L'HYGIÈNE INFORMATIQUE DE VOTRE ENTREPRISE

GUIDE DE BONNES PRATIQUES à l'attention des dirigeants

QU'EST-CE QUE L'HYGIÈNE INFORMATIQUE ?

Indispensable pour protéger les systèmes d'information, l'hygiène informatique est considérée comme une composante majeure dans la stratégie des entreprises.

Elle s'inscrit directement dans les opérations de sensibilisation à la cybersécurité et a pour but de diffuser une culture de la cybersécurité pour développer des bons réflexes au travail. Bien protéger les informations confidentielles confiées par ses clients et ses partenaires peut désormais créer un avantage concurrentiel.

Il est de la responsabilité de chaque dirigeant de vérifier que les mesures de protection mises en place sont adaptées, opérationnelles, comprises et connues de tous.

ELLES DOIVENT FAIRE L'OBJET D'UNE POLITIQUE DE SÉCURITÉ ÉCRITE DONT L'APPLICATION DOIT ÊTRE RÉGULIÈREMENT VÉRIFIÉE PAR L'ENCADREMENT.

QUEL EST SON OBJECTIF ?

Dans son Panorama des cybermenaces 2022 publié en janvier 2023, l'ANSSI préconise aux dirigeants d'entreprise d'adopter une bonne hygiène informatique pour se prémunir des cyberattaques toujours plus nombreuses et diversifiées.

Les entreprises et, plus globalement l'ensemble des structures doivent se protéger et mettre en place des solutions de sécurité afin de garantir la protection des données.

La perte ou le vol de certaines informations ou l'indisponibilité de son système d'information peut avoir des conséquences dommageables pour l'entreprise : perte de confiance des clients et des partenaires, avantage pris par un concurrent, perte d'exploitation suite à une interruption de la production.

EN SUIVANT CES RECOMMANDATIONS, L'ENTREPRISE ATTÉNUE LES RISQUES D'INCIDENTS MAJEURS, S'INSCRIT DANS UNE DÉMARCHE D'AMÉLIORATION CONTINUE ET FAVORISE SA COMPÉTITIVITÉ.

LES THÉMATIQUES

- SÉCURISATION DES POSTES
- SENSIBILISATION & FORMATION
- CONNAISSANCES DU SYSTÈME D'INFORMATION
- GESTION DU NOMADISME
- AUTHENTIFICATION & CONTROLE DES ACCÈS
- SÉCURISATION DU RÉSEAU

QUELQUES RÈGLES DE BONNES PRATIQUES

1. **SÉCURISER LES POSTES**
   Activer et configurer le pare-feu local des postes de travail
2. **SENSIBILISER & FORMER**
   Former les équipes opérationnelles à la sécurité des systèmes d'information
3. **CONNAITRE LE SYSTÈME D'INFORMATION**
   Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau
4. **GÉRER LE NOMADISME**
   Sécuriser la connexion réseau des postes utilisés en situation de nomadisme
5. **AUTHENTIFIER & CONTROLER LES ACCÈS**
   Protéger les mots de passe stockés sur les systèmes
6. **SÉCURISER LE RÉSEAU**
   Mettre en place des capacités de détection d'intrusion

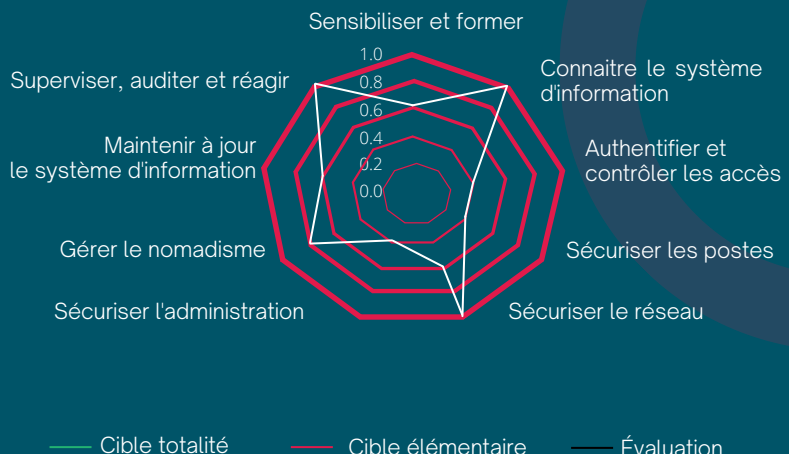
RÉALISEZ UN DIAGNOSTIC DE VOTRE HYGIÈNE INFORMATIQUE ÉVALUEZ VOTRE SÉCURITÉ

Notre offre d'audit à 1 200 € vous permet de bénéficier d'une analyse plus approfondie de votre niveau de sécurité et d'un accompagnement de qualité dans les changements nécessaires à mettre en place.

Audit informatique pour hygiène informatique - Référentiel : guide d'hygiène informatique ANSSI

THÈME	NIVEAU	N° DE FICHE	CRITÈRES	POINTS DE CONTRÔLE	NOTE	CIBLE	EVAL CRIT1	CIBLE CRIT1	RÉPONSES	QUICK WIN	PROPOSITIONS IPGARDE
Sensibiliser et former	1	1	Les équipes opérationnelles sont-elles formées régulièrement à la sécurité générale des systèmes d'information ?	1. Formation lors de la prise de poste 2. Formation tout au long de la carrière 3. Règles de la PSSI connues et appliquées en fonction de la spécificité des services et connaissances des équipes opérationnelles	2	4	0,8	2,5	Pas de formation à la prise de poste Sensibilisation au Phishing/Ransomware.	NON	
Connaitre le système d'information	1	7	Autorisez-vous uniquement la connexion au réseau de l'entité aux seuls équipements maîtrisés ?	1. Avoir des réseaux dédiés pour les équipements externes 2. L'identification des actifs internes est possible et réalisée 3. Il existe des contrôles des connexions externes pour filtrer et autoriser uniquement les actifs internes	4	4	1,6	2,5	L'ensemble du réseau est cloisonné et toutes les connexions externes se font par le biais d'un VPN. Cependant, il n'y a pas de 802.1X sur le wifi et le réseau filaire.	NON	
Authentifier et contrôler les accès	1	8	Identifiez-vous nommément chaque personne accédant au système (éviter les comptes génériques) ?	1. Aucune utilisation de compte générique non indispensable 2. Compte générique connu et rattaché à moins de trois personnes 3. Chaque administrateur a aussi un compte utilisateur avec des accès restreints	5	4	2	2,5	Tous les utilisateurs ont un compte personnel, les administrateurs aussi. À part le compte admin générique IPgarde mais dont les accès sont loggués nominativement dans notre outil. Les comptes admins sont différents des comptes utilisateurs bureautique.		
Sécuriser les postes	1	14	Mettez-vous en place un niveau de sécurité minimal sur l'ensemble du parc informatique ?	1. L'ensemble des actifs sont sécurisés (pare-feu, antivirus) 2. L'ensemble des disques contenant des données sont chiffrés 3. Aucune application inutile installée sur un poste 4. Désactiver les exécutions automatiques (autorun)	5	4	2	2,5	Oui toutes ces choses sont en place.		
Sécuriser le réseau	1	22	Mettez-vous en place une/des passerelle(s) d'accès sécurisé(es) à Internet ?	1. Présence d'un pare-feu avec paramétrage strict 2. Présence d'un proxy avec journalisation des requêtes 3. Pas de DNS manuel sur les postes utilisateurs	5	4	2	2,5	Présence d'un pare-feu et d'un proxy pour filtrage et log des flux web. La configuration réseau est distribuée via DHCP.		
Sécuriser l'administration	1	27	Protection renforcée des ordinateurs d'administration	1. Interdisez-vous l'accès à Internet depuis les postes ou serveurs utilisés par l'administration du système d'information ? 2. Alternative en cas d'accès distant impératif : passer par une solution de prise en main à distance d'un tiers de confiance ?	0	4	0	2,5	N/A		
Gérer le nomadisme	1	32	Sécurisez-vous la connexion réseau des postes utilisés en situation de nomadisme ?	1. Utilisation de VPN SSL ou équivalent 2. VPN non débrayage par l'utilisateur en mode « FULL » 3. Assurer que le poste nomade qui tente de se connecter en VPN est légitime	3	4	1,2	2,5	La plupart des utilisateurs ne se connectent pas en VPN car FULL SasS. Ceux qui s'y connectent (compatible) sont en mode FULL mais aucun contrôle n'est effectué.	NON	
Maintenir à jour les systèmes d'information	1	35	Anticipez-vous la fin de la maintenance des logiciels et systèmes ?	1. Inventaire des systèmes et applications à jour 2. S'assurer que le support est assuré pour une durée correspondant à leur utilisation avec suivi des mises à jour 3. Reco : conserver des versions de logiciels homogènes 4. Reco : réduire les dépendances fonctionnelles avec les logiciels en fin de vie 5. Inclure dans les contrats avec les fournisseurs des clauses garantissant le suivi des correctifs de sécurité et la gestion des obsolescences 6. Identifier les délais et ressources nécessaires à la migration des systèmes et logiciels en fin de vie	5	4	2	2,5	Sur la partie infrastructure, serveur et bureautique, c'est suivi et les versions sont toutes supportés et dans l'air du temps. Concernant les logiciels, ils ont tous été mis à jour lors de la migration car réinstallés.		
Superviser, auditer et réagir	1	1	Activez et configurez-vous les journaux des composants les plus importants ?	1. Cartographier les composants critiques du SI 2. Analyser pour chaque composant des journaux de sécurité à mettre en place et à maintenir 3. Utiliser une source de temps unique pour les composants critiques 4. Mettre en place une solution pour assurer la corrélation des événements et leurs qualifications rapidement	5	4	2	2,5	Oui le CTN dispose d'un SIEM permettant de collecter, centraliser et corréler tous les événements du SI. Derrière ce service, il y a des humains qui caractérisent les alertes et sollicitent l'hébergeur pour remédiation si besoin. Un serveur NTP est en place sur le SI. Mais aucune cartographie applicative		

DÉTERMINONS ENSEMBLE VOTRE NIVEAU DE MATURITÉ CYBER



PROFITEZ DE LA PRESTATION À SEULEMENT

1 200 €

IPgarde Paris
Tour de l'Horloge
4 place Louis Armand
75012 PARIS

IPgarde Valence
Immeuble Rhovalparc
1, avenue de la Gare TGV
26300 ALIXAN

IPgarde Lyon
12, avenue Antoine Dutrievoz
69100 VILLEURBANNE

contact@ipgarde.com
01 77 49 24 50
www.ipgarde.com