Image not found or type unknown

Cybercriminalité en entreprise

Actualité législative publié le **16/10/2019**, vu **1900 fois**, Auteur : Droit de la sécurité informatique

Face aux nouveaux risques auxquels sont exposées les entreprises, des précautions adaptées s'imposent. Reste à identifier les premiers pour mieux les prévenir ou y faire face...

Internet génère désormais sa propre délinquance, avec des malfrats qui se reconvertissent au numérique dans la mesure où les risques sont moins importants pour eux et les gains plus élevés que dans la criminalité classique.

Un simple courriel d'un collègue de travail peut capter les informations les plus sensibles d'une entreprise, tels que les fichiers clients, les offres de remise et la marge opérationnelle. Les cyber-attaques peuvent aussi relever de l'espionnage industriel et menacer alors sa survie.

Dès lors, quelles précautions prendre et à quel niveau ? Et que faire en cas d'intrusion malveillante ?

IDENTIFIER LES ZONES À RISQUE

Mettre en place une protection pour les seuls utilisateurs d'ordinateur se révèle insuffisant, tellement les nouvelles technologies ont envahi notre quotidien professionnel. Il s'agit d'abord des téléphones portables, qu'ils soient professionnels ou privés, des tablettes et des livres électroniques. Mais ce sont aussi les imprimantes-photocopieurs, désormais connectées à l'intranet de l'entreprise, quand elles ne sont pas reliées aux messageries électroniques et au web. On peut y ajouter les machines et le matériel de fabrication, souvent connectés aux fabricants, afin de prévenir l'usure des pièces et de détecter les pannes. Sans parler des contrôles d'accès, des badgeuses ou des outils-systèmes décomptant les temps de travail, tous, eux aussi, connectés.

Summum de la technologie numérisée, le système informatique relie tous ces outils entre eux dans le but d'une gestion assistée par ordinateur et offrent, de ce fait, autant de portes d'entrée aux cybercriminels. Cette gestion numérique généralisée fournit une masse colossale d'informations, mais rend aussi les données de l'entreprise particulièrement vulnérables.

En d'autres termes, il s'agit de bien cerner l'ensemble de son environnement informatique, y compris à l'échelle du groupe : logiciels de gestion, bases de données, « *cloud computing* » et plates-formes, outils d'analyse et d'intelligence artificielle, sans oublier les cyberespaces collaboratifs et les réseaux sociaux. Cet inventaire met en évidence les possibilités d'intrusion hostiles et permet d'identifier les collaborateurs ayant accès à ces outils ou à ces données dans le cadre de leur travail. La limitation d'accès à un personnel sélectionné, formé et expressément autorisé, réduit à elle seule le risque de moitié (*voir* **tableaux** *ci-après*).

Membres du personnel susceptibles d'utiliser les nouvelles technologies sans plan de prév

OUTILS INFORMATIQUES	CADRES DIRIGEANTS	DIRECTEURS ADJOINT	MANAGERS	TECHNICIENS	EMPLOYÉS	OPÉRATEURS	P D
Gestion de la production	OUI	OUI	OUI	OUI	OUI	OUI	1
SIRH	OUI	OUI	OUI	OUI	OUI		9
Intranet	OUI	OUI	OUI	OUI	OUI	OUI	1
Messagerie	OUI	OUI	OUI	OUI	OUI	OUI	1
Gestion financière	OUI	OUI	OUI	OUI	OUI		9
Plates-formes collaboratives	OUI	OUI	OUI	OUI	OUI	OUI	1
Gestion de la chaîne logistique	OUI	OUI	OUI	OUI	OUI	OUI	1
Gestion de la relation client	OUI	OUI	OUI	OUI	OUI		9
Gestion du planning des visites	OUI	OUI	OUI	OUI	OUI		9
Badgeuses parking	OUI	OUI	OUI	OUI	OUI	OUI	1
Téléphones portables	OUI	OUI	OUI	OUI	OUI	OUI	1
Tablettes	OUI	OUI	OUI	OUI	OUI	OUI	1
Gestion des temps	OUI	OUI	OUI	OUI	OUI	OUI	1
Évaluation du risque de cyberattaque							**S**

Copyright © 2025 Légavox.fr - Tous droits réservés

Membres du personnel autorisés après la mise en place d’un plan de prévention							
OUTILS INFORMATIQUES	CADRES DIRIGEANTS	DIRECTEURS ADJOINT	MANAGERS	TECHNICIENS	EMPLOYÉS	OPÉRATEURS	q D
Gestion de la production	OUI	OUI	OUI				5
SIRH	OUI	OUI					3
Intranet	OUI	OUI	OUI				5
Messagerie	OUI	OUI	OUI	OUI			7
Gestion financière	OUI	OUI					3
Plates-formes collaboratives	OUI	OUI	OUI	OUI			7
Gestion de la chaîne logistique	OUI	OUI	OUI				5
Gestion de la relation client	OUI	OUI					3
Gestion du planning des visites	OUI	OUI	OUI				5
Badgeuses parking	OUI	OUI	OUI				5
Téléphones portables	OUI	OUI					3
Tablettes	OUI	OUI					3

Copyright © 2025 Légavox.fr - Tous droits réservés

Membres du personnel autorisés après la mise en place d'un plan de prévention							
OUTILS INFORMATIQUES	CADRES DIRIGEANTS	DIRECTEURS ADJOINT	MANAGERS	TECHNICIENS	EMPLOYÉS	OPÉRATEURS	q F D
Gestion des temps	OUI	OUI	OUI				5
Évaluation du risque de cyberattaque							4

QUELLES SONT LES DIFFÉRENTES FORMES DE DÉLINQUANCE INFORMATIQUE ET LEURS SANCTIONS ?

Infractions

La délinquance informatique a fait l'objet d'une convention du Conseil de l'Europe sur la cybercriminalité qui est entrée en vigueur le 1er juillet 2004.

Quatre grandes catégories d'infractions y sont répertoriées :

celles se rapportant aux contenus prohibés, tels que les actes de production, diffusion, pornographie enfantine. Un protocole additionnel devrait inclure la propagation d'idées racistes et la xénophobie à travers les réseaux ;

la violation de la confidentialité, de l'intégrité et de la disponibilité des données et des systèmes ;

les falsifications et les fraudes informatiques ;

les atteintes à la propriété intellectuelle et aux droits connexes, telles que la distribution à grande échelle de copies illégales d'œuvres protégées, etc.

Le Parlement français a autorisé, le 19 mai 2005, la ratification de la convention, ainsi que son protocole additionnel du 28 janvier 2003 (1)

À ce dispositif, il convient d'ajouter le projet de loi sur le renseignement, adopté en première lecture à l'Assemblée nationale le 5 mai dernier.

Sanctions encourues

Les atteintes à un système informatisé sont sanctionnées par les articles 323-1 et suivants du Code pénal. Ainsi, « *le fait d'accéder* [...] *frauduleusement, dans tout ou partie d'un système de traitement automatisé de données, est puni de deux ans d'emprisonnement et de 30 000 euros d'amende* ».

Le délit d'atteinte volontaire au fonctionnement d'un système informatisé est prévu et puni par l' article 323-2 du Code pénal « *de cinq ans d'emprisonnement et de 75 000 euros d'amende* ».

Copyright © 2025 Légavox.fr - Tous droits réservés

L’article 323-3 du Code pénal soumet aux mêmes sanctions « *le fait d’introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu’il contient* ».

Enfin, l’article 323-3-1 du même code incrimine « *le fait, sans motif légitime* [...] *de détenir* [...] *un programme informatique* [...] *conçu ou spécialement adapté pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 du Code pénal* ».

QUELLES PRÉCAUTIONS PRENDRE ?

L’entreprise doit avant tout se protéger contre les intrusions informatiques malveillantes via internet ou les messageries.

Accès internet

La direction peut fixer à cette fin les conditions et limites des connections des salariés.

Des systèmes de filtrage de sites non autorisés sont préconisés.

A minima, deux types d’outils doivent être déployés pour sécuriser un réseau : les pare-feux et les sondes de détection/prévention d’intrusions.

La Cnil autorise également l’entreprise à fixer des limites dictées par un souci de sécurité, telles que l’interdiction de télécharger des logiciels, de se connecter à un forum ou d’utiliser le « *chat* », d’accéder à une boîte aux lettres personnelle par internet compte tenu des risques de propagation de virus.

Ces systèmes de protection contre les intrusions numérisées doivent être portés à la connaissance des salariés.

Concrètement, ceux-ci doivent connaitre la finalité du dispositif de contrôle et la durée pendant laquelle les données de connexion sont conservées. Six mois sont suffisants, dans la plupart des cas, pour être suffisamment dissuasif.

Le CE doit avoir été préalablement consulté et informé.

Lorsque l’entreprise met en place ce type de dispositif de contrôle, assorti d’un relevé des connexions ou des sites visités, poste par poste, celui-ci doit être déclaré à la Cnil (déclaration normale), sauf si un correspondant informatique et libertés a été désigné, auquel cas aucune déclaration n’est nécessaire.

Messageries électroniques

Pour prévenir les cyberattaques, la direction d’une entreprise peut aussi mettre en place des outils de contrôle de la messagerie.

La Cnil cite à titre d’exemple les outils de mesure de la fréquence, de la taille des courriels et ceux analysant les pièces jointes (détection des virus, filtres « *anti-spam* » destinés à réduire les messages non sollicités, etc.).

Ce type de dispositif de contrôle de la messagerie doit aussi faire l’objet d’une consultation du CE et d’une information individuelle des salariés.

Il convient par ailleurs d’informer les membres du personnel de la finalité du dispositif et de la durée pendant laquelle les données de connexion sont conservées ou sauvegardées, ainsi que les modalités de cet archivage, la durée de conservation des messages et les conditions

Copyright © 2025 Lédavox.fr - Tous droits réservés

d’exercice de leur droit d’accès.

Comme pour le contrôle des connections, ces dispositifs doivent être déclaré à la Cnil, et ce dans les mêmes conditions.

Mise en garde solennelle du personnel

L’information du personnel joue un rôle essentiel, car elle permet prévenir les attaques hostiles et de dissuader les salariés de participer à ce type de délinquance informatique.

Pour être efficace, la mise en garde doit revêtir une forme particulièrement impérieuse, ce qui lui confère un caractère disciplinaire.

Dans ce cas, sa diffusion devra respecter la procédure inhérente aux notes de service annexées au règlement intérieur (2) .

La direction doit dès lors recueillir l’avis du comité d’entreprise ou, à défaut, des délégués du personnel.

En même temps qu’elle fait l’objet des mesures de publicité, cette note doit être communiquée en deux exemplaires à l’inspecteur du travail accompagné de l’avis des représentants du personnel (3)

EXEMPLE DE MISE EN GARDE Attention aux cyber-attaques !

Afin de protéger notre entreprise des agressions informatiques par des délinquants cherchant à pirater notre système ou dérober nos fonds ou encore capter nos procédés les plus secrets, nous avons mis en place un système de contrôle systématique des connexions sur internet et des courriels reçus ou émis par notre société.

Ce dispositif permet de détecter les sites dangereux pour notre sécurité et les messages électroniques suspects en raison de leur fréquence, leur taille ou des pièces qui y sont jointes...

Le système bloque les messages ou connexions indésirables et l’utilisateur en est informé.

Pour débloquer la communication ou la connexion suspecte, ce dernier doit en faire une demande expresse par messages électroniques au service informatique : *Svp.informatique@lentreprise.com.*

QUELS SONT LES INVESTIGATIONS ET LES CONTRÔLES ENVISAGEABLES ?

La mise en place de systèmes de protection ne suffit pas. L’entreprise doit pouvoir lancer des investigations en cas de suspicions de cybercriminalité.

Dès lors se pose la question des conditions dans lesquelles celles-ci doivent être menées.

L’enjeu réside dans le fait qu’il faut respecter les libertés individuelles, tout en se protégeant efficacement.

Respect de la vie personnelle

Les communications électroniques émises ou reçues par un salarié peuvent relever du secret des correspondances privées dont la violation est pénalement sanctionnée (4) . Toutefois, les fichiers qui ne sont pas identifiés comme « *personnels* » sont réputés être professionnels, de sorte que la direction peut y accéder librement, y compris en dehors de la présence du collaborateur.

Copyright © 2025 Légavox.fr - Tous droits réservés

Tel est le cas des messages dans lesquels n'est pas mentionné le terme « *personnel* » ou « *privé* » (5)

En revanche, les fichiers classés dans un dossier « *personnel* » ne sont pas accessibles à l'entreprise sans l'accord du salarié.

Pour ce faire, la Cnil préconise d'en informer les collaborateurs, afin qu'ils différencient leurs courriels professionnels et personnels (qualification par l'objet, création d'un répertoire spécifique dédié au contenu privé, etc.).

Dans ce cas, si la direction décide de procéder à des investigations, celles-ci doivent être incontestables sur le plan de la preuve. Dès lors, il est conseillé de n'accéder aux données numérisées du salarié qu'en présence de témoins ou d'un huissier qui en dressera le constat.

Enfin, en cas de forts soupçons de cybercriminalité, par ailleurs justifiés, la direction peut demander au juge l'autorisation d'ouvrir les fichiers et courriels personnels du salarié, même hors de sa présence.

Dans les cas les plus avérés de fraude informatique, il sera possible de saisir la police pour mener des investigations plus approfondies (*voir ci-après*).

Pour l'usage d'internet, le juge estime que l'employeur a aussi le droit de surveiller les connexions Internet de ses salariés grâce à l'historique des sites visités durant le temps de travail, à l'aide de l'ordinateur professionnel, étant précisé que pour contrôler les connexions Internet, la présence du collaborateur n'est pas requise (6) .

Quels moyens de surveillance utiliser ?

En cas de soupçons de cybercriminalité de la part de salariés, l'entreprise peut recourir à des dispositifs de contrôle et de surveillance du personnel (7) , à condition qu'il ne s'agisse pas de procédés clandestins mis en place à leur insu.

Un service d'audit ou d'enquête interne peut observer leur travail au quotidien, dès lors que cette surveillance est limitée au temps de travail et qu'elle ne porte pas atteinte à la vie privée des intéressés (8) .

Ces contrôles ne constituent pas, même en l'absence d'information et de consultation préalable du CE, un moyen de preuve illicite.

Quand et comment organiser une enquête en interne ?

Lors d'une cyber-alerte, l'entreprise peut lancer immédiatement des investigations internes et fouiller les ordinateurs et portables professionnels de ses collaborateurs pour y rechercher les indices d'une attaque.

Informations des IRP, de la Cnil et du personnel

Bien que la jurisprudence admette que de telles enquêtes puissent ne pas être soumises à l'avis du comité d'entreprise, sa consultation participe à la bonne diffusion de l'information auprès du personnel et donc à la dissuasion.

Comment organiser une enquête interne ?

Copyright © 2025 Légavox.fr - Tous droits réservés

ÉTAPES	OBJET	DÉCISIONNAIRE
Élaboration des séquences de l’enquête et des moyens de contrôle	Préparation de l’information interne	DRH, DSI et sécurité
Préparation de la communication	Rédaction des notes d’information à destination du CE et du personnel	DRH
Convocation du CE	Remise d’un document d’information	Chef d’entreprise ou DRH
Réunion du management	Remise d’un document d’information	Chef d’entreprise ou DRH
Réunion du CE	Consultation du CE	Chef d’entreprise ou DRH
Déclarations à la Cnil	Moyens de contrôle et de surveillance	DRH ou DSI
Note d’information	Information sur les moyens de contrôle et l’enquête	DRH

Déroulement de l’enquête

Les moyens de surveillance électronique vont permettre de détecter l’existence d’indices de délinquance informatique. Dès lors, le service en charge de l’enquête doit se mobiliser pour déployer rapidement des investigations et prendre immédiatement des mesures pour sauvegarder les intérêts de l’entreprise.

L’objectif est double :

préserver immédiatement l’ensemble des outils informatiques et les données qu’ils contiennent ;

identifier les cybercriminels.

En tout premier lieu, il va s’agir d’isoler le secteur attaqué en coupant tous les accès à internet, les messageries et les ordinateurs susceptibles d’être visés par l’agression numérique. Pour ce faire, il faut interrompre tous les accès informatiques externes. Il faut aussi s’assurer qu’il ne s’agit pas d’un leurre destiné à cacher une attaque encore plus importante sur un autre service. Un salarié peut consulter le « *dark web* » et utiliser TOR, un logiciel qui permet de brouiller son IP, afin de dissimuler aux enquêteurs internes ses connexions illégales. Dans ce cas, la vraie difficulté est de cerner le caractère nocif ou de la cyberattaque ou de la connexion illicite.

Copyright © 2025 Légavox.fr - Tous droits réservés

En second lieu, le service d'enquête interne doit intervenir auprès du moteur de recherche afin d'en effacer les données sensibles.

Durant ce laps de temps, il convient, pour ne pas neutraliser une partie de l'activité de l'entreprise, de réutiliser les supports de communication traditionnels, tels que le téléphone fixe, la prise de rendezvous et les notes papiers.

L'enquêteur analysera ensuite les différentes traces laissées par les cybercriminels.

Pour ce faire, il étudiera l'historique du système informatique afin d'identifier les dysfonctionnements, les failles et les auteurs et complices internes.

Cette méthode d'enquête permet de lister et analyser les processus numérique en cours, afin de cerner les applications suspectes sur le système informatique.

Cette première étape se déroule souvent sans qu'il soit nécessaire d'organiser des rencontres physiques des différents protagonistes.

Ce n'est qu'une fois le système protégé et les premiers indices relevés qu'il va être possible de s'entretenir avec les collaborateurs de l'entreprise.

Toutefois, cette enquête ne doit pas prendre un caractère trop contraignant, rigoureux et formel, au risque d'être assimilée à une sanction disciplinaire.

La Cour de cassation a en effet jugé qu'une demande d'explications écrites faite à un salarié, à la suite de faits considérés comme fautifs, constituait une sanction disciplinaire, dès lors :

que l'intéressé avait dû répondre, seul et immédiatement, aux questions qui lui étaient posées ;

que son refus pouvait être sanctionné ;

que le procès-verbal, consignant les demandes formulées par l'employeur et les réponses écrites du salarié, avaient été conservées dans son dossier individuel (9) .

Les Hauts Magistrats s'étaient déjà prononcés dans le même sens dans une affaire comparable (10) .

Durant l'audition des salariés, l'enquêteur doit donc être prudent. Au vu des éléments rassemblés, une mise à pied à titre conservatoire peut, le cas échéant, être notifiée à ceux sur lesquels pèsent de graves soupçons.

Exemple de convocation (par courriel) à un rendez-vous organisé pour les besoins de l'enquête Bonjour,

Suite à l'incident survenu sur notre système informatique le < **date** >, nous souhaiterions vous recevoir afin d'en discuter avec vous et recueillir des explications nous permettant de comprendre ce qui s'est réellement produit.

Nous vous proposons d'organiser cette entrevue informelle, le < **date** >, à < **heure** >, dans le bureau de *Madame (ou Monsieur)* < >.

Nous comptons sur votre coopération.

Copyright © 2025 Légavox.fr - Tous droits réservés

Merci de contacter *Madame (ou Monsieur)* < > par courriel (< **adresse** >) ou par téléphone (< **numéro** >) pour confirmer votre venue.

Bien à vous

Signature

Faire appel à la police

L'enquête interne permet surtout d'évaluer la gravité de l'attaque ou de l'infraction et son caractère malveillant.

Dès lors que ceux-ci sont avérés, la direction a tout intérêt à passer la main aux services *ad hoc* de la police ou de la gendarmerie.

Ces derniers sont mobilisés depuis plusieurs années sur ce nouveau type de criminalité. Pour y faire face, la police nationale dispose de 389 investigateurs spécialisés, coordonnés entre eux et formés par la Sous-direction de la lutte contre la cybercriminalité (SDLC).

Leur rôle est essentiellement préventif. Des fiches pratiques sont disponibles sur leur site internet.

De son côté, la gendarmerie a mis en place des structures, dont le Département cybercriminalité du service technique de recherches judiciaires et de documentation (STRJD).

Ces services assurent la surveillance des activités sur internet en recherchant les infractions portant atteinte aux personnes et aux biens, ainsi que les connections ou les téléchargements à caractère illicites (« *Internet Relay Chat* », newsgroups, réseaux d'échanges communautaires, *peer to peer*...).

Parce qu'il est très facile, en quelques clics, de devenir un cybercriminel, l'entreprise doit aujourd'hui mieux se protéger, y compris à l'égard de son personnel. Mais cela doit se faire dans les règles du droit et le respect des libertés individuelles.

(1)

L. n° 2005-493, 19 mai 2005 ; D. n° 2006-580, 23 mai 2006.

(2)

Cass. crim., 26 juin 1990, n° 88-84.251.

(3)

C. trav., art. R. 1321-4.

(4)

Copyright © 2025 Légavox.fr - Tous droits réservés

C. pén., art. L. 226-15.

(5)

Cass. soc., 30 mai 2007, n° 05-43.102.

(6)

Cass. soc., 9 févr. 2010, n° 08-45.253, Cass. soc., 9 juill. 2008, n° 06-45.800.

(7)

Cass. soc., 10 janv. 2012, n° 10-23.482.

(8)

Cass. soc., 5 nov. 2014, n° 13-18.427.

(9)

Cass. soc., 19 mai 2015, n° 13-26.916.

(10)

Cass. soc., 7 juin 2011, n° 10-14.444

Copyright © 2025 Légavox.fr - Tous droits réservés