberattaque par la possibilité de contacter l'ANSSI (l'agence nationale de la sécurité des systèmes d'information affiliée au Ministère de l'Intérieur) et obtenir une réponse de celle-ci.

Spécificités de l'application mobile

1. Prévention et enseignement

En se calquant sur les rubriques du site du gouvernement[2], l'application possède quatre blocs pour apprendre sur différents thèmes des risques cyber : cybercriminalité, atteinte à l'image, espionnage et sabotage. Le texte contenu s'inspire du site et se doit d'être d'actualité.

Ensuite, l'application propose un cours en ligne sous forme de fiches récapitulatives à mémoriser, des vidéos à analyser et plusieurs QCM à répondre pour inciter à l'apprentissage. Ce cours en ligne doit être crée par un collectif d'experts en cybersécurité afin de partager les meilleurs connaissances.

2. Contact

Grâce à la flexibilité du téléphone portable, l'application possédera des fonctionnalités qui feront l'intérêt de cette application. D'abord, c'est de pouvoir organiser un rendez-vous avec un expert de la cybersécurité et se voir par visioconférence. Pendant ce rendez-vous,

[2] https://www.gouvernement.fr/risques/risques-cyber

plusieurs sujets peuvent être demandés : demander des renseignements, se faire conseiller sur l'achat de matériel informatique, demander un audit etc…

Ensuite, en cas de tentative d'intrusion avérée, il sera possible de contacter l'ANSSI afin d'avoir un échange téléphonique puis d'organiser une intervention rapide et efficace sans le moindre coût.

En d'autres termes, cet outil se veut comme un intermédiaire efficace entre différents acteurs pour lutter contre les risques cyber. Plus l'intervention est rapide, plus les dégâts sont moindres.

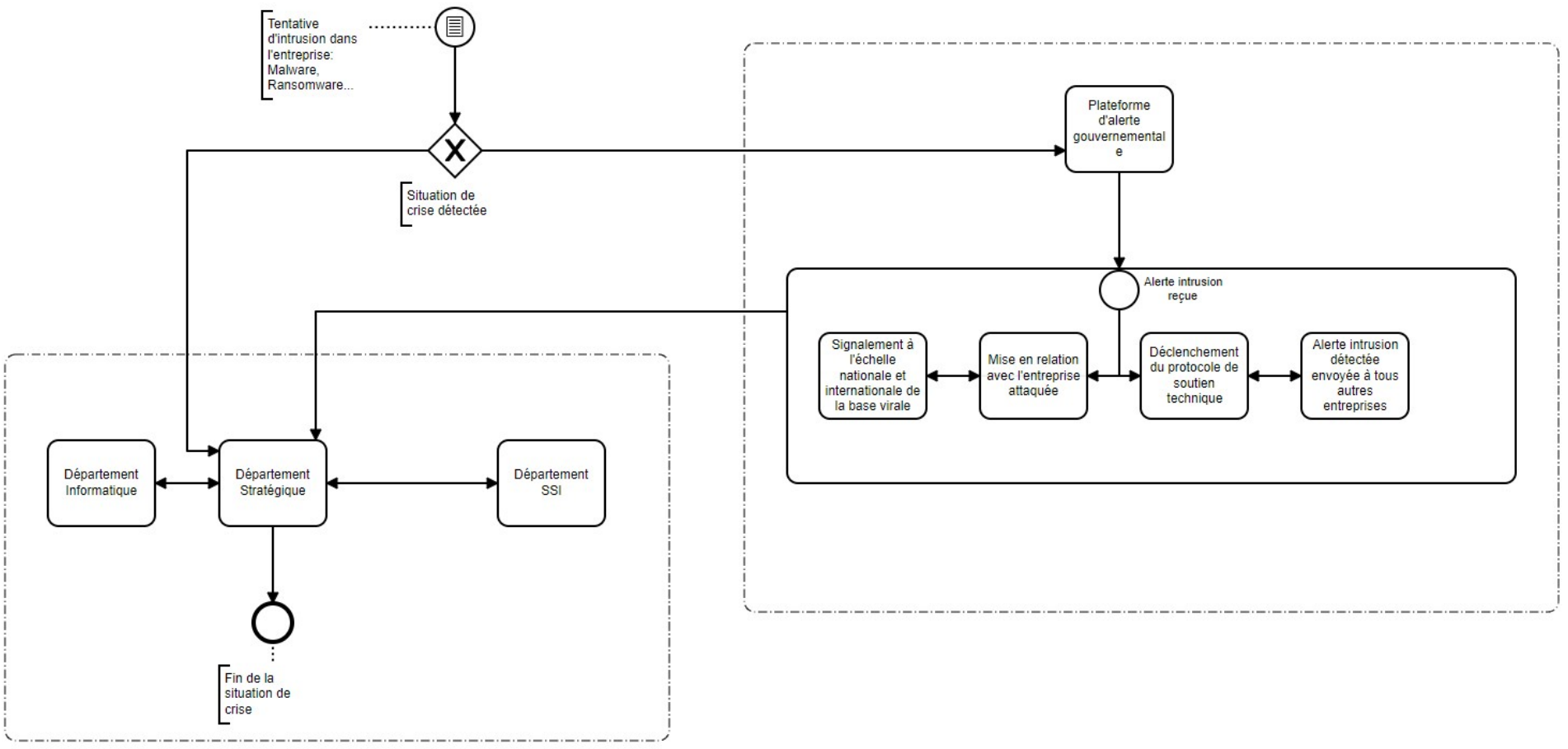

Diagramme explicatif en cas de tentative d'intrusion (crée sur bpmn.io)

3. Fonctionnement interne

Sur le principe de l'application « Tous AntiCovid », cette application est une application de "contact tracing" (traçage) pour avoir des indications utiles sur l'évolution de l'épidémie et sur les démarches à suivre. Dans notre cas, on s'intéressera à l'évolution d'une base virale récemment détectée et déclarée. L'événement sera déclaré en temps réel, avec un timestamp et une adresse IP de la cible touchée pour pouvoir délimitée, mesurée et

essayée de « confiner » ou de mettre en quarantaine immédiatement le malware ou le ransomware en temps et en lieu.

Il assurera une interopérabilité avec tous les systèmes d'exploitation utilisés en entreprise et ne collectera pas de données de l'entreprise ainsi que de ses employés.

L'efficacité de cette application sera assurée uniquement par le nombre important de ses utilisateurs. Plus il y aura d'entreprise enregistré, plus vite sera la réponse à l'attaque. En effet, plus il y aura d'utilisateurs, plus de monde pourra mettre à jour en ligne les nouvelles bases virales, plus vite seront informés les autres alors plus nombreuses seront les entreprises informées et préservées.

Pour que le système marche, il est impératif que le réseau inter-entreprise soit sécurisé sinon cela pourra générer un fausse alerte ou une intrusion non détectée.

Dans le cas d'une tentative d'intrusion, une alerte sera envoyée automatiquement à la direction de sécurité des systèmes de l'information (DSSI) de l'entreprise et mettra en copie un message crypté vers le centre responsable du traitement des messages au sein du ministère de l'Intérieur.

Publics visés

Toutes les entreprises privées peuvent utiliser l'application bien qu'ils possèdent eux-mêmes une protection cyber. C'est notamment le cas de grandes entreprises. Dans ce cas, cet outil se veut comme un complément de sécurité.

Pour des petites et moyennes entreprises qui ne possèdent pas une défense suffisante, l'application peut grandement aider leur protection cyber en conseillant et en orientant vers des meilleurs pratiques et matériels.

Dans tous les cas, pouvoir déclarer une tentative d'intrusion est une fonctionnalité qui s'adresse à tous types d'entreprises qui pourrait justifier l'installation de cette application.

Description fonctionnelle des besoins

Avant de programmer l'application, il faudra mener des discussions avec des acteurs privées pour décider des besoins de chacun et de recueillir leurs avis sur un potentiel outil de cette nature. Pour cela, la mobilisation d'un groupe parlementaire se chargera de mener des discussions avec des experts de la cybersécurité et des entreprises proches du numérique.

Ensuite, pour la création et la maintenance de l'application, la sollicitation d'une entreprise privée spécialisé dans le développement mobile est envisagée. Ce groupe sera constitué d'une dizaine de développeurs.

Délais

Il est envisagé le calendrier suivant : neuf mois de discussions par des parlementaires au bout duquel ils doivent rendre un rapport complet sur les besoins et les attentes. Ensuite, s'il y a un accord massif à la création de cet outil, le développement commencera pendant trois mois pour une date de sortie début 2022.

L'expérimentation durera au moins 6 mois avant de faire un premier bilan. Il est question de savoir principalement le nombre de téléchargements, le nombre d'alertes à une tentative d'intrusion, la rapidité et l'efficacité des interventions. En cas de succès, l'application sera régulièrement mise à jour avec de nouvelles fonctionnalités pour devenir encore plus indispensable aux yeux des entreprises.

Enveloppe budgétaire

Environ 2 à 3 millions d'euros seront engagés pour cette expérimentation. On peut estimer le coût des discussions parlementaires et le développement à un million d'euros. Ensuite, en s'inspirant du coût de l'application « Tous AntiCovid »[3], on peut estimer la maintenance à environ 100 000 euros par mois au vu de la similarité de ces deux applications.

---

[3] https://www.leparisien.fr/high-tech/stopcovid-a-quoi-va-ressembler-la-facture-de-l-appli-anti-epidemie-08-06-2020-8331903.php