Cyberattaques : Les DSI doivent identifier les actifs les plus exposés

Technologies, médias, télécoms, e-commerce, assurance, industrie et retail sont des secteurs particulièrement ciblés par les cyberattaques. Pour mieux gérer le risque, les DSI ont tout intérêt à identifier les actifs les plus exposés, observe le cabinet **Deloitte**. Celui-ci propose dans son étude « Global Cyber Executive Briefing » un panorama des menaces par secteur.

« Le risque zéro n'existe pas. Les entreprises doivent accroître leur cyberdéfense en comprenant et en anticipant les menaces pour préparer une réponse appropriée », commente **Marc Ayadi**, associé risques et services IT Advisory chez Deloitte France.

Du vol de données aux menaces avancées persistantes

Tous secteurs confondus, les attaques par applications web, l'espionnage à grande échelle et l'intrusion des points de vente ont été les incidents IT les plus fréquents l'an dernier, d'après le rapport sur les violations de données produit par l'opérateur américain Verizon (DBIR 2014). Outre la perte ou le vol de données, le détournement de cartes de paiement ou encore les attaques par déni de service (DoS) constituent d'autres menaces. À chaque secteur son lot de joyeusetés…

Le **secteur high-tech** est, selon le cabinet Deloitte, le plus menacé par **la perte ou le vol d'actifs propriété intellectuelle** par des États, des concurrents ou des initiés. Les **médias en ligne** sont davantage sujets aux **attaques web et en déni de services**. Le risque d'exfiltration de données par des particuliers et des réseaux organisés est élevé.

Les **télécoms** font face à la recrudescence d'attaques complexes, aux **menaces avancées persistantes** (**APT** – Advanced Persistent Threat). Après infiltration, des pirates, qui recherchent des données sensibles, peuvent établir une surveillance sur le long terme. Applications et infrastructures peuvent être ciblées par de puissantes organisations, agences gouvernementales en tête. Le **commerce électronique** est plus touché par l'attaque de ses **bases de données** clients. Ses **systèmes et terminaux de paiement** sont également vulnérables. Les **compagnies d'assurance**, de leur côté, font aussi l'objet d'attaques sophistiquées combinant **logiciels malveillants** (*malwares*) et **escroquerie** (ingénierie sociale).

Quant à l'**industrie**, elle est le plus souvent victime de **cyberespionnage**. Le **phishing** et le vol de données par malwares constituent d'autres menaces sérieuses pour le secteur. Enfin, dans le domaine du **retail**, le détournement de **cartes et données de paiement** devient la nouvelle monnaie d'échange pour les cybercriminels. « *Aucun secteur n'est à l'abri,* observe Marc Ayadi. *Les dirigeants se doivent donc de mieux comprendre les menaces et d'identifier les actifs les plus exposés — généralement ceux constituant leur cœur de métier* ».

crédit photo © Duc Dao – shutterstock

Lire aussi

Deloitte IT Advisory ouvre un labo data et sécurité en France

IBM recense les cyberattaques à haut risque pour 2014