Sécurité des SI en temps de crise

Les principaux aspects à connaître

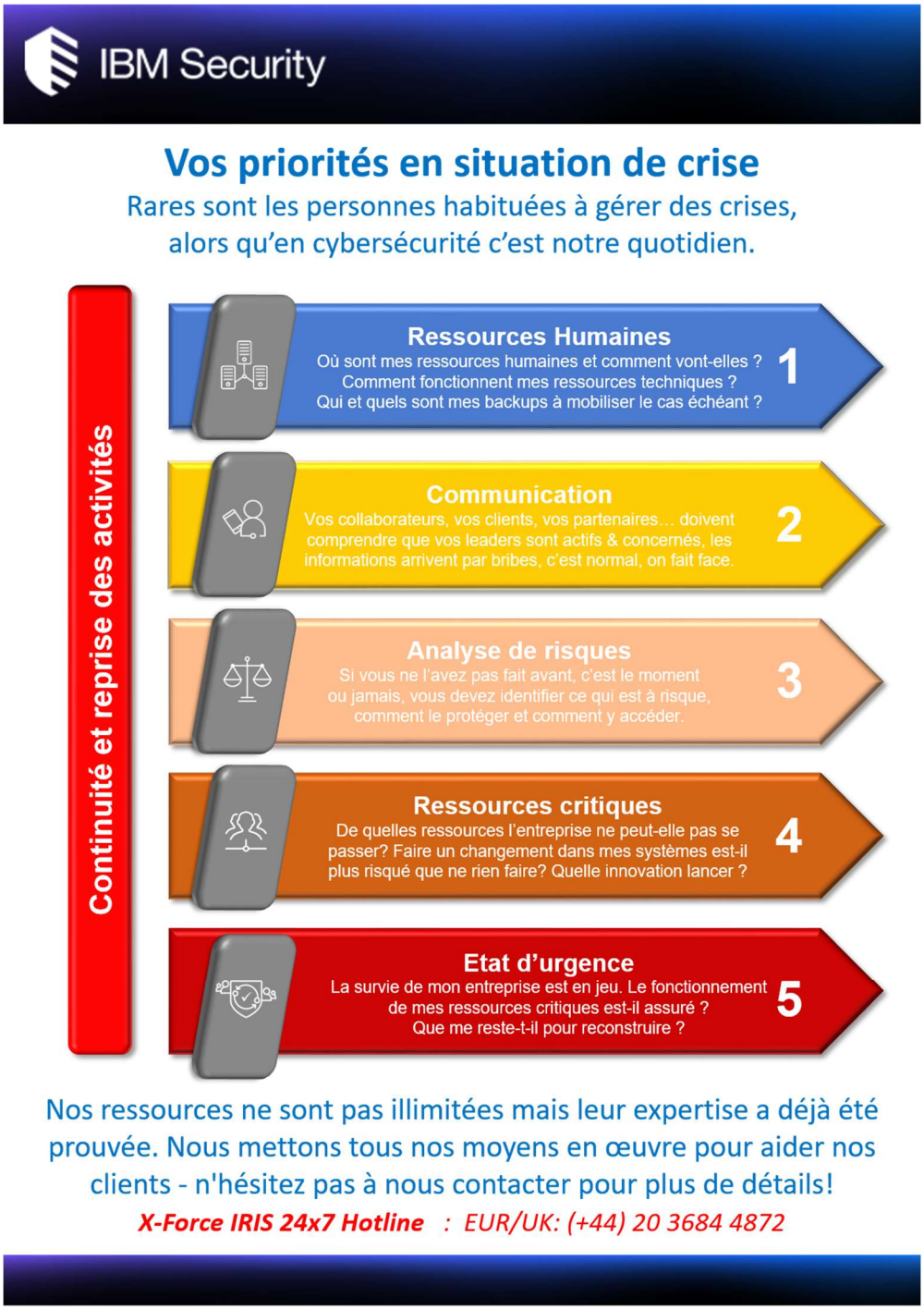

Table des matières

Rappel Important *: Les recommandations génériques contenues dans ce document sont issues de notre expérience sur le terrain et de quelques bonnes pratiques que nous en avons retirées. Elles n'ont pas vocation à se substituer à une analyse plus fine et spécifique des attaques auxquelles votre entreprise pourrait être exposée ou des failles de sécurité de votre système d'information, en particulier dans un environnement évolutif et difficile, impliquant le déploiement subi du télétravail. Les conditions des offres qui sont décrites sont disponibles sur le site internet d'IBM, les descriptions sommaires figurant dans ce document ne pouvant s'y substituer ou les amender ou compléter d'aucune manière.*

Introduction

En cette période atypique, les entreprises ont déclenché des plans de crise et les organisations sont contraintes à :

- réagir très rapidement,
- répondre aux besoins massifs de télétravail,
- exposer à l'extérieur de leur Système d'Information (SI) certaines de leurs applications sans que cela soit prévu en amont,
- s'adapter à l'explosion de la demande (par exemple dans les secteurs de la vente à distance, de la distribution ou de la santé).

Dans ce contexte d'évolution rapide et d'urgence, la priorité des organisations va à la santé des employés, des clients et de la population. Les effectifs opérationnels sont donc restreints et les entreprises ne disposent pas de visibilité sur la date et l'état de sortie de la crise. En même temps, le télétravail modifie radicalement les méthodes de travail.

La situation inédite, les efforts concentrés pour sortir de la crise et l'impossibilité de s'y être préparés complètement impliquent une période propice aux attaques ciblées ou d'ampleur. Les attaques se multiplient déjà. Et elles vont augmenter nettement, pour profiter des faiblesses induites par la priorité donnée à la continuité de l'activité de l'entreprise et moins aux mesures de sécurité qu'il faudrait y associer.

IBM, en tant qu'entreprise internationale ayant eu à gérer des crises d'ampleur et en tant que spécialiste de la Cyber Sécurité, vous propose de vous faire bénéficier de son expérience.

Au sein de votre cellule de crise, les points ci-dessous nous semblent essentiels :

1) La communication rapide et maintenue au fil du temps vers vos équipes et votre écosystème est fondamentale ;
2) La sensibilisation de vos employés pour lutter contre la menace constante du phishing et des autres Cyber Attaques. En effet, ces attaques sont facilitées par des utilisateurs non avertis allant sur des sites compromis ou utilisant des outils non agréés par votre charte SI ;
3) L'analyse des risques pour identifier et mesurer le risque de la situation actuelle sur vos activités et vos actifs les plus critiques qui doivent être en fonctionnement pour assurer la continuité de l'entreprise ;
4) Le renforcement de la sécurité des terminaux permettant les connexions à distance (audits de configuration, règles de paramétrage, ...) ;

5) La bonne gestion et le contrôle des accès à distance (gestion, protection, détection) pour les utilisateurs et matériels se connectant sur le réseau.

Dans ce contexte, les solutions Unified Endpoint Management (UEM), Identity and Access Management (IAM) sont cruciales dans le dispositif de protection, ainsi que la mise en place d'un résolveur DNS bloquant directement certains domaines qui sont liés à des botnets, des attaques par phishing et d'autres pratiques malicieuses.

Aussi, pour accompagner ses clients à travers cette crise mondiale, IBM Security a annoncé le 18 Mars 2020 que ses solutions IBM Security MaaS360 with Watson (pour l'UEM), IBM Cloud Identity (pour l'IAM) seraient mises gratuitement (*) à disposition pour une durée de 90 jours - pour toute entreprise n'utilisant pas déjà ces solutions. IBM Security rappelle également que le Résolveur DNS QUAD9 reste disponible pour protéger les utilisateurs travaillant depuis leur domicile.

(*) les informations relatives à ces dispositions exceptionnelles sont disponibles sur le blog suivant : https://securityintelligence.com/posts/how-we-learned-to-stop-worrying-and-embrace-remote-work/

Basé sur nos retours d'expérience ainsi que sur les expertises d'IBM Security dédiées à la gestion de crise et à la remédiation post incident, ce document a pour objectif de vous aider à trouver des réponses concrètes et rapides pour vérifier les mesures de sécurité à mettre en place sur votre système d'information et ainsi limiter le risque de Cyber Attaques durant la crise.
Ainsi, nous vous proposons de nous positionner dès le début de la « Kill-Chain », à savoir avant qu'une attaque ait déjà eu lieu pour en réduire les impacts et soulager les équipes de réponses.

Rappel sur la « Kill-Chain »

Le terme « Kill-Chain » provient à l'origine du domaine militaire pour décrire les différentes phases d'une attaque. Il a été repris dans le domaine de la cyber-sécurité et se compose des phases suivantes :

- Reconnaissance ;
- Intrusion ;
- Déplacement latéral ;
- Exfiltration des données ;
- Suppression des traces.

Il existe des boucles dans la Kill-Chain : suite à un déplacement latéral, l'attaquant peut recommencer une phase de reconnaissance et ainsi de suite.

Lors de la phase de reconnaissance, l'attaquant va généralement chercher des failles et des points d'entrées dans l'infrastructure cible. Ces techniques se traduisent par des scans réseau ou des scans d'application qu'il faut chercher à détecter. En effet, une attaque détectée dans une phase amont de la Kill-Chain est plus facile à contrer qu'une attaque détectée plus en aval.

Si la phase de prévention a été convenablement menée, avec entre autres des logiciels à jour et des applications testées, l'attaquant ne pourra rien détecter de pertinent pour rentrer en phase d'intrusion.

C'est la raison pour laquelle nous mettons en avant dans ce guide des techniques de détection et de prévention directement actionnables pour éviter une attaque ou la détecter au plus tôt.

La détection

La détection arrive généralement à la fin d'une phase de sécurisation d'un SI.
Cependant, en situation de crise, la détection est en première ligne, le reste des opérations classiques de sécurisation pouvant difficilement être mis en œuvre.

En complément des moyens de détection standards déjà en place, un axe important de renforcement porte sur le poste de travail de l'utilisateur, point de départ d'une part importante des compromissions. Ceci d'autant plus que les employés télétravaillent et opèrent depuis des réseaux domestiques non fiables.

Les attaquants risquent de profiter de ces moments de flottement pour mener des attaques opportunistes ou lancer une attaque ciblée préparée de longue date.
Autant il est difficile de se prémunir contre une attaque ciblée, autant les attaques opportunistes sont plus facilement détectées.
Dans le cadre d'attaques opportunistes, il est vraisemblable que les attaquants vont privilégier des canaux simples :

- Envoi de mail corrompu (à destination d'adresses personnelles ou professionnelles) ;
- Repérage grossier des infrastructures depuis des points d'accès publics (site web, ...).

Ces deux types d'attaques se repérent au niveau des terminaux de filtrage périmétrique tels que les passerelles mails ou les firewalls.

• Sur les scans

Essayez de détecter les scans :

- Scan de réseau (IP/port), utilisé pour la recherche de vulnérabilités du SI ;
- Scan des applications Web, utilisé pour rechercher des failles dans la programmation (points d'injection SQL par exemple).

Si vous disposez d'un SOC, vérifiez si ces cas d'usage sont en place et demandez une modification des seuils. Attention, cela risque de générer des faux positifs et un surcroît de travail pour vos équipes.

Si vous ne disposez pas de SOC, essayez de paramétrer vos firewalls dont certains (avec IPS/IDS intégrés) permettent la détection de tels scans.

Focalisez-vous sur la défense périmétrique (les accès externes), les flux Est-Ouest (internes) pouvant être gérés par la suite.

En cas de détection de scan, n'hésitez pas à « black-lister » les adresses voire les sous-réseaux d'où proviennent les attaques.

• Sur les mails

Une campagne de phishing opportuniste peut se repérer car une masse d'emails semblables est envoyée simultanément.

Si vous disposez d'un SOC, demandez si des cas d'usages ayant trait aux mails et au virus sont mis en place.
Si vous ne disposez pas de SOC, reposez-vous sur les rapports du système anti-spam et anti-virus.

Si vous détectez une campagne de phishing, prévenez immédiatement vos collaborateurs. De manière temporaire, vous pouvez aussi configurer votre passerelle de mail pour supprimer les pièces jointes ou remplacer les liens par des « sanitizers » d'URL. Ces solutions de nettoyeurs d'URL reçoivent les mails, remplacent les liens par des liens renvoyant vers des systèmes qui analysent la cible du lien.

Exemple : un lien http://www.malveillant.com contenu dans un mail sera transformé en http://url-sanitize.prooftrend.com/?lien1234. En cliquant sur ce dernier lien, la requête sera redirigée vers *url-sanitize.prooftrend.com* qui analysera la cible originale (www.malveillant.com) avant de rediriger la requête vers la cible originale si cette dernière est considérée comme sûre ou vers une erreur si elle est considérée comme malveillante.

Il existe des systèmes basés sur des solutions SaaS rapides à déployer.

- ### Sur les EDR et EPP

Les EDR (Endpoint Detection and Response) et les EPP (Endpoint Protection Platform) visent à éviter des attaques par rebond du réseau domestique vers le réseau d'entreprise. Ces solutions vont plus loin que les antivirus traditionnels car elles surveillent l'activité des applications sur les postes de travail et alertent (ou bloquent) en fonction de celle-ci.
Ces solutions renvoient des logs qui peuvent être exploités par un SOC ou par une analyse de log ad-hoc. Elles sont abordées dans la section suivante.

La prévention

Il est généralement trop tard pour mettre au point des mécanismes de prévention qui n'auraient pas déjà été déployés.
Nous proposons ici la vérification de mécanismes déjà en place ou la mise en place de mécanismes Cloud permettant un déploiement et un retour rapide vers la situation initiale pour reprendre les évolutions prévues.

La prévention va surtout se passer au niveau du poste de travail utilisateur devenu critique. Une entreprise non préparée au télétravail doit faire face à la dissémination des postes de ses employés :

- Sur des réseaux domestiques non fiables ;
- Prêtés à des personnes n'appartenant pas à l'entreprise (famille pour les devoirs, ...) et non sensibilisées aux problèmes de sécurité ;
- ...

Par ailleurs, il ne faut pas oublier que dans certains cas, des postes de travail personnels risquent d'être utilisés (en particulier dans les entreprises où les postes de travail sont fixes). Si ce cas se présente, le risque qu'ils ne soient ni à jour ni correctement protégés est important.

Il est essentiel d'éviter de conserver des documents sensibles sur les postes des collaborateurs afin de prévenir le vol de données en cas de vol de poste non chiffré ou d'attaque par rebond.

Les postes n'étant pas forcément prêts, il faut ajouter des contrôles secondaires pour s'assurer d'une sécurité minimum (pas de navigation sur des sites pouvant être compromis, éviter les ouvertures de mails personnels avec le poste de travail, etc.).

Cela est rendu possible par les EDR (Endpoint Detection and Response) et les EPP (Endpoint Protection Platform). La mise en place de ce type de solution en interne est délicate, aussi nous préconisons de mettre en place un EDR ou un EPP « Cloud » en mode SaaS car la majorité de la maintenance sera assurée par le fournisseur.

Des solutions simples à déployer et disponibles sur le Cloud existent et impliquent parfois le déploiement d'un seul agent sur les terminaux.

Enfin, des mesures simples d'hygiène doivent être prises immédiatement :

- S'assurer de l'absence de vulnérabilités connues ;
- S'assurer de la mise à jour des anti-virus.

En temps de crise, il vaut mieux des mesures imparfaites - recherche de vulnérabilités sur un périmètre « simple », EDR sur la moitié des postes collaborateurs seulement - que des mesures perfectionnistes qui seront mise en œuvre lors du retour à la normal.

- Effectuer une revue des vulnérabilités immédiatement sur le périmètre accessible ;
- Effectuer des mises à jour régulièrement (plusieurs fois par jour) des anti-virus ;

- Créer un site web de téléchargement des agents propres à l'entreprise pour éviter de récupérer des éléments fallacieux ou corrompus (agent EDR, ...) ;
- Vérifier les politiques d'authentification au niveau des passerelles VPN ;
- Mettre en place un EDR ou un EPP Cloud ;
- Dans le cas où des postes personnels sont utilisés pour l'accès à distance, mettre en place le plus de validation possible de sa configuration : certains paramètres, tels que le niveau de patch, peuvent être validés par le logiciel de VPN avant d'autoriser la connexion vers le réseau d'entreprise ;
- Utiliser un résolveur DNS tel que le Quad9 d'IBM (9.9.9.9) qui évite de renvoyer vers des adresses IP malveillantes ou de répondre vers un domaine malveillant.

La communication est un élément essentiel

Basé sur l'expérience d'IBM dans la gestion de crise, les priorités à donner sont claires :

1- La santé physique et morale de tous les collaborateurs
2- La continuité opérationnelle de nos clients
3- Le maintien de l'activité métier

Aussi, dans ce contexte de crise actuelle, les points essentiels pour accompagner vos collaborateurs sont :

- ⇨ Maintenir le contact et fixer les priorités aux équipes ;
- ⇨ S'assurer de la disponibilité et de la mobilisation des ressources critiques en particulier en cas d'attaque sur le SI ;
- ⇨ Renforcer le niveau de vigilance des utilisateurs.

Ces points nous paraissent d'autant plus essentiels qu'ils laisseront certainement une empreinte forte une fois le retour à la normale.

Il nous semble important de maintenir un contact continu depuis le plus haut niveau de management puis par cercles de responsabilité afin de s'assurer de la mobilisation des équipes :

- ⇨ Leaders présents, actifs et concernés par la situation, la santé des équipes, leurs préoccupations ;
- ⇨ Communication cohérente à tous les niveaux, régulière et centrée sur des messages clés qui donnent les priorités et une direction claire aux équipes, par exemple :
  - La sécurité des personnes : employés, tiers intervenants, etc. ;
  - La continuité des services et des opérations (à minima les plus critiques) des clients ;
  - La continuité des opérations (production, distribution…) de l'organisation ou de l'entreprise ;
  - …
- ⇨ Capacité à informer et à supporter au mieux les personnes en fonction de l'évolution des situations personnelles et du contexte global.

Cette présence auprès des équipes doit permettre aussi d'évaluer et de s'assurer du niveau de disponibilité des équipes en général, et des ressources critiques en particulier :

- ⇨ Si cela n'avait pas été réalisé avant crise : cerner les périmètres critiques du SI sur lesquels l'attention en matière de cyber sécurité doit être maximale et identifier quelles sont les ressources critiques pour prévenir, détecter et intervenir (contenir, remédier, restaurer) en cas d'attaque ;

- ⇨ S'assurer continuellement de la disponibilité des personnels (internes ou tiers intervenants) critiques, des moyens de pallier une indisponibilité, des modalités et capacités d'intervention en urgence en cas d'attaque sur le SI.

Enfin, la vigilance et la sensibilisation des utilisateurs restent essentielles afin de prévenir les incidents de sécurité :

- ⇨ Communication et rappel des risques en particulier auprès des utilisateurs qui travaillent et accèdent au SI à distance : ne pas conserver d'informations sensibles sur le poste à moins qu'elles ne soient nécessaires à l'activité du moment, vigilance quant aux courriels et messages qui peuvent être suspects (expéditeurs inconnus, contenu des messages…), aux fichiers joints, à la navigation sur des sites et au téléchargement de fichiers sur Internet… ;
- ⇨ Communication spécifique et vigilance accrue pour les populations couvrant des activités (traitements, données) sensibles et pouvant faire l'objet de fuite d'informations ou de fraude : par exemple vérifier les demandes inhabituelles y compris de personnes sensées être des collègues ou supérieurs hiérarchiques ;
- ⇨ Vigilance particulière et exigence de rigueur des utilisateurs IT disposant de comptes à privilèges (administrateurs des systèmes…) pour lesquels une compromission pourrait avoir un effet dévastateur sur la disponibilité, l'intégrité et la confidentialité des informations de l'organisation et du SI.
- ⇨ La sensibilisation est d'autant plus importante dans la période que nous vivons que les barrières habituelles de l'entreprise sont fragiles :
  - Des opérations critiques d'entreprise peuvent être réalisées depuis des réseaux non fiables (domicile des employés) ;
  - Les terminaux peuvent être utilisés à des fins professionnelles et personnelles (en particulier si utilisation d'équipements personnels)
  - Utilisation par les enfants favorisée par l'état de confinement et les devoirs à distance ;
  - …

Pour aller plus loin avec IBM sur la gestion de la crise actuelle

IBM envisage toutes les options pour aider les entreprises et les organisations :

1) Mise à disposition gratuite de solutions de transfert de fichiers sécurisés

Compte tenu de l'adoption massive et en urgence des restrictions de voyage et des politiques de travail à domicile, il est possible que de nombreux employés de ces organisations puissent ne pas être correctement autorisés à travailler à distance. Pour soutenir ses clients et les aider à maintenir la continuité de leurs activités pendant cette période difficile, IBM élimine le coût d'utilisation du service Cloud Aspera pour le partage de fichiers à haut débit et la collaboration d'équipe. Jusqu'au 30 avril 2020, nous offrons aux nouvelles organisations la possibilité de s'abonner gratuitement à IBM Aspera on Cloud pendant quatre-vingt-dix (90) jours. Les nouveaux abonnés pourront utiliser gratuitement l'offre SaaS pour un maximum de 2500 utilisateurs, 1 téraoctet (To) de transfert de données, 1 To de stockage Cloud et 10 To de sortie. Ce service hébergé comprend une sécurité intégrée et permet aux utilisateurs situés n'importe où d'utiliser pleinement leur bande passante disponible pour échanger des fichiers et des ensembles de données volumineux de manière rapide et fiable. En tant que solution SaaS entièrement hébergée, il n'y a aucune infrastructure à déployer et aucun réseau spécial à configurer. Après leur inscription, les employés peuvent immédiatement commencer à envoyer, recevoir et partager des fichiers de toute taille en toute sécurité sur l'Internet public.

2) IBM Summit

Tout comme le supercalculateur Blue Gene d'IBM a joué un rôle essentiel dans l'identification des médicaments et traitements révolutionnaires il y a une génération, IBM Summit, le supercalculateur le plus rapide du monde, travaille avec les laboratoires nationaux américains pour simuler la croissance du coronavirus et trouver rapidement des composés pharmaceutiques qui peuvent le combattre. Sur plus de 8 000 combinaisons de médicaments qui pourraient fonctionner, IBM Summit a aidé le DOE (Département américain de l'Energie) à identifier 77 réponses possibles, et nos scientifiques travaillent avec le DOE pour accélérer les recherches.

3) Système de développement clinique IBM

Au début de cette année, l'entité Watson Health d'IBM a mis gratuitement le système de développement clinique d'IBM à la disposition des agences nationales de santé afin d'aider à accélérer le développement des traitements médicamenteux. Il s'agit d'une technologie utilisée par les sociétés pharmaceutiques pour réduire le temps/coût des essais cliniques en centralisant et en organisant les détails des essais cliniques, et qui

permet d'accéder aux données des essais cliniques à partir de n'importe quel appareil connecté au web.

Conclusion

IBM partage ici son expérience de la gestion de crise et de la continuité du Business pour vous accompagner dans cette période unique et inédite.
Les bonnes pratiques appliquées, le bon accompagnement et l'expertise déployée seront parmi les points cruciaux qui vous aideront à surmonter cette crise d'ampleur mondiale aux conséquences encore inconnues.