Le FBI remonte une Cyberattaque jusqu’à Abidjan

Le FBI remonte une Cyberattaque jusqu’à Abidjan

La Banque centrale des Etats-Unis d'Amérique reçoit sur son système d'information (SI) un flux important de données provenant d'un réseau de machines inconnues. Lorsque les cyberdétectives du Bureau fédéral d'investigation (FBI) essaient de remonter jusqu'à l'origine de l'offensive, ils sont dirigés vers plusieurs continents, via des serveurs informatiques qui interagissent entre eux. Autant de rebonds sur des machines, rendant la piste des attaquants difficile à suivre.

Toutefois, des empreintes laissées sur internet permettent aux agents du FBI de localiser des serveurs situés en Côte d'Ivoire. Signe de la gravité de la cyberattaque, les fins limiers du web américain débarquent à Abidjan.

Sur place, après une séance de travail avec l'équipe d'experts en sécurité informatique du**CI-CERT (Côte d'Ivoire – Computer emergency response team)**, le FBI parvient à identifier à partir d'une liste d'adresses IP, des entreprises ivoiriennes, dont les machines infectées, sont utilisées à leur insu par des hackers basés en Thaïlande, pour lancer des offensives contre le SI de la Banque centrale des Etats-Unis d'Amérique.

Ce n'est pas le scénario d'un film américain, mais une réelle attaque informatique qui s'est déroulée dans le premier trimestre de l'année 2013, et qui a été décrite à CIO Mag par Jean-Marie Nicaise Yapoga, chef de service du CI-CERT, alors responsable technique adjoint. Pointant la vulnérabilité des entreprises qui s'exposent à des risques dus au non-respect des bonnes pratiques en matière de cybersécurité (Cf. CIO Mag N°29 – décembre 2013/janvier 2014).

L'expertise du CERT ivoirien dans cette affaire a permis aux entreprises infiltrées de limiter les dégâts et de réduire le coût du retour à un fonctionnement normal. Mais elle rappelle surtout l'essentiel de sa mission : assurer, au niveau local, la fonction de point focal pour toutes les questions de cybersécurité.

Des couches de sécurité sans protection suffisante

Vu l'ampleur des menaces sur les fleurons de l'économie ivoirienne, un pan de la mission de sensibilisation du CI-CERT est toujours orientée vers les chefs d'entreprise. Moins réceptives à l'idée d'investir dans le recrutement d'un responsable de la sécurité des systèmes d'information (RSSI), nombre d'entreprises empilent en effet des couches de sécurité (pare-feu, anti-virus, etc.), qui n'offrent souvent pas de protection suffisante.

Une situation que le chef de service déplore dans la parution de CIO Mag susmentionnée : « C'est lorsqu'elles (ces entreprises) doivent faire face à des incidents informatiques qu'elles se rendent compte de l'importance de la cybersécurité. Malheureusement, entre l'alerte et le temps mis pour rétablir le réseau, l'entreprise peut avoir déjà perdu plusieurs millions de FCFA. »

Partenariat public/privé

Côte d'Ivoire – Computer emergency response team.

Aujourd'hui, le CI-CERT peut se vanter d'avoir favorisé le recrutement de RSSI dans des entreprises de télécommunications. « On en retrouve également au sein des banques et de plusieurs groupes d'entreprises », révélait l'analyste-administrateur de sécurité des SI.

Pour limiter les incidents informatiques, le CERT ivoirien organise des ateliers et séminaires de formation, notamment avec les directeurs de système d'information (DSI) et les RSSI. Objectif ? Créer un partenariat public/privé destiné à poser des actions de prévention. C'est-à-dire, diffuser des bulletins d'information et des avertissements, et établir un réseau d'information et d'alerte gouvernementale sur les attaques et les menaces.

Au cours de ces rencontres, les responsables informatiques et de cybersécurité sont briffés sur les menaces répertoriées sur le cyber espace national mais également sur les types d'attaques rapportées au CI-CERT par ses partenaires internationaux : IMPACT (Organisation internationale de lutte contre les cyber-menaces) et la communauté des CERT étrangers.

La nécessité de se doter d'un CERT

En Côte d'Ivoire, la nécessité de se doter d'un CERT (Computer incident response team) a été perçue dès 2009. Dans un contexte où l'image du pays était fortement écorchée sur le plan international du fait des nombreux cas de défacement de sites web gouvernementaux et de cyberescroquerie.

Hormis les pertes financières provoquées par ces actes de piratage avérés, d'autres conséquences majeures ont été enregistrées : « Adresse IP ivoiriennes mises sur des listes noires ; achats en ligne interdits avec IP des FAI ivoiriens sur les plateformes telles que PayPal et Yahoo », peut-on lire dans un document dont CIO Mag a reçu copie.

C'est donc pour faire face à la récurrence de ces incidents qui constituent une menace, à la fois sur l'économie et la notoriété du pays que le CI-CERT a vu le jour, en 2009. Depuis leurs bureaux situés à l'époque dans la commune du Plateau, en plein centre des affaires, cinq ingénieurs informaticiens se sont activés à écrire les premières pages du CI-CERT.

Sous tutelle de **l'Autorité de régulation des télécommunications/TIC de Côte d'Ivoire (ARTCI)**, leurs actions consistaient à lutter contre la cyberescroquerie et à émettre des alertes et annonces de sécurité.

Plus de 40 000 incidents traités au 1er semestre 2015

Aujourd'hui, cette structure joue pleinement son rôle de cyber pompier de l'Etat avec une quinzaine d'ingénieurs menant une série d'activités regroupées en deux axes:

• Protection du cyber espace national avec un portefeuille de services réactifs (alertes et avertissements, traitement d'incidents, coordination de traitement de vulnérabilité, etc.) et proactifs (annonces, veille technologique, détection d'intrusion, partage d'informations), ainsi qu'un service de management de la qualité de la sécurité orienté sur la sensibilisation, la formation et la consultance.

• Lutte contre la cybercriminalité dans le cadre de la Plateforme de lutte contre la cybercriminalité (PLCC) grâce à une convention de partenariat entre l'ARTCI et la Police nationale.

Au cours du premier semestre de 2015, le CI-CERT a collecté et traité 40 264 incidents de sécurité informatique, envoyé 145 bulletins et avis de sécurité et participé aux cyberdrill UIT- IMPACT et OIC-CERT, traduisant son leadership sur le cyber espace national.

Article original de CIO-Mag

Réagissez à cet article

Original de l’article mis en page : Cyberattaque : quand le FBI débarque à Abidjan | CIO MAG