Le risque de cyberattaques SAP est sous-estimé

Commandée par un spécialiste de la sécurité d'applications métiers, Onapsis, l'enquête portant sur la **cybersécurité des applications SAP** est diffusée. Aux yeux de l'IT, les cadres dirigeants sous-estiment les risques de cyberattaques qui pèsent sur les applications SAP. C'est ce qui ressort de l'enquête rendue publique le 24 février. Ce même jour SAP a confirmé avoir nommé **Justin Somaini** au poste de directeur de la sécurité (CSO, Chief Security Officer). Sa nomination est effective depuis le 1er janvier.

Le sondage a été réalisé par le Ponemon Institute, de la mi-décembre 2015 au 4 janvier 2016, auprès d'un échantillon de **607 décideurs IT et managers de la sécurité informatique** basés aux États-Unis. Plus de la moitié d'entre eux ont déclaré que la plateforme SAP de leur entreprise a été attaquée en moyenne deux fois dans les 24 derniers mois. Et 56 % jugent que leur organisation n'est pas à l'abri d'une violation de données du fait d'applications SAP non sécurisées. Il est *« probable »* pour 42 % des répondants, voire *« fort probable »* pour 33 % des managers IT interrogés, que les systèmes SAP soient, un jour ou l'autre, infectés par un ou plusieurs malwares.

Mais qui est responsable ?

63 % des professionnels IT interrogés estiment que les cadres dirigeants de leur entreprise ont tendance à **sous-estimer le risque** que représente des applications SAP non sécurisées pour les données stratégiques de l'organisation. Or, l'impact d'un vol de données, d'un détournement ou d'une intrusion dans les systèmes SAP utilisés par leur entreprise, serait *« trés grave »* ou *« catastrophique »* pour 60 % des répondants. Ainsi, le **coût moyen** d'une mise hors service de ces systèmes ciblés par une cyberattaque est estimé à **4,5 millions de dollars** (coûts directs et indirects inclus).

Qu'en est-il des responsabilités ? 54 % des répondants pensent que c'est à **SAP**, et non à leur entreprise, d'assurer la sécurité de ses applications et plateformes. En interne, pour 30 % du panel, personne n'est responsable en cas de violation des données d'un système SAP de l'entreprise. Mais 26 % considèrent que cette responsabilité incombe au DSI et 18 % seulement au RSSI.

Un Chief Security Officer chez SAP

« Les données de l'enquête montrent que les cyberattaques ciblant des applications SAP risquent d'augmenter, mais qu'il n'y a pas d'équipe dédiée ou de poste spécifique pour y répondre », a déclaré Larry Ponemon, président et fondateur du Ponemon Institute. *« Il semble que la cybersécurité SAP ne relève ni des attributions d'équipes en charge de la sécurité, ni des responsables de la sécurité des informations. Il est important qu'ils se mobilisent pour combler cette faille et en faire une priorité »*, a-t-il ajouté.

C'est dans ce contexte que SAP a ouvert un premier poste de **CSO** (Chief Security Officer) et recruté **Justin Somaini**. Ancien Chief Trust Officer du fournisseur de services Cloud Box, et ex-manager

chez Yahoo et Symantec, Justin Somaini a plus de 20 ans d'expérience dans la sécurité IT.

Lire aussi :

ERP : SAP domine Oracle, Infor déboulonne Microsoft Dynamics
Avec Hana, SAP redécouvre la sécurisation des données

crédit photo © Gil C / Shutterstock.com