Crédit photo : DR

DES SOLUTIONS DE CYBERSÉCURITÉ INNOVANTES
FOCUS SUR LE **CENTRE LÉON BÉRARD** À LYON

Sensibiliser pour améliorer sa cybermaturité. À Lyon, le Centre Léon Bérard s'est donné pour mission de sensibiliser ses utilisateurs tout en déployant des solutions de sécurité innovantes. Centre de recherche et de lutte contre le cancer, l'établissement a entamé sa transformation numérique dès le début des années 90. Focus sur un pionnier dans la transformation numérique.

DEVENIR CYBER RÉSILIENT

En commençant par les dossiers patients informatisés, puis en transformant totalement son système, le Centre Léon Bérard a su s'adapter aux changements imposés par le numérique. Pourtant, une ombre plane au-dessus du Centre, celle de la cyberattaque.

Face à cette menace, le Centre a mis en place des processus pour prévenir et pouvoir, en cas d'attaque, reprendre une activité au plus vite. Ces processus se sont organisés en 5 axes.

Dans un premier temps, sensibiliser les utilisateurs et les instances : « *Il faut que tout le monde soit sensibilisé dans son champ d'application, explique Franck Mestre, Responsable de la Sécurité des Systèmes d'Information au Centre Léon Bérard. Cela passe par des actions de communication, des campagnes de fishing, du e-learning, et même un escape game.* »

L'objectif est de faire rentrer l'utilisateur dans un cursus lui permettant d'avoir l'expérience suffisante afin de faire face à la menace. Le Centre Léon Bérard mise sur une « hygiène » de cybersécurité. « *Si l'utilisateur n'est pas un minimum sensibilisé, il ne va pas pouvoir comprendre les enjeux de l'escape game. Le but est de le sensibiliser progressivement pour que, demain, il soit plus apte à comprendre parce qu'il saura mieux appréhender les risques.* » ajoute Franck Mestre.

Le deuxième axe consiste à protéger les flux de messagerie. Les cyberattaques trouvent généralement leurs origines dans des mails qui incitent les utilisateurs à changer leur mot de passe. L'utilisateur clique sur le lien, ce qui permet aux cybercriminels d'infiltrer le réseau. « *Dans ce cas de figure, le but est de mettre en place des filtres sur les messageries pour limiter les utilisateurs à cliquer sur des liens malveillants.* » développe Franck Mestre.

Le troisième axe consiste à protéger le poste de travail. Une fois les composants pathogènes installés sur le poste de l'utilisateur, les cybercriminels peuvent se répandre sur le réseau. C'est ce qu'on appelle les déplacements latéraux, c'est-à-dire aller affecter tous les postes proches à partir d'un poste de travail. « *Aujourd'hui, il faut aller sur des mécanismes d'EDR. Ce sont des outils qui travaillent sur le comportement de l'utilisateur pour essayer de détecter ce qui n'est pas habituellement constaté sur le poste de travail, explique Franck Mestre. C'est tout un tas d'informations qui remontent. Derrière, il faut qu'il y ait des équipes capables d'analyser ces flux 7j/7 et 24h/24, pour faire de la détection et de la prévention.* » En augmentant la capacité à détecter, l'objectif du Centre est de basculer de l'EDR (Endpoint Detection Response) à l'XDR (Extended Detection and Response) afin d'augmenter son champ de vision et d'alerter rapidement en cas de suspicion d'attaques.

Le quatrième axe consiste à protéger l'Active Directory. « *L'Active Directory est un composant crucial dans les systèmes d'information. Il est comme le coffre contenant les clés d'accès au royaume.* » explique Franck Mestre. L'Active Directory gère et stocke les informations d'identifications, d'authentifications et d'autorisations liées aux utilisateurs et aux ressources du réseau. Un travail de mise en conformité, au regard des bonnes pratiques, est nécessaire afin de durcir son accès. Au-delà de cette sécurisation, la mise en place d'outils de supervision est primordiale. Cela permet d'informer en temps réel de toutes les modifications substantielles, par exemple l'élévation de droits sur des ressources, la modification des groupes administrateurs, etc.

Enfin, le dernier axe consiste à assurer l'intégrité des sauvegardes avant de les rendre immuables.

CENTRE DE LUTTE CONTRE LE CANCER LÉON BÉRARD

Franck Mestre
Responsable de la Sécurité des Systèmes d'Information au Centre Léon Bérard
Crédit photo : DR

« *Aujourd'hui, le concept du « 3-2-1 », 3 copies sur 2 supports différents et 1 externalisée ne sont plus suffisantes, car toutes les copies peuvent être corrompues, détaille Franck Mestre. Il est nécessaire de pouvoir mettre en place une solution déconnectée du réseau.* » Dans cette solution, seules des nouvelles données peuvent être ajoutées, les anciennes n'étant pas modifiables. Avant d'être ajoutées, les données doivent être analysées par un système capable de détecter d'éventuelles corruptions, par exemple à l'aide de mécanisme d'IA (Machine Learning, Deep Learning...). Tout cela doit permettre de restaurer rapidement un système d'information à partir de sauvegardes saines. En résumé, il faut pouvoir sanctuariser les données en s'assurant de leur immuabilité par une analyse en continu sur un système autonome.

LA COMMUNICATION COMME SOLUTION

Aujourd'hui, le Centre Léon Bérard a conscience du risque cyber. Tout le travail du RSSI en lien étroit avec la DSI consiste à reculer dans la liste d'attente du prochain attaqué. La première étape fut de trouver et de mettre en lumière les failles afin de définir les besoins. « *On ne va pas ajouter des outils supplémentaires, mais on va travailler en lien avec les équipes de la DSI, notamment les équipes infra sur des approches différentes pour arriver à un choix partagé.* » détaille Franck Mestre. L'objectif est de réorganiser et de repenser les processus afin de les adapter aux nouvelles menaces. La seconde étape est de définir l'outil qui répondra aux besoins de cybersécurité du site. Ce choix passe par des discussions entre les équipes infra, les administrateurs et le RSSI. Ainsi, chacun peut exprimer ses attentes afin de choisir l'outil le plus adapté.

« *Aujourd'hui, nous sommes en train de mettre en place une politique de Gestion des Risques et de Conformité (GRC), avec différents processus comme la gestion documentaire, un inventaire, une cartographie ou encore un outil propre à la GRC*, indique Franck Mestre. *On s'aperçoit qu'on a une connaissance collective du système d'informations, mais que l'on n'a pas de documentation centralisée, classée et accessible à tous.* »

Cibler la faille dans les usages pour devenir cyber résilient, c'est le choix stratégique du Centre Léon Bérard. Aujourd'hui, la communication est au centre de ses usages pour pouvoir définir des solutions adaptées à tous les acteurs du site afin de tendre vers une meilleure cybermaturité.

Romane Laferté