Image : Pete Linforth, pixabay.com

Mots de passe forts et authentification à deux facteurs pour une meilleure cybersécurité

Le vol d'un montant total de 1,5 milliard de dollars en bitcoins par des pirates nord-coréens a brusquement remis le thème de la cybersécurité sur le devant de la scène en février 2025. Même siles entreprises de technique agricole ne disposent généralement pas d'énormes sommes d'argent sur leurs comptes, elles sont elles aussi constamment menacées de cyberattaques. Les attaques par ransomware (ou rançongiciels) qui cryptent toutes les données de l'entreprise, le vol d'informations confidentielles ou les virements d'argent frauduleux peuvent également causer des dommages dévastateurs aux PME.

Jamais trop petit pour être victime d'un piratage

Les PME ont tendance à penser qu'elles sont trop petites et donc peu intéressantes pour les pirates informatiques. Or, c'est précisément cette réflexion qui rend la situation intéressante pour les cybercriminels. Les PME utilisent fréquemment des structures informatiques similaires qui sont souvent obsolètes. La plupart du temps, elles n'ont pas de service informatique propre qui s'occupe régulièrement des mises à jour de sécurité, des programmes antivirus et de la formation des utilisatrices et utilisateurs. De plus, les pirates informatiques « ajustent » leurs demandes de rançon et exigent des sommes que la PME attaquée est tout juste en mesure de supporter.

Informatique dans le nuage : pas automatiquement sécurisée

L'externalisation des activités informatiques à un fournisseur externe peut être une source de simplification, mais donne souvent une fausse impression de sécurité. Lorsque des pirates informatiques obtiennent le mot de passe d'accès grâce à une ingénierie sociale sophistiquée, les données et sauvegardes stockées en externe peuvent également être cryptées ou volées.

Risque numéro 1 : manipulation insouciante des mots de passe

Les deux principaux points d'entrée des pirates informatiques sont les mots de passe faibles et l'inattention des utilisatrices et utilisateurs de l'ordinateur. Les mots de passe faibles tels que «Tracteur777 » ou le nom de son chat sont déchiffrés en quelques minutes par des ordinateurs performants. La situation est particulièrement critique si le même mot de passe (faible) est utilisé pour plusieurs comptes. Les règles suivantes sont les plus importantes pour les mots de passe :

- Les noms, prénoms, dates de naissance, numéros de téléphone ou plaques d'immatriculation sont tabous, car ces informations sont publiquement accessibles.
- Ne pas utiliser de mots ou de termes existants.
- Le mot de passe doit comporter au moins 12 caractères, des majuscules et des minuscules ainsi que des chiffres et des caractères spéciaux (p. ex. ç, &, *, /, $, ^). Un mot de passe

administrateur doit comporter au moins 16 caractères.
- Utiliser des mots de passe différents pour différents comptes. Il est possible d'utiliser un gestionnaire de mots de passe tel que « KeePass » pour gérer plusieurs mots de passe. Mais attention : si le mot de passe principal du gestionnaire de mots de passe n'est pas protégé de manière conséquente, tous les mots de passe de l'entreprise risquent d'être dévoilés en un seul coup !
- Ne pas enregistrer de mots de passe dans des listes Excel ou des documents Word. Ceux-ci sont faciles à trouver pour les pirates.
- Les meilleurs mots de passe ne servent à rien s'ils sont collés sur un post-it à l'écran ou s'ils sont notés sur un billet que tout le monde peut voir.
- Les mots de passe doivent être changés à intervalles réguliers.

Activer l'authentification à deux facteurs

Les fournisseurs informatiques, les prestataires de services bancaires, mais aussi les boutiques en ligne offrent généralement la possibilité de sécuriser une connexion par une authentification à deux facteurs (2FA). La 2FA peut se faire au moyen d'un SMS envoyé automatiquement avec un code d'accès, d'applications d'authentification spéciales telles que Google Authenticator ou encore de reconnaissance faciale ou d'empreintes digitales. Cette mesure de protection supplémentaire efficace peut être sélectionnée lors de la création d'un compte et peut généralement aussi être activée ultérieurement.

L'ingénierie sociale pour tirer profit des faiblesses humaines

L'une des méthodes les plus répandues des cybercriminels est ce qu'on appelle l'« ingénierie sociale » (social engineering), qui consiste à exploiter de manière ciblée les caractéristiques et les faiblesses humaines. Exemple : un collaborateur de la comptabilité reçoit un e-mail d'un fournisseur. L'expéditeur indique qu'une livraison attendue par le chef de toute urgence ne peut être expédiée que si le montant dû de CHF 22 500.– est versé immédiatement. Une heure après la réception de l'e-mail, le « fournisseur » demande à nouveau ce virement avec insistance. Le collaborateur ne veut pas contrarier le chef et vire le montant qu'il perdra à jamais.

Quand le chef envoie un e-mail …

Une autre forme d'ingénierie sociale est la « fraude au CEO » (arnaque au président), également connue sous le nom de « Business E-Mail Compromise » (BEC). Dans un e-mail qui semble provenir du supérieur hiérarchique, le destinataire est invité à virer de l'argent ou à acheter des bons d'achat dans des boutiques en ligne et à envoyer leurs codes par e-mail. La formation et la sensibilisation sont particulièrement utiles pour lutter contre les attaques par « ingénierie sociale ». Il peut également être très judicieux de définir les transactions pour lesquelles il faut impérativement demander un numéro de rappel à l'interlocuteur. De manière générale, il ne faut jamais fournir de renseignements sur des données sensibles par téléphone ou par e-mail. Les collaboratrices et collaborateurs doivent également être sensibilisés au fait qu'en divulguant des informations personnelles sur les réseaux sociaux, ils peuvent devenir des cibles de l'ingénierie sociale.

Autres conseils pour une meilleure sécurité des données dans les PME

- **Établir un inventaire du matériel et des logiciels disponibles**
  C'est le seul moyen de savoir par exemple si l'entreprise est concernée par une nouvelle faille de sécurité.
- **Droits d'accès restrictifs**
  Dans le travail quotidien, les collaboratrices et collaborateurs ne devraient disposer que de droits d'accès limités. Les droits d'administrateur doivent être réservés aux administrateurs système professionnels.
- **Sensibiliser le personnel aux e-mails de hameçonnage**
  Le hameçonnage (phishing) permet aux cybercriminels d'obtenir des informations d'accès ou d'installer des logiciels malveillants. Les caractéristiques du hameçonnage sont les suivantes :
  - Promesse de bénéfices ou d'avantages en cliquant sur un lien
  - Mettre sous pression, faire peur (menacer p. ex. de bloquer une carte de crédit ou un envoi à la douane)
  - Se faire passer pour une autorité ou un service officiel (police, office des poursuites, etc.)
  - Fausses URL et adresses e-mail. Celles-ci sont souvent difficiles à identifier, car les criminels opèrent également via des serveurs piratés d'entreprises sérieuses ou utilisent un service de raccourcissement d'URL (« https:/t.ly/xxxxxx »). Pour afficher la destination effective d'un lien, il est possible de passer le curseur de la souris dessus. Mais attention de ne pas cliquer !
- **Maintenir le logiciel à jour**
  Les logiciels obsolètes sont l'une des principales portes d'entrée pour les pirates informatiques.
- **Réglementer clairement l'utilisation d'appareils privés**
  Des directives claires sont nécessaires lorsque des collaboratrices ou des collaborateurs accèdent à des informations de l'entreprise (serveur ou nuage) via des appareils mobiles privés. Il en va de même pour l'échange de données via des clés USB.

Une assurance contre les cyberrisques peut offrir une protection supplémentaire

Le respect des règles décrites ici et en particulier la sensibilisation de l'équipe permettent de mieux contrer les cybermenaces dans les PME. Au vu des méthodes d'attaque sans cesse perfectionnées, il n'existe pas de protection absolue. Une assurance spéciale contre les cyberrisques, telle qu'elle est également proposée par le partenaire d'assurance d'AM Suisse PROMRISK AG *(promrisk.ch),* peut constituer un filet de sécurité supplémentaire.

L'assurance responsabilité civile d'entreprise ne couvre en effet que les dommages corporels et matériels causés à des tiers par la faute de l'assuré. Les préjudices pécuniaires subis par le client d'une entreprise de technique agricole en cas de vol de données ne sont pas couverts. Les coûts élevés résultant d'interruptions d'exploitation, de pertes de revenus, de remise en état d'infrastructures informatiques et d'éventuels litiges juridiques ne sont généralement couverts que si une assurance spécifique contre les cyberrisques a été conclue. ■

Emanuel Scheidegger