Les essentiels d'Euler Hermes 2018

Cyberfraude : la grande menace

Les nouvelles tendances de la cybercriminalité

www.eulerhermes.fr

EULER HERMES

Sommaire

1 Éditorial

En quelques années, la cyberfraude a pris une nouvelle dimension. Elle est désormais le fait, non plus d'individus isolés, mais de véritables bandes organisées, qui y ont trouvé un relais de croissance bien moins dangereux, mais tout aussi profitable pour elles, que leurs activités criminelles traditionnelles.

Le monde des affaires est en réseau, les échanges se sont dématérialisés, et les technologies de l'information constituent la colonne vertébrale des organisations. Les fraudeurs ont suivi ce mouvement et multiplié les armes pour attaquer les entreprises quelle que soit leur taille. La dimension cyber est venue s'associer aux techniques éprouvées d'usurpation d'identité, permettant de construire des scénarios d'escroquerie encore plus solides, ou de développer des attaques plus massives.

Le risque s'est diversifié. La trésorerie, l'exploitation, les résultats, mais aussi la réputation, sont en danger. La RGPD, si elle contribue à responsabiliser les entreprises quant à la collecte et à la protection des données personnelles, y ajoute désormais un risque règlementaire très lourd.

Plus que jamais, il est indispensable de protéger son entreprise par tous les moyens. Nous avons conçu ce dossier pour vous aider à maîtriser et à communiquer les enjeux de la cyberfraude aujourd'hui, mais aussi pour vous proposer des solutions.

Sébastien Hager
Responsable Souscription Assurances Fraudes,
Euler Hermes France

2 La cyberfraude, un phénomène plus que jamais d'actualité

La cyberfraude a rejoint la fraude au fournisseur au triste hit-parade des fraudes aux entreprises (étude DFCG/Euler Hermes, Mars 2018). Ses ravages se comptent en milliards d'euros, d'après le Parquet de Paris – et au niveau mondial, elle génère des profits supérieurs au trafic de stupéfiants, d'après Interpol. Grandes entreprises, PME, artisans, particuliers, gouvernements, administrations, chacun d'entre nous court aujourd'hui le risque d'une attaque qui peut mettre en danger ses finances, sa réputation, et parfois même son existence.

Des chiffres qui font froid dans le dos

- **600 milliards de $**
  Coût annuel de la cybercriminalité = 0.8% du PIB mondial
  Center for Strategic and International Studies

- **40 Secondes**
  La fréquence des attaques par ransomwares sur les entreprises
  2017, *Association of Certified Fraud Examiners* (ACFE)

- **250,000,000 €**
  La perte d'exploitation indiquée par Saint-Gobain suite aux cyberattaques subies par l'entreprise en 2017

- **500 000 ordinateurs**
  ont été infectés par Avalanche, un réseau pirate, grâce à l'envoi de courriers frauduleux

- **20 millions d'euros**
  Amende maximum pour les entreprises qui n'auraient pas respecté les règles de collecte et de conservation des données personnelles des tiers

Top 5 des tentatives de fraudes

54%	50% (dont 20% d'attaques au ransomware)	43%	42%	35%
Fraude au faux fournisseur	Cyber-criminalité	Autres usurpations d'identité (banques, avocats...)	Fraude au faux président	Fraude au faux client

DFCG/Euler Hermes 2018 - "La fraude, un phénomène en voie de professionnalisation"

Une menace difficile à maîtriser

« *L'expertise des cybercriminels est vraiment pointue et les types de menaces sont toujours plus difficiles à détecter* », déclarait récemment Éric Freyssinet, conseiller auprès du Préfet en charge de la lutte contre les cybermenaces au ministère de l'intérieur.

Les fraudeurs disposent en effet, d'un arsenal à large spectre leur permettant de conduire leurs attaques avec les meilleures probabilités de réussite. Les grandes catégories de menace sont actuellement les suivantes :

Ransomwares

Une cyberfraude sur 5 a été le fait d'un ransomware, d'après l'étude DFCG/Euler Hermes 2018. Le cryptage des données qui résulte d'une attaque par ransomware est susceptible de paralyser l'exploitation, voire de mettre en danger l'entreprise si sa politique de sauvegardes n'était pas à la hauteur.

Vol de données

S'introduire dans les systèmes d'information pour y voler des données confidentielles constitue un classique de l'espionnage industriel. Fichiers clients, fichiers fournisseurs, fichiers du personnel et secrets de fabrication peuvent faire l'objet d'une véritable guerre de l'ombre dont les conséquences sont lourdes : perte de compétitivité, détournement de clientèle, pertes de contrat…

Chantage à la réputation

Après avoir dérobé des fichiers, les fraudeurs menacent leur propriétaire de les publier sur le web, les rendant accessibles à tous – médias, concurrents, salariés, administrations, etc. C'est le doxing qui rend vulnérables à l'usurpation d'identité des tiers dont l'entreprise détenait des données personnelles.

Chantage à la conformité

En menaçant de rendre publiques ces données personnelles, les cybercriminels mettent en danger la conformité de l'entreprise à la RGPD. Or la société qui aurait mal protégé ces données, ou qui aurait tardé à annoncer l'attaque dont elle a été victime, peut faire l'objet de lourdes amendes : jusqu'à 150,000 € au premier manquement, et ensuite jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial du dernier exercice clos.

> "Le RGPD a réveillé les consciences des entreprises quant à la sécurisation de leurs données"

Sébastien Hager, Euler Hermes

Première sanction pour infraction à la protection des données personnelles

Le 18 juin 2018, la société Optical Center a été sanctionnée par la CNIL d'une amende de 250,000 € pour une « fuite de données conséquente » suite à une faille de sécurité datant de 2017.
Trois millions de dossiers ont été téléchargés depuis le site du commerçant.
Si la fuite avait eu lieu après la mise en application de la RGPD, l'amende aurait pu atteindre 20 millions d'euros.

Les Cyber-fraudeurs ont changé

Les fraudeurs sont en pleine transformation numérique, rappelle Tanguy de Coatpont, Directeur Général de Kaspersky Lab France. Le hackeur indépendant d'autrefois a laissé le clavier aux mains de véritables entrepreneurs du crime, bien décidés à réaliser de coquets bénéfices. Il n'y a plus de pirates en solo, et l'on parle désormais de « groupes » criminels – Lazarus, Carbanak, Avalanche… Autant d'organisations qui s'appuient sur un véritable business model, avec une vision extrêmement ROIste ! Ils font appel à la sous-traitance, et proposent maintenant des plates-formes de Malware as a Service, qui mettent à disposition outils et campagnes d'attaque, prêts à l'emploi… et même parfois rémunérés à la performance.

« La criminalité traditionnelle a compris l'intérêt de la cybercriminalité, et les bénéfices qu'ils pouvaient en tirer. On trouve une composante cyber de plus en plus présente dans les schémas classiques d'usurpation d'identité. Car aujourd'hui les fraudeurs ne fouillent plus les poubelles de l'immeuble… Ils louent les services de petits cybercriminels, recrutés sur internet, qui leur donneront accès aux informations qu'ils convoitent », témoigne encore Tanguy de Coatpont.

> "La criminalité fait sa transformation numérique"
>
> Tanguy de Coatpont, Directeur Général de Kaspersky Lab France

3 Les dimensions du danger

L'activité des cyberfraudeurs met les entreprises en danger. Ce qui les intéresse ? Le cash ! Pour ces professionnels, tous les moyens sont bons pour s'enrichir – en particulier ceux qui ne leur font courir qu'un risque relativement faible par rapport à leurs activités criminelles traditionnelles.

Le détournement de fonds ou de marchandises

Les cyberfraudeurs ont développé une expertise quant à la manière dont sont gérées les transactions financières. Leur objectif est d'opérer un transfert de fonds. Parmi les scénarios possibles : l'intrusion dans un système d'achats pour détourner les règlements destinés aux vrais fournisseurs. Ou dans un SIRH pour créer des employés fictifs et générer les fiches de paie et les versements correspondants. Ou encore : hacker les systèmes d'un entrepôt et faire envoyer des marchandises de valeur à une adresse complice.

Le vol ou la compromission de données

Dans un monde de plus en plus numérique, les actifs immatériels ont pris une grande valeur. Par exemple, selon une analyse du cabinet américain Gartner, publiée début novembre 2017, la capitalisation boursière d'une entreprise qui exploite intelligemment ses données serait trois fois supérieure à la moyenne. Sans parler des nombreuses start-up, à la valorisation spectaculaire, dont les business modèles sont entièrement fondés sur l'exploitation des données de leurs utilisateurs.

En volant, en détruisant, ou en bloquant l'accès aux données via l'usage d'un cryptologiciel, les cybercriminels montrent qu'ils ont eux-aussi compris les enjeux des entreprises d'aujourd'hui. Leur objectif : vendre ces données sur un marché parallèle, ou obtenir une rançon – à moins qu'ils n'agissent pour le compte d'une autre organisation – Etats ou concurrents sans scrupules.

Le blocage de l'exploitation

Bloquer la production est un puissant levier de chantage, car les conséquences peuvent s'avérer très importantes. Le fabriquant de matériaux Saint-Gobain a indiqué dans son rapport annuel avoir perdu en 2017 pas moins de 250 millions d'euros de chiffre d'affaires – soit 1,1% de ses ventes. Rien que sur le premier semestre, l'impact négatif de la cyberattaque (via le ransomware NotPetya) sur le résultat d'exploitation a été évalué par l'entreprise à 80 millions d'euros, soit 4,4% du résultat d'exploitation. La compagnie maritime danoise Maersk a annoncé une perte de revenus de 300 millions de dollars à cause du ransomware Petya. Le groupe de distribution Auchan, le fabricant d'emballages en verre Verallia, les hôpitaux britanniques, BNP Paribas, le groupe pharmaceutique Merck, le port de Barcelone, mais aussi des dizaines de milliers de petites entreprises, ont été atteint à travers le monde.

La perte de réputation

Une conséquence particulièrement grave de la cyberfraude est la perte de réputation. Selon le cabinet Deloitte, 25% de la valeur d'une entreprise est liée à sa réputation. Alors si le doute s'installe quant au soin mis par leur fournisseur, leur employeur ou leur réseau social favori, à protéger les données des tiers, tout peut arriver. Pour ne citer qu'un exemple : après le scandale Cambridge Analytica (une firme britannique d'analyse de données qui avait pu récupérer des informations sur 87 millions d'utilisateurs du réseau social sans leur consentement), le cours de Facebook a reculé de 11% en quelques jours – pour près de 60 milliards de dollars.

Les dirigeants ne s'y trompent pas, puisqu'ils sont 56% à craindre de perdre la confiance de leurs clients, et 52% de voir leur réputation souffrir (Global Threat Intelligence Report Vanson Bourne/NTT)[1].

> "Nul homme, après avoir perdu l'estime des autres, n'a droit de se plaindre de la méfiance qui la lui rend si difficile à recouvrer"
>
> Pierre Choderlos de Laclos (Les Liaisons dangereuses)

(1) https://www.nttsecurity.com/en-bnl/landing-pages/risk-value-2018

La responsabilité des dirigeants

L'ampleur des conséquences potentielles d'une cyberfraude réussie conduit inévitablement à des remises en cause. Les dirigeants avaient-ils suffisamment investi dans la prévention ? La direction des systèmes d'information avait-elle mis en place les systèmes appropriés, tenu à jour les logiciels ? Les process étaient-ils les bons ? Ont-ils été correctement exécutés ? Le programme de formation interne était-il à la hauteur ?

Autant d'interrogations qui peuvent entrainer des conséquences professionnelles – et humaines – à tous les niveaux.

4 Les mécaniques de la cyberfraude

Fraude externe et cyberfraude sont désormais presque toujours associées. Car pour générer des profits décrits par Interpol[2] comme supérieurs au trafic de stupéfiants, les criminels utilisent les méthodes et les moyens des professionnels d'aujourd'hui. Une raison supplémentaire pour connaître – et contrer – les mécaniques les plus souvent employées.

> "Aujourd'hui, nous voyons des réseaux cybercriminels très complexes réunir des individus venus du monde entier, en temps réel, pour commettre des crimes à une échelle sans précédent. Les organisations criminelles se tournent de plus en plus vers internet pour faciliter leurs activités et maximiser leurs profits le plus rapidement possible. Les crimes eux-mêmes ne sont pas nécessairement nouveaux : le vol, la fraude, le jeu illégal, la vente de faux médicaments… Mais ils évoluent en même temps que les opportunités, devenant ainsi plus répandus et plus dévastateurs."

Rapport Interpol 2017

(2) https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

La recherche robotisée de la faille

Les cybercriminels déploient des automates pour scanner le web et repérer les cibles les plus vulnérables. Comme l'explique le DSI de l'éditeur Cegid, Sylvain Moussé : « Leurs robots scannent sans relâche l'internet visible et invisible à la recherche des failles de sécurité connues. Les entreprises qui n'auraient pas appliqué les correctifs les plus récents seront attaquées en priorité. » De fait, on estime qu'une grande partie des cyberattaques avérées ont exploité des faiblesses de logiciels ou de matériels, qui auraient pu être protégées si elles avaient bénéficié des correctifs (les patches mis à disposition par les éditeurs).

Le phishing

Un simple clic sur une pièce jointe déguisée en fichier banal, portée par un e-mail ordinaire, suffit à faire entrer sur un ordinateur un malware discret (appelé parfois « cheval de Troie »). Une fois dans la place, les fraudeurs vont pouvoir déclencher toutes sortes d'actions : espionnage, encryption, destruction de données, ou encore détournement d'une partie de la puissance machine pour « miner » de la cryptomonnaie à l'insu de l'entreprise.
Au deuxième trimestre 2018, les solutions anti-phishing de Kaspersky Lab ont détourné plus de 107 millions de tentatives d'attaques par phishing.

Phishing et fraude à la livraison

7 escrocs ont été arrêtés en décembre 2017, accusés d'avoir perpétré une campagne de phishing à l'encontre de clients de l'enseigne Cdiscount. Pas moins de 491 clients ont subi près de 350 000 euros de préjudice. « *Les malfaiteurs, après avoir récupéré les identifiants du compte de la victime, changeaient l'adresse de livraison* », explique Frédéric Fraisse, analyste en cybercriminalité à la Direction Centrale de la Police Judiciaire.

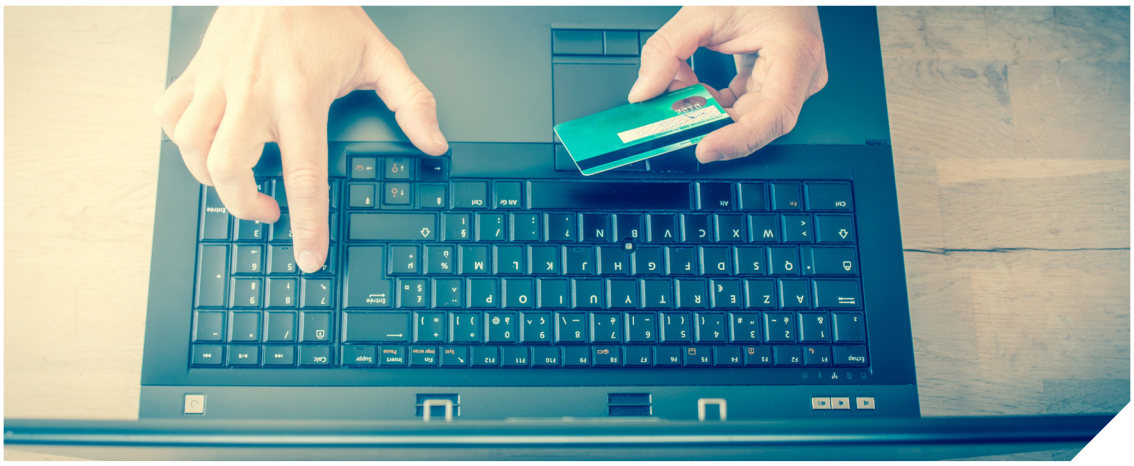
Le ransomware

Un malware introduit lors d'une action de phishing réussie déclenche le cryptage des données d'une machine, et est susceptible de remonter jusqu'aux serveurs de l'entreprise. L'utilisateur est alors confronté à un message lui enjoignant de verser une rançon pour récupérer ses données – des rançons qui vont d'environ 500 euros jusqu'à plusieurs Bitcoins (NB : au 10 octobre 2018, 1 Bitcoin = 5750 €). Les clés de chiffrement utilisées (256 bits) s'avèrent extrêmement résistantes.

Les deux dernières années ont été marquées par l'explosion des ransomwares. Cependant, d'après le spécialiste de la sécurité informatique Kaspersky Lab, les attaques par ransomwares ont baissé de 30% en volume au cours des 12 derniers mois, au profit d'autres techniques.

Ingénierie financière et usurpation d'identité

La délinquance astucieuse, ou fraude à l'ingénierie financière, est réservée à des attaques plus ciblées. Il s'agit de poser des sondes capables d'écouter et de rapporter les éléments clés qui serviront à customiser un scénario d'usurpation d'identité : noms et habitudes du dirigeant pour préparer une fraude au président, liste des fournisseurs pour mettre sur pied un détournement de virement ou de marchandises, fichier du personnel, des clients… L'espionnage des messageries en est la cause.



Doxing et chantage

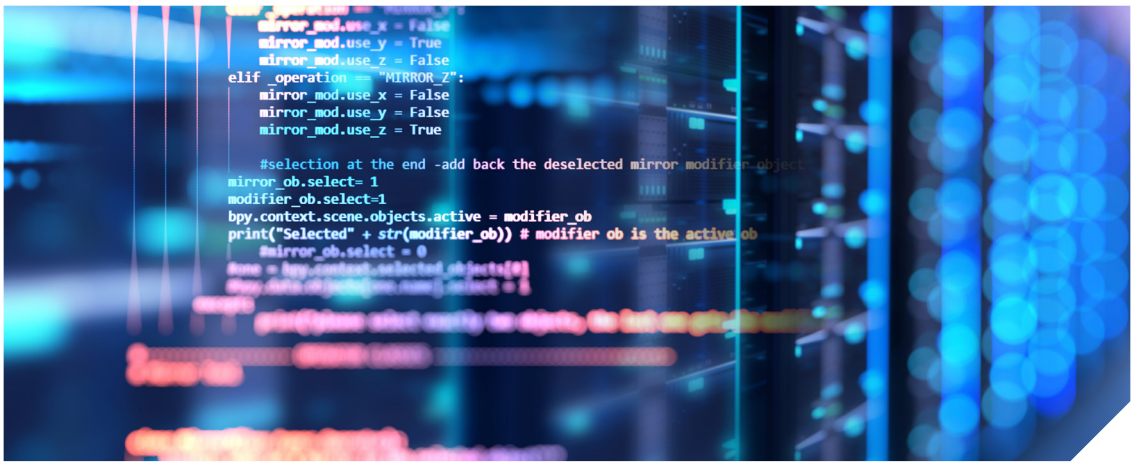
Le doxing, ou doxxing, consiste à rendre publiques sur internet des informations personnelles volées sur les serveurs, les PC ou même les Smartphones. Ces informations tiennent en général à l'identité, l'adresse, le numéro de sécurité sociale, les coordonnées bancaires, les identifiants sur les réseaux sociaux, les mots de passe… En menaçant l'entreprise de rendre, par la divulgation de ces éléments, ces clients vulnérables à l'usurpation d'identité, voire au harcèlement en ligne, les fraudeurs disposent d'un puissant outil de chantage.
Fin 2014, Yahoo a confirmé avoir subi le vol des données personnelles de 500 millions de comptes…

Un levier d'intimidation encore renforcé par la RGPD et les sanctions lourdes qui découleraient d'une mauvaise protection de données, ou du retard pris à faire l'annonce de leur vol.

Le cryptojacking

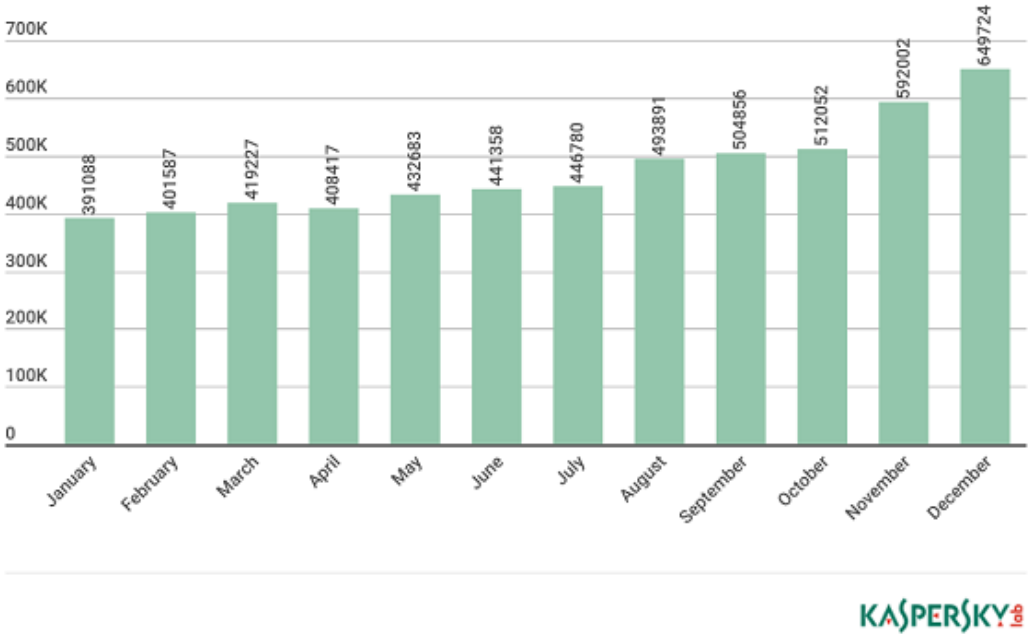
Le cryptojacking consiste à détourner la puissance de calcul d'ordinateurs et de serveurs tiers pour miner de la cryptomonnaie. Ce parasitisme connait une importante progression en 2018 : +44,5%. Un succès qui s'explique par différents facteurs. « Avec un ransomware, un fraudeur peut espérer obtenir une rançon dans 3% des cas. Avec le cryptojacking, 100% des machines infectées vont travailler pour le compte du hackeur », déclare Alex Vaystikh, CTO de SecBI.

Si apparemment cette pratique ne met pas en danger immédiat l'entreprise victime, il ne faudrait pas pour autant la prendre pour valeur négligeable. Elle entraîne des surcoûts – achat et entretien de serveurs supplémentaires pour compenser des performances du système d'information en baisse, consommation électrique en hausse… et surtout la présence d'un élément extérieur infiltré dans les systèmes, capables de déclencher d'autres types d'agression.



Le cryptojacking en forte hausse

Nombre de clients Kaspersky touchés par un malware de type cryptominer en 2017.



Le rapport de la DGSI

La Direction Générale de la Sécurité Intérieure souhaite sensibiliser les entreprises sur des actions d'ingérence économique qui réclament une attention particulière.

Parmi les dangers étudiés, outre les ransomwares, figurent :

- **Les risques liés aux prestataires et aux sous-traitants,**
- **Le risque généré par le manque d'encadrement des stagiaires au sein des structures publiques et privées,**

4 Les mécaniques de la cyberfraude

- **Les déplacements à l'étranger, un risque important de captation d'informations,**
- **Les risques liés à l'hébergement des données dans les data centers et les clouds,**
- **Les dangers liés aux objets connectés,**
- **Les dangers liés au WiFi public.**

La DGSI invite toutes les entreprises à mettre en action une véritable politique de sécurité, tant les sources du danger cyber sont aujourd'hui diversifiées.

5 La prévention, indispensable … et insuffisante

S'il n'y a pas de sécurité absolue, en matière de données comme ailleurs, il est aussi exact que les malfaiteurs s'attaquent en priorité aux proies les plus fragiles ; chaque entreprise doit donc s'armer pour ne pas être de celles-là.

Vigilance informatique, process de sécurisation des virements, double signature, sensibilisation et formation internes, responsabilisation des sous-traitants et partenaires, font partie de l'indispensable politique de prévention.

Former tous ses collaborateurs

Il suffit d'un maillon faible pour contaminer la chaîne de données. Tout commence donc par l'éducation de l'ensemble des collaborateurs de l'entreprise, au-delà des services financiers. La formation se doit en outre d'être régulièrement renouvelée, pour parer aux effets du turn-over, et mettre à jour les connaissances.

5 La prévention, indispensable… et insuffisante

Un excellent moyen de faire progresser le niveau de vigilance interne est de procéder à des tests réguliers de résistance, tant au niveau de l'informatique qu'à celui des utilisateurs. Comme dans toute démarche pédagogique, le débriefing contribuera largement à la réussite de l'opération ; il permet d'expliquer les mécaniques employées, de montrer les pièges, et d'apprendre à chacun à développer sa conscience du danger.

Protéger ses messageries

C'est la plupart du temps par les messageries que passent les cybercriminels. La protection des messageries est donc absolument indispensable. « Les e-mails constituent le premier vecteur de compromission des systèmes d'information », précise Tanguy de Coatpont, directeur général de Kaspersky Lab France, spécialiste de la sécurité informatique, qui ajoute « en mai 2018, 51% du trafic mondial d'internet était du SPAM. Des e-mails bien souvent porteurs de pièces jointes ou de liens malveillants. Beaucoup tombent encore dans le piège. » La lutte contre le SPAM représente donc un élément important de la politique de prévention.

Faire usage du cloud

L'externalisation des données via le cloud permet de mutualiser les investissements nécessaires à un niveau de sécurité à la hauteur des risques, ainsi que sa maintenance. Le cloud permet aussi de garantir une mise à jour permanente des applications pour ne pas laisser de faille ouverte à une intrusion malveillante. Mais même le meilleur opérateur de cloud ne peut pas, lui non-plus, garantir un risque zéro. L'attaque par ransomwares des opérateurs cloud a d'ailleurs été classée par le MIT en janvier dernier parmi les 6 principales menaces pour les entreprises…

L'intelligence artificielle au secours de la sécurité

Aujourd'hui, seulement 3 % des fraudes en entreprise sont découvertes grâce à des techniques analytiques, selon une étude de KMPG. Pire ? Une enquête du Ponemon Institute-Service Now, publiée en avril 2018, a révélé que 54 % des entreprises françaises estiment que les pirates maîtrisent mieux qu'elles des technologies telles que l'apprentissage automatique (Machine Learning) et l'intelligence artificielle.

Pourtant, on est en droit d'attendre beaucoup de l'intelligence artificielle quand il s'agit de sécuriser son entreprise et ses données. Par exemple, il est devenu facile de détecter des comportements non logiques lors d'une tentative d'accès. Le moyen le plus utilisé aujourd'hui est le « voyage impossible ». Si vous vous êtes connectés à La Défense à 14:00, il est impossible que vous vous connectiez depuis Perpignan à 15:00. Le système peut alors réclamer un deuxième facteur d'identification, tracer la tentative de connexion, voire lancer une équipe d'intervention.

5 La prévention, indispensable… et insuffisante

Selon Laurent Benoit, manager sécurité d'Avanade France, il est déjà possible d'aller plus loin : « Avec un minimum de temps d'apprentissage, nous pouvons aussi demander au logiciel d'accès de reconnaître votre façon de taper sur votre clavier, et donc de savoir si c'est bien vous qui saisissez votre mot de passe sur votre ordinateur. L'IA est aussi capable d'aller plus loin dans l'analyse des comportements en allant plus « bas » dans les couches de vos systèmes, et de traquer n'importe quelle trace d'activité non logique dans un traitement informatique (est-ce normal que ce programme tente une connexion avec un compte système alors que son travail est d'afficher la vitesse d'un ventilateur ?). » D'autres systèmes de sécurisation issus de l'IA sont déjà en développement.

Ces nouvelles perspectives en matière de sécurité ne doivent pas faire oublier les fondamentaux. Pour protéger son entreprise, un process de sécurisation des virements, une gestion correcte des mots de passe, et la mise en place d'un plan d'urgence et de gestion de crise, sont absolument indispensables.

6 7 bonnes raisons de s'assurer contre la fraude et la cyberfraude

Voici 4 ans, 81% des entreprises ignoraient l'existence de solutions d'assurance dédiées ; aujourd'hui la moitié d'entre elles sont assurées ou considèrent l'assurance comme un élément de la démarche de prévention », rappelle Sébastien Hager, Responsable Souscription Assurances Fraude chez Euler Hermes.

Voici 7 bonnes raisons d'assurer contre les fraudes son exploitation, ses données et sa réputation.

1. **7 entreprises sur 10** ont subi au moins une tentative de fraude en 2017 ; **1 sur 2 était d'origine cyber**, selon le baromètre DFCG/Euler Hermes 2018.

2. **Les sommes en jeu sont importantes :** le préjudice financier peut mettre en danger la trésorerie, voire la survie de l'entreprise.

6 7 bonnes raisons de s'assurer contre la fraude et la cyberfraude

3 **Le lien étroit entre cyberfraudes et fraudes externes.** Les fraudeurs espionnent les messageries pour monter des scénarios d'usurpation d'identité de plus en plus crédibles. Par conséquent, une assurance qui ne couvrirait que les risques cyber s'avérerait en-dessous des enjeux – l'inverse est vrai aussi !

4 **La diversité des menaces implique une vigilance à 360°.** Fraudes aux fournisseurs, ou détournement de virement. Fraude au président. Faux clients, fausses adresses de livraison. Fausse administration, faux informaticiens, faux avocats, faux banquiers… sans oublier la fraude interne, toujours d'autant plus dangereuse qu'elle met en moyenne 18 mois pour être découverte. Difficile de conserver sa vigilance 24/7, surtout sans développer pour autant une paranoïa nuisible à la qualité de vie au travail..

5 **La créativité des fraudeurs.** De nouvelles techniques, de nouveaux outils d'attaque, sont mis au point tous les jours par des groupes criminels qui savent où investir pour tromper les efforts. Dans ces conditions, qui pourrait garantir une sécurité informatique à 100% ?

6 **La professionnalisation des fraudeurs.** S'ils n'ont pas plus de scrupules que leurs homologues du crime classique, les cyberfraudeurs savent utiliser toutes les ressources de la technologie. Eux-aussi commencent à s'intéresser de près à l'intelligence artificielle, pour mieux repérer leurs cibles et mieux tromper leurs victimes…

7 **Il n'y a pas de cible négligeable.** Les plates-formes de Cybercrime-as-a-Service offrent aux petits délinquants un arsenal d'outils destinés à compromettre les données et la trésorerie des PME, des TPE, et même des particuliers. Autrement dit : ce n'est pas parce que l'on est petit que l'on est à l'abri !

7 Protéger son entreprise avec Euler Hermes

EH Fraud Cover

EH Fraud Cover garantit les pertes consécutives à une fraude, qu'elle soit commise par un employé, par un tiers, ou cyber, ainsi que certains frais induits :

- Restauration/décontamination de données,
- Coûts du prestataire consécutifs à une cyber-extorsion,
- Notification en d'atteinte aux données,
- Les frais supplémentaires d'exploitation engagés pour maintenir l'activité,
- Les pertes d'exploitation en cas d'interruption d'activité,
- Frais consécutifs à une intrusion dans les systèmes de téléphonie,
- Rétablissement d'image,
- Procédures judiciaires.

EH Fraud Cover permet de bénéficier d'un accompagnement personnalisé. L'indemnisation est versée dans les 30 jours après accord sur son montant.

Pour en savoir plus sur cette solution, rendez-vous sur notre site :

www.eulerhermes.fr

EH Fraud Reflex

Spécialement conçu pour les petites entreprises ayant leur siège en France et réalisant moins de 10 millions d'euros de chiffre d'affaires, EH Fraud Reflex est accessible à partir de 75 euros par mois. La souscription s'effectue en ligne, sans audit préalable. Trois niveaux de couverture sont proposés. L'assurance est sur-mesure avec une couverture, une franchise et une durée personnalisées et modulables.

Cette assurance couvre les conséquences des fraudes et cyberfraudes. Elle garantit une indemnisation rapide des pertes financières directes ainsi que certains frais induits :

- Restauration/ décontamination des données,
- Coûts du prestataire consécutifs à une cyber-extorsion,
- Frais consécutifs à une intrusion dans les systèmes de téléphonie.

Pour en savoir plus sur cette solution, rendez-vous sur notre site :

EHFraudereflex.fr

Euler Hermes

Euler Hermes est le leader mondial des solutions d'assurance-crédit, et le leader européen de l'assurance fraude.

Avec plus de 100 années d'expérience, Euler Hermes offre une gamme complète de services pour la gestion du poste clients et la protection des actifs de l'entreprise. Euler Hermes garantit plus de 890 milliards d'euros de transactions commerciales dans le monde.

Assurance

Euler Hermes France
Succursale française d'Euler Hermes SA
RCS Nanterre B 799 339 312

Délivrance de garanties et surveillance de la situation financière des entreprises

Euler Hermes Crédit France
Société par actions simplifiée
au capital de 51 200 000 EUR
RCS Nanterre B 388 236 853
Société de financement soumise au CoMoFi

Recouvrement

Euler Hermes Recouvrement France
Société par actions simplifiée
au capital de 800 000 EUR
RCS Nanterre B 388 237 026

Euler Hermes France / Euler Hermes Crédit France / Euler Hermes Recouvrement France
Adresse postale : 1, place des Saisons - 92048 Paris La Défense Cedex - Tél. + 33 1 84 11 50 50 - www.eulerhermes.fr
Euler Hermes SA
Entreprise d'assurance belge agréée sous le code 418
Siège social : avenue des Arts 56 -1000 Bruxelles, Belgique - Immatriculée au RPM Bruxelles sous le n° 0403 248 596

Plus d'informations ?

Contactez-nous au : **01 84 11 50 54**
ou consultez notre site : **www.eulerhermes.fr**