# Les Cyberattaques contre les PME en Nette Augmentation

Les dirigeants des petites et moyennes entreprises sont-ils suffisamment préparés face à l'escalade des menaces cybernétiques?

Ce rapport d'ACI Technology analyse la maturité des efforts de cybersécurité de 217 dirigeants d'entreprises de moins de 500 employés et révèle que les violations sont non seulement courantes, mais souvent récurrentes.

# Une Préparation Organisationnelle Insuffisante

La préparation organisationnelle est essentielle pour se défendre efficacement contre les cyberattaques. Des politiques de bonnes pratiques aux logiciels de cybersécurité, les PME doivent employer un large éventail de protections pour protéger leurs actifs les plus précieux.

**60%**

### Se sentent préparés

Des dirigeants pensent que leur organisation est adéquatement préparée à une cyberattaque.

**45%**

### Se croient ciblés

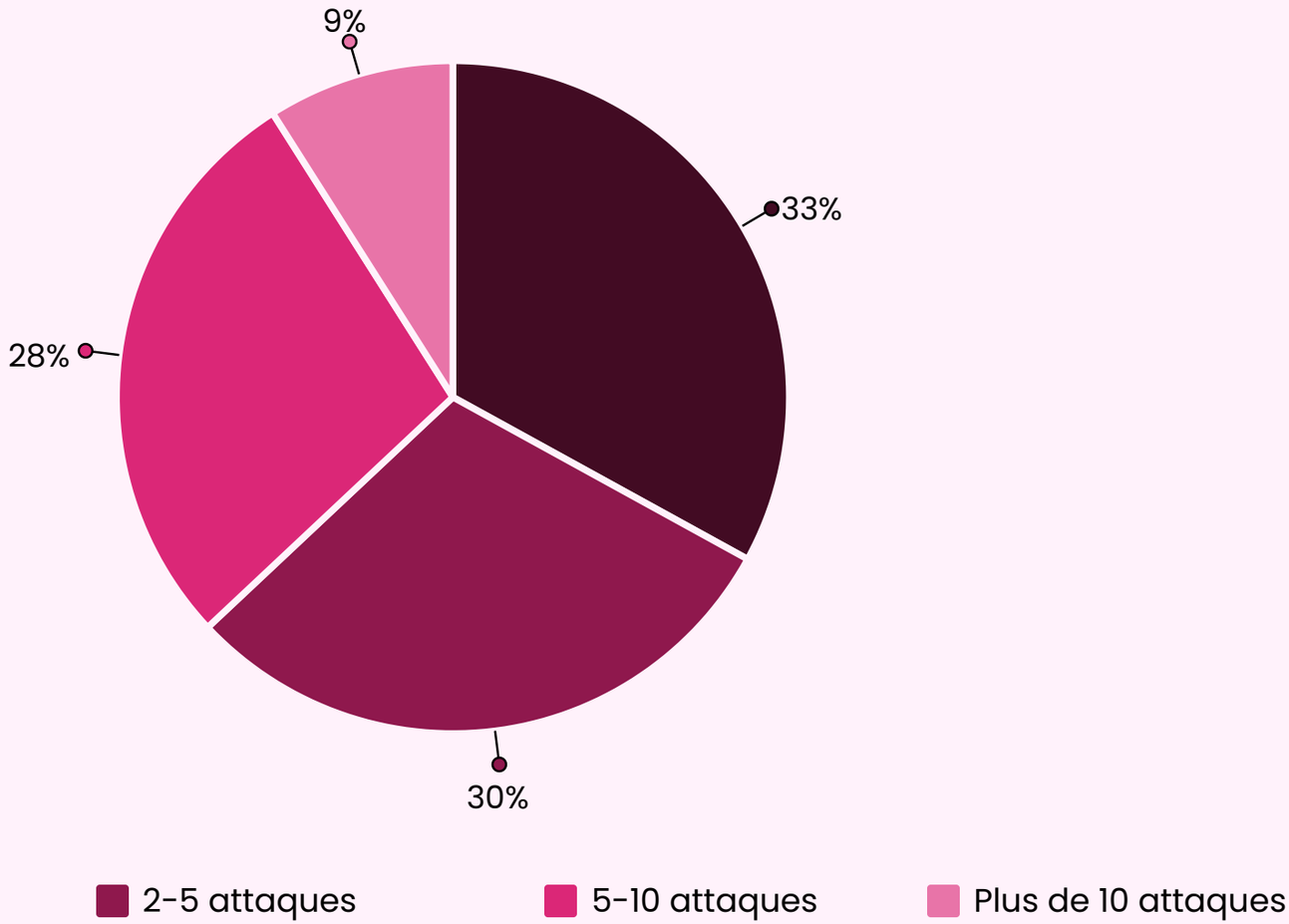
Des responsables estiment que leur entreprise est susceptible d'être ciblée par des cyberattaques.

**3×**

### Plus de risques

Les petites entreprises sont trois fois plus susceptibles d'être ciblées par des cybercriminels que les grandes entreprises.

# La Fréquence Alarmante des Cyberattaques



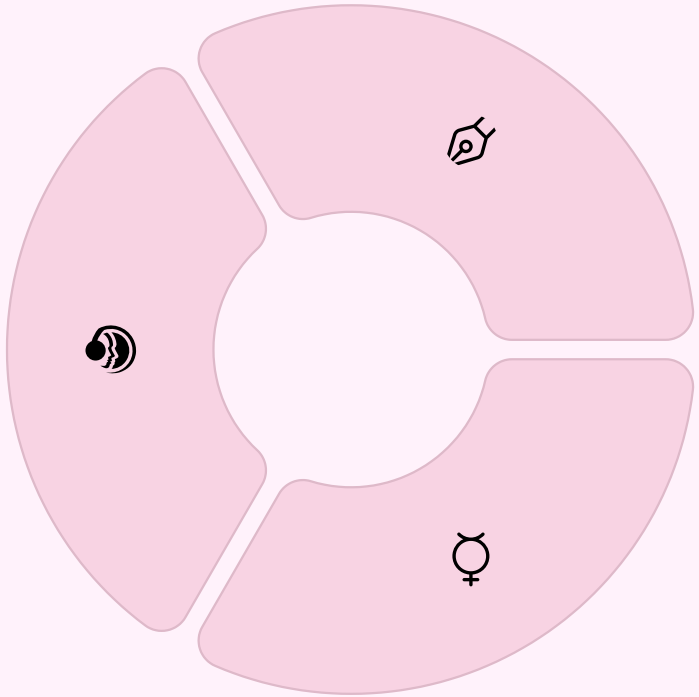

Parmi les entreprises ayant subi une cyberattaque, 67% ont vécu cette expérience plus d'une fois, démontrant l'importance cruciale d'une stratégie de cybersécurité complète et proactive.

# Responsabilité de la Cybersécurité

Un manque de centralisation de la responsabilité en matière de cybersécurité constitue un facteur de risque majeur pour les PME. La responsabilité incombe principalement aux équipes internes, qui gèrent probablement l'informatique quotidienne parallèlement à d'autres priorités concurrentes.

### Équipe interne

La majorité des entreprises confient la cybersécurité à des équipes internes souvent surchargées.



### Prestataire externe

Solution privilégiée par de nombreuses PME pour bénéficier d'une expertise spécialisée.

### Approche hybride

Combinaison d'équipes internes et externes pour une couverture optimale.

# Documentation des Politiques de Cybersécurité

En matière de documentation des politiques et pratiques de cybersécurité, de nombreuses organisations manquent des éléments fondamentaux.

59%

### Politique officielle

Organisations disposant d'une politique officielle de cybersécurité pour les employés.

46%

### Stratégie cybersécurité

Entreprises ayant formalisé une stratégie de cybersécurité documentée.

35%

### Plan de reprise

PME disposant d'un plan de reprise après sinistre en cas d'incident.

29%

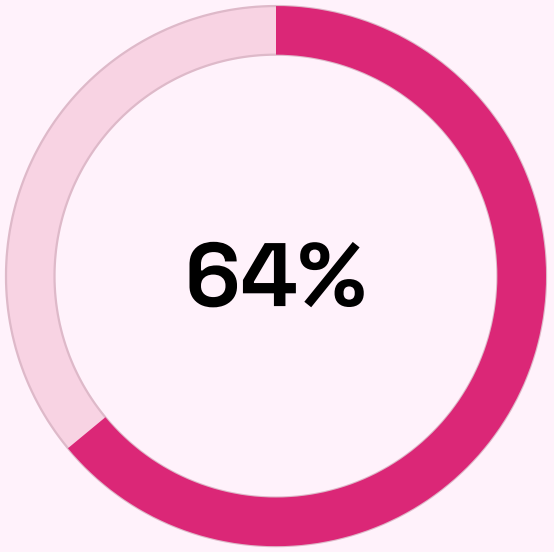
### Politique BYOD

Organisations ayant mis en place une politique d'utilisation des appareils personnels.

Alarmant : 13% des répondants déclarent n'avoir aucune documentation de politique de cybersécurité.

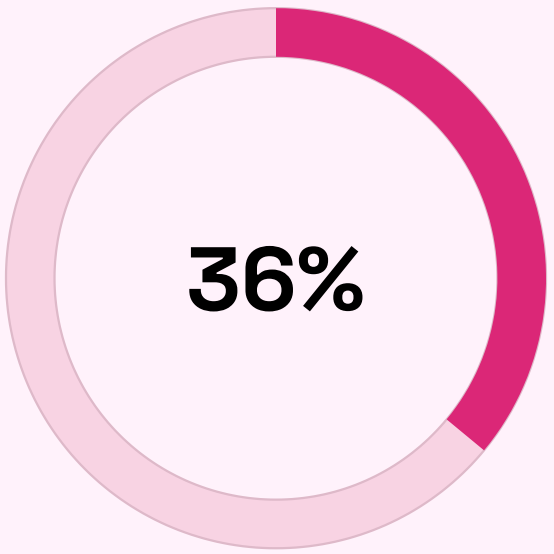
# Adaptation au Travail à Distance

Bien que de nombreux aspects de la documentation sur la cybersécurité semblent sporadiques, les petites entreprises ont été plus proactives dans l'ajustement de leurs politiques pour intégrer le travail à distance et hybride.


**Actualisation**

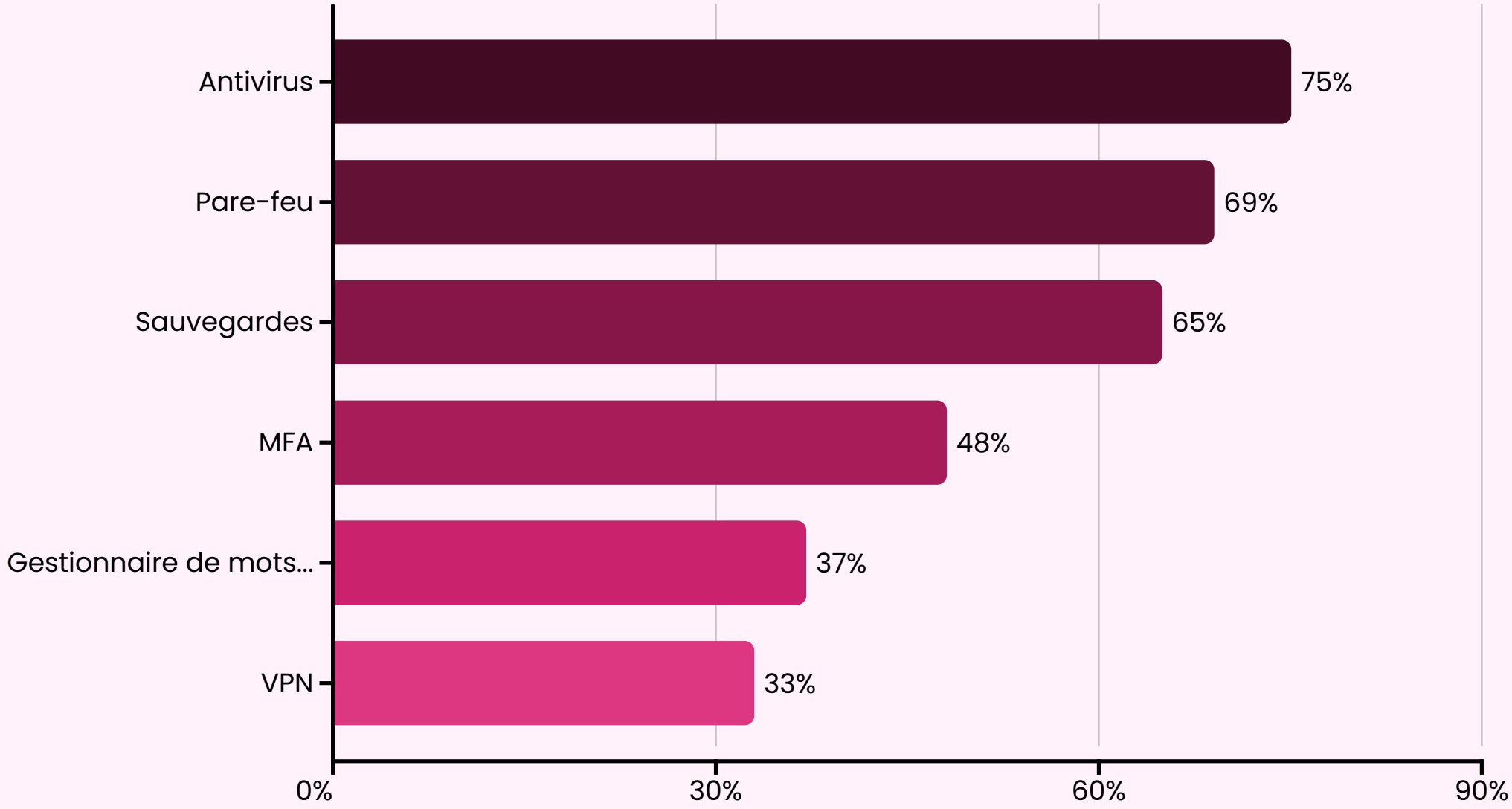
Des organisations ont mis à jour leurs pratiques de cybersécurité en réponse au travail à distance.




**Stagnation**

Des entreprises n'ont pas adapté leur politique de sécurité malgré la transformation du mode de travail.

# Mesures de Cybersécurité Couramment Utilisées




L'efficacité des politiques de cybersécurité dépend de certaines protections en place. La majorité des PME déclarent avoir mis en place des antivirus, des pare-feu et des sauvegardes de données, tandis que l'authentification multifactorielle (MFA) est utilisée par un peu moins de la moitié des organisations.

# Une Plateforme Unique pour Tous vos Besoins de Sécurité

La plateforme ACI Technology répond à tous vos besoins informatiques et de sécurité en un seul endroit. Pour protéger votre organisation et les données de vos clients, notre solution adopte une approche de cybersécurité à plusieurs niveaux.

### Politique et formation

Développement et mise en œuvre de politiques de cybersécurité et de programmes de formation adaptés à votre organisation.

### Sécurité des appareils

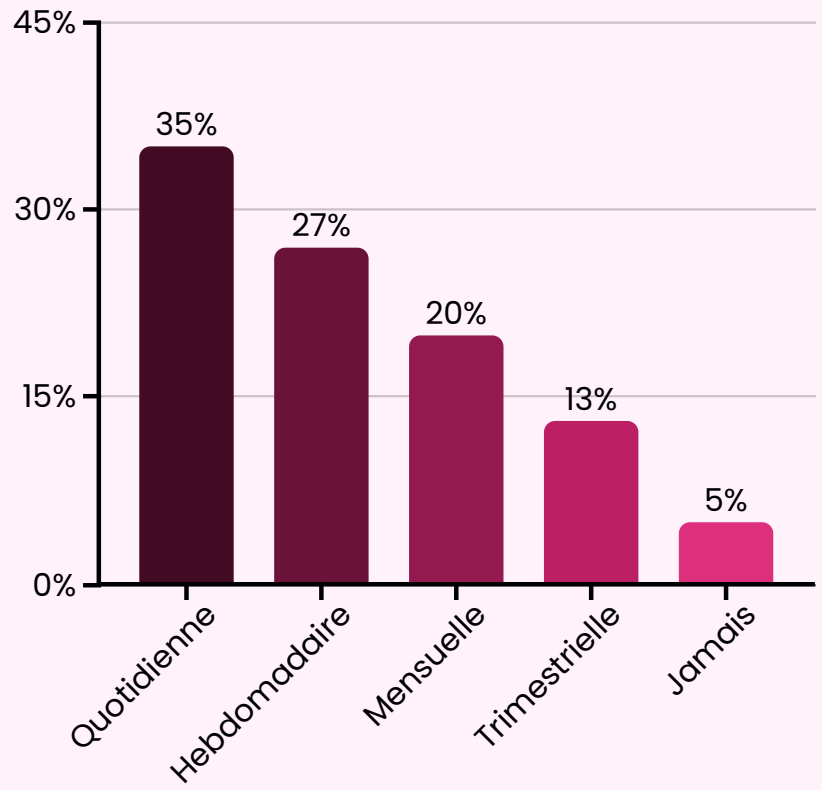
Protection complète de tous les points d'accès à votre réseau d'entreprise grâce à des solutions EDR avancées.

### Sécurité réseau

Surveillance continue et protection contre les intrusions pour garantir l'intégrité de votre infrastructure.

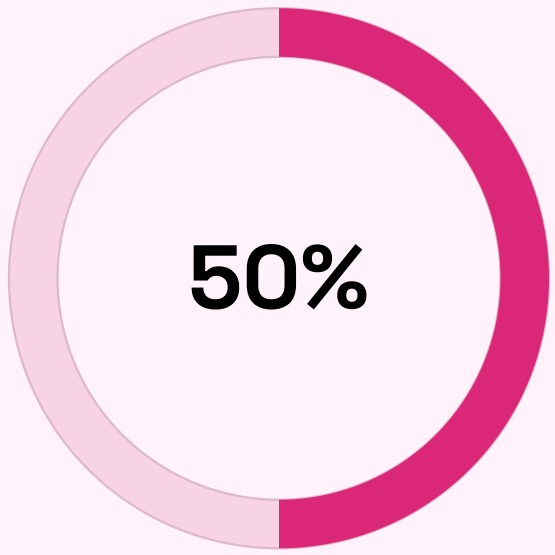
# Pratiques de Sauvegarde des Données

## Fréquence des sauvegardes



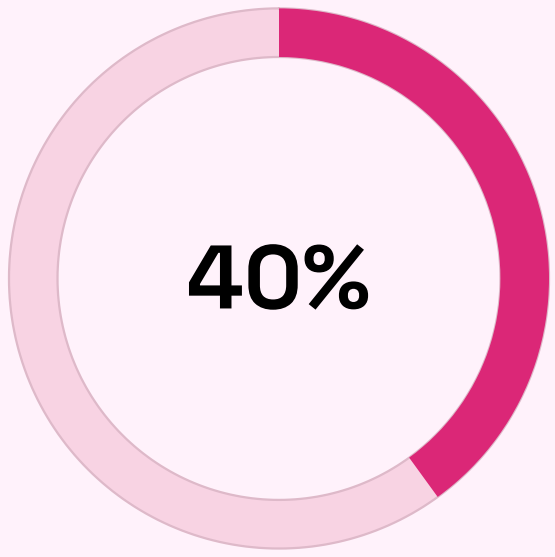

## Méthode de stockage

La moitié des organisations stockent leurs sauvegardes de manière sécurisée dans le cloud. Cependant, 40% s'appuient sur leur réseau d'entreprise pour les sauvegardes de données, ce qui constitue un choix à haut risque en cas d'attaque.




**Cloud**

Stockage sécurisé et isolé des sauvegardes




**Réseau**

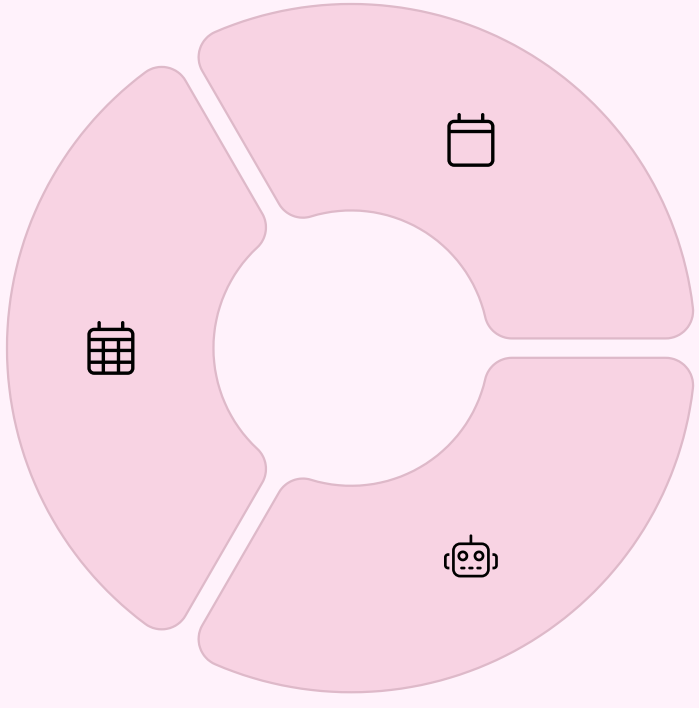
Stockage à risque en cas d'attaque

# Mises à Jour Logicielles et Matérielles

Les mises à jour des logiciels et des appareils sont effectuées "selon les besoins" dans la majorité des petites entreprises, ce qui est positif si elles sont réalisées de manière opportune et régulière.

### Selon les besoins

Approche réactive mais flexible des mises à jour de sécurité



### Planifiées

Mise à jour selon un calendrier fixe pour maintenir la conformité

### Automatisées

Seulement 14% des entreprises automatisent leurs mises à jour

# Sensibilisation des Employés aux Cybermenaces

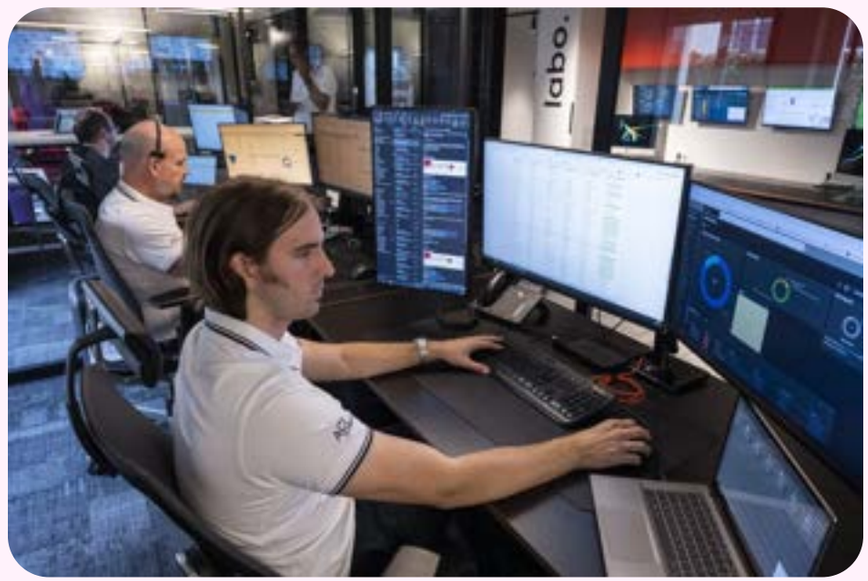
La sensibilisation des employés joue un rôle vital dans la défense contre les cyberattaques, notamment lorsqu'il s'agit d'initier une réponse rapide et efficace.

### Procédure de signalement

65% des organisations disposent d'une procédure officielle permettant aux employés de signaler les attaques suspectées.

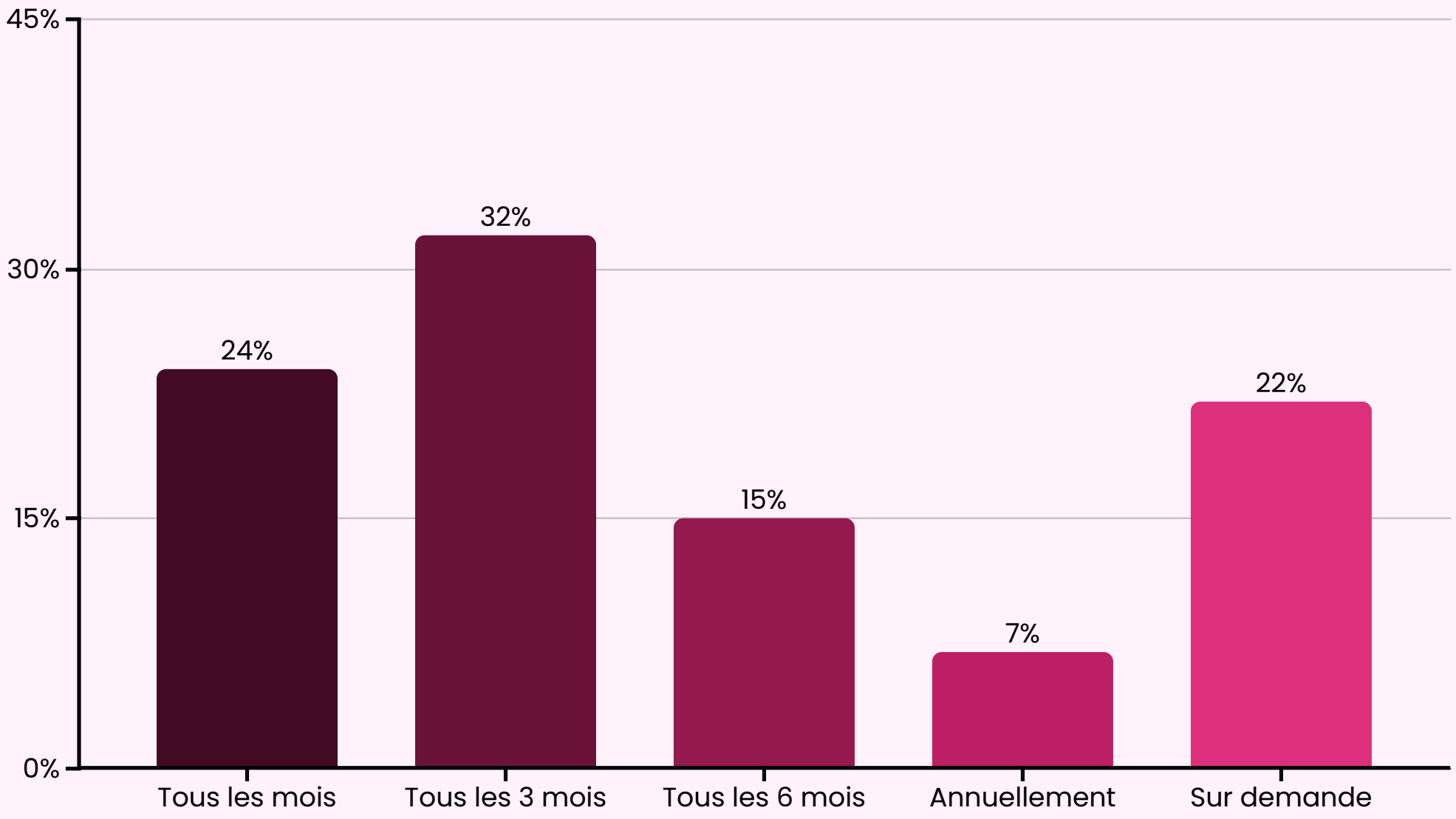
### Reconnaissance du phishing

92% des dirigeants sont confiants dans la capacité de leurs employés à identifier les emails de phishing.




La majorité des dirigeants d'entreprise (83%) ont reçu un email de phishing, et 81% indiquent que d'autres personnes de leur entreprise ont également été ciblées.

# Gestion des Mots de Passe




La fréquence à laquelle les employés mettent à jour leurs mots de passe varie, mais la majorité respecte les bonnes pratiques en les changeant tous les trois mois ou moins. 22% supplémentaires déclarent mettre à jour leurs identifiants lorsqu'ils y sont invités par un gestionnaire de mots de passe.

# Formation en Cybersécurité

La plupart des organisations ont fait des efforts pour améliorer la sensibilisation des employés aux risques cyber, 65% déclarant avoir reçu une formation organisée par l'entreprise sur le phishing.

### Mensuelle

26% des entreprises organisent une formation mensuelle en cybersécurité, créant une culture de vigilance constante.

### Selon les besoins

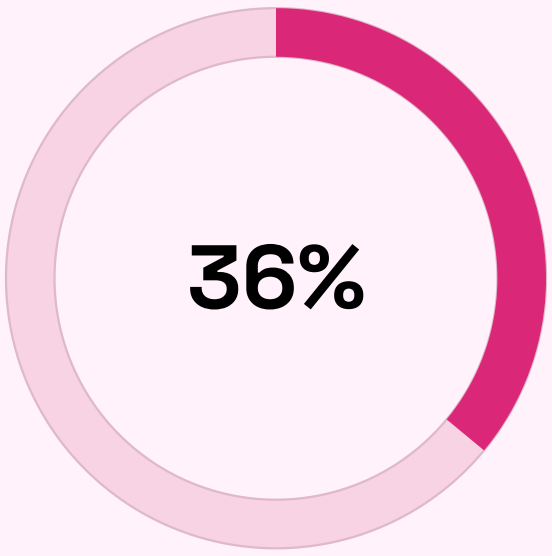
29% dispensent une formation "selon les besoins", adaptant leur approche aux nouvelles menaces émergentes.

### Jamais

18% des répondants affirment que ces formations ne sont jamais organisées dans leur entreprise, créant une vulnérabilité critique.

# Escalade des Tentatives de Cyberattaques

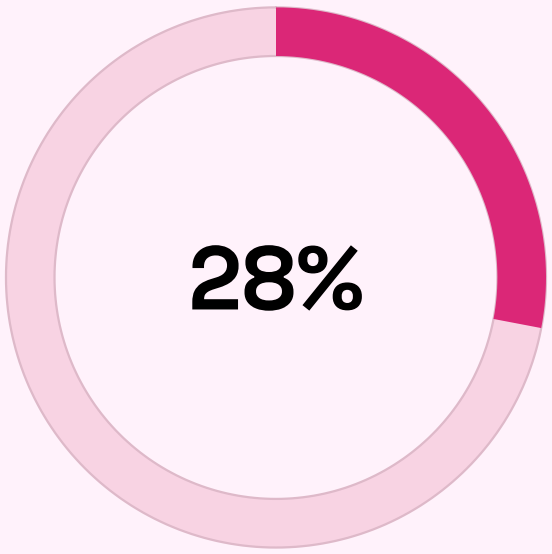
Alors que de nombreuses petites entreprises s'appuient sur des politiques de cybersécurité fragmentées, les attaques se poursuivent à un rythme préoccupant.


**Augmentation**

Des entreprises ont constaté une augmentation des tentatives de cyberattaques au cours de l'année écoulée.

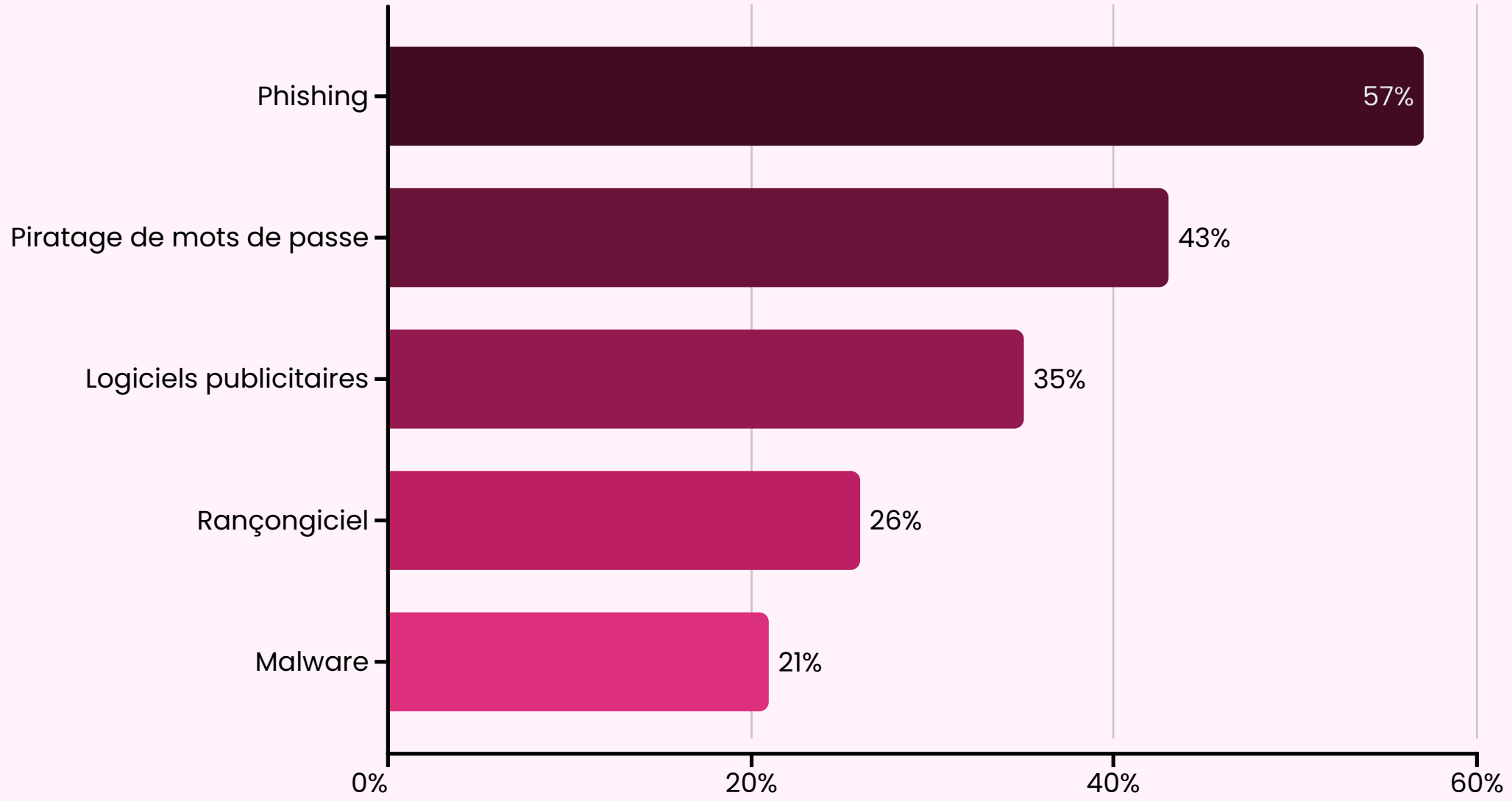
Les employés des petites entreprises subissent **350%** plus d'attaques d'ingénierie sociale que ceux des grandes entreprises, mettant en évidence leur vulnérabilité particulière.




**Incertitude**

Des organisations ne peuvent pas être certaines si de telles tentatives ont augmenté.

# Types de Cyberattaques Subies




47% des petites entreprises ont été victimes de cyberattaques, le phishing, le piratage de mots de passe et les logiciels publicitaires étant en tête de liste des tactiques. Parmi les 26% ciblées par des rançongiciels, 60% ont payé la rançon, dont un tiers n'a jamais récupéré leurs données.

# Vulnérabilités Contribuant aux Attaques

Dans les petites et moyennes entreprises, certaines vulnérabilités de cybersécurité sont systématiquement exploitées par les cybercriminels.

### Erreur humaine

Première cause dans la plupart des attaques réussies, indiquant que les efforts de formation et de sensibilisation ne vont toujours pas assez loin.

### Logiciels obsolètes

Les antivirus, appareils et systèmes d'exploitation non mis à jour constituent des points d'entrée privilégiés pour les attaquants.

### Absence de pare-feu

Le manque de protection réseau élémentaire laisse les systèmes exposés aux intrusions.

# Défenses Efficaces Contre les Cyberattaques

Parmi les entreprises qui ont repoussé des tentatives d'attaques, la majorité attribue leur défense réussie à une combinaison de logiciels antivirus, de sensibilisation des employés, de pare-feu et de mises à jour régulières.

1

**Logiciels de sécurité**

Antivirus et pare-feu modernes avec détection avancée des menaces

2

**Formation continue**

Sensibilisation régulière des employés aux nouvelles menaces

3

**Mises à jour systématiques**

Application rigoureuse des correctifs de sécurité

# Cibles Principales des Cyberattaques

Parmi les petites entreprises ayant subi des cyberattaques, les cibles les plus fréquemment signalées comprennent la perturbation des activités, suivie de près par les données financières des clients et les adresses email ou identifiants de connexion.

### Perturbation d'activité

Interruption des opérations commerciales critiques

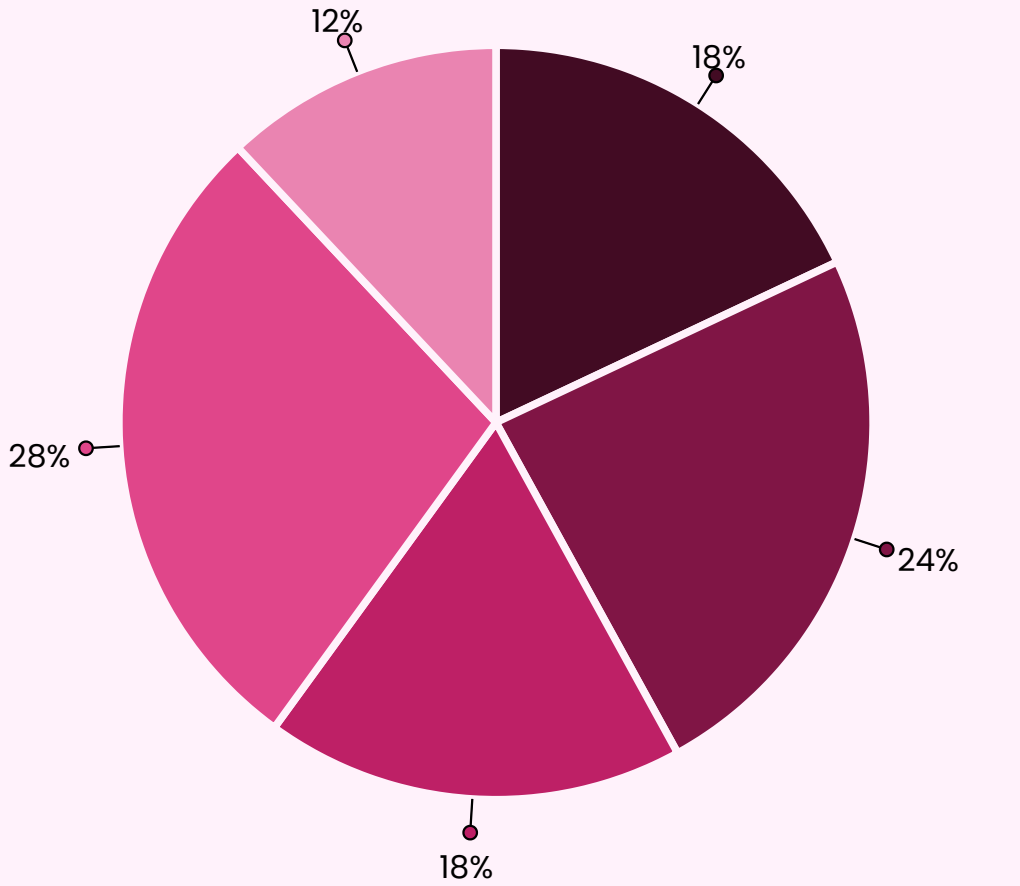
### Données financières

Informations bancaires et de paiement des clients

### Identifiants

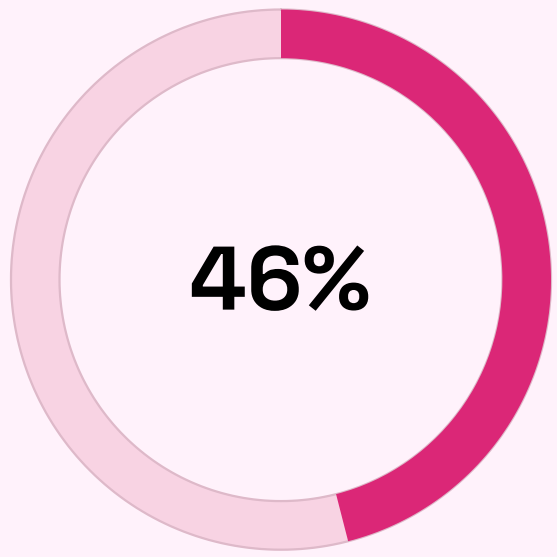
Adresses email et informations de connexion

# Impact des Cyberattaques sur les Entreprises




## Impact financier

22% indiquent que le coût des cyberattaques pour leur entreprise se situe entre 50 000€ et 100 000€, et 20% ont signalé des dommages de plus de 100 000€. Compte tenu du faible taux d'adoption des assurances cybersécurité, ces coûts peuvent être paralysants pour une petite entreprise.




**Indisponibilité**

Des entreprises ont subi une interruption d'activité suite à une cyberattaque

# Combler les Lacunes en Cybersécurité avec ACI Technology

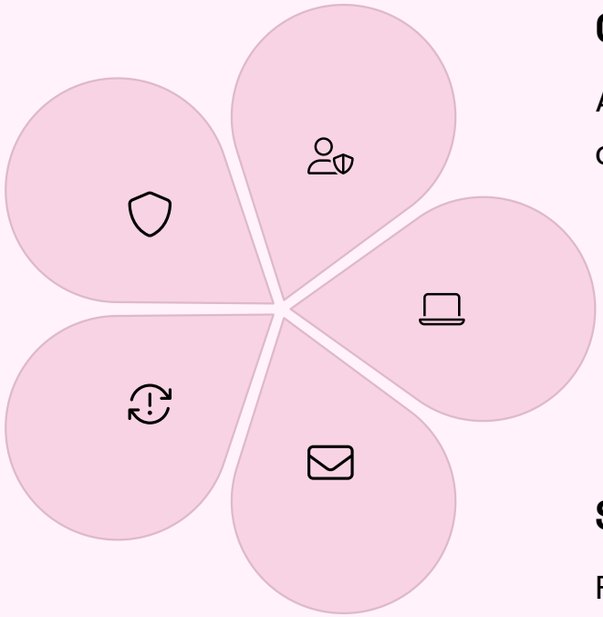
Les ressources limitées sont souvent invoquées pour justifier une cybersécurité inadéquate dans les petites entreprises, mais les implications financières d'une attaque dépassent largement le coût de prévention de tels incidents.

### Protection multicouche

Défense complète contre les menaces avancées

### Sauvegarde cloud

Récupération rapide des données



### Gestion des identités

Authentification sécurisée et contrôle d'accès

### Sécurité des endpoints

Protection de tous vos appareils

### Sécurité email

Filtrage avancé contre le phishing

ACI Technology accompagne les PME dans la protection de leurs données, appareils et applications avec une approche stratégique de la cybersécurité. Contactez-nous pour établir votre plan de sécurité personnalisé.