INTELLIGENCE DATA INNOVATION

Un énorme scandale va secouer le monde de la cybersécurité et de la data-gouvernance

Plagiat
Contrefaçon
Copie servile

Des soupçons,
des informations discrètes,
de la délation
commencent à apparaître
dans le paysage informatique,
des technologies de
l'information.

Cela touche entre-autre la
cybersécurité
et de la data-gouvernance

L'écosystème de la donnée
va connaître des
chamboulements

Plagiat et contrefaçon dans le domaine des technologies de l'information.

Infringement de propriété intellectuelle (PI)

Vous avez posté dernièrement un post sur Linkedin qui parle de contrefaçons, de copies, de plagiat et vous vous posez la question de savoir si cela est possible dans le domaine des TI.

Compte tenu de votre parcours, la réponse n'est-elle pas dans la question ?

Oui, bien sûr, sachant que nous sommes dans une guerre économique internationale sans pitié, tous les coups sont possibles au détriment des humains comme des entreprises.

Un Nouveau monde est en train de naître, basé sur de nouveaux codes, de nouvelles façons de considérer les valeurs, les relations, les interactions, les transactions.

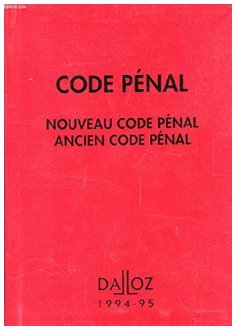
Le monde est en train de passer des codes de performances aux codes de création de valeurs.

Pour recevoir les informations
Complémentaires...

didier@la-machina.xyz

On le voit très clairement au niveau sociologique comme au niveau militaire, j'en ai déjà parlé dans d'autres postes.

Oui, mais pourquoi du plagiat, et de la contrefaçon ?



Parce que, comme à chaque période clé de l'humanité, il y a des personnes qui comprennent, imaginent, créent avec un temps d'avance, ils anticipent sur les tendances, et il y a ceux qui, issus de l'Ancien Monde, essayent de se maintenir coûte que coûte.

Ils ne sont technologiquement, mentalement et psychologiquement pas adaptés ou assez ouverts pour comprendre le monde nouveau qui est en train de se mettre en place.

Donc ils copient, ils plagient, ils deviennent des contrefacteurs persuadés que leur taille, leur notoriété, leur pouvoir les protègeront et qu'au pire, s'ils se font prendre, il leur suffira de signer un chèque, ce qui, selon certains, coûterait moins cher que de payer des droits.

On retrouve cette stratégie ubuesque et burlesque, notamment dans l'industrie pharmaceutique.

Comment faits-vous pour les débusquer dans le domaine des TI / Informatique ?

C'est très simple en fait

Ce qui nous intéresse surtout, ce sont les clients des fournisseurs de technologie, donc toutes les entreprises.

Nous voyons passer les annonces de recrutement en TI / Informatique.

Les annonces nous informent sur les profils recherchés, sur les logiciels avec lesquels ils travaillent et ainsi sur les problèmes qu'ils pensent résoudre.

Nous avons de ce fait accès à la sémantique des annonces qui nous indique les méthodes, les sciences, les processus qu'ils utilisent.

Tout cet ensemble nous permet d'avoir une certaine idée des logiciels utilisés et des problèmes rencontrés.

Nous participons discrètement à des salons, des rencontres, des soirées thématiques, des symposiums, nous y rencontrons des salariés techniciens ou experts en TI qui nous parlent de leurs problèmes internes, de leurs problèmes avec leurs fournisseurs. Et nous lisons aussi les journaux professionnels.

Lors de rencontres avec des prospects, en fonction des questions qu'ils nous posent et de leur réaction face à nos réponses, en fonction des questions que nous posons et de leurs réponses, nous savons avec quels fournisseurs ils travaillent et quels sont leurs problèmes.

Compte tenu des deux premiers points que je viens d'énoncer, nous pouvons détecter s'il sont équipés de matériel plus ou moins contrefait et plagié et ainsi définir si cette entreprise est complice ou victime de cette contrefaçon.

Et puis nous avons les collaborateurs des entreprises de TI / Informatique ou de leurs clients qui informent pour différentes raisons : mauvais management, règlement de compte avec leur employeur, et de plus en plus souvent des problèmes de conscience personnelle.

C'est toute la problématique : être complice ou victime, être lanceur d'alerte ou collabo.

Vous dites victime ou complice ?

Oui, car nous nous sommes aperçus qu'en fait le principal danger des entreprises est leur propre service TI / Informatique.

Il y a, en synthèse, 4 types de responsables TI / Informatique.

A- Celui qui fait exécuter régulièrement des audits de conformité, de sécurité et de contrefaçon par l'intermédiaire d'entreprises spécialisées qui sont en général des TPE ou PME agréées et certifiées SECRETS DÉFENSE.

Ces entreprises avec lesquelles nous travaillons possèdent un matériel et une expertise de très haut niveau parfaitement qualifiés pour ces missions.

Ce responsable-là défend les intérêts de son entreprise

B- Celui qui agit comme la personne du point A, mais qui va organiser les choses pour camoufler la réalité. Et faire échouer l'audit. Dans 90% des cas, nous le localisons.

C- Celui qui refuse les audits et assure à sa direction que tout est sous contrôle, mais qui embauche sans cesse pour mettre un expert derrière chaque problème.

Si les logiciels sont des contrefaçons, il y a des failles.

Ces failles interagissent avec l'ensemble de la structure, et la fragilisent. Le responsable du point C est donc souvent obligé d'avoir un employé par problème à gérer et dans ce type de configuration, plus il y a d'interactions, plus il y a de problèmes et donc plus il est obligé d'embaucher…

et plus il embauche, plus il passe des annonces…. **CQFD**

D- Le responsable qui refuse tout contact, mais dont nous connaissons l'équipement et donc le niveau de risque, il sait que nous savons qu'il sait.

À présent que je vous ai expliqué, mettez-vous à la place d'un hacker qui ferait la même analyse que nous. Il saura facilement quelles entreprises attaquer, quand et comment…

En bref ! L'entreprise cible est non seulement complice et receleuse sans le savoir, mais aussi victime et cible potentielle.

Elle est exposée aux risques juridiques et financiers au même titre que son fournisseur, ce qui représente aujourd'hui des milliards de dommages et intérêts ou autres indemnités.

Pourquoi est-elle exposée aux mêmes risques que son fournisseur ?

Car, bien souvent **dans les contrats que les entreprises signent avec leurs fournisseurs, elles oublient la clause de protection** concernant les plagiats et autres contrefaçons dont nous venons de parler.

Comment se protéger ?

Si je me mets à la place des entreprises qui ont des contrats de vente, de licence et de prestations, avec des fournisseurs

L'audit de sécurité et de conformité est urgent et nécessaire.

La révision des contrats est également indispensable.

Reste également à gérer les collaborateurs des TI / Informatique.

Le domaine des RH dans ce secteur est très sensible. Des employés maltraités peuvent trahir, des managers égocentrés et prétentieux qui refusent ou sabotent les audits sont des dangers graves pour leurs entreprises.

Sans parler des jeux de pouvoir et autres mensonges, voire manipulations que subissent de bonne fois les PDG et membres du conseil d'administration.

Et tout cela se détecte ?

Oui, avec de l'expérience et des technologies spécifiques,

Il est surprenant de constater que, lorsque nous abordons les dirigeants ou les cadres supérieurs, voire certains membres du conseil d'administration ou des actionnaires, ils nous regardent de haut, comme s'ils étaient offensés par notre démarche. Pourtant, notre intention est tout simplement de les protéger ou, au moins, de les informer.

Alors, ceux-là continuent à faire confiance à leurs équipes.

Et comme disait un de mes mentors, il y a des domaines où la confiance est essentielle, mais la confiance sans contrôle est une erreur stratégique.

Et si un PDG demande un audit et que celui-ci est refusé, voire saboté par les V.P. ou les employés du VP, la réponse est claire, il y a déjà une sorte de présomption…

Sur le plan juridique, comment cela se gère

Le plagiat comme la contrefaçon dans ce domaine relève du pénal.

En France, par exemple, les douanes ont un pouvoir de perquisition jour et nuit sur le territoire et les douaniers en charge de ces dossiers sont d'un très haut niveau.

Les conséquences pour les entreprises coupables ?

Elles sont passibles d'action pénale :

Dommages-intérêts compensatoires, dommages-intérêts punitifs, saisie des copies, annulation de la licence. Interdiction d'exercer, voire prison pour les responsables de l'entreprise.

L'entreprise peut être contrainte d'arrêter l'exploitation des logiciels dans des délais tellement courts qu'elle peut disparaître, car, sans les datas, elle quasiment morte.

Sur le plan financier, il peut y avoir une perte importante auxquels s'ajoutent les frais d'avocats, et les frais de réparation que j'ai déjà évoqués.

Les amendes pouvant atteindre 6% du chiffre d'affaires annuel, sans parler de la suspension des certificats obligatoires.

L'Impact commercial, c'est la perte de contrats, la baisse du chiffre d'affaires, le coût de repositionnement marketing. Les pertes de revenus, les coûts de remédiation, les dommages à la réputation.

Dans certains pays les actions pénales peuvent se transformer en prison.

Coût d'entretien accru, risque d'arrêt de fonctionnement, perte de productivité.

Et donc en finale ?

Je dis aux entreprises attention,

Vos employés, parfois involontairement, par méconnaissance du droit et des conséquences peuvent devenir votre pire cauchemar.