Date: 24.10.2022

PLEIN CENTRE

Auflage nicht bekannt

Plein Centre / CP
1001 Lausanne
058 / 796 33 00
www.centrepatronal.ch

Genre de média: Médias imprimés
Type de média: Magazines spéc. et de loisir

Parution: 10x/année

Éditions Slatkine
GENÈVE

Page: 10
Surface: 103'409 mm²

Ordre: 844003
N° de thème: 844.003

Référence: 86021922
Coupure Page: 1/2

Solange Ghernaouti

Comment se protéger face aux cyberattaques?

Des communes de Rolle, d'Yverdon et de Bülach jusqu'à un Etat comme le Costa Rica en passant par de nombreuses entreprises, les cyberattaques sont omniprésentes. Nous avons rencontré Mme Solange Ghernaouti, spécialiste en la matière.

Propos recueillis par Gauthier Dorthe // Photo Michel Duperrex

La cybersécurité est devenue un problème incontournable pour tout un chacun, notamment pour les entreprises. Concrètement, qu'est-ce qu'une entreprise doit faire aujourd'hui pour se protéger au mieux?

La cybersécurité fait partie des solutions pour contribuer à maîtriser les risques informatiques, notamment d'origine criminelle et liés à internet. Ce dernier rend accessibles les systèmes des individus, des organisations et des Etats à des acteurs malveillants qui exploitent les vulnérabilités techniques, organisationnelles ou humaines.
La cybersécurité est une affaire de gestion des risques qui relève de la gestion stratégique et opérationnelle d'une entreprise, laquelle doit comprendre les menaces internes et externes qui pourraient l'affecter, mettre en péril sa compétitivité, sa pérennité ou sa réputation.
Une fois les valeurs à protéger identifiées en sachant contre quoi et pourquoi le faire, il est possible de mettre en œuvre des mesures pour réduire ses vulnérabilités, renforcer sa résistance aux cyberattaques et pouvoir réagir en cas d'incidents avant qu'ils ne se transforment en crise.

Dans le cas où les données d'une entreprise sont piratées et qu'une rançon est exigée, comment l'entreprise devrait-elle réagir?

Cela entraîne une situation de crise majeure à laquelle le dirigeant doit faire face dans l'urgence, mais chaque cas est particulier. Beaucoup d'attaques sont le fait de criminels opportunistes qui procèdent de façon non discriminée, ce qui signifie qu'ils vont pirater n'importe quelle structure privée ou publique qui doit donc s'attendre à être cyberattaquée. «Qu'est-ce que je ferais si mes données étaient bloquées ou volées?» est LA question incontournable à se poser avant. L'anticipation permet de prévenir la prise en otage de ses ressources, d'être préparé à savoir que faire, quelles ressources mettre en œuvre, comment communiquer, comment maintenir la continuité des activités, minimiser ses impacts, etc. Il est préférable d'investir dans des démarches de protection et de prévention afin d'éviter de devoir payer des rançons et d'investir de toute manière postérieurement dans sa cybersécurité.

Dans quelle mesure les pouvoirs publics peuvent-ils ou devraient-ils soutenir les individus et les acteurs économiques face aux cyberdangers?

Une partie du problème provient de la manière dont l'informatisation de la société s'effectue en utilisant des solutions informatiques comportant des défauts de sécurité. L'économie numérique, d'inspiration néo-libérale *made in USA*, est basée sur la performance et la rationalité économiques au profit de certains acteurs. Son modèle économique repose sur l'exploitation des données et non sur leur protection, autorisant ainsi un nouveau champ d'affaire lié à la cybersécurité.
Les usages abusifs, détournés, criminels, terroristes et conflictuels du numérique sont une réalité qui affecte nos sociétés interconnectées à l'échelle mondiale. Plus nous sommes connectés et interdépendants, plus nous sommes vulnérables, et plus notre sécurité dépend de celle de nos voisins. Appréhender les cyberdangers nécessite d'agir de manière globale, complémentaire et cohérente, dans des dimensions politique, économique, juridique, technique et sociale, aux niveaux local et international. Peut-être serait-il temps de changer le paradigme qui consiste à faire porter le prix de la sécurité et le coût de l'insécurité aux usagers et à la société alors qu'il n'y pas de *security by design* dans la majorité des solutions informatiques utilisées.
Dans ce contexte, la sensibilisation des utilisateurs aux dangers, l'éducation aux bonnes pratiques de sécurité sont importants mais pas suffisants.

Date: 24.10.2022

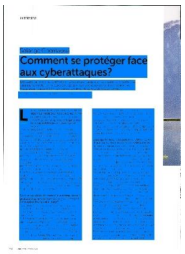
PLEIN CENTRE

Auflage nicht bekannt

Plein Centre / CP
1001 Lausanne
058 / 796 33 00
www.centrepatronal.ch

Genre de média: Médias imprimés
Type de média: Magazines spéc. et de loisir

Parution: 10x/année



Éditions Slatkine
GENÈVE

Page: 10
Surface: 103'409 mm²

Ordre: 844003
N° de thème: 844.003

Référence: 86021922
Coupure Page: 2/2

A propos de Mme Solange Ghernaouti

Professeur à l'Université de Lausanne

Chevalier de la légion d'honneur

Directrice Swiss Cybersecurity Advisory & Research Group

Associée fondatrice Heptagone digital risk management & security

Auteur de l'ouvrage *La cybersécurité pour tous*, Editions Slatkine 2022, soutenu par le Centre Patronal et la FER Genève

Imposer le recours systématique au numérique sans pouvoir s'assurer de son innocuité et de la qualité de sa sécurité, en sous-estimant les cyber risques, revient à fragiliser la société et à transformer citoyens et acteurs économiques et publics en cibles privilégiées de cyberattaques.
Etre vulnérable n'est pas une fatalité mais cela requiert une vision politique forte, des mesures stratégiques et opérationnelles, des ressources financières et des compétences humaines à la hauteur des enjeux.

Cet été, c'est la commune de Bülach qui s'est trouvée sous le feu d'une cyberattaque. Est-ce que les cyberattaques diffèrent selon qu'elles visent les institutions publiques, les entreprises ou les particuliers?
La motivation des attaquants, l'intensité des cyberattaques, leur ampleur et leurs conséquences varient en fonction des cibles et des buts recherchés par leurs auteurs ou commanditaires. Toute une gamme de nuisances existe, allant du cyber harcèlement des individus à la déstabilisation économique ou politique d'un pays en passant par l'atteinte au bon fonctionnement des organisations. La cybercriminalité est de la criminalité dont la performance est liée à internet, tout comme le sont les diverses formes d'espionnage, d'escroquerie, de désinformation, de manipulation de l'opinion et des comportements. Tous les systèmes d'informations, toutes les données (infrastructures critiques et données de santé comprises) sont l'objet de convoitises par des moyens licites et illicites, au profit d'acteurs étatiques et non étatiques agissant de manière isolée ou organisée. Les conflits entre les individus, les organisations et les Etats se déclinent par des actions offensives dans le cyberespace et les mondes virtuels avec des conséquences bien réelles.