Avec le soutien / при поддержке:

20 ans rem CCI FRANCE RUSSIE
CHAMBRE DE COMMERCE ET D'INDUSTRIE FRANCO-RUSSE
ФРАНКО-РОССИЙСКАЯ ТОРГОВО-ПРОМЫШЛЕННАЯ ПАЛАТА

15 ans Le Courrier de Russie
www.lecourrierderussie.com
GROUPE NOVYI VEK MEDIA

Экономические отношения между Россией и Францией

L'économika

№11 (321), 2017

LES RELATIONS ÉCONOMIQUES ENTRE LA RUSSIE ET LA FRANCE

UN TIERS DES SOCIÉTÉS RUSSES IMPUISSANTES FACE AUX ATTAQUES DDOS

31 % des entreprises russes ne savent pas comment se défendre contre les attaques DDoS, et 15 % ne bénéficient d'aucune protection contre cette menace, révèle une étude conjointe de Kaspersky Lab et B2B International.

Selon Kaspersky Lab, 62 % des sociétés comptent sur des moyens de protection intégrés, inutiles en cas d'attaques d'envergure et complexes. Dans seulement 21 % des sociétés, les experts IT ont pleinement conscience de cette menace potentielle.

LA CYBERCRIMINALITÉ FAIT PERDRE 450 MILLIARDS DE DOLLARS À L'ÉCONOMIE MONDIALE

Selon une étude menée par la société d'assurances britannique Hiscox auprès de plus de 3 000 entreprises américaines, allemandes et britanniques, en 2016, les cybercrimes ont coûté 450 milliards de dollars et plus de 2 milliards de données personnelles ont été volées dans le monde. Le montant moyen des dommages s'est élevé à près de 22 000 € pour les petites entreprises allemandes et jusqu'à 100 000 $ pour les grandes sociétés américaines.

DIX ANS DE PRISON POUR LES HACKERS

Fin janvier, la Douma d'État a approuvé en première lecture une série de projets de loi prévoyant le durcissement de la responsabilité pénale pour des cyberattaques visant des infrastructures d'information critiques (IIC). Les peines envisagées sont une privation de liberté de 5 à 10 ans ou une amende pouvant atteindre les 2 millions de roubles.

Selon un de ces projets de loi, les ICC désignent les systèmes d'information et les réseaux d'information et de télécommunication des organes étatiques ainsi que les systèmes automatisés de gestion des procédés techniques dans les domaines suivants : défense, santé, transport, télécommunications, finance et crédit, énergie, nucléaire, aérospatiale, métallurgie, industries chimique et minière.

CHASSE AUX DONNÉES PERSONNELLES : COMMENT NE PAS DEVENIR UNE PROIE

BIEN QUE LA SÉCURITÉ DES DONNÉES PERSONNELLES DES CITOYENS RUSSES SOIT RÉGIE PAR LA LÉGISLATION FÉDÉRALE, LE VOLUME DES INFORMATIONS VENDUES SUR LE MARCHÉ NOIR EN RUSSIE REPRÉSENTE 30 MILLIONS DE ROUBLES ET UN RUSSE SUR DIX EST UN JOUR VICTIME DE HACKERS. TELS SONT LES RÉSULTATS DE L'ÉTUDE « LE MARCHÉ NOIR DES BASES DE DONNÉES », MENÉE PAR LE CENTRE ANALYTIQUE MFI SOFT EN NOVEMBRE 2016. DANS CES CONDITIONS, COMMENT PROTÉGER LES DONNÉES PERSONNELLES DES CLIENTS ET DES EMPLOYÉS D'UNE ENTREPRISE ?

PIERRES D'ACHOPPEMENT

Actuellement, il n'existe aucune définition précise du concept de « données personnelles ». Celles-ci englobent toute information relative à une personne physique : nom et prénom, date de naissance, adresse, situation familiale et sociale, éducation, montant des revenus, etc. Les experts distinguent habituellement trois catégories de données personnelles : accessibles à tous, biométriques et spéciales. Alors que les premières sont faciles à obtenir depuis des sources ouvertes telles que les réseaux sociaux, les deuxièmes permettent d'établir l'identité d'une personne sur la base de ses particularités biologiques et physiologiques : taille, poids, empreintes digitales, groupe sanguin, résultats d'analyses médicales, etc. Les données spéciales, enfin, désignent les informations relatives à l'origine ethnique, la nationalité, les convictions religieuses et politiques, la vie intime et l'état de santé.

L'homme moderne distribue généreusement ses données personnelles : lors de l'achat d'un billet d'avion sur Internet, en s'abonnant à une liste de diffusion ou en s'inscrivant à un événement, par exemple. Ce flux d'informations devient de plus en plus difficile à contrôler. Pour pouvoir le gérer, les entreprises peuvent introduire des services spécifiques et des systèmes de GRC (gestion de la relation client). Mais, en raison de failles de sécurité, ces volumes importants de données se retrouvent souvent aux mains de malfaiteurs, l'ampleur d'un cybercrime pouvant aller d'un simple spam inoffensif au vol de montants considérables.

Voilà pourquoi il vaut mieux éviter de laisser ses données personnelles sur des sites internet librement accessibles ou suspects : un questionnaire ou un jeu en apparence anodins peuvent être des pièges tendus par des cybercriminels. Il convient également de veiller à utiliser des mots de passe sécurisés lors de la création d'un compte sur un réseau social ou un service de messagerie. Il est en outre déconseillé d'enregistrer son nom et ses coordonnées (notamment bancaires) sur son navigateur.

À l'instar des personnes physiques, les entreprises sont également régulièrement la cible des hackers. Seulement, pour elles, les répercussions sont plus lourdes : le vol des données personnelles des employés est synonyme d'une intrusion dans l'ensemble du système. Les bases de données clients, quant à elles, se vendent en moyenne 15 000 roubles pièce sur le marché noir. L'une et l'autre conséquences nuisent à la réputation et à l'activité commerciale de l'entreprise.

Il faut éviter de laisser ses données personnelles sur des sites libres à tous ou suspects : un questionnaire ou un jeu en apparence anodins peuvent être des pièges.

NORMES LÉGISLATIVES

Thème on ne peut plus actuel, la sécurité des données personnelles est réglementée au niveau de l'État. En Russie, ces données sont, à l'instar de la vie privée, protégées par la Constitution, les Codes civil et du travail, la loi fédérale n°149-FZ du 27 juillet 2006 « Sur l'information, les technologies de l'information et la protection de l'information » et la loi fédérale n°152-FZ du 27 juillet 2006 « Sur les données personnelles ». Toutefois, au cours des deux dernières années, de nouvelles

SANCTIONS POUR VIOLATION DE LA LOI SUR LA COLLECTE, LE TRAITEMENT ET LA CONSERVATION DES DONNÉES PERSONNELLES

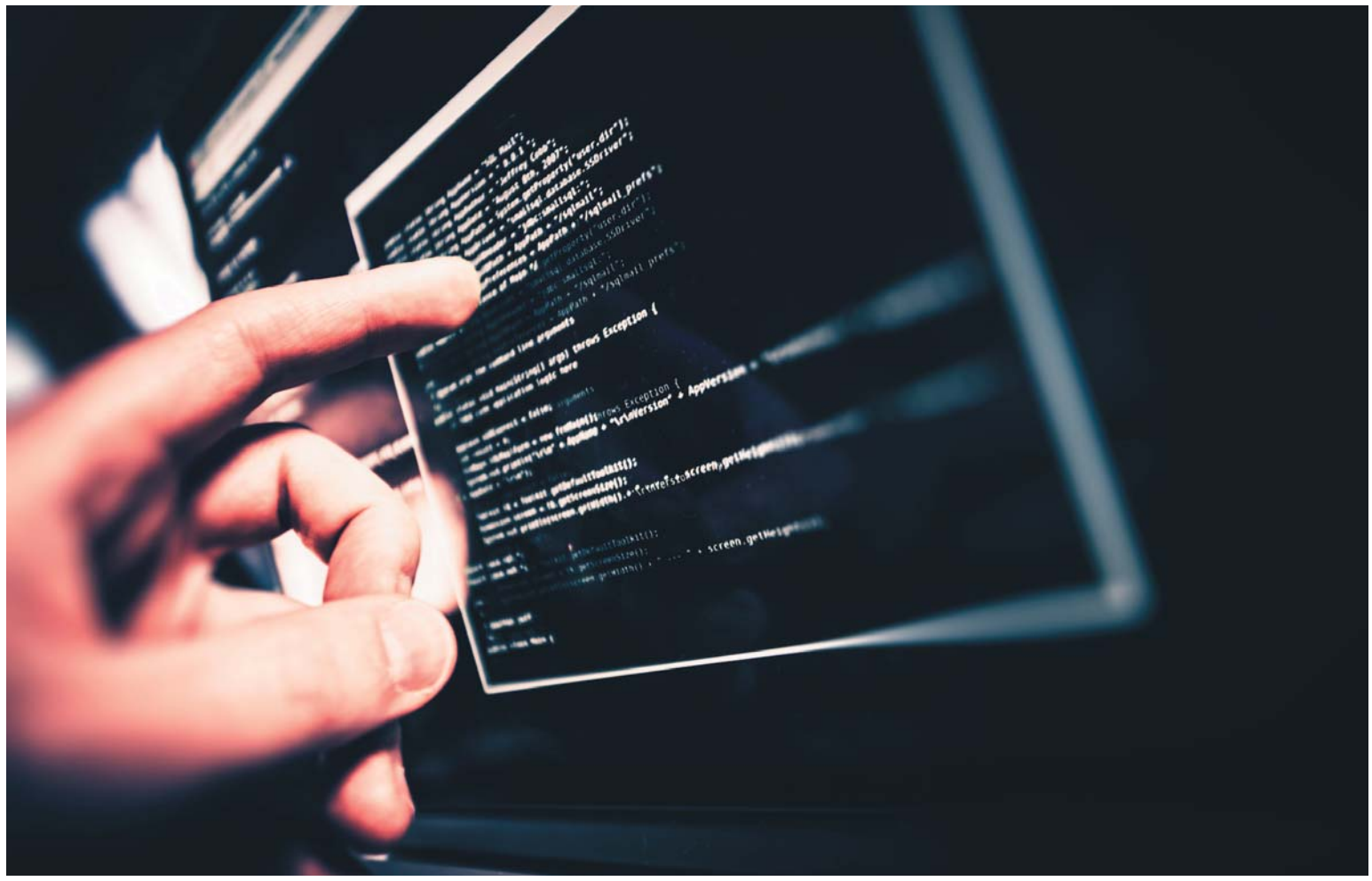
VIOLATION	AMENDE POUR LA PERSONNE PHYSIQUE	AMENDE POUR LA PERSONNE MORALE	AMENDE POUR LES FONCTIONNAIRES
TRAITEMENT DE DONNÉES PERSONNELLES DANS DES CAS NON PRÉVUS PAR LA LOI RUSSE OU TRAITEMENT DE DONNÉES INCOMPATIBLE AVEC LES OBJECTIFS DE LA COLLECTE DE CES DONNÉES	AVERTISSEMENT OU AMENDE DE 1 000 À 3 000 ROUBLES	DE 30 000 À 50 000 ROUBLES	DE 5 000 À 10 000 ROUBLES
TRAITEMENT DE DONNÉES PERSONNELLES SANS LE CONSENTEMENT DU CITOYEN CONCERNÉ	DE 3 000 À 5 000 ROUBLES	DE 15 000 À 75 000 ROUBLES	DE 10 000 À 20 000 ROUBLES
REFUS DE FOURNIR AU CITOYEN DES INFORMATIONS SUR LE TRAITEMENT DE SES DONNÉES PERSONNELLES	AVERTISSEMENT OU AMENDE DE 1 000 À 2 000 ROUBLES	DE 10 000 À 15 000 ROUBLES POUR UNE ENTREPRISE INDIVIDUELLE ET DE 20 000 À 40 000 ROUBLES POUR UNE PERSONNE MORALE	DE 4 000 À 6 000 ROUBLES

mesures législatives sont devenues nécessaires pour protéger les données personnelles des internautes. Ainsi, le 1er septembre 2015, une disposition prévue par la loi n°242-FZ a pris effet, qui contraint toutes les personnes physiques ou morales gérant des données personnelles à traiter et conserver celles des citoyens russes uniquement sur le territoire de la Fédération de Russie.

Néanmoins, presque tout un chacun est concerné par ces exigences sécuritaires. Les systèmes de données personnelles incluent non seulement les bases des boutiques et des services en ligne mais également les systèmes comptables et de gestion des ressources humaines, les centres d'appel et même les systèmes automatisés des bureaux des laissez-passer, présents dans quasiment toutes les entreprises. Si un contrôle effectué par Roskomnadzor, l'agence fédérale chargée de la surveillance des moyens de communication, fait apparaître des violations, la responsabilité de l'entreprise et de ses dirigeants est engagée en vertu des articles «Violation des modalités prévues par la loi relatives à la collecte, la conservation, l'utilisation et la diffusion d'informations sur les citoyens (données personnelles)», «Violation des règles de protection de l'information» et «Activité illégale dans le domaine de la protection de l'information».

Le débat sur la protection des données personnelles a été relancé en été 2016, lorsque le président Vladimir Poutine a signé une série d'amendements législatifs antiterroristes, surnommés par les médias «paquet Iarovaïa», du nom de famille de l'auteur du document. Conformément à la nouvelle législation, les opérateurs de télécommunications doivent conserver tous les enregistrements des appels et des messages échangés entre les utilisateurs pendant six mois, et les informations sur les communications pendant trois ans.

En outre, début 2017, la Douma d'État a augmenté le montant de l'amende pour violation de la loi n°152-FZ sur la collecte, le traitement et la conservation des données personnelles. Selon les amendements adoptés, trois jours sont désormais impartis à l'élimination des violations. Tout manquement est passible de sanctions : amendes pouvant atteindre les 300 000 roubles, confiscation des moyens de protection non certifiés ou sommation de cesser le traitement des données personnelles. Dans tous les cas, l'entreprise s'expose à des frais considérables.



Selon Alexeï Ponomarev, juriste au collège d'avocats Novy Arbat, l'adoption de la loi n°152-FZ sur la conservation et le traitement des données personnelles et le durcissement de la responsabilité pour non-respect de celle-ci sont des mesures nécessaires. «Il s'agit bien entendu des maillons d'une seule chaîne : le renforcement du contrôle sur Internet. Mais l'anarchie qui régnait sur l'Internet russe devait un jour s'achever. Pour la sphère IT, cela signifie des dépenses supplémentaires mais aussi une entrée sur le marché plus coûteuse pour les nouvelles entreprises. Néanmoins, dans la majorité des pays, ces lois ont été adoptées il y a longtemps et sont considérées comme la norme», commente le spécialiste.

Maxime Lagoutine, fondateur et expert en protection des données personnelles de l'entreprise B-152, qui aide les sociétés à remplir les documents juridiques relatifs aux données personnelles, estime pour sa part que la législation russe a ses spécificités en matière de protection des données personnelles. «À l'étranger, on inflige des amendes pour une fuite d'informations, tandis qu'en Russie on punit l'absence de consentement des personnes physiques pour le traitement de leurs données, la non-adéquation entre ce consentement et les objectifs poursuivis, autrement dit l'absence de documents et non le respect des droits de la personne», explique l'expert.

À l'en croire, alors qu'auparavant certaines entreprises faisaient fi de la loi car il était plus simple pour elles de payer une amende que de se conformer aux exigences, le durcissement récent des sanctions oblige les personnes morales à se montrer plus responsables. «Respecter la loi n'exige pas de grands investissements, c'est avant tout une question de coordination et de discipline. J'espère qu'avec le temps toutes les entreprises disposeront d'une procédure d'autorégulation ou qu'elles introduiront un système d'audit régulier dans ce domaine», ajoute le fondateur de B-152.

DES MOYENS DE PROTECTION MODERNES

Toutefois, assurer la sécurité des données personnelles comme l'exige la loi n'est pas aussi simple : on peut rapidement se perdre face à la multitude de moyens de protection et de documents nécessaires.

«Dans ce domaine, la législation russe n'est pas encore complètement au point. Par exemple, des données personnelles communiquées séparément cessent d'être personnelles : un numéro de téléphone donné seul n'est qu'un ensemble de chiffres, tandis qu'un numéro de téléphone accompagné d'un nom et d'un prénom constitue une donnée personnelle. Une page sur un réseau social n'est pas une donnée personnelle mais si un numéro de téléphone y est indiqué, elle se retrouve immédiatement sous le coup de la loi, même s'il s'agit d'un faux compte. Par ailleurs, les données personnelles ne peuvent pas être conservées à l'étranger, mais leur sauvegarde oui», précise Ilia Iachine, fondateur du systémier Jack-IT.

En outre, les cybercriminels s'efforcent toujours d'avoir une longueur d'avance sur les systèmes de sécurité. Par conséquent, les méthodes de protection formelles – du transfert des informations sur un serveur russe à l'installation d'un antivirus – peuvent ne pas fonctionner. La protection des données personnelles exige donc une approche intégrée : à la fois technique et organisationnelle.

S'il n'existe pas de méthode de protection universelle, certaines technologies permettent néanmoins de protéger les informations de n'importe quelle entreprise. Par exemple, l'identification biométrique. Le principe est simple : l'accès aux infrastructures se fait par lecture des empreintes digitales, scan de la rétine ou reconnaissance vocale. L'essentiel est que le système ne conserve pas ces données biométriques mais les crypte. Ces technologies fonctionnent aussi bien quand il est nécessaire de limiter l'accès des employés aux bureaux, aux ordinateurs et à certains fichiers que quand l'utilisateur se connecte à son compte personnel via une application mobile – après le scan de son empreinte digitale.

Un autre moyen de protection est la migration de toutes les informations vers le *cloud*. L'accès aux données se fait alors uniquement via des canaux sécurisés et chaque employé possède sa propre clé d'accès. En outre, les faits et gestes de tous les employés peuvent être contrôlés en temps réel : qui fait quoi à quel moment, qui a quitté son ordinateur, qui télécharge des fichiers suspects, etc. De plus, rien n'est conservé sur les ordinateurs, de sorte que même si des malfaiteurs volent du matériel, ils n'en extrairont aucune donnée.

Pour sécuriser les boutiques en ligne et les sites, il est possible de recourir à des services qui contrôlent le trafic, préviennent les attaques DDoS, prévoient d'éventuelles intrusions et signalent les activités suspectes. Un programme spécial fournit des informations sur le nombre de visites et d'utilisateurs uniques, la durée moyenne passée sur une page, etc. Si ces indicateurs s'éloignent subitement de la norme ou si quelqu'un se met à adopter un comportement suspect sur le site, le programme envoie immédiatement un message d'avertissement au propriétaire du site.

«Grâce à l'historique de comportement des utilisateurs, nous prédisons les valeurs attendues. Si notre pronostic ne coïncide pas avec la valeur réelle, l'utilisateur du programme en reçoit aussitôt la notification», explique Pavel Tiounov, cofondateur de l'entreprise Statsbot.

Toutefois, malgré l'existence de technologies permettant de déjouer les ruses des cybercriminels, aucun code ne peut prémunir contre le facteur humain. Selon une étude menée par l'entreprise MFI Soft, conceptrice de systèmes de sécurité de l'information, les bases de données peuvent se retrouver sur le marché noir de quatre façons différentes. Sachant que l'obtention de données personnelles à la suite d'une intrusion (2%) ou à partir de sources non sécurisées (7%) n'est pas la plus fréquente. Les principaux responsables de fuites de données restent en effet les employés peu scrupuleux : les sources internes malintentionnées sont à l'origine de 78% des fuites, tandis que les 13% restants proviennent de la diffusion ciblée des données clients à des fins commerciales.

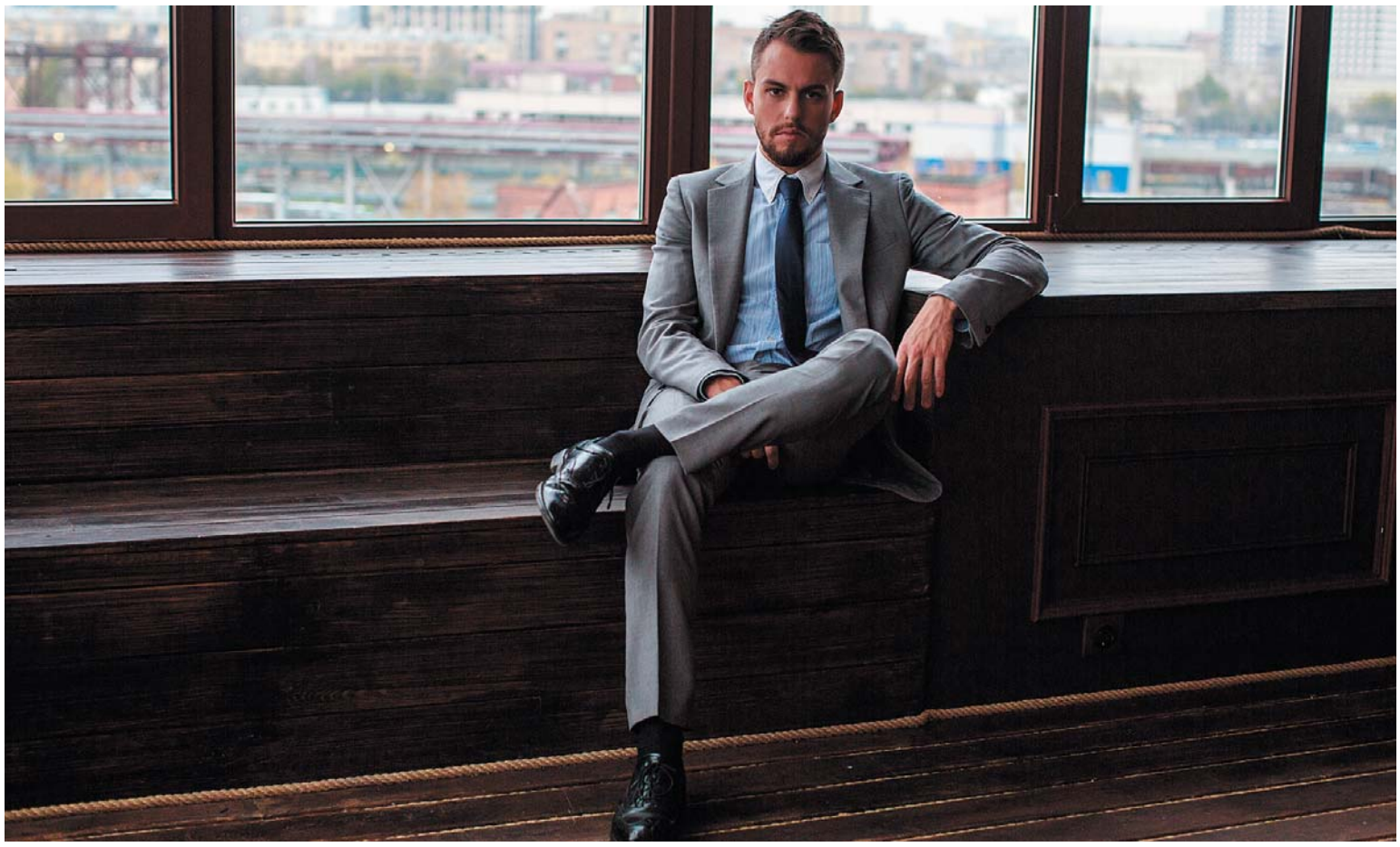
ILMIRA GAÏSSINA
Traduit par MAÏLIS DESTRÉE

« À l'étranger, on inflige des amendes pour une fuite d'informations, tandis qu'en Russie on punit l'absence de consentement des personnes pour le traitement de leurs données, la non-adéquation entre ce consentement et les objectifs poursuivis, autrement dit l'absence de documents et non le respect des droits de la personne »

AIDE-MÉMOIRE POUR LES DIRIGEANTS D'ENTREPRISE

ÉTAPES À SUIVRE POUR RESPECTER LA LÉGISLATION EN MATIÈRE DE TRAITEMENT DES DONNÉES PERSONNELLES :

- INFORMER L'ORGANE DE CONTRÔLE ROSKOMNADZOR DU TRAITEMENT DE DONNÉES PERSONNELLES ;
- RECEVOIR LE CONSENTEMENT DE CHAQUE PERSONNE CONCERNÉE (EMPLOYÉ OU CLIENT) POUR LE TRAITEMENT DE SES DONNÉES PERSONNELLES (CE CONSENTEMENT DOIT CONTENIR LA SIGNATURE MANUSCRITE OU NUMÉRIQUE DE LA PERSONNE) ;
- DÉCRIRE DE FAÇON DOCUMENTÉE LES SYSTÈMES DE TRAITEMENT DES DONNÉES PERSONNELLES (AFFECTATION, CONTENU DES DONNÉES, FONDEMENTS JURIDIQUES DE LEUR TRAITEMENT) ET IDENTIFIER LE GROUPE DE PERSONNES TRAITANT LES DONNÉES PERSONNELLES ET Y AYANT ACCÈS ;
- RÉDIGER UNE SÉRIE DE DOCUMENTS NORMATIFS DÉCRIVANT LES MODÈLES DE MENACES À LA SÉCURITÉ DES DONNÉES PERSONNELLES ET LES MOYENS DE S'EN PROTÉGER ;
- GARANTIR LA SÉCURITÉ DES DONNÉES PERSONNELLES À L'AIDE DE MÉTHODES TECHNIQUES (PROGRAMMES, APPAREILS) ET ORGANISATIONNELLES ;
- SE SOUMETTRE AU CONTRÔLE DE ROSKOMNADZOR EN VUE D'ATTESTER LA CONFORMITÉ DES SYSTÈMES DE PROTECTION DES DONNÉES PERSONNELLES AUX EXIGENCES LÉGISLATIVES.



« LA MAJORITÉ DES CYBERATTAQUES VISENT DES ENTREPRISES »

EN 2016, LE NOMBRE DE CYBERATTAQUES VISANT DES SOCIÉTÉS RUSSES A TRIPLÉ. CHACUNE DE CES ATTAQUES COÛTE EN MOYENNE SIX MILLIONS DE ROUBLES POUR UNE PETITE OU MOYENNE ENTREPRISE ET ONZE MILLIONS POUR UNE GRANDE ENTREPRISE. *L'ÉCONOMIKA* S'EST ENTRETENUE DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ AVEC ILIA SATCHKOV, DIRECTEUR GÉNÉRAL DE GROUP-IB, UNE DES PLUS GRANDES SOCIÉTÉS PRIVÉES SPÉCIALISÉES DANS LA SÉCURITÉ DES SYSTÈMES D'INFORMATION.

– Quelles sont les entreprises les plus exposées aux cyberattaques ?

– La cybercriminalité étant liée à 99 % à la volonté des malfaiteurs de recevoir de l'argent, toute entreprise fait partie du groupe à risque. Selon notre étude annuelle, en 2016, les cybercriminels russes ont obtenu la majorité de leur argent à la suite d'attaques ciblées visant des organismes financiers.

Bien entendu, les particuliers sont également souvent la cible des hackers. Depuis quelque temps, les virus codeurs gagnent en popularité. L'intérêt de ceux-ci pour les criminels est qu'en cryptant les fichiers précieux présents sur l'ordinateur infecté, il leur permet de voler des données bancaires et d'extorquer de l'argent en échange de la clé de décryptage.

En outre, les malfaiteurs utilisent parfois des marques célèbres dans leur propre intérêt. Ils créent des montages frauduleux, de faux concours ou loteries grâce auxquels ils soutirent les données personnelles (bancaires, par exemple) des participants à la vente d'articles contrefaits présentés comme des originaux.

Les sites extrêmement sensibles que sont par exemple les centrales nucléaires ou électriques n'intéressent pas les cybercriminels classiques car les attaquer ne rapporte pas d'argent et a une résonance sociale. Qui plus est, il est très probable que les responsables soient poursuivis en justice. C'est la raison pour laquelle la majorité des hackers se concentrent sur les entreprises et les particuliers.

– De quelles ruses les hackers usent-ils ?

– La réussite d'un cybercrime dépend de deux facteurs. Le premier est lié aux technologies : des programmes malveillants complexes et non détectables par les antivirus et une connaissance des points vulnérables des logiciels. Le second est l'ingénierie sociale, soit la connaissance des différents aspects de la psychologie humaine.

Voici un exemple simple d'ingénierie sociale que nous avons rencontré : un employé de banque reçoit un e-mail d'un client qui lui a téléphoné plus tôt pour ouvrir un compte au sein de cette banque. L'e-mail provient du domaine de l'entreprise mentionnée par le client avec une signature et une pièce jointe au format .doc. Naturellement, l'employé de banque, qui attendait cet e-mail, ouvre la pièce jointe sans réfléchir – et permet ainsi au malfaiteur d'avoir accès au réseau de la banque.

Les hackers ont également souvent recours à l'envoi d'e-mails malveillants contenant des phrases du genre : « Votre boîte de réception va bientôt être bloquée, prouvez que vous n'êtes pas un robot », « Un spam a été envoyé depuis votre adresse e-mail », « Recevez gratuitement 20 Go d'espace supplémentaire », etc. Les principaux défauts de l'être humain sont la peur et la curiosité : elles l'obligent à agir rapidement, ce qui fait le jeu des cybercriminels.

– Comment réduire les risques lors de la conservation et du transfert d'informations ?

– Pour pouvoir diminuer les risques, il faut les connaître. La majorité des incidents impliquent des personnes ou des entreprises qui soit ne connaissent rien à la sécurité de l'information, soit évaluent mal les risques.

Voilà pourquoi estimer correctement les risques encourus par votre entreprise constitue le fondement de sa sécurité. Il est conseillé de chercher des informations sur les affaires pénales concernant des cybercrimes dans votre domaine d'activité et de lire des articles populaires au sujet de la sécurité de l'information. Vous disposerez ainsi d'une base de connaissances dont dépendra 99 % de la sécurité de votre entreprise. Bien entendu, il faut également respecter une hygiène informatique élémentaire : ne pas ouvrir des liens et des documents envoyés par des inconnus, mettre régulièrement à jour son ordinateur, utiliser des mots de passe compliqués et une validation en deux étapes – lors de celle-ci, des informations de deux types vous sont demandées : un identifiant et un mot de passe en premier lieu, et ensuite un code unique envoyé sur votre téléphone ou votre boîte de réception.

– Pourquoi les antivirus sont-ils impuissants ?

– Aujourd'hui, les groupes criminels organisés disposent de budgets et de technologies tels qu'ils sont capables de rivaliser avec les antivirus installés sur les appareils des victimes. Dans 86 % des cas que nous avons étudiés, un antivirus était présent sur les ordinateurs infectés.

Tous les cybercriminels qui envoient un nouveau type de virus au combat le testent toujours sur toutes les bases de données virales et dans des environnements spéciaux pour s'assurer de son indétectabilité.

Pour protéger son ordinateur, un antivirus est nécessaire – mais insuffisant depuis environ cinq ans. Si l'on souhaite augmenter son niveau de sécurité, il faut également utiliser des outils de détection d'intrusion sur le réseau et des instruments de protection contre les attaques ciblées.

EN 2015, LES HACKERS ONT FAIT PERDRE
203
MILLIARDS DE ROUBLES
À L'ÉCONOMIE RUSSE, SOIT 0,25 % DU PIB DU PAYS OU LA MOITIÉ DU BUDGET ALLOUÉ AU DÉVELOPPEMENT DE LA SANTÉ PUBLIQUE.

PARMI CES 203 MILLIARDS, LES PERTES ESSUYÉES PAR LES ENTREPRISES REPRÉSENTENT
123
MILLIARDS
ET LES DÉPENSES ENGAGÉES POUR ÉLIMINER LES CONSÉQUENCES DES CYBERCRIMES 80 MILLIARDS.

SUR 600 ENTREPRISES RUSSES,
92 %
ONT ÉTÉ VICTIMES DE CYBERATTAQUES. CES TROIS DERNIÈRES ANNÉES, LE NOMBRE D'ATTAQUES A AUGMENTÉ DE 75 % ET LES PERTES FINANCIÈRES OCCASIONNÉES ONT DOUBLÉ.

EN RUSSIE,
PLUS DE 1 000
ATTAQUES DDOS
SONT PERPÉTRÉES CHAQUE JOUR.

SOURCES : IIDF, MICROSOFT ET GROUP-IB

– Parlez-nous des principales tendances en matière de sécurité des systèmes d'information. Quels sont les nouveaux moyens de répression des cybercrimes ?

– Aujourd'hui, plusieurs types de technologies existent pour prévenir les cyberattaques.

Premièrement, le cyberespionnage, qui vise à analyser de grands volumes de données en utilisant des pièges et des systèmes de surveillance variés afin de découvrir les indices révélateurs de la préparation d'un crime et ainsi prévoir les agissements du hacker. Sur Internet, il est impossible de passer inaperçu. Les malfaiteurs s'efforcent bien entendu de ne pas laisser de traces mais même une information minime suffit à anticiper une attaque.

La deuxième catégorie de technologies relève de l'analyse comportementale. Celles-ci sont par exemple utilisées pour contrôler les pièces jointes électroniques. Le programme ouvre le fichier reçu au format .pdf ou .doc dans divers environnements virtuels et vérifie s'il est malveillant ou non.

On assiste aussi à l'apparition de technologies d'authentification biométrique des utilisateurs. Pratiques, elles ne sont pas pour autant dénuées de risques. En effet, lorsqu'un internaute est victime d'une intrusion sur son compte d'utilisateur, il change simplement de mot de passe, tandis qu'en cas de vol de données biométriques, c'est, au fond, son identité qu'il perd.

En ce qui concerne la répression des cybercrimes, cela fait déjà longtemps qu'avec nos collègues internationaux nous répétons qu'aujourd'hui, lutter contre les cybercriminels en utilisant uniquement les technologies est inutile et nous fera probablement perdre la course aux armements. Ce combat doit allier le recours aux technologies à l'action en justice. En effet, le principal instrument de répression des cybercrimes reste la poursuite pénale des malfaiteurs.

– Comment évaluer la sécurité des systèmes d'information d'une entreprise ?

– En créant un service de sécurité informatique. Dans le cas contraire, il faut faire appel à des sociétés spécialisées dans l'audit de la sécurité des systèmes d'information extérieure et intérieure de l'entreprise.

En qualité de test, on peut simuler une attaque pour vérifier la configuration des équipements d'interconnexion du réseau et évaluer le degré de préparation des employés, y compris à l'aide de l'ingénierie sociale. L'analyse de la sécurité est un service relativement populaire qui doit être effectué au moins une fois par trimestre.

– Que faire si une menace est détectée ?

– En cas de menace, l'essentiel est de ne pas laisser les choses suivre leur cours. Il est important d'avoir à l'esprit que vous êtes la cible d'un groupe criminel organisé dont l'objectif est de vous voler de l'argent et des informations ou bien de saboter votre travail.

Je conseillerais avant tout de porter plainte à la police car tout crime doit être poursuivi. Ensuite, de faire appel au service de sécurité interne ou à des criminalistes pour localiser l'incident. Si un virus est détecté au sein de l'entreprise, il ne suffit pas simplement de le supprimer mais il faut également comprendre comment il s'est retrouvé dans le système, étudier son fonctionnement, découvrir où il a transmis des données et à quel groupe criminel il est lié, et savoir s'il s'agit d'une attaque ciblée ou aléatoire.

Les moyennes et grandes entreprises doivent mettre en place un système efficace de réaction aux incidents relatifs à la sécurité des systèmes d'information en s'appuyant sur les normes internationales et en recourant à des spécialistes en la matière.

ILMIRA GAÏSSINA
Traduit par MAÏLIS DESTRÉE

publi-reportage

LES PME DANS LE CYBERESPACE

LE CYBERESPACE EST UN MONDE VIRTUEL OÙ DES INFORMATIONS SONT ÉCHANGÉES PAR L'INTERMÉDIAIRE DE RÉSEAUX INFORMATIQUES. INTERNET EN EST UN EXEMPLE. SI Y TRAVAILLER COMPORTE DES RISQUES POUR LES ENTREPRISES, LE RESPECT DE CERTAINES RÈGLES DE CYBERSÉCURITÉ PERMET TOUTEFOIS DE LES ÉVITER.

POURQUOI A-T-ON BESOIN DU CYBERESPACE ?

Le recours au cyberespace permet de simplifier les interactions avec les partenaires et les clients ainsi que d'augmenter la productivité de certaines opérations. Bon nombre d'entreprises n'existeraient tout simplement pas sans lui. Il s'agit par exemple des banques, des sociétés financières et d'autres grands groupes.

Le cyberespace est également important pour les petites et moyennes entreprises dans la mesure où l'échange de données à l'aide des technologies de l'information (IT) leur permet de se développer et de dégager des bénéfices. Grâce à l'introduction constante d'innovations, l'IT apporte des avantages concurrentiels à une entreprise. Par exemple, on développe aujourd'hui activement l'échange de données informatisé (EDI), qui garantit un échange rapide et fiable d'informations entre des partenaires. Le recours à l'EDI permet ainsi de :

– recevoir, traiter et envoyer rapidement une commande dans un magasin ou dans un centre de distribution ;

– réduire au minimum l'échange de documents papier ;

– réduire au minimum le nombre d'erreurs lors de l'échange d'informations ;

– contrôler la qualité et les délais d'exécution d'une commande – aussi bien du côté du magasin que du fournisseur ;

– respecter les exigences du fournisseur / du réseau de magasins à propos de l'échange électronique.

LES RISQUES DU CYBERESPACE

Pour autant, le cyberespace n'est pas uniquement une source d'avantages. Il comporte également une multitude de menaces, parfois ignorées car situées hors du champ d'examen des risques habituellement encourus par l'entreprise. Dans le monde entier, on lutte depuis longtemps contre les causes et les conséquences de la concrétisation des cybermenaces et, à cette fin, différentes normes et approches sont élaborées et mises à jour. Par exemple : la norme ISO/IEC 27032:2012 Technologies de l'information – Techniques de sécurité – Lignes directrices pour la cybersécurité[1], qui inclut une liste de cyber-risques tels qu'une intrusion dans les systèmes d'information, les attaques contre les ressources informatiques de l'entreprise, et l'utilisation de logiciels espions.

LES SOURCES DES CYBERATTAQUES

Grâce au développement considérable de l'infrastructure IT et à la diversité des méthodes utilisées pour perpétrer une cyberattaque, l'instigateur de celle-ci peut se trouver à n'importe quel endroit du monde. L'attaque est souvent lancée indirectement via des employés de l'entreprise ou d'autres participants à l'échange électronique, parfois sans que ceux-ci ne se doutent de leur implication. Ces sources peuvent aussi bien être un seul individu qu'une équipe entière répartie dans le cyberespace.

EXEMPLES DE CONSÉQUENCES DE CYBERATTAQUES

Tandis que les cyberattaques visant de grandes entreprises sont régulièrement relayées par les médias, celles ciblant des PME sont pratiquement passées sous silence. Cette situation est due, premièrement, au fait que, souvent, les entreprises ne remarquent pas ces attaques et leurs répercussions et, deuxièmement, qu'elles ne veulent pas les ébruiter afin de préserver leur réputation. Les conséquences d'une cyberattaque peuvent être imperceptibles à court terme (il peut s'agir, par exemple, d'une fuite d'informations à destination de concurrents ou de l'installation d'un logiciel espion sur les ordinateurs de l'entreprise) ou manifestes (blocage du système de réception des commandes sur la boutique en ligne de l'entreprise ou exécution non autorisée de paiements).

À QUOI LA CYBERSÉCURITÉ SERT-ELLE ?

Du fait de l'objectif spécifique de certaines attaques, par exemple voler les données d'une entreprise précise via un virus intégré à un e-mail, les antivirus ne détectent pas toujours le programme malveillant, ce qui permet à ce dernier de remplir sa fonction. Ainsi, pour identifier et contrer les cybermenaces, des méthodes inhabituelles et un système efficace de cybersécurité sont nécessaires.

MOYENS DE LUTTE CONTRE LES CYBERATTAQUES

Les cyberattaques changeant sans cesse de forme, les entreprises ne sont pas toujours en mesure de les repousser seules. Des systèmes de monitoring, des antivirus ainsi que des services IT internes et externes peuvent les y aider. Depuis quelque temps, l'État crée et développe également des services de lutte contre la cybercriminalité.

Le principe fondamental de la lutte contre les cybermenaces consiste à identifier celles-ci, à introduire des procédures les atténuant, à suivre constamment les innovations IT et les méthodes utilisées pour lancer des cyberattaques, et à sensibiliser le personnel. Grâce à ces mesures, il est possible de détecter à temps et d'empêcher ou de limiter les conséquences des cyberattaques visant les actifs précieux de l'entreprise. Par ailleurs, une nouvelle procédure n'est pas obligatoirement synonyme de nouveau personnel : la cybersécurité est également possible grâce à l'acquisition de nouvelles compétences par les employés.

Au cours de leur activité, les entreprises doivent constamment tenir compte des cyber-risques et les passer en revue grâce à des procédures et des technologies de sécurité informatique déjà introduites. Il faut préparer aux cybermenaces non seulement l'infrastructure IT mais également le personnel de l'entreprise en l'informant et en vérifiant régulièrement ses connaissances en matière de sécurité informatique. De cette manière, on crée un environnement « préparé » qui permet de détecter et de contrer les cyberattaques le plus tôt possible.

Anastasia Terekhina, ACCA,
senior manager du département d'audit,
auditrice certifiée
Lev Batishchev, auditeur senior
des systèmes d'information

1 https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en.

MAZARS
AUDIT, ACCOUNTANCY, TAX, LEGAL AND ADVISORY SERVICES