SAN JUAN – Atelier de DNSSEC - Partie 2
Mercredi 14 mars 2018 – 10h30 à 12h00 AST
ICANN61 | San Juan, Porto Rico

RUSS MUNDY: Je ne sais pas si Geoff fera partie de cette présentation, mais Geoff a préparé ce rapport aussi. Nous avons donc une présentation sur KSK Sentinel. Warren, c'est à vous.

WARREN KUMARI: J'essaie de voir où je peux me mettre pour avoir le micro et pouvoir parler. Merci beaucoup.

Bonjour à tous. Je regarde autour de la salle, je vois qu'il y a des gens qui ont déjà vu cette présentation. Est-ce qu'il y a des gens qui n'ont pas vu la présentation encore ? Très bien.

D'accord, je pense que ce sera assez interactif alors.

C'est un travail conjoint qui a été fait par moi-même et Geoff Huston et Joao qui n'est pas dans la salle. Oh, Geoff arrive. Très bien.

Alors quel est le problème que nous voulions résoudre ? Comme vous l'aviez dit tout à l'heure, nous voulions rouler l'ancre de

confiance DNSSEC. Les utilisateurs qui n'avaient pas encore KSK, ou les utilisateurs qui utilisaient les serveurs validants et qui n'avaient pas la nouvelle KSK, pensaient que l'internet, pour eux, allait s'arrêter. Parce que rien n'allait fonctionner.

Et ce qui nous inquiétait encore plus, c'est que nous n'avions pas un moyen pour pouvoir mesurer le déploiement de cette nouvelle clef, c'est-à-dire que nous ne savions pas combien de personnes tomberaient en panne si cela se produisait.

Alors, très récemment, on a entendu parler du RFC 8145 qui a été publié récemment, en 2017. Que fait ce RFC ? Cela nous montre quelles sont les ancres de confiance que possèdent les différents serveurs. Nous voulions savoir quels étaient les résolveurs qui avaient certaines clefs, et de cette manière nous allions savoir lesquels étaient à l'abri de pannes et lesquels ne le seraient pas.

Malheureusement, on ne pouvait pas tout savoir. Ce rapport concerne les résolveurs validant du DNSSEC. Dans ma [cave], j'ai un serveur validant DNSSEC, et donc je l'ai relancé.

Je pense que je reçois ici l'interprétation ? D'accord, ok.

Alors, je vous disais que j'ai un serveur validant, je l'ai relancé tous les jours pour différentes raisons. Cela veut dire que le

résolveur qui va aller dans ma cave n'a jamais eu de réponse concernant la nouvelle clef.

Et donc, pour obtenir ces informations par rapport à la clef, le serveur doit fonctionner d'affilé au moins 30 jours.

Est-ce que cela est important ? Parce que personne n'a envoyé des requêtes. Si un résolveur est en panne mais que personne ne l'utilise, cela n'a aucun intérêt.

Alors qu'est-ce qu'on voit ici, dans ce graphique ? On voit les résolveurs validants qui font ce rapport par rapport à ce RFC 8145. Vous voyez un graphique qui a été publié par VeriSign en octobre 2017, et il montre la progression du déploiement des nouvelles ancres de confiance.

La nouvelle KSK a été publiée mi-aout, le temps a expiré, c'est-à-dire que le moment où les ancres de confiance devaient être mises en œuvre était clair. Et à un moment donné on a pu voir qu'il y a eu un certain nombre de résolveurs qui n'avaient pas pris en compte cette nouvelle clef.

On a vu des présentations aujourd'hui, on a vu que ce chiffre a augmenté, et on ne sait pas tout à fait pourquoi.

Quoi qu'il en soit, notre RFC 8145 ne fournit des informations que pour des résolveurs et ne donne d'informations par rapport

aux utilisateurs. Et cela ne nous permet pas de savoir quel sera l'impact sur les utilisateurs du roulement de la KSK.

Est-ce que les utilisateurs seront impactés ou pas ?

Ce qui nous intéresse, c'est de savoir si les utilisateurs pourront utiliser internet une fois que la KSK sera roulée.

Alors, que faut-il faire ? Il faut mettre à jour le résolveur, et cela peut permettre à tous ceux qui utilisent internet de mettre en place un service de mesure. Et cela permet de faire connaitre aux utilisateurs les résultats des tests.

Actuellement, on obtient des rapports des serveurs aux opérateurs et cela nous permet de voir ce qu'il se passe de l'autre côté. Et cela nous permet de mesurer le déploiement à une plus large échelle.

Geoff nous a parlé par exemple de Google Adds et le nombre d'utilisateurs qui utilisent Google Ads et cela lui permet d'avoir plus d'informations par rapport à ce qui se passe. Et c'est des échantillons de milliers d'utilisateurs. Cela nous permet de mieux comprendre comment ça se passe.

Alors, comment fonctionne Sentinel ? Quels sont les changements ? Les changements sont assez simples, un serveur validant qui a été mis à jour pour être compatible avec cela fera les processus ordinaires de validation DNSSEC. Quand il reçoit

une requête, il va faire ce qu'il a l'habitude de faire. Mais, en tout dernier, avant d'envoyer la réponse, il regarde si l'étiquette la plus à gauche contient cette chaine magique : KSKroll-sentinel-not-ta et puis la clef.

Si le serveur voit cette clef, alors il donne une réponse normale. Si cette clef n'est pas là, à ce moment-là, il prend la réponse valide et donne une réponse : servfail. Ça veut dire que pendant qu'il y a le processus de validation, il a trouvé un problème, et la réponse qu'il envoie, c'est servfail, qui veut dire qu'il y a quelque chose qui ne va pas.

La deuxième règle consiste à dire : KSK sentinel rol not KEY : c'est-à-dire si vous n'avez pas la clef, vous répondez normalement, et si vous avez la clef, vous répondez servfail.

Donc vous voyez, il y a deux questions qui sont posées, deux questions qui sont opposées l'une par rapport à l'autre. Parce que ces deux questions ne peuvent pas être toutes les deux valables en même temps.

Vous voyez donc un exemple ici. Je suis un résolveur validant DNSSEC, je suis compatible avec Sentinel, je suis donc un serveur validant DNSSEC, et j'ai la nouvelle clef KSK. C'est 20326.

Je reçois donc une requête pour invalid.example.com. Ce nom en particulier implique un enregistrement non valide, donc il n'a pas été signé de manière valable, et j'envoie servfail.

Je reçois une requête, comme celle que vous voyez sur l'écran, KSK, sentinel etc. je fais mon travail, je fais les étapes de validation et de résolution, et je réponds avec 192.0.23. C'est un exemple. Mais comme je suis compatible sentinel et parce que j'utilise l'identificateur de clef 20326, je réponds normalement. Est-ce que c'est une ancre de confiance que vous avez ? Et alors je transmets la réponse que j'ai obtenue.

Quelques secondes après je reçois une requête pour KSKRoll-sentinel, je fais mon processus de validation, je réponds avec l'adresse que j'obtiens du serveur faisant autorité, mais j'utilise l'identificateur de clef 20326, alors je 'n'ai pas l'ancre de confiance et j'envoie une réponse Servfail. Et donc je n'ai pas cette ancre de confiance.

Pour les gens qui nous écoutent à distance, je suis à la diapo 7.

Alors, nous avons ajouté beaucoup de complexité au DNS, et en ajoutant la complexité, il faut se demander : est-ce que c'est utile ? Et si c'est le cas, comment ?

Je pense que la plupart des gens peuvent voir la diapo sur l'écran, vous voyez, invalid.exammple.com/fish,

example.com/kitten, et example.cm/puppy, c'est-à-dire exemple.chaton, exemple.chiot et exemple.poisson.

Et donc je demande aux utilisateurs d'aller sur une page web qui contient ces informations. Alors quand vous écrivez cette page, vous voyez l'image d'un poisson. Si vous voyez l'image d'un poisson, ça veut dire que vous avez pu résoudre le nom de domaine invalid.exemple.com. Si vous avez pu valider invalid.exemple.com, ça veut dire que vous n'utilisez pas un serveur validant. Si vous n'utilisez pas un serveur validant, le roulement de la KSK ne vous concerne pas.

Si vous pouvez voir l'image d'un chaton et d'un chiot, ça veut dire que vous n'avez pas pu valider invalid.exemple.com, mais cela veut dire que vous avez pu obtenir le message de la clef.

Mais, puisque vous ne pouvez pas avoir et ne pas avoir en même temps la clef de confiance, cela veut dire que votre serveur validant n'est pas à jour au niveau de la clef KSK.

Si vous voyez seulement le chaton, ça veut dire que vous avez pu obtenir la clef 20326, et que vous n'avez pas pu obtenir la clef 20326, cela veut dire que vous serez en mesure de rouler la clef KSK, que vous avez l'ancre de confiance, que vous êtes en mesure de pouvoir faire le roulement.

Si vous voyez seulement le chiot, ça veut dire que vous avez seulement l'ancienne clef, ça veut dire que vous ne serez pas capable de rouler le KSK. Ça veut dire que lorsqu'il y aura le roulement de la KSK, la clef sur laquelle repose votre travail fera en sorte que le DNS tombe en panne.

Alors c'est vrai que nous utilisons ces images d'animaux ? Ce serait génial si on pouvait. Mais malheureusement ce n'est pas le cas. On n'a pas pu faire cela.

Mais à la place, nous avons un travail de script, de codes, pour essayer de faire la même chose que l'on a faite avec le chiot, le chaton et le poisson pour essayer de voir quels sont les serveurs validants qui peuvent résoudre l'exemple dont je vous ai parlé pour savoir s'ils sont en mesure de rouler la KSK.

Ce serait génial d'avoir ces chatons, mais ce n'est pas le cas.

Nous avons une démo sur l'adresse que vous voyez sur l'écran, et comme j'ai un petit peu de temps, je vais donc utiliser cet ordinateur. Je vais vous montrer que cela fonctionne. Donc www.ksktest.net, on essaye donc d'enregistrer, de télécharger tous les enregistrements, et on voit qu'on utilise un serveur validant, mais qu'il ne peut pas encore être compatible avec la méthode sentinel. Donc cette machine en particulier, et je pense que tous les ordinateurs des gens qui sont à l'ICANN 61 ne pourraient pas rouler la clef KSK. Voilà.

C'est la diapo numéro 9.

Voilà une vision assez générale de ce que je voulais vous montrer. On n'a pas eu de chatons, et donc voilà un petit peu la photo de ces petits chatons.

Y a-t-il des questions ? Pourquoi les chatons sont déguisés ? Je ne sais pas.

Frederico, vous avez des questions ?

FREDERICO NEVES: Merci Warren. Est-ce que vous collectez des informations sur les résultats dans votre page de ce test ?

WARREN KUMARI: Oui. En quelque sorte. J'ai un serveur qui peut servir ces ressources, et donc j'enregistre le fait que les gens envoient ces requêtes, mais ce que l'on ne voit pas… Parce que chaque enregistrement est associé à un numéro aléatoire. Et je n'ai pas suffisamment d'informations des logs pour savoir… Ou peut-être que j'en ai… pour savoir quels sont les pourcentages. Mais franchement je ne me suis pas penché là-dessus. Parce que la plupart des résolveurs n'ont pas été mis à jour.

Si vous regardez le code vous allez voir que c'est un concept de mise en œuvre.

Je pense que j'aurais suffisamment d'informations pour pouvoir vous répondre, mais franchement, je ne l'ai pas fait.

Bonne question.

VIKTOR DUKHOVNI: Est-ce que vous avez une méthode pour nous permettre d'aller au-delà du RFC 5011 ? Est-ce que vous avez des idées par rapport à cela ?

WARREN KUMARI: Oui et non. Je pense que Frederico aura une question de suivi après ?

Nous avons écrit un document où l'on signale que le RFC5011 est plutôt vague. Et cela rend les choses dangereuses au niveau de l'empreinte. Il y a des choses que l'on pourrait améliorer, certes.

Les problèmes ont surtout été liés, pas forcement au RFC5011, il y a eu une mise en œuvre peut-être incorrecte de ce RFC, et c'est mon point de vue personnel. Ou bien plutôt les gens ont configuré les ancres de confiance du DNSSEC comme nous leur avons dit de faire au départ.

Et pour ceux qui ne lancent pas BIND, les ancres de confiance, la réponse qu'ils reçoivent c'est : voici l'ancre de confiance, il ne

faut pas rouler cette ancre de confiance parce que je vais vous dire quand il faut remplacer cette ancre de confiance.

Et on disait aux gens ça parce que c'était la meilleure pratique à l'époque, c'était la seule pratique en fait à l'époque.

Quand on a commencé à dire aux gens que le RFC5011était introduit dans des résolveurs mais qu'il fallait agir autrement pour le mettre en place, à ce moment-là, les gens ont été peut-être un peu plus confus.

Ensuite, il est assez fréquent pour les gens d'utiliser des [token] pour faire fonctionner les serveurs de nom. La 5011 dit : quand vous voyez une nouvelle key qui est signée avec la vieille key, il ne faut pas la signer pendant au moins 50 jours. C'est-à-dire qu'il faut sécuriser les serveurs en retirer la validité du BIND ou d'autres méthodes que vous utilisiez.

Alors la plupart de ces problèmes ne sont pas des problèmes en eux-mêmes qui seraient liés au 5011, c'est plutôt une configuration incorrecte, parce qu'ils ont fait ce qu'on leur avait demandé de faire, mais après ils n'ont pas suivi les informations les plus actualisées. Ca veut dire que si nous remplaçons 5011 on aura encore ce type de problèmes.

Mais je suis d'accords sur le fait que la RFC 5011pose difficulté. Et beaucoup de gens nous ont dit qu'ils s'attendaient à ce qu'il y ait un document plus opérationnel.

Je suis d'accord pour dire que la 5011 devrait être remplacée On en a parlé un peu de cette possibilité, mais en général ce que l'on fait c'est la retirer la nouvelle ancre de confiance du site IANA, et effectivement il y a eu des discussions là-dessus, mais je ne sais s'il y a de meilleures idées.

VIKTOR DUKHOVNI: Je voulais savoir s'il y a la possibilité de changer ces ancres de confiance, transmettre à partir d'une certaine de signature, de manière immédiate, sans devoir attendre 30 jours.

WARREN KUMARI: Oui, je pense qu'on pourrait faire cela, attendre 30 jours et puis attendre une nouvelle période de 30 jours. Ce serait horrible.

VIKTOR DUKHOVNI: Est-ce qu'on pourrait éliminer ces 30 jours et faire un délai zéro ?

WARREN KUMARI: Alors, les systèmes avec clef roulée, je ne sais si ça fonctionne, on va regarder. Regardez, nous avons un nouveau gTLD, qui marche…

Attendez, je me suis trompé… Système rouleur de clef… Donc ça c'est un site de démonstration que j'avais mis en place il y a très longtemps et qui permet aux gens d'utiliser le 5011 pour faire des tests. C'est une clef en fait qui roule, en fait toutes les 90 minutes.

Le problème, c'est que lorsque j'ai mis ça en place pour la première fois, la majorité des résolveurs n'attendaient pas 90 jours pour installer la nouvelle ancre de confiance. Donc en fait ça marchait. On mettait la machine et ça marchait ; les gens avaient ignoré ce délai de 90 jours, et les résolveurs avaient suivi le RFC 5011, et ils attendaient les 90 jours. Mais bon. C'est bien de savoir que ça fonctionne toujours.

D'autres questions ?

FREDERICO NEVES: Alors pour tous les acteurs, pour faire le suivi, si tout va bien, au cours des semaines à venir, avec l'IETF, quand est-ce – et ça c'est surtout pour Geoff – donc combien de temps faut-il attendre avant de commencer à faire les tests ? Est-ce que vous allez attendre 1 mois, est-ce que vous allez espérer que tout le monde déploie les nouveaux résolveurs ?

Quelles sont vos attentes par rapport à ça ?

GEOFF HUSTON: Là, il y a changement de comportement des résolveurs qui fonctionnent selon un mode qui valide les réponses qu'il renvoie, en utilisant le DNSSEC. Parce que toutes les réponses doivent regarder l'étiquette qui est la plus à gauche pour voir si c'est un morceau de texte important, clef pardon, et à ce moment-là ça modifie le comportement.

Maintenant, il y aun modèle qui a été implémenté dans les résolveurs Knot, mais il n'a pas été implémenté. Donc pour connaitre la part de marché des CZ.NIC des résolveurs Knot, il faudrait que je teste maintenant, et ça me montrerait ça maintenant. CZ.NIC serait utile de cette manière.

Donc l'idée c'était de l'intégrer dans ce qui existe et il serait peut-être bon d'utiliser le Red Hat pour intégrer les résolveurs dans cette publication. Et ce serait bien de faire ça avant le mois d'aout, pour avoir des données.

Mais comme tout dans le DNS, il y a beaucoup de variantes, beaucoup de choses imprévisibles, et il n'y a que le Knot qui a été implémenté pour l'instant. Donc je ne peux pas pousser à une publicité de mesures pour l'instant.

WARREN KUMARI: Un petit suivi par rapport à ce que vient de dire Geoff. Les gens qui ont regardé la présentation CIRA, juste avant la pause,

savent qu'il y avait une ligne plate des résolveurs qui installaient les RC8145. Et ensuite, il y a eu une augmentation. Et apparemment, les gens mettent à jour leur version du résolveur pour des questions de sécurité.

Donc cela veut dire que ce qu'il faut faire c'est attendre le déploiement sur les résolveurs et s'assurer que juste après, les gens mettent à jour.

Donc commencer à considérer ceci maintenant.

FREDERICO NEVES: En fait, ne pas avoir Sentinel, c'est une vulnérabilité.

JAAP AKKERHUIS: Je suis [d'Internet Labs]. Je pense qu'il faut attendre un petit peu que les choses soient mises en place pour Sentinel. Nous sommes au milieu du lancement de Unbound, et dès que ce sera mis en place, on l'utilisera.

WARREN KUMARI: Nous pensons pour l'instant que les systèmes fondamentaux, l'étiquette, sont stables.

Donc pour ceux qui n'avaient pas utilisé la liste opérationnelle du DNS, le [TA – NOT- TA], cette chaine a changé 4 à 5 fois. Je ne sais pas si vous avez suivi tout ça, je crois que c'est 5 fois.

Donc ce n'était pas un changement énorme, mais ça a changé. Nous pensons maintenant que c'est stable et qu'on peut vraiment compter dessus, sur cette implémentation donc.

RUSS MUNDY: D'autres questions ? Geoff allez-y.

GEOFF HUSTON: Je voulais faire un autre commentaire par rapport à ça, qui illustre un petit peu pourquoi est-ce qu'on a un deuxième ensemble et pourquoi il y avait des problèmes avec 8145. Alors lorsqu'on regarde le DNS, on peut le considérer de deux perspectives.

Premièrement essayer de comprendre le comportement des éléments individuels dans le système de résolution du DNS, donc les résolveurs individuels et essayer de comprendre du point de vue individuel comment les résolveurs se comportent.

Mais les utilisateurs ne se comportent pas de cette manière, ils ont des ensembles de résolveurs, une liste pour le .COM, et s'ils ne sont pas comptant de la première réponse, ils vont au deuxième ou au troisième.

Donc la réelle question c'est de savoir ce qu'il se passe au niveau des utilisateurs. Pas ce qu'il se passe au niveau des résolveurs.

Par exemple si vous avez deux résolveurs configurés, l'un qui valide et un qui ne valide pas. Le roulement de la clef n'est pas pertinent parce que du point de vue du résolveur validant, même s'il ne suit pas le roulement de clef, tout ce qu'il va retourner en tant que SERVFAIL c'est ça.

Donc ce programme sentinel ne permettra pas de récupérer les résolveurs récalcitrants, ce n'est pas son objectif et ce n'est pas ce qu'il peut faire ;

Par contre, ce qu'il peut dire, c'est que avant un roulement de clef, quelle est la population d'utilisateurs qui pourraient se retrouver sans résolveur qui fonctionne ?

Donc c'est un petit peu le scénario catastrophe.

Donc la question de Viktor et les résolveurs, comment est-ce qu'on peut réparer le problème ; alors si vous voulez comprendre le DNS de cette manière, il faut aller beaucoup plus loin dans la réflexion, mettre en place d'autres changements, parce que pour l'instant ce n'est pas possible.

WARREN KUMARI: Jaap?

JAAP AKKERHUIS: La question que j'ai, c'est que nous avons l'étiquette qui est réservée pour ça, de manière spécifique. Donc en fait…

GEOFF HUSTON: L'étiquette entraine un comportement, le domaine dans lequel cette étiquette se situe, ça dépend de vous, de moi, et de toute personne qui souhaite utiliser le test.

Alors l'étiquette entraine un comportement. C'est tout. L'étiquette de gauche.

JAAP AKKERHUIS: Donc ma question, c'est : est-ce qu'il y a d'autres étiquettes qui entrainent d'autres comportements ? C'est comme IANA où vous avez des étiquettes de comportement ? Parce que là, on démarre quelque chose de nouveau.

WARREN KUMARI: Oui, il y a XF-- . Alors il y a des gens qui disent que c'est toutes les étiquettes _xmpp, etc. Donc il y a des comportements différents, il y a des résolveurs, par exemple les BIND et des résolveurs minimum, qui vont utiliser les étiquettes avec un enregistrement [A].

Donc oui, je comprends. Nous avons choisi une chaine un peu au hasard, et donc il faudrait qu'il y ait effectivement quelque chose là-dessus quelque part.

Alors il y a des gens qui voudraient choisir un registre, mais il faut faire attention parce que ça peut être dangereux.

[JACQUES]: Un autre commentaire, j'ai oublié de dire au début que la séance est traduite en français et en espagnol et donc vous pouvez écouter la traduction en utilisant les casques.

RUSS MUNDY: Merci Warren, merci Geoff pour cet excellent travail. Il y a une autre question, allez-y monsieur.

NON IDENTIFIE: Un commentaire… Il n'y a pas d'impact sur le DNS, ce --, c'est la couche suivante qui est affectée. Donc voilà c'est autre chose.

RUSS MUNDY: Merci Beaucoup Warren et Geoff. Alors, personne suivante, Ondrej.

Ondrej Filip de CZ.NIC va maintenant nous présenter sa présentation et va nous parler du projet Turris.

ONDREJ FILIP: Bonjour à tous, je m'appelle Ondrej Filip, je travaille pour CZ.NIC et j'aimerais parler d'un aspect du projet TURRIS.

Ce n'est pas un CPE normal, il y a en fait d'autres fonctionnalités que nous avons introduites.

Alors qu'est-ce que c'est que ce projet Turris ? Il a démarré il y a un certain temps, en 2013, et à l'époque l'idée principale c'était la cyber défense. Donc la collecte d'information au centre de validité des informations. Nous avons également une équipe et nous avons des recommandations en matière de sécurité, etc. Donc ça c'était l'idée de base.

Et ensuite, nous avons continué notre travail et nous avons décidé que la meilleure option c'était les routeurs SOHO. Donc nous avons commencé à y travailler et nous avons également ajouté un [inaudible] parce que la situation est vraiment complexe.

La plupart des chercheurs sont d'accord parce que les mises à jour sont complexes, donc on essayait de voir comment solutionner le soutien des technologies, la validation DNSSEC, IPv6, tout ça, ça ne marchait pas très bien.

Donc nous avons continué sur cette lancée, nous allons essayer de voir quels étaient les dispositifs qui existaient. Mais en fait il n'y avait pas grand-chose.

Donc les résolveurs que nous avons créés sont nos propres matériels, donc nos propres routeurs, et l'objectif du projet c'était donc deux, les deux premières générations, et donc nous avons créé plusieurs milliers de ces dispositifs.

Docn vous voyez, c'est le routeur qui est en haut à gauche en bleu.

Les résultats étaient très intéressants, on a voulu élargir le projet, on a créé une nouvelle version, le turris1.1, et donc encore une fois on en a produit 1000. Et nous avons surtout travaillé en République tchèque. Donc on donnait ces dispositifs gratuitement aux gens en République Tchèque, nous en avons donné quelques-uns à l'étranger, mais en majorité les routeurs étaient dans la République Tchèque.

Et ensuite nous avons commencé à publier les résultats de notre projet. Des gens ont commencé à nous demander s'ils pouvaient en acheter un. Il y a même des gens qui m'ont proposé leur carte de crédit, très gentiment ou des petits pots de vin. Certains ont réussi à me convaincre.

Ensuite nous avons décidé d'élargir le projet. Et nous avons fait une campagne de financement participatif. En fait nous avons levé énormément de fonds et nous avons créé ce nouveau routeur. Donc nous avons le routeur Turris Omnia que nous vendons.

Mais nous sommes une organisation à but non lucratif, donc ce n'est pas sur les bénéfices que nous concentrons notre travail, mais l'idée c'était d'améliorer la situation.

Alors, qu'est-ce qui est différent avec le Turris Omnia ? C'est source ouverte, non seulement pour le logiciel mais également pour le matériel. Nous avons également beaucoup de puissance dans ce matériel. Il est très puissant, donc il permet de faire pas mal de choses.

Le système opérationnel c'est le Turris, mais en fait il est basé sur l'OpenWRT. Et ce qui est très intéressant c'est que les mises à jour sont automatiques. Donc lorsqu'il y a un problème, s'il y a un bug de sécurité, nous fournissons de nouvelles clefs de racine et c'est quelque chose qui arrive rapidement. Et nous ajoutons régulièrement de nouvelles fonctionnalités.

Donc vraiment le matériel est très puissant, c'est un dispositif qui peut être utilisé pour d'autres choses, ce n'est pas uniquement un routeur.

Alors en ce qui concerne la sécurité, c'est vraiment la sécurité qui est la base de notre recherche. Ce dispositif ne devrait pas vus permettre d'avoir une installation qui n'est pas sécurisée. Il vous guide dans tout le processus de configuration, et tout ce qui est port ouvert ou mot de passe pas puissant, vous ne pouvez même pas le mettre en place.

Ensuite au niveau de la communication et des mises à jour, tout est très bien conçu. Il y a un ensemble de clés qui est unique. Donc tout ce qui est cryptographie est très solide.

Il y a d'autres fonctionnalités, par exemple [honeypot], pot de miel, il y a également l'analyse des flux, si par exemple il y a un dispositif activé qui fait quelque chose d'inattendu sur l'internet, ce sera identifié. Nous redonnons les résultats de l'analyse collective. Donc il y a un pare-feu qui s'adapte selon les situations. Les serveurs VPN, etc. Donc beaucoup de fonctionnalités supplémentaires.

Il est adapté aux IPv6 et il est très souple, très flexible. Donc vous pouvez utiliser un autre serveur comme machine virtuelle, donc ça vous montre à quel point il est puissant.

Et surtout, ce qui est très important pour nous, c'est qu'il y a une validation DNSSEC par défaut. Et donc c'est en fait à la fois le positif et le négatif de ce projet.

Encore une chose, le DNS est vraiment utilisé, exploité dans ce dispositif. Donc il y a un ensemble de clefs, utilisé par le dispositif en cas d'incidents de sécurité. Et donc les ensembles de clefs s'ils sont compromis ne peuvent passer à un autre ensemble de clef. Donc le DNS est très important et la validation est très importante également dans le dispositif.

Alors quand nous avons commencé, il y a eu beaucoup de leçons que nous avons tirées de notre travail, par rapport au système d'exploitation qui est constamment en évolution. Donc au début, on était un petit peu naïf, c'était un petit peu compliqué, on pensait qu'utiliser un dispositif qui faisait la validation du DNSSEC c'était la même chose, mais en fait c'est pas si facile que ça.

Tout d'abord, il y a beaucoup de problèmes, alors il y a certaines organisations qui provoquent ces problèmes et en général, c'est les FSI. Ils sont très créatifs avec le DNSSEC. Et donc très rapidement, on s'est dit qu'il fallait absolument fournir des pages d'information pour les utilisateurs qui leur disent pourquoi le routeur ne fonctionne pas correctement.

Donc ça c'est une des premières mises à jour que nous avons mises dans le système d'exploitation.

Les principaux problèmes sont les suivants, donc l'infrastructure qui ne fonctionne pas bien chez les FSI, les problèmes

d'implémentation ancienne de DNS, les récurseurs problématiques. Parfois il y a des boitiers intermédiaires qui ne fonctionnent pas, qui sont cassés, et qui modifient le trafic DNS. Parfois il y avait des problèmes qui étaient résolus mais qui étaient oubliés, malheureusement, par le boitier intermédiaire. Et pour certains, le trafic port 53 était rejeté. Donc il était très compliqué de fonctionner sur le réseau si le résolveur ne fonctionne pas. Et malheureusement c'est souvent le cas.

Alors une chose, pas uniquement du côté des FSI, mais un autre problème quand on a commencé, au début on a utilisé le Unbound sur les bleus, mais donc encore une fois, étant donné qu'on pouvait faire des mises à jour automatiques du système, on a identifié pas mal de bugs, et on a pu les résoudre grâce aux résolveurs.

Et enfin, de temps à autre, il y a des problèmes de serveurs faisant autorité qui ne fonctionnaient pas. Surtout la question EDNS. Voilà, on pourra en parler un petit peu plus tout à l'heure de ça.

Donc voilà la page en ce qui concerne le DNS. Comme vous le voyez, la description est assez longue sur ce qui se passe. Il n'y a pas beaucoup de personnes qui l'utilisent. Nous avons beaucoup d'appels mais nous essayons au moins d'éduquer les gens par rapport aux problèmes qui peuvent se produire sur le

DNS. Et il y a plusieurs options. Ils peuvent soit utiliser, soit ne pas utiliser le résolveur, et parfois il faut leur dire de désactiver la validation DNSSEC. Si vous choisissez de désactiver, on informe les gens qu'il faut que ce soit provisoire, mais malheureusement parfois c'est la seule option pour qu'il y ait connectivité. Donc les gens sont obligés d'éteindre DNSSEC pour pouvoir se connecter à l'internet.

Il y a plusieurs tests qui identifient les problèmes. Il y a des gens qui arrivent à faire des rapports aux FSI, mais certaines FSI résistent un petit peu, sont réticentes. Et c'est difficile de les convaincre. Malheureusement, parfois ils ne nous font pas confiance.

Mais déjà le fait de pouvoir cocher, ça permet de résoudre quand même pas mal de problèmes.

Donc je conclus. Donc en grande partie les problèmes sont au niveau des FSI, ils ont souvent des problèmes de sécurité au niveau du DNS. On introduit une solution et ils oublient la solution. Et donc il faut vraiment entrer en discussion avec eux, parce que ce n'est pas aux utilisateurs finaux de le faire. C'est ce qu'on essaye de faire, mais ce n'est pas évident.

Nous avons dû introduire une interface de configuration avec des tests, et ça c'est utile, parce qu'au moins les utilisateurs peuvent comprendre le problème. Si les FSI ont un cerveau, en

général ils arrivent à comprendre ce qu'il se passe. Donc ça a permis de réduire le nombre d'appels à la ligne d'assistance.

Et, autre chose qui a été annoncée la semaine dernière, comme solution, les développeurs des résolveurs open source ont décidé d'envoyer des contournements pour les résolveurs en 2019. Donc ça, ça devrait être lancé en 2019, et vous n'êtes pas les seuls à pouvoir en profiter.

Donc n'hésitez pas à aller sur cette page pour tester par vous-même. Donc ça devrait être résolu après février 2019.

Et si vous me le permettez, je vous montre encore une chose, donc ça c'est un nouvel outil, une nouvelle version qui sera très, très souple. Avec différentes pièces, vous pourrez jouer un petit peu avec ce module.

Et encore une fois, nous sommes une organisation à but non lucratif, donc n'hésitez pas. Donc nous travaillons avec Indiego. Voilà, c'est tout ce que j'ai. Merci beaucoup.

RUSS MUNDY: Merci Andej, Jacques vous avez une question.

JACQUES LATOUR: Oui, quand vous dites que vous êtes flexible, ça veut dire qu'on peut le prendre et faire comme ça ?

ONDREJ FILIP: … Vous pourriez peut-être concevoir vous-même des routeurs.

VIKTOR DUKHOVNI: Est-ce que vous avez des statistiques par rapport aux améliorations dans le panorama des FSI ?

ONDREJ FILIP: Oui, bien sûr. Nous sommes une compagnie publique. Donc les appels téléphoniques ne sont pas très efficaces avec les FSI, et nous avons des estimations. Moins de 1 % des utilisateurs se retrouvent confrontés à ce problème. Donc la plupart des FSI sont ok, fonctionnent bien, mais c'est à peu près 1% des utilisateurs qui se trouvent confrontés à ce problème.

FREDERICO NEVES: Ondrej, les anciennes versions du matériel, est-ce qu'elles sont compatibles avec le nouveau logiciel ?

ONDREJ FILIP: Oui, elles sont compatibles. Les plateformes CPU sont les mêmes et donc la plupart d'entre elles ont fonctionné pendant des années et les versions sont compatibles.

FREDERICO FILIP: Est-ce que vous êtes compatibles avec d'autres plateformes, est-ce que vous êtes compatible avec d'autres matériels avec le Omnia software ?

ONDREJ FILIP: Pas vraiment, il n'y a pas tellement d'autres matériels qui soient compatibles dans le marché. Parce qu'il y a des spécificités qui sont difficiles à rendre compatible. Mais c'est un aspect que l'on pourrait envisager pour l'avenir.

RUSS MUNDY: Il y a un micro derrière ? Oui.

ABDALMONEM GALILA: Je suis coach de l'ICANN. Je pense qu'il y a une grande partie des administrateurs qui ne font pas de validation. Il est difficile d'administrer DNSSEC, ou d'administrer cette validation. Alors Turris, est-ce que ce dispositif Turris rend moins difficile l'administration de cette validation ?

ONDREJ FILIP: On croit qu'en général la plupart de FSI qui utilisent ces routeurs trouvent que c'est plus facile. La validation se rapproche plus des utilisateurs.

Avec Turris, ça s'améliore un peu.

RUSS MUNDY: Très bien Ondrej. Est-ce qu'il y a d'autres questions ? Oui ? S'il vous plait. Il y a un micro là-bas.

S'il vous plait, rapprochez-vous du micro pour parler.

NON IDENTIFIE: J'ai une question. Est-ce que dans ce système la validation se fait pour les [CPE] ? Est-ce que c'est ok ?

ONDREJ FILIP: Pour quoi ce ne serait pas bien ? Oui, la validation se fait au niveau de ce dispositif, oui, c'est bien, c'est ok.

Le titre c'est validation et CPE, et donc c'est un routeur au niveau des foyers, c'était le titre.

NON IDENTIFIE: Qui valide ?

ONDREJ FILIP: Le routeur, chez vous.

NON IDENTIFIE: Quel logiciel utilisez-vous pour le CPE ?

ONDREJ FILIP: Vous parlez de la validation DNSSEC ? HA oui, les anciennes versions que nous utilisions c'était Unbound, et les nouvelles versions utilisent un nouveau logiciel.

NON IDENTIFIE: [Inaudible], Unbound, est-ce que ça utilise CP ? Ça va à travers le CP ?

ONDREJ FILIP: Oui.

NON IDENTIFIE: Merci.

RUSS MUNDY: Je me rends compte, pendant cette présentation que quelqu'un de mon FSI, dans mon pays était ici, et j'ai utilisé le routeur Turris chez moi, et donc j'ai eu accès direct si j'avais eu des problèmes, mais je dois dire que sur 3 ans d'utilisation de ce routeur Turris et de validation DNSSEC, je n'ai jamais eu de problème avec ce routeur.

Alors il fonctionne très bien. Je voulais signaler cela devant vous.

Merci Ondrej de cette présentation. Je pense que nous devons avancer.

NON IDENTIFIE: Le Turris donc, pour le roulement de la clef, est-ce que cela peut se faire automatiquement sur le routeur Turris ou faut-il avoir une intervention manuelle ?

ONDREJ FILIP: Non, c'est automatique, c'est automatisé.

RUSS MUNDY: Merci Ondrej. Notre prochain intervenant de cette matinée est Jack Zack de CIRA. Ha ! c'est vous ? Vous le faites, d'accord, très bien. Alors c'est Jacques Latour qui fera la présentation à la place de Jack Zack.

JACQUES LATOUR: Jack est malade, et donc je ferais la présentation à sa place. J'ai toutes les notes de Jack.

Alors sa présentation concerne la nouvelle génération de signataires de CIRA que Cira a mis en oeuvre très récemment. Nous allons parler de cela.

Très bien, un aperçu général qui rejoint ce qu'on a dit avant on a 2.7 millions de domaines signés, 2400 délégations signées. La plupart des registres sont dans cette salle.

Alors il y a quelques réunions de l'ICANN, il y a quelques années, nous avons présenté notre solution avec BIND et AEP Keyper. Nous avons maintenant utilisé une nouvelle infrastructure qui utilise OpenDNSSEC et Gemalto HSM. Nous avons migré donc pour le roulement de la KSK, nous allons donc basculer vers ces deux nouvelles configurations de signature.

Vous voyez la configuration que nous avons créée il y a 5 ou 6 ans, avec beaucoup de disponibilité au niveau de l'infrastructure, parce que nous voulions atténuer les risques de pannes du DNS.

À l'époque, nous avions deux zones, nous avions généré deux fois la zone, nous signions avec différents signataires, nous signions avec BIND et ensuite nous faisions une validation extensible et nous comparions les deux validations pour nous assurer qu'il n'y avait pas de différence entre les zones.

Maintenant nous publions cette zone sur internet.

Alors quand nous avons mis tout cela en production, la première année nous avons trouvé quelques bugs au niveau opérationnel.

Alors à l'époque on utilisait ce système quand on se méfiait un petit peu du signataire.

Nous avons tiré beaucoup d'apprentissage de cette architecture, et nous avons créé un nouveau système qui est beaucoup plus efficace.

En ce qui concerne la disponibilité, le côté Backup était toujours froid, le processus côté backup était un petit peu compliqué.

Donc nous avons activé une base de données passive, nous utilisons OpenDNSSEC, une version que nous avions utilisée pour la production. Nous ne l'avons pas mise à jour parce qu'elle fonctionnait très bien.

Et ensuite nous avons ajouté d'autres instances de validation. Nous avons donc préparé tout ça sur mesure pour nous assurer que cela fonctionne bien.

Le processus, il nous a pris entre 25 à 35 minutes de générer la zone, cela était basé sur CRON. Nous allons créer, donc générer la zone. On a passé par des étapes de validation, SEP, comparé avec BIND. Et nous assurons que tout se passe bien. Nous copions la zone côté backup et la signons aussi côté backup en temps réel et nous comparons les deux. C'était vraiment un processus de manipulation des données assez important et nous avons réussi à l'optimiser.

Avec ce système nous n'avons pas eu de panne au niveau de la zone.

À l'époque, nous n'avions pas de basculement entre les sites, et tous les signataires, toutes les validations se faisaient sur des serveurs LAN, il y avait beaucoup de copies qui se faisaient, beaucoup de traitement, et c'était trop, c'était trop long.

Alors nous avons décidé et nous utilisions également un [AEP Keyper], et donc nous avons envisagé la possibilité de remplacer ce HSM avec une version beaucoup plus performante au niveau des processus.

Dans la version précédente il fallait faire des interventions manuelles, à l'époque cela fonctionnait, mais il y a des choses plus modernes qui peuvent être plus efficaces et qui proposent les mêmes niveaux de sécurité.

Pour ce qui est de la validation, au début, comme je vous ai dit, on comparait les deux zones et nous avons trouvé beaucoup de bugs, des problèmes au niveau de la mise en œuvre. Pour la plupart, dans .CA, nous avons signé beaucoup de noms de domaine, nous avions [OD, OCA], et nous avions des QC.CA, toutes les délégations, toutes les provinces du Canada, et on a retrouvé des problèmes de validation là-dessus. En général, quand on met un enregistrement DS, nous avions également d'autres zones qui correspondaient à des villes à des provinces,

et quand on ajoute un enregistrement DS à un quatrième niveau, on ne pouvait pas toujours valider ce type d'infrastructure.

Et cela nous a pris du temps pour pouvoir résoudre ces problèmes.

Ensuite, BIND et ODS utilisent des signatures différentes. Donc Jack devait manuellement intervenir pour pouvoir comparer ces deux méthodes, et il a fallu beaucoup d'interventions pour relancer et resigner. Ça nous a pris du temps, ça nous a empêchés de regarder plusieurs Super Bowl.

Maintenant, le nouveau système est beaucoup plus simple, nous passons de 16 machines physiques à 8 VM. Et maintenant 4 VM pour simplifier. Mais nous avons décidé d'avoir la zone distribuée en deux instances. Alors tous ces boitiers sont dans des zones différentes, derrière des pare-feux internes. Donc c'est beaucoup plus optimisé au niveau de l'architecture. Nous avons une génération de zone, une validation, et nous avons de la distribution de zones séparée.

Nous utilisons, comme je vous ai dit, nous avons évalué les possibilités et nous avons décidé d'utiliser Gemalto, Luna et [HSM], c'est un HSM qui vient d'une compagnie reconnue, qui s'appelle Gemalto, et nous avons aimé cette version parce qu'on peut faire avec eux tout ce que vous voulez, on a des partitions.

La principale raison pour laquelle nous avons changé, c'est parce qu'il y a des solutions qui sont intégrées dans un nouveau service que nous voulons mettre en place, service de signature. Donc ce système nous permettait de mettre en place ces solutions que nous voulions mettre en application. Et nous ne devons pas répliquer la même infrastructure. Gemalto donc est une infrastructure qui nous permettait de mettre en place notre projet.

Il y a beaucoup de fonctionnalité, de capacités, 20 partitions, plus de 5 clefs, beaucoup de flexibilité. C'est plus facile également avec Gemalto de faire la cérémonie de signature, de manière plus rapide.

Avec Gemalto, le processus demande une heure, on a 1 heure de processus au lieu de plusieurs heures avec le HSM précédent. Il y a une amélioration au niveau du temps du processus.

Nous avons également changé au niveau de la base de données, nous avons choisi ORACLE ODA, ça veut dire que nous générons dans la zone DNS active, et active dans les deux zones, et nous recevons des informations en temps réel de la zone backup et de la zone primaire.

Notre site backup est à une seconde de différence par rapport au site principal, ça fonctionne très bien. C'est un peu cher, mais ça fonctionne très bien.

Alors nous ne faisons plus de signature de zone deux fois, nous avons choisi ODS, c'était un choix. Nous utilisons Springbatch. La génération de zone fonctionne beaucoup mieux maintenant, au niveau de la signature.

Les HSM ont un équilibrage au niveau des charges. Nous utilisons donc les mêmes contrôles des HSM que nous avions conçus pour les cérémonies de signature, dits DPS, définit la structure pour gérer les clefs. Nous avons donc différentes personnes au bureau, qui jouent différents rôles, et Gemalto permet que l'on travaille avec ces différents rôles. Nous avons un officier cryptographique, nous avons un officier de sécurité, certaines personnes ont accès aux salles, d'autres n'ont pas cette possibilité d'accès. Nous avons pu répliquer donc le CPS dans notre pratique DNSSEC.

Donc tout cela fonctionne maintenant avec le HSM Gemalto. Cela nous permet de faire la signature de clef, la cérémonie de signature de clef beaucoup plus facilement. Il y a un [keypad] qui nous permet de mettre en place cette cérémonie de manière plus efficace.

En même temps que l'on a fait le changement de HSM et le roulement de clef avec le HSM, nous avons dû faire un roulement de KSK, parce qu'on avait une clef dans l'ancien HSM, et la nouvelle clef était dans le nouveau HSM. Alors nous avons

fait ça doucement, nous avons roulé cette clef, et nous avons changé la clef, et nous avons changé le HSM, le module matériel sécurité.

C'est difficile à voir, mais vous avez ici les processus, donc on a la KSK en production, nous avons introduit une nouvelle KSK dans zone du nouveau signataire, et au fil du temps, nous avions une clef, après on a eu les deux clefs avec la nouvelle clef qui signait avec l'ancienne clef, et doucement nous avons basculé, on a changé le HSM et nous avons basculé vers la nouvelle clef.

Vous voyez là les différents changements que nous avons mis en place, c'est assez clair, assez facile. Au niveau de la signature de clef, le processus de changement de clef a été assez direct.

Et à un moment donné, nous avons réfléchi à la possibilité de changer le protocole, à partir des apprentissages que nous avons pu tirer d'autres expériences, on a pensé que ce n'était pas une bonne idée.

Donc on a pris les choses en douceur, nous avons attendu des semaines, nous ne nous sommes pas pressés à mettre en place ce changement, nous l'avons fait progressivement. Nous avons eu à un moment donné des multiples KSK, mais à terme, tout s'est bien passé avec ce processus.

Alors le changement de plateforme s'est bien passé, il n'y a pas eu de problème de signalé. Avant, on générait la zone en une heure, maintenant on le fait en 30 minutes. Le processus de KSK, les cérémonies KSK pardon, peuvent être gérées à distance maintenant avec le HSM. Maintenant le processus est automatisé, avant il fallait intervenir sur place avec des cartes à puce, etc. tout cela a changé. Donc on n'utilise plus [Perl] et voilà pour ce qui est du processus.

Alors, y a-t-il des questions ?

RUSS MUNDY: Merci Jacques. Y a-t-il des questions pour Jacques ?

ROBERT MARTIN-LEGENE: Donc je suis avec PCH. Ha vous parlez espagnol, c'est ça ? On peut parler en espagnol ?

Alors, vous avez mentionné les anciens HSM et les nouveaux HSM, et comme quoi ils sont très différents en termes de gestion.

J'ai eu l'impression dans ce que vous disiez qu'il y avait eu beaucoup d'avantages à tirer, lors du changement parce que vous n'aviez pas besoin de matériel en plus pour le secours. Ça

c'est uniquement parce que vous avez le changement ou c'est parce que vous avez fait l'automatisation en même temps ?

Alors avancez de deux diapositives s'il vous plait, là.

Vous avez : unité de secours Gemalto, même niveau de sécurité. Et avant vous aviez besoin d'un HSM total hors ligne, et vous n'en avez plus besoin, c'est ça ?

JACQUES LATOUR: Avant d'ajouter le HSM hors ligne, on fait la cérémonie de signature de clef avec le HSM hors ligne, ça n'allait pas en matière de sécurité ; donc on a généré une nouvelle clef, on prit la carte à puce et on l'a mis dans tous les autres HSM pour les reprogrammer.

Donc avec Gemalto, ils ont un cadre qui permet d'avoir une commande, en fait c'est un clavier qu'on peut utiliser pour gérer à distance tous les HCM. Vous appuyez sur les clefs, vous changez les clefs en fait d'un endroit sécurisé.

Donc il faut installer, je crois que c'est une clef noire qui crée la confiance parmi tous les HSM, et de notre bureau on peut reconfigurer tous les HSM en utilisant ce clavier.

Plutôt que de protéger… En fait on avait le HSM hors ligne dans un coffre fort, donc ça permet un bon accès maintenant on a, en fait un clavier dans le coffre fort et c'est ça qui est protégé.

ROBERT MARTIN-LEGENE: Alors PCH utilise en fait, fait ce que vous faisiez. Nous, on ne se promène pas dans le monde entier. Je ne comprends pas vous deviez faire ça.

JACQUES LATOUR: Lorsqu'on est hors ligne, tous les HSM sont hors ligne n'est-ce pas ?

ROBERT MARTIN-LEGENE: Pour KSK oui, les HSM sont hors ligne.

JACQUES LATOUR: Donc nos KSK c'était ça. Si on souhaite ajouter un nouveau client, etc. on peut le faire immédiatement on n'a pas besoin d'attendre la cérémonie de signature de clef, qui a lieu tous les trimestres pour ajouter un client. On n'a pas besoin d'attendre.

ROBERT MARTIN-LEGENE: Oui, il y a des pour et des contres. Est-ce que vous avez une vidéo de votre cérémonie de signature de cle ? Vous avez mentionné ça tout à l'heure.

JACQUES LATOUR: C'est pas quelque chose qui est public, mais si vous voulez la voir…

ROBERT MARTIN-LEGENE: Oui, je veux absolument la voir.

JACQUES LATOUR: Alors il va falloir me payer une bière.

JOE ABLEY: Je voulais faire un petit commentaire. Je me souviens qu'au tout début, lorsque vous avez installé les DNSSEC, beaucoup de processus étaient modelés par rapport à ce qu'il se passait sur la racine surtout par rapport au modèle HSM. Et à une époque effectivement c'était le seul HSM qui était certifié au niveau requis par le département de commerce pour l'ICANN. Donc il n'y avait pas beaucoup d'options à l'époque.

Mais apparemment le processus a évolué par rapport à ce qui était approprié pour la zone racine, plutôt que de se focaliser sur la sécurité et en fait de se concentrer sur les opérations.

Je crois que c'est un bon message. Il y a beaucoup de gens qui ont copié l'ICANN, et donc je pense que l'évolution c'est bien de savoir qu'elle a eu lieu.

[VINCENT]: [Inaudible], d'AFNIC. J'ai une petite question de processus. Premièrement, les qualifications, vous avez dit qu'avec un nouveau processus il faut environ 11 minutes. Est-ce que vous faites une génération de fichiers zone totale ?

JACQUES LATOUR: Oui.

NON IDENTIFIE: Et est-ce que vous avez considéré peut-être l'utilisation de quelque chose de plus dynamique ?

JACQUES LATOUR: Oui.

NON IDENTIFIE: Et pourquoi vous ne l'avez pas fait ?

JACQUES LATOUR: Parce qu'il faut 11 minutes pour faire toute la racine. Donc si on peut conserver le processus qui existe et que l'on reste en dessous des 15 minutes, ça va. Mais nous n'avons que 2000 délégations signées. Et quand on arrivera au million…

NON IDENTIFIE: Oui, c'est ça la deuxième question, si vous deviez faire le processus avec 10, 20 % de délégations signées… Est-ce que c'est extensible ?

JACQUES LATOUR: Si on a l'adoption pour le .CA.

NON IDENTIFIE: Je vais aussi rapide que possible pour la dernière question, est-ce que vous avez fait des tests sur une plus large échelle, parce que je sais que le processus de signature est plus long avec le 2048. Est-ce que vous avez testé, et est-ce que c'est extensible ?

JACQUES LATOUR: Je ne crois pas, mais le niveau de performance entre le Gemalto et l'AEP, c'est un facteur, donc c'est 10 fois plus rapide.

NON IDENTIFIE: Je le dis, parce que je sais qu'il y a un facteur entre Gemalto et AEP, mais étant donné la taille différente des clefs, parfois la différence n'est pas énorme. Donc je pense qu'il faudrait faire des tests par rapport à ça.

JACQUES LATOUR: Oui, effectivement, il faut qu'on voie ça.

RUSS MUNDY: Merci beaucoup Jacques. Notre présentation suivante est par Joe Crowe de Comcast qui va nous parler des ancres de confiance négative. Joe, c'est à vous.

NON IDENTIFIE: Petit commentaire, en fait on compare des choses qui sont différentes parce que si j'ai bien compris, le Keyper, c'est le seul niveau de validation d'HSM sur le marché. Gemalto c'est un niveau 3.

JACQUES LATOUR: Et il n'est pas obligatoire de certifier.

NON IDENTIFIE: Oui, tout à fait, ce n'est pas ça. Je fais un commentaire à Joe en fait là-dessus.

JOE CROWE: Bonjour. Je représente Comcast, je suis ingénieur en chef. On a une équipe pour le NTP et DHTP.

Nous faisons la validation depuis 2012, et donc le DNSSEC est extensible. Si vous êtes là-dessus, il faut absolument valider le DNSSEC.

Alors qu'est-ce que ça veut dire pour Comcast ? Lorsqu'il y a un problème de validation DNSSEC, les clients nous blâment, ils pensent que nous bloquons les sites. Les clients sont tout de suite au téléphone lorsqu'ils n'arrivent pas sur le site qu'ils aiment. Je sais que NASA.GOC c'est souvent celui dont on parle. Là vous avez HBO Now. Ils ont lancé HBO Now et dès le lancement, le DNSSEC ne fonctionnait pas. On n'a pas pu valider correctement et Tweeter a explosé.

Donc la neutralité du net, voilà, hein on bloque.

Donc les gens en fait avaient un résolveur non validant, ils essayent de passer à Google et Google fait la même chose étant donné que eux aussi ils ont eux aussi ils ont une validation DNSSEC.

Alors une des solutions temporaires possibles, c'est de mettre une ancre de confiance négative. Alors pourquoi est-ce qu'on utilise cette ancre de confiance négative ? Et bien parce que

c'est trop énorme pour avoir un échec, une défaillance. Et puis il y a le problème de la sécurité.

Sait-on si ce domaine NASA.GOC, STATE.GOV, bon c'est très souvent gouvernemental tout ça, mais est-ce que c'est vraiment une question de sécurité ou est-ce une question opérationnelle ? C'est ça le problème.

Et la plupart du temps, c'est un problème opérationnel. Il est très rare que l'on remarque qu'il y a réellement un problème de sécurité. Et depuis que je suis à Comcast et que je m'occupe de ceci, en fait je ne vois pratiquement jamais de problème de sécurité. En général c'est des problèmes opérationnels.

Alors, que fait-on ? Il y a plusieurs options. Donc on laisse le domaine échouer, on éteint le DNSSEC, ou alors on met une ancre de confiance négative pour ce domaine, pour que ce domaine continue d'être résolu par le résolveur, sachant que la validation DNSSEC a l'arrière, elle ne fonctionne pas.

Alors pour la mise en place de cette ancre de confiance négative, au tout début, il faut déjà avoir un bon processus. Donc rassembler l'équipe, voir un petit peu quand et pourquoi est-ce que vous souhaitez le faire, comment le mettre en place sur les résolveurs.

À l'interne, nous utilisons différents fournisseurs, donc il faut s'assurer de bien avoir un processus pour tous ces fournisseurs, parce que s'il y a u échec de la validation, il faut quand même mettre les choses en place. Et il faut tester le processus. Si par exemple, l'implémentation des NTA par les fournisseurs a changé, il faut bien le savoir, bien mettre à jour votre processus automatisé, et informer toute l'équipe.

Donc il faut connaitre les risques. Si on continue le problème du domaine, est-ce qu'il va y avoir des couts qui seront associés, pendant combien de temps est-ce qu'il y aura échec du domaine ? Plus on reçoit d'appels à Comcast, plus cela est cher. Donc est-ce qu'il y a vraiment un échec, une défaillance du domaine ? Parce que si c'est opérationnel, et bien il faut faire les vérifications, le dépannage, s'adresser aux bonnes personnes que ce soit par email, par tweeter, informer les gens qu'il y a effectivement une défaillance de ce domaine, nous avons informé les personnes. Nous avons en fait un tweeter qui est consacré à ça et qui est surveillé par l'équipe constamment.

Si vous avez plus de 25 serveurs, en fait ça fait 2 en réalité, et que si vous automatisez tout ceci, l'ancre de confiance négative, doit être approuvée par les dirigeants, les cadres supérieurs. Donc si on peut prouver aux dirigeants que oui, il y a un problème opérationnel, à ce moment-là si nous nous sommes adressés aux personnes adéquates, mais s'il faut par exemple 15, 20

minutes pour obtenir une réponse, si c'est un gros site comme NASA.GOV, STATE.GOV, ou HBO NOW, etc. on met en place la NTA, parce que les couts associés seraient énormes. Donc il vaut mieux ne pas laisser échouer ce site.

Mais il faut donc contacter les dirigeants dans ce cas.

L'automatisation permet l'extensibilité. Dans notre cas, nous avons plusieurs fournisseurs avec différentes commandes qui implémentent nos NTA. Et s'il y a une erreur, il y a une erreur dans un endroit, mais tout le reste est interrompu. On sait qu'en fait l'erreur est la même partout et que nous pouvons résoudre le problème relativement facilement.

Comme dans toutes les bonnes équipes opérationnelles, il faut faire les tests dans les labos. Il y a des gens qui disent oui, moi je fais tous mes tests en production, mais à mon avis ce n'est pas la meilleure option.

Donc les opérations de base à Comcast, donc on utilise SaltStack comme outils d'automatisation. Nous avons des données qui nous permettent de mettre à jour le lieu spécifique avec le domaine qui échoue. Cela nous permet d'utiliser les données pour plusieurs fournisseurs, avec un seul script et nous avons un Salt Master qui peut être répandu dans des centaines de serveurs. Et ça, on le fait avec un système de roulement. Donc on teste dans un endroit, on voit si ça fonctionne et ensuite on

dissémine tout ceci, et en général cela prend quelques minutes, jusqu'à 10 minutes, ça dépend un petit peu le rythme auquel on souhaite fonctionner. Une fois qu'on a testé suffisamment, on sait qu'on peut diffuser la solution.

Alors la structure pour nos données pilier, vous voyez donc le format NTA. Nous avons un NTA interne, client interne, qui est en fait plus important. Avec les anciennes pratiques qui parfois à l'interne peuvent casser le DNSSEC, mauvaise délégation, etc. Donc lorsqu'on essaie de mettre en place le DNSSEC à l'interne, c'est en général le plus gros obstacle auquel nous sommes confrontés. Donc nous utilisons le format que vous avez, donc le format YAML, et les scripts sont absorbés par d'autres fichiers, et en fait par la suite nous faisons nos tests.

Je pense que pour la plupart d'entre vous, vous savez comment se passe le dépannage, en cas de problème DNSSEC, vous avez le Servfail comme résultat, ensuite vous ajoutez le CD, vous souhaitez utiliser le dig comme première étape. Et ensuite vous testez avec un autre résolveur validant le DNSSEC pour vous assurer que ce n'est pas uniquement votre résolveur. Ensuite le DNSviz.net, c'est votre ami. Nous avons le [DNSSEC-failed.org], donc si vous voulez allumer la validation, vous pouvez l'utiliser comme domaine pour tester, pour vous assurer que vous avez un problème de validation, pour confirmer vos suspicions.

En termes de roulement de clef, donc on fait une purge du cache pour solutionner le problème de DNSSEC.

Alors une chose qui est ressortie de la conversation avec OARC, c'est de voir comment nous pourrions travailler avec Google, Comcast, d'autres validateurs de DNSSEC, et à l'interne, ce dont on a parlé, c'est d'automatiser vos propres zones et d'utiliser le DNSviz, le CLA pour charger vos propres zones pour effectuer des vérifications pour voir si les zones fonctionnent correctement avec le DNSSEC. S'il y a un problème d'email vous serez alerté, et vous pourrez identifier le problème avant qu'il se répande. Les TTL, parfois, peuvent vous aider aussi.

STATE.GOV avait des problèmes hier à un moment, et au bout d'un instant, il y a eu solution, et en fait c'était simplement, la solution c'était de purger le cache. Voilà.

C'est tout ce que j'avais à dire. Y a-t-il des questions ?

RUSS MUNDY: Ha, voilà, allez y prenez le micro Monsieur. Paul.

PAUL WOUTERS: [John Gilmore] l'a dit, si on ne peut pas faire confiance à ses amis, à qui est-ce qu'on ne fait pas confiance ? Donc dans ce cas, on ne peut pas savoir s'il y a une ancre de confiance négative, de

manière mal intentionnée en fait. Par exemple si le gouvernement est en train de vous menacer avec un fusil et de vous dire ; vous êtes obligé de le faire, je vous l'impose.

Donc est-ce que vous publiez ces ancres de confiance négatives, et comment est-ce que vous évitez la honte aussi ? Mais ce serait bien en fait en terme d'audit, s'il y avait quelqu'un qui vérifiait votre processus.

JOE CROWE: Alors, pour l'instant nous n'avons pas de publication des NTA et je suis d'accord avec vous. Parfois la question de la honte, ce n'est pas forcement la meilleure approche. Oui, votre système est cassé etc. Mais dans le cas de Comcast, nous devons informer nos clients, nous devons leur dire que nous savons qu'il y a un problème. C'est là que le tweeter de Comcast sur le DNS est utile parce qu'on peut dire : nous sommes au courant, ce site web a un problème de validation DNSSEC, nous leur donnons en fait l'option de trouver une solution.

Pour la publication des NTA, j'y pensais justement. Ça, c'est quelque chose qui devrait se passer au niveau de toute la communauté pour qu'on décide en fait de comment publier. Je ne pense pas que Comcast doit être la société qui prenne cette initiative en fait.

RUSS MUNDY: D'autres questions ?

ROBERT MARTIN-LEGENE: Et si le DNSSEC est activé sur Tweeter. Com et que le DNSSEC ne fonctionne pas ?

JOE CROWE: Et bien, je ne sais pas, il n'y a pas de réponse. Effectivement, on essaierait de trouver un autre moyen. Notre équipe assistance saurait que le DNSSEC est en échec pour les grands domaines, par contre les petits domaines, ce n'est pas ce qui nous inquiète. C'est vraiment les partenaires d'affaires qui nous importent, les sites qui vraiment provoquent une réaction très publique.

VIKTOR DUKHOVNI: Je sais que votre équipe courriel a un processus similaire pour une white liste des domaines qui sont en échec. Est-ce que c'est la même logistique ou est-ce que vous gérez ça séparément ?

JOE CROWE: L'équipe courrier, c'est complètement séparé, ils ont leurs propres processus. Et ça n'a rien à voir avec ce que nous faisons.

RUSS MUNDY: Apparemment, il y a des gens qui arrivent dans la salle, leur réunion devrait commencer à midi et quart.

Alors je ne sais pas s'il y a un problème dans l'ordre du jour, est-ce que quelqu'un a fait une erreur?

Alors, notre déjeuner ne sera prêt qu'un petit peu plus tard.

Voilà, nous avons un problème de salle de réunion.

Bon, alors apparemment, il y a eu une erreur dans le calendrier. Tout ce que j'ai moi me montre midi.

Bon, donc notre équipe n'était pas au courant de ce petit changement, donc nous allons devoir sortir de la salle, et donc notre déjeuner, il est prévu pour midi et quart, midi vingt à peu près, donc vous avez amplement le temps d'aller manger et on fera le test, la petite interrogation après.

Alors, les billets les voici, vous les avez là. Alors prenez bien votre billet avec vous avant de monter.

Le déjeuner est servi sur la terrasse du troisième étage, du niveau 3. Donc allez-y, prenez vos billets, vos papiers, vos documents, parce qu'apparemment la salle sera occupée par d'autres personnes.

Donc nous reprenons à 13 h 30.

NON IDENTIFIE: Et ne soyez pas en retard, j'ai beaucoup de diapositives. Et il faudrait vérifier que nous avons bien cette salle à 13 h 30.

RUSS MUNDY: Oui, on se retrouve à 13 h 30.

[FIN DE LA TRANSCRIPTION]