La politique gouvernementale Ã©choue dans la sÃ©curitÃ© Informatique.
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 18/11/2011 15:00:00

Les gouvernements oublient de sâappliquer ce quâils recommandent en matiÃ¨re de sÃ©curitÃ© informatique, surtout avec de plus en plus de cyber criminels sâattaquant, apparemment, aux dÃ©partements les moins risquÃ©s des Ã©tats.

Â« *De fait, les criminels ont accÃ¨s Ã toutes les bases de donnÃ©es des gouvernements* Â» nous dit **Wieland Alge**, Directeur General EMEA chez Barracuda Networks.

Que ce soit le virus **Stuxnet**, crÃ©Ã© pour saboter le programme nuclÃ©aire iranien ou le plus rÃ©cent **Dugu**, qui permet Ã ses utilisateurs dâinstaller des programmes, afficher, modifier ou encore supprimer des donnÃ©es en acquÃ©rant la totalitÃ© des droits dâutilisateur, ils soulignent la menace pour les rÃ©seaux des gouvernements. Par consÃ©quent, les gouvernements cherchent des moyens de protÃ©ger leurs rÃ©seaux, mais malgrÃ© tous les efforts mis en place, **Wieland Alge** pense que ce nâest pas suffisant.

Â«*En reconnaissant la menace posÃ©e par les cyber-criminels, les gouvernements aident Ã sensibiliser sur la nÃ©cessitÃ© de la sÃ©curitÃ© informatique. MalgrÃ© cela, les gouvernements ont besoin de mettre activement en pratique ce qu'ils prÃªchent et de gÃ©rer leur propre sÃ©curitÃ© de maniÃ¨re efficace.* "

Pour exemple, le piratage de la base de donnÃ©e du groupe UMP de lâassemblÃ©e en France la semaine derniÃ¨re qui avait abouti Ã la publication de donnÃ©es trÃ¨s personnelles de chacun des membres du parti.

Alge poursuit: Â«*Le paysage de la sÃ©curitÃ© informatique est constituÃ© d'une variÃ©tÃ© de criminels diffÃ©rents avec des objectifs diffÃ©rents. Les Hacktivistes sont des groupes anonymse qui passent un message. Les Cyber-terroristes cherchent Ã affaiblir la puissance d'un pays par tous les moyens possible. Il y a ceux qui cherchent Ã voler des informations, avec pour ultime but de gagner de l'argent. Les institutions gouvernementales sont conscientes de cela, aident*

significativement Ã sensibiliser Ã la menace que ces criminels portent, toutefois, Ã©coutent-ils leur propre message? "

Wieland Alge constate que malgrÃ© le fait que les gouvernements aient des stratÃ©gies en place pour protÃ©ger leurs rÃ©seaux, avec des procÃ©dures standardisÃ©es et des protocoles de contrÃ´le, presque toutes les institutions gouvernementales sont laissÃ©s seules pour rÃ©soudre leurs problÃ¨mes de sÃ©curitÃ©. Afin de lutter contre cela, Alge pensent que des mesures simples peuvent Ãªtre mises en place.

Â« *La plupart des attaques se font via des applications web mal sÃ©curisÃ©es, et par consÃ©quent il y a beaucoup de services de sÃ©curitÃ© disponible et autant de malfaÃ§ons. Ce n'est pas prudent pour les institutions gouvernementales dâ□□Ãªtre simplement laissÃ©es Ã ellesâ□□mÃªmes pour assurer la sÃ©curitÃ© de leur propre rÃ©seau*Â».

Wieland Alge conclut: Â«*Comme tout le monde, les gouvernements ont besoin de conseils quand il s'agit de gÃ©rer et de protÃ©ger leur rÃ©seau. Un audit peut aider Ã identifier oÃ¹ se situent les failles et proposer des directives pour amÃ©liorer, de faÃ§on continue la sÃ©curitÃ©, et pour dÃ©velopper des pratiques standardisÃ©es pouvant Ãªtre attribuÃ©es aux ministÃ¨res livrÃ©s Ã eux-mÃªmes.*

Aussi, une bien meilleure comprÃ©hension des menaces liÃ©es Ã la cybersÃ©curitÃ© mÃ¨nera Ã une meilleure allocation des budgets. Nous nâ□□essayons pas de crÃ©er la polÃ©mique et dâ□□en tirer parti financiÃ¨rement, il sâ□□agit surtout dâ□□avoir une comprÃ©hension collective du problÃ¨me et de savoir Ã quoi sont allouÃ©s les budgets. Â»