Sécurité des systèmes d'information :

Une nécessité impérieuse

La sécurité des réseaux, des appareils , des programmes et des données constitue une préoccupation majeure particulièrement des gouvernements et des entreprises compte tenu des importants risques qui pèsent sur la modification, le vol et l'endommagement de l'infrastructure informatique ainsi que des préjudices financiers qui peuvent en résulter pour les différents utilisateurs

Selon le site onelogin le cybercrime a couté au monde 6 000 milliards de dollars en 1921, ce qui correspond à près de 6% du PIB. Il risquera de couter 10 500 milliards de dollars en 2025

C'est pourquoi les initiatives se multiplient en Tunisie et dans le monde pour adapter les instruments juridiques, les règlements et les normes aux exigences de la sécurité de l'infrastructure et des données numériques.

C'est pourquoi aussi de nombreuses études sont élaborées par les instituts et les bureaux spécialisés pour présenter des recommandations afin d'affiner les stratégies en matière de cybersécurité et réduire les vulnérabilités des systèmes informatique à l'instar du rapport élaboré en juin 2023 par l'Institut Montaigne dont un résumé est publié ci-après en tant qu'article de référence du Forum Ibn Khaldoun pour le Développement pour le mois d'octobre 2023.

Cybersécurité

Passons à l'échelle

Institut Montaigne (juin 2023)

« Le numérique irriguant désormais tous nos usages, la sécurité doit devenir, dans le milieu professionnel notamment, un réflexe naturel, comme le port de la ceinture de sécurité dans les voitures ou la fermeture de la porte d'entrée de sa maison.

Si la cybersécurité est souvent considérée comme une problématique purement technique, celle-ci recouvre en réalité une multitude d'enjeux cruciaux tels que la compétence des professionnels de la sécurité, les enjeux budgétaires, sociaux, humains et organisationnels**. L'intensification de la cybercriminalité et le développement de directives de cybersécurité appellent une prise de conscience rapide et massive des acteurs diffus du territoire,** petites et moyennes entreprises, établissements de santé et collectivités, diversement engagés jusqu'à présent dans leur protection face aux menaces cyber. **Il s'agit là d'un enjeu majeur de résilience économique et sociale, la moitié des PME attaquées faisant faillite après une cyberattaque.**

Ainsi**, il apparaît nécessaire de créer les conditions d'un passage à l'échelle pour protéger plus**

exhaustivement le territoire. À partir d'une analyse collégiale et de terrain, conduite en partenariat avec La Gendarmerie nationale, le METI et le groupe La Poste, le présent rapport formule 10 recommandations afin d'actionner les leviers pour accélérer ce changement d'échelle dans une logique incrémentale, pragmatique et facilement implémentable.

Une intensification de la menace cyber qui se resserre autour des entités les moins préparées

Sensibles au contexte mondial dans lequel elles évoluaient, les grandes entreprises à portée internationale ont été les premières à prendre des mesures pour se prémunir contre les cyberattaques. Aussi, les politiques régaliennes de sécurisation cyber se sont-elles essentiellement concentrées sur ces grands acteurs économiques et sur les entités critiques, laissant les plus petites structures - TPE/PME/ETI, collectivités et établissements de santé - très largement démunies et exposées aux dangers.

L'élargissement de la surface d'attaque devient un facteur de déstabilisation économique et sociale potentiellement grave, qu'il s'agisse de bloquer l'activité d'une entreprise, d'un établissement de santé ou d'une collectivité, mettant en péril leurs capacités opérationnelles, leur santé financière voire leur survie. Ainsi, en France, la somme des TPE/PME/ETI, collectivités locales et établissements publics de santé représente 73 % des attaques par rançongiciels en 2022 (ANSSI). Le coût, à lui seul, des attaques par rançongiciel subis pour les PME de moins de 50 employés est estimé à plus de 720 M€ par an. De même, au moins 1/10 collectivités a déjà été victime d'un rançongiciel, selon les données de la Gendarmerie nationale.

Les entretiens menés pour cette étude révèlent tout à la fois une prise de conscience de la menace cyber de la majorité des acteurs et une forte volonté de passer à l'action, mais aussi un manque de moyens et d'accompagnement pour franchir le pas.

Quels sont Les cinq obstacles à la cybersécurité des TPE, PME, ETI et collectivités locales ?

1

Un manque de sensibilisation : Selon une étude d'IPSOS, les deux tiers des salariés français n'ont jamais reçu la moindre formation en cybersécurité

2

La surface d'attaque est plus grande : Les offres les plus sécurisées sont souvent les plus chères. Les petites structures font souvent le choix d'investir à moindre cout.

3

Les montants investis dans la cybersécurité n'ont pas été à la hauteur des besoins. La part du budget numérique dédiée à la cybersécurité est souvent faible.

4

Un manque de compétence disponibles dans un marché tendu. les métiers de la cybersécurité sont les plus tendus des métiers du numérique.

5

Un foisonnement des solutions techniques qui désoriente les non-initiés. Faute de moyens les dirigeants des structures abandonnent le sujet.

Une dynamique européenne qui encourage à un passage à l'échelle en France

Le second élément invitant à une action rapide est l'application française de la directive européenne NIS 2 d'ici à septembre 2024, dont les nouvelles orientations visent à entamer la diffusion de la cybersécurité dans l'ensemble de la chaîne numérique, précisément dans cette logique de sécurisation des maillons faibles. Une amende proportionnelle au chiffre d'affaires sera exigée en cas de non-conformité. Surtout, ce respect de la directive sera une condition d'insertion des petits dans les chaînes de décision ou de valeur des plus grands.

Pour mobiliser à tous les niveaux et protéger plus exhaustivement le territoire, il apparaît nécessaire d'encourager l'adoption de mesures spécifiques et adaptées s'adressant à l'ensemble des acteurs, en particulier pour les acteurs les moins matures sur ce thème - TPE/PME/ETI, petites collectivités locales et hôpitaux, de manière à asseoir l'émergence d'un véritable "passage à l'échelle" de la cybersécurité en France.

10 actions concrètes pour un rehaussement collectif du niveau de cybersécurité sur le territoire

Les conditions clés pour un passage à l'échelle effectif et réussi reposent essentiellement sur l'articulation des efforts des différents acteurs nationaux et locaux en temps réel et la mobilisation rapide des moyens identifiés.

Dans cette démarche, le rapport propose une approche incrémentale qui s'appuie sur une méthode simple et rapidement opérationnelle fondée sur les solutions et acteurs existants. En complément des nombreux ateliers, les études de terrain, menées auprès d'entreprises nationales et locales, de collectivités territoriales et d'un Centre Régional de Réponse à Incidents (CSIRT), ont permis de tester la validité des recommandations.

Le coût annuel global de cet effort de l'État pour favoriser le passage à l'échelle des petites entreprises et collectivités représenterait une centaine de millions d'euros par an, englobant tant les moyens humains nécessaires que les subventions en faveur d'offres mutualisées et des structures qui les portent.

Axe 1 - Mobiliser les acteurs locaux en faveur d'un parcours de cybersécurité simple et progressif à même de les protéger et de les préparer aux crises : diagnostic, ambition, précautions, exercices et organisation

1

Inciter à recourir à des diagnostics organisationnels et techniques en proposant un référentiel commun comprenant différentes profondeurs de diagnostic

2

Fixer une cible de cybersécurité à atteindre pour les structures, en fonction de leur criticité et de leurs moyens, et les inciter à progresser dans la durée en proposant un système de badges les aidant à prioriser leurs arbitrages

3

Limiter nativement la présence de vulnérabilités et de failles dans les produits et équipements numériques disponibles sur le marché européen en exploitant tout le potentiel du règlement européen Cyber Resilience Act, et informer les utilisateurs en temps réel en cas de trafic Internet suspect grâce à une “cyber vigie” opérée par les opérateurs de télécommunications

4

Exhorter les entreprises et collectivités à considérer le risque cyber comme une préoccupation stratégique encadrant les choix humains, organisationnels, budgétaires et techniques de leur activité

5

Organiser une simulation annuelle d'alerte cyber (équivalent de “l’alerte incendie”) pour tous les salariés ou agents d'une entreprise ou d’une collectivité, afin de les acculturer à la menace et aux bonnes pratiques numériques

6

Instaurer une fonction de conseiller à la sécurité numérique (CSN) auprès de chaque responsable de structure (dirigeant d’entreprise ou élu) pour accompagner celui-ci sur les questions de cybersécurité

Axe 2 - Coordonner les ressources, les outils et les prérogatives de chaque acteur aux échelles appropriées : nouveaux moyens nationaux et mutualisations locales

7

Mutualiser les compétences et les outils chez les acteurs de confiance publics et privés en charge de la cybersécurité afin de permettre une couverture complète du maillage territorial

8

Faciliter le signalement des attaques cyber via une “Plateforme de Signalement des faits Cyber”, base de données commune aux différents services publics compétents en matière de cybersécurité, permettant un suivi consolidé

9

Renforcer les moyens et l'organisation des acteurs de la lutte contre la cybercriminalité dans une logique de proximité, en mettant l'accent sur la prévention et sur la répression

10

Pérenniser le financement de l'effort public en faveur d'une sécurité numérique collective par un abondement vertueux des budgets »

Forum Ibn Khaldoun pour le Développement : 5 octobre 2023