Communiqués de presse

Étude IBM : La plupart des entreprises luttent pour se défendre contre les cyber attaques sophistiquées

Près de 60% des responsables de la sécurité estiment que les attaquants ont surpassé les capacités de leur entreprise en matière de cybersécurité

Paris - 09 déc. 2014: Selon les résultats de l'étude CISO (Chief Information Security Officer) publiée aujourd'hui par IBM (NYSE : IBM), plus de 80% des responsables de la sécurité des systèmes d'information pensent que le défi que représentent les menaces externes est en hausse, tandis que 60% sont déjà d'accord pour dire que leurs entreprises ne sont pas suffisamment armées pour faire face à la cyber-guerre. L'étude révèle que la technologie est perçue comme un élément essentiel pour lutter contre les problèmes et menaces liés à la sécurité. Et dans ce contexte, le Big Data, le cloud et les terminaux mobiles apparaissent comme des domaines prioritaires.

ette 3ème édition annuelle de l'étude sur les responsables de la sécurité des systèmes d'information (RSSI) a été menée par l'IBM Center for Applied Insights. Elle est basée sur les réponses issues de 138 entretiens approfondis avec les plus hauts responsables de la sécurité informatique des entreprises. Les menaces externes sophistiquées ont été identifiées par 40% des responsables de la sécurité comme leur défi prioritaire suivi de loin par les réglementations à venir, pour un peu moins de 15% d'entre eux. Alors que les chefs d'entreprise continuent à définir leurs priorités business, les menaces externes nécessiteront les efforts organisationnels les plus importants dans les 3 à 5 ans à venir – autant que les règlementations, les nouvelles technologies et les menaces internes combinées.

« Les RSSI ont désormais leur place au comité de direction », explique Brendan Hannigan, Directeur Général, IBM Security. «Ils doivent utiliser leur influence croissante au sein de l'entreprise pour obtenir de meilleurs résultats : donner la priorité à la protection des actifs critiques, se concentrer sur les investissements en matière de renseignements de sécurité et recruter les meilleurs talents pour accroître les efforts internes.»

Aujourd'hui, les entreprises repensent leurs tactiques de cybersécurité

L'étude visait à découvrir et à comprendre comment les entreprises se protègent actuellement contre les cyberattaques. Elle révèle que 70% des responsables de la sécurité pensent avoir des technologies traditionnelles matures, qui mettent l'accent sur la prévention des intrusions réseau, la détection avancée des logiciels malveillants et l'analyse de la vulnérabilité du réseau.

Cependant, près de 50% reconnaissent que le déploiement de nouvelles technologies de sécurité est prioritaire pour leur entreprise. Ils ont identifié trois principaux domaines nécessitant un changement drastique : la prévention des fuites de données, la sécurité du Cloud et la sécurité des appareils et des mobiles.

Voici d'autres conclusions de l'étude IBM CISO:

• La sécurité du Cloud reste en tête de l’ordre du jour : bien que la préoccupation liée à la sécurité du Cloud reste forte, près de 90% des personnes interrogées ont adopté le Cloud ou sont actuellement en train de mettre en place des initiatives en la matière. Dans ce groupe, 75% des responsables s’attendent à voir leur budget dédié à la sécurité du Cloud augmenter, voire de manière significative dans les 3 à 5 ans à venir.

• La sécurité intelligente basée sur l’analyse des données est prioritaire : plus de 70% des responsables de la sécurité déclarent que les renseignements de sécurité en temps réel sont de plus en plus importants pour leur entreprise. Malgré cette constatation, l'étude révèle que des domaines tels que la classification et la découverte des données ainsi que l’analyse des renseignements de sécurité sont relativement peu matures (54%) et ont fortement besoin d’être améliorés ou transformés.

• Les besoins dans la sécurité mobile restent importants : malgré une main-d'œuvre de plus en plus mobile, seulement 45% des responsables de la sécurité déclarent qu'ils ont une approche efficace de la gestion des terminaux mobiles. En fait, selon l'étude, lorsque l’on adresse le sujet de la maturité, la sécurité des mobiles et des appareils arrive en fin de liste (51%).

Gestion de l'incertitude autour du paysage gouvernemental

En plus des menaces externes, l'étude indique que les responsables de la sécurité informatiques font face à des défis supplémentaires posés par les gouvernements. Près de 80% des personnes interrogées disent que le risque potentiel lié aux réglementations et aux normes a augmenté ces trois dernières années. Les responsables de la sécurité sont de plus en plus incertains quant à savoir si les gouvernements vont gérer la gouvernance de la sécurité à un niveau national ou mondial et à quel point ils seront transparents sur ce sujet. Seuls 22% pensent qu'une approche globale de la lutte contre la cybercriminalité sera convenue dans les trois à cinq ans.

Donner plus de pouvoir aux responsables de la sécurité d'aujourd'hui

Ces trois dernières années, avec des cyber-attaques et des règlementations gouvernementales qui continuent à évoluer, la majorité des organisations ont changé leur regard sur la sécurité, accordant un rôle plus important aux RSSI. Selon l'étude, 90% de ces responsables reconnaissent avoir une influence notable dans leur entreprise. 76% d’entre eux indiquent que leur degré d'influence a considérablement augmenté ces trois dernières années. De plus, 71% considèrent qu'ils reçoivent le soutien organisationnel dont ils ont besoin pour faire leur travail.

À propos de l’étude

Pour comprendre les conditions actuelles des responsables de sécurité ainsi que leur vision du paysage futur, l’IBM Center for Applied Insights, en collaboration avec IBM Security, a conduit près de 138 entretiens approfondis avec des hauts responsables IT et des responsables de la sécurité informatique dans l’entreprise. Certains sont des Responsables de la Sécurité des Systèmes d’Information (RSSI) mais en raison de la diversité des structures organisationnelles, ce n’est pas le cas de tous. D’autres personnes interrogées sont des Directeurs des systèmes d’information, des vice-présidents de la sécurité informatique et des directeurs de la sécurité. 63% des entreprises interviewées avaient nommé un RSSI. Les entreprises font partie d’un large éventail de secteurs d’activités et sont issues de 5 pays différents.
Pour télécharger l’étude : www.ibm.com/security/ciso .

Pour plus d'informations : http://www.ibm.com/ibmcai, suivez @IBMCAI sur Twitter ou visitez le blog <http://ibmcai.com/> IBM Center for Applied Insights.

A propos d’IBM Security
Les offres de sécurité IBM apportent la sécurité intelligente pour aider les organisations à protéger les personnes, les données, les applications et les infrastructures. Les solutions IBM couvrent la gestion des identités et des accès, le SIEM (Security Information and Event Management), la sécurité des données, la sécurité des applications, la gestion du risque, la gestion des terminaux, la nouvelle génération de protection contre les intrusions, la lutte contre la fraude financière avec le rachat de Trusteer et d’autres sujets. IBM dispose d’une des plus importantes organisations de recherche et développement et de mise en œuvre dans le domaine de la sécurité. IBM gère 15 milliards d’événements de sécurité par jour dans plus de 130 pays et possède plus de 3 000 brevets.

Pour plus d'informations :
http://ibm.com/fr/security
@IBMSecurity sur Twitter
IBM Security Intelligence blog <http://securityintelligence.com/>