Economie & Finance

23%

LES EMPLOYEURS FINANCENT ENTRE 23 ET 41% des coûts de formation professionnelle supérieure en Suisse, devenant la plus importante source de financement externe, devant les subventions fédérales. Les candidats, eux, prennent en charge environ la moitié de leur formation.

MARGRETHE VESTAGER
Vice-présidente de la Commission européenne

«Nous autorisons la concentration entre Fiat Chrysler et Peugeot car cela facilitera l'entrée et l'expansion sur le marché des camionnettes utilitaires légères», a-t-elle déclaré.

3500

LE NOMBRE D'ENTREPRISES QUI ONT MIS LA CLÉ SOUS LA PORTE EN SUISSE de janvier à fin novembre. C'est près d'un cinquième de moins que sur la même période en 2019, indique le cabinet Bisnode dans son pointage mensuel, mettant en avant les mesures de soutien liées au coronavirus.

SMI 10 305,52 -2,07%	↓	Dollar/franc	0,8858 ↑
		Euro/franc	1,0835 ↑
Euro Stoxx 50 3448,68 -2,74%	↓	Euro/dollar	1,2230 ↓
		Livre st./franc	1,1826 ↓
FTSE 100 6416,32 -1,73%	↓	Baril Brent/dollar	50,09 ↓
		Once d'or/dollar	1881 ↑

Cyberattaque: le diagnostic se poursuit

SÉCURITÉ Le modus operandi de la vaste cyberattaque touchant administration américaine et multinationales met en cause la Russie, ce que Moscou réfute. Des firmes suisses, victimes potentielles, analysent actuellement leurs systèmes informatiques

ANOUCH SEYDTAGHIA
@Anouch

Le nombre de victimes d'une vaste cyberattaque mondiale ne cesse d'augmenter. La semaine passée, Microsoft évoquait le chiffre de 40 cibles, principalement aux Etats-Unis, mais aussi basées au Canada, au Mexique, en Belgique, en Espagne, en Grande-Bretagne, en Israël et aux Emirats arabes unis. «Il est certain que ce chiffre va augmenter», avait déjà averti Brad Smith, président de Microsoft. En Suisse, plusieurs multinationales, cibles potentielles de cette attaque, scannent leurs systèmes informatiques. Et dimanche, la société de cybersécurité américaine FireEye évoquait au moins 50 victimes.

Derrière ce hacking mondial, commencé en mars mais révélé la semaine dernière seulement, se trouverait un coupable: la Russie. «C'était une entreprise très importante, et je crois que nous pouvons maintenant dire assez clairement que ce sont les Russes qui se sont engagés dans cette activité», affirmait vendredi le secrétaire d'Etat américain, Mike Pompeo. Alors que Donald Trump insinuait ce week-end que la Chine pouvait être derrière cette attaque – une «farce», selon Pékin –, Moscou niait aussi toute implication. Mais plusieurs experts affirment que la piste évoquée par Mike Pompeo est la bonne. Brad Smith a mentionné la Russie, sans l'accuser directement.

Brad Smith, président de Microsoft, a mentionné la Russie dans le contexte de ces cyberattaques, sans l'accuser directement. *(PATRICIA DE MELO MOREIRA/AFP)*

> Une chose semble sûre, il ne s'agit pas de simples criminels

Peut-on accuser Moscou avec certitude? «Non. Mais il semble y avoir un certain nombre d'indices qui pointeraient vers APT29, un groupe de hackers appartenant au Service des renseignements extérieurs de la fédération de Russie», affirme Steven Meyer, directeur de la société de cybersécurité ZENData, à Genève. L'expert rappelle que «les attaques précédentes dites «NotPetya», en 2017, et «Olympic Destroyer», en 2018, n'ont qu'été officiellement attribuées qu'en octobre 2020 à la Russie. Il faudra donc être patient afin que l'enquête suive son cours.»

Une chose semble sûre, il ne s'agit pas de simples criminels. «Il s'agit bien d'un gouvernement et pas du crime organisé. La précision, le savoir-faire, la patience ou encore les capacités de camouflage utilisées dans cette opération ne correspondent clairement pas au modus operandi du crime organisé», poursuit Steven Meyer.

«Un affront scandaleux»

Les Etats-Unis veulent déjà contre-attaquer. Ce week-end, le sénateur républicain Mitt Romney affirmait que ce piratage est «un affront scandaleux à notre souveraineté, auquel il faudra qu'il soit répondu de manière très forte, pas juste rhétorique, mais aussi avec une cyberréponse de la même magnitude ou plus grande». Les Etats-Unis emploient d'ailleurs sans doute des méthodes similaires à celle de la Russie, avance Steven Meyer: «Toutes les cyberpuissances travaillent dur pour infiltrer les autres gouvernements. Dans un but d'espionnage, mais aussi pour se positionner en cas de cyberconflit, voire de conflit armé: si un gouvernement peut hacker le système antiaérien d'un pays ennemi, il se sentira en meilleure position lorsqu'il lancera une offensive militaire.»

Pour perpétrer leur attaque, les hackers ont d'abord infecté un logiciel standard d'analyse (Orion) utilisé par plus de 30000 organisations clientes de la firme américaine SolarWinds. En créant une porte dérobée (*backdoor*) dans ce logiciel, les pirates ont pu, dès mars, accéder à des systèmes, voler des informations, voire injecter des données sans être inquiétés. Plusieurs agences américaines ont annoncé avoir trouvé des traces de ce piratage.

Cisco et Intel touchés

Difficile de savoir ce que recherchaient exactement ces pirates. Ils semblent avoir voulu accéder à des informations sensibles et auraient aussi ciblé d'importantes entreprises informatiques de taille. La semaine passée, Microsoft avouait faire partie des victimes et que la moitié de ses clients touchés étaient actifs dans le secteur tech. Mais ce n'est pas tout: lundi, le *Wall Street Journal* affirmait que les géants américains informatiques Cisco Systems, Intel, VMWare et Belkin avaient retrouvé du code malicieux dans leurs systèmes. «Les dégâts vont être massifs. Lorsqu'un réseau informatique est infiltré par des hackers qualifiés pendant plusieurs mois, il est quasiment impossible d'affirmer avec certitude que rien n'a été volé, que rien n'a été corrompu et que ces pirates ont eu tous les accès révoqués», conclut Steven Meyer. ▬

RÉACTIONS

Swisscom analyse, les autres se taisent

Parmi les plus de 30000 clients de l'entreprise américaine SolarWinds qui utilisent son logiciel Orion, environ 18000 ont téléchargé et installé la mise à jour infectée. Sans surprise, le logiciel d'analyse des réseaux Orion est utilisé par de nombreuses entreprises suisses, telles que Swisscom, Novartis, Credit Suisse ou encore Nestlé. Ces multinationales sont peu loquaces sur un sujet sensible. Swisscom est celle qui s'ouvre le plus sur ce sujet. «Notre service de sécurité est au courant de l'attaque de hackers à SolarWinds. Nous pouvons confirmer que Swisscom est un client de SolarWinds, répond un porte-parole. Le vendeur a fourni deux hotfixes. Swisscom a déjà installé ces correctifs. Indépendamment de cela, nous avons étendu sa surveillance. Nos experts en sécurité analysent les systèmes concernés et n'ont trouvé aucun indice d'utilisation abusive. Les analyses se poursuivent.»

Aucun commentaire

De son côté, Credit Suisse répond qu'il ne fait, par principe, aucun commentaire concernant les questions relatives à la cybersécurité. Nestlé n'a pas répondu à nos questions, alors que Novartis nous a demandé de contacter SolarWinds.

Il paraît certain que toutes ces entreprises analysent actuellement leurs systèmes internes.

De son côté, le Centre national pour la cybersécurité (NCSC) – qui n'a lui non plus pas répondu à nos requêtes – affirmait dans la presse alémanique avoir «informé les opérateurs d'infrastructures critiques et fait des recommandations». ▬ A. S.

Les bourses affolées par la nouvelle souche du virus

FINANCE **Toutes les places européennes voyaient rouge ce lundi, les compagnies aériennes faisant partie des actions les plus affectées**

MATHILDE FARINE
@MathildeFarine

Les bourses auraient pu entamer la semaine sur une note positive. Après tout, le Congrès américain venait de se mettre d'accord, dimanche soir, sur un nouveau paquet d'aides à l'économie. Fixé à 900 milliards de dollars (près de 800 milliards de francs), il était en négociation depuis des mois, incluant notamment des mesures de soutien aux petites entreprises, des chèques aux familles précaires, des aides au logement ou chômage. Il devait encore être voté lundi dans la journée.

«Les Etats-Unis ont eu leur plan de relance, mais il semble que c'était largement déjà pris en compte dans les indices», a affirmé Craig Erlam, analyste pour le courtier Oanda, à l'AFP. De fait, ce n'est pas ce qui a retenu l'attention des marchés. Ces derniers s'inquiètent plutôt de l'apparition d'une nouvelle souche du Covid-19, plus contagieuse.

Cette dernière a obligé le Royaume-Uni à prendre de nouvelles mesures de restriction, la situation étant jugée «hors de contrôle» dans certaines régions. Elle a aussi poussé une grande partie de l'Europe à fermer ses frontières à la Grande-Bretagne en général. Si elle ne semble, pour l'heure, pas provoquer de cas plus graves, ni mettre en cause les traitements ou les vaccins qui sont en cours d'homologation, cette forme du virus risque de paralyser encore davantage l'Europe, craignent les investisseurs.

Aviation touchée

Parmi les plus touchés figurent Paris (-2,4%), Francfort (-2,8%) et Milan (-2,6%). Epicentre de cette nouvelle souche, Londres (-1,7%) limitait les dégâts, tandis que Zurich perdait 2,1% à la clôture. Le secteur aérien, comme les constructeurs automobiles, faisait partie des actions les plus touchées par cette nouvelle flambée d'inquiétude. Les bourses américaines ont elles aussi ouvert en recul, mais de façon moins marquée qu'en Europe. Le pétrole chutait également (-4% à 50,24 dollars pour le Brent pour livraison en février et -3,6% à 47,32 dollars pour le WTI pour livraison en janvier).

A l'inverse, les valeurs refuges étaient au centre de toutes les attentions, à l'instar des obligations jugées sûres de certains pays. ▬