GUIDE CYBERSECURITE

25 mesures pour votre PME

Sommaire

Bonjour,

Nous sommes heureux de vous offrir ce guide des bonnes pratiques de la cybersécurité pour votre TPE PME.

Dans ce guide, nous avons regroupé les mesures les plus intéressantes à mettre en place pour votre entreprise, notamment celles de l'ANSSI. Notre objectif est que vous puissiez commencer la mise en oeuvre de votre cybersécurité avec ce guide simple.

Nous intégrons dès le début de votre lecture une liste **"Ma Checklist CyberNum"** pour vous guider facilement et rapidement dans la mise en place de la cybersécurité dans votre entreprise. Nous vous conseillons de l'imprimer.

Bonne lecture.

L'équipe BETANUM

Cybersécurité
Ma Checklist CyberNum

Je forme mes salariés à la cybersécurité

- Organiser une **formation directement après avoir recruté une personne**
- Mettre en place **1x par an** minimum une formation pour mes salariés et un suivi tout l'année
- Proposer régulièrement des campagnes de **phishing et du elearning**

Je mets en place une stratégie

- **Gérer avec rigueur les accès** des créations et des suppressions des comptes de mes utilisateurs
- **Définir des règles pour mes mots de passe et les appliquer**
- **Limiter les accès** à mes données sensibles

Je contrôle mes accès

- Mettre en place une **identification à deux facteurs**
- **Stocker les mots de passe dans un coffre fort électronique**
- Mettre en place des **accès nominatifs**

Je protège mes systèmes et réseaux

- **Mettre à jour régulièrement** vos logiciels et vos systèmes d'exploitation
- **Utiliser un pare-feu** pour protéger le réseau interne
- Installer et mettre à jour mes **antivirus et antimalware**

Betanum

Ma Checklist CyberNum

Je sécurise mes postes nomades

-  Utiliser un **tunnel VPN IPsec**
-  Créer un **fichier** des appareils nomades

Je protège mes données

-  Créer un **plan de sauvegarde régulier de mes données** critiques
-  Faire le **stockage de mes sauvegardes** en dehors du site principal et/ou dans le cloud

Je mets en place un plan pour les incidents

-  Savoir i**dentifier et signaler rapidement des incidents de sécurité**
-  Définir des **étapes pour répondre à un incident**

J'audite et j'optimise régulièrement

-  Savoir réaliser régulièrement des **évaluations des risques**
-  Mettre en place des **audits de sécurité pour vérifier la conformité** de mon informatique

Betanum

Etape 1
Formez vos salariés à la cybersécurité

1 Sensibilisez vos nouvelles recrues

74 % des cyberattaques sont causées par du phising selon Statista. Ainsi, chaque collaborateur doit être informé dès qu'il entre dans votre entreprise pour augmenter vos probabilités de réussite. Il est donc essentiel de pouvoir former vos nouvelles recrues et de les informer des risques du phishing puis des règles de sécurité informatique à respecter dès leur arrivée. **L'idéal est d'organiser des sessions de formations et de sensibilisation au plus tôt dans l'onboarding.**

De plus, les sessions doivent être mis en place régulièrement, adaptées aux différents personnes et proposées sous différentes formes.
Cela peut être des **entrainements aux phising par email, des formations en présentiel ou encore des formations en e-learning**. De plus, vous pouvez mettre en place et faire signer une charte de sécurité.

Les différents sujets abordés peuvent être :

- Les objectifs en termes de sécurité de votre entreprise
- Le phishing
- Les règlementations à respecter (exemple NIS 2)
- Les informations sensibles
- Les règles internes de cybersécurité à respecter (non utilisation des mots de passe professionnels dans son quotidien par exemple)
- Les outils disponibles pour la cybersécurité de votre entreprise

2 Formez régulièrement vos salariés

Aujourd'hui de nombreux collaborateurs peuvent avoir accès à des données privilégiées qui ne sont pas toujours adaptées à leurs besoins. Cela peut constituer un risque pour la cybersécurité.

Il est essentiel de **former régulièrement les équipes opérationnelles, de direction et aussi les infogérants** à la sécurité informatique.

Nous vous conseillons d'effectuer régulièrement des campagnes de phishing et de former vos collaborateurs un grand **minimum 1 fois par an**.

Vous pouvez intégrer la cybersécurité dans un **objectif professionnel annuel.**

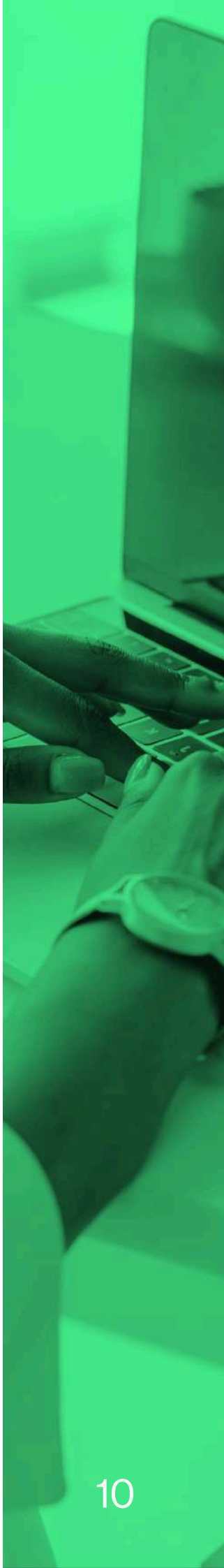
Voici les sujets possibles :
- Les controle d'accès
- Les enjeux de l'entreprise
- Les risques
- Le maintien de la sécurité
- Les règles internes
- Les nouvelles législations
- Les paramètrages système et réseau

Etape 2
Mettez en place une stratégie de sécurité

3 Déterminez vos règles pour vos mots de passe

Vous pouvez mettre en place différentes règles pour la sécurisation des mots de passe pour le choix et le dimensionnement dans votre entreprise.

- **Sensibilisez vos utilisateurs aux risques d'un mot de passe trop simple** ou encore pour la réutilisation d'un mot de passe pour une autre plateforme
- **Mettez en place régulièrement** les changements pour vos mots de passe
- **Bloquez les comptes à la fin de plusieurs essais** de mots de passe
- **Mettez en place un outil d'audit** reconnaissant la robustesse des mots de passe



4 Limitez les accès aux données sensibles

Votre entreprise possède des informations sensibles. Cela peut être sur vos clients, votre activité, vos innovations. Vous devez les identifier pour bien sécuriser votre société.

Nous vous conseillons de créer une liste puis d'identifier les éléments du système et où ils se situent (fichiers partagés, bases de données...). Ces éléments constituent des risques. Ainsi, il est important mettre en place des mesures. Cela peut être en termes de sauvegarde, d'accès...

Cet exercice vous permettra d'obtenir une cartographie des zones avec les IP, les équipements, les serveurs et les connexions.

5

Organisez vos créations et suppressions de compte

Vos effectifs sont toujours en évolution. Cela peut être des départs, des arrivées, de la mobilité en interne. **Ainsi, il est important que les droits des utilisateurs et leurs accès soient mis à jour très régulièrement.**

Vous devez donc définir des instructions de départs et d'arrivées puis que cela soit liée à leur fonction.

Ces instructions doivent prendre en compte en fonction de cela :

- Les droits d'administration
- Les boites emails
- Les téléphones mobiles, tablettes, clés USB...
- Les mots de passe
- Les comptes informatiques
- Les accès aux locaux
- Les accès aux documents...

6

Réduisez les accès aux comptes privilégiés

Les comptes des utilisateurs avec des privilèges spécifiques sont des cibles privilégiées pour les cyberattaquants cherchant à obtenir un accès plus grand au système d'information. Par conséquent, ils doivent étudier avec beaucoup de précaution. Il est essentiel de créer des inventaires de ces comptes, de les maintenir à jour, d'y inclure les informations suivantes et de créer des catégories :

- Tout d'abord, **les utilisateurs qui possèdent assez de droits** pour avoir accès aux répertoires de travail des responsables ou de l'ensemble des utilisateurs
- Les utilisateurs qui ont des **comptes administrateurs ou des droits supérieurs** à ceux d'un utilisateur standard
- Les **utilisateurs qui ont un poste non géré par le service informatique** et non soumis aux mesures de sécurité de la politique de sécurité générale de votre entreprise

Il est recommandé de mettre en place des **réunions régulières de ces comptes** pour vérifier que les accès aux éléments sensibles sont bien gérés.

Enfin, il est important de mettre en place une **classification simplifiée pour reconnaitre les différents comptes**. Cela simplifiera leur analyse.

Etape 3
Contrôlez vos accès

7 Mettez en place une authentification à deux facteurs

Il est recommandé de mettre en place **une authentification à deux facteurs (2FA)** pour que votre entreprise sera plus en sécurité.

Il y a plusieurs facteurs à mixer et à choisir :

- **Quelque chose que l'on connait** : mot de passe, mot de passe à usage unique, PIN
- **Quelque chose que l'on possède** : token, clé/smartcard, carte à puce
- **Quelque chose que l'on est** : empreinte digitale

Les cartes à puce et les mots de passe à usage unique avec jeton, obtiennent des bons résultats de sécurisation.

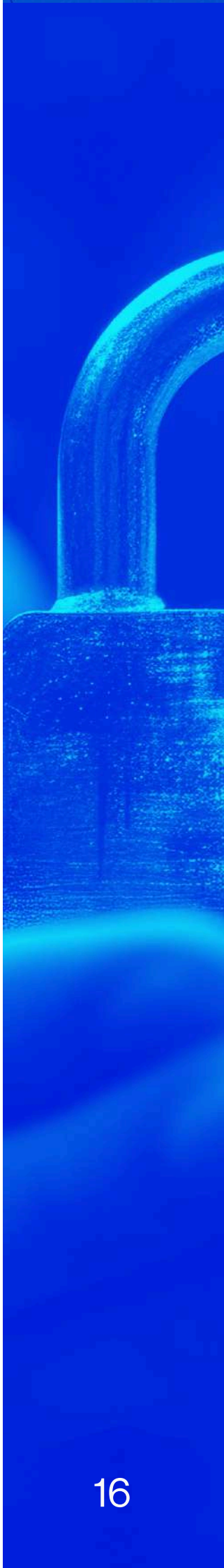
8

Stockez vos mots de passe dans un coffre fort numérique

Aujourd'hui, nous devons utiliser plusieurs mots de passe pour accéder à nos plateformes. Cette utilisation complexe nous encourage à les ranger soit sur une feuille de mémo, des post-it ou encore sur un fichier numérique pour les conserver.

Cependant, il faut être vigilant aux cyberattaquants.

Il est recommandé de garder les mots de passe dans un **coffre-fort numérique** ou avec des mécanismes de chiffrement. Ainsi, vous n'aurez à retenir qu'un seul un mot de passe et votre entreprise sera plus sécurisée.

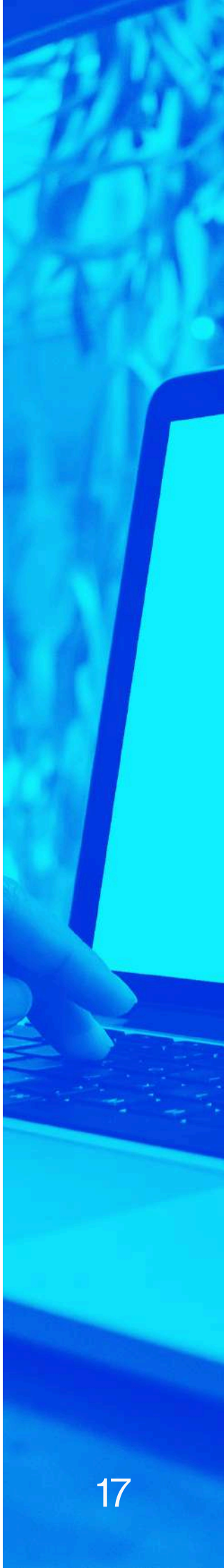


9

Créez des comptes d'accès nominatifs

Les comptes permettant d'avoir accès au système d'information doivent être nominatifs, afin de proposer une réaction efficace et rapide en cas de problème.

- Tout d'abord, il est recommandé de **limiter le nombre de comptes génériques type "admin"**
- Les comptes génériques doivent être formalisés et gérés de **manière stricte**
- **Chaque administrateur disposera de son propre compte**
- Le compte d'administration ne servira **que pour les actions d'administration**



10 Modifiez vos accès par défaut des services

Vos configurations par défaut sont connues par les cyberattaquants.

Elles sont souvent trop simples (mots de passe commun entre chaque plateforme, trop faible...) et accessibles pour les attaquants.

Il est recommandé de :

- **Modifier vos configurations** dès que vous avez un nouvel outil en main
- Mettre en place les **nouvelles procédures de sécurité** de votre entreprise
- De **renouveller régulièrement les accès**

Etape 4
Protégez votre système et votre réseau

11 Mettez à jour vos logiciels et vos systèmes avec les derniers patchs

Vous réduirez les risques d'intrusion en mettant régulièrement à jour vos logiciels et vos systèmes avec les derniers patch de sécurité.
Cela rendra moins vulnérables vos systèmes.

Pour cela, vous pouvez :

- Automatiser toutes les mises à jour
- Surveiller les annonces de sécurité
- Auditer régulièrement les systèmes
- Former les utilisateurs

12 Utilisez un pare-feu sécurisé Internet

Il est possible que vos salariés téléchargent des fichiers risqués ou encore qu'ils aillent sur des sites avec un code malveillant par exemple. Ainsi, il peut y avoir une fuite de vos données. Pour sécuriser votre accès à Internet, il est recommandé que vos terminaux utilisateurs n'aient pas accès directement à Internet, pour cela vous pouvez :

- Mettre en place un accès sécurisé à Internet avec un **pare-feu proche de la connexion Internet** permettant d'épurer les connexions et un serveur proxy avec des processus de sécurisation pour analyser les authentifications
- **Réaliser des interventions en complément** sur le serveur avec des audit antivirus par exemple
- Maintenir la sécurisation du matériel de la passerelle avec des **process à mettre en place**
- **Désactiver les DNS** liés directement aux noms de domaines publics
- **Séparer les connexions Wi-Fi des postes nomades de ceux de l'entité** (SSID et VLAN sont à dissocier) et permettre aux poste nomades d'aller sur Internet à travers la passerelle

13 Vérifiez la sécurité de vos réseaux Wi-Fi

Utiliser le Wi-Fi dans le monde du travail est maintenant de rigueur cependant il existe des menaces sur la sécurité informatique. Nous pouvons noter une disponibilité aléatoire pouvant donner lieu à une cyberattaque.

Pour optimiser cela, voici quelques éléments à mettre en place :

- **Fractionnez votre architecture réseau** pour limiter l'accès à un périmetre donné
- Triez les éléments importants à conserver pour vos postes branchés au Wi-Fi
- Mettez en place un **chiffrement très fort** et une authentification centralisée
- Protégez votre Wi-Fi avec un **mot de passe complèxe**, renouvellé régulièrement et non diffusé en interne
- Distribuez les points d'accès de manière sécurisée avec une interface **dédiée à un administrateur** dans votre structure
- **Dissociez les connexions Wi-Fi des terminaux personnels** de votre entreprise (SSID, VLAN)
- **Créez un Wi-Fi invité**

14 Sécurisez votre messagerie

L'envoi d'email représente un risque de cybersécurité important, cela peut être dans l'ouverture de pièces jointes ou en cliquant sur un lien sur un site hostile. Voici quelques éléments à mettre en place :

- Il est ainsi essentiel de faire de la **sensibilisation pour vos salariés et vos nouveaux arrivants**. Ils doivent se poser la question : est-ce que je connais cette personne ? Est-ce que j'attends quelque chose de cette personne ?
- Ne pas **rediriger d'email professionnel vers une messagerie personnelle** pour qu'il n'y ait pas de fuite de données
- **Héberger votre système de messagerie, mettre en place une analyse de l'antivirus** à l'origine des boîtes et activer un chiffrement TLS des serveurs de messagerie, de ceux de boites aux lettres et aussi des postes utlisateurs

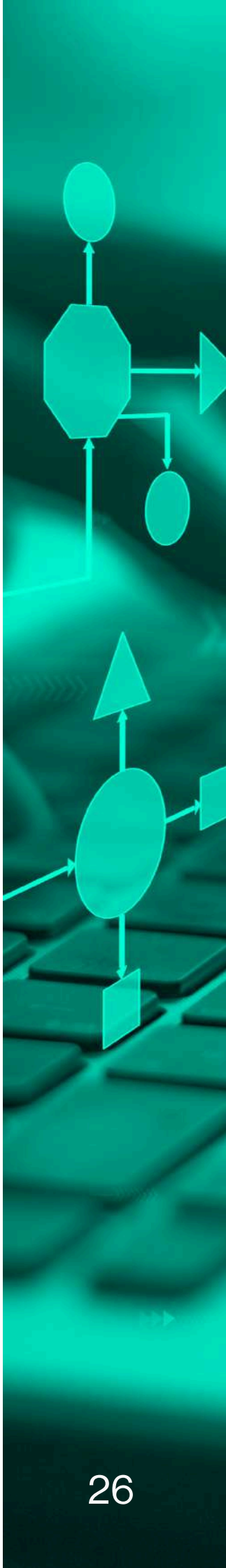
15 Installez des solutions d'anti-virus sur tous les postes

Les solutions d'anti-virus sont essentielles pour vous protéger des cybercriminels.

- Pour commencer, **choisissez un logiciel d'antivirus**, cela peut être : Norton, Kaspersky, McAfee
- Puis, **installez le logiciel sur chaque ordinateur**
- Et **configurez les paramètres de sécurité**
- **Maintenez à jour le système**
- **Sensibilisez vos collaborateurs**

Etape 5
Sécurisez vos postes nomades

16 Etablissez un tunnel VPN IPsec



Lorsqu'un de vos salariés est à l'extérieur avec son équipement informatique, il a souvent besoin d'avoir accès au réseau de votre entreprise. Il est donc important de pouvoir sécuriser cet accès à travers Internet.

Voici quelques recommandations :

- **Mettre en place un tunnel VPN IPsec entre le poste du salarié à l'exterieur et une passerelle VPN IPsec** proposée par votre entreprise et automatiquement créée
- En cas de dérogation d'une mise en place automatique, il est possible de le faire à la demande en étant vigilant ou sinon de proposer à votre salarié d'utiliser un **partage de connexion sur son téléphone**
- **Avoir une authentification robuste** avec si possible une carte à puce, jeton USB ou un mot de passe très fort ou encore avec un mot de passe à usage unique

17 Créez un fichier des appareils nomades

Il peut arriver que vos salariés perdent leur matériel informatique, s'ils sont souvent en déplacement. Ainsi, vos données sensibles peuvent être menacées.

Pour cela, vous pouvez :

- **Stocker seulement le matériel nomade qui a chiffré ses données** (l'utilisateur mettra en place des mots de passe forts sur les différents outils utilisés)
- **Commencer par un chiffrement entier du disque** avant le chiffrement d'archives

Etape 6
Sauvegardez vos données

18 Mettez en place un plan d'actions des données critiques

Mettre en place un plan de sauvegarde de vos données critiques est essentiel pour la poursuite de votre activité de PME en cas d'incident.

Voici quelques étapes pour le mettre en place :

- **Analysez et listez vos données critiques**
- Choisissez votre **méthode de sauvegarde** (totale, partielle en fonction de votre dernière sauvegarde) : nous vous conseillons de sauvegarder en totalité vos données
- **Sélectionnez le lieu de stockage de vos données** : disques durs, cloud...
- **Configurez votre sauvegarde avec le logiciel** de votre choix (Acronis, Veem...)
- **Stockez hors site avec une copie dans le cloud** par exemple dans un autre lieu géograpihique
- **Testez la restauration**
- **Planifiez la sauvegarde** (journalière, mensuelle...)
- **Réalisez des audits de sauvegarde**

19 Conservez les sauvegardes en dehors du site et/ou du cloud

Pour garantir à votre entreprise un niveau de sécurité élevé pour vos données, il est conseillé de mettre en place des sauvegardes en dehors du site principal et aussi dans le cloud. Si vous pouvez faire les deux c'est encore mieux.

- **Pour les sauvegardes hors du site**, vous pouvez utillser des disques durs, des centres de données, des entrepots sécurisés. Si vous avez un autre bureau, vous pouvez envoyer vos données dans ce bureau.
- **Pour les sauvegardes de vos données dans le cloud**, vous pouvez Amazon (AWS), Microsoft Azure ou encore Google Cloud.

Vous pouvez aussi utiliser des **solutions hybrides en mélant aussi bien le les sauvegardes hors site et le cloud.**

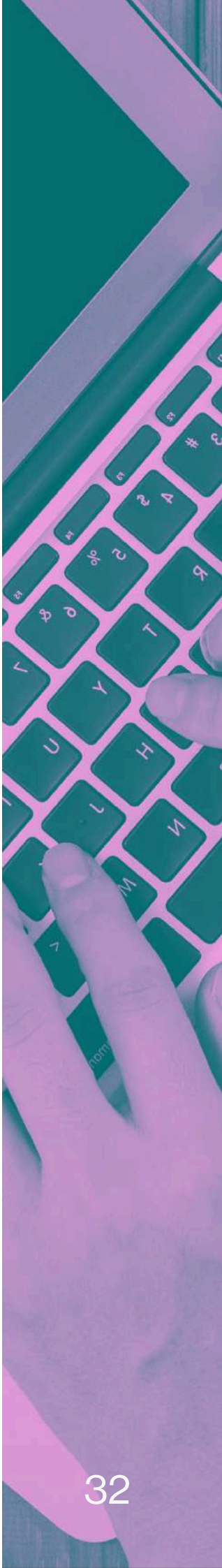
Etape 7
Mettez en place un plan pour la gestion des incidents

20 Identifiez et signalez les incidents

Savoir identifier et signaler un incident représentent des tâches importantes pour garantir la sécurité de votre PME.

Voici quelques étapes importantes :

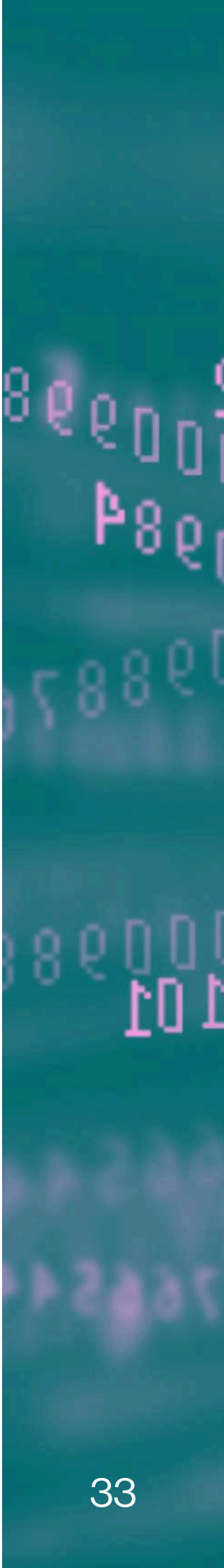
- **Identifiez et choisissez des solutions de détection**, de surveillance et d'anti-virus
- Mettez en place des **procédure de surveillance en continue** avec des alertes automatiques, des tableaux de bord
- Installez un système de gestion des informations et des évènements de sécurité avec un **SIEM**
- **Formez et sensibilisez** votre personnel
- **Mettez en place un plan de réponse d'incident** puis en la communiquant à une équipe dédiée
- **Rédigez un rapport d'incident post-incident** en analysant les éléments
- Mettez en place des **simulations**



21 Définissez les étapes et récupérez vos données

Voici quelques étapes définir votre plan d'action et récupérer vos données :

- **Etablissez vos objectifs** en cas d'incident
- Identifiez les types d'incidents possibles (physique, cyberattaques, fuites de données...)
- **Construisez votre équipe de réponse** avec des responsables et définissez les rôles
- **Identifiez vos actifs critiques**
- **Mettez en place des outils de détection** (anti-virus, surveillance de réseau...)
- **Créez des procédures** de réponse immédiate
- **Analysez et évaluez**
- **Communiquez sur les protocoles**
- **Restaurez les systèmes**
- **Récupérez les données en utilisant les sauvegardes**



Etape 8
Auditez et optimisez régulièrement

22 Auditez régulièrement votre sécurité

Afin de vérifier la conformité de votre sécurité, nous vous conseillons d'auditer régulièrement votre entreprise.

Voici les étapes :

- Planifiez un **audit en interne**
- **Collectez des informations**, notamment, regardez les nouvelles normes dans votre industrie en vigueur et vérifiez si votre système est conforme comme par exemple avec la loi RGPD ou bientôt la directive NIS 2
- **Détecter les faiblesses** et les failles de votre réseau avec des scan de vulnérabilité et de Pentest
- **Effectuez un rapport d'audit**
- Mettez en place un **plan d'actions**
- **Suivez le plan d'actions**
- **Renouvelez la mise en place d'un audit de sécurité au moins 2x par an**

23 Définir une stratégie de maintenance

Il est probable de s'apercevoir d'éventuelles nouvelles vulnérabilité à l'intérieur de vos systèmes informatiques. Cela peut être propice à l'intrusion d'un cyberattaquant.

Pour se prémunir, il est indispensable de mener une stratégie de mise à jour régulière avec différentes procédures.

Voici quels sont les éléments à préciser :

- La façon dont le **bilan du système informatique a été réalisé**
- La **qualité des corrections** et de leur développement sur les systèmes
- L'origine des informations concernant **les mises à jour**
- Les appareils permettant de **mettre en place les corrections sur le matériel informatique**

24 Devancer les obsolesences

Un système d'information obsolète développe le risque potentiel d'intrusion de cyberattaque car les optimisations ne sont plus mises en place.

Voici quelques solutions pour vous prémunir :

- Mettez à jour un **inventaire de tous les systèmes et applications** de votre entreprise
- Sélectionnez seulement des outils qui **assurent un délai qui correspond à votre utilisation**
- Ayez une **seule version de chaque logiciel**
- Freinez les **adhésions** à des logiciels
- Repérez les **dates de fin pour les logiciels** à changer
- Ayez des **contrats garantissant le management de l'obsolescence de vos matériaux**

25 Nommer un responsable sécurité en interne

Il est essentiel d'avoir en interne dans votre entreprise une personne responsable de vos systèmes d'information.

Ce responsable sera identifié de tous vos salariés.

- Il définira les **différents procédures**
- Il examinera **l'application des règles**
- Il **sensibilisera les salariés** et pourra mettre en place un plan de formation
- Il **regroupera** l'ensemble des incidents remontés par les salariés

Il devra être formé à la sécurité informatique et sera à même de pouvoir signaler les problématiques rencontrées par les salariés puis repondre aux besoins de sensibilisation. Et enfin, cela pourra le motiver d'être objectivé tous les ans sur ses résultats en terme de cybersécurité.

Nous vous remercions d'avoir lu ce guide.
Nous espérons qu'il vous a été utile.

Si vous souhaitez aller plus loin dans votre cybersécurité pour être encore mieux protégé, nous serons ravis de pouvoir vous aider. Vous pouvez nous contacter au
01 43 56 37 27 ou par mail contact@betanum.com

A très vite.

L'équipe BETANUM