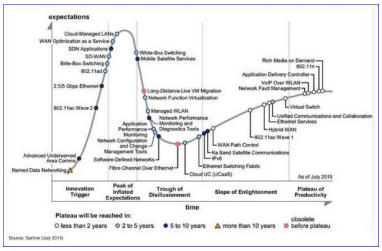
# 2 à 3 ans nécessaires pour contrer les cyber-attaques | Le Net Expert Informatique




## 2 à 3 ans nécessaires pour contrer les cyber-attaques

**La prévention des attaques sur les réseaux, jusqu'au cœur des entreprises, doit-elle redevenir une priorité dans les investissements ? Selon une récente étude du cabinet Gartner (*), seulement 40% des grandes organisations disposeront, en 2018, de plans de sécurité formels pour se prémunir contre les cyber-attaques particulièrement agressives. A ce jour, pratiquement aucune organisation n'aurait mis en place de dispositifs réellement efficaces.**

**Le 'Hypercycle' des tendances Networking et sécurité (Source : Gartner 07-2015)**

La série récente d'attaques sur les réseaux (dont celle visant Sony) a mis en alerte les responsables IT, les incitant à se préoccuper désormais de détecter et de riposter plutôt que de bloquer puis de traiter les cyber-attaques.

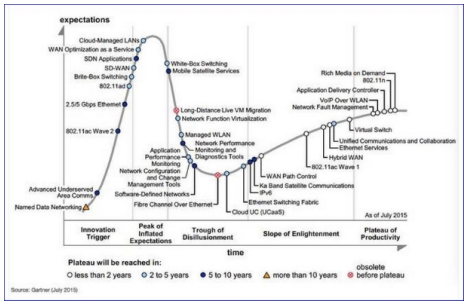
« Ce type d'attaques particulièrement virulent impose d'instituer de nouvelles priorités, de la part des 'CISO' (Chief information security officers – ou RSSI, responsables sécurité du système d'information) mais également de la part des responsables BCM (Business continuity management) », observe le rapport Gartner. De telles attaques, à ce point agressives, « peuvent causer des interruptions d'activité prolongées, capables de perturber gravement les opérations 'métier' ».

**Des attaques très ciblées**

Gartner définit ces attaques agressives comme étant des attaques ciblées de telle sorte qu'elles affectent de façon critique les opérations 'métier' internes. « Le but délibéré est de provoquer des graves dommages dans les activités de l'entreprise», explique un analyste. « Les serveurs peuvent être complètement arrêtés ou pilotés à distance, les données peuvent être effacées et la propriété intellectuelle peut être détournée via Internet par des 'hackers' malintentionnés ».

Les organisations victimes de tels assauts peuvent se retrouver sous la pression des médias en quête d'informations sur le sinistre. Et la réaction des autorités publiques ainsi que la diffusion de notes d'information rendue obligatoire vont accroître la visibilité d'une situation de chaos causée par de telles attaques.

Ces attaques peuvent exposer des informations internes critiques sur les médias sociaux, avec un enchaînement de conséquences bien plus embarrassantes que le vol de données personnelles ou la saisie de numéros de cartes bancaires. Les salariés peuvent ne plus être en mesure d'exercer normalement sur leur lieu de travail habituel, et cela, parfois pour une période de plusieurs jours voire de plusieurs mois.




**Détecter d'abord puis riposter**

Pour lutter contre ce type d'attaques, les RSSI devraient donc adopter une démarche non plus de blocage puis de détection des attaques, mais l'inverse: détecter d'abord puis répondre aux attaques.

« Éviter entièrement toute attaque dans une grande organisation complexe n'est tout simplement pas possible. C'est pourquoi, depuis quelques années, on met plus l'accent sur la détection et la riposte, car il se confirme que les nouveaux modèles d'attaque, avec des preuves d'impact évidentes, peuvent occasionner de graves sinistres », explique le rapport Gartner.

Des contrôles préventifs, à partir des pare-feu, logiciels anti-virus et solutions de gestion des vulnérabilités, ne suffisent plus comme objectif d'un plan de sécurité: « La réalité actuelle impose désormais de bien répartir les investissements entre les outils de détection et les dispositifs de riposte », constate Gartner.

**Un nouvel examen des risques**

La prolifération des terminaux mobiles connectés et l'internet des objets élargit le champ des cyber-attaques, ce qui exige plus de vigilance encore, plus de budget et un nouvel examen plus approfondi des risques. Il convient donc, en priorité, se défaire de ces dépendances technologiques, et d'annihiler sinon réduire l'impact de tels incidents techniques sur les process métier et sur le chiffre d'affaires.

Autre suggestion : les détenteurs d'informations doivent être responsabilisés sur la protection de leurs ressources ; ils doivent s'engager à prendre en considération les risques résultant des solutions 'métier'.

Avec l'arrivée des objets connectés, supposés toujours disponibles, de nouveaux incidents pourraient interrompre des transactions commerciales et à entamer la fidélité des clients.

**Construire de nouveaux cas d'usage**

L'heure est venue, estime Gartner, de construire de nouveaux cas d'usage sans oublier d'investir dans des dispositifs proactifs afin de prévenir ces nouvelles menaces.

« Il faut se projeter sur de nouvelles solutions assurant la gestion de la continuité d'activité ». Et le rapport de conclure: « La sécurité n'est pas un problème technique, traité par des spécialistes cachés quelque part dans le service informatique… Il faut dès aujourd'hui solutionner les problèmes qui peuvent arriver ».

**La sécurité prédictive**

Les grands fournisseurs du monde IT ont commencé à investir dans cette dimension prédictive de la sécurité. Ainsi, HP a fait l'acquisition de plusieurs sociétés spécialisées, comme ArcSight, Fortify, TippingPoint, Attala… Grâce aux technologies Big Data, il devient possible d'analyser en quasi temps réel les événements ou incidents qui peuvent s'amorcer, avant même qu'ils ne se propagent. C'est la phase de prévention de menaces potentielles, avant leur manifestation. Les nouveaux dispositifs sont le fruit de la synergie désormais possible entre des plateforme SIEM (Security information and event management) telles qu'ArcSight et la technologie IDOL d'Automy intégrant un moteur d'analyse Big data en temps réel. Les données de sécurité brutes peuvent être suivies en permanence et analysé à travers des modèles de comportement. Ceci permet de rendre visibles des menaces généralement perçues trop tardivement.

Depuis quelques mois, quantités d'autre solutions et services tirent parti de ces nouvelles possibilités technologiques, que le Gartner conseille d'examiner de près.

_ _ _

(*) Etude Gartner « Formal plans to address aggressive cyber-security business disruption attacks (02/2015, présentée à Londres ce 14/09/2015)

---


Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;

• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;

• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous


---

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : http://www.zdnet.fr/actualites/securite-2-a-3-ans-necessaires-pour-contrer-les-cyber-attaques-39825020.htm