DU BLOG IUSTORIA

Cyberattaque ou fuite de données dans l'entreprise : que faire dans les 72 premières heures

> *Serveurs chiffrés, rançon exigée, base clients divulguée. Que notifier à l'ÚOOÚ sous 72 heures, quand alerter le NÚKIB sous 24 heures, que dire à l'assureur et aux partenaires, pourquoi ne pas payer.*

L'ÉQUIPE IUSTORIA

5/11/2026 · 12 min de lecture

Lundi matin, les fichiers du disque partagé refusent de s'ouvrir et les écrans affichent un message : les données sont chiffrées, et voici où envoyer la rançon. Ou bien un client appelle pour signaler que quelqu'un vend sur Internet ses données issues de votre base. Le premier appel va à l'administrateur informatique, et c'est normal. Au cabinet, nous constatons pourtant qu'on ne pense au volet juridique qu'une semaine plus tard, une fois les serveurs relancés. Les délais de notification sont alors déjà expirés, et les traces qui auraient permis à l'entreprise de se défendre devant l'autorité, l'assureur ou le juge ont disparu avec la réinstallation.

Or, pendant les trois premiers jours, on ne décide pas seulement de questions techniques. On décide aussi de ce qu'il faut notifier et à qui, de qui informer, de la manière de préserver les preuves et de l'opportunité de payer. Nous passons en revue les délais prévus par le règlement général sur la protection des données (RGPD) et par la nouvelle loi tchèque sur la cybersécurité, ce qu'il faut attendre de l'assureur et des partenaires commerciaux, et qui répond de la décision sur la rançon.

Les premières heures : stopper l'attaque sans effacer les traces

L'Agence nationale pour la cybersécurité et la sécurité de l'information (NÚKIB) recommande, une fois le rançongiciel détecté, de déconnecter les appareils du réseau et de ne les éteindre qu'en dernier recours, car l'extinction efface les traces présentes dans la mémoire vive. Le serveur de sauvegarde est déconnecté en premier, pour que l'attaque n'atteigne pas aussi les sauvegardes. Le NÚKIB recommande encore de réaliser des copies bit à bit des systèmes touchés, de recueillir les journaux d'activité (logs) et des échantillons du code malveillant, et de communiquer en dehors du réseau attaqué, par téléphone par exemple. L'attaquant peut en effet continuer à lire la messagerie de l'entreprise.

Sur le plan juridique, nous ajoutons deux choses. Premièrement, tenez dès la première minute un journal de l'incident : quand et par qui l'attaque a été découverte, ce qui s'est passé, qui a décidé quoi et pourquoi. Le moment de la découverte fait courir les délais, et le responsable du traitement doit documenter toute violation de données à caractère personnel, même s'il ne la notifie finalement pas (art. 33, par. 5, du RGPD). Deuxièmement, ne réinstallez rien tant que vous n'avez pas les copies. La police, l'assureur et l'Office pour la protection des données personnelles (ÚOOÚ) ont tous besoin des traces de l'attaque. Mais c'est surtout vous qui en aurez besoin, lorsqu'il faudra prouver que l'entreprise était protégée de manière adéquate.

Violation de données à caractère personnel : notification à l'ÚOOÚ sous 72 heures

Constitue une violation de données à caractère personnel non seulement leur fuite, mais aussi leur destruction, leur perte ou leur altération, de manière accidentelle ou illicite (art. 4, point 12, du RGPD). Un rançongiciel qui chiffre la base clients ou les données de paie constitue donc une violation, même si l'attaquant n'a rien emporté. L'ÚOOÚ comme le Comité européen de la protection des données (CEPD) la classent parmi les violations de la disponibilité.

Il n'est pas pour autant nécessaire de notifier toute violation de ce type. Le CEPD cite l'exemple d'une petite entreprise qui conservait ses données sous forme chiffrée, les a restaurées en quelques heures à partir d'une sauvegarde fonctionnelle sans que son activité soit interrompue, et dont l'analyse des journaux a montré avec certitude que l'attaquant n'avait rien copié ; le risque pour les personnes y était improbable, et il suffisait de documenter l'incident. Pour une entreprise qui a mis cinq jours ouvrables à restaurer ses données à partir de documents papier, il juge en revanche la notification nécessaire. Et lorsque le responsable du traitement ne sait pas avec certitude jusqu'où l'attaquant est allé, il doit, selon le CEPD, retenir l'hypothèse la plus défavorable.

Le responsable du traitement notifie la violation à l'ÚOOÚ dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. Il en est dispensé seulement si la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. S'il notifie plus tard, il doit indiquer les motifs du retard (art. 33, par. 1). Selon le CEPD, le responsable du traitement a « pris connaissance » de la violation dès qu'il a un degré raisonnable de certitude qu'un incident s'est produit et que des données à caractère personnel ont été compromises. Le délai se compte en heures et le week-end ne l'interrompt pas.

N'attendez pas que l'informatique ait terminé son analyse. Si vous ne connaissez pas encore l'ampleur de la violation, notifiez ce que vous savez et complétez de manière échelonnée ; le règlement le permet expressément (art. 33, par. 4, du RGPD). Mieux vaut une notification incomplète déposée à temps qu'une notification complète accompagnée d'excuses pour le retard.
La notification doit décrire la nature de la violation, y compris les catégories et le nombre approximatif de personnes et d'enregistrements concernés, indiquer les coordonnées du délégué à la protection des données ou d'un autre point de contact, et décrire les conséquences probables ainsi que les mesures prises (art. 33, par. 3). L'ÚOOÚ met à disposition un formulaire électronique à cet effet. Le formulaire rempli peut être envoyé par boîte de données (*datová schránka*, la boîte électronique de l'État tchèque pour les communications officielles ; identifiant de l'ÚOOÚ : qkbaa2n), par la poste ou par e-mail à posta@uoou.gov.cz. L'e-mail doit toutefois porter une signature électronique reconnue (*uznávaný elektronický podpis*) ; à défaut, l'autorité ne le considère comme une notification régulière que si vous le confirmez par un formulaire signé de votre main, envoyé par la poste ou remis en personne. La voie la plus sûre est la boîte de données.

La responsabilité incombe au responsable du traitement, c'est-à-dire à celui qui décide du traitement. Si l'attaque a eu lieu chez un prestataire, par exemple un fournisseur de cloud ou l'éditeur du logiciel de paie, celui-ci doit, en tant que sous-traitant, vous la notifier dans les meilleurs délais (art. 33, par. 2) et vous aider à respecter vos obligations (art. 28, par. 3, point f)). C'est néanmoins à vous de notifier l'ÚOOÚ. La violation de ces obligations expose à une amende pouvant atteindre 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu (art. 83, par. 4).

En novembre 2025, dans le cadre de ce qu'on appelle l'omnibus numérique, la Commission européenne a proposé de porter le délai à 96 heures et de ne notifier que les cas présentant un risque élevé. Au 6 novembre 2026, la proposition n'avait pas été adoptée, et le délai de 72 heures s'applique.

Quand écrire aux personnes dont les données ont fuité

Lorsque la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes, le responsable du traitement doit aussi les en informer directement, dans les meilleurs délais (art. 34, par. 1, du RGPD). Il s'agit typiquement de fuites de mots de passe, de numéros d'identification personnels, de numéros de compte, de données de santé ou de tout ce qui peut servir à une fraude. La communication est rédigée en des termes clairs et simples et indique un point de contact, les conséquences probables et les mesures prises (art. 34, par. 2). Nous recommandons d'y ajouter ce que les personnes doivent faire : changer leurs mots de passe, se méfier des e-mails et des appels qui se réclament de votre entreprise, et surveiller les mouvements sur leur compte. Les escrocs aiment se servir des données divulguées pour rendre leurs messages crédibles.

Vous n'êtes pas tenu d'informer les personnes si les données étaient chiffrées et incompréhensibles pour l'attaquant, si vous avez pris des mesures garantissant que le risque élevé n'est plus susceptible de se matérialiser, ou si cette communication exigeait des efforts disproportionnés. Dans ce dernier cas, vous devez toutefois procéder à une communication publique (art. 34, par. 3). L'ÚOOÚ peut exiger que la communication soit faite (art. 34, par. 4).

Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du règlement a le droit d'en obtenir réparation (art. 82, par. 1). Dans son arrêt du 14 décembre 2023, Natsionalna agentsia za prihodite, affaire C-340/21, la Cour de justice de l'UE a examiné une attaque contre l'administration fiscale bulgare, à la suite de laquelle les données de plus de six millions de personnes ont été publiées sur Internet. Elle a jugé qu'une fuite résultant d'une attaque de tiers ne signifie pas à elle seule que les mesures du responsable du traitement n'étaient pas appropriées. Dans un litige en réparation, c'est toutefois au responsable du traitement de prouver qu'elles l'étaient, et il n'est pas exonéré de sa responsabilité au seul motif que la fuite a été causée par l'attaquant. La seule crainte d'une utilisation abusive des données peut en outre constituer un dommage moral, si elle est fondée au regard des circonstances (dispositif, points 1, 3, 5 et 6 ; point 85). Pour une entreprise, cela signifie qu'elle se défendra avant tout par sa documentation : politiques de sécurité, traces des formations, des mises à jour et des sauvegardes, et journal de l'incident.

La nouvelle loi sur la cybersécurité : êtes-vous concerné ?

Depuis le 1er novembre 2025 est en vigueur la loi n° 264/2025 Rec. relative à la cybersécurité, qui transpose en droit tchèque la directive européenne SRI 2 (NIS 2). Elle s'applique aux fournisseurs de services réglementés dans 15 secteurs, de l'énergie, de l'industrie manufacturière et de l'alimentation aux services numériques, en passant par les transports, l'eau, la gestion des déchets et la santé (art. 4, al. 1). Elle vise en principe les moyennes et grandes entreprises ; une petite entreprise seulement si elle revêt une importance particulière pour l'État, et certains services sont enregistrés par l'agence quelle que soit la taille (art. 5). Les services concernés sont fixés par le décret n° 408/2025 Rec. relatif aux services réglementés. N'attendez pas que l'agence vous contacte : c'est au fournisseur de déclarer lui-même son service au NÚKIB, au plus tard dans les 60 jours suivant le jour où il a rempli les conditions (art. 6, al. 1). La taille de l'entreprise se calcule en outre en tenant compte des sociétés du groupe, si bien que la loi peut aussi viser une petite filiale d'un grand groupe ; seules sont exclues du calcul les sociétés du

groupe dont les actifs techniques sont entièrement séparés de ceux que l'entreprise utilise pour fournir le service réglementé (art. 7, let. c)). Une entreprise qui a récemment grandi, s'est lancée dans une nouvelle activité ou a rejoint un groupe devrait le vérifier sans attendre.

Le fournisseur relevant du régime des obligations renforcées (*režim vyšších povinností*) signale les incidents au NÚKIB, celui qui relève du régime des obligations allégées (*režim nižších povinností*) au CERT national, et seulement ceux qui ont un impact important sur le service (art. 15, al. 1 à 3). Les délais sont plus courts que sous le RGPD : un signalement initial au plus tard 24 heures après la détection de l'incident (art. 16, al. 1). Suivent, dans les 72 heures, une notification comportant une première évaluation, puis, dans les 30 jours de celle-ci, un rapport final. Cela vaut, dans le régime des obligations allégées, pour tout incident signalé ayant un impact important sur le service et, dans le régime des obligations renforcées, lorsque le NÚKIB indique que l'incident a un impact important sur le cyberespace de l'État (art. 16, al. 2 et 3). Les signalements se font via le portail du NÚKIB (art. 16, al. 4). Le fournisseur doit commencer à signaler les incidents au plus tard un an après la notification de la décision d'enregistrement (art. 15, al. 4). En cas de manquement, il s'expose à une amende pouvant atteindre 250 millions de CZK ou 2 % du chiffre d'affaires mondial dans le régime des obligations renforcées, et 175 millions de CZK ou 1,4 % dans le régime des obligations allégées, le montant le plus élevé étant retenu (art. 59, al. 4).

Le signalement au NÚKIB et la notification à l'ÚOOÚ sont deux obligations distinctes, et l'une ne remplace pas l'autre. Les autorités se contentent d'échanger des informations afin de ne pas sanctionner deux fois le manquement à une même obligation (art. 64, al. 5). Et une entreprise à laquelle la loi ne s'applique pas peut signaler un incident au NÚKIB de manière volontaire (art. 15, al. 5) ; la loi prévoit que l'agence ou le CERT national se prononce aussi sur un tel signalement et apporte une aide méthodologique (art. 17, al. 5).

La police, l'assureur et les partenaires commerciaux

L'attaque constitue généralement l'infraction d'accès non autorisé à un système informatique et d'atteinte à celui-ci (art. 230 du Code pénal tchèque), et la demande de rançon y ajoute l'extorsion (art. 175). Le NÚKIB recommande lui aussi de contacter la police. La plainte pénale atteste en outre que l'entreprise a été victime, et l'assureur comme les partenaires la demanderont.

Si le dommage est couvert par une assurance, déclarez le sinistre à l'assureur sans retard injustifié, fournissez des explications sincères, produisez les justificatifs et suivez la procédure convenue dans le contrat (art. 2796, al. 1, du Code civil tchèque). Ce dernier point passe facilement inaperçu. Avant de mandater un prestataire d'investigation numérique ou d'engager le moindre échange avec l'attaquant, lisez les conditions de votre police ; ce qu'elles prévoient pour la procédure après sinistre vous engage aussi. Combien de temps l'assureur peut instruire le dossier et quand vous pouvez demander une avance, c'est ce qu'explique notre guide consacré à l'instruction du sinistre et à l'avance (en tchèque).

Les partenaires commerciaux vous concernent sous deux angles. Si, à cause de l'attaque, vous ne livrez pas à temps, vous répondez du préjudice, et seul un obstacle extraordinaire, imprévisible et insurmontable vous en exonère (art. 2913, al. 2, du Code civil). Nous ne parierions pas aujourd'hui sur le fait qu'un tribunal reconnaisse une cyberattaque comme un tel obstacle : les attaques sont courantes, et l'on attend d'une entreprise qu'elle s'en pro-

tège. Passez donc vos contrats en revue pour voir ce qu'ils prévoient en matière de force majeure, de notification des incidents et de délais. Nous décrivons ce que doit contenir une bonne clause de force majeure dans l'article Cinq clauses contractuelles qui peuvent vous faire économiser des millions (et que personne ne lit). Les contrats de sous-traitance de données à caractère personnel prévoient souvent leurs propres délais de notification, tout comme les contrats que le fournisseur d'un service réglementé conclut avec ses propres fournisseurs ; pour ces derniers, la loi sur la cybersécurité impose expressément d'y inclure des exigences de sécurité (art. 13, al. 5). Écrivez à temps et de manière factuelle aux partenaires dont les données ou les systèmes ont pu être touchés, pour leur dire ce qui s'est passé et ce qu'ils doivent faire. Les hypothèses sur le coupable et les réflexions sur ce qui aurait pu être mieux fait n'ont pas leur place dans un tel courrier.

La rançon : une décision dont la direction répond

Le NÚKIB recommande de ne payer la rançon en aucun cas. Le paiement incite l'attaquant à recommencer, rien ne garantit qu'il déchiffrera ou supprimera les données, le déchiffrement n'élimine pas le code malveillant, et payer peut, d'un point de vue juridique, enfreindre le devoir de diligence d'un bon gestionnaire (*péče řádného hospodáře*). Cette dernière raison concerne personnellement le gérant ou le membre du conseil d'administration. Il doit exercer ses fonctions avec la loyauté nécessaire ainsi qu'avec les connaissances et le soin requis (art. 159, al. 1, du Code civil), et c'est à lui de prouver, en cas de litige, qu'il a agi ainsi (art. 52, al. 2, de la loi tchèque sur les sociétés commerciales). Il est protégé par la règle de l'appréciation entrepreneuriale (*business judgment rule*) : satisfait à son devoir celui qui pouvait, de bonne foi, raisonnablement considérer qu'il agissait en connaissance de cause et dans l'intérêt défendable de la société (art. 51, al. 1).

Si la direction envisage de payer, par exemple parce que l'entreprise ne survivrait pas sans ses données, la décision doit reposer sur des éléments concrets : une évaluation de la possibilité de rétablir l'activité à partir des sauvegardes et du délai nécessaire, un chiffrage des dommages, la position de l'assureur et un procès-verbal exposant les raisons de la décision prise. Pour en savoir plus sur la responsabilité du gérant, consultez notre guide sur ce dont répond le gérant (en tchèque).

Deux règles valent toujours. L'argent ne doit pas aller à des personnes et groupes inscrits sur la liste des sanctions de l'UE ; l'Union dispose d'un régime de sanctions propre aux cyberattaques (art. 3, par. 2, du règlement (UE) 2019/796 du Conseil), et la violation de sanctions internationales d'une ampleur importante est une infraction pénale (art. 410 du Code pénal). L'attaquant, bien sûr, ne se présente pas. Avant que la direction ne paie, un prestataire d'investigation numérique doit donc d'abord identifier le groupe en cause, le résultat est confronté aux listes de sanctions et consigné dans le procès-verbal de la décision. Enfin, le paiement ne change rien aux obligations de notification : la violation a déjà eu lieu, et personne ne peut vérifier la promesse de l'attaquant d'avoir supprimé les données.

Rédigez dès aujourd'hui, sur une seule page, qui décide en cas d'attaque, les numéros de téléphone de la direction, de l'administrateur informatique, de l'assureur et de l'avocat, ainsi que la marche à suivre pour notifier l'ÚOOÚ. Conservez-la hors des systèmes de l'entreprise, par exemple imprimée.

Vérifiez si votre service figure dans le décret n° 408/2025 Rec. Quiconque remplit les conditions de la loi sur la cybersécurité doit se déclarer lui-même au NÚKIB dans les 60 jours.
Vérifiez dans vos contrats avec vos prestataires informatiques et cloud dans combien d'heures ils doivent vous signaler un incident et quelles informations ils vous transmettront. Sans elles, vous ne pourrez pas rédiger la notification à l'ÚOOÚ.

En bref

Question	Réponse	Disposition
Le chiffrement de données par un rançongiciel est-il une violation de données ?	Oui, il s'agit d'une perte de disponibilité ; à notifier, sauf si le risque pour les personnes est improbable	art. 4, point 12, et art. 33, par. 1, du RGPD
Délai de notification à l'ÚOOÚ	Dans les meilleurs délais, si possible dans les 72 heures après en avoir pris connaissance ; au-delà, avec les motifs du retard	art. 33, par. 1, du RGPD
Quand informer les personnes concernées	En cas de risque élevé probable, dans les meilleurs délais	art. 34 du RGPD
Amende pour manquement aux obligations de notification	Jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires mondial	art. 83, par. 4, du RGPD
Signalement au titre de la loi sur la cybersécurité	Signalement initial dans les 24 heures ; pour un incident ayant un impact important, notification dans les 72 heures et rapport final dans les 30 jours de la notification	art. 16 de la loi n° 264/2025 Rec.
Déclaration d'un service réglementé au NÚKIB	Dans les 60 jours suivant la réunion des conditions	art. 6, al. 1, de la loi n° 264/2025 Rec.
Déclaration à l'assureur	Sans retard injustifié et selon la procédure prévue au contrat	art. 2796, al. 1, du Code civil
Rançon	Le NÚKIB la déconseille ; tout paiement à des personnes inscrites sur la liste des sanctions est interdit	art. 3, par. 2, du règlement (UE) 2019/796

Vous faites face à une attaque ou à une fuite de données en ce moment ? Nous vous aidons à décider quoi notifier et à qui, nous préparons la notification à l'ÚOOÚ, la communication aux personnes concernées ainsi que les courriers à l'assureur et aux partenaires, et nous donnons à la direction des bases solides pour des décisions qui seront examinées plus tard. Nous traitons la protection des données et la cybersécurité dans le cadre de notre pratique IT compliance. Écrivez-nous.

Conclusion

Les délais juridiques après une cyberattaque courent indépendamment du moment où les systèmes redémarrent : 72 heures pour l'ÚOOÚ, 24 heures pour le NÚKIB ou le CERT national s'agissant des services réglementés, et sans retard injustifié pour l'assureur. Une entreprise qui préserve les traces dès les premières heures, tient un journal et notifie à temps, même avec des informations incomplètes, aura ensuite de quoi se défendre devant l'autorité, l'assureur et le juge.

Une entreprise qui sait à l'avance si elle relève de la loi sur la cybersécurité et ce que ses prestataires lui promettent dans leurs contrats n'aura pas à le découvrir en pleine attaque.

Sources

- Règlement (UE) 2016/679 du Parlement européen et du Conseil, règlement général sur la protection des données, article 4, point 12, article 28, paragraphe 3, point f), articles 33, 34 et 82 et article 83, paragraphe 4.
- Loi n° 264/2025 Rec. relative à la cybersécurité, art. 4 à 8, 13, 15, 16, 17, 59 et 64 (version en vigueur depuis le 1er novembre 2025).
- Décret n° 408/2025 Rec. relatif aux services réglementés.
- Loi n° 89/2012 Rec., Code civil, art. 159, 2796 et 2913.
- Loi n° 90/2012 Rec. relative aux sociétés commerciales, art. 51 et 52.
- Loi n° 40/2009 Rec., Code pénal, art. 175, 230 et 410.
- Règlement (UE) 2019/796 du Conseil concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres, article 3.
- Arrêt de la Cour de justice de l'UE du 14 décembre 2023, Natsionalna agentsia za prihodite, affaire C-340/21.
- Comité européen de la protection des données, Lignes directrices 9/2022 sur la notification de violations de données à caractère personnel en vertu du RGPD, version 2.0, et Lignes directrices 01/2021 sur des exemples concernant la notification de violations de données à caractère personnel, version 2.0, cas n° 01 et 02.
- NÚKIB, Rançongiciels : recommandations pour l'atténuation, la prévention et la réaction, version 1.2 du 22 mai 2023, section 4.
- Office pour la protection des données personnelles, Violation de la sécurité des données à caractère personnel (uoou.gov.cz).

Cet article a un caractère informatif et ne constitue pas un conseil juridique. Il repose sur l'état du droit à la date de publication ; la question de savoir si un incident donné doit être notifié, et à qui, dépend des données et des services qu'il a touchés et du fait que l'entreprise relève ou non de la loi sur la cybersécurité.

Cyberattaque ou fuite de données dans l'entreprise : que faire dans les 72 premières heures

L'équipe IUSTORIA · Publié 5/11/2026

https://www.iustoria.cz/fr/blog/cyberattaque-ou-fuite-de-donnees-les-72-premieres-heures/

Ce texte est protégé par le droit d'auteur. Le partage du document entier et non modifié est bienvenu ; la reprise d'extraits dans d'autres textes suppose la citation de la source. © IUSTORIA, advokátní kancelář, s.r.o.