« L'externalisation des données reste une des stratégies les plus sûres »

Propos recueillis par Milena Radoman

Spécialisé dans la sécurité informatique des TPE et PME, **Xefi Monaco** préconise l'externalisation de l'hébergement des données. Son gérant Jérémy Audegean explique pourquoi choisir cette solution.

Dans le contexte actuel lié au Covid, l'appel au numérique a été primordial avec le développement entre autres du télétravail. Ce contexte a-t-il dopé les cyberattaques ?

Oui bien évidemment. Le télétravail nécessite d'ouvrir le système d'information de l'entreprise pour qu'il soit accessible depuis l'extérieur. Ce qui est un vecteur privilégié pour les cyberattaques, donc beaucoup d'entreprises qui n'avaient pas leur système d'information ouverts, et qui l'ont fait, se sont naturellement exposées.

De plus, le Covid a nécessité que les entreprises fassent cette transition en urgence, et non sur une opération planifiée. Permettre le télétravail lorsqu'il est bien appréhendé, ne présente pas de risque majeur pour l'entreprise. Cependant lorsqu'il est fait avec précipitation, et sans mettre la sécurité au cœur du projet, mais plutôt la rapidité d'être opérationnel, cela conduit à des situations qui peuvent être risquées

Enfin les équipes techniques, qui ont eu la charge d'assurer le déploiement de ces solutions, sont généralement les mêmes qui ont pour mission de s'occuper de la sécurité des infrastructures. Etant donné qu'elles ont été sursollicitées en début de confinement pour le déploiement du télétravail, elles n'ont, de manière logique, pas pu accorder la même énergie que d'habitude pour superviser la sécurité du système d'information.

Ces différents facteurs cumulés ont créé un terrain propice à la multiplication des attaques, et cela s'est vérifié sans attendre, dès le mois de mars.

Quelles difficultés cela engendre pour les PME ? Sont-elles armées pour ce genre d'attaques ?

Les difficultés peuvent être nombreuses, suivant le type d'activité. Cela passe par de la formation et de la sensibilisation des utilisateurs, sur les bonnes pratiques. Sachant que dans la majorité des attaques, c'est l'utilisateur qui est le point d'entrée du piratage, son comportement est primordial.

Certaines entreprises ont dû acquérir en urgence des équipements pour permettre le télétravail, que ce soit de quoi sécuriser le réseau de l'entreprise lors de son ouverture sur l'extérieur, ou la fourniture de terminaux aux salariés pour qu'ils puissent télétravailler depuis leur domicile. Le fait est qu'il y a eu une demande énorme dans un laps de temps très court, sur du matériel qui est majoritairement fabriqué en Asie, là où beaucoup d'unités de production étaient à l'arrêt et avec une logique d'acheminement plus complexe que d'habitude, car la crise sanitaire a commencé là-bas. Nous avons dû faire face à des pénuries et des livraisons au compte-goutte sur les équipements les plus demandés, notamment les ordinateurs portables.

La situation des entreprises est très inégale. Celles qui avaient déjà mis la sécurité informatique et la protection des données au cœur de leur stratégie s'en sont beaucoup mieux sorties que les autres. Certaines entreprises ont pu basculer en télétravail en quelques heures, d'autres ont mis plusieurs jours avant d'être opérationnelles en toute sécurité.

Quelles sont les solutions que devraient développer les PME selon vous (Sécurisation des données dans cloud, serveur, data center) ? Quel est l'avantage de chacune ? Sont-elles complémentaires ?

L'externalisation des données reste une des stratégies les plus sûres. Le fait de mettre ses données en data center permet d'avoir un niveau de sécurité accru, de par les équipements de sécurité en data center qui sont largement plus sûrs et efficaces que ceux

que l'on retrouve dans les entreprises, mais également par les équipes de supervision qui y sont dédiées, avec un très haut niveau de compétence. Une analogie que je prends souvent avec mes clients lorsque l'on parle de l'hébergement de données en data center, c'est celle de la banque. Est-ce que les biens précieux dont on dispose sont plus en sécurité chez soi ou dans le coffre d'une banque ? La réponse est sans équivoque.

L'externalisation des données fait peur au chef d'entreprise, car il a l'impression qu'il perd la maitrise de celles-ci vu qu'elles ne sont plus stockées chez lui. Cela a été marqué notamment par l'apparition de services cloud proposés par certaines grandes sociétés qui proposaient des solutions où l'hébergement de la donnée n'était pas clair, et pouvait se faire dans des pays étrangers avec notamment une législation différente.

Nous rassurons nos clients sur ce point, en leur garantissant que leurs données restent stockées physiquement sur le territoire monégasque, et sur des équipements qui appartiennent au groupe Xefi. C'est l'une de nos forces : le groupe Xefi a une vraie expertise dans ce domaine puisqu'il possède également deux datacenters en France, avec très haut niveau de certification (notamment avec un agrément d'hébergement pour les données médicales). Nous ne sous-traitons pas le stockage de nos données, en la confiant à des tiers. De plus nos offres garantissent contractuellement à nos clients qu'ils restent propriétaires de leurs données, et qu'ils peuvent les reprendre à tout moment.

Vous formez les PME de la place ? Comment ?

Nous accompagnons nos clients sur les sujets de cybersécurité, c'est même devenu notre cœur de métier au fil des années, car le risque est croissant. Etant donné que nous travaillons principalement avec des TPE/PME, nos clients n'ont généralement pas de service informatique en interne, et personne pour les conseiller. C'est pour ça que ce segment d'entreprise reste très vulnérable. Notre mission consiste à informer nos clients sur les risques potentiels sur ces sujets. Nous avons actuellement une quarantaine de clients monégasques en contrat chez nous, je m'occupe également d'une autre agence Xefi à Nice. Au cumul c'est un peu plus de 400 clients que nous accompagnons sur les sujets IT (technologies de l'information).

L'autre point, comme évoqué précédemment, est la sensibilisation et l'accompagnement des utilisateurs. Il est fréquent que nos techniciens profitent de l'assistance d'un utilisateur pour l'informer des bonnes pratiques ou relever un comportement. Il est même fréquent que nos clients nous envoient un email douteux pour nous demander notre avis avant d'en ouvrir sa pièce jointe. Notre savoir faire est de permettre à nos clients de se reposer sur nous pour l'intégralité de ces sujets, qui sont pourtant très stratégiques, afin qu'ils se concentrent sereinement sur leur cœur de métier.

''Storing data externally is still one of the safest strategies.''

Specialising in IT security for small and medium-sized businesses, XEFI Monaco recommends storing company data externally. Company boss, Jérémy Audegean, talks about the reasons for choosing this solution.

In the current Covid-19 context, it was essential for companies to convert to digital working practices including distance working. Have these developments given rise to more cyber attacks?

Yes, of course. Working from home means a company's IT system has to be externally accessible, which is of great benefit to hackers. Many companies did not have an open IT system in place and those who took this measure did, of course, make themselves vulnerable. Also, the pandemic meant that businesses had to undertake a digital transition quickly and not via a planned operation. A teleworking system that has been well-planned does not present a major security risk; however, when it is done in a hurry, putting speed rather than data protection at the top of the list, this can lead to risky situations. The technical teams whose mission it was to carry out these transitions generally consisted of the same people who look after these companies' cyber safety and, given that they were overbooked at the beginning of lockdown to set up teleworking, they were not able, physically, to offer the usual attention when supervising the safety of IT systems. The accumulation of these different factors created an opportunity for multiple cyber attacks – and that is exactly what happened straight away, right from March onwards.

What problems does this create for medium-sized businesses? Are they equipped to deal with hackers?

There can be many problems, according to the nature of the company's activity. We need to train users and make them aware of the best practices. As we know that the user is the main vector and entry point for most cyber attacks, how the user behaves online is of great importance. Some companies had to put distance working equipment in place urgently and, whether it was a matter of making sure the company IT network was secure when opened to the exterior or of providing staff with materials to set up a home office, the fact is that there was a huge demand over a very short period of time: most of these products are made in Asia, where many factories were at a standstill and transportation was much more complicated than usual, as the health crisis had started over there. We were faced with shortages and deliveries took place in dribs and drabs for the most popular products, such as laptops. Not all companies found themselves in the same situation as those which had already placed IT security at the heart of their strategy came out of it much better than those which had not. Some businesses were able to move over to teleworking in a matter of hours, whilst others took several days to become safely operational.

What measures do you think medium-sized companies should take – storing data in a cloud, on a server, or at a data centre? And what are the advantages of each of these? Do they complement one another?

Storing data externally is still one of the safest strategies. Storing company information in a data centre means it is even more secure, because of the security equipment available, which is much more efficient than what is found in-house in businesses, and also because there are highly-skilled, dedicated surveillance teams. I often like to take the analogy of the bank when I am talking to clients about where to store their data: do you think your most precious possessions are safer at your home or in safe deposit box at the bank? The answer is clear-cut. External data storage can scare a company boss as he or she may feel they have lost control over it, if it is not stored in-house. This was seen, in particular, with the emergence of some big companies offering cloud storage in which the information would be stored in an unspecified location, sometimes in a foreign country and under different legislation. We would like to reassure our clients on this point, by offering a guarantee that their data will be physically stored with the territory of the Principality of Monaco; and it is stored on equipment belonging to us, the XEFI Group. This is one of our strengths as XEFI has a real expertise in this domain, also owning two data centres in France, which are certified to a high level, notably authorised to store medical data. We will never subcontract the storage of data and our offers contractually guarantee our clients that they will remain the owners of their data and they can withdraw their information whenever they wish.

How do you train Monaco's medium-sized businesses in this subject?

We guide our clients on questions of cyber security and this has even become our core activity over the years, as it is a growing risk. Given that we mostly work with small or medium-sized businesses, our clients generally do not have an internal IT system or anyone to advise them. This is why that segment has been so vulnerable. Our mission is to inform our clients on the potential risks here. We currently have around 40 clients in Monaco and I also look after another of our XEFI branches in Nice. In total, we currently work with more than 400 clients, advising them on IT matters. The other subject, as mentioned earlier, is raising the awareness of computer users. Our technicians frequently take the opportunity of passing on best practice advice to users when helping a user with something else. And our clients regularly forward us dodgy-looking emails asking for advice on whether to open the attachment or not. Our aim is for our clients to be able to use our expertise and to rely on us for all of these things, all of which are highly strategic, so that they can concentrate fully on their core activities.