Question écrite du 26/11/2020

de FREDERIC André

à DE BUE Valérie, Ministre de la Fonction publique, de l'Informatique, de la Simplification administrative, en charge des allocations familiales, du Tourisme, du Patrimoine et de la Sécurité routière

La crise sanitaire liée à la Covid-19 a malheureusement renforcé les tentatives d'attaques informatiques. Il arrive quotidiennement que des personnes télétravaillant reçoivent des mails suspects leur demandant de l'argent, leur numéro de compte bancaire ou même de participer à des réunions par visioconférence. Ces cas de figure représentent de véritables dangers pour ces personnes, car le simple fait de cliquer sur un lien peut entraîner une fuite de données.

Un des problèmes également épinglés est la non-information du travailleur qui pense qu'avec les systèmes de protection informatiques tels que les antivirus, il est inatteignable et à l'abri de tous problèmes. Or, il apparaît clairement que le travailleur, même protégé, lorsqu'il travaille de manière isolée, est beaucoup plus sensible aux attaques informatiques.

Est-ce que les agents de l'administration ont été informés de la présence de ces dangers et du fait qu'en travaillant à distance, ils pourraient faire davantage l'objet de tentative de piratage ?

Est-ce que ces agents ont reçu des instructions particulières afin qu'ils ne tombent pas dans ces pièges ?

Un protocole a-t-il été établi pour les personnes ayant divulgué des informations ou ayant cliqué sur des liens suspects ?

Réponse du 15/12/2020

de DE BUE Valérie

La situation actuelle liée à la Covid-19 oblige la plupart des entreprises et des organisations, y compris les administrations bien entendu, à privilégier le télétravail. Au niveau de la sécurité informatique, ce mode de travail distant crée, comme l'honorable membre le souligne, une exposition plus importante aux risques d'attaques et d'usurpations d'identité.

La procédure habituelle permettant l'accès au télétravail au sein du Service public de Wallonie prévoit le suivi d'une session de formation au cours de laquelle les modalités de connexion, mais aussi les règles de base de la sécurité informatique sont rappelées. De plus, les agents doivent adhérer à une charte des utilisateurs cadrant une bonne utilisation des ressources informatiques du SPW.

Compte tenu de la généralisation du télétravail et de sa probable pérennisation, cette formation a été adaptée dans son contenu pour y accentuer les aspects sécurité. Les agents sont donc bien informés des risques les plus courants et des mesures préconisées pour y faire face et traiter les incidents de sécurité.

Le département informatique du SPW suit en permanence l'actualité en termes de sécurité via des sources belges, européennes ou mondiales et détermine régulièrement si des vagues d'attaques informatiques en cours peuvent atteindre le SPW. Tout aussi régulièrement des mesures techniques sont déployées pour contrer celles-ci.

De plus, s'il s'avère qu'il y a un risque que des agents soient directement touchés par ces attaques, la sécurité du DTIC prend des initiatives pour alerter/prévenir les agents via le canal de communication l'Com. Ainsi, durant ces derniers mois, les communications suivantes ont été effectuées auprès de tous les agents du SPW :

- l'Com du 17/01/2020 : L'hameçonnage via des pièces jointes ;
- l'Com du 10/03/2020 : L'utilisation de l'adresse e-mail SPW ;
- l'Com du 12/03/2020 : L'hameçonnage en lien avec la Covid-19/coronavirus ;
- l'Com du 21/04/2020 : L'hameçonnage en lien avec la Covid-19/coronavirus ;
- l'Com du 18/08/2020 : Vague d'attaques par SMS en Belgique ;
- l'Com du 24/10/2020 : La connexion VPN.

Les agents de l'administration reçoivent des instructions de prévention en termes de sécurité informatique via les canaux de communication destinés au personnel (i.e. les l'Com), mais aussi au travers de l'organisation IT du SPW et de ses relais de proximité auprès des agents (ce que l'on appelle les Correspondants Informatique Locaux).

Le département informatique a également mis en œuvre une série d'outils de détection et de protection en vue d'éviter les attaques ou tout au moins de limiter leurs impacts :

- antimalware sur les serveurs et sur les postes de travail ;
- anti-spam et anti-Phishing ;
- blocage des sites dangereux et des sites trop « récents » (attaques « zero day ») ;
- détection et protection (IDS/IPS) contre des trafics réseaux malicieux ;
- VPN protégeant l'accès aux ressources intranet du SPW ;
- solution d'évaluation prédictive des risques par rapport aux attaques ;
- détection et réponse aux menaces avancées sur les postes de travail et les serveurs ;
- systèmes de réputation en matière de menaces transmises par des sources externes ;
- solution de protection contre l'usurpation d'identité en cas d'authentification frauduleuse ou supposée telle sur le tenant Microsoft Office 365 qui héberge principalement les outils bureautiques ;
- renforcement de l'authentification en cas d'accès hors de la Belgique via une authentification « multi facteurs » (par exemple, au travers de l'envoi d'un code d'accès via SMS).

En termes de protocole ou de procédure, un incident de sécurité est censé être déclaré par tout utilisateur exactement de la même manière que tout autre incident informatique « classique ». Toutefois, dès lors que l'incident est catégorisé comme « de sécurité », des procédures et des intervenants techniques particuliers et clairement identifiés sont susceptibles d'intervenir afin de répondre le plus rapidement possible et de la manière la plus proportionnée possible à toute tentative d'attaque. L'intervention va le cas échéant jusqu'à la désinfection ou la restauration de systèmes qui auraient été corrompus.