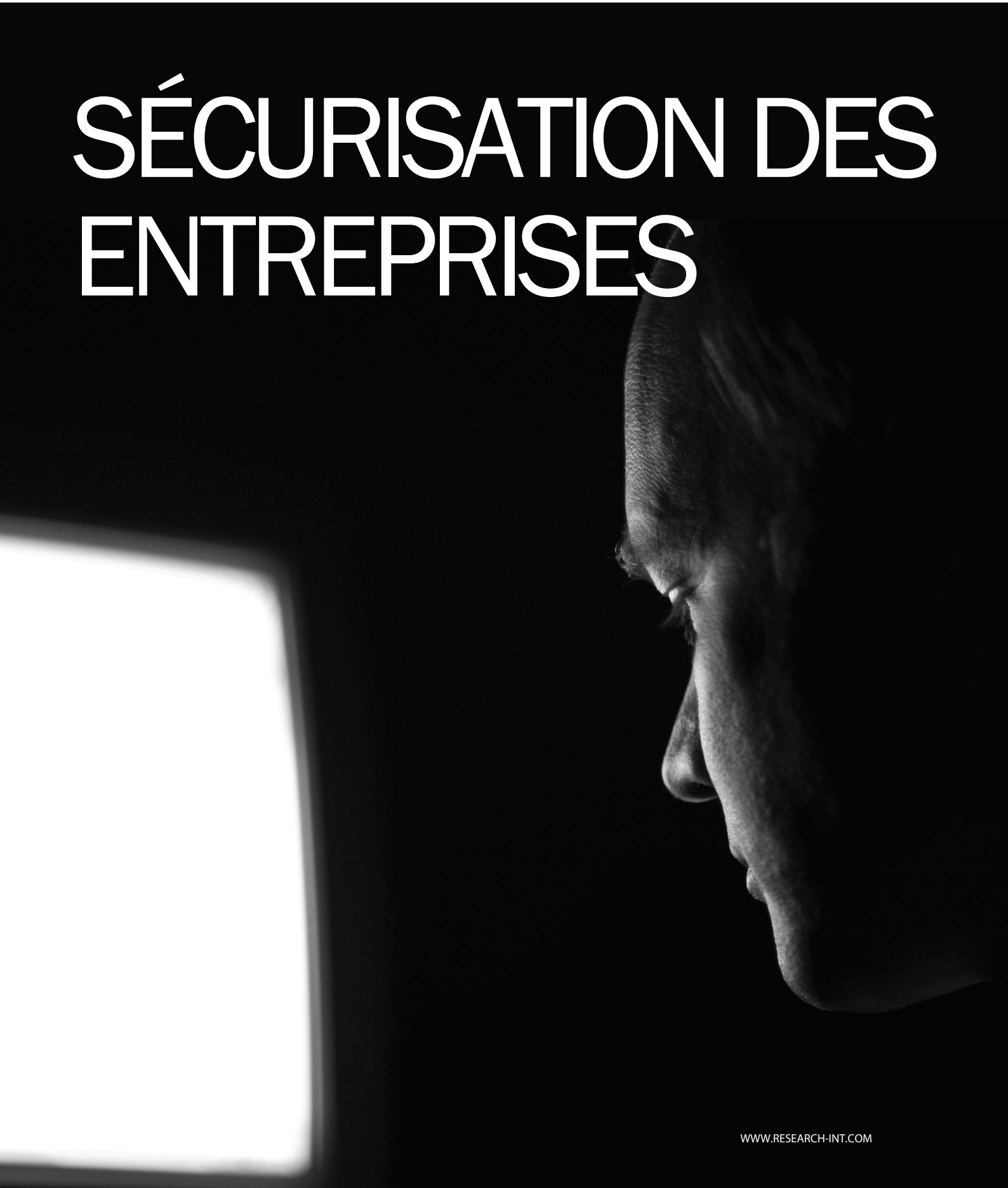
RESEARCH INTERNATIONAL

SÉCURISATION DES ENTREPRISES



WWW.RESEARCH-INT.COM

RESEARCH INTERNATIONAL

SÉCURISATION DES ENTREPRISES

LES ARTICLES ET ANECDOTES QUI, dans les médias spécialisés, relatent des incidents liés à la sécurité informatique atteignent malheureusement des niveaux record. Ordinateurs portables égarés ou dérobés, clés USB et CD disparus, tout cela fait trop souvent les gros titres. Les actes de piratage, de phishing ou de diffusion de virus par e-mail peuvent causer des ravages sur le réseau et dans les technologies d'information et de communication d'une entreprise.

Les recherches récentes ne font que corroborer ces faits rapportés dans les médias. Au Royaume-Uni, l'enquête sur les failles de sécurité des informations (2008), réalisée à l'initiative du BERR (Business, Enterprise & Regulatory Reform), a conclu que 45 % des petites entreprises interrogées (jusqu'à 50 employés), soit près de la moitié d'entre elles, avaient essuyé un incident de sécurité au cours des 12 derniers mois. Une moyenne de six incidents par an était constatée et les pires incidents coûtaient généralement entre 12 000 et 25 000 euros.

Les professionnels de l'informatique en entreprise sont très inquiets, à juste titre, en ce qui concerne la sécurité. Lors d'un sondage, réalisé en 2008 par l'association CompTIA (Computing Technology Industry Association) , près d'un tiers des personnes interrogées ont déclaré que la sécurisation de leur réseau et de leurs données était leur préoccupation principale. D'autres recherches récentes soulignent les manquements en matière de protection des données et de sécurisation des opérations distantes, mobiles et collaboratives.

Toutefois, l'enquête mandatée par Cisco auprès des petites et moyennes entreprises au Royaume-Uni, en France, aux Pays-Bas et en Espagne, réalisée par Research International en 2008 , révèle des attitudes contradictoires lorsqu'il s'agit de sécuriser l'entreprise.

Lorsque les décisionnaires informatiques ont été invités à identifier les principaux avantages de la technologie pour leur entreprise, ceux-ci ont placé la sécurité accrue et la confidentialité renforcée tout en bas du classement, loin derrière d'autres avantages tels que l'amélioration de l'efficacité, la productivité et les communications, ou encore le gain d'argent et de temps. Le grand public s'inquiète pour la sécurité, ou plutôt son absence. Pourtant, une sécurité accrue et le renforcement de la confidentialité ne sont pas perçus comme des avantages clés. Pourquoi ?

De nombreux décisionnaires sont essentiellement préoccupés par leur chiffre d'affaires : productivité, revenus et profits. Peut-être envisagent-ils la sécurité comme rien de plus qu'un coût fixe, lourd à supporter. Lorsqu'il s'agit d'investir dans des solutions informatiques, la principale motivation est l'optimisation du fonctionnement des entreprises. En revanche, la « sécurisation de l'entreprise » est considérée, au mieux, comme un facteur d'hygiène et au pire, comme un tracas.

Les données recueillies par Research International corroborent ces faits. Bien que la sécurité soit classée en dernier dans la liste des avantages, 83 % des PME interrogées ont aujourd'hui recours à des solutions de sécurité réseau et 95 % des décisionnaires considèrent la sécurité comme importante lorsqu'il s'agit d'investir dans des technologies de communications de pointe. En d'autres mots, c'est un sujet important et, bien sûr, nous sécurisons notre entreprise, mais cela ne présente pas beaucoup d'avantages pour nous.

Il semblerait ainsi que la sécurité informatique s'apparente à d'autres coûts de l'entreprise, comme les assurances : c'est de l'argent qui quitte l'entreprise mais dont on ne voit pas les résultats. Elle est considérée comme un mal nécessaire, une action défensive qui empêche la perte plutôt que d'apporter des avantages. À l'instar de l'assurance, le coût de sécurisation d'une entreprise par des solutions informatiques est mis en balance avec le risque d'une protection inadéquate ou insuffisante. Et le risque peut être littéralement immense.

Cependant, la « sécurisation des entreprises » devrait être considérée de façon plus positive et ce pour un certain nombre de raisons.

RESEARCH INTERNATIONAL

Une sécurité inadaptée annule les avantages de la technologie
Toute intervention suite à une faille de sécurité monopolise des ressources qui, à l'origine, étaient affectées à d'autres tâches. Une faille de sécurité grave peut compromettre le dialogue permanent entre l'entreprise, ses clients et les autres parties prenantes. Les outils de « chat » avec les consommateurs et les blogs en ligne pouvant attirer l'attention des médias, des programmes de gestion de crise peuvent s'avérer nécessaires. En bref, une faille de sécurité, c'est l'assurance d'une productivité réduite, de communications amputées et d'une perte de temps et d'argent. Lorsque ces failles peuvent se produire jusqu'à 6 fois par an, la sécurité devient un véritable investissement dans les autres avantages offerts par la technologie !

Une entreprise sécurisée préserve votre réputation
Les entreprises sont le reflet de leur réputation : nous vivons dans une ère numérique où la réputation se forge ou se détruit à la vitesse de la lumière, grâce aux chats et aux buzz Internet. Quels sont les coûts pour votre entreprise, et donc pour votre réputation, d'un incident de sécurité informatique inopiné ? Dans le processus de décision des clients potentiels, la sécurité de vos informations personnelles (et les garanties utilisées) peuvent devenir aussi importantes que les politiques sociales de votre entreprise.

Une sécurité garantie peut devenir un argument de vente
Les entreprises doivent se focaliser sur la sécurité pour se défendre contre les menaces informatiques électroniques ou humaines, mais également pour rassurer leurs clients : elles doivent leur garantir que leurs données, leur argent ou leur propriété intellectuelle sont entre de bonnes mains, que ce soit à l'intérieur ou à l'extérieur du réseau de votre entreprise.

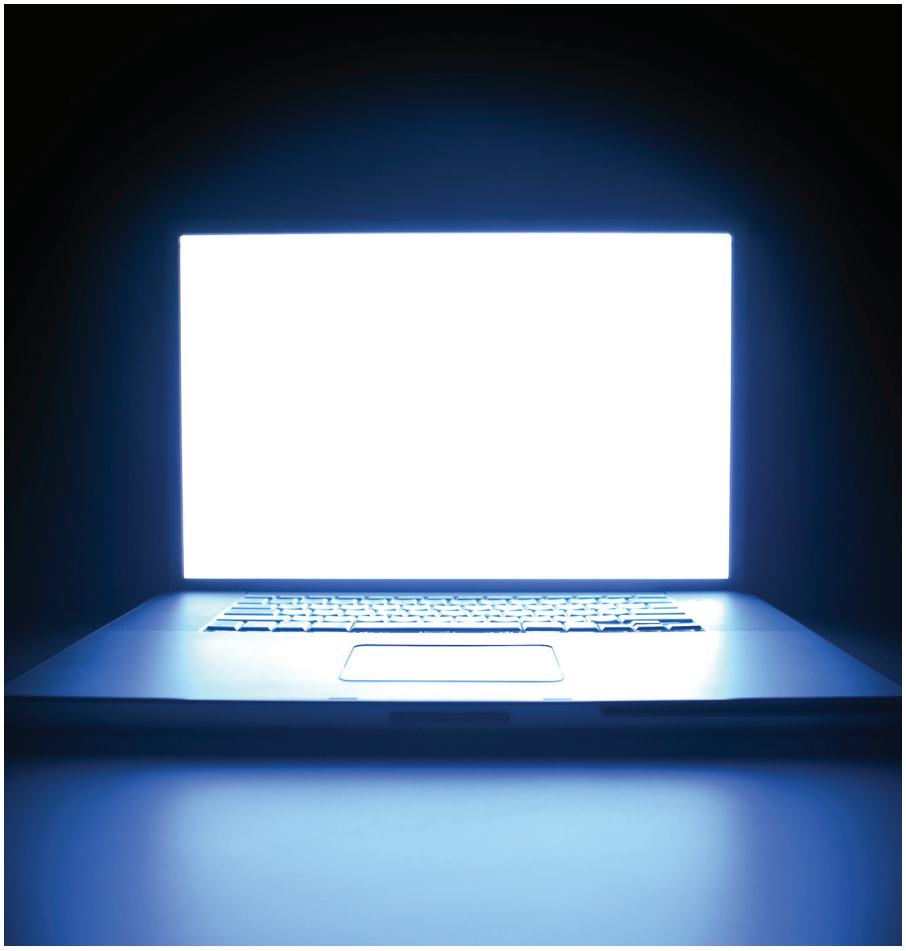
Résumé
Est-ce cela vaut la peine de vous équiper d'une infrastructure de sécurité adéquate, et pouvez-vous réellement vous permettre de ne pas le faire ? Un réseau robuste et sécurisé ne doit pas être considéré comme une simple action défensive ou comme un coût supplémentaire, mais comme un investissement économique judicieux pour la réussite de votre entreprise. Il est désormais temps de faire évoluer les mentalités. Les entreprises progressistes considèrent leur personnel comme une ressource dans leur bilan financier, et non comme un coût : pourquoi un système informatique fiable et sécurisé ne serait-il pas traité de la même façon ? Partez du principe que la « sécurité » est un état d'esprit positif à inculquer aux employés, de même que la mise en place des logiciels et du matériel adéquats.

Une sécurité proactive permet de bénéficier des autres avantages de la technologie.
Alors, que faire pour faciliter la communication, et le commerce, en toute confiance ? Réalisez un audit de votre réseau et de vos équipements actuels. Comment réagiraient-ils face à diverses menaces électroniques ou humaines (internes et externes) ? L'élaboration d'un DRP (*Disaster Recovery Plan*, plan anti-sinistre) informatique vous ouvrira les yeux et l'esprit à différents scénarios réalistes. Il vous montrera également comment réagir si ces scénarios devenaient une réalité.

Si votre audit ou votre planification de scénarios révèle certains manquements, que faire ? Qu'il s'agisse d'un problème de réseau, d'aspects techniques ou d'une non-conformité aux législations gouvernementales, contactez votre partenaire Cisco pour obtenir de l'aide. Les produits et services proposés par Cisco, associés à un DRP complet, vous permettront de vous concentrer sur votre entreprise plutôt que sur vos craintes.

Ne vous contentez pas de nous croire sur parole. En matière de sécurité, Cisco est un partenaire incontournable. Selon Research International, 100 % des clients qui ont fait appel à Cisco pour la sécurité de leur réseau ont été satisfaits (dont 70 % « très » ou « extrêmement satisfaits ») des technologies mises en œuvre dans leur entreprise.

Pour plus d'informations sur la sécurisation de votre entreprise, consultez le site



[1] Enquête 2008 sur les failles de sécurité au niveau des informations, BERR (*Business Enterprise and Regulatory Reform*), première publication en avril 2008. Enquête réalisée par PriceWaterhouseCoopers entre octobre 2007 et janvier 2008 sur un total de 1 007 réponses.
[2] Enquête de la CompTIA (*Computing Industry Association*) réalisée entre juin et août 2008 auprès de 934 personnes
[3] Enquête de Research International réalisée en 2007 et 2008 auprès des PME clientes de Cisco et d'autres entreprises externes au Royaume-Uni, en France, aux Pays-Bas et en Espagne. 607 entreprises ont répondu.

Independent research commissioned by:

CISCO