1. Incidents de sécurité majeurs

a. Attaques contre les détaillants britanniques

En avril 2025, plusieurs détaillants britanniques, dont Marks & Spencer (M&S), Co-op et Harrods, ont été victimes d'attaques informatiques. Les cybercriminels ont utilisé des techniques d'ingénierie sociale pour tromper les services informatiques et réinitialiser les mots de passe des employés, permettant un accès non autorisé aux réseaux internes. Ces attaques ont entraîné des perturbations dans les services, notamment des retards de livraison et des problèmes de paiement .([The Scottish Sun, Latest news & breaking headlines](#))

b. Violation de données chez Yale New Haven Health

Le système de santé Yale New Haven Health a subi une violation de données majeure, exposant les dossiers médicaux de 5,5 millions de patients. Cette brèche souligne la vulnérabilité persistante du secteur de la santé face aux cyberattaques .([strokes.co](#))

c. Campagne de phishing ciblant les services de marketing par e-mail

Une campagne de phishing à grande échelle a compromis les comptes de services de marketing par e-mail tels que Mailchimp, SendGrid, HubSpot, Mailgun et Zoho. Cette attaque a permis aux cybercriminels d'accéder à des informations sensibles et de diffuser des e-mails malveillants . ([Formation Cybersécurité UK](#))

2. Vulnérabilités critiques (CVE)

a. CVE-2025-26686 – Microsoft Windows TCP/IP

- **Score CVSS** : 7.5 (Élevé)
- **Description** : Vulnérabilité dans l'implémentation TCP/IP de Windows permettant l'exécution de code à distance via des réponses réseau spécialement conçues.
- **Correctif** : Inclus dans le Patch Tuesday d'avril 2025 .

b. CVE-2025-27491 – Microsoft Hyper-V

- **Score CVSS** : 7.1 (Élevé)
- **Description** : Vulnérabilité de type "use-after-free" dans Hyper-V permettant à un attaquant authentifié d'exécuter du code arbitraire.
- **Correctif** : Corrigé dans les mises à jour de sécurité d'avril 2025 .([crowdstrike.com](#))

c. CVE-2025-26647 – Authentification Kerberos

- **Description** : Problème d'authentification Kerberos lié à une autorité de certification présente dans le magasin racine Windows mais absente du magasin NTAAuth, affectant les comptes privilégiés.
- **Correctif** : Mise à jour de sécurité publiée le 8 avril 2025 .([Support Microsoft](#))

3. Outils et techniques utilisés par les attaquants

- **Ingénierie sociale avancée** : Les cybercriminels ont utilisé des techniques sophistiquées, telles que le "SIM swapping" et l'usurpation d'identité, pour tromper les services informatiques et obtenir un accès non autorisé aux systèmes .([Latest news & breaking headlines](#))
- **Exploitation de l'IA** : L'utilisation de modèles de langage avancés (LLM) par les attaquants a permis des attaques plus ciblées et efficaces, notamment en identifiant rapidement les vulnérabilités et en automatisant les campagnes de phishing .

4. Tendances observées

- **Adoption croissante de l'authentification sans mot de passe** : À l'occasion de la Journée mondiale du mot de passe 2025, l'industrie a mis en avant les alternatives telles que les passkeys et l'authentification biométrique pour améliorer la sécurité des identifiants .
- **Augmentation des attaques ciblant les infrastructures critiques** : Les secteurs de la santé, de l'énergie et des télécommunications ont été particulièrement visés, soulignant la nécessité de renforcer la résilience de ces infrastructures .