Etude Globale sur les comportements de Sécurité 2021, réalisée par CrowdStrike

Cette étude annuelle a pour but de comprendre et d'exposer le comportement des professionnels de la sécurité, selon plusieurs axes parmi lesquels :

- La défense face aux ransomwares ou « rançongiciels », et les coûts d'une attaque par ransomware qui n'aurait pas été freinée et serait parvenue jusqu'au chiffrement
- La capacité des entreprises à respecter le triptyque des SLA CrowdStrike « **1-10-60** » pour « **détecter en 1 minute, enquêter et investiguer en 10 minutes, et résoudre en 60 minutes** » avant que l'attaquant ne parvienne à effectuer des mouvements latéraux, conformément à la phase d'attaque définie par MITRE ATT&CK.

En surface, le but ultime des professionnels de la cybersécurité est très simple : s'assurer que leur organisation est en sécurité en empêchant les intrus de la pénétrer. En réalité, il y a tellement d'éléments à prendre en compte pour ce faire, que cet objectif devient de plus en plus difficile à atteindre. Il est impossible de tout contrôler, en terme d'utilisateurs, d'accès, d'outils applicatifs, d'authentification ou encore de processus.

Du point de vue des attaquants, le paysage des menaces évolue sans cesse, notamment avec la mutation des vecteurs connus comme le ransomware ou les attaques de supply chain vers plus de sophistication et de furtivité – attaques « fileless », sans fichier et donc plus difficiles à détecter. Le rapport de force est en faveur des attaquants si l'on considère que les équipes de DSI / RSSI des entreprises de taille petite à intermédiaire sont moins nombreuses et moins focalisées que les groupes d'assaillants.

Du point de vue des équipes IT, le défi est autre : il y a deux ans, on ne prévoyait pas le changement de paradigme qui allait propulser le travail à distance en tête des projets de migration. La crise du COVID-19 a accéléré de manière fulgurante l'adoption du poste de travail distant, élargissant ainsi de façon considérable la surface d'attaque potentielle.

Les équipes IT, d'une manière globale, nagent contre le courant depuis bien longtemps, notamment lorsque l'on considère par exemple les ressources limitées dont elles disposent, et le déséquilibre entre l'offre et la demande en terme de recrutement. Là où les cybercriminels utilisent des techniques de pointe et emploient des équipes de plus en plus étoffées, les responsables de sécurité doivent gérer des milliers d'alertes quotidiennes, au moyen d'outils ne répondant pas toujours aux dernières exigences technologiques. On trouve là une des explications du nombre sans cesse grandissant d'attaques avérées.

Au vu de ce constat, le défi qui s'impose est de répondre, par les mesures adéquates et sans tarder, à la menace qui pèse assurément sur les entreprises. Il faut réduire la probabilité de devenir la prochaine victime d'un groupe étatique ou d'une équipe indépendante et plus opportuniste. Alors même que les adversaires deviennent capables d'outrepasser les outils de sécurité historiques, il devient important de combiner une technologie de pointe avec une expertise humaine, pour détecter et enrayer les menaces sophistiquées d'aujourd'hui.

CrowdStrike a conduit une étude sous forme de questionnaire auprès de 2200 cadres et responsables de la sécurité informatique entre septembre et novembre 2021. Le panel s'étend de la zone Amériques à l'Asie Pacifique en passant par l'Europe et l'Afrique. Les entreprises interrogées sont composées d'au moins 100 collaborateurs.

63%

Admettent que leur entreprise perd confiance dans les éditeurs à mesure que les incidents se produisent

96%

De celles qui ont payé la rançon initiale ont dû subir une extorsion supplémentaire au moment de récupérer leurs données

45%

Ont eu à subir au moins une attaque logicielle sur leur chaîne d'approvisionnement au cours des 12 derniers mois, contre 32% en 2018

Seulement 36%

Ont réalisé un audit sur leurs dispositifs de sécurité en place, et exploré les solutions disponibles sur le marché

84%

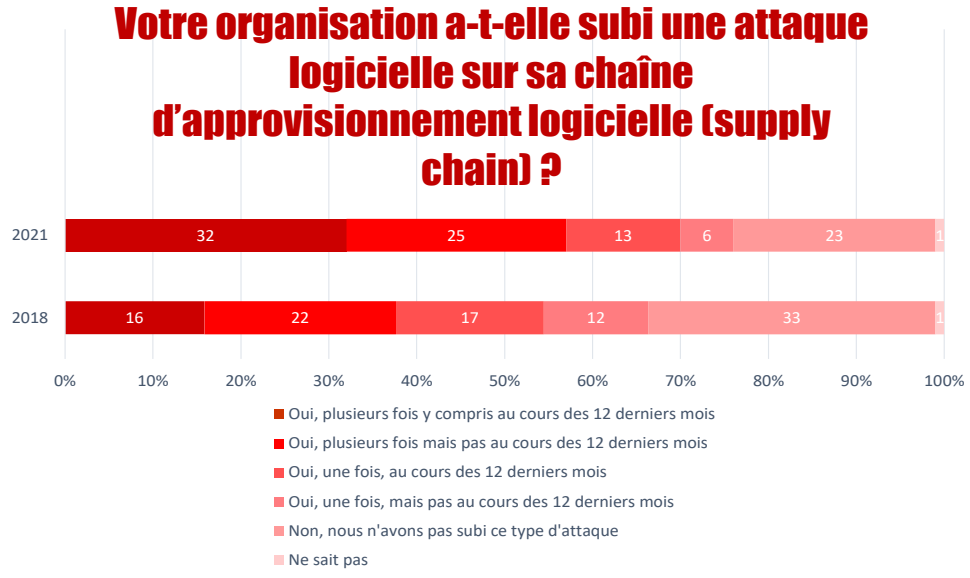
Pensent que les attaques logicielles visant la chaîne d'approvisionnement (Supply Chain Attacks) pourraient devenir l'une des plus grandes menaces envers les entreprises semblables à la leur dans les 3 prochaines années

66%

Ont subi au moins une attaque par ransomware au cours des 12 derniers mois

Voici ce que l'étude révèle :

- L'accélération des attaques sur la chaîne d'approvisionnement logicielle, dont on peut citer en exemple les attaques Kaseya ou Sunburst, provoque une baisse de confiance envers les dispositifs historiques de défense. Ce type d'attaque s'est produite pour 77% des personnes interrogées, contre 66% en 2018. De plus, 45% déclarent que leur entreprise a souffert d'une attaque sur leur chaîne d'approvisionnement au cours des 12 mois précédents, contre 32% en 2018.
  Et bien que ce type d'attaque soit fréquent, 59% admettent que lorsqu'elles ont subi ce type d'attaque pour la première fois, elles ne disposaient pas d'une stratégie de réponse adaptée ou même coordonnée.



- Les attaques par Ransomware (ou « Rançongiciel ») demeurent une menace persistante, et les coûts qui y sont associés vont grandissant. Au cours des deux dernières années, beaucoup de choses ont changé pour les entreprises à travers le monde, mais le danger que représentent les Ransomware n'a pas fléchi. On peut dire que ce type d'attaque a été le plus fructueux dans l'Histoire récente.
- Et alors que les équipes de cybersécurité continuent de s'adapter aux nouveaux usages et aux environnements hybrides, on peut penser que les attaquants qui utilisent ce type de technique ont encore quelques belles années d'avance. Il est donc logique qu'il représente la principale inquiétude (44%) pour les entreprises quand on leur demande de citer les menaces qu'ils redoutent le plus pour les 12 prochains mois. Ce chiffre est aligné avec les résultats des études sur 2019 et 2018, mais en baisse par rapport à 2020, où il était de 54%.
- Cela veut-il dire que les entreprises sont préparées à répondre efficacement à une attaque par Ransomware ? Pour faire court, la réponse est clairement « Non ». Les deux tiers des entreprises interrogées admettent avoir été victimes d'une attaque par Ransomware au cours des douze derniers mois – alors que ce chiffre était de 56% en 2020. Plus inquiétant, 33% ont subi plusieurs attaques lors des douze derniers mois, contre 24% l'année passée.
- Que la rançon soit payée ou non, ce type d'attaque cause une monopolisation des ressources, un sentiment de vulnérabilité face à des attaques qui se révèlent parfois incessantes, un certain stress et un impact négatif en terme de réputation. Sans parler de conséquences possibles sur la carrière d'un employé qui aurait permis le déclenchement de l'attaque, ou d'un responsable qui aurait pu négliger l'importance de la protection contre de telles menaces.
- Une fois ce constat établi, il est primordial pour une entreprise touchée, de procéder aux ajustements nécessaires afin de se prémunir contre de prochaines attaques du même type. Pour **60%** des entreprises ayant subi une attaque au cours des 12 derniers mois, des mesures ont été prises et des investissements déclenchés afin de réduire le risque, et **58% ont étoffé leurs équipes de sécurité** dans le même but.
- Quoi qu'il en soit, presqu'un quart (24%) ont fini par payer la rançon réclamée, un chiffre similaire à 2020 (27%). Cependant, le montant des rançons a augmenté de **63% entre 2020 et 2021**, passant de **1.10 million** de dollars US à **1.79 million** de dollars US.
- Bien malheureusement, pour la vaste majorité (96%) des entreprises ayant payé la rançon, leur mésaventure ne s'est pas arrêtée là, car elles ont dû payer des frais supplémentaires estimés à **792 000 dollars**, en moyenne.
- **57%** des entreprises attaquées admettent qu'elles n'avaient pas mis en place de stratégie globale et complète pour répondre à ce type d'attaque.

57%

De celles qui ont subi une attaque par ransomware n'avaient pas établi de stratégie de remédiation afin de coordonner leur réaction

En moyenne

Les personnes interrogées estiment qu'il leur faudrait **146 heures** pour détecter un incident de cybersécurité, contre 117 en 2020 et 120 en 2013

En plus du temps de détection

On estime que les organisations mettraient **11 heures** à catégoriser, comprendre et investiguer sur l'attaque, et **16 heures** pour la contenir et y remédier

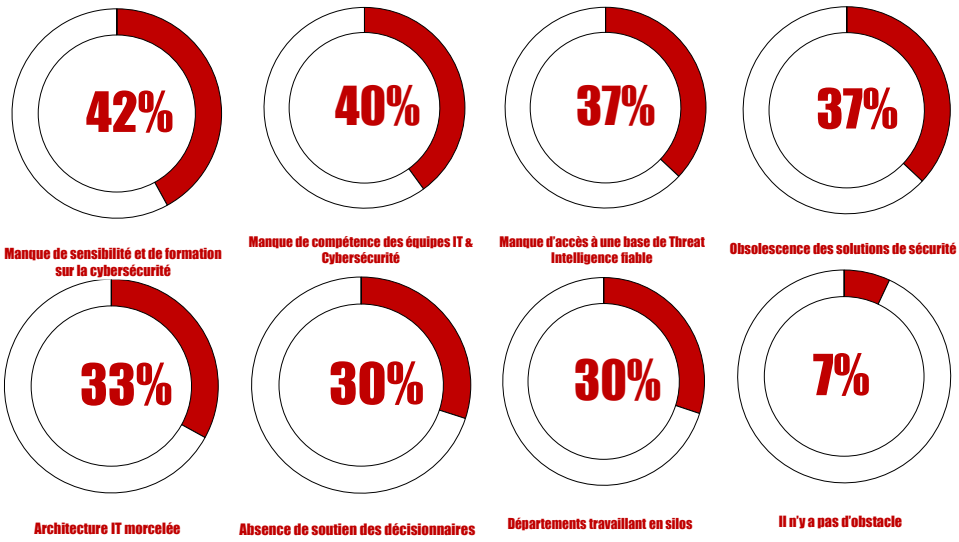
69%

Ont subi un incident de cybersécurité directement lié au travail à distance

Comment se prémunir plus efficacement face aux attaques ?

- A l'avenir, il est important, voire impératif, que les entreprises améliorent leurs systèmes de défense, car la question n'est plus de savoir « **si** » une attaque va se produire, mais plutôt « **quand** ». Et les équipes ne doivent pas faire face uniquement à des attaques frontales en terme de Ransomware. Ce dernier peut pénétrer à partir de plusieurs points de la chaîne d'approvisionnement, et les élévations de privilège permettent aux attaquants de rapidement acquérir une facilité de mouvement à l'intérieur du réseau. Plus des deux tiers (**69%**) admettent que si une attaque survenait et paralysait leur chaîne d'approvisionnement, et qu'une partie de leurs données se trouvait cryptée, ils réfléchiraient sérieusement à **payer la rançon** pour mettre fin à la menace.
- Cependant, même si le Ransomware paraît quelque peu inexorable, et en admettant comme un fait établi qu'il est crucial de réfléchir à une stratégie de récupération (recovery plan), les entreprises sont encouragées à rechercher et déployer les moyens de se prémunir de façon proactive contre ce type d'attaque, afin d'éviter qu'elles ne percent leurs défenses. Cela implique des choix stratégiques : 93% des entreprises ayant participé à l'étude avouent qu'il existe au moins un obstacle organisationnel à l'établissement d'une stratégie efficace contre le ransomware.
- Il est clair que les organisations doivent adresser le sujet de la cybersécurité, et notamment la formation et la sensibilité aux sujets de cybersécurité de leurs membres (42%) ainsi que la compétence de leurs équipes IT (40%), afin de changer leur posture face aux cybermenaces, et remettre la sécurité au premier plan. Le graphique ci-dessous permet d'identifier les sujets perçus comme des freins à l'établissement durable d'une politique de sécurité efficace.
- La posture face aux attaques ne sera pas améliorée sans un travail sur les infrastructures consacrées à la cybersécurité. Accéder et utiliser avec pertinence des bases de threat intelligence (bases de connaissances liées par exemple aux cybermenaces, aux groupes d'attaquants et à leur comportement) peut représenter un bond en avant pour 37% des personnes ayant répondu à l'étude.

Lequel des obstacles suivants se dresse devant vous lorsqu'il est question d'établir une posture de sécurité contre les attaques par ransomware ?



Quel avenir pour les attaques par Ransomware ?

- Le Ransomware est bel et bien là, et il a même de beaux jours devant lui. Une période tourmentée telle que les deux années qui viennent de s'écouler est propice à la multiplication des attaques, les équipes IT étant occupées notamment à mettre en place le télétravail. Et les conséquences vont au-delà du paiement de la rançon, il en va de la réputation de l'entreprise, de la confiance que ses clients lui apportent, et de sa pérennité.
- Dans un monde idéal, les entreprises doivent être capables de réagir selon la devise de CrowdStrike « **1-10-60** » qui définit le temps imparti à chaque étape de la défense contre une attaque cyber : **1** minute pour détecter, **10** minutes pour investiguer et **60** minutes pour remédier à l'attaque.
- Si l'on doit retenir un aspect positif à la crise du Covid-19, on notera que celle-ci a propulsé la cybersécurité au premier plan des sujets cruciaux à la survie des entreprises. Pour **86%** des interrogés, le Covid-19 a représenté un virage significatif pour la cybersécurité pour cette raison précise, et l'on réalise aujourd'hui l'importance de ce poste. Cela constitue une nouvelle positive pour les équipes IT, et l'on constate que les investissements sur la cybersécurité ont de nouveau la faveur des décisionnaires.

La proposition d'Exaprobe

Le constat est donc sans appel : les cyberattaquants ont un coup d'avance sur les entreprises en terme d'investissement, d'effectifs et de stratégie. Nous faisons face à des organisations dont le métier est de lancer des attaques sur les entreprises dans le monde entier. Celles-ci n'ont souvent pas les moyens d'embaucher un ou deux spécialistes dédiés sur le sujet. Le combat est donc inégal de prime abord.

Mais nous avons les moyens de nous défendre efficacement :

D'une part, CrowdStrike propose des outils éprouvés et reconnus permettant de renforcer efficacement la sécurité des endpoints (PC et serveurs).

D'autre part, Exaprobe permet de protéger le système d'information, de superviser les évènements et de remédier aux alertes avérées, agissant comme le feraient les membres d'une équipe IT dédiée au sein de l'entreprise, et ce en heures ouvrées comme non-ouvrées. Le coût lié à ce poste est donc bien moins inférieur au déploiement d'une équipe de cybersécurité « en propre ». Exaprobe propose en effet, grâce à l'offre Go4Detect, basée sur la technologie **Falcon** de **CrowdStrike**, de surveiller et de remédier aux attaques pour **1€** par utilisateur et par mois. Et grâce à une méthode de déploiement éprouvée et basée sur des solutions 100% Cloud, nos équipes peuvent rendre une solution opérationnelle en **1 mois** environ.

Contactez-nous dès aujourd'hui pour discuter ensemble du renforcement de votre politique de sécurité !