Déséquilibre des forces : comment le décalage des incitants nuit à la cybersécurité

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 toujours une longueur d'avance sur leurs victimes, non pas parce qu'ils sont meilleurs, mais en raison d'un décalage entre les incitants des pirates et des responsables de la sécurité. Pour vous aider à mieux cerner ce décalage, nous avons interrogé 800 professionnels de la cybersécurité issus de cinq grands secteurs d'activité. Le rapport identifie 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.

Trois niveaux de décalage en matière d'incitants qui placent les équipes de sécurité en position de faiblesse

Cybercriminels contre professionnels de la sécurité	Les incitants des pirates trouvent leur origine dans un marché fluide et décentralisé, favorisant l'agilité et la rapidité d'adaptation, tandis que les professionnels de la sécurité sont entravés par la bureaucratie et par un modèle décisionnel descendant.
Stratégie contre implémentation	Bien que plus de 90 % des entreprises aient défini une stratégie de cybersécurité, moins de la moitié l'ont implémentée dans son intégralité.
Cadres contre exécutants	Les cadres dirigeants qui conçoivent les stratégies de cybersécurité mesurent le succès différemment des responsables de l'implémentation, limitant ainsi leur efficacité.

intel Security

Structure d'entreprise contre entreprise criminelle

Si les cibles de la plupart des cyberattaques sont généralement des entreprises régies par une organisation hiérarchique et bureaucratique, les cybercriminels opèrent quant à eux dans un monde clandestin mais ouvert, peuplé d'électrons libres motivés par des incitants clairs. Le marché de la cybercriminalité répond aux signaux envoyés par les prix en innovant et en proposant chaque jour de nouveaux produits et services. Lorsque le potentiel des anciennes fonctionnalités est épuisé, des solutions de rechange sont rapidement mises en ligne. Cela favorise une concurrence dynamique et une innovation rapide entre les différents acteurs du marché de la cybercriminalité, des cybercriminels particulièrement ingénieux ou des groupes financés par un État aux cyberactivistes et aux utilisateurs de la cybercriminalité sous forme de service. Dans le cadre de cette étude, nous avons interrogé des experts techniques en cybersécurité et des représentants des forces de l'ordre afin de mieux cerner ces marchés.

Les marchés de la cybercriminalité regorgent de spécialisations en tous genres, qui permettent aux pirates professionnels de parfaire leurs compétences. Les spécialisations les plus courantes sont les suivantes : programmeurs de logiciels malveillants, concepteurs de sites web malveillants, experts en infrastructure, experts en exploits et vulnérabilités et escrocs spécialisés dans la conception de techniques d'ingénierie sociale. Les spécialistes se partagent les profits à hauteur de leur contribution. La concurrence dynamique et les informations sur la réputation éliminent constamment du jeu les pirates les moins compétents et hissent les meilleurs au sommet.

L'un des principaux effets de ce modèle de concurrence et de compensation directes est la vitesse à laquelle les nouveaux exploits et vulnérabilités sont mis à profit. 42 % des vulnérabilités sont exploitées par les criminels dans les 30 jours suivant leur détection. Par exemple, lorsque les développeurs du kit d'exploits Angler (qui était autrefois dominant et représentait, d'après une estimation, 82 % de l'activité des kits d'exploits de l'époque) ont été arrêtés, il n'a fallu que quelques semaines aux pirates pour se tourner vers le kit d'exploits Neutrino afin de distribuer leurs charges actives. La plupart des pirates n'effectuent que peu de recherches, voire aucune, préférant tirer parti du travail des cybercriminels de haut vol, souvent distribué rapidement via les marchés du Web clandestin (Dark Web), ainsi que des nombreux systèmes corrigés bien trop tardivement. Cette approche a en outre l'avantage de limiter leurs coûts.

Les anecdotes concernant la cybercriminalité laissent penser que de nombreux cybercriminels proviennent de Russie et d'Europe de l'Est. Ce n'est pas entièrement faux, principalement en raison de la multitude de programmes mathématiques et informatiques avancés disponibles, et du manque d'opportunités d'emploi légitime. Même les employés légitimes des entreprises informatiques et de télécommunications de ces régions travaillent souvent au noir en tant que cybercriminels, allant même parfois jusqu'à publier ouvertement sur leur page Facebook l'identité qu'ils utilisent sur le Web clandestin. Les équipes de cybersécurité des entreprises ont beaucoup à apprendre de ces marchés clandestins. Des incitants clairs et des distinctions honorifiques peuvent avoir un impact positif considérable sur l'état d'esprit et l'efficacité.

Décalage entre stratégie et implémentation

D'après la majorité des répondants, la cybersécurité représente désormais le principal risque auquel les entreprises sont exposées. Plus de 70 % des dirigeants sont aujourd'hui informés des risques en matière de cybersécurité lors des réunions du conseil d'administration, et sont en particulier mis au fait de difficultés qui ne figuraient même pas parmi les dix préoccupations principales il y a à peine six ans. La quasi-totalité d'entre eux (93 %) ont indiqué que leur entreprise dispose d'une stratégie de cybersécurité destinée à contrer les menaces existantes et émergentes.

C'est ici qu'apparaît le premier décalage. De nombreux dirigeants estiment que leur stratégie est implémentée dans son intégralité au sein de l'entreprise, mais seuls 30 % des opérateurs partagent cet avis. Pour les deux groupes, le nombre de compromissions constitue la principale mesure de l'efficacité de la cybersécurité, mais leurs avis divergent en ce qui concerne les autres mesures. Les cadres dirigeants s'appuient essentiellement sur les mesures de performances, telles que le coût de reprise à la suite d'une compromission ou le retour sur les dépenses en matière de cybersécurité. Les opérateurs s'appuient davantage sur des mesures techniques, telles que les analyses des vulnérabilités et les tests d'intrusion. Plus de la moitié (54 %) des cadres dirigeants interrogés sont davantage préoccupés par l'impact sur la réputation que par les effets réels d'un incident de cybersécurité. Le fait que moins d'un tiers (32 %) de ces professionnels pensent qu'un incident de cybersécurité entraîne une perte de revenus ou de bénéfices est assez inquiétant car cela peut leur donner un sentiment de sécurité trompeur.

Il existe un autre décalage entre la stratégie et l'implémentation, qui concerne les méthodes utilisées pour s'assurer que les mesures de cybersécurité n'exposent pas l'entreprise à de nouveaux risques. Si la majorité des répondants (71 %) ont indiqué avoir mis en place une plate-forme de sécurité intégrant à la fois des technologies existantes et nouvelles, 64 % ont déclaré se doter également de technologies redondantes. Bien que cette stratégie d'implémentation puisse sembler judicieuse, les technologies redondantes qui ne sont pas suffisamment intégrées peuvent parfois engendrer des failles de sécurité dans la mesure où une configuration et des systèmes de surveillance différents peuvent entraver la création et la mise en œuvre de stratégies de sécurité cohérentes.

Des incitants différents pour les cadres 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. Notre étude montre non seulement qu'il manque d'incitants pour les professionnels de la sécurité, mais également que les dirigeants sont davantage confiants dans les effets des incitants existants que le personnel opérationnel qu'ils tentent motiver.

Près de la moitié des opérateurs interrogés ont déclaré que leur entreprise ne proposait aucun incitant, soit plus de cinq fois plus que le nombre de dirigeants ayant signalé cet état de fait. Il est possible que les employés situés aux échelons inférieurs de la structure organisationnelle ignorent l'existence d'incitants liés aux performances, ou qu'ils ne les considèrent pas comme efficaces. Heureusement, près de 65 % des professionnels interrogés ont fait état d'une motivation personnelle à renforcer les cyberdéfenses de leur entreprise.

Les dirigeants qui ont mentionné l'existence d'incitants pour les professionnels de la cybersécurité ont principalement mis en avant les compensations financières (60 %) et la reconnaissance (58 %). Ces mêmes incitants n'ont toutefois été cités par le personnel non dirigeant que dans une proportion moindre (15 à 25 % de moins). Interrogés sur la nature des incitants qu'ils aimeraient se voir proposer, les opérateurs ont donné quasiment le même poids aux compensations financières (63 %) et à la reconnaissance ou à une distinction honorifique (62 %). Ces résultats confirment les observations d'autres études qui montrent que les opportunités de développement professionnel sont aussi, voire plus appréciables que les primes.

Les enseignements à tirer de la cybercriminalité

Les entreprises peuvent s'inspirer des cyberpirates pour corriger ces décalages. La sécurité sous forme de service peut offrir la flexibilité nécessaire pour contrer la cybercriminalité sous forme de service. Des consultants spécialisés peuvent renforcer l'équipe interne en apportant leur expertise et des ressources ciblées, le cas échéant. Des incitants liés aux performances et une reconnaissance honorifique peuvent favoriser un renforcement des défenses et l'accélération des cycles de correction. Une certaine expérimentation est nécessaire pour trouver le parfait équilibre entre mesures de l'efficacité et incitants pour chaque entreprise, mais l'amélioration de la réactivité et de la cohérence des mécanismes de protection, de même que des performances de la sécurité sont à la portée de chacune.

Enseignements à tirer du marché criminel	Marché criminel	Professionnels de la sécurité
Exploitation des forces du marché	**Cybercriminalité sous forme de service** Ouvert et décentralisé, le marché criminel tire parti de la concurrence et des prix du marché pour élargir l'accès, encourager l'innovation et aider les projets fructueux à prendre rapidement de l'ampleur.	**Sécurité sous forme de service** Le recours accru à l'externalisation et aux travailleurs indépendants peut contribuer à réduire les coûts, à renforcer la concurrence et à favoriser la généralisation de technologies et pratiques de sécurité efficaces.
Utilisation des divulgations publiques	**Ciblage des vulnérabilités divulguées publiquement** 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 leur correction par les équipes de sécurité.	**Amélioration des pratiques de correction** 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 pirates.
Amélioration de la transparence	**Forums ouverts et publicité en ligne** Les forums ouverts et la publicité en ligne favorisent la prolifération des nouvelles attaques et des modèles économiques fructueux adoptés par les cybercriminels, ainsi que la généralisation des meilleures pratiques.	**Partage d'informations et collaboration** La généralisation du partage d'informations peut contribuer à réduire 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.
Ouverture de l'accès au marché	**« Tout détenteur de connaissances informatiques »** En l'absence de diplômes ou autres qualifications officielles et de contraintes géographiques, l'écosystème criminel peut attirer les talents sous-évalués par l'économie légitime afin de tirer au maximum profit de leurs compétences.	**Exploitation des ressources du monde entier** L'extension du vivier de compétences, par exemple en ouvrant la porte aux jeunes générations et aux experts en TIC étrangers qui basculent souvent dans la cybercriminalité, peut contribuer à pallier la pénurie de compétences pour les entreprises, en plus de priver les marchés criminels de ces talents.
Ajustement des incitants	**Récompense des performances par les marchés indépendants** Sur le marché des cybercriminels indépendants, les opérateurs de tous les niveaux et de tous les domaines fonctionnels de la chaîne d'attaque voient leur excellence récompensée par le marché, et leur médiocrité pénalisée.	**Incitants liés aux performances** Pour renforcer la motivation à tous les échelons, des dirigeants aux opérateurs, des incitants tels que des primes et des distinctions honorifiques doivent être proposés aux employés et aux responsables qui assurent une protection performante.

Pour plus d'informations sur le décalage en matière d'incitants dans le domaine de la cybersécurité, notamment une ventilation par pays et par secteur d'activité, téléchargez le rapport complet, Déséquilibre des forces : comment le décalage des incitants nuit à la cybersécurité, publié par le CSIS (Center for Strategic and International Studies) en mars 2017.

intel Security

McAfee. Part of Intel Security.
Tour Pacific
13, Cours Valmy - La Défense 7
92800 Puteaux
France
+33 1 47 62 56 09 (standard)
www.intelsecurity.com

2480_0217_exe-misaligned-tilting-playing-field
Mars 2017