Audits externes de sécurité informatique

Les intrusions sur commande

Les audits de sécurité sont incontournables pour détecter les failles de ses systèmes d'information… et pour souscrire une assurance contre les cyber-risques

©Freepik

Les menaces informatiques ne cessent de se multiplier. Poussées par une prise de conscience et par des réglementations toujours plus contraignantes, les entreprises cherchent de plus en plus à se protéger contre les cyber-risques. Que ce soit en se dotant de défenses efficaces et/ou en souscrivant une assurance cyber. Mais dans les deux cas, il convient au préalable de réaliser un audit de sécurité afin de détecter les failles et les axes de progression du système informatique. Celui-ci peut aller du simple questionnaire jusqu'au recours à un hacker éthique, mais ils doivent toujours être pratiqués avec doigté.

FABIEN HUMBERT

L'actualité ne cesse de mettre sur le devant de la scène les cyber-risques qui menacent les entreprises. En 2017, c'est le virus ransomware WanaCry qui montrait à quel point les entreprises et même les administrations (le système de santé britannique NHS a notamment été touché), pouvaient être vulnérables face aux périls venus du net. En 2018, c'étaient les données de 29 millions d'utilisateurs de Facebook qui étaient piratées. Et il ne s'agit là que de deux exemples frappants et d'ampleur, qui font pourtant figure de goutte d'eau dans un océan d'incidents informatiques.

"Selon une étude du cabinet PWC, en 2017, 76 % des entreprises de taille intermédiaire ont déjà eu une attaque d'envergure et 23 % des pertes financières. Il ne s'agit plus d'un risque probable, mais certain" estime Pierre Lorcy, fondateur de Lorcyber.

Les marchés jumeaux de la sécurité informatique et de l'assurance contre les cyber-risques sont en progression dans l'Hexagone

À ceci vient s'ajouter le règlement RGPD, qui sensibilise les entreprises à la nécessaire sécurisation des données personnelles qu'elles détiennent. Avec à la clé de des sanctions lourdes pouvant aller jusqu'à 4 % du CA annuel mondial ou 20 millions d'euros en cas de négligence coupable. Résultat: si certaines entreprises font encore l'autruche, la grande majorité est désormais consciente des risques encourus en cas d'attaque informatique. C'est pourquoi les marchés jumeaux de la sécurité informatique et de l'assurance contre les cyber-risques sont en progression dans l'Hexagone.

"Le marché a réellement démarré il y a 5 ou 6 ans avec les grandes entreprises qui sont les plus exposées, comme les institutions financières et la grande distribution, se souvient Jérôme Gossé, responsable de la souscription cyber-risque pour l'Europe continentale chez l'assureur Chubb. *Aujourd'hui, toutes les entreprises de tous les secteurs sont concernées car toutes utilisent des systèmes d'information pour exercer leur activité et toutes possèdent des données personnelles, ne serait-ce que celles de leurs employés."*

Questionnaires déclaratifs

La première chose à faire lorsqu'une entreprise prend conscience de sa vulnérabilité, ou lorsque son assureur le lui demande, c'est de commander un audit de ses défenses et de ses failles. Dans la pléthore de spécialistes de la sécurité informatique, certains ont une double, voire une triple casquette, car outre des audits, ils font aussi de la formation, proposent leurs services pour intervenir en cas d'attaque ou vendent des logiciels censés les prévenir, ou au moins les limiter. On pourrait donc les soupçonner de livrer une version catastrophiste de la situation

"Être catastrophiste et trop insistant pour vendre des solutions après un audit peut paradoxalement conduire les entreprises à ne rien faire pour se protéger." Guillaume de Lavallade, Hub One.

"Afin de proposer une offre à un futur assuré, nous travaillons sur un questionnaire très précis afin de comprendre le degré de maturité quant aux risques informatique." Jérôme Gossé, Chubb.

après l'audit pour mieux vendre leurs autres services… *"Être catastrophiste en termes de dégâts potentiels d'une attaque cyber, et trop insistant pour vendre des solutions après un audit, peut paradoxalement conduire les entreprises à ne rien faire pour se protéger"*, prévient Guillaume de Lavallade, directeur général de Hub One. Il existe différents types d'audits de sécurité. Il y a d'abord l'audit déclaratif, qui est communément fait par les assureurs. *"Afin de proposer une offre à un futur assuré, nous travaillons sur un questionnaire très précis afin de comprendre le degré de maturité quant aux risques informatiques,* explique Jérôme Gossé. *Les questions porteront sur l'organisation des systèmes d'information, l'architecture, la gouvernance, la politique de sauvegarde, la formation des salariés aux cyber-risques, et si des audits de sécurité et des tests de pénétration sont faits de manière régulière."* Ici, les questions posées par l'assureur vont pousser l'entreprise à se questionner sur ce qu'elle a réellement mis en place pour se protéger. Certains assureurs iront plus loin et demanderont un audit de sécurité plus poussé pour mieux cerner leur futur client, tandis que certaines entreprises le feront d'elles-mêmes parce qu'elles ont été sensibilisées par des conférences, des campagnes des pouvoirs publiques, ou par les médias.

Certaines entreprises vont plus loin encore dans la détection des failles éventuelles de leur réseau informatique. Il s'agit alors de confier à des hackers éthiques la tâche d'entrer dans le système

Tests de pénétration et hackers éthiques

Un niveau supérieur d'audit consiste à pratiquer des scans de vulnérabilité, ou tests d'intrusion. *"Nous allons chercher à scanner tous les ports et routeurs de l'entreprise depuis l'extérieur, afin de voir si nous parvenons à récupérer des mots de passe, des adresses mails…"*, explique Guillaume de Lavallade. Ces tests peuvent être pratiqués par des ingénieurs informatiques, ou être semi-automatisés. Ils peuvent aussi être couplés avec des tentatives d'intrusion physiques. *"Dans ce cas de figure, nous allons chercher à entrer dans les locaux de l'entreprise en racontant des histoires à certains salariés (comme les vigiles), afin de nous connecter au réseau depuis l'intérieur"*, révèle celui-ci.

Dans tous les cas, l'entreprise qui pratique l'audit a bien sûr signé un accord de confidentialité et agit avec un mandat de son client. Ces tests de pénétration peuvent durer de une à plusieurs semaines. *"Lorsque cela en vaut la peine, certains attaquants peuvent passer plusieurs semaines, voire plusieurs mois, à tenter de trouver des failles dans la sécurité informatique de leur cible,* prévient Pierre Lorcy, *il faut prendre cela en compte lorsqu'on prévoit la durée du 'pentest' [test de pénétration, ndlr]."*

Le test d'intrusion est le moyen le plus fréquent utilisé lors d'un audit de sécurité, mais certaines entreprises veulent aller plus loin encore dans la détection des failles éventuelles de leur réseau informatique. Il s'agit alors de confier à des hackers éthiques la tâche d'entrer dans le système. *"Nous utilisons alors le terme de sécurité offensive",* précise Guillaume de Lavallade. Certains acteurs, comme Hub One, ont leurs propres hackers éthiques, formés en continu aux nouvelles menaces et *"maintenus dans un état de motivation permanent".*

Mais il existe aussi des plateformes de "bug bounty", où fraient des hackers éthiques indépendants. Ceux-ci ne sont payés que s'ils trouvent des failles particulièrement graves et compliquées, et ont donc les crocs particulièrement acérés. Certaines entreprises sont abonnées à l'année à des plateformes, c'est-à-dire qu'elles sont en permanence auscultées par des petits génies qui cherchent le moindre défaut de leur cuirasse. Cependant seuls les grands groupes ou les start-up du web ayant réussi peuvent se payer les services d'une plateforme de bug bounty. Les PME auront avantage à se rabattre sur les tests de pénétration, moins onéreux mais déjà très complets. Un audit semi-automatisé coûte plusieurs centaines d'euros, un audit en profondeur plusieurs dizaines de milliers d'euros et jusqu'à plusieurs millions pour des examens plus poussés encore sur une plateforme de bug bounty.

Un audit demande de la diplomatie

Dans tous les cas, mieux vaut faire appel à un prestataire extérieur lorsqu'on veut auditer sa sécurité cyber, même lorsqu'on possède un service informatique en interne. *"On ne peut pas être juge et partie,* explique Pierre Lorcy. *Un audit externe permet d'avoir à disposition des preuves fiables, mais il n'exempte pas l'entreprise de faire des audits internes, importants pour la gestion au quotidien. Les deux se complètent."*

Il faut aussi savoir gérer avec doigté cette intrusion d'une entreprise étrangère dans le pré carré de la direction informatique, lorsqu'il en existe une au sein de l'entreprise. Car pour un DSI, il n'est jamais agréable de voir que son système est faillible. Or *"les systèmes sont toujours plus ou moins vulnérables compte tenu de l'évolution constante des menaces. Il est rare de ne rien trouver"*, prévient Pierre Lorcy.

Et une fois que les failles ont été, inévitablement, révélées, comment réagir ? *"Au sein des grands groupes, certains DSI peuvent parfois sembler sur la défensive, or nous ne sommes pas là pour les juger, mais pour apporter aux débats le fruit de notre expérience sinistre, mettre en lumière les vulnérabilités d'exposition et aider à définir les axes prioritaires d'amélioration possible"*, rappelle Emmanuel Silvestre, senior vice-président risques financiers chez l'assureur Liberty. Et les entreprises, que font-elles après un audit ? *"Une entreprise qui demande un test d'intrusion a déjà pris conscience qu'elle était faillible, elle va donc prendre les mesures nécessaires,* estime Guillaume de Lavallade. *Ce qui m'inquiète, c'est lorsque l'entreprise l'ignore."*

Seuls les grands groupes ou les start-up du web ayant réussi peuvent se payer les services d'une plateforme de bug bounty. Les PME auront avantage à se rabattre sur les tests de pénétration, moins onéreux mais déjà très complets

Cyber-risques, le point sur les menaces

Les cybermenaces font désormais équipe avec les bonnes vieilles "fraudes au président"

Les entreprises font communément face à deux grands types de menaces. D'abord la perte des données personnelles qu'elle détient sur ses clients ou ses salariés, et qui, selon le RGPD, doivent être protégées. Ne plus y avoir accès peut avoir un impact sur le business de l'entreprise, mais pire encore, cela peut ruiner sa réputation et détourner ses clients.

Ensuite viennent les fameux ransomwares, du nom de ces attaques informatiques qui vont crypter toute ou partie des systèmes informatiques et des données de l'entreprise. Elles sont là mais on ne les comprend plus. Les pirates proposeront alors à sa cible de les rendre à nouveau déchiffrables et utilisables, contre une rançon. *"En 2017, des sociétés ont été liquidées en quelques semaines après avoir été victimes d'un ransomware"*, témoigne Pierre Lorcy, fondateur de Lorcyber. *"Nous avons récemment géré un incident sur une entreprise de taille moyenne et le coût total des pertes s'est monté à 500000 euros"*, prévient Jérôme Gossé, responsable de la souscription cyber-risque pour l'Europe continentale chez l'assureur Chubb.

Mais ce n'est pas tout, car les cybermenaces font désormais équipe avec les bonnes vieilles "fraudes au président". Dans ce scénario très fréquent en France, un malfaiteur se fait passer pour le président ou un exécutif et demande, par téléphone ou par e-mail, un virement sur un fournisseur fictif. Les fonds sont souvent d'abord virés vers un pays limitrophe, puis vers un pays plus lointain. *"D'un point de vue pratique, les fraudes au (faux) président (et plus généralement les fraudes par détournement de coordonnées fournisseurs) font pour le moment officiellement plus de dégâts financiers dans nos livres, que les attaques cyber sur des TPE, des PME et même des grands groupes"*, nous apprend Emmanuel Silvestre, senior vice-président, risques financier chez Liberty. À première vue il s'agit d'usurpation, et non d'attaque numérique. Mais de plus en plus adviennent des attaques hybrides où un attaquant entre dans le système pour récupérer les informations sur l'entreprise et ses salariés avant de tenter une usurpation. On n'arrête pas le progrès ! ■

"Le problème inhérent au cyber tient au déséquilibre constaté entre l'ampleur de l'impact d'une attaque numérique susceptible de toucher un très grand nombre d'assurés et de contrats d'une part et le pourcentage encore relativement restreint de sociétés ayant souscrit à ce jour des garanties d'assurance dédiées aux risques cyber." Emmanuel Silvestre, Liberty.

Cyber-assureurs, quoi couvrir et comment ?

"Les garanties spécifiques cyber, conçues autour de la donnée, ne peuvent suffire à couvrir la globalité du coût engendré par une attaque sur les actifs intangibles de la société"

Les assureurs portent le risque cyber depuis une vingtaine d'années. Mais comment l'assurent-ils ? Ils mutualisent un risque, par rapport à un nombre d'assurés. *"Le problème inhérent au cyber tient au déséquilibre constaté entre l'ampleur de l'impact d'une attaque numérique susceptible de toucher un très grand nombre d'assurés et de contrats d'une part, et le pourcentage encore relativement restreint de sociétés ayant souscrit à ce jour des garanties d'assurance dédiées aux risques cyber,* analyse Emmanuel Silvestre, senior vice-président, risques financiers chez Liberty. *Si la majorité des entreprises du CAC40 et des Opérateurs d'Importance Vitale sont bien couverts, un important travail de sensibilisation reste à mener auprès des ETI, PME et TPE, en parallèle des chantiers entamés sur la protection de leurs données personnelles."*

Les assureurs doivent aussi faire face à un problème de cumul, qui n'est pas sans rappeler la problématique des catastrophes naturelles ou des actes terroristes. *"Un virus peut toucher n'importe quelle entité dans le monde, donc plusieurs de nos assurés, à la fois dans des pays et des secteurs de l'économie différents, peuvent être impactés,* explique Jérôme Gossé, responsable de la souscription cyber-risque pour l'Europe Continentale chez Chubb. *Des pools d'assureurs ont été mis en place pour faire face à des sinistres systémiques comme les catastrophes naturelles, mais ce n'est pas encore le cas pour les cyber-risques".*

Ensuite, quoi indemniser et à quelle hauteur ? *"Les principaux postes indemnisés sont les frais d'experts informatiques, de relations publiques, la perte du chiffre d'affaires générée par la dégradation du système d'information et le fait que les données ne sont pas accessibles"*, précise Jérôme Gossé. Mais la couverture reste partielle. *"Les garanties spécifiques cyber ont été initialement conçues autour de la donnée (frais de reconstitution, de notification, pertes d'exploitation suite à déni de service, "ransomware", responsabilité civile, etc.) et ne peuvent suffire à couvrir la globalité du coût engendré par une attaque sur les actifs intangibles de la société, tels que sa réputation ou la perte de sa valeur due à la défiance des clients ou des marchés,* analyse Emmanuel Silvestre. *Contrairement au risque maîtrisé et modélisable de l'incendie, l'indemnisation du risque cyber pose la double question de sa juste évaluation et de la preuve du lien de causalité entre le dommage et le fait générateur numérique."* À noter qu'une assurance permet aussi de bénéficier d'une équipe technique, d'une équipe spécialisée dans les RP ou des services d'un avocat. ■