Nikola Mihajlovic Février 2026

Les cyberattaques majeures de 2024–2025 et leurs impacts sur les organisations.

Depuis plusieurs années, la transformation numérique des entreprises s'accélère. Les systèmes d'information deviennent plus complexes, interconnectés et dépendants d'Internet. Cette évolution apporte de nombreux avantages en matière de productivité et de communication, mais elle augmente également la surface d'attaque des organisations. En 2024 et 2025, les cyberattaques ont connu une intensification significative, tant en nombre qu'en sophistication. Les groupes cybercriminels se professionnalisent, utilisent des outils avancés et exploitent des vulnérabilités de plus en plus rapidement après leur découverte.

Cette veille technologique a pour objectif d'analyser les principales cyberattaques observées en 2024 et 2025, d'en comprendre les mécanismes techniques et d'étudier leurs conséquences sur les entreprises, les administrations et les infrastructures critiques.

Méthodologie de veille

Cette veille a été réalisée à partir de sources institutionnelles et spécialisées reconnues dans le domaine de la cybersécurité. Les rapports de l'ANSSI, du CERT-FR et de l'ENISA ont constitué une base fiable pour identifier les tendances majeures. Des analyses issues du rapport IBM X-Force Threat Intelligence Index ainsi que des bulletins de sécurité publiés par Kaspersky ont également permis de compléter les informations. Des articles issus de sites spécialisés en cybersécurité ont été consultés afin d'obtenir des exemples concrets d'attaques récentes.

Les informations ont été collectées via des flux d'actualités, des alertes automatisées et des publications officielles afin de garantir l'actualité des données étudiées.

Les ransomwares en 2024–2025

Les ransomwares demeurent la menace la plus répandue et la plus impactante. Le principe reste identique : les attaquants parviennent à pénétrer le système d'information d'une organisation, chiffrent les données essentielles et exigent une rançon en échange de la clé de déchiffrement. Toutefois, les méthodes ont évolué.

En 2024 et 2025, la pratique de la double extorsion s'est généralisée. Les attaquants ne se contentent plus de chiffrer les données, ils les exfiltrent également afin de menacer leur publication. Cette pression supplémentaire pousse davantage d'organisations à payer la rançon. Dans certains cas, une triple extorsion est observée, avec des pressions exercées sur les partenaires ou les clients de la victime.

Les secteurs de la santé et des collectivités locales ont été particulièrement touchés. Plusieurs hôpitaux européens ont subi des interruptions de service majeures, entraînant des retards de soins et des pertes financières importantes. Les petites et moyennes entreprises sont également des cibles privilégiées, car leurs systèmes sont souvent moins protégés.

L'EXPLOITATION DES FAILLES ZERO-DAY

Une autre tendance forte concerne l'exploitation de vulnérabilités zero-day. Une faille zero-day correspond à une vulnérabilité inconnue du fournisseur du logiciel au moment où elle est exploitée par des attaquants. En 2024 et 2025, la rapidité d'exploitation des failles s'est considérablement réduite. Il arrive désormais que des systèmes soient compromis quelques heures seulement après la publication d'un correctif.

Les serveurs VPN, les solutions de gestion à distance et certains logiciels d'entreprise ont été ciblés. Une fois la faille exploitée, les attaquants procèdent généralement à une élévation de privilèges puis à un mouvement latéral dans le réseau afin d'étendre leur contrôle. Cette technique permet de compromettre un grand nombre de machines avant que l'intrusion ne soit détectée.

LE PHISHING ASSISTÉ PAR INTELLIGENCE ARTIFICIELLE

L'intelligence artificielle joue un rôle croissant dans les cyberattaques. En 2024 et 2025, des campagnes de phishing ont utilisé des outils d'IA pour générer des messages extrêmement crédibles. Les courriels imitent le style d'écriture de dirigeants ou de partenaires commerciaux, rendant la fraude plus difficile à détecter.

Des cas d'usurpation d'identité par deepfake audio ont également été signalés. Des employés ont été convaincus de transférer des fonds ou de communiquer des informations sensibles après avoir reçu un appel imitant la voix d'un supérieur hiérarchique. Cette évolution démontre que la menace ne repose plus uniquement sur des failles techniques, mais également sur la manipulation psychologique.

Les secteurs les plus touchés

Les infrastructures critiques figurent parmi les principales cibles. Les établissements de santé, les réseaux énergétiques et les administrations publiques présentent des enjeux stratégiques élevés. Une attaque réussie peut provoquer une interruption de services essentiels, affecter la population et engendrer une crise de confiance.

Les entreprises technologiques et les fournisseurs de services cloud sont également exposés. Les erreurs de configuration dans les environnements cloud ont permis l'exposition de bases de données sensibles. Ces incidents montrent que la sécurité ne dépend pas uniquement des outils utilisés, mais aussi de la compétence des équipes chargées de les configurer.

Les conséquences pour les organisations

Les impacts financiers des cyberattaques sont considérables. Outre le paiement éventuel d'une rançon, les coûts incluent la restauration des systèmes, l'arrêt de production et les pertes de chiffre d'affaires. Les sanctions liées au non-respect du RGPD peuvent également être importantes en cas de fuite de données personnelles.

Les conséquences juridiques et réputationnelles sont tout aussi préoccupantes. Une entreprise victime d'une cyberattaque peut perdre la confiance de ses clients et partenaires. Cette perte de crédibilité peut avoir des effets durables sur son activité.

L'évolution des stratégies de défense

Face à l'augmentation des menaces, les organisations adaptent leurs stratégies de sécurité. Le modèle Zero Trust gagne en popularité. Ce principe repose sur l'idée qu'aucun utilisateur ou appareil ne doit être considéré comme fiable par défaut, même s'il se trouve à l'intérieur du réseau.

L'authentification multi-facteurs se généralise afin de limiter les risques liés au vol d'identifiants. La segmentation des réseaux permet de contenir la propagation d'une attaque. Les sauvegardes hors ligne deviennent essentielles pour se prémunir contre les ransomwares.

Par ailleurs, la formation des employés est désormais considérée comme un pilier fondamental de la cybersécurité. Une grande partie des attaques exploitent des erreurs humaines. Sensibiliser les utilisateurs permet de réduire significativement le risque.

Analyse et perspective

Les cyberattaques observées en 2024 et 2025 montrent une professionnalisation croissante des groupes criminels. Certains fonctionnent comme de véritables entreprises, avec des services d'assistance et des modèles économiques structurés. La cybersécurité doit donc être intégrée à la stratégie globale des organisations et non plus considérée comme un simple coût informatique.

L'avenir laisse présager une intensification de l'utilisation de l'intelligence artificielle, tant du côté des attaquants que des défenseurs. Les entreprises devront investir davantage dans des solutions de détection avancées et adopter une approche proactive.

Conclusion

Les cyberattaques majeures de 2024 et 2025 démontrent que la menace numérique évolue rapidement et touche tous les secteurs d'activité. Les ransomwares, l'exploitation de failles zero-day et le phishing assisté par intelligence artificielle représentent des risques majeurs pour les organisations.

La cybersécurité devient un enjeu stratégique incontournable. Les entreprises doivent renforcer leurs systèmes de défense, former leurs employés et adopter des modèles de sécurité adaptés aux nouvelles menaces. Dans un monde de plus en plus connecté, la protection des systèmes d'information est désormais essentielle à la continuité des activités.