ARBONIA

Information Security Newsletter

Chers collaborateurs,

Conformément au slogan ***THINK BEFORE YOU Click.Post.Type***, nous souhaitons vous informer des risques actuels liés aux technologies de l'information et attirer votre attention sur votre coresponsabilité en termes de protection face à la cybercriminalité. Il n'y a qu'ensemble que nous pouvons maintenir la sécurité informatique et par là préserver le groupe Arbonia d'importants dégâts en termes d'activité ainsi que face à la concurrence.

La mise en réseau et la numérisation croissantes en lien avec internet entraînent une hausse fulgurante de la cybercriminalité. On remarque un renforcement de la vulnérabilité, celle-ci ayant adopté un caractère pluridimensionnel. Notre environnement professionnel direct n'a pas non plus échappé à de graves attaques informatiques au cours des derniers mois (notamment Meier Tobler). Il est impossible de parvenir à une protection suffisante des données en ne misant que sur des mesures techniques: celle-ci dépend également dans une large mesure de votre façon de manipuler et de traiter les données et les systèmes informatiques. En tant que collaborateur Arbonia, vous représentez un membre central de la chaîne de sécurité et devez adopter un comportement actif en lien avec cette responsabilité. Nous portons un très grand intérêt à la promotion d'une culture de la sécurité des informations au sein du groupe Arbonia.

Le vecteur d'attaques le plus répandu et le plus souvent utilisé est, et reste, l'e-mail, suivi par l'ingénierie sociale (manipulation ou influence sur une personne) et internet. Pour cette raison, il est primordial de reconnaître les sources suspectes en tant que telles. Un comportement inapproprié pourrait grandement porter préjudice aux activités du groupe Arbonia et entraîner d'importantes pertes financières. En cas d'événement suspect, déconnectez votre ordinateur du réseau (débrancher le câble réseau, désactiver le Wi-Fi) et informez votre service informatique le plus tôt possible.

Vous trouverez ci-dessous des conseils pour mieux gérer vos interactions numériques au quotidien, au travail comme chez vous:

- **Ayez un esprit critique et ne faites pas aveuglément confiance aux e-mails d'expéditeurs que vous pensez connaître**, car il pourrait s'agir de faux e-mails. Ne vous laissez pas tromper par un discours personnalisé ou un texte rédigé sans fautes d'orthographe!
- En cas de doute, contactez l'expéditeur en envoyant un e-mail séparé ou par téléphone et demandez-lui s'il a réellement envoyé cet e-mail. Pour ce faire, n'utilisez jamais le bouton «Répondre» mais choisissez plutôt le contact depuis l'annuaire Outlook.
- Ne répondez jamais aux e-mails suspects.
- **N'ouvrez jamais les pièces jointes suspectes.** En cas de doute, supprimez l'e-mail ou faites-le vérifier par le service informatique.
- **Lors d'un appel téléphonique douteux, ne faites aucune action à laquelle on vous contraindrait sous la menace**. L'interlocuteur souhaite vous piéger, éveiller votre curiosité ou vous effrayer pour vous faire agir de façon irréfléchie. Dans ce cas, tournez-vous immédiatement vers votre supérieur.
- N'autorisez aucune connexion à distance en cas d'assistance sur votre appareil personnel si vous ne connaissez pas la personne qui se connecte à votre ordinateur (par ex. département du service d'assistance informatique).
- **Ne communiquez à personne vos informations de connexion personnelles.** Aucune raison ne le justifierait.
- Gardez toujours en tête les informations personnelles ou professionnelles que vous divulguez. Evitez toute communication professionnelle sur les réseaux sociaux (par ex. Facebook, Instagram).
- **Utilisez toujours des mots de passe forts et modifiez-les régulièrement.**
- N'utilisez votre adresse e-mail professionnelle que dans le cadre de correspondances professionnelles et en aucun cas à des fins privées, par exemple sur des boutiques en ligne ou pour participer à des concours.
- N'enregistrez aucune donnée professionnelle sur votre appareil privé et ne copiez aucune donnée privée sur votre appareil professionnel.
- N'hésitez pas à informer et à impliquer vos supérieurs ou le service informatique en cas d'incident.

Merci pour votre aide!

Meilleures salutations

Alexander von Witzleben	Daniel Wüest	Patrick Langenegger
CEO	CFO	CIO