De par sa mobilité et sa visibilité, le TRM est plus vulnérable que n'importe quel secteur. La confiance numérique devient alors un vrai défi stratégique pour les organisations. Les transporteurs en ont-ils conscience ? Comment prévenir les attaques qui sont plus sophistiquées et mieux ciblées ? On vous dit tout.

À NE PAS PRENDRE À LA LÉGÈRE !

Véronique Vigne-Lepage


Sadio Ba, coordinateur sectoriel transports de l'ANSSI, conseille de faire appel à des prestataires qualifiés pour sécuriser son SI. Le site de l'agence en liste quelques-uns.

Patrick Gaillardin - Hanslucas

Six entreprises sur 10 n'ont pas alloué de budget spécifique pour lutter contre la fraude et la menace cyber.
Source : Étude Euler Hermes-DFCG 2019

DOSSIER RÉALISÉ PAR FLORENCE FALVY

La digitalisation étant de plus en plus présente dans les entreprises, il est plus que probable de voir les attaques informatiques se répéter. D'ailleurs, la moitié des organisations tricolores s'attendent à une montée des cybermenaces en 2020 (enquête mondiale FireEye). « *Les pirates sont de plus en plus structurés et les attaques sophistiquées à l'image des menaces persistantes avancées ou APT. Il suffit de cliquer sur un lien ou de plugger une clé USB pour déployer un logiciel espion extrêmement silencieux et indétectable qui 1, 2 ou 5 ans plus tard va transférer de la donnée vers l'extérieur de manière très discrète* », introduit Benoit Bougnoux, associé du cabinet parisien Arengi spécialisé dans la gestion des risques.

Il est donc essentiel de ne pas sous-estimer ce risque. Les attaques ayant ciblé de grandes entreprises connues sont largement médiatisées. Sadio Ba, coordinateur sectoriel transports de l'ANSSI - l'agence nationale de la sécurité des systèmes d'information traite une vingtaine de grosses affaires par an- cite l'exemple de Saint-Gobain victime d'une attaque en 2017 et ses 250 millions d'euros de pertes de chiffre d'affaires. Mais il ne faut pas oublier que « *tout le monde est clairement concerné* », prolonge-t-il. « *Des TPE/PME ont dû mettre la clé sous la porte à cause d'attaques informatiques* ». Effectivement, les conséquences peuvent être dramatiques. Perte de données, divulgation d'informations confidentielles, perte de compétitivité et de confiance sur les marchés, perte d'exploitation suite à l'interruption du réseau et/ou paralysie du système d'information... Pourtant, selon une récente enquête Ifop, 55 % des dirigeants d'ETI sous-estiment encore le cyber-risque qualifié comme important mais « non prioritaire ». « *La prise de conscience est là mais elle n'est pas suffisante* », confirme Sadio Ba. Et d'ajouter : « On ne s'improvise pas expert en informatique. D'où la nécessité de s'appuyer sur les prestataires pour sécuriser son système. » Le site internet de l'ANSSI et la plateforme www.cybermalveillance.gouv.fr référencent notamment des professionnels qualifiés.


« *L'informatique, c'est l'organe moteur de l'entreprise de transport* », souligne Alain Malgogne au sein des transports éponymes (44).

Florence Falvy

LE TRM : UNE CIBLE

Géolocalisation des véhicules, mise en place d'un EDI (échange de données informatisées), numérisation des documents, bourse de fret sur internet... Le transport où gravitent des acteurs de plus en plus connectés est lui aussi vulnérable à des intrusions. « Les transporteurs ont pignon sur rue. Ils sont donc peut-*être plus impactés. Et plus on est informatisé, plus le risque est certain* », remarque Alexis Saupin, agent associé du cabinet d'assurances MMA Liaigre-Lesage-Saupin (85) qui diffuse notamment un livre blanc sur la prévention et la gestion des cyber-risques. Alors que la montée en puissance de la digitalisation impacte aussi la supply chain. « *Avec la multiplication des capteurs et des puces pour le suivi des conteneurs et le traçage des marchandises, la surface d'attaque augmente de manière exponentielle* », complète Benoit Bougnoux.

Nombreux sont d'ailleurs les exemples qui illustrent la vulnérabilité du TRM. Certaines sociétés en ont fait les frais, comme les Transports Rabouin (Loire-Atlantique) victimes en 2019 d'une escroquerie aux faux ordres de virement pour un montant de 156 000 euros. Le directeur Eric Rabouin n'a pas souhaité répondre à nos questions mais précise que les mesures déjà en place ont été renforcées depuis l'incident. Les Transports Grimaud ont eux aussi été ciblés. Voilà 4 ans, ses ordinateurs ont été infectés par le virus Locky qui a crypté certains fichiers. « *Les cybercriminels nous ont demandé une rançon de 5 000 à 6 000 euros, en échange d'une clé de déchiffrement. Heureusement, notre prestataire informatique était justement présent lorsque c'est arrivé. Et grâce aux sauvegardes, les fichiers stockés sur le serveur ont été récupérés* », témoigne Nicolas Grimaud. L'entrée en application du RGPD a eu le mérite de remettre la question de la protection des données au centre de la stratégie des Transports Malgogne. « *L'informatique, c'est l'organe moteur de l'entreprise. Du coup, si du jour au lendemain, on n'a plus accès à notre système informatique, on risque d'être paralysé. Nous sommes donc très sensibilisés sur ce sujet d'autant que nous avons été victimes d'un hacker en mai 2019. Un salarié avait ouvert un mail, à première vue anodin. Seulement, il avait mis le loup dans la bergerie. Le virus s'est propagé et le système informatique a été bloqué. Il a fallu 6 heures pour relancer nos trois serveurs externes et nous n'avons pu retrouver une activité normale que le lendemain matin. Par chance, nous n'avons pas perdu d'informations grâce à un système qui copie toutes les 24 heures l'essentiel des activités* », raconte de son côté Alain Malgogne.

Preuve que le sujet est également pris au sérieux chez Mousset, Anais Babin, directeur des systèmes d'information, fait état d'une augmentation significative de l'enveloppe allouée à la sécurité informatique, sans précision sur le budget. Dès son arrivée dans l'entreprise début 2019, ce dernier a fait appel au cabinet CGI (entreprise de services-conseils en technologie de l'information) pour réaliser une cartographie des risques. Objectifs ? Identifier et évaluer la maturité du système informatique pour ensuite définir les chantiers à prioriser pour 2020 : sécu- ...

L'Officiel des transporteurs – N° 3009 du 21 février 2020