kaspersky

Cybermenaces, habitudes numériques et investissements : **quelle maturité cyber pour les entreprises marocaines ?**

Comment les petites et moyennes entreprises du Maroc envisagent-elles la cybersécurité ? Se sentent-elles exposées aux risques ? Quels conseils peut-on apporter aux entreprises pour une meilleure résilience en matière de cybersécurité ?

kaspersky

TABLE DES MATIÈRES

Mot d'accueil

PASCAL NAUDIN,
Head of B2B Sales, Afrique du Nord, de l'Ouest et Afrique Centrale.

La question de la cybersécurité **est indissociable de la question de la transformation numérique.** À ce titre, les entreprises devraient en saisir à la fois le sens, mais aussi les tenants et aboutissants. Alors que l'un des plus grands salons internationaux dédiés à la technologie a lancé sa première édition Afrique cette année, le GITEX Africa, on est sûrs d'une chose : l'Afrique est un territoire présentant d'énormes enjeux, et de grandes opportunités sur le plan du numérique, et par effet de bord, de la cybersécurité.

Le Maroc et la Tunisie sont des viviers de talents en matière d'informatique et de technologies. Toutefois, les entreprises dans ces deux pays tendent à sous-estimer, tout comme dans une grande partie du monde, le risque cyber en pensant qu'elles ne sont pas personnellement exposées, ou que l'investissement n'en vaut pas la chandelle. Si le business plan est un élément essentiel dans le développement d'une stratégie commerciale, la cybersécurité l'est tout autant dans le développement d'une stratégie numérique. En 2023, il va sans dire que la digitalisation n'est plus un projet lointain, mais une réalité pour la majorité des entreprises.

Depuis presque 20 ans, Kaspersky exerce dans la région. Par conséquent, nous échangeons régulièrement avec des entreprises et des administrations sur notre thème de prédilection, la cybersécurité, en complément de la cyber-immunité, et ce afin qu'elles développent une stratégie cyber. L'environnement virtuel dans lequel nous gravitons rend complexe cette question de cyber. Les entreprises n'en maitrisent pas toujours le sens. Elles n'identifient pas non plus la réalité de leurs besoins ou de leur exposition. Bien souvent, la conscience d'un phénomène n'aboutit d'ailleurs pas sur une prise d'initiative éclairée. Il est difficile de faire la part des choses entre les tendances et les besoins réels individuels.

Nous, les éditeurs, sommes en partie responsables de cette confusion. Pendant longtemps, nous avons été précurseurs sur plusieurs technologies, en décalage vis-à-vis de la maturité numérique de nombreuses entreprises. À cet égard, nous n'avons pas toujours su adresser les bons enjeux, ou communiquer de manière appropriée. **Être précurseur sur le plan technologique est un atout puisque cela nous permet d'être toujours plus performants que les cybercriminels.** Pour autant,il est indispensable que nos clients puissent s'approprier ces technologies, ce que nous nous efforçons de faire dans le cadre notamment de nos événements KNext.

Alors que les petites et moyennes entreprises représentent l agrande majorité du tissu économique local et international, les médias et les experts se focalisent avant tout sur les risques auxquels sont exposées les grandes administrations, les industries et les multinationales. Comment se positionnent les PME dans cet écosystème ? **Devraient-elles se préoccuper davantage de la réalité du paysage des menaces pour mettre en œuvre des stratégies de cybersécurité adaptées à leurs besoins, età leur exposition ?** À ce propos, existe-t-il des technologies et des services à disposition des entreprises de petite et moyenne taille ? Est-il possible d'investir dans une stratégie de cybersécurité sans dépenser des centaines de milliers de dirhams ?

Chez Kaspersky, nous avons à cœur de protéger les entreprises de toutes les tailles contre les menaces cyber. Pour cela, il est d'abord important de faire comprendre à chacune d'entre elles son champ d'exposition aux menaces, de leur faire prendre conscience des risques qui se cachent derrière des cyberattaques et de démystifier un certain nombre d'idées reçues. Non, la cybersécurité n'est pas réservée aux grandes entreprises, non, ce n'est pas trop compliqué. Il ne s'agit pas non plus d'une contrainte au développement économique. La cybersécurité ne peut pas reposer entièrement sur des solutions automatisées à 100% ne nécessitant plus l'intervention humaine. Elle a pour vocation d'être intégrée directement à la politique de digitalisation et de développement économique.

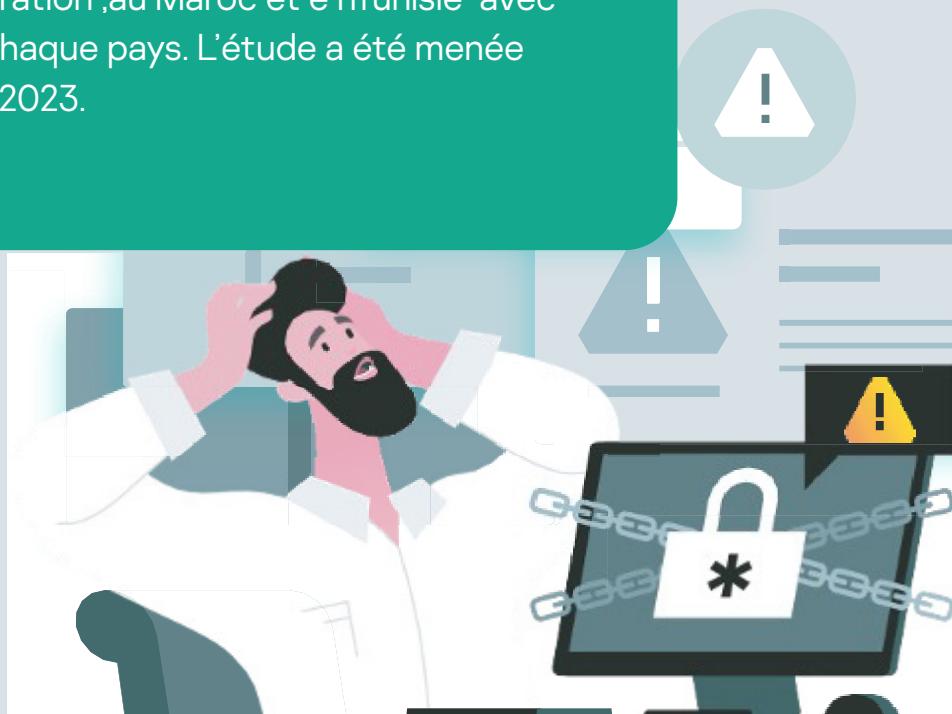
Pour l'ensemble des raisons évoquées ci-dessus, nous avons décidé de faire appel à un cabinet d'étude, Arlington Research, afin de tenter d'étayer notre constat : la conscience de la cybersécurité existe mais la maturité cyber en tant que tel est encore fragile. Tous les pays disposent de leurs spécificités, en témoignent les différences fondamentales entre les répondants marocains et tunisiens. Prendre

des décisions éclairées et adaptées à la réalité du besoin des entreprises n'est pas chose aisée. Avec le concours de notre écosystème de partenaires, nous avons la volonté d'accompagner les entreprises et de les faire monter en compétences progressivement pour qu'enfin, elles puissent **reprendre le pouvoir sur leur cybersécurité et avoir une longueur d'avance sur la cybercriminalité.**

Méthodologie

Les données relatives aux menaces touchant les petites et moyennes entreprises ont été remontées grâce au Kaspersky Security Network, le Cloud de réputation de l'entreprise Kaspersky, qui a observé, avec le consentement des entreprises participant à ce cloud, les différentes menaces ciblant des entreprises de moins de 1000 salariés, sur toute l'année 2022, puis sur la première partie de l'année 2023. Ainsi, les données relatives aux menaces ciblant les entreprises marocaines et tunisiennes correspondent aux dates suivantes : du 1er janvier au 30 juin 2023.

Les données relatives au marché, marocain et tunisien ont été récoltées et analysées par le cabinet d'étude Arlington Research, mandaté par Kaspersky. 600 décideurs IT et business d'entreprises allant de 10 à 250 salariés, basés au Maroc (300) et en Tunisie (300) ont été interrogés afin de mieux comprendre leur perception de la cybersécurité, leur niveau de connaissance mais aussi les actions déployées dans leur entreprise pour lutter contre les cybermenaces. Arlington Research a mené cette étude en ligne, par un principe d'autoadministration ,au Maroc et e nTunisie avec 300 répondants dans chaque pays. L'étude a été menée entre le 7 et le 24 juillet 2023.



Les entreprises demeurent une proie lucrative pour les cybercriminels

D'après les données des Nations Unies, les petites et moyennes entreprises (PME) représentent 90 % des entreprises dans le monde et contribuent à 50%duproduitintérieur brut mondial. Il devient donc impératif de renforcer les mesures de cybersé- curité pour protéger ces leviers économiques.

Le dernier rapport de Kaspersky sur les menaces pesant sur les PME fait état d'une réalité persistante et inquiétante : les cybercriminels continuent de cibler les PME en recourant à toutes sortes de méthodes sophistiquées. Le rapport révèle que le nombre d'employés de PME rencontrant des logiciels malveillants ou indésirables déguisés en applications professionnelles légitimes est resté relativement stable d'une année sur l'autre, et que les cybercriminels persistent dans leurs efforts pour infiltrer ces entreprises.

Quelle situation à travers le monde ?

Les fraudeurs emploient une multitudedeméthodes,notamment l'exploitation des vulnérabilités, l'utilisationd'e-mailsdephishing, de SMS trompeurs, voire même de liens YouTube d'apparence inoffensifs, le tout dans le but d'obtenir un accès non autorisé à des données sensibles. Cette tendance préoccupante souligne le besoin urgent de renforcer les mesures de cybersécuritépourprotégerlesPME contre les attaques incessantes des cybermenaces. Le rapport révèle que le nombre total de détection ces fichiers malveillants visant les PME au cours des cinq premiers mois de 2023 a atteint 764 015 à travers le monde.

L'exploitation de vulnérabilités a constitué la menace la plus répanduepourles PME à travers le monde, représentan t63% de toutes les détections au cours des cinq premiers mois de 2023. Ces programmes malveillants ciblent les vulnérabilités logicielles, permettant aux cybercriminels d'exécuter des logiciels malveillants, d'accroître leurs privilèges ou d'entraver le fonctionnement d'applications critiquessansqu'aucuneinteraction avec l'utilisateur ne soit nécessaire.

Les menaces de phishing et d'escroquerie représentent également un risque important pour les PME, les cybercriminels sachant habilement tromper les employés pour qu'ils divulguent des informations confidentielles ou qu'ils soient victimes d'escroqueries financières. Parmi ces tactiques trompeuses, on trouve les fausses pages de services bancaires, de livraison et de crédit conçues pour tromper les personnes peu méfiantes.

En outre, le rapport de Kaspersky attire l'attention sur une méthode fréquemment utilisée pour infiltrer les smartphones des employés, appelée «smishing» - une combinaison rusée de SMS et d'hameçonnage. Cette technique consiste à envoyer à la victime un message texte contenant un lien, distribué par le biais de diverses plateformes telles qu'un SMS, WhatsApp, Facebook Messenger, WeChat, etc. Si l'utilisateur peu méfiant clique sur le lien intégré, son appareil devient vulnérable au téléchargement de code malveillant, ce qui compromet sa sécurité.

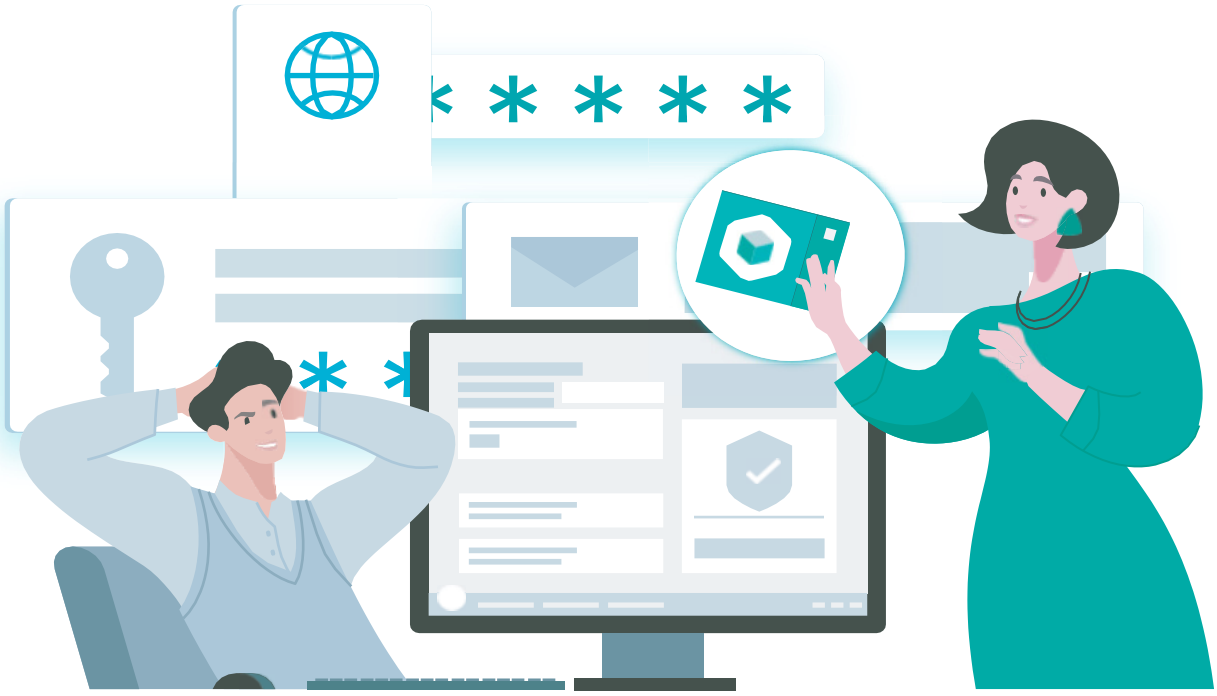
Les données rapportées ont été collectées de janvier à mai 2023 via le Kaspersky Security Network (KSN), un système sécurisé de traitement des données anonymisées relatives aux cybermenaces volontairement partagées par les utilisateurs de Kaspersky.

Les experts de Kaspersky ont passé au crible les logiciels les plus utilisés par les PME du monde entier, notamment MS Office, MS Teams et Skype. En croisant ces logiciels avec les données télémétriques de KSN, les chercheurs ont déterminé l'étendue des logiciels malveillants et indésirables distribués sous le couvert de ces applications.

«Les vulnérabilités auxquelles ont sujettes les PME exigent une attention soutenue. Ces entreprises constituent le socle de l'économie dans la plupart des pays, il est donc essentiel que les gouvernements et les organisations redoublent d'efforts pour les protéger. La sensibilisation et l'investissement dans des solutions de cybersécurité robustes doivent devenir une priorité absolue pour protéger les PME de l'évolution des cybermenaces», commente Pascal Naudin, Head of B2B Sales pour Kaspersky Afrique du Nord, de l'Ouest et Afrique Centrale.

Et quelle situation au Maroc et en Tunisie selon les radars Kaspersky ?

Si l'on s'intéresse de plus près aux chiffres relatifs aux pays qui nous intéressent aujourd'hui, à savoir le Maroc et laTunisie, les chiffres sont assez évocateurs d'une croissancedeladigitalisationdes PME, d'une part, mais également de l'attractivité de ces entreprises pour les cybercriminels. La tendance



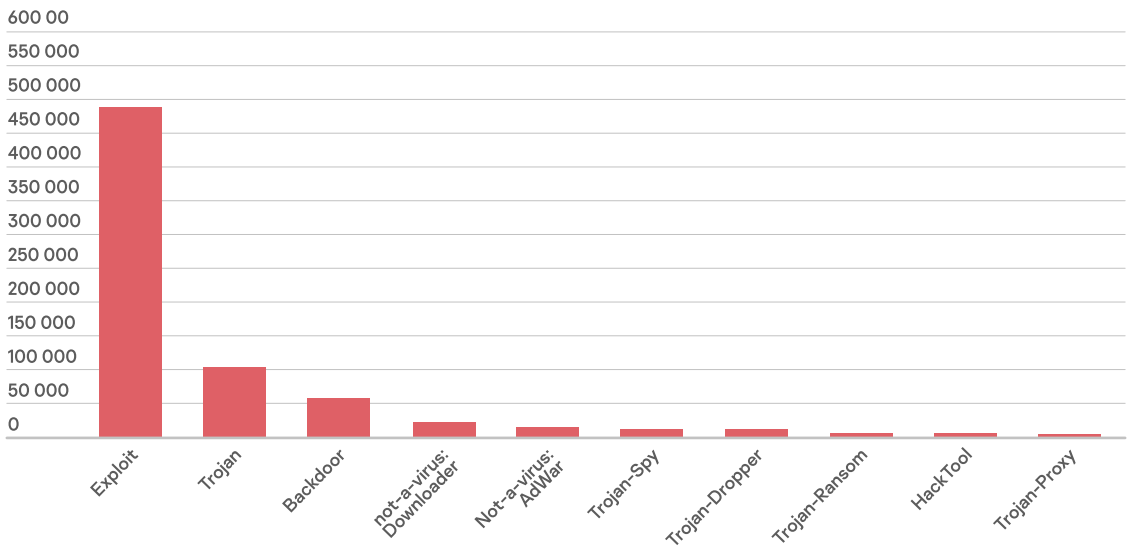
est malheureusement à la hausse entre le premier semestre 2022 et le premier semestre 2023 sur les 2 pays, et à la fois en nombre d'attaques détectées, en nombre d'employés ciblés directement, et en nombre de fichiers malveillants uniques identifiés par les outils Kaspersky.

En effet, au Maroc, sur le premier semestre 2023 (1er janvier – 30 juin), 324 types de fichiers malveillants ciblant les PME ont été détectés par les outils Kaspersky. Ces derniers ont ciblé 430 employés uniques, et ont été détectés, et bloqués, 4176 fois, ce qui signifie que chaque fichier malveillant a été propagéde nombreuses fois. Il est intéressant de noter, non sans inquiétude, une forte croissance de la menace sur lemoisdejuin 2023. En effet, sur ce simple mois, 84 fichiers malveillants unique sont été détectés, ciblant 158 utilisateurs uniques, et repérés1771 fois en tout à travers le Royaume. En comparaison, en 2022 sur la période janvier-juin, 165 fichiers malveillants ciblant les PME marocaines avaient été détectés. Ces fichiers avaient été rencontrés par 90 employés uniques, et détectés à plus de 2 212 reprises sur la même période.

« Les chiffres permettent de donner une indication de la diversité des menaces qui peuvent cibler les entreprises, mais également de la multiplication de la diffusion d'un type de fichier . Compte tenu des chiffres, il est vraisemblable que chaque employé ayant été ciblé par un fichier malveillant ait en fait été exposé à plusieurs types de menaces durant l'année – d'où l'importance de la sensibilisation et d'une politique de cybersécurité robuste. Être attaqué une fois ne donne pas l'immunité, bien au contraire face auxautres types d'attaques. Il ne faut en revanche – malheureusement – pas prendre ces chiffres pour argent comptant puisque Kaspersky n'a de la visibilité que sur une base de données correspondant à ses propres utilisateurs. Non seulement nous ne sommes pas les seuls sur le marché, mais en plus, tous les utilisateurs de l'entreprise n'acceptent pas de partager des données anonymisées pour aider la recherche. Si l'on ajoute à cela toutes les entreprises n'étant pas protégées du tout, on peut vite se rendre compte de l'étendue probable du problème de cybersécurité à travers le monde, y compris au Maroc et en Tunisie. » **explique Pascal Naudin, Head of B2B Sales de Kaspersky au Maroc et en Tunisie.**

Compte tenu de ces analyses et de ces constats, nous avons souhaité comparer les faits, avec la perception de la menace des entreprises marocaines et tunisiennes, ainsique de leur équipement et des volontés d'investissement dans la cybersécurité. Ce, afin de mettre en perspective les niveaux de maturité des entreprises en matière de cybersécurité, de pouvoir prodiguer des conseils en phase avec la réalité des besoins tout en continuant à accompagner les entreprises vers une meilleure résilience cyber et ainsi, de poursuivre notre objectif de construction d'un monde numérique plus sûr.

Top 10 des types de menaces rencontrées par les PME – à travers le monde – au premier semestre 2023



Quelques conseils pour protéger votre entreprise contre les cybermenaces :

1. Mettez en place une formation de base pour sensibiliser votre personnel aux bonnes pratiques en matière de cybersécurité. Organisez une simulation d'attaque par hameçonnage pour vous assurer qu'ils savent reconnaître les e-mails dephishing.

2. Optez pour une solution de protection avec des fonctionnalités anti-phishing pour les terminaux et les serveurs de messagerie, comme Kaspersky Endpoint Security for Business ou Cloud-Based Endpoint Security, afin de minimiser les risques d'infection par phishing.

3. Si vous utilisez le service cloud Microsoft 365, n'oubliez pas de le protéger également. Kaspersky Security for Microsoft Office 365 dispose d'un anti-spam et d'un anti-phishing dédiés, ainsi que d'une protection pour les applications SharePoint, Teams et OneDrive afin de sécuriser les communications professionnelles.

4. Mettez en place une politique d'accès aux ressources de l'entreprise, notamment aux boîtes mail, aux dossiers partagés et aux documents en ligne. Tenez-la à jour et supprimez l'accès si un employé n'en a plus besoin pour faire son travail ou lorsqu'il quitte l'entreprise. Utilisez un logiciel de gestion de la sécurité de l'accès aux services en nuage qui peut vous aider à gérer et à surveiller l'activité des employés dans les services cloud et à mettre en œuvre des politiques de sécurité.

5. Effectuez des sauvegardes régulières des données essentielles pour garantir la sécurité des informations de l'entreprise en cas d'urgence.

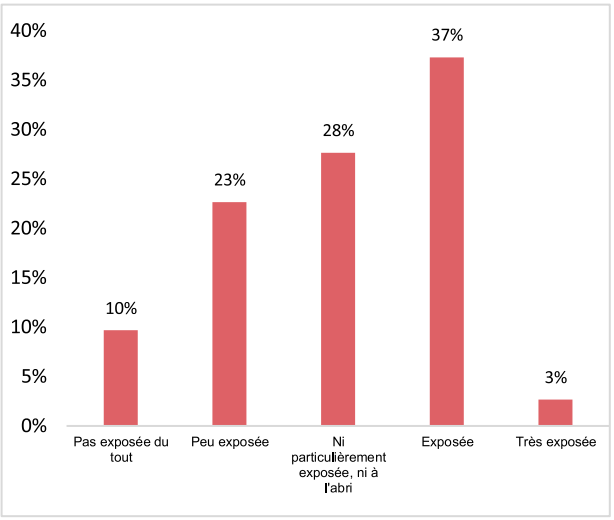
6. Faitesappelàdesservicesprofessionnelspouroptimiserl'efficacitéde vos ressources en matière de cybersécurité. Les nouveaux packs de services professionnels Kaspersky pour les PME permettent de s'appuyer sur les experts de Kaspersky pour l'évaluation, le déploiement et la configuration : il suffit d'ajouter les packs au contrat, et les experts font le reste.

Chapitre 2

État de la maturité des PME au Maroc

Quelle perception de l'exposition aux risques ?

Les entreprises marocaines sont assez lucides quant aux risques de dommages qu'une potentielle cyberattaque pourrait causer à leur entreprise. Un équilibre est par ailleurs constaté face à la perception du risque cyber : 40% des entreprises répondantes s'estiment personnellement exposées au risque cyber et 33% ne s'estiment absolument pas concernées. D'autre part, lorsqu'on leur pose la question des conséquences d'un potentiel incident de cybersécurité, une forte proportion d'entre elles perçoivent les risques de pertes de clients (42%), de pertes d'argent (40%), ou de pertes de données sensibles (44%), comme probables. Deux entreprises sur 5 (42%) estiment probable le risque d'espionnage de la part de pirates, ou d'acteurs tiers et à peu près le même nombre considère possible qu'un ransomware ne bloque les accès aux données et cause une baisse d'activité ponctuelle. De même, 42% des répondants estiment qu'une cyberattaque peut causer des dommages physiques. Enfin, la perte de réputation, ou le départ des salariés inquiète respectivement 38% et 39% des entreprises répondantes.

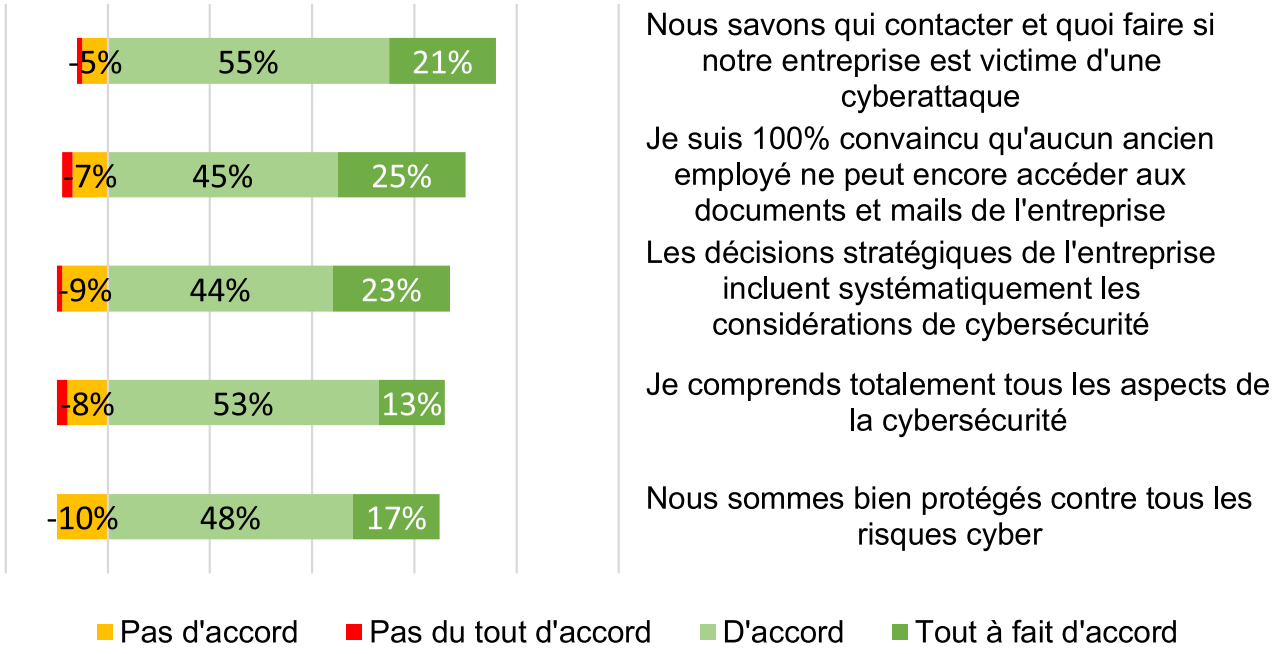


Selon vous, à quel point votre entreprise est-elle exposée aux cyberattaques et failles de données ?

Pourtant, l'actualité médiatique concernant des entreprises se retrouvant prises dans des tourmentes financières, voire même légales pour cause de fuite de données et de non-respect des normes de traitement et stockage des données à travers la planète ne cesse d'être plus prégnante. Les événements récents liés aux ransomwares et aux attaques visant les chaines d'approvisionnement sont en constante évolution sur la scène internationale. Des centaines d'entreprises ont été touchées, rappelant des incidents notables tels que l'attaque Sunburst contre l'entreprise SolarWinds, la propagation mondiale de WannaCry et des attaques spécifiquement ciblées contre des entreprises en particulier. Cette situation malheureuse démontre la persistance et la variété des menaces cybernétiques qui continuent d'affecter le monde entier.

Des chiffres qui font sens au Maroc puisque 65% des entreprises estiment être bien protégées face aux cybermenaces. 66% des répondants estiment également comprendre tous les aspects de la cybersécurité. 72% répondent aussi que toutes les décisions stratégiques de l'entreprise sont prises en fonction des considérations de cybersécurité. D'un point de vue pratique, lorsqu'on pose la question aux décideurs marocains afin de savoir s'ils sont certains que les anciens employés de l'entreprise n'ont plus accès aux anciens fichiers de l'entreprise, 70% répondent que oui. 76% des entreprises sont également certaines de savoir qui contacter en cas de cyberattaque.

Dans quelle mesure êtes-vous en accord ou en désaccord avec les points suivants ?



Le Maroc est un pays où les PME sont plutôt sensibilisées,et semblentmatures enmatièrede cybersécurité.

Toutefois, la prudence est de mise car **Pascal Naudin, Head of B2B Sales sur la région est d'avis que** « les entreprises pêchent par excès de confiance. Un nombre conséquent d'entre elles sont convaincues que le simple fait de mettre un firewall ou un antivirus les protège de

toutes les menaces. En tout état de cause, les entreprises marocaines ont conscience de la nécessité de se protéger. Cependant, à l'instar de multiples pays, le problème se situe au niveau de l'exploitation des informations et des données remontées par les solutions technologiques. Cette dernière ne peut souvent être faite correctement, faute de temps, ou de compétences ».

Alors quelles sont les habitudes et pratiques adoptées au sein des entreprises qui rendent si confiants lesdécideursinformatiquesainsique les directions générales au Maroc ? 39 % des répondants à notre étude affirment avoir une politique de mots de passe forte corrélée à des stratégies de sauvegardes fréquentes. Si ce chiffre est

prometteur, parce que l'approche est en effet importante, on est en droitdesequestionner:qu'enest-il des 61% qui répondent ne pas avoir cettepolitique?La suite est en adéquation avec ce constat. 37% des répondants indiquent utiliser des solutions de sécurité grand public, c'est-à-dire qu'elles ne peuvent pas être opérées et gérées directement par l'entreprise. Afin de saisir pleinement cet enjeu : une solution de sécurité grand public dispose des mêmes fondations de sécurité que les solutions dédiées en entreprise. En revanche, elles laissent l'utilisateur du poste directement administrer la sécurité sur son poste. Il n'est donc pas possible pour l'entreprise d'avoir une politique de sécurité robuste car les mises à jour et l'installation des patchs de vulnérabilité reposent uniquement sur le bon vouloir du salarié. En règle générale, les recommandations de Kaspersky portent sur l'utilisation de solutions dédiées aux entreprises – peu importe leurs tailles – puisque qu'il existe des solutions à l'échelle, et adaptées à tous types de besoins, de ressources et de compétences. Une des réponses aux questions est, dans ce contexte, d'autant plus préoccupante puisque seuls 20% des répondants indiquent disposer d'une solution de sécurité entreprise, permettant au responsable informatique de gérer l'intégralité des mises à jour et patchs de sécurité.

Parmi les autres réponses inquiétantes en matière de protectionfaceauxcybermenaces, on peut noter : 21% des répondants soulignent avoir une parfaite compréhension de leur écosystème informatique et sont capables

de cartographier leur réseau, 10% prônent l'anticipation et investissent dans la threat intelligence et enfin, 15% d'entre eux n'ont pas de stratégie de cybersécurité, parce qu'ils ne se sentent pas exposés.

D'ailleurs, ces chiffres illustrent des dynamiques contradictoires en ce qui concerne les raisons pour lesquelles les dirigeants n'investissent pas plus en cybersécurité : si seuls 27% des répondants estiment qu'ils n'ont jamais été victimes de cyberattaques, 41% justifient leur manque d'investissement parce qu'ils ne sont pas exposés.

Lesquelles de ces propositions définissent le mieux votre stratégie de cybersécurité, votre perception de la cybersécurité pour votre entreprise ? (Plusieurs réponses possibles).

Pascal Naudin explique : « On constate un vrai décalage entre la conscience du risque cyber et l'action prise pour pallier les éventuels risques. Les entreprises savent que la cybersécurité est un sujet important, mais elles peinent à prendre des décisions éclairées. Le besoin de sensibilisation est encore grand. »

Il ajoute « de plus, même quand certains souhaitent déployer des politiques de sécurité, on se retrouve aujourd'hui confrontés à plusieurs problèmes. Tant que les décideurs verront la sécurité informatique comme un coût non essentiel, il sera toujours question de réduire ce coût, quitte à opter pour des solutions non adaptées, telles que les solutions grand public par exemple. En fonction de la taille des entreprises, il peut se présenter des situations dans lesquelles le DSI occupe également le poste de RSSI, ce qui ne permet pas d'avoir un contre-pouvoir qui impose une stratégie de cybersécurité à l'entreprise. Enfin, le manque de compétences, qui permet d'opérer les différents outils et d'en maximiser l'exploitation est un problème à l'échelle internationale, et donc également au Maroc.»

La cybersécurité, au cœur des décisions stratégiques de l'entreprise.

Dans le cadre d'un déploiement d'une stratégie de cybersécurité, l'approche trop segmentée au niveau des prises de décision représente l'un des freins régulièrement identifiés par Kaspersky. Dans le monde connecté d'aujourd'hui, la cybersécurité doit être prise en considération dans les décisions stratégiques et liées au développement de l'entreprise, mais également intégrée dans le plan de croissance. Il semble que les entreprises marocaines aient intégrées cet état de fait, puisque 8 répondants sur 10 indiquent que les enjeux cyber sont abordés durant les comités de direction, au moins de temps en temps.13% des entreprises attestent aborder la question

de la cybersécurité de manière systématique, et 35% indiquent l'aborder au moins une fois sur deux. D'ailleurs, 66% des répondants indiquent aussi toujours intégrer des considérations de cybersécurité dans leurs décisions stratégiques.

Un tiers des répondants avouent toutefois rarement placer ces sujets au cœur des agendas des comités de direction.

Un autre facteur déterminant du poids accordé à la cybersécurité dans la prise de décision au niveau le plus stratégique de l'entreprise est celui de la personne est en charge de ces questions. Si 65% indiquent qu'il s'agit du département informatique, peu ont fait la différence entre le responsable informatique, et le responsable de la sécurité des systèmes d'information, ce qui ne permet donc pas de contrebalancer l'aspect purement technique de la sécurité avec la gouvernance nécessaire pour une approche résiliente. En effet, la simple technologie ne permet pas de répondre à tous les enjeux de sécurité qui doivent également être accompagnés d'analyse, de formation, de communication, de gestion de risque… et de gouvernance en somme. La question de gouvernance semble primordiale, à l'ère où les modèles de travail ne cessent de se digitaliser et le travail à distance se démocratise un peu partout à travers le monde. Il convient de noter qu'il s'agit d'un sujetépineux,puisquelaquestionde la gestion de son parc informatique à distance est centrale dans une approche résiliente en matière de cybersécurité. Alors que seuls 21% des répondants à notre étude sont certains d'avoir une vision exhaustive de leur cartographie du réseau, les politiques en matière de travail à distance sont encore assez bancales et laxistes. En effet, 36% des répondants affirment avoir une politique stricte en termes de travail à distance. Or, 31% uniquement affirment que leurs employés utilisent des appareils séparés pour leurs usages personnels et professionnels. Ces usages non différenciés constituent des portes d'entrée extrêmement faciles pour les cybercriminels qui peuvent accéder au réseau de l'entreprise par le biais de l'appareil personnel d'un employé, connecté via son wifi personnel. Danscescirconstances,nil'outil,ni le réseau, ne sont protégés selon les normes del'entreprise.

Les attaques par chaine d'approvisionnement, un vrai problème, trop peu souvent considéré.

Les propriétaires de petites entreprises peuvent penser qu'ils sont à l'abri des cyberattaques car les cybercriminels s'intéressent davantage aux très grandes entreprises. C'est d'ailleurs le cas des entreprises interrogées dans

ce rapport : 32% des entreprises marocaines de moins de 300 salariés ne se sentent pas exposées aux cyberattaques. Cependant, il est important de considérer deux points supplémentaires. Premièrement, les grandes entreprises consacrent une grande part de leur budget

à leur défense et sont donc plus difficiles à attaquer. Deuxièmement, une autre option peut être plus attrayante : une attaque à travers la chaine d'approvisionnement. Les malfaiteurs peuvent atteindre des centaines de petites entreprises en ne compromettant qu'une entreprise.

Généralement,êtreattaquéàtravers une chaine d'approvisionnement signifie qu'un service ou un programme que vous utilisez

depuis un certain temps est devenu malveillant. Quelques exemples relativement récents,

et médiatisés, permettent de mieux comprendre ce dont il s'agit, notamment le cas d'ExPetr. En se concentrant sur les conséquences destructrices d'ExPetr (aussi connu sous le nom de NotPetya), peu se souviennent véritablement comment cela a commencé.

C'est bien dommage : l'un de ses vecteurs de distribution définit pratiquement ce qu'est l'« attaque delachained'approvisionnement».

Les cybercriminels ont compromis le système de mise à jour automatique du logiciel de comptabilité appelé M.E.Doc en l'obligeant à distribuer

le ransomware à tous ses clients. En conséquence, ExPetr a causé des millions de pertes, infectant à la fois les grandes et les petites entreprises.

Un autre exemple est celui de CCleaner : CCleaner est l'un des programmes les plus connus pour le nettoyage du registre du système.

Il est largement utilisé par les particuliers et les administrateurs système. Inévitablement, les cybercriminels ont mis en péril l'environnement de compilation

du développeur du programme, équipant plusieurs versions d'une porte dérobée. Pendant un mois, ces versions compromises ont été distribuées à partir des sites officiels de l'entreprise. CCleaner a été téléchargé 2,27 millions de fois.

Dans cette étude, nous avons posé la question aux répondants concernant leurclientèle,et11%desentreprises de taille moyenne marocaine ont répondu avoir, parmi leurs clients, de très grandes entreprises ou des gouvernements. Il s'agit d'autant de raisons pour un attaquant de chercher à compromettre leurs systèmes.

Dans une attaque de la chaine d'approvisionnement, les cybercriminels n'ont pas à vous choisir comme cible. Dans une certaine mesure, vous vous exposez vous-même, en utilisant simplement un service ou un programme particulier .

Tous les appareils professionnels disposant d'un accès Internet doivent être protégés. Cela comprend les ordinateurs, les serveurs, les téléphones portables, etc. Même si vous êtes sûr de ne pas

installer de programmes inconnus sur un ordinateur , cela ne garantit pas que les logiciels malveillants ne se présenteront pas à vous comme une mise à jour de logiciels anciensetfamiliers.Enparticulier,les ordinateurs devraient être protégés par des technologies capables de contrer les mineurs malveillants et les ransomwares. Ces deux méthodes d'attaque sont les plus faciles

à monétiser ; les cybercriminels persistent donc à les utiliser .

Pascal Naudin explique : « Un nombre considérable d'entreprises estiment avoir été victimes de cyberattaques. La réalité est conforme sur le terrain vis-à-vis de la détection des attaques. Au cours de nos rendez-vous clients à travers l'Afrique – le Maroc et la Tunisie compris –, nous sommes amenés à établir des POC (Proof of Concept) auprès d'entreprises pour des solutions XDR (solutions capables d'analyser et de détecter des menaces dites avancées non détectables avec une solution type EPP). Il arrive parfois que l'outil détecte, moins d'une heure après son installation et son paramétrage, des alertes inquiétantes qui n'étaient jusqu'alors pas visibles chez le client, et ce malgré les solutions déjà déployées.»

Comment Kaspersky Endpoint Security Cloud protège votre entreprise.

Une seule attaque ciblant une entreprise qui ne s'est pas préparée à affronter de tels risques peut entraîner :

- la perte de données sensibles, y compris de propriété intellectuelle ;
- la fuite d'informations confidentielles relatives aux clients et aux collaborateurs ;
- un impact négatif sur la productivité des collaborateurs qui se répercute directement sur la rentabilité.

Contrairement aux grandes sociétés, les TPE/PME ne disposent généralement pas d'équipes informatiques internes importantes. Elles ont besoin d'une solution de sécurité facile à installer et à mettre en œuvre, voire d'externaliser sa gestion à distance.

La solution Kaspersky Endpoint Security Cloud couvre les besoins spécifiques de ces entreprises en les aidant à protéger l'ensemble de leurs terminaux Windows et Mac, de leurs serveurs de fichiers Windows et de leurs appareils mobiles Android et iOS. La protection leader du marché qu'elle offre est rapide à déployer, à mettre en œuvre et à exécuter sans qu'il soit nécessaire d'acheter du matériel supplémentaire. En outre, tous les paramètres de sécurité peuvent être gérés à distance, depuis tout appareil doté d'une connexion Internet.

Atouts principaux de cette solution pour les PME :

- Toutes les fonctionnalités de sécurité sur l'ensemble des ordinateurs de bureau et ordinateurs portables Windows ou Mac, des serveurs de fichiers Windows, sans oublier des appareils mobiles Android et iOS, peuvent être configurées et gérées via une console d'administration centralisée. Vous n'avez pas besoin de compétences particulières en matière de sécurité informatique pour utiliser la console et gérer votre sécurité. Par ailleurs, les politiques de sécurité que vous appliquez sur tous vos terminaux sont faciles à définir.
- La console basée dans le Cloud et prête à l'emploi permet aux administrateurs d'utiliser quasiment n'importe quel appareil doté d'une connexion à Internet pour configurer et régler l'ensemble des fonctionnalités de protection, pour tous les terminaux. Si vous choisissez d'externaliser la gestion de votre sécurité informatique, la console permettra également à vos consultants externes de la gérer à distance, en toute simplicité. Étant basée dans le Cloud, vous n'aurez pas besoin d'investir dans du matériel supplémentaire ou d'en assurer la maintenance et bénéficierez d'une configuration initiale extrêmement rapide.

Kaspersky EDR Optimum : garder une longueur d'avance sur les menaces grâce à une solution complète qui ne drainera pas vos ressources.

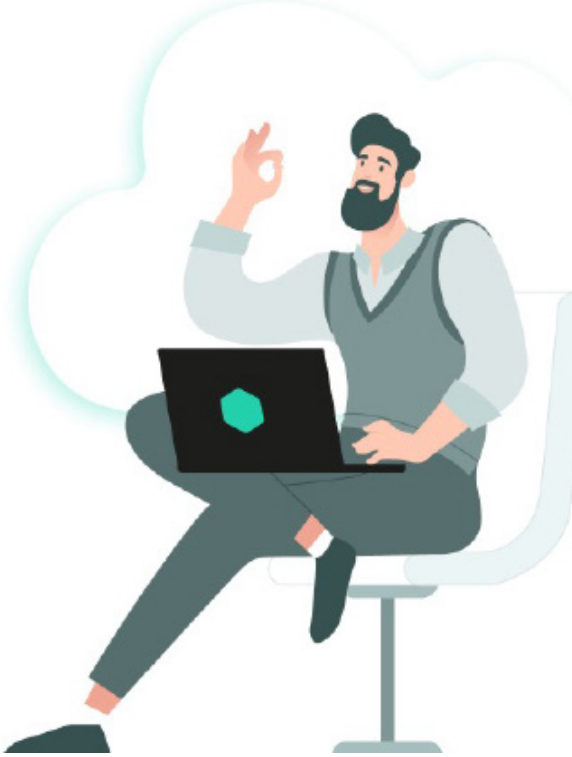
Kaspersky EDR Optimum a été développé afin de répondre au besoin d'une solution de sécurité de qualité, capable de faire face aux menaces actuelles complexes malgré les ressources limitées. Il est conçu pour détecter les menaces de manière robuste, y répondre de façon proactive, et simplifier les opérations quotidiennes. Ce type

de solution permet aux entreprises qui ne disposent pas d'équipes dédiées à la gestion d'un EDR de disposer des meilleures technologies même si elles n'ont pas les moyens d'avoir un SOC. Kaspersky Optimum Security offre une solution efficace de détection et de réponse aux menaces,soutenueparunesurveillancedelasécurité24h/24,7j/7,des réponses automatisées et une recherche des menaces, ainsi que par le soutien et les conseils des experts de Kaspersky.

Les méthodes de prévention automatique constituent le fondement de toute protection des terminaux, mais elles doivent être complétées par des outils avancés si vous vous retrouvez à devoir gérer les menaces évasives les plus dangereuses. Kaspersky Optimum Security offre

des capacités avancées de détection basée sur le Machine Learning

et de réponse rapide, le tout fourni depuis le loud. Votre équipe peut désormais traiter avec rapidité et précision les menaces qui auparavant l'empêchaient de dormir la nuit. Kaspersky Optimum Security vous permet de réduire les risques liés à la perte d'argent, de clients et de réputation, et renforce vos défenses contre les nouvelles menaces inconnues et évasives.



Chapitre 3

La formation & la sensibilisation à la cybersécurité : un enjeu d'avenir et de développement

La cybersécurité est une question de technologies, certes, mais aussi d'humains. D'une part, parce qu'il faut des humains qui soient capables de comprendre et d'opérer les différentes technologies déployées sur le parc informatique - il n'est pas judicieux de multiplier les couches de sécurité si les collaborateurs ne disposent pas des compétences nécessaires pour mettre à jour les bases et mener des actions en fonction des alertes remontées. D'autre part, parce que de nombreuses vulnérabilités et failles de sécurité en entreprise sont également dues à des erreurs humaines à cause d'employés pas toujours sensibilisés aux risques cyber ou formés aux bonnes pratiques d'hygiène numérique.

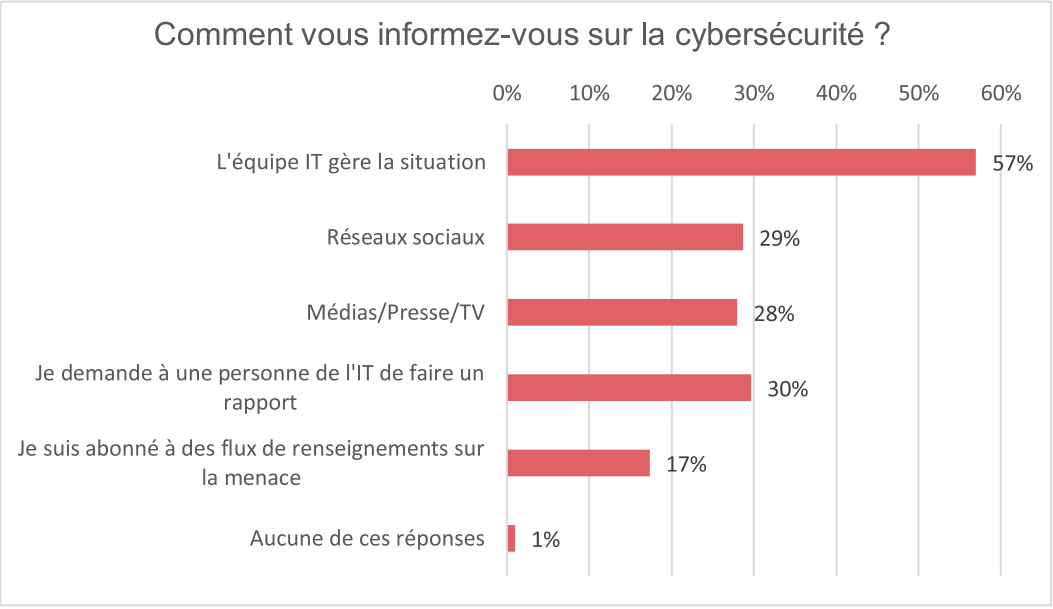
Chez Kaspersky nous sommes convaincus qu'une bonne stratégie de cybersécurité commence par une politique interne de bonnes pratiques et d'outils. Dans un monde qui se digitalise de plus en plus avec des salariés amenés à travailler en dehors du bureau,

et dont le périmètre de sécurité peut plus difficilement être maitrisé, une formation de base aux bonnes règles du numérique semble indispensable. Cela commence par le fait d'imposer des mots de passe fort, la double authentification, la capacité de savoir distinguer des mails de phishing des mails légitimes. En outre, il est crucial de ne pas utiliser les appareils professionnels pour des usages personnels, de systématiquement scanner les appareils amovibles avant de les insérer dans le lecteur USB de l'ordinateur, de ne pas cliquer sur des liens suspicieux et d'uniquement utiliser des sites de e-commerce officiels etc. Cela requiert d'avoir acquis des notions sur les portes d'entrées des différents malwares, des notions sur les différents types de menaces qui existent ainsi que des codes liés à la cybersécurité. Si la grande majorité des répondants disposent de notions en termes de sécurité et est au fait de termes tels qu'attaque DDoS, ingénierie sociale, attaque APT ou encore EDR ou MSP, les connaissances réelles des tenants et aboutissants sont plus limitées.

En effet, seuls 51% des répondants admettent avoir beaucoup d'informations sur les ransomwares, principale menace ciblant les entreprises, et médiatisée, de ces dernières années. 46% en

savent beaucoup concernant le phishing et 22% des répondants admettent avoir déjà entendu parler

des protections EDR mais n'avoir aucune idée de ce dont il s'agit. Beaucoup rencontrent des difficultés à s'informer et ne savent pas forcément où aller chercher l'information en matière de cybersécurité. Lorsqu'on aborde la question des sources d'informations sur le paysage des menaces cyber, seuls 17% sont abonnés à des flux de données sur la menace, les autres s'informent via les médias (28%), les réseaux sociaux (29%), et la grande majorité fait confiance au service informatique (57%), dont seuls 30% réclament des rapports au sujet de ces menaces.



Parmi les chiffres qui nous interpellent : **seules 23% des entreprises admettent avoir une culture de la cybersécurité en entreprise, avec des formations régulières et des informations à jour concernant les bonnes pratiques, et ce chiffre descend à 14% parmi les entreprises « n'estimant pas être exposées au cyber-risque ».** Pour qu'une société soit bien protégée, il faudrait que ce chiffre atteigne les 100%. **Pour rappel, 66% des entreprises tunisiennes estiment être bien protégées face au risque cyber.** Paradoxalement, lorsqu'on demande si les salariés sont régulièrement formés à la cybersécurité et à l'importance de la protection des données, 31% répondent que c'est le cas. En ce qui concerne leur propre formation, les décideurs se sentent plus équipés, avec 27% des répondants indiquant suivre eux-

mêmes des formations régulières en cybersécurité.Celaresteinsuffisant car la majeure partie des incidents peut être évitée avec une bonne politique de mots de passe et

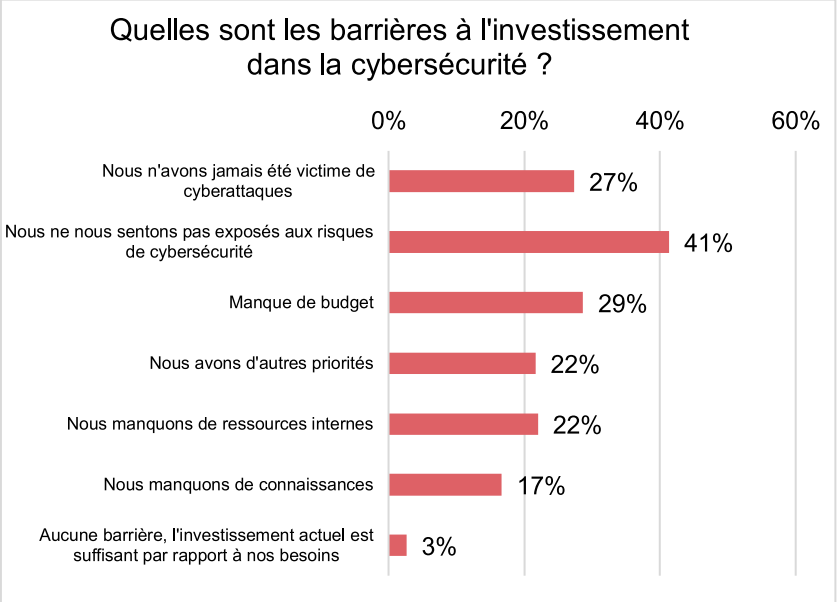
des bonnes pratiques d'hygiène numérique. La mise en œuvre de ces deux dispositifs permet aux salariés de différencier un mail de phishing d'un mail légitime ou encore d'éviter de cliquer sur des liens suspects.

Lorsqu'on leur pose la question des barrières en matièred'investissement dans la cybersécurité, 22% seulement indiquent manquer de ressources

en interne alors que 17% estiment manquer de connaissances sur le sujet. Pour la plupart, ils n'investissent pas parce qu'ils ne se sentent

pas exposés (41%) ou parce qu'ils n'ont jamais fait l'expérience d'une cyberattaque (27%).

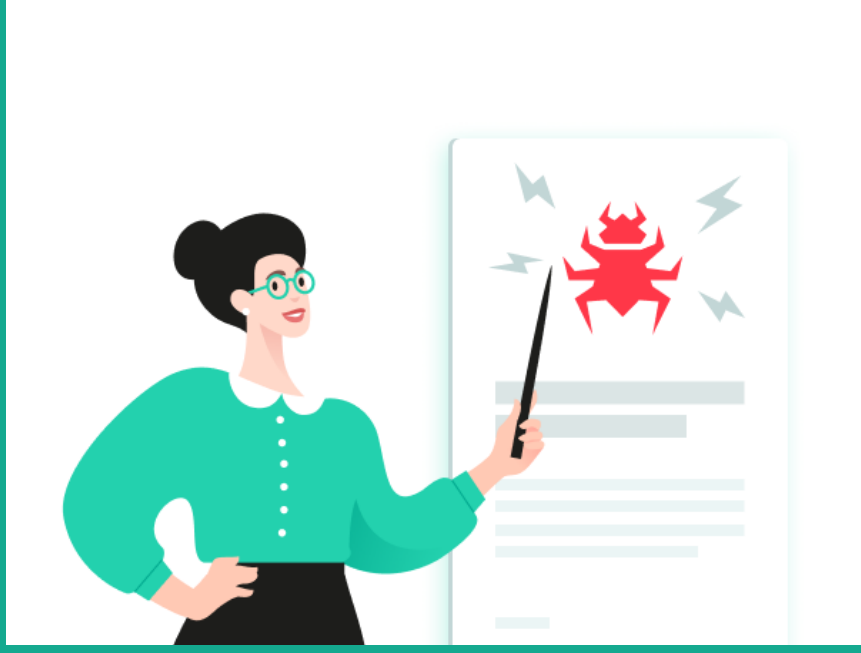
Quelles sont les barrières à l'investissement dans la cybersécurité ?



Selon Pascal Naudin, « la première barrière liée à l'investissement en cyber est le manque de connaissance des risques cyber par les dirigeants des entreprises. Tantqu'ilsverrontlacybersécurité comme une ligne de couts dans un bilan, ils n'auront pas pleinement conscience des risques encourus. Je regrette que les RSSI ne puissent pas déployer les solutions qu'ils souhaitent pour protéger leur entreprise par faute de moyen financier ou humain. In fine, en cas de cyberattaque poussée, les montants dépensés pour y remédier sont très largement supérieursaubudgetqu'ilaurait fallu investir pour éviter que l'incident ne se produise. » Il ajoute aussi que « le problème rencontré sur le marché à des multiples reprises s'articulent autour du caractère inadapté de solutions adoptées par les entreprises. En effet, celles-ci ne sont adaptées ni à la taille et à l'exposition réelle de l'entreprise, ni à leur capacité d'exploiter lesdites solutions. Il s'agit d'une complication supplémentaire car les entreprises n'en exploitent pas toute la quintessence. Par ailleurs, une inadaptation des solutions déployées est toujours un échec. Si elles sont surdimensionnées, le coût sera trop élevé pour l'exploitation réelle des opportunités de la solution, et le ROI sera mauvais. Si elles sont sous-dimensionnées, le risque d'exposition à la menace est plus important. Les éditeurs et partenaires sont alors décrédibilisés, jugés défaillants et donc responsables en cas de menace. Dès lors, la notion de partenaire de confiance prend alors toute son importance et devient indispensable pour s'assurer que les déploiements soient en phase réelle avec le besoin de l'entreprise. »

Pourpalliercesproblématiquesde manque de ressources humaines, un défi international en soi, Kaspersky a déployé des outils qui permettent d'automatiser une partie de la détection et de la réponse aux incidents. Ainsi les équipes informatiques peuvent se concentrer sur les tâches plus importantes. En cas de manque cruel de personnel, des solutions telles que le Managed Detection and Response sous-traitent toute cette partie détection et réponse aux incidents de cybersécurité.

Les formations Kaspersky en matière de cybersécurité



Afin d'ajouter les compétences humaines à la stratégie de cybersécurité d'une entreprise, Kaspersky a également déployé des programmes de formations, allant de la sensibilisation de tous les salariés d'une entreprise aux bonnes bases d'hygiène numérique, aux formations plus techniques dédiées aux professionnels de l'informatique et proposées par nos chercheurs du GREAT.

Tour d'horizon de quelques-unes des principales formations proposées par Kaspersky, pour les entreprises. Certains de ces modules sont intégrés directement dans les offres de sécurité 360°.

KASAP : Il s'agit d'une plateforme en ligne, destinée à tous les employés d'une entreprise pour les aider à développer progressivement des connaissances efficaces et pratiques en matière d'hygiène numérique. Le programme est composé de leçons interactives, de renforcements constants, de tests et de simulations d'attaques de phishing pour s'assurer que les compétences puissent être appliquées. Les principaux thèmes abordés pendant la formation sont les mots de passe et comptes, les mails, la navigation web, les messageries et réseaux sociaux, la sécurité du PC, les appareils mobiles, les données confidentielles et le RGPD.

CITO : Cybersecurity for IT online. Il s'agit d'une formation en sécurité interactive qui fournit des compétences approfondies en cybersécurité et un premier niveau de compétences en réponse à incidents. Cette formation est dédiée aux spécialistes informatiques généralistes et est composée de 6modules:logicielsmalveillants,programmesetfichierspotentiellement indésirables, basiques de l'investigation, réponse aux incidents de phishing, sécurité des serveurs et sécurité de l'active directory.

Le programme équipe les professionnels de l'IT de compétences pratiques pour reconnaître un scénario d'attaque possible dans un incident apparemment bénin, et pour collecter les données relatives à l'incident afin de les transmettre à la sécurité informatique. Il suscite également une passion pour la chasse aux signes d'activité malveillante, cimentant le rôle de tous les membres de l'équipe informatique en tant que première ligne de défense de la sécurité.

X-TRAINING : Le paysage des menaces étant en constante évolution, il est essentiel que les spécialistes de la sécurité informatique maintiennent leurs compétences à jour. Grâce à notre formation en ligne, vous pouvez apprendre des stratégies efficaces de détection et d'atténuation des menaces depuis le confort de votre maison, grâce à des cours pratiques très concrets. Nos auteurs experts savent comment gérer au mieux les menaces posées par les plus de 400 000 échantillons de logiciels malveillants que nous rencontrons chaque jour, et comment partager ces connaissances avec ceux qui luttent contre les dangers en constante évolution de la cyber-réalité d'aujourd'hui.d'aujourd'hui.

Les relations partenaires : Comment externaliser les experts et les technologies pour être plus efficaces dans la gestion de la cybersécurité. Zoom sur le MSP.

Une solution de cybersécurité complexe ne garantira pas la meilleure protection si elle n'est pas mise en œuvre par un spécialiste compétent. Pour les entreprises, la recherche d'un travailleur qualifié dans ce domaine est rendue d'autant plus difficile du fait de la pénurie mondiale d'experts en sécurité informatique. Ce phénomène a été quantifié par (ISC)2 qui a fait état d'un déficit de compétences de 3,4 millions de professionnels sur le marché de l'emploi cyber dans son étude 2022. Cette situation a contraint les entreprises à externaliser certaines fonctions informatiques auprès de fournisseurs de services managés (MSP ou managed service provider) ou de fournisseurs de services de sécurité managés (MSSP ou managed security service provider) afin d'obtenir une expertise adaptée et de perfectionner leurs équipes.

L'étude de Kaspersky, menée auprès de décideurs informatiques à l'international,arévéléquepour65% des PME et de grandes entreprises, la raison la plus courante de transférer certaines responsabilités en matière de sécurité informatique à des MSP/MSSP en 2022 est tout simplement l'efficacité apportée par ces spécialistes externes. Parmi les autres raisons les plus fréquemment citées,lesentreprisesontégalement fait référence au besoin de connaissances spécifiques, à la pénurie de personnel informatique, à la complexité des processus d'entreprise et aux exigences relatives à la mise en conformité.

Aujourd'hui, les PME au Maroc ne font pas encore beaucoup appel à des prestataires de solutions de services de sécurité externe, dans la mesure où seuls 16% des répondants à l'étude indiquent qu'un partenaire tiers est responsable de la cybersécurité. La confiance dans les partenaires, fournisseurs de solutions (et non de services) est d'ailleurs également relative puisque seuls 29% des répondants indiquent « faire confiance à leurs fournisseurs de sécurité et leurs partenaires IT » en ce qui concerne la résolution de problématiques informatiques. Pour autant, 76% des répondants indiquent « savoir qui contacter » en cas de problème informatique.

Le modèle MSP, pour les entreprises ne disposant pas de toutes les ressources humaines en interne.

Afin de pallier le manque de maturité des entreprises, quelles que soient leurstailles,nouspouvonségalement recommander de passer par un partenaire MSP. Un MSP est une entreprise de services informatiques qui gère les systèmes informatiques de ses clients à distance. Fini

le temps où le professionnel de l'informatique attend d'être contacté par le client en cas de panne (modèle Break/fix). Maintenant, avec le modèle MSP, le professionnel est proactif dans le management des parcs informatiques dans l'optique d'assurer un fonctionnement optimal de ces derniers. L'autre plus-value de ce modèle est la méthode de

facturation. Cette dernière se fait de façon forfaitaire avec le plus souvent un abonnement mensuel. La plupart des solutions de Kaspersky sont proposées sur un modèle MSP, ce qui est également le cas pour les offres et flux de threat intelligence depuis peu. Cela permet à la fois aux partenaires de l'entreprise de développer une forte valeur ajoutée sur le marché de la cybersécurité et aux entreprises de pouvoir travailler avec des prestataires de confiance, capables de gérer de bout en bout l'opérationnel en matière de cybersécurité.

Au Maroc, et pour toute l'Afrique, le distributeur informatique MIPS a lancé en juin, MSP for Africa, la première plateforme MSP proposant les produits et solutions de Kaspersky en Afrique.

Chez Kaspersky, le modèle MSP existedepuisenviron5ans.L'objectif de l'entreprise est de permettre aux partenaires, prestataires de services experts en cybersécurité d'avoir un modèle d'abonnement économique plus souple mais également de pouvoir proposer une véritable valeur ajoutée, une prestation de service auprès de ses entreprises clientes. Le partenaire MSP est le chef d'orchestre : il gère et administre les solutions de ses différents clients.

La plateforme MSP développée par MIPS permet aujourd'hui aux revendeurs de générer des licences via les API chez Kaspersky de manière totalement autonomes afin qu'il puisse se concentrer sur le service à fournir. Aujourd'hui la plateforme MSP for Africa propose toute la gamme de solutions de Kaspersky pour les entreprises : de la threat intelligence aux solutions best-seller d'EDR Optimum, ou EDR Expert en passant par le Kaspersky Endpoint Security Cloud ou encore le Kaspersky Managed Detection and Response. Kaspersky propose également des formations expertes, à la fois accessibles à la vente pour les entreprises et à la fois, pour former les revendeurs, afin que ces derniers puissent délivrer la meilleure capacité de service Kaspersky à leurs clients.

Emna Haouala, directrice générale de MIPS explique : « Nous sommes fiers de proposer cette offre, première plateforme MSP Kaspersky en Afrique parce que nous savons que nous adressons un marché en pleine croissance. Pour le moment, cela n'adressera que quelques revendeurs déjà initiés, mais l'idée est de faire grandir nos revendeurs existants et d'en convaincre d'autres, à l'avenir, de nous faire confiance en proposant des offres de services. »

Choisir son partenaire de confiance

Choisir son partenaire et son prestataire de services, ou de solutions, de confiance semble aujourd'hui être une priorité. En effet, il est essentiel à la fois de s'équiper d'outils en phase avec lastratégiedel'entreprisemais également d'être accompagné par une notion de services qui permet d'être à même d'identifier les options à notre disposition en cas de problème de sécurité. Kaspersky a toujours positionné la confiance et la transparence comme deux valeurs centrales dans son approche: la transparence dans la manière de traiter les données, dans ses mises à jour de sécurité, dans ses procédures et la confiance dans la créationet l'entretien de son écosystème de partenaires, dans la sécurité et l'intégrité de ses solutions et dans sa réactivité. A noter que cette notion de confiance est primordiale à l'heure où encore une minorité des entreprises estime que la notion de cybersécurité est « une arnaque », bien que la protection des données soit une priorité pour les années à venir.

PAROLE DE PARTENAIRE

EMNA HAOUALA,
Directrice générale de MIPS

« L'engagement de MIPS, en tant que partenaire distributeur des solutions de sécurité Kaspersky se reflète dans notre approche d'accompagnement des entreprises vers l'excellence en cybersécurité.

Face à l'explosion de la cybercriminalité, notre mission est de guider nos partenaires dans leur montée en compétences, notamment grâce au modèle MSP qui leur offre une grande agilité.

Notre partenariat avec Kaspersky repose sur les fondements d'une relation durable et de confiance. En collaborant main dans la main, nous facilitons l'accès à des solutions de pointe qui répondent aux besoins de sécurité actuels. Nous comprenons que la cybersécurité évolue sans cesse, c'est pourquoi nous travaillons sur l'offre Service de notre modèle MSP afin d'apporter la meilleure réponse aux besoins des clients sur l'ensemble du continent Africain.

L'évolution rapide des menaces et des technologies demande une approche proactive. C'est ainsi que nous restons à l'avant-garde des tendances, en anticipant les besoins changeants des entreprises. Notre partenariat avec Kaspersky s'inscrit dans cette dynamique, nous permettant d'offrir des solutions qui non seulement répondent aux défis actuels, mais qui préparent également nos clients pour un avenir numérique plus sûr . »

Top 5 des menaces que les petites et moyennes entreprises doivent surveiller en 2023.

Risque #1 : Les fuites de données causées par les employés

Les données d'une entreprise peuvent être divulguées de différentes manières, et dans certains cas, de manière involontaire.

Pendant la pandémie, de nombreux travailleurs à distance ont utilisé leurs ordinateurs professionnels dans le cadre de leurs loisirs, que ce soit pour jouer à des jeux en ligne, regarder des films ou utiliser des plateformes de cours. Cette nouvelle habitude est un facteur de risques pour les entreprises.

Le niveau de cybersécurité depuis l'adoption massive du télétravail s'est amélioré. Néanmoins, les ordinateurs professionnels utilisés à des fins de divertissement demeurent l'un des principaux moyens d'obtenir un accès initial au réseau d'une entreprise. En cherchant des sites pour télécharger le dernier épisode d'une série ou un film récemment sorti, les internautes peuvent rencontrer divers types de logiciels malveillants, notamment des chevaux de Troie, des logiciels espions, des portes dérobées, et des logiciels publicitaires. Si ces logiciels malveillants se retrouvent sur un ordinateur professionnel, les attaquants peuvent pénétrer dans le réseau de l'entreprise, rechercher et voler des informations sensibles.

D'autre part, il n'est pas rare de voir attribuer d'éventuelles fuites de données à d'anciens employés. Pourtant, selon une étude récente, seuls 40% des dirigeants de PME interrogés ont répondu être convaincus que leurs anciens employés n'ont pas accès aux données de l'entreprise stockées dans les services cloud, ou ne peuvent pas utiliser les comptes de l'entreprise. Si ces chiffres sont plus faibles en Tunisie (77% pensent que les salariés ne peuvent accéder aux données de l'entreprise après leur départ), le manque de rigueur en ce qui concerne les politiques de travail à distance (38% en disposent d'une) laisse à penser que les entreprises tunisiennes courent elles aussi ce genre de risque.

Risque #2 : Les attaques DDoS

Les attaques par déni de service distribué tirent parti des limites de capacité spécifiques qui s'appliquent à toutes les ressources du réseau, comme l'infrastructure qui permet la mise en place du site web d'une entreprise. L'attaque DDoS envoie de multiples requêtes à la ressource web attaquée, dans le but de dépasser la capacité du site web à traiter toutes les requêtes et ainsi empêcher le site de fonctionner correctement.

Les cyberpirates recourent à différentes sources pour agir sur des organisations telles que les banques, les médias ou les détaillants, fréquemment victimes d'attaques DDoS. Récemment, des cybercriminels ont pris pour cible le site Takeaway.com (Lieferando.de), et exigé deux bitcoins (environ 11 000 dollars) pour mettre fin à l'afflux de trafic. A noter que les attaques DDoS contre les sites de vente en ligne ont tendance à augmenter pendant les vacances, périodes où les clients sont plus actifs.

Il convient de souligner que de nombreuses attaques DDoS ne sont pas signalées, car les montants versés sont généralement peu élevés.

Risque #3 : La chaine d'approvisionnement

Être attaqué par le biais d'une chaine d'approvisionnement signifie généralement qu'un service ou un programme utilisé par une entreprise depuis longtemps est devenu malveillant. Il s'agit d'attaques menées par l'intermédiaire des vendeurs ou des fournisseurs de l'entreprise : il peut s'agir d'institutions financières, de partenaires logistiques, ou encore d'un service de livraison à domicile. Ces attaques peuvent varier en complexité et en puissance.

Risque #4 : Les malwares

Les fichiers malveillants peuvent se cacher partout : si vous téléchargez des fichiers illégitimes, assurez-vous qu'ils ne puissent pas vous nuire. Alors que plus d'un quart des petites et moyennes entreprises optent pour des versions piratées ou sans licence des logiciels professionnels afin de réduire leurs coûts, il convient de mentionner que ces logiciels peuvent contenir des fichiers malveillants ou indésirables susceptibles de compromettre les systèmes de l'entreprise.

En outre, les dirigeants de PME doivent se méfier des brokers d'accès, car il est probable que ces groupes causent beaucoup de torts aux entreprises. Leurs clients, demandeurs d'accès illégaux, comprennent aussi bien des personnes adeptes de cryptojacking que des voleurs d'identifiant bancaires, des ransomwares, des voleurs de cookies et d'autres logiciels malveillants problématiques.

Risque #5 : L'ingénierie sociale

La suite Office 365 de Microsoft est de plus en plus utilisée et, sans surprise, ses utilisateurs sont de plus en plus ciblés par des tentatives de phishing. Les fraudeurs ont recours à toutes sortes d'astuces pour inciter les utilisateurs professionnels à saisir leur mot de passe sur un site Web illégitime ressemblant à la page de connexion de Microsoft.

Les experts de Kaspersky ont mis au jour de nombreuses nouvelles façons dont les cybercriminels spécialisés en phishing tentent de tromper les dirigeants d'entreprises. Ces stratagèmes s'avèrent parfois très élaborés : certains imitent des services de prêt ou de livraison, en partageant un faux site Web ou envoient des e-mails contenant de faux documents comptables.

Certains attaquants se font passer pour des plates-formes en ligne légitimes afin de tirer profit de leurs victimes. Il peut même s'agir de services de transfert d'argent très populaires, tels que Wise Transfer.

Conclusion

Le paysage des cybermenaces est en constante évolution et de manière exponentielle, à l'image du développement des usages du numérique. Alors que la transformation digitale des entreprises et des administrations semble être une priorité d'aujourd'hui comme de demain pour s'inscrire dans une société en mouvement et interconnectée, il est nécessaire qu'elle soit envisagée avec une approche la plus résiliente possible. Qu'est-ce que cela signifie ? Que pour faire en sorte que le numérique apporte plus d'opportunités que de dangers, il est nécessaire de réfléchir à la valeur des données traitées par l'entreprise, à la valeur de son activité et aux dommages que pourraient provoquer une cyberattaque, ou une faille de sécurité. Au fil du rapport, les principaux facteurs de risques identifiés par l'entreprise tournent autour de la perte de clients, de la fraude financière et de la perte de réputation. Si un problème lié à l'informatique peut à la fois paralyser la capacité de production, faire fuiter des données sensibles de clientèle, bloquer la capacité opérationnelle pendant un temps donné ou encore faire perdre un avantage stratégique vis-à-vis d'un concurrent, pour ne citer que ces risques, il semble primordial d'anticiper le risque et d'intégrer la question de la cybersécurité à la transformation numérique.

In fine, quels sont les éléments constitutifs d'une bonne stratégie cyber ? Une bonne stratégie cyber repose sur la compréhension de son parc informatique, de son périmètre et sur la nécessité de s'équiper avec des outils adaptés. Il est parfois inutile de se suréquiper avec des technologies certes robustes, mais inadaptées aux équipes et au quotidien de l'entreprise. Cela requiert également de savoir s'entourer de professionnels de qualité à travers un réseau de partenaires de confiance, auprès d'un éditeur réactif et capable d'offrir des services en adéquation avec son besoin. C'est comprendre ses « faiblesses » : manque de ressources, manque de moyens ? Un modèle de services sur abonnement ne serait-il pas plus pertinent pour la trésorerie de l'entreprise ainsi que pour pallier le manque de compétences ? Une bonne stratégie cyber, c'est également intégrer de la gouvernance numérique au sein de l'entreprise. Quelles règles établir auprès des salariés ? Quelles formations d'hygiène numérique de base imposer à tous ? Quels outils utiliser, quelle approche en matière de travail à distance ?

Enfin, une bonne stratégie de cybersécurité, c'est aborder toutes les décisions stratégiques de l'entreprise en y intégrant le prisme de la sécurité. Intégrer la cybersécurité dans les prises de décision et dans les comités de direction. Cela permettra d'éviter l'inertie, mais plutôt d'encourager l'action en toute conscience, de manière cyber-sécure. Chez Kaspersky, nous avons à cœur d'accompagner la montée en maturité des entreprises au Maroc sur les enjeux de cybersécurité en travaillant avec un écosystème local qualifié et de confiance, en proposant des solutions adaptées aux besoins des entreprises quelles que soient leurs tailles et en développant des offres de services telles que des formations allant des cours de base de bonne hygiène numérique aux sessions très qualifiées pour développer des compétences pointues quand on est déjà un professionnel de l'informatique. Les petites et moyennes entreprises produisent énormément de valeur et sont en contact avec des organisations et entreprises de plus grande taille, parfois hautement stratégiques. Pour ces raisons, elles sont également la cible de cybercriminels qui n'ont pas d'état d'âme, ils suivent l'argent et les opportunités. Pour ces raisons, il est temps de briser les idées reçues et de prendre conscience de sa valeur et donc, de la protéger. Chez Kaspersky, nous avons pour objectif d'aider tous nos clients à se protéger contre toutes les menaces, d'où qu'elles viennent et quel que soit leur objectif, et cela passe aussi par de la sensibilisation.

ANNEXE – GLOSSAIRE

Ransomware : Les ransomware, ou rançongiciels sont des logiciels malveillants qui cryptent les données (crypto-malware) ou bloquent l'accès aux données (lockers), exigeant une rançon en échange de l'accès.

Cheval de Troie : Les chevaux de Troie sont des programmes malveillants qui effectuent des actions non autorisées par l'utilisateur : ils suppriment, bloquent, modifient ou copient des données et perturbent le fonctionnement des ordinateurs ou des réseaux informatiques. Contrairement aux virus et aux vers, les menaces de cette catégorie sont incapables de se copier ou de s'autoreproduire

Spyware : Type de logiciel qui s'installe secrètement sur l'ordinateur d'un utilisateur pour collecter ses données. Contrairement aux logiciels malveillants, les logiciels espions n'endommagent pas le système d'exploitation ni les programmes et les fichiers.

Phishing : Le phishing (ou hameçonnage) est une forme de cybercriminalité basée sur des techniques d'ingénierie sociale. Il s'agit de voler des données confidentielles sur l'ordinateur d'une personne et d'utiliser ces données pour lui voler de l'argent. Le cybercriminel crée une réplique presque parfaite d'une institution financière ou d'un site web de commerce en ligne (par exemple). Il tente ensuite d'attirer des victimes peu méfiantes sur le site pour les inciter à divulguer entre autres leur identifiant, leur mot de passe, leur numéro de carte de crédit, leur code PIN dans un faux formulaire. Ces données sont collectées par l'hameçonneur qui les utilise ensuite pour accéder frauduleusement aux comptes des personnes.

Ingénierie sociale : L'ingénierie sociale fait référence à la manipulation de la psychologie humaine. Dans le contexte de la sécurité informatique, il s'agit d'une violation non technique de la sécurité qui s'appuie fortement sur l'interaction humaine, c'est-à-dire le fait de tromper les gens pour qu'ils fassent quelque chose qui mette en péril leur sécurité ou celle de l'organisation pour laquelle ils travaillent. Les cybercriminels s'appuient largement sur le déguisement de logiciels malveillants et de messages de spam en communications légitimes, qui peuvent même prétendre offrir des conseils sur la manière de lutter contre la cybercriminalité. L'objectif est d'inciter la victime à répondre : cliquer sur une pièce jointe infectée, cliquer sur un lien vers un site web compromis ou répondre à un faux avis de désabonnement.

SOC : Le Security Operations Center, SOC, désigne dans une entreprise l'équipe en charge d'assurer la sécurité de l'information. Le SOC est une plateforme permettant la supervision et l'administration de la sécurité du système d'information au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance. L'objectif d'un SOC est de détecter, analyser et remédier aux incidents de cybersécurité à l'aide de solutions technologiques et d'un ensemble de démarches. Ils surveillent et analysent l'activité sur les réseaux, les serveurs, les terminaux, les bases de données, les applications, les sites Web et autres systèmes, à la recherche de signaux faibles ou de comportements anormaux qui pourraient être le signe d'un incident ou d'un compromis en matière de sécurité

EDR : Endpoint Detection and Response (EDR) désigne une classe de solutions de détection et d'analyse des activités malveillantes sur les terminaux : postes de travail, serveurs, appareils IoT, etc. Contrairement aux logiciels antivirus, qui sont conçus pour lutter contre les menaces typiques et de masse, les solutions EDR sont orientées vers la détection des attaques ciblées et des menaces complexes. Cela dit, les solutions EDR ne peuvent pas remplacer complètement les programmes antivirus (EPP) ; les deux technologies traitent des défis différents.

Threat Intelligence : Les renseignements sur les menaces sont des informations sur les menaces actuelles et les acteurs de la menace. Les entreprises peuvent utiliser ces informations pour étudier les objectifs, les tactiques et les outils et élaborer une stratégie défensive efficace contre les attaques. Les entreprises peuvent collecter elles-mêmes des renseignements sur les menaces ou les acquérir auprès de fournisseurs tiers.

Exploit : Le terme «exploit» décrit un programme, un morceau de code ou même certaines données écrites par un pirate informatique ou un auteur de logiciels malveillants, conçu pour tirer parti d'un bogue ou d'une vulnérabilité dans une application ou un système d'exploitation. En utilisant l'exploit, un pirate obtient un accès non autorisé à l'application ou au système d'exploitation, ou l'utilise.

Adware : Programmes conçus pour lancer des publicités sur les ordinateurs infectés et/ou pour rediriger les résultats des moteurs de recherche vers des sites web promotionnels.

kaspersky