businews

MAI 2018
N° 172

TOUTE L'ÉCONOMIE DE LA PROVENCE

CYBERCRIMINALITÉ

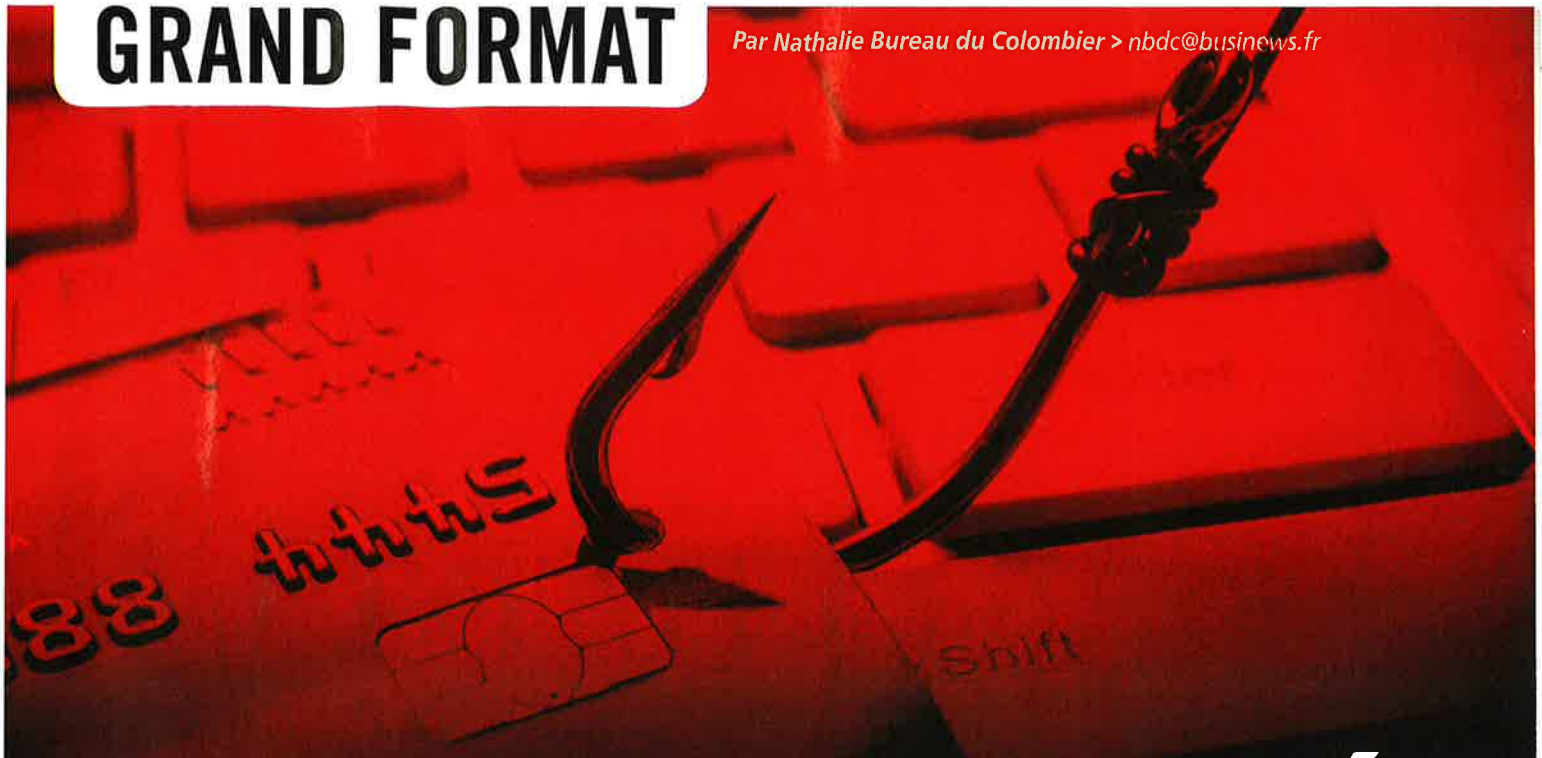
LE CASSE DU SIÈCLE

Parcs informatiques, terminaux de paiement, objets connectés... Les criminels ne se contentent plus d'entrer par effraction dans les bâtiments des entreprises et des administrations. Sournois, ils détournent la technologie pour dérober de l'argent, des marchandises ou réclamer des rançons astronomiques. Analyse de la cybercriminalité, un phénomène qui prend de l'ampleur et qui n'épargne personne.

P. 28
L'ENQUETE IMMOBILIER 2.0 : HOME SUITE HOME

4 € (Abonnement 37 € / An)

Par Nathalie Bureau du Colombier > nbdc@businews.fr



CYBERCRIMINALITÉ : LE CASSE DU SIÈCLE

Parcs informatiques, terminaux de paiement, objets connectés... Les criminels ne se contentent plus d'entrer par effraction dans les bâtiments des entreprises et des administrations. Sournois, ils détournent la technologie pour dérober de l'argent, des marchandises ou réclamer des rançons astronomiques. Analyse de la cybercriminalité, un phénomène qui prend de l'ampleur et qui n'épargne personne.

Une attaque informatique coûte en moyenne 800.000 euros à une entreprise quelles que soient sa taille et son activité ! Les cyber attaques prennent une ampleur inégalée. 6 milliards d'euros en France en 2017, selon Symantec, et 600 milliards d'euros dans le monde, d'après Gartner. Le préjudice a triplé en seulement un an en 2016. Insidieux, les criminels n'affrontent plus directement leurs victimes et optent pour un modus operandi bien plus confortable, cachés derrière les réseaux informatiques. Les organisations criminelles, agissant à plusieurs dizaines de milliers de kilomètres de leurs proies, sont difficilement repérables.

PHOTO XDR

43% des attaques ciblent les Pme

Toutes les entreprises sont exposées aux attaques, les plus vulnérables étant les Pme, insuffisamment informées et disposant de peu de moyens pour se défendre. Ainsi, 43% des cyberattaques ciblent spécifiquement les Pme.

> « 98% des informations sont accessibles sur Internet, y compris celles classées confidentiel défense. »

Vols de mots de passe et identifiants mettant en danger la confidentialité des données de l'entreprise, cryptage à distance des fichiers et blocage des systèmes de production... Les risques opérationnels, financiers sont colossaux sans compter l'impact sur la réputation de l'entreprise, soudain pointée du doigt.

Le site de rencontres extra-conjugales « Hasley Madison » qui a été victime de hackers en 2015 n'avait pris aucune mesure de protection. Résultat : les données personnelles (nom, prénom, téléphone, mail) des 37 millions d'infidèles ont été diffusées sur le net. Pire encore, leurs pratiques sexuelles étaient dévoilées au grand jour. Deux personnes se sont suicidées suite à cette dramatique affaire. La même année, les programmes de TV Monde ont cessé d'émettre durant deux jours. A la place, la chaîne de télévision francophone, victime d'une cyberattaque, diffusait des messages de soutien à l'Etat Islamique.

Les ravages de NotPetya dans l'industrie en 2017

Les grands groupes ne sont donc pas à l'abri en dépit des moyens déployés. En juin 2017, le virus «NotPetya» a fait des ravages dans l'industrie. Selon, nos confrères du Monde, les pays occidentaux – Washington et Londres en chef de file – l'attaque serait originaire de Russie et visait l'Ukraine. Les industriels ayant des liens commerciaux avec l'Ukraine ont subi les dommages collatéraux. Ces derniers s'élèveraient à 1 milliard de dollars pour Maersk Line, Fedex, Saint-Gobain et leurs sous-traitants.

La fraude au président : 300 MDE par an

Les grands groupes et ETI doivent également se méfier d'une autre ruse, à savoir le coup de fil du faux Pdg qui donne un ordre de virement ou le faux fournisseur qui modifie une simple lettre d'une adresse mail... « *La fraude au président mêle intelligence économique, espionnage et cybercriminalité. 98% des informations sont accessibles sur Internet, y compris celles classées confidentiel défense. La fraude au président joue sur l'ego de la personne ou consiste à faire preuve d'autorité. Dans une affaire, des délinquants ont résilié l'abonnement téléphonique d'un Pdg pour détourner sa ligne. Le préjudice avait atteint 10M€. La fraude au président a généralement lieu les veilles de week-end. Les failles sont toujours humaines* », précise Xavier Leonetti, substitut du Procureur de la république de Marseille. Cette arnaque représente quelque 300 millions d'euros par an dérobés aux entreprises.

« *Lorsque les sommes sont particulièrement élevées, l'entrepreneur doit toujours vérifier le bénéficiaire du virement par un appel téléphonique* », souligne Bernard Ordines, président de la Chambre transports. Egalement vice-président du Tribunal de commerce de Marseille, il note une montée en puissance de ce type d'affaires. « *Cette menace est prise en compte au niveau européen. La Convention sur la cybercriminalité de Budapest, du 23 novembre 2001, prévoit une série de pouvoirs de procédures, tels que la perquisition de réseaux informatiques et l'interception* », précise le procureur de la République auprès du TGI de Marseille Xavier Tarabeux. Ce dernier vient de confier à Xavier Leonetti, procureur adjoint, la mission de sensibiliser les juges aux cyberattaques.

PHOTO NBDC

Xavier Tarabeux

> **« Lorsque les sommes sont particulièrement élevées, l'entrepreneur se doit de toujours vérifier le bénéficiaire du virement par un appel téléphonique »**
>
> *Bernard Ordines, président de la Chambre Transports au Tribunal de commerce de de Marseille*

PHOTO NBDC

« Il faut savoir identifier le type de menace et de vulnérabilité car le risque évolue constamment. Les entreprises doivent également évaluer l'exposition au cyberisque. Tous les employés doivent être formés au danger potentiel qu'il représente », détaille Nathalie Dumas, experte en transformation digitale et membre élue à la Chambre de Commerce et d'Industrie de Marseille-Provence.

Nathalie Dumas

A compter de mai 2018, entrée en vigueur du RGPD

Malgré une réalité alarmante, les entreprises françaises ne se protègent pas suffisamment et sous-estiment la menace. L'entrée en vigueur en mai 2018 du Règlement européen de protection des données personnelles (RGPD) viendra durcir la responsabilité des entreprises. En cas de vol de données, elles seront soumises à de fortes amendes (4% du chiffre d'affaires mondial du groupe, sous-traitants inclus...) si elles n'en informent pas la CNIL sous 72 heures. Le RGPD impose de notifier aux individus les attaques et renforce le droit des individus à l'oubli au cas où les données personnelles seraient rendues publiques.
Aujourd'hui considérées comme victimes, les entreprises devraient bientôt être perçues comme coupables si elles ne mettent pas en place les mesures nécessaires à la protection de leurs données et de celles de leurs clients. Celles-ci ne se limitent pas à l'aspect technique, mais s'étendent à la communication de bonnes pratiques en interne, avec l'appropriation d'une culture de la sécurité des données au sein de l'entreprise.

Un marché à 20 milliards d'euros

Plusieurs types d'attaques existent visant à récupérer des informations stratégiques afin de les exploiter ou de les revendre (données bancaires, identifiants de connexions à des sites marchands). Le hameçonnage (phishing), la demande de rançon ou « rançongiciel », l'arrêt de l'accès au service (Deny of Service), la webase attack, le maleware, les pièces jointes contaminées sont les modes d'actions les plus répandus.
La cybercriminalité mute à chaque évolution technologique. Lors d'attaques semi-automatiques les virus colportés par les mails, cryptent les données de milliers d'entreprises. Avec la multiplication des supports (tablettes, smartphones, ordinateurs), les cybercriminels bénéficient d'un terrain de jeu encore plus vaste pour sévir.

Quand le Parquet sensibilise les juges au cybercrime

Les adolescents hébergent désormais les milliers de films qu'ils téléchargent illégalement sur les serveurs des entreprises. Cette technique est également largement utilisée par les pédophiles. Ainsi, un chef d'entreprise peut se retrouver mis en cause et arrêté pour possession d'images ou de films à caractère pédophile. Vous imaginez le préjudice moral et réputationnel ? », a expliqué, le 13 mars dernier, Xavier Leonetti, substitut du Procureur de la république de Marseille aux juges consulaires. Cette réunion, initiée par le président du Tribunal Bruno Nivière, visait à sensibiliser et informer les juges sur les nouveaux modus operandi des cybercriminels. Des paiements suspects sur votre relevé bancaire ? Histoire de ne plus se faire pincer, les criminels choisissent désormais de ponctionner 5€. L'opération qui passe inaperçu prend une ampleur phénoménale lorsque des centaines de milliers de personnes sont concernées.

Le procureur adjoint de la République Xavier Leonetti et Bruno Nivière, président du tribunal de commerce de Marseille, lors d'une réunion de sensibilisation des juges aux cyberattaques.

PHOTO NBDC

Le web n'est que le reflet numérique de notre société. Le moteur de recherche Tor vous emmène dans les bas-fonds du web un peu comme si vous marchiez dans un quartier malfamé. Tor rend anonyme la navigation grâce à l'adresse IP qui change en permanence. *« Le dark web est un univers totalement obscur où il est possible d'acheter des numéros de carte bleue, des armes, de la drogue »*, explique Xavier Leonetti.
Un des juges, victime d'un ransomware, avoue avoir failli surfer bien malgré lui sur ce darkNet. Pour récupérer ses fichiers, il devait s'acquitter d'une rançon en bitcoins. *« Je me suis vite ravisé ! J'ai récupéré ma dernière sauvegarde »*, confie-t-il à ses confrères. Comme quoi personne n'est à l'abri, pas même les juges !

Sessions d'information pour les Pme

Pour fournir aux Pme locales, les moyens de se prémunir conte les cyberattaques, la CCI du Var, propose depuis dix ans, des sessions d'information animées par des experts enquêteurs en cybercriminalité de la gendarmerie nationale.

En 2016, un domaine viticole varois a été victime d'un ransomware. Le chef d'entreprise a reçu un mail demandant une rançon. Moyennant le versement d'un million d'euros, il a reçu un mot de passe pour réactiver son système.
« Il ne faut surtout pas payer. Les entreprises doivent réaliser des sauvegardes régulièrement. Le problème peut être réglé en revenant à la dernière sauvegarde », explique Sébastien Bondoux, conseiller numérique à la CCI du Var. Récemment, une franchise implantée dans le Var a été victime de phishing et le virus s'est répandu dans le serveur bloquant tous les accès. *« Nous organisons depuis 2007, des sessions de formation à l'attention des entreprises en partenariat avec le service N-Tech de la gendarmerie nationale dédié à la protection des entreprises et des particuliers contre les cybercriminels »*, précise Sébastien Bondoux.
Si toutes les entreprises sont concernées, le secteur de la Défense dans le Var constitue une cible privilégiée des hackers. Lors de ces réunions qui se tiennent tous les trois mois à Six-Fours, Toulon, Saint-Raphaël, Saint-Tropez et Draguignan, les enquêteurs cybercriminalité de la gendarmerie nationale précisent les actions à mettre en place pour se protéger et la procédure de reprise d'activité en cas d'attaque du système informatique. *« Nous sensibilisons les entreprises à sécuriser leurs données telles que les fichiers clients, les comptes bancaires, les données métiers, les brevets, modèles et marques. Ce peut être les plans d'un architecte »*, détaille Sébastien Bondoux qui organise ces sessions aux côtés de l'Union Patronale du Var et la Gendarmerie Nationale.

L'argent de la cybercriminalité blanchi dans les monnaies virtuelles

Entre 80 et 200 milliards de dollars en bénéfices illégaux de la cybercriminalité sont blanchis chaque année. Ce chiffre alarmant résulte de l'étude « Into the Web of Profit » conduite par Mike McGuire, maître de conférences en criminologie à l'Université de Surrey.

Le rapport, publié le 20 avril 2018, révèle que les produits de la cybercriminalité représentent 8 à 10 % du total des profits illégaux blanchis à l'échelle mondiale. Les monnaies virtuelles sont devenues le principal outil utilisé par les cybercriminels pour blanchir de l'argent. Ces derniers s'éloignent du Bitcoin pour adopter des crypto monnaies moins connues, comme le Monero, pour préserver l'anonymat.

Les achats et les devises inhérents aux jeux en ligne entraînent une augmentation du blanchiment. 10 % des cybercriminels utilisent PayPal pour blanchir de l'argent. 35 % utilisent d'autres systèmes de paiement numérique, notamment Skrill, Dwoll, Zoom et des systèmes de paiement mobile tels que M-Pesa. La Chine et la Corée du Sud deviennent des foyers de blanchiment d'argent.

De nombreux cybercriminels emploient la monnaie virtuelle pour effectuer des achats de biens et convertir ainsi les produits illégaux en argent et en actifs légitimes. Des sites Web tels que Bitcoin Real Estate proposent des appartements en terrasse et des demeures luxueuses en passant par des îles privées de 65 hectares. Il est possible d'acheter ces biens via des bitcoins.

Contrairement aux achats en espèces qui sont soumis à une réglementation et à un contrôle, les biens achetés avec des crypto-monnaies ne font pas l'objet d'un examen aussi approfondi. Selon l'étude, près de 25 % des ventes totales de biens devraient s'effectuer en crypto-monnaies dans les prochaines années. Ceci inquiète les analystes financiers. Ces transactions rapides et discrètes, dont beaucoup ont des origines criminelles, risquent de perturber les marchés immobiliers mondiaux.

PHOTO PIXABAY

Les pirates informatiques, nouveau fléau des mers

Au lendemain du piratage des terminaux informatiques du port d'Anvers par un cartel de la drogue en 2011, l'Agence européenne de cybersécurité, a pris très au sérieux cette menace dans le transport maritime. Pour autant, l'attaque en juin 2017 du virus NotPetya a démontré l'ingéniosité des pirates et la vulnérabilité des installations portuaires.

« Lors de l'attaque du virus NotPetya, nous avons fait le nécessaire pour informer nos clients. Nos systèmes étaient à jour. Avec les objets connectés, nous assistons à une montée en puissance de la délinquance. Les armateurs sont confrontés à la problématique des données embarquées et doivent se protéger des cyberattaques grâce à des systèmes d'information à jour et une politique de mots de passe draconienne », explique Alain Perez, directeur du projet Ci5 et chargé des systèmes d'information de MGI. Pour l'élaboration du cargo community system Ci5, MGI a collaboré étroitement avec Thales Services et l'ANSSI (agence Nationale pour la Sûreté de l'information). Les grands ports maritimes français sont classés par le gouvernement comme des OIV, c'est-à-dire un opérateur d'intérêt vital au vu de leur importance stratégique. Cependant, les cybercriminels peuvent tirer parti de l'instauration du guichet unique (*) concernant les formalités déclaratives applicables aux navires à l'entrée et/ou à la sortie des ports. *« A l'image de l'augmentation des escroqueries, les entreprises du transport maritime sont confrontées à des faux documents pouvant permettre de détourner des conteneurs par exemple »*, précise Xavier Tarabeux, procureur de la République, près le TGI de Marseille.

Le virus NotPetya a paralysé 17 terminaux portuaires d'APMT en juin 2017

PHOTO APMT

Des conteneurs d'olives et d'acier volatilisés

Des conteneurs entiers d'olives expédiés depuis la Provence se sont volatilisés en Angleterre. Cette étrangère affaire, d'un nouveau genre, est arrivée sur le bureau des juges marseillais. Le grossiste local ayant été simplement berné par un mail d'un pseudo client britannique. Une simple lettre du mail habituel de commande ayant été modifiée. *« Cela peut arriver à n'importe qui. Nous avons dû débouter le demandeur qui a perdu sa cargaison »*, explique Bernard Ordines. Le président de la Chambre transport du Tribunal de commerce de Marseille a également été saisi d'affaires de détournements de règlements. *« Un commissionnaire de transports qui devait livrer une quinzaine de conteneurs au Moyen-Orient a sous-traité l'opération à un autre commissionnaire. Un tiers s'est immiscé dans les échanges de mails modifiant le compte bancaire à Taïwan. Le préjudice de cette affaire s'est élevé à 32 000 € et le commissionnaire, responsable de négligence, a été condamné à payer une deuxième fois »*, détaille le juge consulaire. Les sommes dérobées par les faux fournisseurs et clients, peuvent parfois conduire au dépôt de bilan. Des faux connaissements ont également conduit au vol de plusieurs milliers de tonnes d'acier en 2012. Les fraudeurs avaient alors créé une fausse agence bancaire et émis de faux titres de paiement. *« Le destinataire floué en possession des connaissements originaux n'a pas pu récupérer la marchandise. Des centaines de conteneurs ont été dérobés. Ce qui démontre qu'il existe une vraie filière industrielle capable d'acheter de l'acier de contrebande. Le recel n'a pas de limite »*, souligne Bernard Ordines qui enregistre une augmentation des contentieux liés à la cybercriminalité devant les tribunaux.

> ***« Il existe une vraie filière industrielle capable d'acheter de l'acier de contrebande »***

(*) Directive 2010/65/UE du Parlement Européen et du Conseil du 20 octobre 2010

Alain Perez, directeur du projet Ci5 et chargé des systèmes d'information et de l'organisation de MGI.

PHOTO NBDC

Nicolas Swaton

CODIRIGEANT DE LA SOCIÉTÉ DE COURTAGE EN ASSURANCES EUROSUD SWATON

« Les entreprises ont une responsabilité digitale »

PHOTO EUROSUD

Existe-t-il des contrats spécifiques pour se protéger contre les cyberattaques ?

C'est un sujet qui se met progressivement en place. Dans le domaine de la cybercriminalité nous travaillons avec les assureurs anglo-saxons : Hiscox, AIG et AXA. Les Anglais et les Américains ont été précurseurs dans ce domaine. Certains assureurs ajoutent un volet cybercrimininalité dans leurs contrats. Il y a une partie assurance contre les dommages en cas d'attaque et une partie responsabilité civile pour les dommages causés à autrui. 2018 sera l'année de la cybercouverture !

Que se passe-t-il en cas de cyberattaque ?

Une expertise évalue les frais de réparation, de restauration des données. La police d'assurance dépend des capitaux assurés, du chiffre d'affaires de l'entreprise et de son exposition au risque. Les contrats couvrent la fraude interne ou externe à l'entreprise.

Quel est le profil des entreprises qui se couvrent ?

Les grandes entreprises sont couvertes à près de 80%. En revanche, les Pme sont moins vigilantes et sont exposées aux ransomware, intrusions, vols d'informations. Elles n'ont pas pris réellement la mesure de la nécessité de se couvrir mais avec l'entrée en vigueur du RGPD, les pénalités seront très sévères. Les entreprises ont une responsabilité digitale.

L'ANSSI publie un guide pour les entreprises :

https://www.ssi.gouv.fr/actualite/charte-dutilisation-des-moyens-informatiques-et-des-outils-numeriques-le-guide-indispensable-pour-les-pme-et-eti/

La CNIL explique comme se préparer au RGPD :

https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes