Documentation et Normes SSI

GROUPE BRETAGNE PAYS DE LA LOIRE
UGECAM
Soigner, rééduquer, réinsérer : la santé sans préjugés

UN GROUPE DE
l'Assurance Maladie
Agir ensemble, protéger chacun

Dans le cadre de mes missions, j’ai aussi été impliqué dans la partie “organisationnelle” de la sécurité, en travaillant sur la documentation SSI et les procédures internes, en complément des aspects techniques. L’objectif était de structurer les bonnes pratiques de sécurité déjà appliquées dans l’entreprise et de les formaliser sous forme de documents clairs, compréhensibles et réellement utilisables au quotidien par les équipes et les utilisateurs.

Concrètement, j’ai participé à la rédaction et à la mise à jour de plusieurs procédures de sécurité : gestion des comptes et des droits, création et suppression d’utilisateurs, règles de mot de passe, conduite à tenir en cas de suspicion d’e-mail frauduleux, gestion de la perte ou du vol de matériel, etc. Pour chaque sujet, je partais soit d’un document existant à remettre à jour, soit de pratiques informelles déjà appliquées par les équipes, que je reformulais de manière structurée (contexte, périmètre, étapes détaillées, rôles et responsabilités). Les documents étaient ensuite relus et validés par les personnes référentes (support, administrateurs, responsable SSI ou DSI) avant d’être diffusés officiellement.

J’ai également veillé à ce que ces procédures restent cohérentes avec les règles générales de sécurité de l’entreprise et avec les bonnes pratiques recommandées (par exemple issues de guides de l’ANSSI ou de référentiels internes a l’entreprise). L’idée n’était pas de recopier des normes “sur le papier”, mais d’adapter ces principes à la réalité du terrain : contraintes des utilisateurs, outils réellement disponibles et niveau de maturité des équipes.

En plus de la documentation, j’ai participé à la mise en place de nouvelles règles de sécurité concrètes, notamment autour de l’usage des cartes/badges et de la gestion des mots de passe. J’ai sensibilisé les utilisateurs à la valeur de leur badge (accès aux locaux, à des services internes, traçabilité), en rappelant qu’il s’agit d’un moyen d’identification personnel qui ne doit pas être prêté, laissé sur un bureau ou rangé n’importe où. J’ai également encouragé l’utilisation d’un gestionnaire de mots de passe plutôt que le stockage “sauvage” des identifiants (post-its, fichiers texte, carnets papier), afin de renforcer la sécurité des comptes tout en simplifiant le quotidien des utilisateurs.

En parallèle, j’ai contribué à la sensibilisation des utilisateurs aux risques numériques, car une grande partie de la sécurité passe par les comportements du quotidien. Lors de mes interventions de support, je profitais des échanges pour rappeler quelques réflexes simples : vérifier l’expéditeur d’un e-mail avant de cliquer, ne pas réutiliser le même mot de passe partout, verrouiller sa session en quittant son poste, éviter de stocker des données sensibles dans des emplacements non adaptés, etc. J’ai également participé à la diffusion et à l’amélioration de supports de sensibilisation internes, notamment via des mails de sensibilisation et des campagnes physiques (affiches, communications ciblées) mises en place par le service SSI.

Cette expérience m’a permis de comprendre que la sécurité ne repose pas uniquement sur les outils techniques, mais aussi sur des procédures claires, à jour, et sur l’accompagnement des utilisateurs. Travailler sur la documentation SSI m’a aidé à développer ma capacité à structurer l’information, à rédiger des consignes applicables et à faire le lien entre les exigences de sécurité et la réalité opérationnelle du terrain, tout en renforçant ma capacité à vulgariser les notions techniques auprès d’utilisateurs moins expérimentés en informatique.