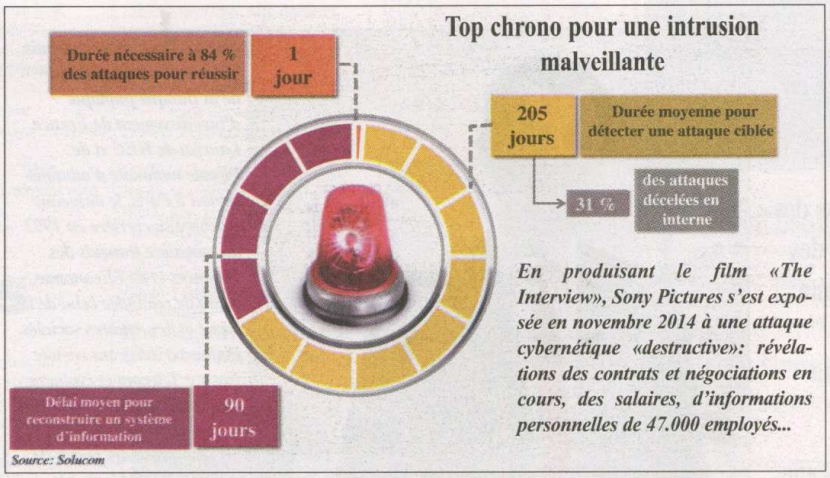
ENTREPRISES

Attention à la prise en otage numérique

- **Attaque cybernétique: Rançon contre données**
- **Mesures d'hygiène pour le système d'information**



En produisant le film «The Interview», Sony Pictures s'est exposée en novembre 2014 à une attaque cybernétique «destructive»: révélations des contrats et négociations en cours, des salaires, d'informations personnelles de 47.000 employés...

«LE retour de la menace diffuse». Tel pourrait être l'intitulé d'un film de série Z. Or c'est plutôt l'un des trois types d'attaques cybernétiques alerte Fréderic Goux, expert en sécurité informatique chez Solucom. Quitte à vous inquiéter encore plus, «la tendance ira crescendo dans les années à venir», pronostique vendredi dernier à Casablanca l'invité de la Chambre française de commerce et d'industrie du Maroc. Particuliers et entreprises risquent de se faire voler leurs données privées ou professionnelles. Les banques restent une cible de choix: «près de 2 millions de malwares financiers déjoués en 2015», annonce Kaspersky Lab (voir ci-dessous). Les hackers utilisent un hameçon informatique, the phishing. Envoi d'un email «anodin» d'abord. En l'ouvrant, la cible donne accès à «des petits logiciels espions» sur son PC. L'intrusion se propage ensuite aux autres postes de travail. Puis capture et analyse des documents sensibles et stratégiques. «Serveurs et PC sont cryptés et vos données deviennent illisibles. Ransomwares et autres cryptolokers engendrent la perte d'accès aux fichiers et une désorganisation de l'entreprise. Un tiers des directions des systèmes d'information sont touchées», déclare l'expert en s'appuyant sur des données de Webroot, société US de sécurité sur internet.

Une vraie prise d'otage numérique commence. Remise d'argent contre remise de données. «Sinon, vous les perdez à jamais», menacent les pirates. Un compte à rebours s'affiche alors sur les écrans! Une vraie mise en scène pour une activité très lucrative: «300 dollars par menace». Il ne reste plus qu'à la multiplier par cent, par mille... Le plus cocasse dans l'histoire? Le paiement se fait aussi par bitcoin. Le recours à une monnaie virtuelle rend la filature des malfrats quasi-impossible. De quoi compliquer l'imbroglio judiciaire. Car l'attaque est transfrontalière: faite au Maroc via la France en passant par le Mexique et le Vietnam! Victime et enquêteurs finissent par abandonner face aux méandres des réseaux et de la coopération judiciaire parfois. Que faire?

Prévenir vaut mieux que guérir. Fréderic Goux, ingénieur en télécom, insiste sur «la bonne hygiène des systèmes d'informations: correctifs, antivirus, droits...». Sauvegarde régulière des données et déconnexion rapide des postes permettent aussi de limiter les dégâts en cas d'attaque. Ceux qui cherchent à savoir le coût d'un exercice de cyber-attaque resteront sur leur fin: «20 jours de charge» pour une PME. Mounim Zaghloul, DG de Consilium, est plus explicite. «En moyenne, entre 4.000 et 5.000 DH par jour», confie-t-il à L'Economiste. Pour une entreprise, revoir la protection des données critiques s'impose. Un ciblage préalable et hiérarchisé est une évidence. Au même titre que la sensibilisation et la responsabilisation de tous les intervenants. A garder en tête: «Passer d'un modèle historique de protection, le château-fort, à un modèle ouvert, celui de l'aéroport», conseille Solucom. Plus vous accédez aux espaces sensibles, plus la sécurité augmente. Avec une tour de contrôle qui veille en permanence. Et ce n'est pas de la science-fiction! ❑

Faiçal FAQUIHI

Pour réagir à cet article: courrier@leconomiste.com

Le braquage virtuel des banques se popularise

LE secteur financier est une cible de choix. Kaspersky Lab annonce dans son bulletin sur la sécurité en 2015 «avoir déjoué des tentatives d'exécution de malwares conçus pour voler l'argent via les systèmes de banques électroniques sur les ordinateurs de 1,9 million d'utilisateurs. Soit une hausse de 2,8% par rapport à 2014». L'éditeur russe d'antivirus a établi une répartition géographique planétaire des malwares financiers. Ses calculs sont basés sur «le pourcentage d'utilisateurs de nos produits dans chaque pays»: 2 à 4 % au Maroc.

«Rares et pointues», les attaques retentissantes sont surtout liées à un contexte géopolitique. «Le gain financier figure, avec l'idéologie, parmi les motivations des cybers-attaques», assure Frédéric Goux, directeur-associé à Solucom. Carbanak est apparu en 2013. Ce virus a infiltré les distributeurs de billets: «Une dizaine de banques et d'institutions financières ont enregistré des pertes entre 2,5 millions et 10 millions de dollars», selon l'expert en sécurité informatique. D'après Verizone, tous les secteurs sont touchés: banque-assurance arrive en premier (36%), distribution (24%). Services et industrie également victimes d'intrusions malveillantes en 2013. «Nous sommes tous sujets à des attaques», commente avec justesse André Robelin, président de la commission appui aux entreprises à la Chambre française de commerce et d'industrie du Maroc. TV5 en a fait les frais la nuit du 8 avril 2015. «Le Groupe OCP, qui est une émanation de l'Etat (marocain), ou les banques sont des cibles. Cela viendra: plus les procédures se dématérialisent, plus le risque augmente», estime sans gêne l'expert français. Sara Mekouar, chef d'une agence de voyage, témoigne: «75.000 DH sont partis dans la nature». Sa plainte chez la police est «toujours sans réponse». Les pirates informatiques ne font pas de différence entre petites et grandes entreprises. Pourvu qu'il y ait un gain aussi minime soit-il.❑