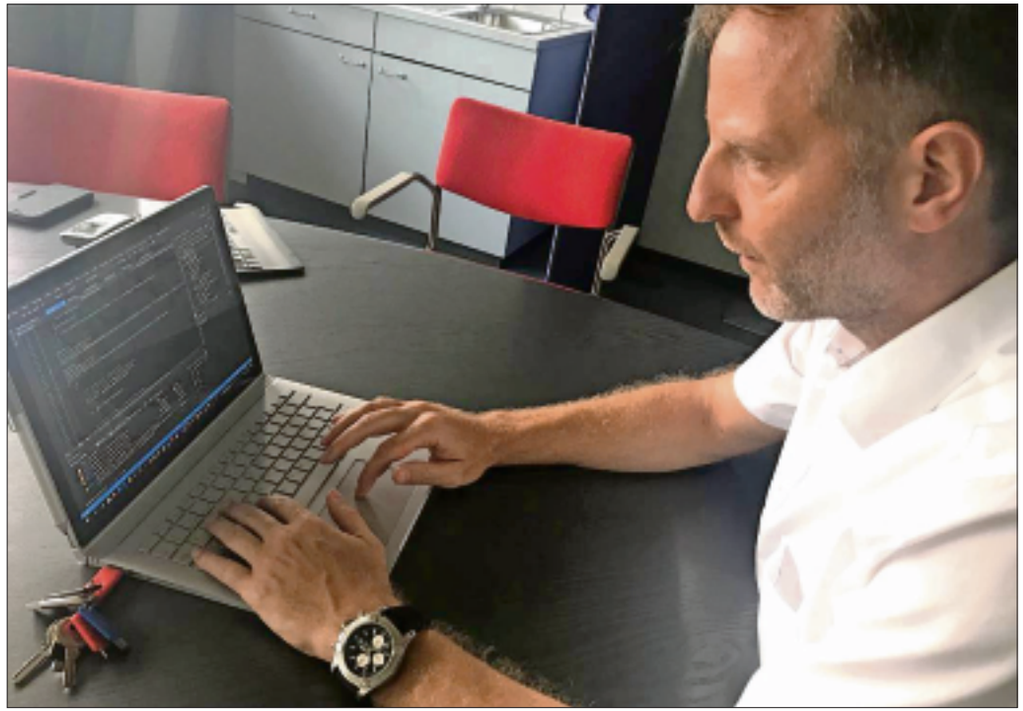
Le Quotidien Jurassien, 06 septembre 2019

On n'a pas assez conscience des dangers

La sécurité numérique dans les entreprises: tel était le thème de l'événement organisé hier à Delémont par BaselArea.swiss.

On doit plutôt parler de lacunes dans les entreprises qui ne sont pas assez conscientes des dangers, à entendre les spécialistes.

La première entreprise à s'installer dans l'antenne jurassienne de Basel-Area.swiss est une spécialiste de la sécurité numérique. Interview avec Philippe Kapfer, CEO de NextDay.Vision, et Sébastien Jaquier, de l'Institut de lutte contre la criminalité économique de Neuchâtel.



Une simple clé ressemblant à une clé USB permet à Philippe Kapfer de sécuriser son ordinateur. PHOTO GM

Le 25 octobre sera inaugurée l'antenne jurassienne du Switzerland Innovation Park Basel Area. Ce doit être un pilier de l'innovation dans les entreprises jurassiennes, dédié en particulier aux technologies médicales. Et pourtant, la première entreprise à s'y installer sera une spécialiste de la sécurité numérique. Preuve de l'importance de la sécurité numérique dans le monde d'aujourd'hui, et spécialement dans les entreprises innovantes. Philippe Kapfer, patron de NextDay.Vision, en a fait la démonstration hier soir lors de l'événement organisé par BaselArea.swiss. Pénétrer l'informatique d'une entreprise insuffisamment protégée se fait avec une facilité déconcertante. La visite d'un site internet infecté peut aboutir en quelques secondes au vol de données extrêmement sensibles, notamment les mots de passe donnant accès à la substance d'une entreprise.

Philippe Kapfer. – Les entreprises ne se protègent pas assez. Elles n'ont pas conscience du risque et pas l'état d'esprit de se protéger. Souvent, les entreprises ne se préoccupent que de l'informatique fonctionnelle, imprimer, ouvrir son logiciel, pouvoir travailler de la maison, mais on ne se préoccupe que peu de la sécurité.

***Le Quotidien Jurassien.* – Quels sont les risques?**

– Le cryptovirus, qui chiffre des données de manière irréversible, le risque de vols ou de modification de données, la manipulation comme l'arnaque au président: l'idée est qu'on manipule le comptable ou quelqu'un de la société en se faisant passer pour le président pour faire effectuer un paiement sur un nouveau compte. Des sociétés ont perdu de grosses sommes de cette manière. C'est relativement simple d'accéder à ces données si l'entreprise n'est pas suffisamment sécurisée.

– Et le risque dans la région?

– La conscience des dangers manque, de même que les compétences dans ce domaine.

– Que propose votre société?

– Des audits et une application pour remplacer le mot de passe. En termes de sécurité, le mot de passe est un point faible. Il est de plus en plus complexe et difficile à mémoriser. On le note, on utilise souvent le même, et il peut être volé à distance, ce qui ne le rend pas sûr. Nous proposons des solutions innovantes pour remplacer ce mot de passe dans l'environnement de l'entreprise: l'identification du visage de la personne, une clé de sécurité sur son ordinateur, bien plus rapide que le mot de passe, ou le recours à une application sur smartphone pour ouvrir une session. Cela simplifie la vie de l'utilisateur et décomplexifie la sécurité tout en l'améliorant.

GEORGES MAILLARD

Quand la webcam est piratée...

Pour les escrocs de l'informatique, «c'est beaucoup plus simple maintenant d'atteindre une population importante car tout le monde est connecté», constate Sébastien Jaquier, responsable adjoint de l'Institut de lutte contre la criminalité économique de Neuchâtel. On dit que les criminels ont toujours un temps d'avance, est-ce vrai dans le domaine numérique? Sébastien Jaquier: «Ils anticipent les outils à notre disposition. Par exemple la webcam: les entreprises qui ont inventé cela n'ont pas anticipé que d'autres acteurs pourraient se demander ce qu'on pourrait en faire. Ils ont trouvé des moyens de se connecter dessus et d'espionner.» Même topo avec les robots aspirateurs. «Les criminels imaginent des utilisations pour les biens auxquels les fournisseurs et utilisateurs n'ont pas pensé au départ, car la sécurité ne fait pas partie du cahier des charges de ces produits. C'est un des problèmes que le politique et les entreprises ont commencé à empoigner.»

«On peut se protéger, mais on ne peut pas ériger une muraille infranchissable. L'époque des châteaux forts est terminée, poursuit Sébastien Jaquier. On peut se protéger avec une infrastructure informatique à jour, avec les outils antivirus, mais ces outils ne reconnaissent que les virus déjà connus. Cela ne suffit pas. Les processus de travail doivent intégrer la sécurité numérique. Enfin il y a le facteur humain, le plus important. Je suis fondamentalement opposé à l'idée de dire que le facteur humain est le maillon faible. Il l'est si on lui donne ce rôle. Mais si on le conscientise, il devient un acteur de la sécurité numérique.»

Les entreprises piratées se taisent. Un problème, c'est qu'un certain nombre d'entreprises sont touchées sans le savoir. Des informations, de la propriété intellectuelle volée, ce n'est pas sûr qu'on s'en rende compte tout de suite. Or les cyberattaques ont de plus en plus d'effets sur les entreprises. Sébastien Jaquier est persuadé que des banques sont attaquées tous les jours et perdent de l'argent. Mais elles ne le diront jamais. GM