Le 11/01/2022,

Objet : Lettre d'information #202201-1

Bonjour,

A nos clients à qui nous ne l'avons pas encore souhaité de vive voix : nous vous présentons nos meilleurs vœux pour cette année 2022, de réussite, de bonheur et surtout de santé.

Comme chaque année, l'heure est au bilan.

1/ Bilan 2021 - Retour sur la pire année de l'histoire de l'hébergement

Comme vous l'aurez compris à travers nos posts Linkedin, l'année 2021 a été dense - très dense.

Tout ce que l'on pensait jusqu'alors inimaginable s'est produit, engendrant par effet de bord un réarbitrage de certaines analyses risques, voici une liste des incidents les plus sensibles :

- Destruction d'un centre de données engendrant la perte de plus de 15 000 ordinateurs (serveurs) - OVH - 10/03/2021

- Corruption d'un centre de téléchargement d'une suite logicielle Open Source - dépôt Github PHP - 29/03/2021

- Pénurie mondiale de composants électroniques engendrant des retards de livraison sur certaines gammes de plus de 90 jours - depuis Mars 2021 et toujours en cours, à minima jusqu'à S1 2023

- Panne d'envergure mondiale chez Microsoft Azure - 01/04/2021

- Double panne de plus d'une heure chez les deux plus gros opérateurs CDN mondiaux - Fastly et Akamai - été 2021

- Corruption évitée de justesse d'une offre CLOUD Microsoft - 08/09/2021

- Blackout complet de plus de sept heures d'un service tiers d'envergure mondiale - étant une dépendance critique pour certains d'entre vous - Facebook - 05/10/2021

- Blackout complet d'une heure d'un hébergeur au niveau mondial (32+ centres de données coupés du réseau sur 4 continents) - OVH 13/10/2021

- Anomalie d'envergure mondiale (toutes les pages en 404 sur tous les sites concernés) - Google - 16/11/2021

- Blackout continental d'un hébergeur ayant un impact mondial - Amazon - Décembre 2021 (triple panne)

- Tsunami sur l'un des écosystèmes techniques les plus utilisés au monde - Java - Faille critique Log4j - Décembre 2021 et toujours en cours - toute l'année a été rythmée par des piratages majeurs impactant des PME (dont des ETI) et des TGE

2/ A tous nos clients et partenaires nous ayant soutenus : un grand Merci

A toutes celles et ceux qui nous ont soutenus pendant les cas de force majeur de 2021 dont un est toujours en cours, nous vous remercions de nouveau, vous avez été notre moteur.

La confiance que vous nous accordez est chère à notre cœur et nous vous réaffirmons notre engagement de tout mettre en œuvre pour en être digne en continuant de consolider notre service - votre service.

Les milliers d'heures de travaux abattus sur la période 2016-2021 nous ont permis d'être prêts pour gérer ces désastres, et la confiance de nos Grands Comptes et Très Grands Comptes nous a permis de limiter l'impact économique de ces ouragans.

Merci, infiniment.

Nous remercions également **les milliers de bénévoles** œuvrant pour les projets PHP, NodeJS, Debian, Varnish, ElasticSearch, Apache2, PHPMyAdmin, Symfony, Java, ... (la liste est bien trop longue pour les citer tous) pour l'extraordinaire travail qu'ils fournissent sans contre-partie et **qui permettent à vos (et nos) projets professionnels d'exister sous cette forme.**

Ces communautés de bénévoles ont été particulièrement mises en tension récemment à cause des failles critiques de sécurité découvertes sur Java et Apache2 pendant les fêtes de fin d'année. Nous continuerons de vous soutenir financièrement du mieux que l'on peut.

3/ Réarbitrage des probabilités d'itération en conséquence

- Les pannes de Cloudflare de 2019 et 2020 avaient déjà mis en exergue un risque non nul d'**incident majeur sur les réseaux CDN** ayant un impact mondial, la probabilité d'itération a été réhaussée - elle **passe de "faible" à "moyenne"**, en conséquence nous enjoignons tous nos partenaires techniques concernés à consolider leurs plans de continuité de l'activité en mettant tout en œuvre pour repenser leurs systèmes d'information pour qu'ils soient capables de fonctionner sans CDN en mode dégradé.

- **La probabilité de perdre un hébergeur** / fournisseur de service critique d'envergure mondiale **passe de "quasi-inexistante" à "faible"** - il devient obligatoire d'intégrer dans les plans de continuité de l'activité ce risque et d'ajuster en conséquences les infrastructures - toutes les infrastructures critiques pour la continuité de service doivent être résistantes à des pannes d'au moins un hébergeur - à minima sur tous les projets ayant plus de 4 millions d'euros de chiffre d'affaires HT dépendant à cette continuité de service.

- **La probabilité de corruptions de centre de téléchargement** de suites logicielles Open Source (dépôt) **passe de "quasi-inexistante" à "moyenne"** - tout le monde a eu beaucoup de chance que la corruption du dépôt PHP ait été détectée rapidement - l'actualité nous rappelle encore que trop peu de professionnels (ici pour une VF) suivent avec soin et rigueur les différentiels de données sur les suites logicielles Open Source qu'ils utilisent.

Aux éventuels intervenants techniques concernés : nous vous invitons à consolider la surveillance des différentiels de données (diff) des centres de téléchargement (dépôts Github, orchestrateur de dépôts, etc) et de tout mettre en œuvre pour temporiser professionnellement les propagations de mises à jour en vous obligeant à observer des phases de gel.

- **La probabilité d'une découverte de faille critique** ayant des effets de bord mortifères sur un écosystème technique majeur **passe de "moyenne" à "élevée"**.

Si l'on doit retenir quelque chose du tsunami Log4j, c'est que l'heure est à la maîtrise des écosystèmes techniques incluant leurs dépendances techniques (ce que certains qualifient de "supply chain"). Nous enjoignons tous les éventuels intervenants techniques concernés à tout mettre en œuvre pour consolider les outils de surveillance de leurs écosystèmes techniques avec un suivi strict et rigoureux des dépendances logicielles et de leurs versions.

Un tsunami équivalent frappera un jour l'écosystème PHP dont vous dépendez tous et il faudra être prêt.

4/ Plus de 500 000€ ont été réinjectés en Recherche et Développement pour consolider le service TOUCHWEB

Plus de 4000 heures de R&D ont été réinjectés pour faire évoluer le service TOUCHWEB en l'accord avec ces réarbitrages de probabilité d'itération de dysfonctionnement majeur d'envergure nationale et internationale.

Comme à l'accoutumée depuis 6 ans, vos intervenants techniques peuvent suivre cela en toute transparence ici.

A/ Suppression définitive des dépendances mono-hébergeur de l'infrastructure de service TOUCHWEB

L'infrastructure de service TOUCHWEB - composée à date de plus de 90 serveurs - a évolué pour améliorer sa résilience face à des dysfonctionnements majeurs mono-hébergeur, tous les silos sont dorénavant propulsés via des infrastructures très haute disponibilité (VHA) - multi-hébergeur (généralement OVH / Scaleway) en mode standard si critique (donc sous répartiteur dynamique de charge) sinon en mode dégradé (sans répartiteur de charge).

Le plan de continuité de l'activité de TOUCHWEB se voit de nouveau consolidé, tous nos services sensibles à critiques sont dorénavant répliqués chez plusieurs hébergeurs.

Nos coûts d'infrastructure de service ont évolué également passant d'environ 20 000€ HT / an (2020) à plus de 50 000€ HT / an (2021)

On ne gèrera pas le risque d'une panne multi-hébergeur partant du principe que si cela arrive c'est qu'il y a obligatoirement un impact national à international sur l'Internet, ingérable de facto.

B/ Ouverture à nos clients d'une offre VHA résistante à une panne globale mono-hébergeur

A tous nos clients dont le chiffre d'affaires dépendant à la continuité de service de leurs sites E-Commerce dépasse les quatre millions d'euros HT par an, nous avons le plaisir de vous annoncer que depuis Novembre 2021 **nous vous proposons des infrastructures très haute-disponibilité - VHA** - résistantes à des pannes mono-hébergeur.

Compte tenu de la complexité de ces infrastructures et des garanties de temps d'intervention attendues (moins de 15 minutes), l'offre a été fixé à 1 500€ HT / mois côté TOUCHWEB. Côté hébergeur (généralement OVH et Scaleway), compter à minima 300€ HT / mois.

Pour les intéressés, vous trouverez plus d'informations à ce propos ici.

C/ Encadrement professionnel de vos écosystèmes techniques via nos propres centres de téléchargement

Comme vous le savez, tout a été mis en œuvre entre juillet 2020 et juin 2021 (https://www.touchweb.fr/lettre-information-21061 point 8 clôturant le point 1 de https://www.touchweb.fr/lettre-information-20081) pour propulser notre propre centre de téléchargement pour vos dépendances critiques (le projet PHP dont vous dépendez tous).

Grâce à cet investissement d'environ 120 000€ et représentant plus de 80 000€ HT / an de charge fixe, nous vous garantissons contractuellement un maintien jusqu'en 2026 de vos éventuelles dépendances obsolètes (PHP 7.3) à gravement obsolètes (PHP 7.2 et moins).

Cela vous donne de l'air pour plusieurs années sur toutes vos éventuelles applications métier obsolètes à gravement obsolètes incluant entre autres choses, toutes les versions de Prestashop antérieures à la version 1.7.8 pour vous permettre de survivre aux éventuels effets de bord délétères du Covid19 sur vos activités professionnelles en temporisant vos investissements sur le maintien à jour de vos systèmes d'information (report de vos dettes informatiques sur 2025-2027)

L'ensemble, comme d'habitude, est fourni **sans aucun surcoût par TOUCHWEB** (à nos nouveaux clients, nous vous suggérons de lire le point 2 de https://www.touchweb.fr/lettre-information-20081)

Nous avons pris la décision mi 2021 d'aller encore plus loin et de tout mettre en œuvre pour supprimer définitivement toutes dépendances à un centre de téléchargement distant (dépôt), tout en encadrant professionnellement l'ensemble via l'hexa-staging d'application de mises à jour (voir https://www.touchweb.fr/lettre-information-21061 point 5).

Dorénavant, nous avons le plaisir de vous affirmer que **100% des mises à jour appliquées sur vos serveurs passent obligatoirement par nos propres centres de téléchargement** (dépôt Debian privé auto-géré par TOUCHWEB propulsé par une infrastructure VHA multi-hébergeur), systémiquement soumis à notre hexa-staging.

Cela consolide également de fait vos plans de rétablissement de l'activité dont **vos dépendances à des services externes critiques pour vos réinstallations systèmes ont été** grandement atténués et pour la quasi-totalité d'entre vous : **complètement neutralisées.**

D/ Professionnalisation de la soumission des accès systèmes (FTP / SSH) sur un mindset ZERO-TRUST

Vous êtes encore trop nombreux à utiliser vos boîtes emails pour stocker des données critiques incluant d'éventuels accès système.

L'un d'entre vous s'est fait pirater en 2021 sa boîte email (son mot de passe a été piraté sur un blog improbable et gravement obsolète où il était inscrit) et par effet de bord, son Wordpress a été piraté.

Nous vous invitons de nouveau à **NE PAS utiliser votre boîte email pour stocker des données critiques** ainsi qu'à privilégier des solutions de stockage de mot de passe validées par l'ANSSI telles que Keepass ou LockSelf.

Pour nous assurer que notre processus de soumission d'accès systèmes ne vous permette pas "simplement" un stockage de ce type de données, dorénavant les emails émis sont inutilisables en l'état et le contenu soumis à nos PrivateBin est auto-détruit dans l'heure pour vous contraindre à copier/coller le contenu dans un container sécurisé tel que Keepass ou LockSelf.

E/ Révision de l'offre SAUVEGARDE MULTI-SITE - Délocalisation à venir en Pologne

Dans la continuité du sinistre de Strasbourg, un risque partagé a été découvert entre les centres de données OVH de Gravelines et de Roubaix du fait de la centrale nucléaire de Gravelines.

Nous avons donc pris la décision de délocaliser le groupe de stockage géopositionné sur le centre de données OVH de Roubaix vers le centre de données OVH de Varsovie en Pologne.

Cela va permettre d'affirmer que toutes les géopositions des serveurs de stockage sont distantes au minimum de 100Km au lieu de 80Km et au maximum de 1400Km au lieu de 300Km.

Si depuis 3 mois nous mettons à jour vos contrats en l'accord, la bascule finale (Roubaix vers Varsovie) n'aura effectivement lieu qu'au deuxième semestre 2022 afin de tout traiter d'un bloc.

Nous sommes également en pourparlers avec nos avocats et un organisme de certification sur l'aspect RGPD compliant du groupe de stockage géopositionné dans nos locaux à Orléans. Il existe un risque que l'on soit contraint de fermer cette géoposition du fait de l'absence de la norme ISO 27001 et de l'impossibilité de l'obtenir avant 2024 à minima. Nous réfléchissons actuellement à l'externaliser chez l'hébergeur Hetzner (2° plus gros hébergeur Allemand) sur son centre de données Finlandais pour ajouter une géoposition la plus éloignée possible en Europe.

Par effet domino vertueux, l'ensemble de ces décisions va améliorer votre résilience face au risque de guerre nucléaire et/ou de troubles sévères à l'ordre public impactant un pays de l'UE dont la probabilité est passée depuis peu de "très faible" à "faible".

F/ Finalisation de la prise en charge de nouvelles applications métiers : Dolibarr, Marello, Pimcore, Akeneo et MediaWiki

Vous avez été nombreux à nous réclamer des supports natifs incluant des préproductions "clés en main" et sans effort sur ces solutions métiers.

Nous avons donc le plaisir de vous annoncer qu'après plusieurs mois de tests, ces cinq nouvelles applications métiers sont parfaitement gérées par nos outils.

Vous pouvez donc vous sentir libre de nous les réclamer à tout moment sous réserve qu'un développeur procède à leur installation initiale.

5/ Notre résolution pour 2022 : stabiliser le projet TW après 3 ans de forte croissance

Grâce à vous nous sommes en pleine croissance depuis 3 ans, trois nouvelles embauches ont été possibles à la rentrée 2021.

Merci encore pour votre confiance - tout cela est permis grâce à vous.

L'année 2022 sera consacrée en grande partie à la stabilisation du projet TW et de son équipe, composée à date de cinq personnes (un responsable projet, un administrateur système, une assistante de direction et deux directeurs : technique et juridique).

De nombreux outils vont évoluer sur la période pour permettre l'agrégation de plus de profils techniques, deux embauches supplémentaires sont planifiées sur S2 2022 / 2023 et vont nécessiter un investissement d'environ 300 000€ pour repenser nos outils en allant toujours plus loin dans la sécurité de vos données.

On reviendra plus en détails sur ces sujets dans une prochaine lettre d'information.

6/ Phishing : toujours supprimer à réception tout email contenant "HTTPS" ou "SSL" dans son titre

Une vague d'attaque de type phishing est en cours. Nous vous invitons de nouveau à toujours supprimer à réception tout email contenant les mots clés "HTTPS" ou "SSL" dans l'objet sauf s'ils sont émis par TOUCHWEB.

Le seul et unique écran ayant autorité sur vos certificats SSL nécessaires au fonctionnement de votre "HTTPS" est disponible ici. Nous vous contactons toujours 2 semaines avant les expirations annuelles sans **JAMAIS** vous demander vos codes de carte bleue.

Nous vous prions d'être vigilant. En cas de doute, nous vous suggérons de nous demander une confirmation par retour d'email.

7/ PHP 8.1 est maintenant disponible sur Buster et Bullseye (Debian 10 et Debian 11)

Le ton continue de se durcir chez PHP contre les mauvaises pratiques de développement, cette nouvelle version majeure continue de forcer les tiers à se professionnaliser tout en allant toujours plus loin en matière de performance.

La version PHP 8.1 est dorénavant disponible sur tous les serveurs du staging 2/6 (bêta testeur niveau 1), elle sera débloquée sous 2 semaines sur le staging 3/6 (bêta testeur niveau 2), puis progressivement sur février à tous les stagings supérieurs.

Par ailleurs, nous vous informons également que l'application système PHP 7.3 permettant au langage de programmation PHP - avec la syntaxe de la version 7.3 - de fonctionner, a atteint la fin de son cycle de vie : il n'y aura donc plus jamais de mise à jour (incluant des mises à jour de sécurité).

Si vous utilisez PHP en version 7.3 ou antérieure (entre autres choses : toutes les versions Prestashop inférieures à la 1.7.7.8 sont concernées), nous vous invitons à contacter votre développeur pour qu'il fasse évoluer votre application métier pour qu'elle soit éligible à PHP 7.4 à minima puis à nous solliciter pour la mise à disposition.

Nous vous souhaitons une belle fin de semaine.

L'équipe TW - Votre spécialiste en infogérance Prestashop