Renforcer la cyber résilience du secteur public : un enjeu crucial

Eléna POINCET
Co-fondatrice et CEO
TEHTRIS

Le secteur public est, comme le secteur privé, confronté de manière croissante aux cyberattaques, et ce d'autant plus avec la crise liée à la COVID-19 qui a impliqué un recours au télétravail et une digitalisation des services publics. Les administrations, les métropoles, les collectivités et les structures hospitalières, quelle que soit leur taille, sont particulièrement exposées à ces actes de cybercriminalité. L'obsolescence de leur parc informatique, la plus faible acculturation au numérique, l'utilisation croissante d'outils connectés engendrent un élargissement de la surface d'attaque qu'il est plus complexe à défendre… Autant d'enjeux à relever pour que le secteur public devienne cyber résilient.

Regardons de plus près les menaces et enjeux liés aux structures hospitalières, aux métropoles et collectivités locales.

Le secteur de la santé a été particulièrement touché depuis 2017 avec les attaques Wannacry et NotPetya. Le système de santé britannique a notamment été paralysé. En France, les hôpitaux de Dax, d'Oloron-Sainte-Marie, de Villefranche-sur-Saône, de Saint-Gaudens ou encore l'Assistance Publique - Hôpitaux de Paris (AP-HP) ont été touchés. Il est estimé qu'un établissement de santé est victime chaque semaine d'une cyberattaque. Quant aux métropoles et collectivités locales affectées par de telles attaques, la liste s'allonge si bien qu'il est plus difficile de la suivre…

Ces acteurs sont particulièrement vulnérables pour plusieurs raisons.

Les métropoles, collectivités et les structures hospitalières sont en pleine transformation digitale avec une numérisation rapide des parcours « citoyens » et « patients ». Le recours aux dispositifs médicaux connectés, à la télémédecine, à la télésurveillance médicale, ou encore aux chatbots est croissant…. Ces acteurs collectent et stockent une très grande quantité de données à caractère personnel. Ils disposent par ailleurs d'un parc informatique vaste et hétérogène au service des agents de la collectivité, des écoles et maternelles, des médiathèques, du public, des patients...

La chaîne logistique de ces écosystèmes devient dès lors plus complexe et engendre ainsi un élargissement de la surface d'attaque, rendant ces acteurs publics attractifs pour les cybercriminels.

La prise de conscience des risques cyber est aussi relativement limitée dans le secteur. Selon

Cybermalveillance[1], 65% des communes de moins de 3 500 habitants pensent que le risque est faible, voire inexistant, ou ne savent pas l'évaluer. Seules 35% identifient un risque numérique élevé, voire très élevé, mais s'interrogent sur les moyens pour y pallier (budgets, outils, ressources humaines). L'utilisation d'outils personnels dans ces petites structures est aussi répandue.

Les menaces sont quotidiennes, qu'ils s'agissent d'une clé USB infectée, d'e-mail de phishing, d'attaques DDOS, de rançongiciels ou encore de vol de données combiné à du doxing[2].

Les attaques par phishing sont très efficaces. Ces attaques par ingénierie sociale visent à perturber le fonctionnement des structures, à voler les données, à récupérer une rançon en dupant les utilisateurs (médecins, tiers de confiance) qui sont de plus en plus pressés. Les ransomware constituent la menace la plus fréquente. Ces attaques contre les hôpitaux ont augmenté de 123% en 2021 par rapport à l'année précédente. Le coût par attaque de ransomware est en moyenne de 8 millions USD. Les attaques par déni de service (DDOS), qui visent à couvrir généralement une seconde attaque, sont aussi redoutables.

Le vol de données est répandu. Les données constituent notre patrimoine et valent de « l'or » pour les cybercriminels. Les métropoles, collectivités locales et hôpitaux regorgent d'informations sensibles : données personnelles (noms, dates de naissance, numéros de sécurité sociale, adresses, numéros de téléphone), documents de recherche, informations sur la propriété intellectuelle… L'espionnage est une réalité et ces données récupérées alimentent le marché du darkweb. Un dossier médical peut valoir par exemple jusqu'à 350 USD sur le marché noir, soit 50 fois plus qu'un dossier bancaire[3].

Les conséquences de telles attaques sont de plusieurs ordres.

Financières d'abord. Ces actes nécessitent la remise en service des systèmes informatiques et la récupération des données, avec potentiellement le paiement d'une rançon. Le secteur public est néanmoins moins disposé à la payer que les entreprises qui disposent de plus de moyens. Les coûts sont aussi liés à l'inactivité du personnel qui ne peut poursuivre son travail.

Humaines ensuite. D'une part, les cyberattaques affectent directement les citoyens qui se retrouvent privés de services et qui sont susceptibles de voir leurs données utilisées à mauvais escient (divulgation, suppression). Cela porte atteinte à la vie privée des individus. Le lien de confiance entre le citoyen et l'entité publique, dont l'image est dégradée, s'en trouve rompu. D'autre part, dans le secteur de la santé, les attaques peuvent impliquer en quelques secondes une paralysie du système d'un hôpital : SI, système de communication, scanners, IRM, pompes à perfusion. La vie des patients est dès lors en jeu. Imaginez que demain un robot de chirurgie soit contrôlé par un cybercriminel…

La question est désormais de savoir « quand » ces acteurs seront la cible d'une attaque, et non plus « si ».

Le système d'information est au cœur du bon fonctionnement des opérations et doit être constamment en état de marche. Certes, on parle de

1 Etude: la sécurité numérique dans les collectivités françaises de moins de 3 500 habitants (mai 2022)
2 Divulgation de données personnelles
3 Proofpoint, paysage des menaces dans le secteur de la santé (2020)

sensibilisation et la dimension cyber doit être intégrée à la culture de ces structures. Mais la problématique de la cybersécurité ne peut pas porter uniquement sur l'utilisateur. Nous sommes actuellement dans une jungle numérique, constituée de matériels et de logiciels provenant la plupart du temps de l'étranger. Les systèmes d'informations et d'exploitations pour ordinateurs ou serveurs (Windows, iOS ou encore Linux) présentent des failles ouvrant la voie à des cyberattaques.
Parallèlement, la surface d'attaque s'élargit, comme mentionné précédemment. Or, la chaîne des acteurs que composent ces écosystèmes complexes doit être sécurisée de bout en bout.

Dans ce contexte, les solutions qui reposent sur l'hyperautomatisation sont clés pour se protéger de ces cyberattaques fulgurantes.

Les métropoles, collectivités et hôpitaux souhaitent de plus en plus faire évoluer et moderniser leur dispositif de cybersécurité afin d'y apporter une couche de sécurité supplémentaire. Pour se protéger de ces cyberattaques et des conséquences engendrées, ils recherchent des solutions performantes, souples, faciles à opérer et compatibles avec un antivirus existant. La préservation de la souveraineté et de l'intégrité des données (aussi bien des collaborateurs, des citoyens que des patients) est par ailleurs une préoccupation croissante. Enfin, lutter contre des attaques de plus en plus nombreuses et évoluées avec des équipes limitées est un enjeu clé pour ces acteurs. Rappelons qu'il est particulièrement difficile de recruter du personnel qualifié en sécurité informatique.
Il a été démontré qu'une attaque pouvait ne durer que 37 minutes, entre l'intrusion, l'exfiltration des données et le déploiement du ransomware sur un parc numérique. Face à ces menaces, les équipes responsables des systèmes d'information ne peuvent pas s'en sortir en recourant seulement à de la détection pour certains et à de la neutralisation gérée par l'humain pour d'autres. Aujourd'hui, les outils traditionnels, les anti-virus, ne suffisent plus pour se protéger. Adopter une technologie pensée et conçue pour simplifier, centraliser et orchestrer permet aux analystes de se concentrer sur des tâches à haute valeur ajoutée.

Pour assurer la protection en temps réel de son parc informatique, la proactivité et la réactivité sont désormais cruciales. Il est alors important d'intégrer une solution hyper automatisée qui permet d'effectuer la détection, l'analyse, la mise en quarantaine et la remédiation en temps réel. Grâce au machine learning et au deep learning, les aspects subtils des menaces qui seraient invisibles à l'œil nu sont détectés. Ces techniques permettent de mieux connaître les comportements des cybercriminels et de prévenir les attaques.

En 2022, le secteur public doit pouvoir se défendre et être protégé du cyber espionnage et du cyber sabotage. Recourir à une solution de sécurité efficace, hyper automatisée permettant une visibilité à 360° et une couverture globale est primordiale. Pour une protection optimale des données, il convient enfin de s'assurer que les solutions de cybersécurité utilisées soient « secure and ethics by design ». Il est effectivement crucial que les logiciels soient conçus, produits, configurés en tenant compte, dès la conception et par défaut, de la vie privée et de la sécurité du contenu des fichiers protégés.

C'est en prenant en compte ces enjeux et en recourant à des technologies performantes et souveraines, de détection et de neutralisation en temps réel et sans action humaine, que le secteur public sera en mesure de renforcer sa résilience.