Club de l'Audace

Conférence sur la sécurité économique dans les PME

Le Club de l'Audace a organisé à Paris une conférence sur la sécurité économique dans les PME. Animée conjointement par Jean-Marc Allouët, associé du cabinet d'expertise comptable BDO, Isabelle Renard, Avocate associée au sein du Cabinet IRenard Avocats et le hacker *Super Benoit, afin de mettre en avant les enjeux de la sécurité économique au sein des PME.*

Chaque année, près de 1 000 atteintes économiques sont recensées en France par les services de l'Etat en charge de la sécurité des entreprises. Si le piratage informatique en est la forme la plus connue, ces attaques peuvent être extrêmement variées. Garantir la sécurité économique des entreprises est une nécessité absolue, afin de préserver leur compétitivité dans un contexte de plus en plus concurrentiel.

I. LE CONCEPT DE SECURITE ECONOMIQUE EN CINQ POINTS

1. Toutes les entreprises possèdent des informations stratégiques qui doivent être protégées

Les protections relèvent à la fois de la sûreté et de la stratégie juridique. Internet accroît considérablement la vulnérabilité des entreprises. Tout l'enjeu pour le dirigeant consiste à réduire les risques à un niveau de vigilance qui n'entrave pas le fonctionnement de son entreprise.

2. La sécurité économique vise plusieurs objectifs simultanément

• **L'identification et l'analyse des menaces** dont les entreprises sont la cible.

• **La protection des informations stratégiques des entreprises**, quelles que soient leur taille ou le secteur d'activité dans lequel elles évoluent. Toutes les entreprises sont concernées. Il ne faut pas se croire à l'abri sous prétexte qu'on est une TPE/PME ou que l'on intervient sur un secteur peu concurrentiel.

• **La diffusion d'une culture de la sécurité du patrimoine matériel** et immatériel au sein de l'ensemble des entreprises. Se protéger est un réflexe qui s'apprend. Il est essentiel pour le dirigeant d'entreprise d'obtenir l'appui de l'ensemble des collaborateurs à travers des actions de sensibilisation et de formation.

3. Les protections relèvent à la fois de la sûreté et de la stratégie juridique

• **La sûreté** recouvre par exemple le contrôle des accès aux locaux ou la sécurisation des systèmes d'informations. Les entreprises ont également l'obligation légale de **protéger leurs collaborateurs** et de veiller à ce que les informations les concernant soient sécurisées,

• **La stratégie** juridique recouvre notamment la protection des marques et des modèles, les dépôts de brevets ou encore les preuves des créations protégées par le Droit d'auteur. Tant que l'entreprise n'a pas **protégé juridiquement sa créativité et son innovation, elle doit mettre en place des procédures de confidentialité** et contractualiser cette confidentialité, que ce soit avec ses collaborateurs, ses partenaires ou ses prestataires.

Jean-Marc Allouët, Isabelle Renard, Thomas Legrain et le hacker Super Benoit

Photo © Club de l'Audace

4. Internet accroît considérablement la vulnérabilité des entreprises

Avec le développement du commerce électronique et l'utilisation croissante d'Internet, de plus en plus d'informations sont partagées et stockées partout dans le monde sur des serveurs qui peuvent s'avérer vulnérables *(cloud computing)*. Il existe dès lors un risque accru de sabotage, d'altération, d'effacement ou de fraude.

5. Tout l'enjeu pour le dirigeant consiste à réduire les risques à un niveau de vigilance qui n'entrave pas le fonctionnement de son entreprise

• Il doit veiller à **adapter la politique de sécurité** à la taille de sa société et à sa situation.

• Il doit s'efforcer de protéger uniquement ce qui doit l'être : **il ne s'agit pas de tout verrouiller, mais d'être vigilant sur l'essentiel** afin de réduire au maximum les vulnérabilités.

• **La politique de sécurité de l'entreprise doit impérativement s'inscrire dans le temps**, malgré les changements de personnes, d'équipements ou d'organisation.

II. L'EXISTENCE DE PIEGES NOMBREUX ET VARIES

Avant de mettre en place des portiques de sécurité ou de s'équiper en logiciels spécialisés, la protection des informations de l'entreprise passe d'abord par le bon sens. La majorité des informations sensibles étant transmises par les personnes, il faut faire comprendre aux collaborateurs qu'ils doivent apprendre à être discrets. Il convient de les

sensibiliser et de leur faire prendre conscience de certains pièges afin qu'ils puissent les éviter.

1. Parler de son entreprise et des projets dont on a la charge en dehors de l'entreprise, dans des lieux où il est très facile pour des concurrents d'ouvrir grand leurs oreilles

Un collaborateur doit absolument éviter de parler de son entreprise à l'extérieur, notamment lors des pauses cigarettes ou durant un *afterwork*. Il doit s'interdire d'avoir une conversation de travail dans les transports (taxi, avion, train, métro...) ou dans les lieux publics (salles d'attente, restaurants, hôtels, salons professionnels...). Le pire, c'est lorsqu'un colloque réunit tous les acteurs d'une filière économique dans une ville. Il suffit alors de prendre le bon train ou le bon avion et d'écouter les discussions ! Les langues se délient également trop facilement dans les salons professionnels ou au téléphone.

2. Laisser des documents sur une imprimante ou un photocopieur partagés

Les collaborateurs ne pensent pas toujours à reprendre l'ensemble des documents, originaux ou copies, quitte à en détruire certains plus tard.

3. Cliquer de manière automatique sur des liens placés dans les e-mails que l'on reçoit

Une des attaques classiques visant à tromper l'internaute pour lui voler des informations personnelles consiste à l'inciter à cliquer sur un lien placé dans un message.

4. Ouvrir mécaniquement les pièces jointes dans les e-mails que l'on reçoit

Une des méthodes les plus efficaces pour diffuser des codes malveillants est d'utiliser des fichiers joints aux e-mails. Les collaborateurs vont souvent ouvrir sans faire attention des pièces jointes malveillantes dont les extensions sont les suivantes : .pif ; .corn ; .bat ; .exe ; .vbs ; .lnk.

5. Divulguer des informations stratégiques lors de l'utilisation d'un traducteur en ligne

6. Utiliser en toute innocence une borne WiFi dans un lieu public (gare, aéroport, salon professionnel, ...)

Tout le contenu stocké dans un ordinateur peut être capté.

7. Laisser dans sa chambre d'hôtel des informations confidentielles

Il est possible que la chambre, bagages et coffre-fort compris, soit *« visitée »* en l'absence de son occupant.

8. Se rendre à l'étranger avec des informations confidentielles dans son ordinateur

Si l'ordinateur d'un collaborateur est saisi durant un passage à la douane d'un pays, puis lui est rendu dans les cinq minutes, il peut avoir été copié de fond en comble.

III. UNE DEMARCHE DE SECURITE ECONOMIQUE EN TROIS ETAPES

1. La première étape consiste à repérer les informations stratégiques de l'entreprise

• **Inventaire de toutes les informations sensibles ou confidentielles** : plan stratégique, fichiers clients, contrats, données comptables, dossiers du personnel, inventions brevetables, procédés de fabrication...

• **Recensement des supports sur lesquels reposent les informations de l'entreprise** : ordinateurs, Internet, messageries électroniques, clefs USB, téléphones, armoires, locaux d'archivage, ...

2. La seconde étape consiste à analyser les principaux risques et menaces qui peuvent peser sur l'entreprise

• **Analyse insuffisante des sources ouvertes**, c'est-à-dire des informations provenant de l'entreprise elle-même (salons, colloques, interviews, publications, sites internet...). Assurez- vous notamment que les plaquettes, les documents promotionnels ou encore le site Internet de l'entreprise ne laissent pas filtrer des renseignements confidentiels.

• **Manque de prudence** (bavardages, conversation dans des lieux publics, étalage de sa vie professionnelle sur les réseaux sociaux type Facebook, Viadeo, LinkedIn...) ; **manque de vigilance** (données confidentielles dans la poubelle, perte de matériels informatiques, absence de surveillance de prestataires extérieurs intervenant dans l'entreprise...) ; **manque de rigueur** dans l'application des procédures par les collaborateurs (documents confidentiels emportés à l'extérieur de l'entreprise, non-respect des mesures de sûreté...).

• **Collaborateurs peu scrupuleux** qui, pour des motivations personnelles diverses et variées (vengeance, jalousie, intérêt...), sont amenés, dans l'exercice de leurs fonctions, à commettre des fautes (détournement de patrimoine, divulgation d'informations ou de contacts...).

3. La troisième étape vise à mettre en place des bonnes pratiques et à bâtir une politique de sécurité globale qui couvrira des aspects variés

Il est vivement recommandé de mettre en place dans chaque entreprise une **charte de bonnes pratiques professionnelles** (à respecter aussi bien en interne qu'à l'extérieur) qui permet notamment de lister les comportements à adopter pour conserver la confidentialité des informations stratégiques. Il y sera fait référence aussi souvent que nécessaire, notamment lors de salons professionnels ou de conférences.

IV. SIX BONNES PRATIQUES EN MATIERE DE SECURITE ECONOMIQUE

1. Identifiez les informations stratégiques dans votre entreprise et qualifiez-les en fonction de leur niveau de sensibilité

• Protégez vos documents à travers **un travail de classement et d'archivage.**

• Apposez une **marque de propriété sur tous les documents que votre entreprise produit** (logo, footer avec les coordonnées de l'entreprise...).

• Identifiez les **documents confidentiels avec un sigle spécifique** apposé sur la couverture des rapports papiers ou avec un sigle visible à l'écran sur vos supports numériques. Mettez en place une gestion spécifique de ces documents pour contrôler leur usage et leur diffusion.

2. Protégez les innovations techniques, marques, dessins et modèles qui constituent le patrimoine de votre entreprise

• Sachez que la protection de la propriété industrielle s'effectue auprès de **l'Institut national de la propriété industrielle** (INPI – www.inpi.fr).

• **Pensez notamment à protéger le nom de domaine de votre entreprise.** Déposez au minimum le .fr et le .com ; si le nom de domaine comprend plusieurs mots, le déposer avec et sans tirets.

• **Consultez un Avocat** afin d'organiser la propriété intellectuelle et de rédiger les clauses contractuelles indispensables (en particulier les clauses de confidentialité dans les contrats de travail et de prestation de services).

3. Sécurisez vos locaux et définissez une procédure pour les visites

• **Votre entreprise ne doit pas être ouverte à tous les vents** : un visiteur ne doit pas pouvoir entrer librement. L'accès aux locaux doit être protégé en installant un accueil, une porte blindée, une alarme...

• **Lors d'un entretien, chaque collaborateur doit penser à fermer les dossiers confidentiels** qui peuvent traîner sur son bureau et sur son ordinateur. Ces documents doivent également être mis sous clé lors de la pause déjeuner, le soir ou durant le nettoyage des bureaux. Des armoires fortes doivent être installées afin d'y ranger les documents stratégiques de l'entreprise ainsi que les supports informatiques.

• Un collaborateur doit avoir le réflexe de

ranger son bureau, de broyer les documents sensibles devenus inutiles y compris les brouillons, de retirer la feuille du paperboard après toute réunion.

• Il faut également penser à jeter et à détruire les supports informatiques susceptibles de contenir des informations confidentielles qui pourraient être récupérées, dès lors que ces supports ne sont plus utilisés au sein de l'entreprise.

• Selon la sensibilité des activités de l'entreprise, l'accès à certains locaux doit faire l'objet de mesures de restriction (laboratoires, salles de serveurs informatiques, bureaux d'études…).

• Toute intervention d'un sous-traitant à l'intérieur des locaux doit être effectuée sous surveillance constante d'un collaborateur averti (entretien d'un photocopieur, travaux d'aménagements des bureaux, réparations diverses…).

4. Encadrez les stagiaires

• Vérifiez que vous avez bien reçu la convention de stage et que celle-ci a bien été signée par les trois parties (l'entreprise, l'organisme de formation, le stagiaire lui-même).

• Si le stagiaire est étranger, assurez-vous qu'il a un visa en règle.

• Faites-lui signer une clause de confidentialité avant l'entrée dans l'entreprise et assurez- vous qu'il a bien compris à quoi cette clause l'engage.

• Délimitez l'activité du stagiaire au sein de l'entreprise dès le début de son stage.

• Assurez-vous que le stagiaire n'aura pas accès aux informations confidentielles de l'entreprise. Par exemple, ne lui donnez pas de droits d'accès sur son ordinateur qui lui permettent de prendre connaissance de toutes les informations stockées sur les serveurs de l'entreprise.

• Récupérez le badge et les clefs à l'issue du stage ainsi que les éventuels codes d'accès que vous lui avez communiqués (accès aux locaux, accès informatiques).

• Déterminez qui sont les destinataires du rapport de stage et vérifiez attentivement qu'il n'y soit pas divulgué d'informations confidentielles sur l'entreprise.

• Assurez-vous que le stagiaire ne mette pas en ligne un rapport de stage contenant des informations sensibles. Informez-le de cette interdiction avant même le début de son stage.

5. Sécurisez vos systèmes d'information

• La plupart des destructions et des vols d'informations proviennent de mauvaises manipulations internes sur les ordinateurs, les serveurs ou les téléphones. Tous ces matériels doivent être protégés, afin d'éviter les intrusions d'une part et les maladresses d'autre part.

• Les ordinateurs doivent disposer de logiciels de détection d'erreurs ou d'intrusion. Il convient d'installer des logiciels de sécurité (antivirus, anti spam, pare-feux, …). Il faut notamment sécuriser le logiciel antivirus de tous les ordinateurs de l'entreprise afin qu'il analyse automatiquement, à intervalles réguliers, tous les fichiers enregistrés sur chaque ordinateur.

• Le dirigeant doit s'assurer que les logiciels installés sur les ordinateurs de son entreprise sont à jour. Il doit notamment veiller à bien faire mettre à jour régulièrement les logiciels de protection : anti spam, antivirus, pare-feu.

• Des dispositifs de sauvegarde sûrs et redondants doivent être mis en place et fonctionner à l'aide de bases de données centrales ou de supports gravés. Les données stratégiques de l'entreprise doivent être dupliquées régulièrement et les sauvegardes doivent être placées à l'abri des tentatives d'intrusion, des risques d'incendie ou d'inondation sur un site différent, en les confiant, par exemple, à une société extérieure spécialisée dans l'archivage informatique.

• Les mots de passe ne doivent rien évoquer *a priori,* ils doivent être tous différents en fonction des dossiers et des postes informatiques, ils doivent être renouvelés régulièrement et ne doivent être communiqués à personne. Il ne faut pas les écrire sur un post-it que l'on colle sur son ordinateur ou sur un papier que l'on range dans son portefeuille… !

• Les profils utilisateurs à l'intérieur de l'entreprise et les droits d'accès associés doivent être définis au cas par cas.

• Le dirigeant doit savoir précisément combien de personnes dans son entreprise disposent du mot de passe administrateur permettant d'accéder au système central de gestion des droits. Il doit s'efforcer de limiter le nombre de titulaires de comptes disposant de privilèges élevés aux seules personnes pour lesquelles ces privilèges sont absolument nécessaires dans l'accomplissement de leur mission. Des listes doivent être tenues à jour pour tous les comptes de ce type.

• Les collaborateurs de l'entreprise qui ont un code administrateur ne doivent l'utiliser que lorsqu'ils travaillent sur des tâches administratives. Ils doivent se servir d'un code utilisateur lorsqu'ils effectuent des actions plus exposées, comme lire leurs e-mails ou naviguer sur Internet, par exemple.

• Les comptes utilisateurs d'un collaborateur doivent être supprimés dès qu'il quitte l'entreprise définitivement. Lorsqu'une personne dispose d'un compte temporaire dans l'entreprise (ex : stagiaire, prestataire), il faut bien penser à configurer une date d'expiration lors de la création du compte.

• Les disques durs des ordinateurs doivent être nettoyés avant d'être affectés à un autre collaborateur. Toutes les données doivent être effacées.

• Le mot de passe utilisé pour installer les imprimantes au sein de l'entreprise doit être contrôlé. Il faut en particulier éviter que ce mot de passe soit celui qui permet le contrôle total du système d'information de l'entreprise.

• Le dirigeant doit disposer d'une cartographie du réseau informatique de son entreprise, afin de pouvoir identifier les vulnérabilités et les faire corriger.

• Après usage d'un photocopieur ou d'une imprimante numérique, le dirigeant doit s'assurer que les données en mémoire sont systématiquement effacées.

• En cas d'intrusion sur un poste informatique, il ne faut pas se contenter de vérifier uniquement le poste concerné. La recherche d'éventuelles autres traces d'intrusion sur le système informatique de l'entreprise est indispensable après la découverte d'une intrusion. Généralement, les attaquants s'ouvrent de multiples portes d'entrées dans le système.

• La taille des fichiers qui sortent du système d'information de l'entreprise, les jours et les horaires de sortie ou encore les destinataires doivent être contrôlés. L'analyse des journaux d'évènements permet de repérer les activités inhabituelles et de détecter d'éventuels signes d'intrusion. Les journaux d'évènements doivent être activés, configurés et centralisés pour permettre cette analyse.

• Il convient de tout faire pour protéger le réseau sans fil de l'entreprise. Le point d'accès du réseau doit de préférence être placé au centre de l'entreprise, loin des murs extérieurs. Le nom du réseau doit être modifié par défaut (Service Set Identifier : SSID) et il convient d'activer les fonctions de sécurité, de préférence la fonction WPA2 (WiFi Protected Access). On peut éventuellement activer le filtrage Media Access Control (MAC).

• Un collaborateur qui travaille sur son ordinateur portable dans le train via le wifi doit être conscient du fait que son travail peut être récupéré par un tiers. Les données confidentielles doivent uniquement être traitées et stockées sur des postes de travail non connectés en réseaux.

6. Protégez l'image et la réputation de votre entreprise et de ses principaux dirigeants

Assurez une veille de ce qui se dit sur l'entreprise et ses dirigeants sur les forums et les réseaux sociaux.

Une rumeur ou une campagne calomnieuse à l'encontre d'un produit ou d'un service orchestrée par un concurrent peu scrupuleux peut causer de sérieux dommages à l'entreprise. Apprenez à y répondre.

2016-1514 *Michel Léger*