Checklist

30 choses à vérifier dans votre entreprise pour améliorer votre cybersécurité

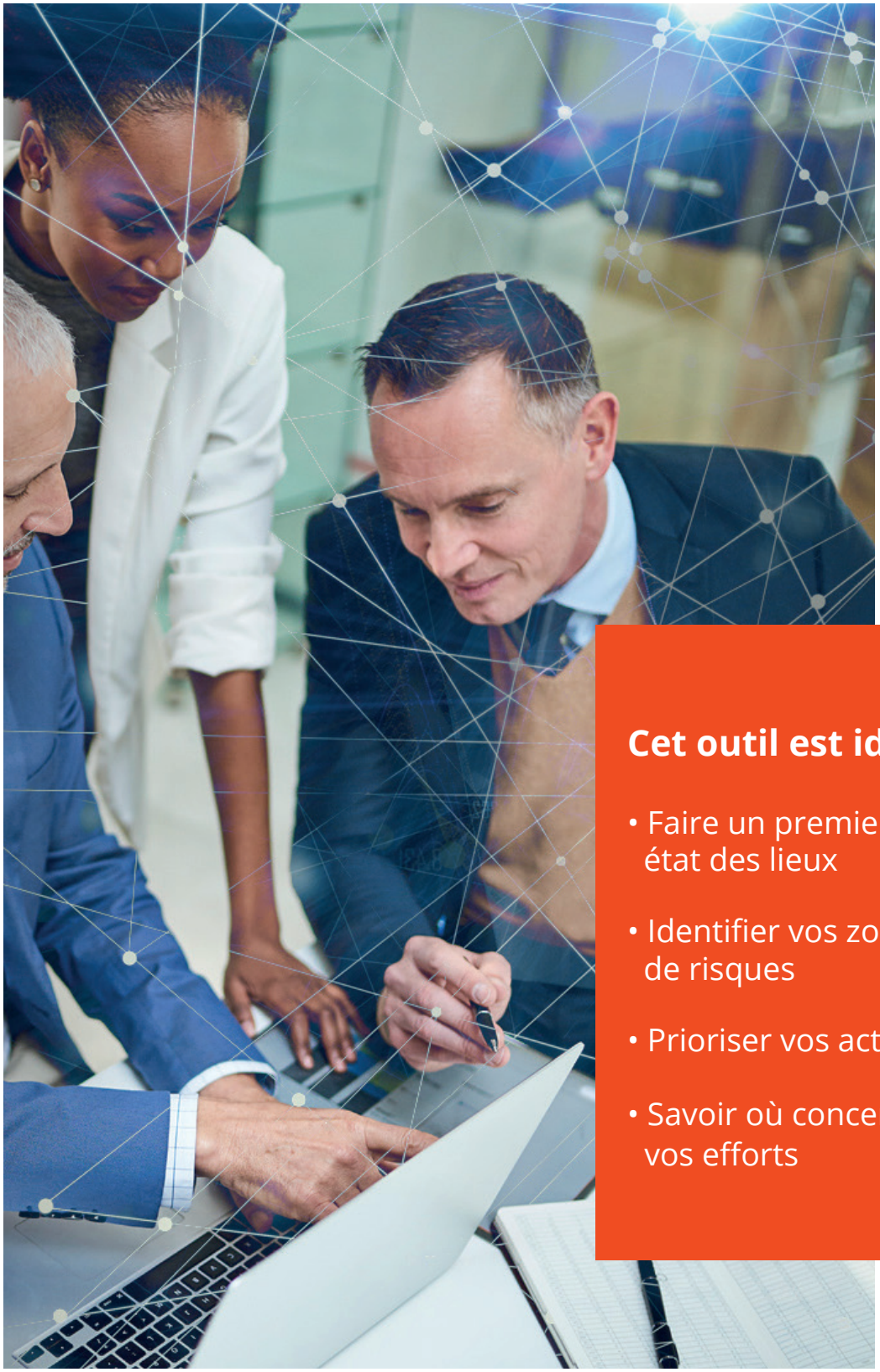
ABAKUS
IT-SOLUTIONS

Saviez-vous que la majorité des cyberattaques qui touchent les PME ne proviennent pas de techniques sophistiquées ?

Ces dernières années, nous constatons une forte augmentation du nombre de cyberattaques. Logiciels obsolètes, mots de passe faibles, Wi-Fi mal configuré, sauvegardes incomplètes, firewall non mis à jour…
Et ce sont les PME, moins protégées, qui ont le plus à perdre.

Le problème ?
La plupart des dirigeants pensent être protégés, jusqu'au jour où un incident survient. Et dans 70% des cas, l'analyse après coup révèle que quelques mesures simples auraient pu éviter la catastrophe.

Et si vous preniez ces mesures dès maintenant ?
Cette check-list regroupe 30 points essentiels, issus de notre expérience terrain, dont la vérification vous permet d'évaluer le niveau de sécurité de votre entreprise.



Cet outil est idéal pour :

- Faire un premier état des lieux
- Identifier vos zones de risques
- Prioriser vos actions
- Savoir où concentrer vos efforts

30 choses à vérifier dans votre entreprise

RÉSEAU & INFRASTRUCTURE

- ☐ Un pare-feu est-il présent et correctement configuré sur le réseau ?
- ☐ Les licences de sécurité du pare-feu (IPS, antivirus, filtrage web) sont-elles actives et à jour ?
- ☐ Les accès distants utilisent-ils un VPN sécurisé de type IPsec ?
- ☐ Une authentification multi-facteurs (MFA) est-elle activée pour les accès VPN ?
- ☐ Les logs de sécurité sont-ils conservés suffisamment longtemps (au moins 4 à 6 mois) ?
- ☐ Le réseau est-il segmenté pour isoler les équipements sensibles ou vulnérables ?
- ☐ Un réseau Wi-Fi « Guest » séparé du réseau interne est-il en place ?
- ☐ Le Wi-Fi interne utilise-t-il un chiffrement sécurisé de type WPA2/WPA3 Enterprise ?
- ☐ L'accès au Wi-Fi est-il lié aux comptes utilisateurs via un serveur RADIUS ?
- ☐ Les serveurs sont-ils physiquement protégés (armoire sécurisée, accès limité) ?

SYSTÈMES, POSTES DE TRAVAIL & SERVEURS

- [ ] Les systèmes d'exploitation des serveurs et postes sont-ils à jour et toujours supportés par l'éditeur ?
- [ ] Une maintenance régulière (patchs de sécurité, correctifs CVE) est-elle assurée ?
- [ ] Une solution antivirus professionnelle est-elle installée sur tous les postes et serveurs ?
- [ ] Les événements et alertes de l'antivirus sont-ils surveillés et analysés ?
- [ ] Une solution EDR (Endpoint Detection & Response) est-elle en place ?
- [ ] Les disques durs des postes de travail (surtout portables) sont-ils chiffrés ?
- [ ] Les applications des postes de travail sont-elles mises à jour automatiquement ?
- [ ] Les utilisateurs disposent-ils uniquement des droits strictement nécessaires (least privilege) ?
- [ ] Les droits administrateur locaux sont-ils supprimés ou gérés via une solution sécurisée (ex. LAPS) ?
- [ ] Une authentification multi-facteurs (MFA) est-elle activée pour l'accès aux systèmes critiques ?

DONNÉES, SAUVEGARDES & CONTINUITÉ

- ☐ Une stratégie de sauvegarde respectant la règle 3-2-1 est-elle en place ?
- ☐ Les sauvegardes sont-elles chiffrées et protégées contre les accès non autorisés ?
- ☐ Des tests réguliers de restauration des sauvegardes sont-ils réalisés ?
- ☐ Les données centralisées (serveurs, SharePoint, fichiers partagés) sont-elles sauvegardées ?
- ☐ Les données non centralisées (postes utilisateurs) sont-elles également protégées ?
- ☐ Les données M365 (Exchange, Teams, SharePoint) sont-elles sauvegardées par une solution dédiée ?
- ☐ Un plan de reprise d'activité (DRP) existe-t-il et est-il documenté ?
- ☐ Une solution de reprise après sinistre dans le cloud (DRaaS) est-elle prévue ?

ORGANISATION, UTILISATEURS & GOUVERNANCE

- ☐ Une politique de sécurité informatique formalisée existe-t-elle et est-elle communiquée aux utilisateurs ?
- ☐ Les utilisateurs sont-ils formés et sensibilisés régulièrement aux risques cyber (phishing, bonnes pratiques) ?

Ce qu'Abakus peut faire pour vous en cybersécurité

ABAKUS est votre partenaire IT complet.

Nous accompagnons les entreprises dans leurs besoins IT variés :
recherche de talents, gestion des infrastructures, implémentation d'outils...

En cybersécurité, nous vous aidons pour transformer les vérifications de cette checklist en véritable plan d'action adapté à votre entreprise.
Nos experts réalisent une analyse complète de votre environnement, identifient vos vulnérabilités, renforcent votre infrastructure et mettent en place les bonnes pratiques essentielles pour réduire vos risques.

Notre objectif ?
Rendre votre entreprise plus résiliente, plus sûre et mieux préparée face aux menaces actuelles.

4 PÔLES POUR RÉPONDRE À VOS BESOINS IT

Chez ABAKUS, nous sommes convaincus que toutes
les entreprises méritent du confort IT.
Nous vous aidons à l'atteindre grâce à une diversité de services.

Consultance IT

Accompagnement expert pour vos projets IT, avec gouvernance, sélection de talents et conseil en développement et cybersécurité.

Gestion d'infrastructure

Supervision complète de votre infrastructure, du cloud au support, en passant par réseau, sauvegarde et maintenance.

Implémentation Odoo

Conception et déploiement de solutions Odoo sur mesure, incluant développement Python/API et optimisation métier.

Cybersécurité

Gouvernance, conformité et protection de vos systèmes grâce aux audits, à la gestion des risques et à la sécurisation opérationnell