Datum: 14.05.2014

Bilan
LA RÉFÉRENCE SUISSE DE L'ÉCONOMIE

Bilan
1204 Genève
022/ 322 36 36
www.bilan.ch

Medienart: Print
Medientyp: Publikumszeitschriften
Auflage: 14'249
Erscheinungsweise: 26x jährlich

Themen-Nr.: 999.082
Abo-Nr.: 1078757
Seite: 16
Fläche: 40'162 mm²

Les cyberattaques montent en puissance

PAR DINO AUCIELLO

L'interdépendance des entreprises intensifie les assauts contre les infrastructures informatiques dans le monde. Les sociétés suisses doivent-elles seules assumer les risques?

Gérald Vernez, délégué du chef de l'armée pour la cyberdéfense.

GÉRALD VERNEZ AVERTIT: «IL NE FAUT PAS S'ATTENDRE À CE QUE L'ÉTAT SUBVIENNE À TOUS LES BESOINS DES ENTREPRISES»

Datum: 14.05.2014

Bilan
LA RÉFÉRENCE SUISSE DE L'ÉCONOMIE

Bilan
1204 Genève
022/ 322 36 36
www.bilan.ch

Medienart: Print
Medientyp: Publikumszeitschriften
Auflage: 14'249
Erscheinungsweise: 26x jährlich

Themen-Nr.: 999.082
Abo-Nr.: 1078757
Seite: 16
Fläche: 40'162 mm²

RÉVÉLÉE LE 6 AVRIL DERNIER, «Heartbleed», la faille majeure de sécurité informatique qui a touché plus d'un demi-million de sites, a soufflé un vent de panique parmi les entreprises.

«Nous avons été très rapidement alertés, témoigne Daniel Stocco, chef IT et sécurité à la BCGE, lors d'une conférence sur la cybercriminalité organisée par la banque début mai. Il fallait déterminer si des systèmes étaient impactés et les corriger au plus vite. La réactivité fait ici toute la différence.»

Si l'hémorragie a globalement été stoppée, ce «cœur saignant» a montré la vulnérabilité croissante des sociétés, grandes et petites, en matière de protection des données. «Les cyberrisques peuvent désormais se propager d'une organisation à une autre par un effet domino, du fait de l'interdépendance des infrastructures techniques et informatiques notamment, relève Solange Ghernaouti, experte internationale en cybercriminalité et professeure à HEC Lausanne. Ce qui déclenche des effets en cascade: une panne d'électricité, des télécoms, jusqu'aux marchés financiers...» Les escroqueries ont augmenté en nombre et en intensité, avec des cibles bien définies. «C'est une croissance logique, qui suit l'évolution du web, des services, des technologies et des usages.»

Le groupe de distribution américain Target a récemment subi un piratage massif de données personnelles et bancaires: jusqu'à 110 millions de clients étaient concernés. La Suisse n'est pas en reste. D'après la cartographie en temps réel de la société spécialisée Kaspersky Lab, elle occupe début mai la 36e position des pays les plus touchés par la «cyberguerre» à travers le monde. Le Service national de coordination de la lutte contre la criminalité sur internet (SCOCI) a, lui, enregistré 9208 dénonciations en 2013, soit une augmentation de 12% par rapport à 2012, avec une majorité d'infractions économiques.

Un continuum sécurité défense

Quel rôle doit jouer la Confédération? Pour Gérald Vernez, délégué du chef de l'armée pour la cyberdéfense, c'est aux entreprises de se réapproprier leur souveraineté digitale et de définir leurs réels besoins informatiques. «Il ne faut pas s'attendre à ce que l'Etat subvienne à tous les besoins de l'entreprise. Ce qui est primordial, c'est que chacun comprenne sa propre responsabilité. Car le problème commence souvent au niveau de l'utilisateur.»

Si l'individu ou l'entreprise ne fait pas son travail à l'interne en termes de sécurité, ajoute-t-il, «les échelons supérieurs et les moyens de la Confédération seront submergés par des bagatelles. Même les meilleurs moyens de défense ne serviraient alors à rien.»

Pour Solange Ghernaouti, le gouvernement suisse a relativement bien saisi les enjeux de la maîtrise des cyberrisques: «Il existe une stratégie nationale de cybersécurité, mais la feuille de route et les ressources pour l'appliquer sont insuffisantes. Globalement, nous devrions être plus proactifs.»

C'est au final pour la mise en place d'un continuum sécurité défense efficace que plaide Gérald Vernez: «L'armée est un élément du dispositif national et on attend d'elle qu'elle fournisse aussi un certain nombre de prestations subsidiaires. Mais l'armée avec ses miliciens, tout comme l'Etat, ne peut intervenir dans tous les cas, car il y a des limites qu'on ne peut franchir. C'est pourquoi une solution décentralisée, avec des observatoires et des plateformes d'échange d'information et de collaboration, est mise en place pour que se développe une compétence distribuée, et qu'en bout de chaîne les victimes puissent trouver des réponses au plus vite.» B