RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

MESURES CYBER PRÉVENTIVES PRIORITAIRES

AVANT-PROPOS

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) préconise la mise en œuvre de 5 mesures préventives prioritaires :

- **renforcer l'authentification sur les systèmes d'information ;**
- **accroître la supervision de sécurité ;**
- **sauvegarder hors-ligne les données et les applications critiques ;**
- **établir une liste priorisée des services numériques critiques de l'entité ;**
- **s'assurer de l'existence d'un dispositif de gestion de crise adapté à une cyberattaque.**

Ces mesures prioritaires de cybersécurité sont essentielles et leur mise en œuvre à court terme permet de limiter la probabilité d'une cyberattaque ainsi que ses potentiels effets. Pour être pleinement efficaces, elles doivent cependant s'inscrire dans une démarche de cybersécurité globale et de long terme.

RENFORCER L'AUTHENTIFICATION SUR LES SYSTÈMES D'INFORMATION

Afin de réduire le risque d'une cyberattaque, il est recommandé de renforcer l'authentification des comptes particulièrement exposés, notamment ceux des administrateurs qui ont accès à l'ensemble des ressources critiques du système d'information et ceux des personnes exposées de l'entité (personnel de direction, cadres dirigeants, etc.).

Il est ainsi vivement conseillé de mettre en œuvre une authentification forte nécessitant l'utilisation de deux facteurs d'authentification différents soit :

- un mot de passe, un tracé de déverrouillage ou une signature ;
- un support matériel (carte à puce, jeton USB, carte magnétique, RFID) ou a minima un autre code reçu par un autre canal (SMS).

Pour les administrateurs, l'activation d'une authentification renforcée doit se faire sur l'ensemble de leurs comptes : Active Directory, administration d'applications, cloud, etc.

ACCROÎTRE LA SUPERVISION DE SÉCURITÉ

Un système de supervision des événements journalisés doit être mis en place. Il permettra de détecter une éventuelle compromission et de réagir le plus tôt possible. Par ailleurs, en cas d'incident, ces événements permettront de gagner du temps dans la compréhension de l'incident. En l'absence de supervision de sécurité en place, la centralisation des journaux des points les plus sensibles du système d'information est conseillée. On peut lister à titre d'exemple les points d'entrée VPN, les bureaux virtuels, les contrôleurs de domaine, ou encore les hyperviseurs.

Le renforcement de la vigilance des équipes de supervision est indispensable, en investiguant les anomalies susceptibles d'être ignorées en temps normal. Plus particulièrement, en environnement Active Directory, les connexions anormales sur les contrôleurs de domaine doivent être inspectées. Les alertes dans les consoles d'antivirus et EDR concernant des serveurs sensibles doivent également être systématiquement étudiées.

Pour les entités qui en ont la capacité, l'accélération des déploiements d'outils donnant de la visibilité sur l'état de sécurité des systèmes d'information (Sysmon, EDR, XDR) est également préconisée.

SAUVEGARDER HORS-LIGNE LES DONNÉES ET LES APPLICATIONS CRITIQUES

Des sauvegardes régulières de l'ensemble des données, y compris celles présentes sur les serveurs de fichiers, d'infrastructures et d'applications métier critiques, doivent être réalisées.

Ces sauvegardes, au moins pour les plus critiques, doivent être déconnectées du système d'information pour prévenir leur chiffrement, à l'instar des autres fichiers. L'usage de solutions de stockage à froid, comme des disques durs externes ou des bandes magnétiques, permettent de protéger les sauvegardes d'une infection des systèmes et de conserver les données critiques à la reprise d'activité.

L'actualisation fréquente de ces sauvegardes est également préconisée.

ÉTABLIR UNE LISTE PRIORISÉE DES SERVICES NUMÉRIQUES CRITIQUES DE L'ENTITÉ

Avoir une vision claire de ses systèmes d'information et de leur criticité est essentielle pour prioriser les actions de sécurisation ainsi que pour réagir efficacement en cas d'incident.

Il est donc conseillé pour les entités, en associant les métiers, de réaliser un inventaire de leurs services numériques et de les lister par sensibilité pour la continuité d'activité de l'entreprise. Les dépendances vis-à-vis de prestataires doivent également être identifiées.

S'ASSURER DE L'EXISTENCE D'UN DISPOSITIF DE GESTION DE CRISE ADAPTÉ ÀUNE CYBERATTAQUE

Une cyberattaque peut avoir un effet déstabilisateur sur les organisations. Les fonctions support comme la téléphonie, la messagerie mais aussi les applications métier peuvent être mises hors d'usage. Il s'agit alors de passer en fonctionnement dégradé et dans certains cas, cela signifie revenir au papier et au crayon. L'attaque cause en général une interruption d'activité partielle et, dans les cas les plus graves, une interruption totale. Définir des points de contact d'urgence, y compris chez les prestataires de services numériques et s'assurer d'avoir les numéros en version papier est particulièrement utile dans ces situations.

Au-delà, il s'agit pour les organisations de définir un plan de réponse aux cyberattaques associé au dispositif de gestion de crise – quand il existe – visant à assurer la continuité d'activité, puis son retour à un état nominal. La mise en œuvre d'un plan de continuité informatique doit permettre à l'organisation de continuer à fonctionner quand survient une altération plus ou moins sévère du système d'information. Le plan de reprise informatique vise, quant à lui, à remettre en service les systèmes d'information qui ont dysfonctionné. Il doit notamment prévoir la restauration des systèmes et des données.