CONSEILS AUX ENTREPRISES : PRÉPARER LA REPRISE D'ACTIVITÉ AU DÉCONFINEMENT

L'annonce du début du déconfinement va vous permettre d'envisager une reprise au moins partielle et progressive de votre activité.
Si, dans une première étape, le recours au tététravail reste toujours à privilégier partout où c'est possible,vous devez vous préparer à cette reprise, tant au plan sanitaire que pour reprendre le contrôle de votre sécurité numérique.

Les 10 mesures suivantes visent à vous aider dans la réalisation de votre plan d'action cybersécurité de déconfinement.

1. Recenser et analyser les incidents de sécurité
exemples : hameçonnage de mot de passe, document suspect reçu en pièce-jointe d'un message…, pour cerner le plus précisément possible les incidents survenus.

2. S'assurer du bon fonctionnement de ses outils de protection
antivirus, pare-feu, systèmes de détection d'intrusion…

3. Rechercher les indices de compromission
comme des connexions inhabituelles, les annuaires de comptes pour déceler toute création de nouveau compte suspect, des règles de transferts de messages vers des comptes externes illégitimes.

4. Contrôler et tester les sauvegardes
Avant de reprendre l'activité de l'organisation, il est particulièrement important de vérifier leur bon fonctionnement, notamment en procédant à des tests de restauration et de s'assurer de disposer d'une copie récente des données qui soit déconnectée du réseau afin de pouvoir faire face à une attaque par rançongiciel.

5. Réaliser les mises à jour de sécurité
Si durant le confinement certains systèmes n'ont pas pu recevoir leurs mises à jour de sécurité, il convient de mettre en œuvre un plan de rattrapage cohérent et sans précipitation pour éviter tout effet de bord sur l'activité opérationnelle. La priorité sera donnée aux systèmes de sécurité, puis aux systèmes ou serveurs critiques exposés directement ou indirectement sur Internet, et enfin aux postes de travail des collaborateurs.

6. Recentraliser les données

Durant le confinement, des données de l'organisation ont pu être dispersées sur les postes des télétravailleurs ou de manière temporaire sur certains services de d'hébergement externes (cloud). Il convient donc de les recentraliser au sein de l'organisation pour s'assurer de leurs sauvegardes et de les supprimer dans les règles de l'art sur les stockages inappropriés pour limiter tout risque d'atteinte en matière de confidentialité.

7. Contrôler les équipements nomades avant de les reconnecter au réseau de l'entreprise

Avant d'en ré-autoriser la connexion au système d'information de l'entreprise, tous les équipements nomades utilisés durant le confinement (ordinateurs portables, téléphones mobiles, tablettes) doivent faire l'objet d'un contrôle strict pour s'assurer qu'ils n'ont pas été compromis, et idéalement faire l'objet d'une réinstallation complète depuis une matrice maîtrisée, sécurisée et convenablement mise à jour par l'organisation.

8. Refermer les accès externes devenus inutiles

L'organisation doit s'attacher à réduire son exposition, et donc sa surface d'attaque, en refermant tous les accès externes ouverts qui seraient devenus inutiles. Il peut s'agir d'accès externes à fermer au niveau des pare-feux mais aussi de comptes avec droits privilégiés ouverts à titre exceptionnel sur certains systèmes de l'organisation qu'il faudra clôturer.

9. Mettre fin aux usages à risques dérogatoires

Pour faire face au confinement, de nombreux usages d'applications, de services ou de pratiques ont pu être autorisés à titre exceptionnel mais peuvent présenter un risque de sécurité pour l'organisation. Il convient donc de communiquer avec pédagogie et transparence sur l'arrêt d'autorisation de ces pratiques dérogatoires.

10. Tirer rapidement les enseignements du confinement pour traiter tout ce qui doit l'être

L'organisation doit savoir tirer les enseignements de la crise pour se préparer à être en capacité de mieux l'affronter en cas de résurgence. Cela peut concerner sa politique d'équipement matériel en postes nomades professionnels maîtrisés pour les télétravailleurs, en équipements logiciels ou outils de travail à distance (visioconférence, téléconférence, hébergements de données…), en outils et procédures sécurisées de télétravail ou de télé-administration de ses systèmes, en infrastructures de sécurisation de ses systèmes, en formation et sensibilisation de ses collaborateurs, etc.

Nous contacter

securite-economique-nouvelleaquitaine@gendarmerie.interieur.gouv.fr

EN CAS D'URGENCE, APPELEZ LE 17 OU LE 112

VOUS ÊTES VICTIMES ?

Une question ?
Besoin d'aide ?

On vous accueille en ligne

Scanner le QR Code et dialoguer par tchat

BRIGADE numérique Gendarmerie