# Cybersécurité : les perspectives pour le secteur public en 2021

***Christophe AUBERGER***
*Evangéliste Cybersécurité*
*Fortinet France*

**Le secteur public est aujourd'hui, comme le secteur privé, de plus en plus confronté aux risques numériques, et ce d'autant plus après la crise liée à la COVID-19.**

Le recours forcé au télétravail dès mars 2020 a en effet bouleversé la façon dont les services administratifs sont fournis. Auparavant, les fonctionnaires assuraient la prestation de services aux citoyens en personne. En 2021, ils sont encore nombreux à travailler à distance et à fournir une assistance numérique aux citoyens. Par ailleurs, l'utilisation d'outils tels que les chatbots, les agents intelligents et le RPA (Robotic Process Automation, à savoir l'automatisation de processus métier basée sur des règles) est de plus en plus courante. Cela élargit considérablement la surface d'attaque. De plus, le domicile des télétravailleurs ne dispose pas du même niveau de sécurité que les environnements professionnels.
Par conséquent, les cybercriminels et auteurs de menaces persistantes avancées ou APT ont rapidement perçu les failles potentielles du télétravail. Pour exemple, le volume de données compromises dans le secteur public aux États-Unis a pratiquement doublé l'an dernier. Les administrations gèrent un tel volume de données personnelles et sensibles que la vigilance est plus que jamais un impératif.

## Les défis à relever par les RSSI en 2021 pour sécuriser les administrations publiques

Le secteur public est tout sauf homogène, allant de grandes administrations nationales avec des centaines de milliers de fonctionnaires aux petites municipalités qui n'emploient qu'une poignée de personnes. Que ce soit à l'échelle nationale ou locale, le défi reste le même : en faire davantage avec moins, les ressources ayant fortement diminué dans le contexte pandémique actuel. Dans le même temps, la demande de services, souvent numériques, s'est accélérée.

Par ailleurs, la pérennité annoncée du télétravail signifie que cela continuera de faire partie du paysage des menaces pour les administrations. La sérendipité a joué un rôle dans la mise en œuvre de la sécurité du télétravail pour de nombreuses administrations. Pour celles-ci, le succès de cette sécurisation relevait souvent du hasard, de là où elles en étaient dans leur mise à niveau et leurs choix technologiques. Cependant, l'idée qu'il vaut mieux être chanceux à défaut d'être bon ne peut certainement pas remplacer une stratégie intelligente.

Le RPA et l'automatisation intelligente viennent s'ajouter à cette périphérie élargie de réseau, entraînant un nombre croissant de connexions à des bases de données internes et hétérogènes.

La sécurisation de ces nouvelles connexions, souvent vulnérables, est vitale et doit être prioritaire

2021 sera donc l'année de l'hybride pour le secteur public, c'est-à-dire des activités mixtes et hybrides des administrations… mais aussi des cybercriminels. Le travail à distance est appelé à perdurer. Les modèles de travail changent à mesure que la robotisation et l'automatisation intelligente se développent. De la même manière, les acteurs malveillants déploient des attaques utilisant plusieurs techniques, par exemple en panachant DDoS (attaque par déni de service) et phishing. Elles peuvent avoir des conséquences multiples, comme dans le cas d'un ransomware (ou rançongiciel) combiné à du doxing (divulgation de données personnelles). Les attaques mixtes de type best of breed (attaque associant plusieurs techniques éprouvées) ou Digital Frankenstein (association d'informations réelles et falsifiées pour créer une nouvelle identité) peuvent prendre la forme de logiciels malveillants élaborés en associant des composants très performants de malware déjà existants.

## Intelligence artificielle, SD-WAN et sécurisation des Edge au programme

Bien que l'intelligence artificielle (IA) et le machine learning (ML) soient, dans l'ensemble, plus utiles aux RSSI qu'aux assaillants, ces derniers ont potentiellement un avantage sur des niches telles que la génération de contenu pour le spear phishing (attaque ciblée et message personnalisé). En effet, des approches hybrides exploitant l'IA peuvent analyser un nombre suffisant d'emails pour tenter d'imiter leur syntaxe et leur style. Le RSSI dispose de suffisamment de données pour définir ce qu'est un comportement normal et repérer les anomalies grâce à l'IA et au ML. Les intrus tentent et échouent à plusieurs reprises avant de réussir à infiltrer leur cible. L'identification de ces échecs permet aux professionnels de la sécurité de repérer une attaque en cours, pour ensuite protéger le patient zéro ainsi que tous les autres collaborateurs.

Pour les administrations publiques, il est essentiel d'aller de l'avant en investissant efficacement, et en évoluant vers le SD-WAN. Le SD-WAN sécurisé est un levier d'économies et de productivité pour les équipes IT et de sécurité. Il améliore également l'expérience utilisateur, renforce la sécurité, la productivité et la résilience. Cet aspect est essentiel si l'on considère que la pandémie de COVID-19 a démontré la nécessité de maintenir les services publics, même lorsque les fonctionnaires et les citoyens sont confinés.

Enfin, l'informatique et les technologies industrielles (Operational Technonology) convergent dans la droite ligne d'une recherche d'économies et de productivité. Ceci est illustré notamment par l'automatisation des bâtiments intelligents et les connexions entre les objets connectés IoT et les dispositifs stratégiques, ainsi que les services externes. Pour cette raison, la sécurisation de l'edge OT est également devenue plus critique.

Au-delà de l'investissement technologique et de la nécessité de recruter du personnel qualifié en sécurité, l'enjeu de la cybersécurité réside également dans la question de l'évolution de la culture des administrations pour intégrer cette nouvelle dimension, transverse par nature.