Protégez votre entreprise contre les attaques de rançongiciel

Selon le Rapport annuel officiel sur la cybercriminalité de 2019, une entreprise est victime d'une attaque de rançongiciel toutes les 14 secondes. Avec des employés en télétravail et opérant en dehors du pare-feu de l'entreprise, le risque augmente.

De quoi s'agit-il ?

Le rançongiciel est un logiciel malveillant qui bloque l'accès de l'utilisateur au système informatique ou à son appareil jusqu'au versement d'une somme d'argent. Le logiciel malveillant trouve et chiffre des données précieuses et bloque les utilisateurs en dehors de leurs systèmes d'exploitation, puis exige un paiement, en général sous la forme de bitcoins ou une autre cryptomonnaie, pour révéler la clé de décryptage.

Il n'y a aucune garantie qu'en payant la rançon, les victimes puissent retrouver l'accès à leurs appareils et données.

Sauvegarder et mettre à jour

Utilisez plusieurs solutions de sauvegarde et assurez-vous qu'au moins l'une d'entre elles est hors ligne en permanence. N'oubliez pas : les services de synchronisation sur le cloud comme Dropbox ou Google Drive peuvent se synchroniser une fois que les données ont été chiffrées, ce qui rend la sauvegarde inutile.

Mettez à jour régulièrement le logiciel antivirus de l'entreprise et choisissez un fournisseur qui propose des modules complémentaires repérant le chiffrement des fichiers et effectuant automatiquement des copies des fichiers menacés.

Choisissez un mot de passe sécurisé et changez-le régulièrement. N'oubliez pas que les attaques en force représentent 31 % de l'ensemble des attaques.

L'élément humain

Formez les employés à reconnaître et signaler les e-mails suspects. Les rançongiciels peuvent facilement se propager à partir des spams et des e-mails de hameçonnage.

Utilisez l'analyse de contenu et les filtres de courrier électronique pour ajouter un niveau supplémentaire de protection. Ces outils peuvent détecter les liens malveillants et supprimer les e-mails dangereux avant qu'ils n'atteignent le personnel.

Assurez-vous d'appliquer un protocole de sécurité standardisé au sein de l'entreprise, depuis les employés jusqu'aux postes de direction.

Développez un plan de reprise d'urgence qui prévoit une réponse à une attaque potentielle. Incluez-y des directives techniques mais également des stratégies pour atténuer les conséquences juridiques et sur la réputation.

Vérifiez avec vos assureurs si votre police couvre les coûts associés à une attaque de rançongiciel.

Créez une stratégie de relations publiques pour expliquer la situation à vos clients, investisseurs et à la presse en cas d'attaque.

Pour plus de conseils d'expert en matière de cybersécurité dans votre usine intelligente, consultez le www.euautomation.com