Exclusif

Comment l'université de Corse fait face à sa première cyberattaque

Paris - Publié le jeudi 27 juin 2019 à 9 h 49 - Actualité n° 150375

« Aucun élément ne nous permet de dire que la cyberattaque subie par l'université de Corse était ciblée. Le point d'entrée dans le SI ainsi que le cheminement de l'attaque font l'objet d'un audit de sécurité par un prestataire d'audit de la sécurité des systèmes d'information. L'enquête de gendarmerie est aussi en cours » déclare Dominique Federici, vice-président du conseil d'administration dans un entretien à News Tank le 26/06/2019.

L'Université de Corse Pasquale Paoli a été l'objet d'une cyberattaque par un rançongiciel de type Dharma le samedi 25/05/2019 à 6 h 10. Le propre de ce genre d'attaque est d'infiltrer un système d'information pour ensuite chiffrer les données présentes sur les machines, puis de demander une rançon afin de les déchiffrer. Dans le cas de l'université de Corse, aucun montant n'a été demandé. Selon une première estimation non définitive de la DSI, ce sont 40 machines, serveurs et clients, qui ont été touchées par ce virus. Des données de la recherche peuvent avoir été perdues.

« Nous savons que l'université a eu des pertes de données, mais nous ne sommes pas encore en mesure de tout quantifier. L'analyse des journaux des serveurs n'indique pas d'aspiration de données. Les machines concernées sont très différentes : certaines relèvent de l'administration, d'autres la recherche. Il n'y a pas un motif particulier d'attaque », dit Laurent Capocchi, responsable de la DSI de l'université.

Le motif aléatoire de l'attaque peut s'expliquer par la nature même du virus, qui va viser en priorité le sous-réseau infecté avant d'aller chercher à contaminer d'autres domaines du SI.

Une cellule de crise a été mise en place pour trois jours entre le 27/05/2019 et le 29/05/2019. Le travail de la DSI a permis une reprise de l'activité en mode dégradé à compter du 30/05/2019 pour un retour à la normale estimé le 07/06/2019. En parallèle, le prestataire a réalisé un audit sur tout le SI de l'établissement afin de comprendre les raisons de l'attaque et proposer des pistes d'amélioration.

Identifier le point d'entrée de l'attaque

Identifier l'origine de l'attaque, c'est l'objectif de l'audit de sécurité et de l'enquête de police en cours. Interrogés sur une attaque lancée en interne, les représentants de l'établissement ne privilégient pas cette piste :

> *« Nous n'avons pas été alertés par une intrusion physique avant ou au moment de l'attaque. Nous savons que l'université est un site ouvert, avec une large amplitude horaire. Pour autant, les informations dont nous disposons ne nous orientent pas vers une attaque interne », dit Laurent Capocchi.*

L'attaque par un agent extérieur implique de pouvoir rendre opérable le rançongiciel sur le système d'information de l'établissement. Pour cela, plusieurs scénarios vont être privilégiés.

Les types d'attaque *1/4*

Par du phishing ou du spear-phishing

- Dans le cas du phishing, la cible va faire l'objet d'une campagne massive de courriels contenant par exemple des pièces-jointes, ou des liens infectés vers un fichier exécutable.
- Un agent connecté au SI avec sa machine peut être victime. Ceci permet au virus de se déployer sur la machine.
- Le spear-phishing suit le même raisonnement que le phishing, mais il cible précisément les victimes potentielles.

Les types d'attaque *2/4*

Par l'installation d'un logiciel

Un logiciel qui semble dédié à une fonction peut abriter un virus.

De même, un logiciel dont l'authenticité n'est pas vérifiée peut contenir un virus qu'une personne autorisera à s'exécuter sur la machine lors de l'installation du programme.

Les types d'attaque *3/4*

Par l'utilisation d'un kit « exploit » de sécurité

En cas de défaut de mise à jour d'un SI, des attaquants peuvent utiliser un kit dédié à l'exploitation d'une faille de sécurité permettant de s'introduire dans le système. En s'introduisant, la possibilité d'exécuter un virus comme Dharma est facilitée.

Les types d'attaque *4/4*

Par une attaque par force brute

- Les attaquants vont se concentrer sur des points du SI dont la robustesse peut être défiée.
- Ce type d'attaque vise à combiner un très grand nombre d'identifiants et de mot de passe en vue de s'introduire sur le SI.
- L'attaque par force brute va s'appuyer sur la faiblesse des mots de passe ou sur la diffusion de ceux-ci précédemment dans des bases de données.

Les cyberattaques se sont développées et complexifiées

Fabian Rodes, expert en cybersécurité et membre de la réserve citoyenne de cyberdéfense en affectation gendarmerie, analyse le contexte de cette attaque :

Depuis trois ans, les cyberattaques se sont développées et complexifiées :

> *« On parle de ransonmwares as a service, pour désigner des offres complètes pour attaquer une cible. Pour 1000 €, une souche de virus qui est garantie indétectable par un antivirus est cédée à un attaquant. Par ailleurs, des adresses IP qui ont une capacité de compromission sont vendues avec leurs identifiants et mots de passe. Tout ceci permet de rentrer sur un réseau et de déposer une charge virale. »*

La question de l'intérêt de cette attaque doit être posée : « Le secteur de l'ESR n'est pas une priorité pour les cyberattaques, qui ciblent généralement des domaines plus en vue, comme l'industrie. Cette attaque peut servir à compromettre des données stratégiques, comme la recherche, ou alors l'établissement attaqué sert de cheval de Troie pour attaquer une plus large partie du réseau. »

La demande de rançon peut intervenir dans un second temps : « Même si le rançongiciel n'indique pas de rançon directement, la prise de contact peut se faire après, par un mail à la direction de l'établissement. Cela pourrait ainsi prouver que l'attaque est ciblée. »

Les sites distants de l'université font l'objet d'une attention particulière

Laurent Capocchi, DSI de l'université, indique que l'attaque sur un serveur de l'université en utilisant un port qui permet des connexions distantes à ces serveurs peut être privilégiée comme hypothèse principale. Ce type d'attaque est souvent plébiscité.

> *« L'attaque par force brute sur le port utilisant Remote desktop protocol est privilégiée comme hypothèse principale, entre 60 et 70 % de probabilité. L'infection a commencé par un sous-domaine du réseau avant de se diffuser.*
>
> *Le virus n'a pas chiffré massivement le parc machine de l'établissement, mais il s'est propagé davantage en rebond jusqu'à toucher le cœur du SI. ».*

Pour l'expert Fabian Rodes, cette piste est corroborée par des cas déjà traités :

> *« Même sur un système qui respecte globalement les protocoles de sécurité, une attaque par force brute sur ce protocole fonctionnera et restera indétectée par l'antivirus. Le protocole d'accès distant aux systèmes Microsoft, Remote Desktop Protocol, est un élément exposé et trop souvent sans protection ni contrôle d'accès.*
>
> *Il est commun de voir des attaques tenter 11 000 combinaisons d'identifiants par jour jusqu'à entrer dans le SI. C'est la première étape pour lancer un rançongiciel. »*

D'après le DSI de l'université de Corse, le travail de recherche sur les origines de l'attaque peut mener sur une piste liée aux sites distants de l'université. Ces sites ont des besoins spécifiques en informatique, notamment des serveurs physiques.

L'université de Corse comprend quatre sites, dont deux abritent des UMS :

- Le site distant de Cargèse, avec l'infrastructure de l'institut d'études scientifiques de Cargèse, commune avec le CNRS et l'Université de Nice Sophia Antipolis. D'après le site de l'université, « ce lieu accueille toute l'année des conférences internationales organisées par de grandes institutions comme la Nasa, le CEA, le Cern et des écoles thématiques à caractère scientifique. » Il s'agit de l'UMS 820.
- Le site distant de Bastia/Biguglia, qui accueille la plateforme de recherche Stella Mare, commune avec le CNRS. Il s'agit de l'UMS3514.
- Le site distant d'Ajaccio/Vignola, qui héberge les plateformes Myrte et Paglia Orba.
- Le site central de Corte.

Un bilan non définitif

L'attaque par rançongiciel a pour but de chiffrer des serveurs et des ordinateurs de l'université. Si le nombre de machines infectées est très faible comparé au parc de l'établissement, 40 sur 2 500, le centre de l'activité a été touché.

L'ensemble du SI est concerné par l'attaque. L'infrastructure est virtualisée sur 150 serveurs. La gestion administrative et financière et tous les services nécessaires au travail des agents ont été impactés, dont les courriels. La DSI annonce que et que certaines données de la recherche sur les sites distants ont pu faire l'objet de perte suite au chiffrement du rançongiciel.

Les données étaient hébergées soit dans les salles serveur locales du site de Corte, soit dans les serveurs physiques des sites distants.

Les mails des étudiants et l'ENT n'ont pas été impactés. Cela s'explique par le choix de la DSI de ne pas héberger localement ces données et de recourir à un prestataire externe.

Les dégâts font toujours l'objet d'une évaluation définitive, d'après le vice-président du conseil d'administration, Dominique Federici. Deux raisons sont évoquées :

• le chiffrement par *rançongiciel* contraint de restaurer un système par rapport à une sauvegarde précédente et il est nécessaire de s'assurer qu'il ne reste pas de fichiers vérolés susceptibles de pouvoir infecter à nouveau le système ;
• par ailleurs, l'évaluation dans les sites distants demande aux équipes des déplacements pour s'assurer de l'intégrité des systèmes.

Les enseignements de cette attaque

Après la gestion de la crise et un retour progressif des services à la normale, l'établissement tire des enseignements permettant d'améliorer la gestion de cet accident.

- Informer la Cnil : le SI contient des données à caractère personnel. À ce titre, l'attaque contrevient à la disponibilité, l'intégrité ou la confidentialité de ces données. De ce fait, une déclaration de violation de données personnelles doit être faite. Si la Cnil indique que la notification doit être faite « dans les meilleurs délais », son site indique la procédure. Il s'agit de procéder à une déclaration initiale dans les 72 h « si possible », suite à la constatation de violation. Si le délai est dépassé, le retard devra être expliqué lors de la notification. Une notification complémentaire sera faite lorsque les informations complémentaires seront disponibles. L'établissement n'a pas réalisé cette déclaration dans les 72 h.

- Ne pas payer la rançon : dans le cas de l'université de Corse aucun montant n'est indiqué. De plus, rien ne garantit de recouvrir les données chiffrées. Seule une restauration des données par des sauvegardes est une solution à considérer.

- Mettre en place une cellule de crise : le choix de l'établissement de mettre en place une cellule de crise pendant 3 jours à compter du lundi suivant l'attaque a permis d'organiser une remontée du cœur du SI et de travailler en concertation entre la gouvernance et la DSI.

- Faire appel à une compétence extérieure sur la sécurité des systèmes d'information : l'université de Corse étant associée au CNRS, elle a fait appel au fonctionnaire sécurité des systèmes d'information (FSSI) du CNRS après l'attaque. Il a participé à donner les premières orientations, donner les

bonnes conduites, transmis les règles d'usage. L'établissement a également fait appel à un Passi (prestataire d'audit de la sécurité des systèmes d'information) pour réaliser un audit global de sécurité. Plus généralement, un établissement peut faire appel à l'Agence nationale de la sécurité des systèmes d'information qui fait référence dans le domaine en France.

- Intégrer dans le plan de reprise d'activité une attaque par rançongiciel : le PRA (plan de reprise d'activité) indique l'ensemble des étapes à suivre lors d'un accident survenant sur le SI. Si le risque de cyberattaque était identifié, celui spécifiquement d'une attaque par rançongiciel ne l'était pas.

- Communiquer auprès de la communauté universitaire : l'activité de l'établissement ne s'arrête pas pendant la cyberattaque. L'enjeu de communication est donc essentiel pour le vice-président du conseil d'administration. Cette communication s'entend aussi sur la diffusion en interne de bonnes pratiques liées à l'hygiène numérique pour minimiser les biais liés aux attaques par manque de vigilance des agents.

- Communiquer auprès des médias : une cyberattaque génère de l'attention chez les médias, bien au-delà des médias locaux ou spécialisés. La gestion de la crise implique une communication de crise pour répondre à la presse et faire parvenir les premières informations.

« Cette attaque ne remet pas en cause notre stratégie d'hébergement de données »

L'établissement fait le choix d'héberger ses données dans des salles serveur. Son SI est réparti entre le site central de Corte qui accueille la majorité de l'infrastructure et des sites distants. Ce choix qui s'inscrit dans une décision de souveraineté pour l'université est-il remis en question suite à la cyberattaque ?

« Cette attaque ne remet pas en cause notre stratégie d'hébergement de données. Nous allons maintenir nos salles serveurs et durcir la sécurité générale de notre système d'information », dit Dominique Federici.

La souveraineté des établissements sur leurs données est un argument souvent mis en avant pour conserver les serveurs sur site.

Au niveau national, la Dgesip, par son conseiller stratégique Mehdi Gharsallah, rappelait les dimensions stratégiques d'un passage au cloud dans l'ESR français lors des Assises du CSIESR à Strasbourg le 16/05/2019. Parmi les enjeux principaux nommés, celui de la « mutualisation et de la rationalisation » qui permet d'améliorer la disponibilité et la sécurité des SI.

Université de Corse Pasquale Paoli

L’université de Corse Pasquale Paoli est la seule université présente sur le territoire insulaire de la Corse.

Université de Corse Pasquale Paoli
7 Avenue Jean Nicoli
20250 Corte - FRANCE

Fiche n° 1749, créée le 28/04/14 à 12:14 - MàJ le 08/09/16 à 15:46