CYBERSECURITE : LES PROPOSITIONS DE L'ANSSI

GROUPE exentys

www.exentys.com

office@exentys.com

L'agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité. Elle a créé un **guide d'hygiène informatique** à mettre en place pour garantir la sécurité de vos systèmes d'information. Il comprend 42 mesures. L'intégrité et la confidentialité de vos informations seront ainsi respectées.

Le guide très complet vous propose également un **outil de suivi** pour chaque règle afin de faire un état des lieux afin de savoir si votre entreprise a atteint le niveau standard ou le niveau renforcé de chaque mesure.

Vous pourrez ainsi mettre en place un **plan d'actions** pour obtenir le niveau standard pour toutes les règles, puis dans un second temps, essayer d'atteindre le niveau renforcé.

Exentys vous explique – et vous résume ! - les mesures définies dans le guide d'hygiène informatique de l'ANSSI.

I. LES MESURES DE SENSIBILISATION ET DE FORMATION

Mesure 1 : la formation de vos équipes opérationnelles à la sécurité des systèmes d'information

Niveau standard

Formez vos équipes opérationnelles (administrateurs réseau, sécurité et système, chefs de projet, développeurs, RSSI) sur :

- la législation en vigueur ;
- les risques et menaces ;
- l'authentification et le contrôle d'accès ;
- le paramétrage et le durcissement des systèmes ;
- le cloisonnement réseau ;
- la journalisation.

Pour rappel, votre système d'information (SI) comprend les ressources et les dispositifs permettant la collecte, le stockage, le traitement et la diffusion des informations nécessaires au fonctionnement de votre entreprise.

À noter
Pensez à insérer une clause de formation régulière pour le personnel externe, lors de la contractualisation.

Mesure 2 : la sensibilisation des utilisateurs aux bonnes pratiques de sécurité informatique

Niveau standard

Faites des actions de sensibilisation et de formation (par exemple par l'envoi d'e-mails ou lors de réunions) pour informer vos utilisateurs aux enjeux de la sécurité informatique.

La sensibilisation doit porter sur :
- vos objectifs de sécurité des systèmes d'information ;
- les informations sensibles ;
- les réglementations et les obligations légales ;
- les règles et les consignes de sécurité pour votre activité quotidienne (par exemple, le respect de la politique de sécurité, la non-connexion d'équipements personnels au réseau de votre entité, la non-divulgation des mots de passe, le signalement d'événements suspects) ;
- les moyens disponibles et participant à la sécurité du système (par exemple, le verrouillage de la session lorsqu'une personne quitte son poste).

Niveau renforcé

Élaborez une **charte des règles à respecter** par les utilisateurs.

Mesure 3 : la maîtrise des risques de l'infogérance

Niveau standard

Évaluez les risques liés à l'infogérance (le fait d'externaliser votre système d'information) en prenant en considération vos besoins en matière de sécurité. À savoir :
- analyser les conditions du prestataire choisi : offres, adaptabilité et limitation de responsabilité ;
- édicter des exigences au prestataire (par exemple le maintien d'un niveau de sécurité).

Demandez un **plan d'assurance sécurité (PAS)** au prestataire.

II. LES MESURES EN MATIERE DE CONNAISSANCE DU SYSTEME D'INFORMATION

Mesure 4 : l'identification des informations et des services sensibles, et le maintien d'un schéma du réseau

Niveau standard

Identifiez et listez vos données sensibles sur votre activité ou vos clients pour déterminer où elles se trouvent (postes de travail, bases de données, etc.). Vous pourrez ainsi mettre en place des mesures de sécurité sur ces composants comme la sauvegarde des données.

Créez et maintenez à jour un schéma simplifié du réseau représentant :
- les différentes zones IP et le plan d'adressage associé ;
- les équipements de routage et de sécurité ;
- les interconnexions avec l'extérieur et les partenaires.

Mesure 5 : la création d'un inventaire des comptes privilégiés

Niveau standard

Faites un inventaire à jour des comptes privilégiés, c'est-à-dire les comptes ayant des droits spécifiques. À savoir :
- les comptes autres que les comptes standards ;
- les droits pour accéder aux répertoires de travail des responsables ou de tous les utilisateurs ;
- les postes non administrés ne faisant pas l'objet de mesures de sécurité édictées par la politique de sécurité générale de votre entreprise.

Faites une **revue périodique** de ces comptes pour garantir que les accès aux informations sensibles soient maîtrisés et supprimez les accès obsolètes.

Pour cela, définissez une **nomenclature simple** pour identifier les comptes de services et les comptes d'administration.

Mesure 6 : l'organisation des procédures d'arrivée, de départ et de changement de fonction des utilisateurs

Niveau standard

Veillez à mettre à jour les droits et les accès à votre système d'information au regard de l'évolution du personnel**.** Cela signifie être particulièrement attentif à :
- la création et la suppression des comptes informatiques et boîtes emails associées ;
- les droits et accès à attribuer ou retirer à un salarié changeant de fonction ;
- la gestion des accès physiques aux locaux ;
- l'affectation des équipements mobiles ;
- la gestion des documents et informations sensibles.

Niveau renforcé

Formalisez et mettez à jour les procédures ci-dessus.

Mesure 7 : L'autorisation de connexion au réseau de votre entreprise aux seuls équipements maîtrisés

Niveau standard

- **N’autorisez que la connexion sur vos réseaux d’accès aux équipements maîtrisés par votre entreprise.**
- **Mettez en place des solutions pour les équipements personnels et les utilisateurs** comme un réseau Wi-Fi avec SSID.

Niveau renforcé

Mettez en place des mesures techniques telles que l’authentification des postes sur le réseau.

III. L’AUTHENTIFICATION ET LE CONTROLE DES ACCES

Mesure 8 : l’identification de chaque personne accédant à votre système

Niveau standard

- **Créez des comptes d’accès nominatifs** pour faciliter l’attribution d’une action sur le SI en cas d’incident ou pour identifier les comptes compromis.
- **Optez pour une gestion stricte des comptes nominatifs, génériques et de service**. Les comptes génériques sont à rattacher à un nombre limité de personnes.
- **Attribuez un compte administrateur nominatif** dédié aux actions d’administration à chaque administrateur.

Niveau renforcé

Procédez à l’activation de la journalisation liée aux comptes.

Mesure 9 : l’attribution des bons droits sur les ressources sensibles de votre système d’information

Niveau standard

Établissez une **liste de vos ressources constituant une source d’information précieuse** pour un attaquant avec les informations suivantes :

- la définition de la population pouvant y avoir accès ;
- le contrôle de l’accès à chaque ressource avec l’identification des utilisateurs ;
- les moyens pour éviter la dispersion et la duplication de chaque ressource à des endroits non maîtrisés ou ayant un accès moins strict.

Mettez en place un contrôle d’accès précis pour les répertoires des administrateurs et les informations sensibles sur des partages réseau.

Effectuez une revue régulière des droits d’accès pour identifier les accès non autorisés.

Mesure 10 : la définition et la vérification des règles des mots de passe

Niveau standard

Sensibilisez vos utilisateurs aux risques liés au choix d'un mot de passe.

Mettez en place :
- le blocage des comptes suites à plusieurs échecs de connexion ;
- la désactivation des options de connexion anonyme ;
- l'utilisation d'un outil d'audit de robustesse des mots de passe.

À noter
Communiquez pour expliquer le recours à ces règles.

Mesure 11 : la protection des mots de passe stockés sur les systèmes

Niveau standard

Protégez les supports de stockage des mots de passe, notamment avec un coffre-fort numérique ou des mécanismes de chiffrement.

Le mot de passe du coffre-fort numérique devra respecter les règles des mots de passe.

Mesure 12 : le changement des éléments d'authentification par défaut

Niveau standard

Modifiez les éléments d'identification par défaut pour qu'ils soient conformes aux recommandations. En cas d'impossibilité, signalez-le au distributeur du produit.

Niveau renforcé

Procédez au renouvellement régulier des éléments d'authentification.

Mesure 13 : le recours à une authentification forte

Niveau standard

Mettez en place le recours à une authentification forte avec deux facteurs d'authentification différents, soit l'alliance de deux éléments :
- mot de passe, tracé de déverrouillage, etc. ;
- carte à puce, carte magnétique, un téléphone pour recevoir un code, etc. ;
- empreinte biométrique, reconnaissance faciale, etc.

Niveau renforcé

Privilégiez les cartes à puce et les mécanismes de mots de passe à usage unique avec jeton physique.

IV. LA SECURISATION DES POSTES

Mesure 14 : La mise en place d'un niveau de sécurité minimal pour le parc informatique

Niveau standard

Mettez en place un niveau de sécurité minimal pour votre parc informatique dont :

- la limitation des applications installées et modules optionnels des navigateurs web ;
- l'installation d'un pare-feu et d'un anti-virus sur chaque poste utilisateur ;
- le chiffrement des partitions stockant les données utilisateurs ;
- la désactivation des exécutions automatiques.

Isolez les postes ne respectant pas ces règles.

Niveau renforcé

Sauvegardez régulièrement les données vitales au bon fonctionnement de votre entreprise des postes utilisateurs et des serveurs et stockez les sur des équipements déconnectés. Leur restauration est à vérifier périodiquement.

Mesure 15 : la protection des menaces relatives à l'utilisation de supports amovibles

Niveau standard

Traitez les risques liés aux supports amovibles. Pour cela, identifiez des mesures adéquates. Par exemple, proscrivez le branchement de clés USB inconnues et limitez celui des clés non maîtrisées sauf inspection du contenu par un antivirus. Et de nouveau, sensibilisez les utilisateurs aux risques de l'utilisation des supports amovibles

Niveau renforcé

Utilisez des solutions permettant d'interdire l'exécution de programmes sur les supports amovibles et implémentez une procédure de mise en rebut des supports amovibles en fin de vie.

Mesure 16 : l'utilisation d'un outil de gestion centralisée pour homogénéiser les politiques de sécurité

Niveau standard

- **Homogénéisez la gestion des politiques de sécurité de votre parc informatique**. Ces politiques doivent être simples et rapides pour les administrateurs.
- Prenez un **outil de gestion centralisée** incluant vos équipements informatiques.

Mesure 17 : l'activation et la configuration d'un pare-feu local sur les postes de travail

Niveau standard

Activez un pare-feu local sur les postes de travail à l'aide de logiciels intégrés ou spécialisés.

Niveau renforcé

- Bloquez l'accès aux ports d'administration par défaut des postes de travail (excepté depuis les ressources identifiées comme les postes d'administration) et les flux par défaut et n'autorisez que les services nécessaires depuis les équipements correspondants.
- Menez une analyse des flux entrants utiles pour définir la liste des autorisations à configurer.
- Configurez un pare-feu pour journaliser les flux bloqués afin d'identifier les erreurs de configuration d'applications ou les tentatives d'intrusion.

Mesure 18 : le chiffrement des données sensibles transmises par voie Internet

Niveau standard

- **Procédez au chiffrement systématique de toutes les données envoyées par e-mail ou transmises par un cloud**.
- Utilisez un canal de confiance pour l'envoi du secret, c'est-à-dire du mot de passe.

V. LA SECURISATION DU RESEAU

Mesure 19 : la segmentation du réseau

Niveau standard

Procédez à la segmentation en zones composées de systèmes ayant des besoins de sécurité homogènes pour éviter que l'attaque d'une machine mette en péril les autres machines connectées.

Une zone se compose de VLAN, sous-réseaux IP et infrastructures dédiés.

Mettez en place des mesures de cloisonnement comme un filtrage IP.

Mesure 20 : la sécurité des réseaux d'accès Wi-Fi

Niveau standard

- **Segmentez l'architecture réseau** pour limiter les incidences d'une intrusion.
- **Filtrez et restreignez aux seuls flux nécessaires** les flux venant des postes connectés au Wi-Fi.
- Utilisez un chiffrement robuste et une authentification centralisée. Le Wi-FI doit être protégé par un mot de passe complexe et renouvelé.
- **Administrez de manière sécurisée les points d'accès**.
- **Séparez les connexions** des appareils de votre entreprise et les connexions des terminaux personnels ou visiteurs.

Mesure 21 : l'utilisation des protocoles réseaux sécurisés

Niveau standard

Utilisez des protocoles réseaux sécurisés sur les réseaux publics, mais aussi sur votre réseau interne.

Mesure 22 : la mise en place d'une passerelle d'accès sécurisé à Internet

Niveau standard

Mettez en place une passerelle sécurisée d'accès à Internet avec un pare-feu filtrant les connexions et un serveur mandataire ayant des mécanismes de sécurité. Les utilisateurs ne doivent pas avoir d'accès réseau direct à Internet.

Niveau renforcé

- Installez d'autres mécanismes selon les besoins de votre entreprise comme l'analyse antivirus du contenu.
- Désactivez les résolutions DNS en direct de noms de domaines publics.
- Établissez une connexion sécurisée au SI de votre entreprise à l'aide d'une passerelle pour les postes nomades.

Mesure 23 : le cloisonnement des services visibles depuis Internet du reste du système d'information

Niveau standard

- **Garantissez un haut niveau de protection de l'hébergement en interne des services visibles sur Internet** avec des administrateurs compétents. En cas d'impossibilité, recourrez à un hébergeur externe.
- **Cloisonnez physiquement les infrastructures d'hébergement Internet** des infrastructures du système d'information non visibles depuis Internet.

- **Mettez en place une infrastructure d'interconnexion** de ces services avec Internet pour filtrer les flux liés à ces services de manière distincte des autres flux de votre entreprise.
- **Imposez le passage des flux entrants par un serveur mandataire inverse** ayant différents mécanismes de sécurité.

Mesure 24 : la protection de la messagerie professionnelle

Niveau standard

- **Sensibilisez vos utilisateurs quant à l'utilisation de la messagerie professionnelle** et créez des mesures organisationnelles.
- **Interdisez la redirection de messages professionnels** vers une messagerie personnelle. D'autres moyens d'accès distant à la messagerie peuvent être mis en place.

La messagerie professionnelle doit assurer :
- la disposition d'un système d'analyse antivirus ;
- l'activation du chiffrement TLS des échanges entre serveurs de messagerie et entre les postes utilisateur et les serveurs hébergeant les boîtes mails.

Niveau renforcé

- Créez un serveur relais dédié à l'envoi et à la réception des messages en coupure d'Internet pour ne pas exposer directement les serveurs.
- Mettez en place un service anti-spam.
- Demandez la création de mécanismes de vérification d'authenticité et de la bonne configuration des enregistrements DNS publics liés à votre infrastructure de messagerie à votre administrateur de messagerie.

Mesure 25 : la sécurisation des interconnexions réseau dédiées aux partenaires

Niveau standard

Votre entreprise peut avoir besoin d'une interconnexion avec un fournisseur ou un client. Dans ce cas, l'interconnexion peut se faire via votre réseau privé ou sur Internet.

Établissez un tunnel site à site pour l'interconnexion via Internet.

Faites un filtrage IP via un pare-feu et réduisez la matrice des flux au besoin opérationnel. La configuration des équipements devra y être conforme.

Niveau renforcé

Prenez un équipement de filtrage IP pour les connexions partenaires dédiées si votre entreprise a des besoins exigeants en matière de sécurité.

La connaissance d'un point de contact à jour chez le partenaire est requise pour réagir lors d'un incident de sécurité.

Mesure 26 : le contrôle et la protection de l'accès aux salles serveurs et aux locaux techniques

Niveau standard

- **Identifiez les mesures de sécurité physique adéquates** et sensibilisez vos utilisateurs aux risques engendrés par leur contournement.
- **Contrôlez les accès aux salles serveurs et aux locaux techniques** avec des serrures ou des mécanismes de contrôle d'accès par badge.
- **Interdisez les accès non accompagnés des prestataires extérieurs**, sauf si vous tracez les accès et les limitez en fonction des plages horaires.
- **Effectuez périodiquement une revue des droits d'accès** pour identifier les accès non autorisés.
- **Retirez les droits d'accès lors d'un départ d'un collaborateur ou d'un changement de partenaire**.
- **Restreignez ou désactivez les prises réseau dans les zones ouvertes au public**.

VI. LA SECURISATION DE L'ADMINISTRATION

Mesure 27 : l'interdiction d'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système d'information

Niveau standard

- **Coupez l'accès à Internet** des postes de travail ou serveurs utilisés pour les actions d'administration.
- **Mettez en place un poste de travail distinct** ou une infrastructure virtuelle distante pour la bureautique pour les usages nécessitant Internet.

Niveau renforcé

- **Obtenez les mises à jour logicielles des équipements administrés depuis une source sûre.**
- Transférez-les sur le poste (ou le serveur) utilisé pour l'administration non connecté à Internet. Le transfert peut être effectué sur un support amovible dédié.

La mise en place d'une zone d'échanges est recommandée pour l'automatisation de certaines tâches.

Mesure 28 : l'utilisation d'un réseau dédié et cloisonné pour l'administration du système d'information

Niveau standard

Cloisonnez le réseau d'administration.

Pour rappel, le réseau d'administration interconnecte les postes ou serveurs d'administration et les interfaces d'administration des équipements.

Privilégiez un cloisonnement physique des réseaux ou mettez en œuvre un cloisonnement logique cryptographique avec des tunnels IPsec ou un cloisonnement logique par VLAN.

Mesure 29 : la limitation au besoin opérationnel des droits d'administration sur les postes de travail

Niveau standard

- **Ne donnez pas de privilèges d'administration à un utilisateur du SI** sur son poste de travail. En revanche, vous pouvez proposer un magasin d'applications validées par votre entreprise.
- Tracez, limitez dans le temps et retirez à échéance l'attribution de privilèges nécessaire.

VII. LA GESTION DU NOMADISME

Mesure 30 : les mesures de sécurisation physique des terminaux nomades

Niveau standard

Prévoyez des mesures de sécurisation des terminaux nomades (ordinateurs portables, tablettes et ordiphones).
Par exemple, vous pouvez :

- sensibiliser les utilisateurs ;
- banaliser les terminaux nomades ;
- installer un filtre de confidentialité sur les écrans.

Niveau renforcé

Mettez en place un support externe complémentaire pour la conservation des secrets de déchiffrement ou d'authentification. Il doit être conservé à part.

Mesure 31 : le chiffrement des données sensibles

Niveau standard

- **Chiffrez les données stockées sur le matériel nomade**. Elles doivent être accessibles à partir d'un mode de passe. Vous pouvez recourir à une solution de chiffrement de partition, d'archives ou de fichiers.
- Commencez par un chiffrement complet du disque, puis ensuite un chiffrement d'archives ou de fichiers.

Mesure 32 : la sécurisation de la connexion réseau sur des postes utilisés en situation de nomadisme

Niveau standard

Établissez un tunnel VPN IPsec entre un poste nomade et une passerelle VPN IPsec pour une utilisation de votre SI en dehors de l'entreprise. Ce tunnel doit être automatiquement établi et ne pas être contournable.

Vous pouvez autoriser une connexion à la demande ou encourager le partage de connexion depuis un téléphone de confiance.

Niveau renforcé

Ayez recours à une authentification forte.

Mesure 33 : l'adoption des politiques de sécurité dédiées aux terminaux mobiles

Niveau standard

- **Ne mutualisez pas les usages personnels et professionnels** sur un seul terminal. Les terminaux de l'entreprise doivent faire l'objet d'une sécurisation à part entière.
- Privilégiez l'utilisation d'une solution de gestion centralisée des équipements mobiles.
- Configurez des politiques de sécurité homogènes.

Dans le cas contraire, une configuration préalable et une séance de sensibilisation des utilisateurs sont souhaitables.

Niveau renforcé

N'utilisez pas les assistants vocaux intégrés.

VIII. LE MAINTIEN DU SYSTEME D'INFORMATION A JOUR

Mesure 34 : la définition d'une politique de mise à jour des composants du système d'information

Niveau standard

Informez-vous sur l'apparition de nouvelles vulnérabilités.

Appliquez les correctifs de sécurité sur votre système dans le mois suivant leur publication.

Définissez une politique de mise à jour précisant :

- la manière dont l'inventaire des composants du système d'information est réalisé ;

- les sources d'information relatives à la publication des mises à jour ;
- les outils pour déployer les correctifs ;
- l'éventuelle qualification des correctifs et leur déploiement progressif sur le parc.

Isolez les composants obsolètes qui ne sont plus supportés par leurs fabricants.

Mesure 35 : l'anticipation de la fin de la maintenance des logiciels et des systèmes et la limitation des adhérences logicielles

Niveau standard

Anticipez les obsolescences à l'aide des bonnes pratiques suivantes :
- l'établissement et la tenue d'un inventaire des systèmes et des applications du SI ;
- le choix de solutions dont le support est assuré pour une durée correspondant à leur utilisation ;
- le suivi des mises à jour et des dates de fin de support des logiciels ;
- le maintien d'un parc logiciel homogène (ayant la même version) ;
- la limitation des adhérences logicielles ;
- l'inclusion de clauses garantissant le suivi des correctifs de sécurité et la gestion des obsolescences dans les contrats avec les prestataires et les fournisseurs ;
- l'identification des délais et des ressources nécessaires à la migration des logiciels en fin de vie.

IX. LA SUPERVISION, L'AUDIT ET LA REACTION

Mesure 36 : l'activation et la configuration des journaux des composants importants

Niveau standard

Disposez de journaux pertinents pour détecter les dysfonctionnements et tentatives d'accès illicites aux composants du SI.

Identifiez les composants critiques du SI.

Analysez la configuration des éléments journalisés et adaptez-les. Les événements critiques pour la sécurité doivent être journalisés et gardés pendant un an au minimum.

Effectuez une étude contextuelle du SI et journalisez les éléments suivants :
- les zones bloquées par le pare-feu ;
- les authentifications, les autorisations et les arrêts inopinés des systèmes et des applications ;
- les erreurs de protocoles et la traçabilité des flux d'application aux interconnexions des services.

Les sources de synchronisation de temps doivent être identiques.

Niveau renforcé

Centralisez les journaux sur un dispositif dédié.

Mesure 37 : la définition et l'application d'une politique de sauvegarde des composants critiques

Niveau standard

Formalisez une politique de sauvegarde régulièrement mise à jour et intégrez les éléments suivants :

- la liste des données vitales pour l'entreprise et les serveurs concernés ;
- les différents types de sauvegarde ;
- la fréquence des sauvegardes ;
- la procédure d'administration et d'exécution des sauvegardes ;
- les informations de stockage et les restrictions d'accès aux sauvegardes ;
- les procédures de test de restauration ;
- la destruction des supports ayant contenu les sauvegardes.

Les tests de restauration peuvent être réalisés :

- systématiquement par un ordonnanceur de tâches pour les applications importantes ;
- ponctuellement en cas d'erreurs sur les fichiers ;
- de façon globale pour une sauvegarde et restauration entières de SI.

Niveau renforcé

Planifiez une fois par an un exercice de restauration des données et conservez une trace technique des résultats.

Mesure 38 : des contrôles et des audits de sécurité réguliers

Niveau standard

Faites des audits réguliers du SI pour évaluer l'efficacité des mesures mises en œuvre. Ils mesurent les écarts persistants entre la règle et la pratique. Ils sont réalisés par des équipes d'audit internes ou externes.

Des audits techniques et/ou organisationnels seront à effectuer par les professionnels.

Identifiez les actions correctives à effectuer.

À noter
Un tableau de bord pourra indiquer l'état d'avancement du plan d'actions.

Mesure 39 : la désignation d'un référent en sécurité des systèmes d'information

Niveau standard

Disposez d'un référent en sécurité des systèmes d'information. Il sera formé à la sécurité des systèmes d'information et à la gestion de crise.

Il devra être connu de tous vos utilisateurs et sera le premier contact pour toutes les questions relatives à la sécurité des systèmes d'information. À savoir :

- la définition des règles à appliquer selon le contexte ;
- la vérification de l'application des règles ;
- la sensibilisation des utilisations et la définition d'un plan de formation des acteurs informatiques ;
- la centralisation et le traitement des incidents de sécurité constatés ou remontés par les utilisateurs.

Il pourra devenir le relais du RSSI.

Mesure 40 : la définition d'une procédure de gestion des incidents de sécurité

Niveau standard

Le **constat d'un comportement inhabituel** de la part d'un poste de travail ou d'un serveur peut alerter sur une intrusion.

Une mauvaise réaction en cas d'incident de sécurité peut faire empirer la situation. La procédure est de :

- déconnecter la machine du réseau ;
- maintenir sous tension la machine pour ne pas perdre d'informations utiles pour analyser l'attaque ;
- prévenir la hiérarchie et le référent.

Le référent peut prendre contact avec un prestataire spécialisé dans la gestion des incidents pour réaliser les opérations techniques nécessaires et déterminer si d'autres éléments du SI ont été compromis.

Il faudra supprimer les codes malveillants et les accès dont disposerait l'attaquant et procéder au changement des mots de passe compromis. Tout incident devra être inséré dans un registre centralisé.
Une plainte pourra être déposée.

Pour aller plus loin

Mesure 41 : l'analyse de risques formelle

Niveau renforcé

Votre entreprise évolue dans un environnement informationnel propre. Vous devez prendre en compte les risques de sécurité du SI pour toute prise de position ou plan d'actions.
Il vous faut :

- définir le contexte ;
- apprécier les risques ;
- les traiter.

L'**évaluation de ces risques** s'opère selon deux axes : leur probabilité d'apparition et leur gravité.

Vous pourrez alors **élaborer un plan de traitement du risque** à faire valider par une autorité désignée.

Trois types d'approches peuvent être envisagés pour maîtriser les risques du SI :
- le recours aux bonnes pratiques de sécurité informatique ;
- une analyse de risques systématique fondée sur les retours d'expérience des utilisateurs ;
- une gestion structurée des risques formalisée par une méthodologie dédiée.

Dans ce dernier cas, la **méthode EBIOS** référencée par l'ANSSI est recommandée. Elle permet :
- d'exprimer les besoins de sécurité ;
- d'identifier les objectifs de sécurité ;
- de déterminer les exigences de sécurité.

Mesure 42 : l'usage de produits et de services qualifiés par l'ANSSI

Niveau renforcé

La qualification prononcée par l'ANSSI offre des **garanties de sécurité et de confiance**.