7 façons de lutter contre les menaces avancées

1 Sensibiliser et responsabiliser à toutes les échelles de l'entreprise

Le premier enjeu de la protection des SI réside dans la sensibilisation et la responsabilisation des salariés aux différentes attaques informatiques. Il s'agit d'une problématique tant stratégique qu'administrative : stratégique car les décideurs doivent avoir conscience de l'environnement des menaces numériques afin d'impulser des choix vers davantage de sécurité, administrative car la politique de sécurité des entreprises n'obtient parfois pas la couverture et la médiatisation requise.

Ainsi, la protection du SI face à la multiplicité des menaces passe d'abord par l'instauration d'un système de « bonnes pratiques » à tous les échelons de l'entreprise et la mise en place de chartes informatiques s'adressant à tous les utilisateurs : mise à jour régulière des logiciels, meilleur choix de mots de passe, sécurisation des connexions wifi pour se protéger des malwares, etc.

> ***Si 75% des entreprises disposent de politiques de sécurité, 40% des salariés de ces mêmes entreprises n'en ont pas conscience***[1]

2 Evaluer correctement l'état de sécurité de son SI

L'évaluation de l'état de sécurité de son système d'information est un prérequis à la gestion et l'anticipation des menaces informatiques avancées. La méthode DICP est un moyen efficace pour analyser l'état de sécurité de différentes parties d'un système d'information : Disponibilité, Intégrité, Confidentialité et Preuve. Mais cela requiert en amont de faire des tests d'intrusion (blackbox, greybox), réalisés par des auditeurs de sécurité.

Ces tests ont pour objectif de détecter les failles possibles de son système d'information, ses points de vulnérabilité avant l'attaque : il s'agit ainsi d'une logique proactive d'anticipation des risques plutôt que de réaction.

« D'après le Ponemon Institute, 67% des entreprises admettent que leurs activités de sécurité actuelles sont insuffisantes pour bloquer une attaque ciblée[2] »

3 Suivre les plans de sécurité établis

La gestion des risques et menaces avancées est avant tout une question de méthode : ENISA a mis au point un inventaire des protocoles de SSI, au sein duquel se démarque notamment la MEHARI (Méthode Harmonisée d'Analyse de Risques). Tracée par la norme ISO 27005, la MEHARI repose sur trois éléments fondamentaux : la phase préparatoire qui segmente et identifie les risques potentiels sur le système d'information, la phase d'analyse des risques qui met en place des scenario de risques pour dégager, en fonction de la probabilité de réalisation de ces risques, les besoins en matière de sécurité et la phase de planification du traitement des risques.

D'autres méthodes, comme l'expression des besoins et identification des objets de sécurité (EBIOS), constituent une base intéressante pour sensibiliser les décideurs sur la gestion des risques informatiques.

> ***Développée par l'ANSSI (Agence Nationale de sécurité des systèmes d'information), la méthode EBIOS est un excellent moyen de sensibiliser les décideurs à la gestion des risques informatiques***

4 L'infogérance, une bonne idée ?

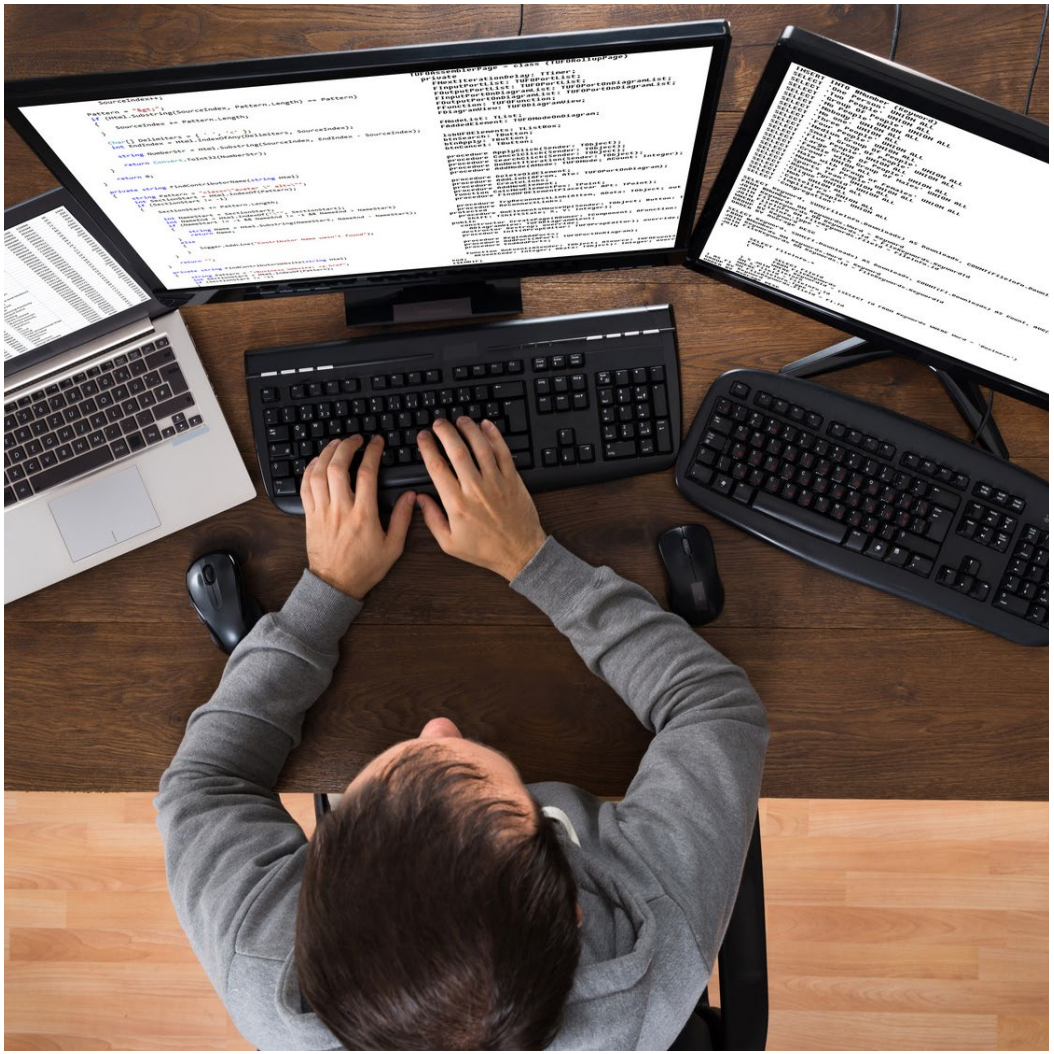
L'infogérance, ou l'externalisation des systèmes d'information (qu'il s'agisse de l'utilisation de tierce maintenance applicative, de SAAS ou de MCO) peut se révéler un moyen pertinent de gestion des menaces avancées, à condition de faire l'objet d'une réflexion ou d'un audit préalablement à sa mise en place. 40% des entreprises qui mettent en place l'infogérance n'y font jamais appel, ce qui confirme l'importance d'une réflexion préalable.

Enfin, le recours à une société de sécurité pour externaliser son SI doit se faire en fonction d'une évaluation des différents risques associés : les risques liés à la localisation des données ou aux techniques des prestataires de service.

44% des entreprises françaises ont placé leur SSI en infogérance en 2016[3]

40% des entreprises qui mettent en place l'infogérance n'y font jamais appel[4]

5 Installer un système de « défense en profondeur »



85% des menaces cybernétiques pourraient être anticipées ou prévenues, à condition de mettre en place les 3 procédures suivantes :

- ***L'application whitelisting,*** qui restreint les applications pouvant être utilisées sur un système informatique donné. L'AW permet d'éviter l'intrusion de certains malwares ou virus par téléchargement.
- ***Les software patch*** (ou logiciels correctifs) rendent possible une réaction rapide contre une invasion informatique. L'installation de patch dans un laps de 48h est un correctif souvent suffisant pour gérer les attaques numériques avancées.
- ***La restriction des privilèges administrateur (et cryptographie):*** moins le nombre d'utilisateur avec un profil d'administrateur est élevé, plus il est difficile pour un virus ou un malware de s'infiltrer dans le système d'information.

> ***85% des menaces cybernétiques pourraient être anticipées ou prévenues par la mise en place de méthodes basées sur la cryptographie, le whitelisting ou les softwares patch[5]***

6 Recourir à des systèmes de défense en plusieurs couches

Emprunté au vocabulaire militaire, le système de défense en profondeur consiste à multiplier les couches de protection pour s'assurer que l'attaque d'un malware ou toute autre menace avancée ne compromette pas l'entièreté du système d'information.

Il s'agit ainsi de créer des lignes de défense indépendantes (pour éviter qu'une attaque ciblée n'entraine la chute de tout le système): au pare-feu classique doit donc s'ajouter le pare-feu applicatif, des services de gestion des menaces par mail ou par spam, un IPS (Intrusion Prevention System) qui cible les attaques cybernétiques par signature, ou encore des outils de récupération et de prévention de la perte de données (DLP).

« Pare-feu classique, pare-feu applicatif, des services de gestion des menaces par mail ou par spam, IPS… La multiplication des couches de protection réduit mécaniquement le risque d'attaques. »

7 Installer un système de défense intégré

Quelle que soit l'efficacité du système de défense en plusieurs couches, la nature ciblée des menaces avancées (attaques sans signature, logiciels malveillants non répertoriés) amène à repenser l'approche de la SSI. La vulnérabilité aux menaces non répertoriées (zero-day threats) a augmenté de 125% entre 2014 et 2015.

La sécurité du système d'information face à ces nouvelles menaces passe par l'instauration d'un système de défense intégré se servant des potentialités ouvertes par le Big Data : voir plus, voir mieux et anticiper plus efficacement. La mise en place de SIEM (Security incident and event management) ne suffit pas. Il faut intégrer les attaques dans un contexte et un environnement : l'ère des antivirus s'achève.

> ***La vulnérabilité aux menaces non répertoriées (zero-day threats) a augmenté de 125% entre 2014 et 2015[6]***

Sources

1/ Australian Government Information security Manual, Department Of Defense – Strategic Policy and Intelligence, 2016

2/ Cost of Data Breach Study, Ponemon Institute, 2016

3/ Menaces informatiques et pratiques de sécurité, Rapport Clusif, 2016

4/ Maîtriser les risques de l'infogéance, Agence Nationale de Sécurité des Systèmes d'information, décembre 2010

5/ Top four mitigation strategies to protect your ICT System, Australian Government, Department Of Defense, 2012

6/ Internet Security Threat Report, Symantec, 2016

Guides comparatifs

A propos de Guides comparatifs

Né du partenariat avec des consultants IT et professionnels du secteur de l'informatique et des NTIC, ITfacto.com a pour vocation de fédérer l'expertise de l'industrie IT et de la mettre gratuitement à disposition des chefs de projets et responsablesinformatiques des moyennes et grandes entreprises françaises.