Ransomware :

Les enjeux des premières heures de la gestion de crise

« Vos données ont été chiffrées. Pour récupérer l'usage de votre système d'information, il vous faut payer une rançon dont voici les modalités de versement ». C'est pour ne pas recevoir ce type de message que les entreprises investissent significativement dans des solutions et services de cybersécurité qui doivent interdire l'accès de leurs systèmes d'information aux cyber délinquants. Mais la multiplication des attaques de type Ransomware, et leur sophistication croissante, montrent que le préventif ne suffit pas. Toutes les organisations doivent aujourd'hui être prêtes à réagir selon les meilleures pratiques, au cas où les protections ne seraient pas suffisantes pour contrer les attaquants.

Thomas Hutin, Head of Cybersecurity France et Guillaume Granier, Head of Strategic Communications France, expliquent pourquoi beaucoup se joue dès les premières heures et comment il convient d'organiser la capacité de riposte.

Une attaque de type Ransomware est une crise pour toute l'entreprise, pas seulement une crise IT

Un Ransomware, c'est un choc majeur pour l'entreprise. C'est toute l'organisation qui est atteinte, dans son fonctionnement le plus intime, dans sa capacité à servir ses clients et à remplir son rôle économique, et dans sa crédibilité auprès de ses différents publics. Au demeurant, le blocage de tout ou partie du système d'information de l'entreprise ne constitue qu'une des modalités du ransomware. L'attaque s'accompagne souvent d'un vol de données préalable, dont la menace de divulgation publique fera partie des moyens de pression des attaquants pour obtenir le paiement de la rançon, en mettant en cause ses procédures de sécurité ou en révélant certains aspects stratégiques confidentiels.

Une attaque de type Ransomware, c'est donc un affrontement entre une entreprise et un adversaire expérimenté, qui dispose de moyens importants et qui a eu le temps de préparer minutieusement son attaque, le tout avec une très forte somme d'argent en jeu. Dans ces conditions les attaquants utilisent tous les leviers à leur disposition, et en particulier celui de la déstabilisation psychologique. On a ainsi pu voir dans une affaire récente les malfaiteurs appeler directement par téléphone les conjoints des dirigeants pour ajouter de la pression.

Face à des équipes d'attaquants expertes et bien organisées, il est donc nécessaire de déployer rapidement au niveau de l'entreprise une équipe de spécialistes de haut niveau, capable de les mettre en échec, et en tout cas dans un premier temps de réduire le niveau de menace. L'enjeu va consister à reprendre l'initiative et à mobiliser dans la durée les ressources nécessaires.

Face au Ransomware, des priorités à mettre en œuvre sans délai

Face à un Ransomware, les premières heures de la gestion de crise sont décisives. Il faut en particulier :

— Agir très vite pour circonscrire l'attaque sur le plus petit périmètre possible.

— Mobiliser les personnes compétentes et en nombre.

— Identifier et isoler les parties du système d'information atteintes par l'attaque.

— Evaluer les conséquences, les dommages et les réactions en chaîne.

— Identifier les parties prenantes potentiellement atteintes.

— Définir l'opportunité et les modalités de communication auprès de ces parties prenantes de l'entreprise.

Le défi des premières heures est en partie lié à l'incertitude de la situation. Il va falloir agir sans connaitre l'étendue des dommages, alors que les agresseurs bénéficient, quand l'attaque est révélée, d'un avantage d'initiative.

Dès la découverte de l'attaque, il importe de faire remonter l'alerte aux services spécialisés de police et aux autorités compétentes, en fonction de la situation et du profil de l'entreprise. Police ou gendarmerie seront contactés sachant que le dépôt de plainte va devenir obligatoire en France pour bénéficier d'indemnisations éventuelles de la part des assurances.

Dès le départ, il faut être conscient qu'une attaque de type Ransomware intègre une « scène de crime ». Il faut donc dès la mise en place de la cellule de crise penser à collecter les éléments de preuve et à préserver les indices, de manière à nourrir le volet judiciaire de l'affaire le cas échéant.

Un aspect très important de la capacité de riposte est son maintien dans le temps, le risque d'épuisement des équipes en charge étant réel. Il faut prévoir la relève d'acteurs mobilisés dans des séquences longues et stressantes, avec la mise en place d'une logistique et de ressources adaptées.

Mettre en place les protocoles de communication de crise

Ce qui caractérise le début d'un Ransomware, c'est que l'on ne sait pas exactement ce qui se passe. Il faut donc être capable de prendre les bonnes décisions, sans avoir toutes les informations. Cette incertitude initiale - sur la durée de l'infiltration préalable, la portée de l'attaque, les dégâts réels subis, les parties prenantes victimes, le fait que des données personnelles aient pu être altérées ou dérobées - est d'ailleurs une constante dans les situations de communication de crise.

Malgré ces incertitudes, prendre la main sur la communication dès les premières heures est essentiel. Il faut très vite mettre en place la cellule de crise, identifier les porte-paroles au cas où une communication serait décidée, définir les éléments de langage, les questions / réponses et surveiller étroitement les médias, réseaux sociaux et sites spécialisés.

Un enjeu immédiat est de calibrer la communication des premiers jours. La question de la révélation publique ou non de l'attaque est un enjeu important. Révéler trop tôt risque d'inquiéter inutilement l'écosystème de l'entreprise et de déstabiliser encore plus son activité. Révéler trop tard pourrait passer pour une tentative de dissimulation et un manque de loyauté vis-à-vis des clients, salariés, partenaires, dont les données pourraient être compromises. Cette question est d'autant plus épineuse que la révélation publique peut à tout moment émaner de l'agresseur lui-même dans sa stratégie de mise sous pression.

Les premiers messages sont forcément très concis, à l'aune du faible niveau d'information fiable disponible. Ils adresseront généralement les points suivants :

— Reconnaître qu'un incident est en cours.

— Annoncer que l'on met en œuvre les moyens adaptés et l'équipe pluridisciplinaire compétente.

— Observer que l'on est préparé et que l'on applique un protocole validé.

— Promettre des points réguliers et tenir cet engagement.

— Adresser, s'il y en a, des points d'inquiétude particuliers en fonction de la situation et de l'évolution de la crise.

L'élaboration de la stratégie de communication suivra un certain nombre de principes clés :

— La crédibilité, en ne délivrant que des informations fiables et vérifiées.

— La transparence, en fournissant aux parties prenantes de l'entreprise le niveau d'information qu'elles sont en droit d'attendre d'un partenaire de confiance.

— L'empathie, en reconnaissant et partageant les inquiétudes et difficultés que la situation crée auprès des salariés, clients, partenaires, etc. et les solutions que l'entreprise entend mettre en œuvre au plus vite.

Parmi les parties prenantes, l'interne jouera comme toujours dans les situations sensibles un rôle clé, il sera plus que jamais le « premier porte-parole » de l'entreprise. Une communication régulière et adaptée à destination des salariés sera donc indispensable. Si les clients sont un autre public évidemment prioritaire, les investisseurs et les marchés financiers, si l'entreprise est cotée, seront aussi à traiter en priorité, un Ransomware étant un événement critique qui aura souvent un effet sur le cours de bourse.

La réduction progressive de l'incertitude permettra progressivement d'adresser des messages de plus en plus précis et ciblés. Deux savoir-faire très importants sont susceptibles d'accélérer la reprise de contrôle :

— La capacité à récupérer, traiter et qualifier très vite un volume considérable de données non structurées, réparties dans une multitude de fichiers. Ce travail va permettre de prendre la mesure exacte des conséquences des données accédées par les attaquants, notamment le type de données concernées (données « basiques » ou alors données « sensibles » de type personnelles, confidentielles, etc.).

— La veille permanente des groupes de Ransomware les plus actifs. Actualiser en permanence la connaissance de leurs TTP (tactiques, techniques et procédures) est la clé pour mieux les contrer et surtout pour aller plus vite dans la mise en opposition en cas d'attaque.

Enfin, il est important de noter qu'en matière d'alerte, des règles strictes existent dès lors que des données personnelles sont potentiellement altérées ou dérobées. En France, l'entreprise est tenue d'alerter la CNIL dans les 72 heures. Dans d'autres pays, le délai peut être plus court. Les règles en la matière varient selon les pays mais aussi selon les activités. Un opérateur de services dit essentiels sera par exemple beaucoup plus contraint dans son obligation d'alerte.

Les premières heures de la gestion d'un Ransomware se jouent en réalité… en amont de l'attaque !

Le fait de ne pas être bien préparé est évidemment un facteur aggravant quand une crise survient. C'est pourquoi une grande partie du succès de la parade se construit en anticipation de la crise. Le plan de réponse à incident doit prévoir de multiples scénarios d'attaque et identifier pour chacun les protocoles de réponse.

Si l'entreprise n'est pas préparée, le risque est grand de perdre du temps au début de l'attaque, dans un moment où chaque heure compte pour l'endiguer et en réduire ses effets.

Une bonne préparation inclut notamment des procédures de sauvegarde très strictes des données. Il importe que les données vraiment critiques bénéficient de protocoles d'accès, de sauvegarde et de stockage particulièrement durcis.

Le fondement de la cybersécurité est évidemment de déjouer les attaques dès la phase de préparation. Cela demande une capacité de protection contre les attaques, par exemple en exigeant une authentification forte notamment, et une capacité de détection pour déceler au plus tôt les signes d'une attaque en cours.

En conclusion, une attaque de type Ransomware exige la mobilisation immédiate de compétences multiples et sur un large front :

— Pour apporter une expertise technique : comprendre ce qui est en train de se passer.

— Pour isoler les parties infectées, protéger les parties indemnes du système d'information et orchestrer un redémarrage progressif de l'activité.

— Pour définir une stratégie cohérente de communication de crise.

— Pour documenter les aspects juridiques de l'attaque.

Aujourd'hui, toutes les entreprises sont sous la menace et la plupart sont la cible d'attaques régulières. L'entreprise attaquée se voit très clairement en incapacité de fonctionner de façon normale faute de payer. Et sa réputation sera atteinte, surtout s'il paraît évident qu'elle était mal préparée et mal défendue.

Investir dans des systèmes de protection, de détection pour déjouer les attaques, avoir des plans éprouvés, une équipe entrainée, et être accompagné de professionnels expérimentés dans les différentes disciplines quand une brèche est ouverte doivent figurer tout en haut de l'agenda anti-Ransomware !

THOMAS HUTIN
Head of Cybersecurity France
thomas.hutin@fticonsulting.com

GUILLAUME GRANIER
Head of Strategic Communication France
guillaume.granier@fticonsulting.com