



L'espionnage industriel existe aussi dans l'industrie belge !

LORS DE NOS VISITES D'ENTREPRISES, NOUS PERCEVONS CHEZ BON NOMBRE DE CONSTRUCTEURS UNE PEUR QUASI PARANOÏAQUE DE L'ESPIONNAGE INDUSTRIEL. LES PORTES DES ATELIERS DE FABRICATION NE S'OUVRENT SOUVENT QU'APRÈS MOULT DEMANDES. PARFOIS, ELLES RESTENT MÊME FERMÉES. DURANT LES INTERVIEWS, DE NOMBREUSES QUESTIONS (SOUVENT TECHNIQUES) RESTENT SANS RÉPONSE DE CRAINTE QUE LA 'CONCURRENCE' PUISSE ABUSER DE CES INFORMATIONS. NOUS NOUS SOMMES DONC ADRESSÉ À L'IR YVAN DE MESMAEKER, L'EXPERT BELGE PAR EXCELLENCE DANS LE DOMAINE DE L'ESPIONNAGE INDUSTRIEL, POUR SAVOIR SI UNE TELLE ATTITUDE ÉTAIT BIEN JUSTIFIÉE. IL APPARAÎT, DE FAIT, QU'UN PEU DE MÉFIANCE ET DE PRUDENCE NE SEMBLent PAS FAIRE DE MAL!

L'espionnage industriel ou économique existe bel et bien en Belgique. Bien qu'il soit quasiment impossible de donner des chiffres exacts sur cette

forme de criminalité, environ 20% des informations utilisées dans les entreprises proviendraient de la 'matière grise' et 10% de pratiques illégales. «Les entreprises



Ir Yvan De Mesmaeker est Security Auditor chez Omega Risk et Secrétaire général de la European Corporate Security Association.



Récepteur du microphone sans fil.

cherchent continuellement à améliorer leurs processus et produits» explique Yvan De Mesmaeker. «Les fabricants de produits alimentaires aiment savoir quelles technologies, paramètres de processus, ingrédients, recettes... la concurrence utilise. Ils s'intéressent naturellement aussi à leurs fournisseurs, conditions d'achat, clients, politique de prix et marges bénéficiaires, stratégie de marketing... De telles informations peuvent être obtenues de trois façons différentes. En première instance, nous avons la voie légale normale: Internet, la presse, la littérature professionnelle, les salons professionnels, les bureaux d'étude, les consultants... Les informations obtenues par l'indiscrétion de fournisseurs et de membres du personnel de la concurrence relèvent aussi de cette catégorie. Le problème, c'est que tout le monde accède à ces données et qu'elles ne feront dès lors pas toujours la différence que vous souhaitez. Raison pour laquelle certaines sociétés vont un pas plus loin et entrent dans la zone floue: elles optent pour des actions qui ne sont juridiquement pas réprimandables

mais qui s'avèrent douteuses sur le plan déontologique. Pensez par exemple à l'observation des installations de production de la concurrence. Il est parfois possible de distinguer assez facilement à distance la capacité de stockage et une partie de la chaîne de production, vous pouvez compter le nombre de camions qui arrivent et repartent, vous voyez le nombre de personnes travaillant par shift... Il est aussi assez facile de suivre les livraisons jusque chez le client. Et quantité d'entreprises présentent de très grandes fenêtres: lors des présentations PowerPoint données dans les bureaux de la direction, une personne située à l'extérieur peut dès lors très aisément suivre la présentation. Lorsque vous révisez des documents dans l'avion ou le train, vous ne savez jamais qui regarde par-dessus votre épaule. Fouiller dans les déchets de bureaux peut aussi se révéler une précieuse source d'informations. Vous pouvez – éventuellement sous un autre nom – visiter une entreprise ou engager quelqu'un ayant pour mission de négocier les produits et les prix en tant que client potentiel. Une autre



méthode consiste à suivre le personnel à midi ou après le travail et à écouter leurs conversations au café/restaurant, voire à entamer avec eux une conversation soi-disant innocente. Il arrive aussi qu'une société place une fausse annonce. Les chances sont en effet grandes que du personnel de la concurrence y réponde, ce qui permet de soutirer des informations. Même des

signes indiquent parfois clairement qu'il se passe quelque chose» remarque Yvan De Mesmaeker. «Pensez par exemple à un cambriolage au cours duquel l'ordinateur a été volé, mais pas les écrans et les imprimantes. Ou au PC qui a disparu tandis que le portable est resté. Cela indique que les cambrioleurs n'avaient probablement aucune intention

personnel au risque de parler de leur travail à l'extérieur de l'entreprise. Et veillez à ce qu'ils ne travaillent pas à l'extérieur – chez un client, dans le train ou dans l'avion... - sur des informations confidentielles. Désignez une personne responsable de la communication avec le monde extérieur et donnez-lui un briefing très intensif sur ce qu'il peut et ne peut pas dire. Et si quelqu'un d'autre doit parler avec la presse, veillez alors à établir des accords clairs avec le porte-parole officiel et assurez-vous de sa présence lors de l'interview. La bonne ambiance au travail joue naturellement

treprise: réfléchissez auparavant à ce que vous montrerez et ne montrerez pas à vos visiteurs! Et lorsqu'un nouveau client potentiel souhaite vous rendre visite, n'hésitez pas à appeler sa société afin de confirmer le rendez-vous. De la sorte, vous êtes sûr qu'il travaille auprès de cette société et qu'il n'a pas été engagé pour vous soutirer des informations. Dernier point encore: une grande quantité d'informations confidentielles tombent par négligence entre les mains de personnes non autorisées. Combien de fois n'arrive-t-il pas que des personnes donnent des présentations importantes

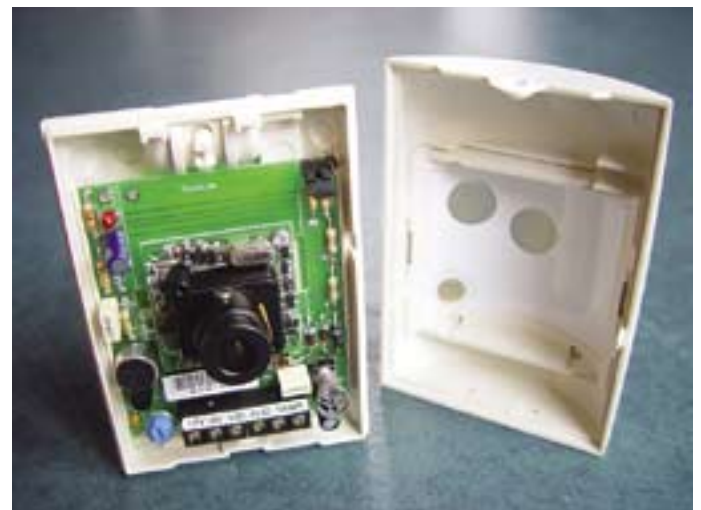
“On estime en règle générale qu'environ 10 % des connaissances sont collectées de la sorte. Ce sont surtout les secteurs dans lesquels le faible nombre d'acteurs fabriquent des produits quasi identiques pour lesquels l'innovation est primordiale, qui doivent se méfier de ce type de délit. Voilà pourquoi l'industrie alimentaire est certainement prédisposée à l'espionnage industriel!” <<

chasseurs de têtes peuvent être engagés dans ce contexte, sans savoir naturellement qu'il n'y a pas d'offre vacante! De telles actions ne sont donc pas punissables. Cependant, si elles arrivent aux oreilles du grand public, il y a de fortes chances que votre réputation en prenne un coup. Pourtant, bien plus d'entreprises que vous ne le penseriez estiment que cela vaut la peine d'acquiescer des informations par des méthodes relevant de la zone floue. Nous estimons que certainement 20% des connaissances des entreprises sont acquises de la sorte! Finalement, il y a les entreprises qui se moquent complètement de la législation et de la déontologie et qui font du véritable espionnage économique-industriel. Nous parlons ici d'effractions physiques, d'engagement de pirates, de corruption du personnel afin de transmettre des informations, de placement d'appareils d'écoute... Les informations ainsi obtenues étant très précieuses, il serait naïf de penser que de telles pratiques n'ont pas cours en Belgique. On estime en règle générale qu'environ 10 % des connaissances sont collectées de la sorte. Ce sont surtout les secteurs dans lesquels le faible nombre d'acteurs fabriquent des produits quasi identiques pour lesquels l'innovation est primordiale, qui doivent se méfier de ce type de délit. Voilà pourquoi l'industrie est certainement prédisposée à l'espionnage industriel!»

de voler des biens dans l'intention de les revendre par la suite. Il se peut aussi que quelqu'un essaie de vous vendre des listes de clients ou des données de processus et que vous remarquiez que celles-ci proviennent de votre propre entreprise. Il arrive également que des collaborateurs finissent par avouer au cours d'une conversation. Cependant, les cas d'espionnage économique-industriel découverts de la sorte ne constituent probablement qu'une faible part du nombre véritable d'actes malveillants. C'est pourquoi je conseille à toutes les entreprises de prendre un maximum de précautions afin d'éviter de telles pratiques illicites. Vous avez aussi tout intérêt à mettre des bâtons dans les roues des concurrents qui veulent acquiescer des informations en recourant à des méthodes relevant de la zone floue!»

QUELLES ACTIONS ENTREPRENDRE ?

Mais comment protéger votre entreprise contre ces actions relevant de la zone floue ou contre l'espionnage industriel effectif? «Pour commencer, la direction de l'entreprise et les collaborateurs doivent prendre conscience de la valeur des informations qu'elles manipulent tous les jours. Et même lorsqu'ils en sont conscients, ils font encore trop souvent preuve d'une grande naïveté par rapport aux moyens que peut utiliser un concurrent pour s'en approprier. Voilà pourquoi les entreprises doivent sensibiliser chaque employé à la prudence. Sensibilisez par exemple votre



Caméra et microphone dissimulés sous la forme d'un détecteur de présence.

aussi un rôle car elle évite que les collaborateurs ne répondent à des annonces ou offres d'emploi – vraies ou fausses – de la concurrence et s'y montrent trop indiscrets. Une quantité d'interventions sur le plan structurel peuvent aussi apporter une aide sérieuse. Pensez à un enclos opaque autour de l'usine et du parking des visiteurs, à des rideaux devant les fenêtres, pensez à conserver les déchets derrière des portes closes, à rendre le site entièrement inaccessible aux personnes non autorisées... Un système de contrôle d'accès efficace est indispensable. Toutefois, il doit être bien utilisé : l'identité des visiteurs est rarement vérifiée. Informez aussi vos collaborateurs sur les locaux, machines... qui ne peuvent être montrés à des tiers. Soyez prudents quant à l'organisation des visites d'en-

dans un hôtel et laissent traîner durant le lunch leurs documents dans la salle? Ou que les copies aboutissent par la suite dans la poubelle de cet établissement? Si la concurrence recherche activement de telles données, elle peut facilement y arriver de manière quasiment légale! D'ailleurs, assurez-vous toujours que les documents importants ne soient pas jetés tels quels: détruisez-les toujours en petits morceaux à l'aide d'une bonne déchiqueteuse à taille croisée. N'utilisez pas un appareil qui coupe les documents en bandes car avec un peu de patience, ils peuvent être reconstitués. Consacrez aussi suffisamment d'attention aux documents qui sont envoyés : indiquez clairement le destinataire, utilisez des enveloppes doubles et notez distinctement sur l'enveloppe intérieure la mention 'confidentiel', optez

UN HOMME AVERTI...

Il est toutefois très difficile de détecter si votre entreprise est la victime d'un espionnage économique ou industriel. «Certains



plutôt pour des coursiers que pour la poste...»

L'ICT: LE MAILLON FAIBLE

En matière de réel espionnage industriel, le système informatique constitue le principal maillon faible. Veillez dès lors à intégrer les protections nécessaires au moyen de divers mots de passe, coupe-feu... de qualité. Une surveillance continue des tentatives de piratage est également requise. «Il est par ailleurs essentiel d'appliquer une bonne gestion des documents: assurez-vous que les données délicates ne puissent être consultées que par les personnes autorisées,



instaurez des restrictions dans les possibilités d'impression et d'envoi..." remarque Yvan De Mesmaeker. "Et mieux vaut encrypter les informations importantes qui doivent être envoyées par courriel. Si vous ne disposez pas de cette possibilité, protégez au moins les données envoyées par un mot de passe. L'espionnage industriel arrive aussi souvent via de simples cambriolages. Raison pour laquelle il est absolument nécessaire de prévoir suffisamment d'obstacles sur votre domaine/entreprise: une protection périmétrique avec

surveillance par caméra, des portes et fenêtres anti-effraction, une détection anti-effraction raccordée à une centrale de surveillance permanente, des gardiens qui contrôlent physiquement que tout soit en ordre, des systèmes qui génèrent des alarmes si une fenêtre ou une porte est restée ouverte, des armoires anti-effraction... Finalement, vous devez aussi tenir compte de l'existence d'un réel équipement d'espionnage. Celui-ci doit naturellement être installé: une protection efficace contre les effractions et un bon contrôle d'accès limitent déjà fortement ce risque. Vous pouvez aussi réduire le risque en accueillant des tiers dans des salles de réunion situées en dehors de l'entreprise. Cependant, si vous voulez aller encore plus loin, vous pouvez engager à intervalles réguliers des sociétés spécialisées qui passent au crible vos locaux: elles vérifient au travers d'une détection poussée la présence d'un quelconque équipement d'espionnage. Vérifiez toutefois qui vous engagez pour ce travail car bon nombre d'entreprises prétendent disposer des connaissances et de l'équipement nécessaires alors que ce n'est pas le cas. Peu de sociétés en Belgique peuvent vraiment assumer une telle détection. Les véritables spécialistes se trouvent surtout au Royaume-Uni. Et ce n'est pas bon marché: vous atteindrez rapidement un prix de 5000 euros."

QUID DES FOURNISSEURS INDISCRETS?

Les fournisseurs représentent un autre grand risque. En effet, les intégrateurs système, les fournisseurs d'ingrédients et les consultants disposent par la force des choses de nombreuses informations confidentielles sur votre entreprise, informations qu'ils peuvent transmettre à des

personnes non autorisées. "Il ne faut pas toujours y rechercher un but malintentionné. Pensez par exemple au vendeur qui est tellement enthousiaste d'une solution technique sur mesure réalisée par sa société, qu'il en parle à votre concurrence. Ou pensez encore au constructeur qui, en l'absence d'accords clairs, décide de commercialiser

"Le management doit donner l'exemple: vous ne pouvez espérer de votre personnel qu'il fasse preuve de la prudence nécessaire si vous laissez traîner des documents importants sur votre armoire par exemple. Il est par ailleurs absolument nécessaire de fournir à vos collaborateurs tous les instruments de protection possible!"

la machine qu'il a fabriquée pour votre société, vous faisant ainsi perdre un avantage compétitif. Il existe aussi des fournisseurs moins professionnels qui utilisent les informations d'un client pour en gagner un autre. Raison pour laquelle il faut bien vérifier avec qui vous vous engagez. Les premières conversations vous permettront probablement déjà de vous faire un avis sur le sérieux du fournisseur. Mais puisque vous ne pourrez jamais être sûr à cent pour-cent, il est impératif de faire signer à tous les fournisseurs un accord de confidentialité. Seule cette méthode vous donnera un recours si vous constatez une quelconque violation. Je tiens encore à signaler qu'il est préférable de prévoir une clause dans laquelle vous stipulez que l'amende dépend des dommages encourus. La clause doit pouvoir être appliquée en cas de négligence démontrable car il est souvent difficile de montrer un lien de cause à effet entre la fuite d'informations et les dommages encourus."

LE PRÉVENTIF MIEUX QUE LE RÉPRESSIF

Quoi qu'il en soit: le facteur humain reste le véritable maillon faible. D'où l'importance de la sensibilisation. "Le management doit donner l'exemple: vous ne

peuvent espérer de votre personnel qu'il fasse preuve de la prudence nécessaire si vous laissez traîner des documents importants sur votre armoire par exemple" poursuit Yvan De Mesmaeker. "Il est par ailleurs absolument nécessaire de fournir à vos collaborateurs tous les instruments de protection possible! Il est évidemment recommandé d'imposer

contractuellement le secret des informations confidentielles. Cependant, pour pouvoir réellement en profiter, vous devez identifier clairement les informations qui sont confidentielles et celles qui ne le sont pas. Raison pour laquelle nous vous recommandons de donner à tous les documents une classification: par exemple utilisation interne, confidentiel et très confidentiel. Vous pourrez alors punir les infractions par des sanctions pouvant aller jusqu'au licenciement. Les membres du personnel licenciés restent toutefois un grand problème car ils sont naturellement libres de fournir toutes les informations à la concurrence. Dans de tels cas, vous pouvez accuser ces personnes au tribunal sur la base de clauses de non-concurrence. Cependant, dans la pratique, vous avez peu de chances de gagner. Il est donc préférable de créer une bonne ambiance de travail et de construire de bonnes relations avec votre personnel. Néanmoins, il faut toujours garder les règles formelles comme une épée de Damoclès. En effet, vous ne serez jamais assez prudents!"

Els Jonckheere



Vous pouvez télécharger cet article sur www.mainpress.com