Le 15/01/2019,

Objet : Lettre d'information #1901-1

Bonjour,

Pour nos quelques clients à qui nous ne l'avons pas encore souhaité de vive voix, nous vous présentons nos meilleurs voeux pour cette nouvelle année 2019, de bonheur, de santé et de réussite pour vos projets :)

Dans cette lettre d'information, nous allons faire un bilan de 2018, revenir sur les pannes de vos fournisseurs de service, et parler de bien d'autres choses dont la professionalisation des spammeurs qui abusent de vos formulaires de contact.

1/ Bilan 2018 - retour sur une année mouvementée

2018 aura été une année noire pour les infogérances applicatives, du jamais vu en 9 ans : incidents en constante augmentation chez vos fournisseurs de services, démultiplication des mises à jour critique de sécurité, fin de vie PHP / TLS, RGPD ..

Comme vous le savez, nous fonctionnons au forfait avec une entrée de gamme à 30€ HT / mois / serveur, que nous y passions 5 minutes ou 5 heures, c'est le même prix pour vous.

Intuitivement, on comprend assez vite que ce mode de fonctionnement impose d'être efficace et nécessite un excellent recul (de plusieurs années d'exercices) des temps engagés. Ce recul, permet de faire des statistiques et d'ajuster nos grilles tarifaires (en n+3) en fonction du volume moyen d'intervention et des temps qu'elles engagent.

Cependant, cela n'a jamais été prévu que vos fournisseurs subissent régulièrement des incidents, nous contraignant à assumer sur nos forfaits, les identifications et dans certains cas, la curation. Tout comme cela n'a jamais été prévu que le volume de mise à jour critique de sécurité augmente de plus de 300%.

Nous sommes toujours les premiers contactés en cas d'anomalie, indépendamment de l'origine de l'anomalie, donc même si elle n'a rien à voir avec les services que nous supervisons. Cela signifie que les incidents de vos fournisseurs ont un impact direct sur notre rentabilité.

La très forte augmentation du volume moyen d'intervention aurait donc dû être répercutée sur nos grilles tarifaires (les prochaines - 2021 - 2024) via une augmentation d'a minima 50%

Nous avons cependant refusé d'impacter nos tarifs en conséquence et choisis d'investir de nouveau dans nos outils de supervision système et applicatif.

Comme vous pourrez le constater en toute transparence sur le Manager TW en consultant l'historique des versions du superviseur (ici : https://manager.touchweb.fr/infrastructure/supervisor-version.html), **c'est plus de 1500 heures de R&D (recherche et développement) qui ont été réinjectées (soit environ 90 000€ d'investissement)**

Grâce à la rationalisation de nos processus de gestion, et l'enrichissement continu de nos superviseurs, nous pouvons ainsi continuer de vous assurer une évolution tarifaire raisonnable tout en fournissant un service toujours plus qualitatif.

2/ Professionnalisation des spammeurs - ReCaptcha devient indispensable

Nous observons depuis 1 mois une nette professionnalisation des spammeurs, il devient de plus en plus compliqué de contrôler leurs agissements sans dégrader votre service.

Les dernières attaques subies exploitent des centaines de serveurs répartis dans le monde entier, qui nous contraindraient à bannir plus de la moitié des pays du globe, impensable en l'état. (historique de l'une des attaques : https://pastebin.com/drCf5mv4 - vous pourrez constater plus de 500 adresses différentes - un seul appel par adresse)

Si vos formulaires de contact ne sont pas déjà protégés par Google ReCaptcha, nous vous invitons à prendre contact avec nos pôles partenaires d'ingénierie logicielle pour qu'ils les mettent à jour (rapidement si vous êtes sur Prestashop en version 1.6.1.17-) .

ATTENTION : Si vous recevez déjà des SPAMS depuis vos formulaires de contacts en nombre (plus de 50 par jour, directement issus de votre site Internet) et que vous décidez de ne pas protéger vos formulaires de contact cela engendrera des dégradations de service possiblement forte côté EMAIL ayant pour conséquence : l'impossibilité pour vos clients de recevoir leurs mots de passe, leurs récapitulatifs de commande, etc.

3/ Incidents chez vos fournisseurs de service (API en panne)

A raison (et nous vous soutenons dans cette démarche), vous solilcitez de plus en plus des spécialistes pour vous accompagner dans vos projets Web.

La démarche est saine, qui mieux qu'un spécialiste pour répondre efficacement à un besoin spécifique ?

Doofinder / Algolia pour enrichir vos moteurs de recherche, Carts Guru / Nosto / Target2Sell / etc pour faciliter les transformations de vos paniers (entre autres choses), SendInBlue / Mailjet / Mailchimp pour communiquer en masse efficacement sur vos bases clients, SoColissimo / Chronopost / TNT / Mondial relay qui vous proposent d'optimiser vos logistiques, entre autres choses : via une impression automatique d'étiquettes préaffranchies pour vos colis.

Ces spécialistes vous permettent d'augmenter votre chiffre d'affaire, d'améliorer votre productivité, et **ils deviennent incontournables pour assurer la réussite de votre projet professionnel.**

Ce que vous n'avez cependant pas nécessairement en tête **quand vous entreprenez une délocalisation de fonctionnalités à un spécialiste, c'est que vous êtes en train de créer des dépendances**, possiblement fortes, entre votre site Internet et ce tiers. La santé de votre site, pouvant dépendre en tout ou partie de la santé des services fournis par ce tier (certains sont moins ""intrusifs"" que d'autres, de par la nature de la fonctionnalité délocalisée - API synchro vs API non synchro avec une navigation, maillage sur le FRONT et/ou le BACK)

Prenons un exemple (cas de nos clients utilisant Prestashop) :

La société Prestashop affiche des informations issues de son propre site Internet (son API pour être exacte : api.prestashop.com) sur les back-offices Prestashop (dernières actualités du blog de Prestashop, dernière version disponible, ...). De nombreux propriétaires de Prestashop ont vécu un cauchemar en octobre 2018 s'ils avaient le malheur de se connecter après 8h à leur shop (période de surcharge de l'API Prestashop).

Ou encore, plus récemment, Prestashop a oublié de mettre à jour le certificat SSL de l'une de ses API (Gamification), cassant mécaniquement le HTTPS et a mis plus de 40h à réparer cela, résultat, tous les propriétaires n'ayant pas suivi notre conseil de désinstaller le module Prestashop Gamification ont de nouveau eu de grandes difficultés à se connecter à leur backoffice.

Vous noterez que pour les incidents Prestashop, l'heure de la première connexion est importante, la majorité de nos clients démarrant leurs activités avant 7h30 du matin n'ont subi aucun dysfonctionnement car leurs Prestashop sollicitaient l'API de Prestashop à des heures où elles n'étaient pas en surcharge. C'est pour cette raison qu'en octobre dernier, certains de nos clients sous Prestashop n'ont pas eu de problème.

Comme nous vous l'avons indiqué sur Facebook en début d'année, nous avons mis à disposition nos outils de supervision de services Web externes, voici le lien : https://www.touchweb.fr/statut-externe (vous pouvez aussi le retrouver sur le Manager TW : Global | Application | WS Externe)

Grâce à ces nouveaux outils ainsi qu'aux évolutions du superviseur, nous avons fortement amélioré notre vitesse de détections d'incidents des services tiers ainsi que nos outils de communication ciblée. Ainsi, vous pouvez prendre plus rapidement les bonnes décisions pour protéger vos projets des incidents des tiers.

4/ Nouvelle protection chez OVH engendrant des retards de livraison en cas de transferts d'emails de service OVH vers des emails gérés par OVH

Comme vous avez sans doute déjà dû le lire sur notre page Facebook, OVH subit depuis plusieurs mois des campagnes de phishing (comme la plupart des sociétés d'envergure internationale)

L'objectif de ces campagnes organisées par des criminels est toujours le même : voler vos codes de carte bleue et/ou voler vos accès au Manager OVH pour voler vos domaines.

Au-delà des conseils que nous vous donnons régulièrement, à savoir : **essayer le plus que possible de s'astreindre à passer par le site ovh.com puis par le lien officiel du Manager OVH** (sur le site ovh.com, en haut à droite), OVH a mis en place une protection induisant une "temporisation" dans le cadre d'un "transfert" des emails de service entre deux emails gérés par OVH.

Concrètement, si vous nous transférez un email reçu par OVH (expiration de service, livraison d'un service, ..) sur nos emails (gérés par OVH), nous le recevrons 2 à 6 jours plus tard.

Ce n'est pas faute d'avoir essayé d'expliquer à OVH que cette mécanique nous semblait contre-productive, et que cela serait "difficile" pour nous de détailler cela à nos clients, mais ils ne veulent pas entendre nos plaintes à ce propos partant du principe que c'est une protection "nécessaire et indispensable" compte tenu du volume colossal d'emails pirates qu'elles bloquent (selon un interne, plus de 100 000 emails par jour)

Nous espérons cependant qu'OVH mettra en place rapidement la solution que nous leur avons proposée, à savoir : gérer une "liste blanche" autorisant nos emails à ne pas subir cette temporisation inappropriée.

Pour l'heure, si vous souhaitez nous transférer "rapidement" un email de service d'OVH, donc sans souffrir du retard de livraison imposé par OVH, nous vous invitons à enregistrer l'email reçu par OVH puis à nous l'envoyer en pièce jointe (et non pas "simplement" transférer l'email).

Nous sommes toujours à votre disposition au 09 70 44 42 84 si vous avez besoin d'informations complémentaires.
Nous vous souhaitons une agréable semaine,

L'équipe TW