<CAMPUS CYBER>

RAPPORT MISSION PME & CYBERSÉCURITÉ

Le Président du Campus Cyber, Michel Van den Berghe, et son équipe : Yann Bonnet, Directeur général délégué du Campus Cyber ; Lucile Briolat, Chargée de projets écosystème et international ; Magali Marques, Directrice de Cabinet ; Mathilde Pareau, Alternante veille et écosystème

<Synthèse>

Bien que notre dépendance aux outils numériques soit en constante hausse, la pandémie du COVID a marqué un tournant en termes d'exposition au risque numérique. Le virage forcé effectué vers un monde connecté a augmenté les surfaces d'attaque possibles. D'après le panorama de la menace de l'ANSSI, les rançongiciels ont été multipliés par 4 entre 2019 et 2020[1]. La menace est protéiforme, croissante et ne cesse de se renouveler. C'est pourquoi, en 2022, pour la première fois, la cybersécurité a été classée dans le TOP 10 des risques business par le Forum économique mondial[2].

Les conséquences d'une attaque cyber sont multiples : économiques, sociales, humaines, etc. Car si le coût d'une attaque s'élève de plusieurs dizaines de milliers à plusieurs millions d'euros, elle a également un impact réel sur le quotidien des individus : arrêt d'un hôpital, pertes de données personnelles, stress élevé, etc. La dernière attaque contre la collectivité de la Martinique au mois de mai 2023 s'est traduite, par exemple, par une incapacité à verser les prestations sociales pendant plusieurs semaines. Trois mois plus tard, les systèmes ne sont toujours pas rétablis. Il est donc nécessaire de protéger les systèmes en anticipant le risque et identifiant les faiblesses de la structure informatique.

Dans ce contexte, dépendantes aux technologies numériques mais peu préparées à faire face aux risques, les plus petites entreprises sont des acteurs fragiles. En effet, 56% des PME ont connu au moins un incident cyber en 2021[3]. La cybersécurité des TPE/PME/ETI[5] constitue donc un réel risque pour notre santé économique, d'autant que les PME représentent plus de 99% du tissu économique français, soit plus de 4 millions d'entreprises[6].

La cybersécurité est une préoccupation des grands groupes depuis plusieurs années. L'ANSSI a noté pour la première fois en 2022 une diminution d'attaque réussie vers ces acteurs et un détournement de la menace vers les PME, moins bien protégées[7]. Cela s'explique notamment par : un manque de moyens financiers, de temps et de connaissance sur l'état réel de la menace mais également une difficulté à s'orienter vers les solutions adaptées au sein d'un marché foisonnant et usant d'un vocabulaire parfois complexe. Ainsi, la cybersécurité doit permettre aux PME d'assurer la continuité de leurs activités, sans devenir une difficulté technique.

Face à ce constat, les législations françaises et européennes se renforcent pour inciter et obliger à la sécurisation des PME. D'ici octobre 2024, la directive européenne NIS2 sera transposée en droit français : elle vise à renforcer la cybersécurité des acteurs les plus faibles en responsabilisant l'ensemble de la chaine d'approvisionnement. Dans les prochains mois, les PME vont donc devoir mettre en place des solutions de cybersécurité pour être en conformité avec la législation. Par ailleurs, le développement en cours d'une offre d'assurance cyber va nécessairement s'accompagner d'une définition des niveaux minimum de sécurité informatique à atteindre pour y souscrire.

Concernant les politiques françaises, ces dernières se sont concentrées sur la protection des acteurs sensibles et acteurs publics. Le GIP ACYMA et le développement en cours des CSIRT régionaux représentent la possibilité pour les PME de disposer d'interlocuteurs privilégiés en cas d'attaque. Néanmoins, il est nécessaire d'accentuer ces politiques pour passer à l'échelle rapidement en termes de sécurisation des PME, notamment en clarifiant les besoins et les offres du marché adaptés au niveau de maturité et au secteur d'activité de chaque PME.

De nombreux acteurs se sont d'ores et déjà organisés pour apporter une réponse à cet enjeu : guides de bonnes pratiques et solutions de sécurisation des systèmes d'information existent, au niveau privé comme public. Néanmoins, cette offre foisonnante est parfois désorganisée et souvent complexe à appréhender par des PME novices, d'autant qu'un vocabulaire technique est souvent utilisé. Une réelle coordination entre les acteurs et activités existantes est donc à trouver pour passer de la prise de conscience du risque en cours (75% des dirigeants ont conscience du risque[8]) à la mise en place concrète d'outils de sécurité numérique.

Il est urgent d'agir collectivement car il existe un risque de crise majeure. Une attaque massive des PME constituerait un blocage sans précédent des activités économiques et sociales du pays.

Michel Van den Berghe, Président du Campus Cyber, a donc été missionné en décembre 2022 par le Ministre Jean-Noël Barrot pour la conduite d'un plan de recommandations pour une plus grande sécurisation des TPE, PME et ETI françaises[9]. Cette mission s'est appuyée pour produire ce rapport sur des auditions des acteurs publics et privés[10], des questionnaires recensant[11] les dispositifs existants chez les acteurs publics et privés[12], des focus groupe PME, des restitutions groupées et une analyse des modèles mis en place dans 7 pays[13].

[1] Panorama de l'état de la menace de l'ANSSI 2020, CERTFR-2021-CTI-001.pdf (ssi.gouv.fr)
[2] The global risks report 2022, WEF_The_Global_Risks_Report_2022.pdf (weforum.org)
[3] Rapport du Sénat sur la cybersécurité des entreprises 2021, Modèle pour la frappe des Rapports Parlementaires (senat.fr)
[4] Jean-Noël Barrot, ministre délégué chargé de la transition numérique et des télécommunications
[5] Définitions selon l'art. 51 de la loi de modernisation de l'économie : « Une microentreprise est une entreprise dont l'effectif est inférieur à 10 personnes et dont le chiffre d'affaires ou le total du bilan annuel n'excède pas 2 millions d'euros. Une PME est une entreprise dont l'effectif est inférieur à 250 personnes et dont le chiffre d'affaires annuel n'excède pas 50 millions d'euros ou dont le total de bilan n'excède pas 43 millions d'euros. Une ETI, entreprise de taille intermédiaire, est une entreprise qui n'appartient pas à la catégorie des PME, dont l'effectif est inférieur à 5000 personnes et dont le chiffre d'affaires annuel n'excède pas 1 500 millions d'euros ou dont le total de bilan n'excède pas 2 000 millions d'euros. »
Utilisation du termes PME pour désigner l'ensemble dans le rapport
[6] INSEE, les entreprises en France, édition 2021, Catégories d'entreprises – Les entreprises en France | Insee
[7] Panorama de l'état de la menace de l'ANSSI 2022, CERTFR-2023-CTI-001.pdf (ssi.gouv.fr)
[8] Etude IPSOS pour cisco, Etude Cisco : Le risque cyber est perçu comme faible voire inexistant pour un quart des entreprises françaises - Cisco News The EMEA Network
[9] Voir annexes « Lettre de mission »
[10] Voir annexes « Liste des personnes et entités entendues »
[11] Voir annexes « Synthèse des réponses au questionnaire »
[12] Voir annexes « Cartographie (non exhaustive) des dispositifs »
[13] Voir annexes « Synthèse des questionnaires des services économiques des ambassades »

<Recommandations>

Rendre plus lisible les premières étapes clés pour amorcer puis renforcer la sécurisation des PME.

1

LA PROBLÉMATIQUE

Bien qu'une multitude de diagnostics existe, leur réalisation est insuffisamment suivie par la mise en place de mesures par les PME. Cela est dû à leur complexité et technicité, souvent inadaptées au niveau de maturité des entreprises qui les réalisent.

LA SOLUTION

Nous proposons de rendre plus lisibles les dispositifs de diagnostics. Il existe un consensus sur, d'une part le besoin d'harmoniser les travaux de diagnostics et, d'autre part, le nécessaire accompagnement des entreprises dans le passage à l'action une fois le diagnostic réalisé.

<Pour les PME les moins matures, étendre l'expérimentation MonAideCyber portée par l'ANSSI>

En cours en Nouvelle-Aquitaine, d'autres régions pourraient tester ce dispositif comme l'Ile-de-France via l'EDIH CYBIAH, la Bretagne ou encore les Haut-de-France via le Campus Cyber Territorial. L'initiative doit être généralisée au niveau national.

MON AIDE CYBER

La startup d'Etat de l'ANSSI « MonAideCyber » expérimente un dispositif avant son déploiement fin 2023.

Il s'agit d'un diagnostic cyber (une quarantaine de questions) rapide destiné aux entités publiques et privées faiblement matures dites « sensibilisées au cyber mais souhaitant structurer leur action ».

Ce diagnostic est réalisé par des « aidants cyber » de confiance, sélectionnés, formés et accompagnés par l'ANSSI (gendarmerie, police, douanes, associations sectorielles) et bientôt via le réseau des Campus Cyber en région.

Il propose en sortie 6 recommandations priorisées à réaliser en 6 mois avec un accompagnement possible durant ces 6 mois afin que ces actions soient bien mises en œuvre.

<Pour les PME plus matures, la DGE et l'ANSSI doivent publier un référentiel adapté. L'accompagnement doit être réalisé par des acteurs privés, à l'exception faite des dispositifs financés par l'Etat>

Utilisée pour estimer la maturité cyber de plus de 900 collectivités territoriales, les « parcours » de l'ANSSI est une méthode pouvant être déclinée pour les PME. Ce référentiel doit devenir un commun accessible à tous les acteurs publics et privés, y compris à des fins commerciales.

LES « PARCOURS DE L'ANSSI »

A destination des collectivités territoriales, ce parcours permet de définir le niveau de maturité et les actions à mettre en place rapidement.

Condition préalable : avoir une structure informatique et une personne en charge de sa sécurisation.

Processus développé en plusieurs étapes : audit, modules de sensibilisation des responsables, définition d'un plan d'action et des moyens humains associés. Ce processus permet de responsabiliser les équipes tout en étant directif dans la mise en place des actions de sécurisation des systèmes d'information.

<Recommandations>

Créer une place de marché nationale de prévention au risque cyber pour les PME.

2

Centraliser les outils et services adaptés à la taille, localisation et secteur d'activité de la PME.

LA PROBLÉMATIQUE

Bien que les PME aient de plus en plus conscience du risque cyber, elles ne savent pas vers qui s'orienter pour leurs démarches de sécurisation. En parallèle, les acteurs de l'écosystème qui proposent des dispositifs de sécurisation ont des difficultés à adresser le vaste marché que représentent les PME.

LA SOLUTION

Nous proposons **la mise en place d'une place de marché centralisée nationale** recensant des offres packagées pour permettre l'orientation des PME vers les outils adaptés en fonction de leur taille, niveau de maturité, localisation et secteur d'activité. De par son rôle de lieu totem de l'écosystème, le Campus Cyber est le bon acteur pour porter cette plateforme.

<Points clefs à mettre en avant>

</> **Diagnostics et dispositifs de scoring, y compris financiers, pour aider les dirigeants à prendre conscience du risque.**

</> **Offres proposées par des acteurs publics et privés** (Sélections et labellisation des solutions selon des critères transparents ainsi qu'un processus de test par des acteurs de l'écosystème).

</> **Services disponibles en termes de sensibilisation et de réaction, notamment cybermalveillance.gouv.fr**

</> **Formation en ligne (MOOC) à destination des salariés et dirigeants.**

</> **Dispositifs d'obtention d'un label ou d'un badge, pouvant par exemple faciliter la souscription à une assurance cyber, visant à inciter les PME à se sécuriser.** (Ce concept d'attribution de badge existe dans le dispositif Boost Aerospace. Il est une recommandation du rapport de l'Institut Montaigne Cybersécurité, passons à l'échelle. Cela permettrait d'aider les structures à préciser leur objectif en termes de cybersécurité. Une telle initiative aurait beaucoup de sens si elle était réalisée au niveau européen).

</> **Dispositifs d'entrainement à la gestion d'une crise cyber majeure en impliquant des PME au niveau des régions, via le réseau associatif local**

Pour réaliser cette plateforme, nous recommandons une approche UX design (expérience utilisateur) visant à simplifier son usage pour le grand public. Cette plateforme serait à coconstruire avec les PME pour définir la boite à outils nécessaire à leur sécurisation.

<Recommandations>

Créer une campagne de prévention cyber et un kit de sensibilisation clé en main.

3

Sensibiliser et prévenir largement les 4 millions de PME

LA PROBLÉMATIQUE

Bien que les PME aient de plus en plus conscience du risque cyber, il est nécessaire de poursuivre et d'intensifier collectivement les actions afin que l'ensemble des PME françaises passent à l'action.

LA SOLUTION

Nous proposons d'utiliser deux canaux de communication de prédilection pour atteindre le plus grand nombre :

<Sensibiliser largement les PME en organisant une campagne de prévention cyber 360° sur le modèle des spots TV dédiés à la prévention routière>

Cette campagne serait coconstruite entre ACYMA et Campus Cyber. Elle redirigerait les PME vers la plateforme cybermalveillance.gouv.fr, guichet unique de lutte contre les cyber malveillances, ainsi que le projet de future plateforme «17 cyber», portée par le ministère de l'Intérieur. Elle redirigerait également vers la place de marché nationale de prévention. Sa diffusion sur les réseaux sociaux utilisés par les chefs d'entreprise, comme LinkedIn, augmenterait son impact.

<S'appuyer sur les interlocuteurs de proximité et de confiance des PME, dits « connecteurs », afin de rapidement passer à l'échelle>

La production d'un kit de communication partagé et actualisé permettrait la diffusion d'un discours harmonisé et compréhensible vers les PME par ces acteurs clefs afin de renforcer la sensibilisation et prévention. L'objectif serait notamment de rediriger vers la place de marché.

Exemples de « connecteurs » : banques, assurances, La Poste, opérateurs de télécommunications, experts comptables, Campus Cyber Territorial, les CSIRT, Experts Cyber, communauté des aidants de MonAideCyber, associations professionnelles, associations locales, intégrateurs locaux, grands groupes pour les chaines d'approvisionnement, conseillers numériques, forces de l'ordre (dont la formation doit être renforcée).

Le réseau des Campus Cyber territoriaux aura un rôle particulier dans l'activation des connecteurs.