RAPPORT DE SYNTHÈSE

Le décalage des incitants, ou pourquoi les cybercriminels ont une longueur d'avance — Coup de projecteur sur le secteur des services financiers

Les cybercriminels, qui imaginent sans cesse de nouvelles façons de voler les données, d'interrompre les services et de perturber le flux légitime des informations, ont depuis longtemps une longueur d'avance sur les équipes responsables de la sécurité. Cela ne signifie pas pour autant qu'ils sont meilleurs. En réalité, ils bénéficient d'un décalage entre les incitants qui leur sont proposés et ceux offerts aux professionnels de la sécurité. Pour mieux cerner ce décalage, nous avons interrogé 200 professionnels de l'informatique issus du secteur des services financiers, et comparé leurs réponses à celles de 600 responsables informatiques d'autres secteurs d'activité. Le **rapport** a identifié trois décalages principaux en matière d'incitants : entre les structures d'entreprise et la liberté d'action des entreprises criminelles, entre la stratégie et l'implémentation, et entre les dirigeants et les exécutants.

Un décalage à trois niveaux en matière d'incitants qui place les équipes de sécurité en position de faiblesse

Cybercriminels et équipes de sécurité	Les incitants des cybercriminels trouvent leur origine dans un marché décentralisé fluide, qui favorise l'agilité et une adaptation rapide, tandis que les équipes de sécurité sont soumises aux contraintes de la bureaucratie et d'un processus de prise de décisions hiérarchisé.
Stratégie et implémentation	Bien que plus de 90 % des entreprises disposent d'une stratégie de cybersécurité, moins de la moitié d'entre elles l'ont entièrement implémentée.
Dirigeants et exécutants	Les cadres dirigeants qui conçoivent les stratégies de cybersécurité mesurent le succès différemment des exécutants qui les implémentent, ce qui limite l'efficacité globale.

Structure d'entreprise contre entreprise criminelle

Le secteur des services financiers est depuis longtemps conscient des effets que peuvent avoir des incitants clairs et directs. Les cybercriminels opèrent dans un monde clandestin mais ouvert qui propose des incitants clairs aux pirates indépendants, encourageant ainsi une concurrence dynamique et une innovation rapide. Ce modèle favorise un haut niveau de spécialisation, permettant ainsi aux cybercriminels les plus chevronnés d'affiner leurs compétences tout en créant un vaste réseau de prestataires de services et de clients. Les informations sont partagées par le biais d'un large éventail de canaux de communication et les nouvelles vulnérabilités sont exploitées très rapidement. Les marchés extrêmement actifs permettent de trouver des clients intéressés et de monnayer les nouvelles informations et lignes de code en toute simplicité.

Selon cette étude, parmi les sociétés interrogées, les entreprises de services financiers sont celles dont les pratiques s'apparentent le plus à un marché d'informations ouvert en matière de cybersécurité. En effet, elles sont les plus susceptibles de partager des informations avec d'autres, notamment des partenaires (63 % contre 52 % des répondants issus de secteurs non financiers), des consultants externes (49 % contre 39 %) et même des concurrents (26 % contre 19 %). Seuls 7 % des répondants ont déclaré ne pas partager d'informations sur les cybermenaces, contre 14 % dans les autres secteurs d'activité.

Cette attitude vis-à-vis du partage d'informations influe sur les sources utilisées par les entreprises de services financiers lors de la prise de décision en matière de cybersécurité. Pour preuve, elles sont légèrement plus enclines à utiliser des informations partagées par des sources externes que les entreprises des autres secteurs. Il peut notamment s'agir d'informations provenant d'éditeurs de solutions de sécurité (63 % contre 57 %), de consultants externes (51 % contre 46 %) ou de groupes sectoriels (26 % contre 22 %). Parfois, ces informations sont analysées et synthétisées par des opérateurs dans la mesure où les professionnels des services financiers sont également bien plus enclins à avoir recours à des notes d'information internes que les entreprises des autres secteurs (70 % contre 61 %).

L'adhésion du secteur des services financiers au principe des marchés ouverts en matière de cybersécurité dépasse le simple partage d'informations pour s'étendre aux services et aux consultants. En effet, les entreprises de services financiers sont les plus susceptibles de consacrer une part importante du budget alloué à la cybersécurité au recrutement de consultants (49 % contre 40 % des entreprises des autres secteurs), et légèrement plus enclines à consentir des dépenses dans des services professionnels de surveillance et de réponse aux incidents (38 % contre 34 %). Il a été démontré que cette ouverture à des informations et des spécialistes externes a un impact positif sur l'efficacité de la sécurité.

Décalage entre stratégie et implémentation

Pour la majorité des répondants, tous secteurs d'activité confondus, la cybersécurité représente aujourd'hui le principal risque auquel les entreprises sont exposées. Près de 80 % des entreprises de services financiers portent les risques en matière de sécurité à l'attention de leur conseil d'administration à pratiquement chaque réunion, contre seulement 70 % dans les autres secteurs. Si presque tous les répondants du secteur financier (95 %) ont indiqué que leur entreprise dispose d'une stratégie de cybersécurité destinée à contrer les menaces existantes et émergentes, la difficulté réside essentiellement dans l'implémentation. À peine plus de la moitié (51 %) des entreprises interrogées ont déclaré l'avoir entièrement mise en œuvre, tandis que 8 % n'en ont implémenté aucun aspect.

Le décalage entre les stratégies de sécurité définies et leur implémentation peut être dû pour partie à une préoccupation mal placée quant à la nature des risques auxquels l'entreprise est confrontée. En moyenne, la direction et le conseil d'administration de ces entreprises de services financiers seraient plus préoccupés par l'atteinte à la réputation (67 %) que par la perte de revenus ou de bénéfices (50 %). Au vu de la multiplication récente du nombre de vols directs au sein du secteur financier, par opposition aux pertes dues à la fraude liée au vol de numéros de carte de crédit, cette attitude peut conférer un sentiment de sécurité illusoire.

Les entreprises qui implémentent leur stratégie de sécurité semblent avoir un niveau de maturité de la sécurité supérieur à la moyenne. Parmi les tâches à charge des équipes de sécurité de ces entreprises, la défense proactive est celle à laquelle elles consacrent le plus de temps, suivie de l'étude de nouvelles stratégies et solutions, la défense réactive n'arrivant qu'en troisième position. Peut-être plus important encore, elles consacrent moins de temps à des tâches non liées à la cybersécurité (à peine 8 % de leur temps) que les entreprises des autres secteurs (14 %).

Étant donné que le secteur des services financiers constitue depuis longtemps une cible des cyberattaques, il n'est guère surprenant que 73 % des professionnels de la sécurité de ce secteur aient indiqué disposer d'un budget suffisant pour implémenter leur stratégie, contre seulement 58 % dans les autres secteurs d'activité. Seul un petit nombre d'entre eux ont déclaré que leur budget (4 %) ou leur dotation en personnel (9 %) était insuffisant et risquait d'entraver la mise en œuvre de leur stratégie.

Un autre décalage entre la stratégie et l'implémentation concerne les méthodes employées pour s'assurer que les mesures de cybersécurité n'exposent pas l'entreprise à de nouveaux risques. Si la majorité des entreprises financières (73 %) ont affirmé disposer d'une plate-forme de sécurité intégrant technologies nouvelles et existantes, un nombre comparable d'entreprises (70 %) ont indiqué se doter également de technologies redondantes. Si cette stratégie d'implémentation peut de prime abord sembler judicieuse, des technologies de sécurité redondantes qui ne sont pas suffisamment intégrées peuvent parfois engendrer des failles dans la sécurité. En effet, la disparité des systèmes de configuration et de surveillance complique la création et la mise en œuvre de stratégies de sécurité cohérentes.

Incitants différents pour les dirigeants et les exécutants

Les cybercriminels sont motivés par des incitants directs tels que l'argent, la publicité ou les embarras causés à leur cible. Les équipes de sécurité des entreprises de services financiers sont les plus susceptibles de bénéficier d'incitants existants tels que des distinctions (55 % contre 48 % pour les autres secteurs) et des primes (53 % contre 43 %). Seuls 9 % des répondants ont déclaré qu'aucun programme d'incitation n'existait au sein de leur entreprise, contre 21 % dans les autres secteurs d'activité. Le principal facteur de dissuasion contre les comportements de cybersécurité à risque des employés réside dans la menace de poursuites judiciaires (69 % contre 59 %). Par ailleurs, 56 % des professionnels de l'informatique du secteur financier indiquent que l'implémentation de la stratégie est intégrée dans leurs évaluations de performances individuelles, contre seulement 46 % pour les autres secteurs.

Pour déterminer si la stratégie répond aux objectifs, il est nécessaire de disposer d'un ensemble de mesures suffisamment détaillé. 1 % seulement des répondants du secteur des services financiers ont déclaré ne pas être en mesure de déterminer s'ils atteignaient leurs objectifs, contre 7 % pour les autres secteurs. Bien que cette majorité reste faible, un plus grand nombre d'équipes de sécurité du secteur financier ont indiqué disposer de méthodes appropriées pour l'évaluation de la stratégie que dans les autres secteurs. Il peut notamment s'agir des activités de gestion des risques (66 % contre 57 %) ou du délai moyen de résolution (52 % contre 45 %).

Les enseignements à tirer de la cybercriminalité

Actives depuis longtemps sur différents types de marchés, les entreprises de services financiers semblent présenter le décalage des incitants le plus réduit en matière de cybersécurité. Elles sont d'ores et déjà les plus grandes utilisatrices de consultants et de services de sécurité externes, mais pourraient peut-être accorder davantage de poids à la cyberveille et aux informations de sécurité externes qu'à leurs notes d'informations internes. Si les processus de sécurité mis en place par les équipes de sécurité de ces entreprises démontrent un niveau de maturité satisfaisant, ces dernières doivent continuer de privilégier des solutions intégrées plutôt que de s'appuyer sur des produits de sécurité redondants. Dans la mesure où les cybercriminels cherchent de plus en plus à voler directement des fonds, comme en témoignent l'augmentation du nombre de chevaux de Troie dans les applications bancaires mobiles, le vol subi par la banque centrale du Bangladesh par le biais du réseau SWIFT et la compromission des comptes Tesco Bank, elles devraient peut-être également se concentrer davantage sur les nouvelles menaces et les risques de pertes financières réelles plutôt que sur les risques d'atteinte à la réputation.

Enseignements à tirer du marché cybercriminel	Marché cybercriminel	Application à la cybersécurité
Exploitation des forces du marché	**Cybercriminalité en tant que service**	**Sécurité en tant que service**
	Ouvert et décentralisé, le marché cybercriminel exploite la concurrence et la fixation des prix par le marché pour réduire les barrières à l'entrée, favoriser l'innovation et aider les entreprises fructueuses à se développer rapidement.	Le recours accru à l'externalisation et à la sous-traitance ouverte peut contribuer à réduire les coûts, à accroître la concurrence et à favoriser la généralisation de technologies et pratiques de sécurité efficaces.
Utilisation des divulgations publiques	**Ciblage des vulnérabilités divulguées publiquement**	**Amélioration des pratiques d'application de patchs**
	L'exploitation de vulnérabilités mises au jour permet d'éviter les coûts liés à leur recherche et au développement d'exploits, et d'intégrer rapidement les nouvelles divulgations dans les attaques afin d'en profiter au maximum avant l'application de patchs.	Une réaction accélérée aux divulgations publiques de vulnérabilités par la mise en œuvre de pratiques de correction plus efficaces et le remplacement plus rapide des anciens systèmes peut renforcer la sécurité et augmenter le coût des attaques pour les cybercriminels.
Amélioration de la transparence	**Forums ouverts et publicité en ligne**	**Partage d'informations et collaboration**
	Les forums ouverts et la publicité en ligne favorisent la prolifération et le succès des nouvelles attaques et des nouveaux modèles économiques adoptés par les cybercriminels, ainsi que la généralisation des meilleures pratiques.	La généralisation du partage d'informations peut contribuer à diminuer les coûts encourus par les équipes de sécurité en réduisant la duplication, et à faire connaître les technologies et pratiques offrant des améliorations significatives de la sécurité.
Réduction des barrières à l'entrée	**« Toute personne maîtrisant l'outil informatique »**	**Exploitation des talents du monde entier**
	Ignorant les qualifications officielles et les contraintes géographiques, l'écosystème cybercriminel peut dévoyer les talents sous-évalués de l'économie légitime et maximiser leur valeur.	Le recours à des talents internationaux issus de couches démographiques et de milieux divers peut permettre aux entreprises de pallier la pénurie de compétences en cybersécurité et de détourner ces talents du marché cybercriminel.
Alignement des incitants	**Récompense des performances par les marchés indépendants**	**Incitation à la performance**
	Le marché cybercriminel indépendant récompense l'excellence à tous les niveaux et dans tous les domaines fonctionnels de la chaîne d'attaque, et pénalise les performances insuffisantes.	Pour renforcer la motivation à tous les échelons, des dirigeants aux exécutants, des incitants tels que des primes et des distinctions honorifiques doivent être proposés aux employés et aux responsables qui assurent une sécurité efficace.

En savoir plus

Pour plus d'informations sur le décalage des incitants en matière de cybersécurité, notamment une ventilation par pays et par secteur, téléchargez le rapport complet **Le décalage des incitants, ou pourquoi les cybercriminels ont une longueur d'avance**.

McAfee™
Together is power.

11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr