maiage
Les hommes et les entreprises de la maintenance environnementale
HEBDO

CYBERSECURITE – 5 TENDANCES A SUIVRE EN 2024

Les attaques assistées par l'IA vont accélérer la cybercriminalité, tandis que les entreprises rencontreront de plus en plus de difficultés pour souscrire des polices de cyberassurance. Plusieurs conditions sont susceptibles d'affecter les entreprises de toutes tailles en 2024 dans le domaine de la sécurité IT.

Selon **Dirk Schrader, Vice-President Security Research de Netwrix, et Ilia Sotnikov, Security strategist**, cinq tendances majeures devraient se dégager :

1. **Les conditions d'accès aux contrats de cyberassurance vont se resserrer**. Face au succès des cyberattaques et à l'augmentation des paiements, les assureurs exigeront que davantage d'organisations implémentent des mesures de sécurité solides pour bénéficier d'une police d'assurance ou réduire les primes. Les principales conditions à remplir sont : l'authentification multifacteurs (MFA), la gestion des correctifs et la formation régulière à la cybersécurité des employés. En 2024, la gestion des accès et des identités (IAM) devrait s'ajouter, particulièrement pour les grands comptes. De plus, les assureurs devront s'associer à des fournisseurs de services managés pour garantir un niveau de sécurité minimum aux PME.

2. **Les attaquants vont récolter de plus en plus de données chiffrées, même inexploitables.** La rapide progression de l'informatique quantique encouragera les cybercriminels les plus avant-gardistes à s'emparer de données chiffrées que la technologie actuelle ne permet pas encore de déchiffrer. Les principales cibles seront les organisations détenant d'importantes quantités de données sensibles (agences gouvernementales et de défense, sociétés financières, cabinets d'avocats, ou encore entreprises à la propriété intellectuelle de grande valeur).

Pour réduire les risques, les organisations ne doivent pas considérer le chiffrement comme la panacée, mais élaborer une stratégie à plusieurs niveaux : classification des données, évaluation et atténuation des risques, détection et réponse aux incidents. Elles doivent également tenir compte du fait que la collecte de données peut passer inaperçue sans demande de rançon immédiate ou toute autre conséquence visible, tout en améliorant la surveillance des activités qui entourent leurs données sensibles, incluant les contenus chiffrés.

3. **Les outils d'IA permettront aux cybercriminels de collecter facilement les informations nécessaires.** Grâce à l'IA, les acteurs malveillants localiseront rapidement les informations personnelles utiles à la rédaction d'emails de phishing convaincants et l'exploitation des bases de données qui renferment des identifiants volés afin de lancer des offensives efficaces basées sur des mots de passe. Imposer l'utilisation de mots de passe uniques et forts, contrôler étroitement les accès à privilèges et investir dans des solutions de détection et réponse aux menaces d'identité (ITDR — Identity Threat Detection and Response), permettra de réduire les risques.

4. **De plus en plus difficiles à repérer, les emails de phishing vont proliférer dans les pays non anglophones.** Les emails de phishing ont longtemps été rédigés en anglais et truffés de coquilles ou d'erreurs grammaticales. Mais en 2024, les outils d'IA permettront aux attaquants de créer plus facilement des missives convaincantes dans la langue de leur choix. Pour riposter, les entreprises doivent actualiser les formations consacrées au phishing et faire en sorte que leurs employés puissent facilement signaler les messages suspects. Dans les régions non anglophones, les équipes IT doivent également avertir les utilisateurs de la probabilité croissante de recevoir des emails malveillants en langue maternelle.

5. **Personne n'est à l'abri de la lassitude inhérente aux contrôles de sécurité.** Dans la mesure où il suffit qu'un seul compte soit compromis pour pénétrer dans l'écosystème IT d'une entreprise, les identités des utilisateurs constituent une cible privilégiée des cybercriminels. Toutefois, submerger les utilisateurs d'avertissements envoyés par des outils tels que les agents de messagerie ou les inviter à de fréquentes formations de sensibilisation peut avoir un effet inverse et faire naître un sentiment de lassitude. Un contrôle excessif de la sécurité peut provoquer les erreurs et les négligences que les entreprises tentent d'éviter. Plus efficace encore, l'adoption d'un modèle ZeroTrust basé sur le principe du moindre privilège. En outre, adapter les formations de sensibilisation aux besoins de chaque groupe d'employés facilitera l'assimilation.

Source : IT CHANNEL - Novembre 2023