InfoSecNews ISCeco

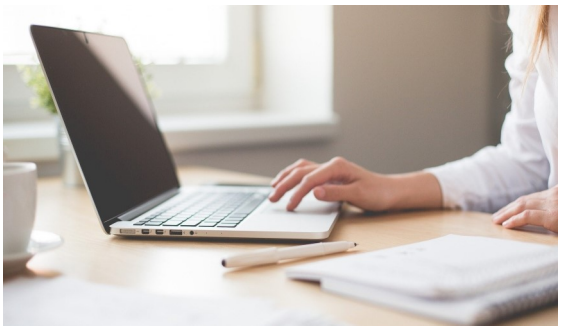
La Newsletter Sécurité de l'Information de l'ISCeco DFER

Thème : Home Office durant le Covid-19

Edition mars 2020

Face à la propagation rapide du coronavirus et à la menace qu'il représente, l'ISCeco, comme de nombreuses entreprises, a envoyé ses collaborateurs travailler à domicile et les étudiants se tournent vers les cours en ligne. La distance sociale s'accompagne d'une nouvelle menace - une menace cybernétique.

Alors que les établissements d'enseignement et les entreprises poussent à la numérisation des services, les cybercriminels intensifient leurs activités pour exploiter spécifiquement ceux qui ne sont pas conscients des dangers de l'internet ou qui ne savent pas encore comment utiliser les ressources informatiques en toute sécurité.



Travailler à domicile ou utiliser des cours en ligne n'est pas fondamentalement nouveau. Toutefois, la délocalisation massive des travailleurs des environnements informatiques des entreprises, qui sont gérés et surveillés par des professionnels, vers des réseaux privés Wi-Fi domestiques non supervisés et souvent peu sûrs, dans le sillage de la crise Covid-19, ouvre une nouvelle cible extrêmement attrayante pour les cybercriminels.

Les approches criminelles ciblant les étudiants à distance et les télétravailleurs sont basées sur les craintes et les inquiétudes concernant ce qui les a renvoyés chez eux - le Covid-19 lui-même.

Il y a de bonnes raisons de se préoccuper : les cybercriminels ont déjà lancé de nombreuses attaques thématiques liées au Coronavirus, pendant que la préoccupation autour de la pandémie mondiale se poursuit. Celles-ci comprennent diverses attaques de logiciels malveillants impliquant des Emotet (chevaux de Troie bancaires) et d'autres logiciels malveillants. Par exemple, on a récemment découvert un APT (Advanced Persistent Threat) qui, dans le cadre d'une vague de spam COVID-19, diffuse à distance des virus individualisés (personnalisés pour l'utilisateur) et uniques, qui sont en mesure de prendre des captures d'écran, télécharger des fichiers et plus encore.

L'Organisation Mondiale de la Santé (OMS) ainsi que l'OFSP ont émis des mises en garde contre les fraudeurs qui se font passer pour ces organisations dans des courriels. Les appels provenant de faux services d'assistance, qui se font passer pour des services d'assistance Microsoft, par exemple, et qui demandent aux utilisateurs d'installer des logiciels (malveillants) sur leurs appareils, sont également fréquents. On s'attend à ce que ces activités augmentent avec l'élargissement de la surface d'attaque (travail à domicile).

En général, les cybercriminels recherchent des vulnérabilités spécifiques afin de mener des attaques. Actuellement, la peur des gens face au virus est le point faible que les attaquants peuvent exploiter. Si une personne est inquiète ou stressée à cause du virus, elle se souviendra moins de la formation à la sécurité et se montrera plus téméraire en cliquant sur un lien dans un courriel de phishing ou en saisissant ses identifiants de connexion sur un faux site web.

Le domaine des mobiles est un vecteur d'attaque qui présente un potentiel de menace élevé. Les étudiants et les télétravailleurs sont très dépendants de leurs appareils mobiles. Les attaques de mobiles via des plateformes de communication telles que SMS, iMessage, WhatsApp et autres sont particulièrement efficaces car elles déclenchent souvent des réactions immédiates et irréfléchies de la part des destinataires.

Et de ne pas oublier : L'infrastructure informatique de l'entreprise (ordinateur portable, téléphone mobile, tablette, courrier électronique, ...) est destinée exclusivement à un usage professionnel et ne doit pas être mise à la disposition de toute la famille dans l'intérêt de la protection des données et de la sécurité de l'information. Merci pour votre engagement !