LES PME ET ETI FACE AU CYBERMENACES

Stratégie CyberFactory

infoclip

SOMMAIRE

Stratégie CyberScore

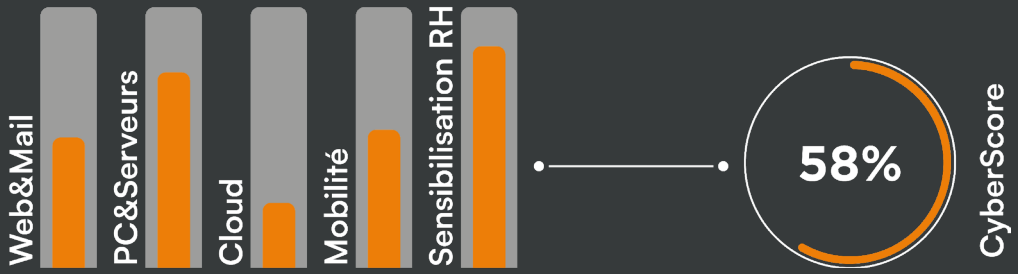
PRÉAMBULE
Qu'est-ce que votre score CyberScore ?

Une évaluation technique, organisationnelle et méthodologie de vos vulnérabilités face au risque Cyber. Votre niveau de CyberScore se matérialise par l'obtention d'un score par vecteur d'attaque puis est consolidé sous forme d'un score global.

Votre CyberScore est consultable sur notre portail dans votre Dashboard mensuel CyberFactory. Vous pouvez le partager avec vos services et/ou partenaires.

Il s'accompagne d'un plan progrès permettant de diminuer votre surface d'attaque en fonction de vos enjeux et priorités. Vous pouvez ainsi suivre visuellement vos progrès et garder le cap !

Votre score CyberScore et notre processus d'amélioration continue vous rendent éligible à la CyberAssurance pour couvrir le risque résiduel Cyber.



Pourquoi votre score de CyberScore est-il important ?

Pour mesurer la solidité et l'attractivité de votre compagnie, les ratios habituels, financiers, R&D, investissements doivent être complétés par votre score de CyberScore pour être pertinent.

Vos partenaires, vos clients et vos collaborateurs vous confient leurs données. La confiance qu'ils placent en vous est cruciale pour le développement de votre business.

Alors que se passe-t-il après une cyber attaque occasionnant une fuite de données, un arrêt de vos services ou une usurpation d'identité ?

La confiance fonde le commerce, nous vous proposons une méthode éprouvée et reconnue d'évaluation de votre résistance cyber. Ce processus d'évaluation se matérialise par l'obtention de votre score CyberScore.

Scoring et amélioration continue

En complément de l'obtention de votre score CyberScore qui permet de vous situer dans votre industrie et de définir vos axes d'amélioration.

Nous vous accompagnons sur le chemin de l'amélioration de votre excellence Cyber avec notre offre CyberFactory.

INTRODUCTION

Les PME et ETI ne sont plus à l'abri des attaques informatiques

La cybercriminalité est une des plus grandes menaces qui pèsent sur les entreprises. Les attaques sur l'informatique (*malware*), les violations de données, le phishing, les attaques de rançongiciel (*ransomware*) ou le cyber-espionnage leur font perdre des milliards chaque année, et représentent un danger pour leur survie.

Les PME et ETI se sont longtemps crues à l'abri des attaques informatiques.

Elles ne sont aujourd'hui qu'une cible parmi tant d'autres - les grandes entreprises, les administrations, les services de santé, les particuliers, etc.

Le résultat des attaques est multiple :
perte ou vol de données, interruption des services, destruction d'infrastructure, versement d'une rançon, perte de confiance des clients, perte de revenus...

La PME est seule face à l'attaque, avec une chance de survie réduite.

1 RISQUES Que craignent les responsables sécurité des entreprises ?

50 %
une compromission de comptes cloud (Cloud Account Compromise), principalement Microsoft Office 365 ou Google G suite

42 %
les attaques par compromission des emails professionnels

41 %
les menaces internes

37 %
les attaques sur la chaîne logistique

31 %
les rançongiciels ou ransomware

Le coût des cyberattaques

Le coût des cyberattaques ne cesse de s'élever, au rythme de la sophistication des attaques et de l'évolution de leurs modèles chance de survie réduite.

En France, en cas d'attaque par ransomware :

25% des entreprises optent pour le paiement d'une rançon

130 000 € : la rançon moyenne versée

39,44 % des données sont récupéres en moyenne par les entreprises

913 000 € : impact financier moyen

L'environnement réglementaire

La lutte contre le cybercrime est difficile, l'origine des attaques est dispersée, les droits nationaux s'opposent, et les auteurs sont parfois protégés par des États.

C'est pourquoi les législateurs cherchent plutôt à sensibiliser les entreprises, avec éventuellement des sanctions, afin qu'elles s'emparent du sujet.

A l'exemple du RGPD, le Règlement général de la protection des données, qui est "*relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*".
Le RGPD s'applique à toute organisation qui traite des données personnelles, établie sur le territoire de l'Union européenne, ou dont l'activité cible directement des résidents européens… ainsi que leurs sous-traitants.

L'application du RGPD dans les PME et ETI est à prendre en considération comme un acte de cybersécurité.

La responsabilité

La cybersécurité n'est pas seulement une affaire de technologie, c'est un engagement et une responsabilité.

En cas de cyberattaque, **c'est au dirigeant de démontrer que sa responsabilité n'est pas engagée.**

Il doit prouver qu'il a utilisé tous les moyens nécessaires pour limiter les risques : stratégie de protection, sécurité du système d'information, formation des collaborateurs, et bon fonctionnement de l'ensemble.

> **LORSQU'UN INCIDENT INTERVIENT DANS UNE ENTREPRISE, C'EST LE DIRIGEANT QUI PEUT ÊTRE DÉCLARÉ RESPONSABLE.**

La cybersécurité au service du business de l'entreprise

La sécurité est généralement considérée comme une charge, et non comme un investissement…
Mais en cas d'attaque, le prix à payer est considérable.

La cybersécurité est une composante incontournable au service du business.
L'entreprise doit concevoir, fabriquer et commercialiser des produits et des services 'secure by design', et sensibiliser ses collaborateurs afin qu'ils ne se prêtent pas aux cyberattaques.

L'entreprise doit limiter sa surface d'attaque et se tenir prête à affronter les cybermenaces et à réagir aux attaques éventuelles, défendre et assurer le maintien de ses activités.
Mais les investissements dans la protection des systèmes et des données ne sont pas à la hauteur des menaces.

En se protégeant, et protégeant ses partenaires, l'entreprise assure la pérennité et renforce la confiance qui la lie à son écosystème.

Connaissance du risque

Trop souvent les dirigeants de PME déclarent que leur petite entreprise n'intéresse pas les pirates. Et qu'en cas d'attaque, il sera toujours temps de réagir.

Si le risque cyber demeure flou, il est devenu un risque majeur. Mais PME et ETI restent vulnérables.
La transformation numérique et la pandémie de COVID-19 ont entraîné une intensification de certains schémas d'attaque, dont le ransomware et les erreurs humaines.
Mais les investissements dans la protection des systèmes et des données ne sont pas à la hauteur des menaces.

> L'ANSSI PRÔNE QUE 5 À 10 % DU BUDGET INFORMATIQUE DEVRAIT ÊTRE CONSACRÉ À LA CYBERSÉCURITÉ.

L'effet démultiplicateur du cloud

+ de 9 entreprises sur 10 déplacent leurs données non structurées vers le cloud.
3/4 des entreprises rencontrent des difficultés pour protéger leurs données non structurées.
4 entreprises sur 10 ne savent pas où elles sont stockées !

La multiplication des points d'entrée vers les données de l'entreprise s'accompagne de pratiques déviantes, comme le shadow IT (usage d'applications tierces non validées par l'entreprise.

90 % des entreprises s'appuieront sur des applications SaaS pour atteindre leurs objectifs.
Il y a **3 à 4 fois plus** plus d'applications SaaS utilisées dans une entreprise que le département informatique ne le sait.

Le périmètre de défense

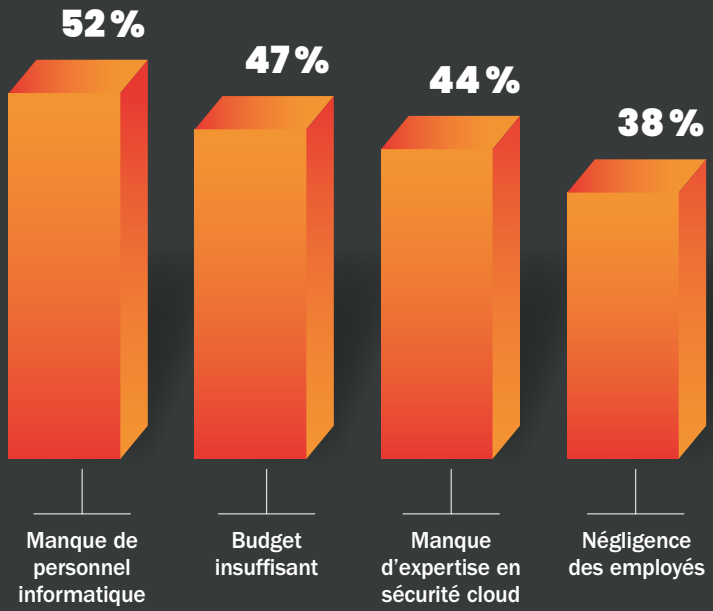
Le périmètre de sécurité de l'entreprise s'étend largement au-delà des serveurs et des postes de travail, avec le télétravail, le cloud, l'IoT et le shadow IT qui sont des sources de risques.

Les secteurs de l'industrie et de la logistique (Supply Chain) affichent aujourd'hui **des vulnérabilités critiques** et étendent la surface d'attaque.

Les attaques de logiciels malveillants sur les appareils IoT (en hausse de 144%) **et les mobiles** (en hausse de 41%) **ont explosé en Europe.**
Source Check Point Research

La sécurité des données dans le cloud

L'exemple de la sécurité des données dans le cloud est assez significatif des obstacles qu'accumulent les entreprises dans leur démarche de cybersécurité, exacerbés par la volonté des entreprises de se digitaliser rapidement.



2 | STRATÉGIE DE CYBERDÉFENSE POUR LES PME

Les PME n'ont pas suffisamment de défenses en place pour protéger, détecter ou réagir aux attaques. Elles manquent de ressources, d'expertise, de compréhension, d'information, de temps, et d'entraînement.

Elles se concentrent naturellement sur le fait d'être opérationnelles au jour le jour, afin de pouvoir servir les clients pour maintenir l'activité et payer le personnel.

Et trop souvent, elles n'ont pas l'adhésion des dirigeants pour répondre à leurs besoins en matière de sécurité.

Quant aux défis liés au cloud, à la mobilité, au télétravail, aux filiales, à l'ouverture de leur écosystème, à l'explosion du périmètre traditionnel de sécurité, ils deviennent de plus en plus complexes.

Les PME représentent une cyber-cible facile et lucrative.

Tester et renforcer la résistance et la résilience

La PME doit comprendre ce qu'elle peut faire et ne pas faire pour mettre en œuvre une stratégie de cyber-résilience.

Elle va tester sa résistance, mesurer son engagement, et montrer comment certaines menaces se répercutent sur les objectifs de l'entreprise.
Les menaces internes représentant la grande majorité des cyberattaques, la PME doit s'attaquer à la racine du problème : le comportement humain.

Pour inspirer le changement et engager la sensibilisation, elle doit réfléchir globalement, identifier les points faibles et traiter l'impact potentiel qu'elle pourrait subir si ces derniers étaient ciblés.

Alerter, conseiller et former

Les menaces ne viennent pas toujours de l'extérieur. Bien que l'on constate parfois des menaces provenant d'employés malhonnêtes et mécontents, la très grande majorité des menaces provient de l'intérieur, de collaborateurs non avertis.

Les collaborateurs doivent accéder à des formations régulières, pour se familiariser avec la politique sécurité de l'entreprise, se tenir informés des risques et des nouveaux types d'attaques, renforcer leur vigilance et leur réactivité, et s'assurer qu'ils sachent ce qu'on attend d'eux.

90 %
des menaces proviennent de collaborateurs non avertis.

Par la sensibilisation et la formation, on évitera la distraction que cherche le pirate.

Protéger le business

La majorité des dirigeants de PME n'ont pas d'expérience en cybersécurité.

La barre du prix ne doit pas les écarter des stratégies et solutions retenues par les grandes entreprises, avec le même niveau de protection.

La solution choisie invitera à l'usage des bonnes pratiques, d'outils d'inventaire, de contrôle des identités, de surveillance des équipements, de gestion des configurations et des mises à jour, de ségrégation du réseau, de sauvegarde des données, et des approches Zéro Trust jusqu'aux postes de travail.

> **LA QUESTION N'EST PAS DE SAVOIR SI L'ON VA ÊTRE ATTAQUÉ MAIS QUAND... ET COMMENT MAINTENIR LE BUSINESS ?**

La sauvegarde

Une stratégie de cybersécurité ne peut plus se contenter de chercher à bloquer les attaques et à fermer les portes. Elle doit pallier au vol et la destruction de données, et à la mise en danger des clients et des personnes.

- En cryptant les données pour les rendre illisibles.
- En assurant la sauvegarde des données.

Avec l'évolution des attaques, en particulier la menace des rançongiciels, la sauvegarde est plus que jamais l'un des piliers incontournables de la sécurité des données de l'entreprise.

Sa mise en application est simple et peut être automatisée. Le cloud peut apporter des réponses qui transforment la mécanique opérationnelle en un service simple à déployer et à exploiter.

La continuité d'activité

L'entreprise doit également disposer de capacités de récupération des données.

A la suite d'une cyberattaque, l'entreprise doit pouvoir soit relancer son activité à partir du jeu de sauvegarde, c'est à dire réinstaller les données sur une base saine, avec un minimum de perte ; soit continuer son activité sur une base de données ou un SI dupliqué de manière transparente pour l'utilisateur.

Le déploiement d'une sauvegarde et d'outils de reprise d'activité impose une forte implication des dirigeants, à la fois dans la sensibilisation des équipes et dans l'évaluation des capacités de récupération des données.

La cyberAssurance

Une fois appliquée la stratégie de sécurité, une nouvelle analyse des risques s'impose pour décrire les mesures d'amélioration continue de la sécurité et identifier les risques cyber résiduels.

Ces risques sont réels et permanents, aucun système de cybersécurité n'est infaillible.

La cyberAssurance transfère le risque cyber résiduel vers un produit d'assurance cyber dédié.

Un contrat de cyber-assurance s'articule autour de quatre piliers :

1. **La prévention des risques** avec la sensibilisation, le cyber diagnostic, les alertes ;
2. **La gestion de la crise** avec assistance, remédiation, et appui d'experts ;
3. **La prise en compte des dommages** subis par l'entreprise, comme les pertes d'exploitation, les frais d'assistance informatique, les pertes pécuniaires subies ;
4. **Les frais juridiques et financiers** issus des réclamations des tiers pour atteinte à la vie privée et défaillance de la sécurité du SI.

Devenir éligible à la cyberAssurance

L'objectif de la cyber-assurance est de couvrir le risque résiduel, celui qui n'est pas couvert par la stratégie de cybersécurité déployée par l'entreprise.

L'éligibilité demande un travail préparatoire, qui participe à une meilleure maîtrise des risques numériques, et permet de répondre aux pré-requis des compagnies d'assurance.
L'entreprise se voit affecter un scoring qui repose sur sa stratégie de cybersécurité. Plus il est élevé, plus l'accès est facilité, et plus l'offre peut être meilleure.

PME et ETI se feront accompagner de partenaires dans la compréhension et la prévention des risques numériques, dans le choix et le déploiement de solutions de sécurité, dans la sensibilisation et la formation des collaborateurs, dans l'analyse des risques, dans le calcul du scoring, et dans le choix des contrats.

Le choix du partenaire

La cybersécurité est un défi majeur à relever par les PME et ETI. Et les dirigeants n'ont pas une perception réaliste d'un risque qui reste flou. C'est une mission quasi impossible à relever en interne.

Aucune solution n'est parfaite, et les stratégies de défense reposent généralement sur un millefeuille d'applications et de services qui devient très vite ingérable, sauf à disposer de ressources et de compétences.

Les PME doivent être accompagnées pour mieux appréhender la cybersécurité, et passer de l'abstraction au concret.

Elles doivent mesurer les risques et les impacts des menaces cyber sur leur métier, leur activité, leurs collaborateurs, et sur leurs dirigeants.

3 | LA DÉMARCHE Infoclip CyberRésistance

La cybersécurité des PME et ETI est devenue un enjeu majeur. Infoclip, spécialiste de l'informatique des PME, a pris l'engagement d'y répondre en proposant une stratégie adaptée à ses clients :

Notre démarche consiste à accompagner nos clients, apporter les compétences, proposer des solutions personnalisées, évaluer et analyser des risques jusqu'à la cyber-assurance, également en cas d'attaque, et à un tarif adapté.

InfoclipRésistance propose les services de :

CyberScore

- Mesure de votre maturité Cyber
- Etude et analyse de vos vulnérabilités
- Evaluation de votre exposition technique
- Pondération métier
- Elaboration de votre score CyberRésistance

Sécurisation Globale

- Recommandations
- Protection
- Solutions techniques
- Sensibilisation utilisateurs
- Processus de gestion de crise

SOC PME

- Détection
- Identification
- Correctifs au fil de l'eau
- Etat des services de production

Cellule de crise

- Communication interne et externe
- Gestion 24h/24 de l'évènement
- Suivi des parties prenantes
- Relance des systèmes

Continuité Business

- Remédiation
- Restauration des données et systèmes
- Reprise des activités
- Retour à la normale
- Capitalisation

CyberAssurance

- Accompagnement à l'obtention d'une Cyber Assurance
- Sélection du fournisseur idoine
- Questionnaire Cyber
- Suivi dans le temps des contraintes liées au contrat

CONCLUSION

Les cyberattaques sont une menace qui perturbe gravement le fonctionnement des entreprises, avec des conséquences qui peuvent aller jusqu'à la cessation définitive d'activité.

La question, pour les PME et ETI, n'est plus de savoir si elles seront attaquées, mais quand, et surtout comment elles pourront y répondre.

Le cyber-partenaire de la PME joue un rôle essentiel.
Elle y trouve les ressources et les compétences qui lui manquent pour construire une stratégie, des outils et un modèle de cyber-défense adaptés à ses besoins et à sa taille. Ainsi qu'un accompagnement, tant dans la construction que dans la validation de ses objectifs, et dans l'accès à des services qui deviennent incontournables, comme la gestion de crise, le plan de continuité d'activité ou la cyberAssurance.

Infoclip CyberRésistance réunit les 5 piliers qui permettent aux PME et ETI d'accéder aux mêmes niveaux de compétence, défense et de sortie de crise que les grandes entreprises - Évaluation, Sécurisation, SOC, Gestion de crise, Continuité d'activité - mais à l'échelle d'un partenaire qui depuis 30 ans oeuvre pour les PME, et qui adapte les stratégies de cybersécurité à leurs modèles et pratiques.

Avec Infoclip CyberRésistance, les PME et ETI peuvent enfin affronter les risques cyber sur un pied d'égalité avec les grandes entreprises, mais à leur échelle, et avec l'agilité et les ressources des PME.

4 | ANNEXE
Comprendre comment les cyberattaques fonctionnent

En France, le premier semestre 2022 a été l'occasion de franchir un triste record, 1 million de Français ont été touchés par une violation de leurs données personnelles.

Les attaquants savent s'adapter à l'entreprise qu'ils ciblent.

Ils étudient leurs futures victimes et dans le cas des PME les soumettent à des rançons en bitcoin (monnaie virtuelle), qui représentent plusieurs milliers d'euros.

Le coût de résolution des infections par logiciels malveillants est aussi à prendre en compte.

Pour résoudre une attaque de malware, une grande entreprise américaine devra payer en moyenne 807 506 dollars en 2021. Les PME sont particulièrement désarmées pour faire face à cette dépense, qui va peser sur leur capacité de survie.

Plus l'entreprise est préparée, plus ces coûts seront réduits.

Si les attaques sont considérées comme inévitables, dans les entreprises qui sont préparées ces sommes peuvent être divisées par deux, voire plus, et les charges annexes peuvent être sensiblement réduites.

Déroulement et conséquences d'une cyberattaque

Le cybercrime est devenu une industrie, la troisième économie du monde, ses attaquants sont riches et organisés, et parfois ils sont sponsorisés par les Etats.

L'univers du hacking est une grande communauté, avec sa face cachée, le Dark Web.
Sur le côté sombre de l'Internet, il est possible d'acheter des listes de diffusion pour le spam, des informations personnelles - comme des identités, adresses mail, numéros de carte bancaire -, ou encore des malwares prêts à l'emploi, vendus avec le support, voire de faire appel à des plateformes de services de hacking !

Les vulnérabilités sont très recherchées. Ce sont des failles dans les systèmes dont l'exploitation permet de pénétrer un système d'information (SI). pour certaines *'zero day'*, qui n'ont pas encore été dévoilées et ne sont donc pas corrigées.

La majorité des attaques consistent à frapper à la porte de l'entreprise en invitant les collaborateurs à l'ouvrir. Le spam est l'outil le plus répandu pour transporter ces attaques.

Les pirates pratiquent l'ingénierie sociale, qui cible les attaques et adapte les messages pour leur donner une apparence de légitimité, et tromper l'humain qui demeure le maillon faible.

Avec le cloud, le télétravail ou encore l'Internet des Objets (IoT), les couches applicatives se sont démultipliées et dispersées, ce qui ne fait que complexifier la tâche des défenseurs.

Une fois la porte ouverte, le malware s'installe dans le SI. Les pirates peuvent agir impunément sur de longues périodes, dérober des informations comme les transactions financières, les identités, des données commerciales ou des fichiers relevant de la propriété industrielle, ou lancer un rançongiciel.

Le périmètre de sécurité de l'entreprise s'étend largement au-delà des serveurs et des postes de travail, avec le télétravail, le cloud, l'IoT et le shadow IT qui sont des sources de risques.

Les secteurs de l'industrie et de la logistique (Supply Chain) affichent aujourd'hui **des vulnérabilités critiques** et étendent la surface d'attaque.

Le rançongiciel est aujourd'hui considéré comme l'une des principales menaces.

L'effet démultiplicateur du cloud

52 % des vols sont dus à des actes malveillants.

33 % des pertes de données ont une origine accidentelle, erreur de manipulation ou de configuration.

L'ANSSI (Agence nationale de sécurité des systèmes d'information) a noté une hausse de **92 %** des interventions suite à rançongiciels.

777

En Europe en 2022, la moyenne hebdomadaire des attaques est de 777 par organisation en augmentation de 36 %

Source Check Point Research

Sensibilisation

La sensibilisation est une démarche essentielle pour surmonter les difficultés liées à la cybersécurité.

Il faut travailler sur le maillon considéré comme le plus faible, l'humain, pour former les collaborateurs à des pratiques reconnues qui réduisent sensiblement le danger lié aux cyberattaques.

Également sensibiliser le dirigeant au risque encouru et à la nécessité d'augmenter les budgets consacrés à la cybersécurité.

La vigilance doit être constante, et la formation continue. Le collaborateur doit être en mesure d'identifier les informations sensibles ou confidentielles, de mesurer les risques, et d'appliquer les bonnes pratiques.

infoclip

CyberFactory.

Sécurisez à 100% la continuité de votre business

Cyber Résistance

Scoring et plan d'amélioration pour la sécurité des données des identités, des accès et des SI

Cyber Cloud

Cloud sécurisé par design, souverain, hautement disponible et Green IT pour vos applications et vos données

Cyber MCO

Maintien en Conditions Opérationnelles des SI répondant aux règles strictes de sécurité et de qualité conformes aux normes ISO

Cyber Excellence

Le lab.
Se préparer aux évolutions.
Répondre rapidement aux nouvelles modalités d'attaque

Le Campus.
Former et maintenir un haut de niveau de compétences Cyber pour vos collaborateurs et vos experts Sécurité

infoclip

Expérimentés, collaboratifs et éco-responsables,
nous sommes l'ESN partenaire des PME et de ETI
depuis 30 ans.

20 rue de la Michodière - 75002 Paris
+33 (0)1 43 18 19 20

contact@infoclip.fr
www.groupe-infoclip.com