L’humain au cœur du dispositif de cybersécurité

Etat des lieux et préconisations

Juin 2021

Abington ADVISORY

Préambule

Pierre Fabre, Facebook, Microsoft Exchange, Ubisoft, Bouygues Construction, Orange, Dassault Aviation, le groupe M6, E-Leclerc, les hôpitaux français, la Commission européenne…

les cyberattaques se multiplient et entraînent des blocages importants et des pertes significatives. Pourquoi alors que les dépenses de protection augmentent, les organisations publiques et privées n'arrivent-elles pas à juguler ce fléau ?

Contexte

Dans un contexte de pandémie mondiale, le recours au télétravail s'est répandu comme une solution nécessaire à la continuité de l'activité professionnelle et à la survie économique des organisations.

Pourtant bien qu'indispensable, il n'est pas apparu sans risque. En effet, même les entreprises ayant sécurisé le matériel interne n'ont pu anticiper les risques cyber induit par l'utilisation d'outil externe.

Bien souvent les ordinateurs personnels transposés du jour au lendemain en accessoire de travail ne disposent pas des mesures de sécurité aussi efficaces que ceux des postes de bureaux.

Les cybercriminels l'ayant bien compris, les attaques informatiques ont redoublé d'intensité depuis janvier 2020. Pour exemple l'ANSSI (l'Agence Nationale de la Sécurité des Systèmes d'Information) indiquait avoir traité, depuis début 2020, 104 attaques de ransomwares contre 54 en 2019.

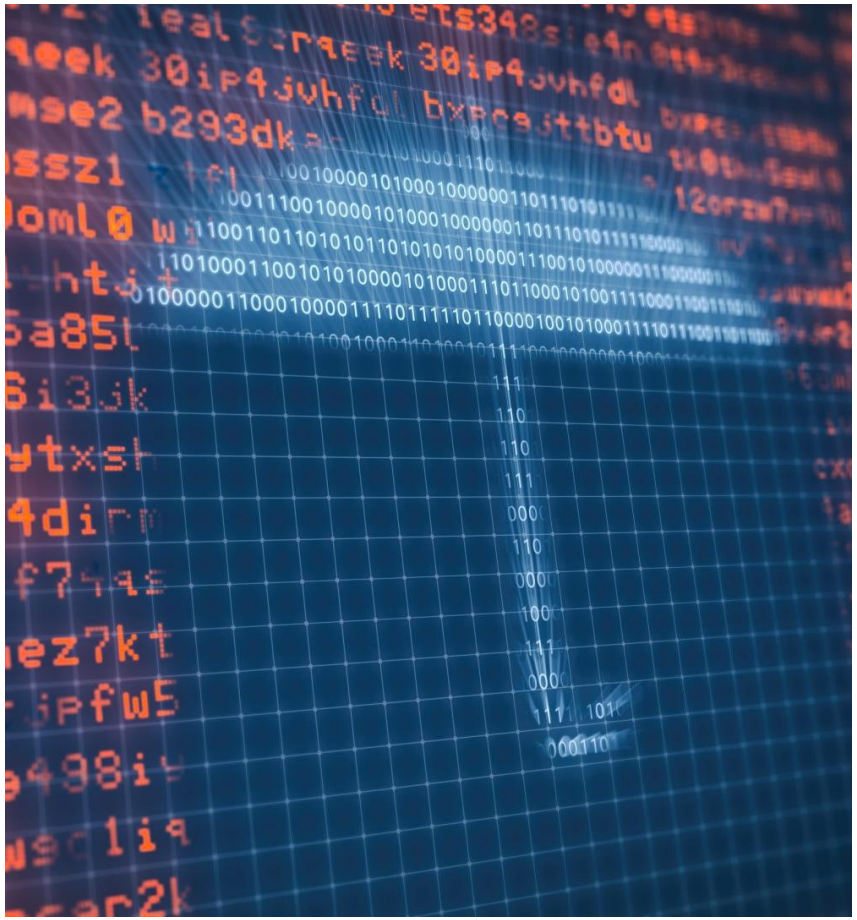
Dans le même temps les investissements dans la sécurité des systèmes d'information n'ont jamais été aussi importants. Selon le rapport sur la gestion des risques cyber mené par Hiscox, il est possible de constater que les entreprises françaises ont porté leur budget de 1,9 millions d'euros à 2,8 millions d'euros entre l'année 2019 et 2020.

Face à cette tendance, de nouvelles assurances couvrant les risques de cyberattaques se sont développées.

Schématiquement, en cas d'attaque et de paiement d'une rançon, l'assureur rembourse le montant demandé dans la limite d'un plafond et après paiement d'une franchise.

Il est donc important de se demander si ces investissements sont véritablement appropriés quant à la réalisation des objectifs de sécurité cyber ?

Des investissements curatifs insuffisants et incomplets



Toujours selon ce rapport « les entreprises qui ont dépensé une part à deux chiffres de leur budget informatique dans la cybersécurité ont eu tendance à subir moins d'incidents ou de vulnérabilités que celles dépensant moins de 5%.

Toutefois les plus dépensières, qui sont généralement les plus grandes entreprises, ont payé en moyenne un prix plus fort après avoir subi une attaque Cyber. La taille est corrélée à davantage de clients, des coûts de notification plus élevés et des rançons plus onéreuses.

Le constat est sans appel, le développement de mesures de cybersécurité est nécessaire mais insuffisant. L'ensemble des technologies sécurisant les systèmes d'informations apparaissent incomplètes, elles constituent un véritable frein aux attaques mais s'avèrent davantage être une solution curative ciblée plus qu'un moyen préventif de lutte contre la cybercriminalité.

Une étude menée par Thycotic illustre le propos en indiquant que 77% des entreprises interrogées déclarent que c'est un incident de sécurité qui a convaincu le conseil d'administration d'investir dans des projets de cybersécurité.

La question est alors de savoir comment entreprendre une démarche de cybersécurité pertinente ?

Des investissements préventifs plus pertinents

Selon l'éditeur de logiciel de sécurité Kaspersky, plus de 80% des incidents de sécurité découlent d'une erreur humaine.

En effet selon knowBe4, les attaques par phishing ont par exemple augmenté de plus de 600 % sur le premier semestre 2020. Par exemple 18 millions d'emails quotidiens de Phishing et contenant un logiciel malveillant liés à la COVID 19 ont été détectés par Google au cours de la semaine du 16 avril 2020. (Source : Google).

Alors que grand nombre d'analyses sur le piratage informatique se focalisent sur les failles techniques, il apparait judicieux de se concentrer sur un sujet parfois sous-estimé par un certain nombre d'observateurs : **l'humain**.

Le principal vecteur d'attaque reste l'utilisateur. C'est la raison pour laquelle les virus, malware, ransomware, phishing, cheval de Troie, keylogger constituent un panel de dangers dont chacun doit avoir conscience dans son quotidien professionnel. Les sensibilisations et formations aux menaces cyber sont l'affaire de tous. Il devient essentiel d'acquérir les bonnes pratiques pour compliquer la tâche des pirates informatiques, les mesures de gouvernance de la cybersécurité doivent s'inscrire dans le quotidien des actions des opérateurs métier.

Comme tout changement et toute contrainte, ces formations peuvent être un levier de business à moindre coût pour les organisations.

Conclusions

Dans le « Monde d'après » hyperconnecté et dans lequel les systèmes d'informations sont démultipliés, la cybercriminalité est devenue une immense menace pour les organisations.

Pour faire face à cette nouvelle criminalité, les investissements dans les outils de cyber sécurité curatives n'ont fait que croitre. Pourtant bien qu'indispensables, ces dernières sont bien souvent, apparues insuffisantes et incomplètes.

Il est aujourd'hui essentiel de développer une stratégie préventive de lutte contre ces cybermenaces. Pour cela la question de l'humain et de l'organisation doit être au cœur des réflexions. Maitriser les comportements des utilisateurs constituera la clé de voute d'une stratégie de cybersécurité réussie.

Recommandations

Mettre en place une politique de sécurité des systèmes d'information	/ Effectuer une analyse des risques liées au SI / Etablir une feuille de route de sécurisation du SI / Réaliser un plan d'actions palliant les risques de sécurité du SI
Mettre en place une charte informatique destinée à tout utilisateur de la donnée	/ Définir les règles d'usages des outils informatiques, des sites internet et des réseaux sociaux et préciser les mesures de contrôles mises en place et réguler les accès en présentiel et en distanciel / Spécifier les sanctions encourues par le salarié / Communiquer la charte informatique et s'assurer de son opposabilité à chacun des collaborateurs
Sécuriser le matériel de travail interne comme externe	/ Recenser le matériel de travail / Sécuriser le matériel par des mesures physiques (fermeture porte, accès par badge etc.) et sécuriser le matériel à l'aide d'antivirus, de segmentation réseaux etc. / Mettre en place une politique de byoD (bring your own device)
Considérer la cybersécurité dans tout projet	/ Définir des personnes chargées de cybersécurité / Inclure ces expertises dans tout nouveau projet / Réaliser des comptes rendus des actions de cybersécurité dans chacun des projets
Sensibiliser et former les utilisateurs	/ Réaliser une sensibilisation et une formations e-learning adaptée à chaque service / Les diffuser à l'ensemble des collaborateurs / Effectuer des ateliers de questions réponses sur les formations / sensibilisations