Réponse sur incidents et bonnes pratiques | Le Net Expert Informatique

	Réponse sur incidents et bonnes pratiques

Les 2/3 des cyberattaques mettent plusieurs mois à être détectées et près de 70% le seraient par des tiers ! Aujourd'hui c'est un fait, plus personne n'est à l'abri d'une cyberattaque, il est donc indispensable de se mettre en ordre de marche pour être prêt à réagir en cas d'attaque. La mise en place d'une politique de réponse sur incident de sécurité permet, en effet, de détecter la cyberattaque le plus tôt possible, de réagir très rapidement pour la contrer et de réduire ainsi au maximum les impacts d'image et business. Econocom nous livre son expertise en la matière, aux côtés de Maître Garance Mathias, à l'occasion de la 15ème édition des Assises de la Sécurité.

En 2014, 81% des entreprises ont déjà fait l'objet d'une cyberattaque, constate Marc Cierpisz, Directeur de l'offre Cybersécurité chez Econocom. 66% de ces attaques ont été découvertes après plusieurs mois, et 69% d'entre elles ont été découvertes par des tiers. Il observe, de plus, une difficulté à arrêter ce type d'attaque ; une incertitude plane quant aux délais de détection et de traitement de ce type d'incident.
La réponse sur incident est à la fois un défi technique, organisationnel et juridique pour les entreprises. L'enjeu est aussi de savoir s'adapter aux circonstances particulières.
Concernant les mesures techniques, il s'avère que la sécurité périmétrique reste inadaptée ou inefficace, car le SI est aujourd'hui de plus en plus diffus. La mise en place de firewalls n'a, par exemple, pas empêché TV5 Monde de se faire pirater. Il existe une grande diversité à l'heure actuelle des moyens de réaction : audits (test d'intrusion, tableaux de bord…), détection (SIEM, SOC, CERT, veille…). Toutefois, on constate beaucoup de manquements à ce niveau-là, à la fois en termes de budgets et de ressources adéquates, même si les enjeux de sécurité sont de mieux en mieux compris.
Au niveau juridique, le droit n'a pas encore clairement défini de manière intrinsèque la notion d'incident de sécurité, contrairement aux fuites de données, explique Me Garance Mathias. L'approche devra donc passer par une définition précise des incidents de sécurité et des responsabilités avec les différents prestataires.
Un cadre réglementaire existe néanmoins, avec la Loi Informatique et Libertés notamment mais pas seulement. Le projet de règlement européen relatif à la protection des données personnelles, le règlement eIdas, ou encore les différentes réglementations sectorielles, viennent compléter et complexifier les obligations relatives à la protection de l'information et au traitement des incidents. Le projet européen concernant la protection des données à caractère personnel va venir imposer l'obligation de déclaration pour le CIL des incidents de sécurité, ce qui changera la donne surtout dans un pays où la fuite de données se fait soi-disant plus « rare » qu'ailleurs. Le bénéfice d'être assuré sera certainement demain de plus en plus prégnant.

Les réponses juridiques diffèrent sur le plan civil et pénal, et les sanctions aussi. Le risque est bien réel pour les entreprises, en termes de dommages et intérêts bien sûr, d'atteinte à l'image et à la réputation également. Les illustrations jurisprudentielles varient, quant à elles, selon le fait que l'entreprise ait effectué ou non préalablement des audits de sécurité par exemple… La question est de savoir comment démontrer s'il y a eu un défaut de sécurisation ou non. Les incidents de sécurité ont mis globalement en avant un manque de sécurisation des systèmes d'information, qu'il faudra donc renforcer si les entreprises ne veulent pas être sanctionnées.

Parmi les mesures à mettre en place en entreprise pouvant réduire ces incidents de sécurité, elle cite entre autres :
– La politique interne à l'entreprise : la charte informatique est essentielle, mais combien la font signer aux employés… pourtant celle-ci permettrait de responsabiliser les utilisateurs ; la politique de sécurité en elle-même ; la politique contractuelle avec les prestataires, les sous-traitants… ; ou encore la sensibilisation des différentes acteurs ;
– Ensuite, des mesures de sécurité spécifiques doivent venir renforcer cette politique interne selon l'activité de l'entreprise : OIV, secteur médical, assurance, banque…

La cadre juridique est donc là, mais il est aussi à venir. On connaît déjà les textes, donc on n'est pas dans l'incertitude, que ce soit dans le secteur de la santé, ou dans le domaine de la protection des données à caractère personnel, conclut-elle.

La réponse n'est pas que technique ou juridique. Plusieurs défis se posent au niveau de l'organisation en matière de réponse à incident, reprend Marc Cierpisz :
– Identifier un incident de sécurité ;
– Etablir les objectifs de toute opération d'enquête et de nettoyage ;
– Analyser les informations relatives aux incidents ;
– Déterminer ce qui s'est réellement passé ;
– Identifier les réseaux et systèmes compromis ;
– Déterminer les informations divulguées à des tiers ;
– Etc.

Quelles démarches convient-il de mettre en place ? « Le bon stratège se prépare à tout, même au pire… »
– Concernant la partie renseignement sécuritaire, il convient en premier lieu d'évaluer la criticité de l'entreprise, d'analyser la menace sécuritaire du SI, les risques IT et métiers, d'examiner les implications des personnes, des processus, de créer un cadre de contrôle approprié, d'examiner l'état de préparation dans la réponse aux incidents de sécurité…
– Au niveau de la réponse sur incident, il faut déjà identifier les incidents de sécurité, définir les objectifs que l'on veut couvrir et les mesures à prendre quand on a qualifié les incidents de sécurité, récupérer les systèmes, les données et la connectivité…
– Le suivi post-intervention est également fondamental pour remettre en état l'entreprise : il s'agit ici d'enquêter sur l'incident de manière plus approfondie, de le signaler aux parties prenantes, d'effectuer un examen a posteriori, de réagir et de prendre les bonnes décisions, de communiquer et de s'appuyer sur les leçons apprises, de mettre à jour les informations clés, les contrôles et les processus, d'effectuer une analyse de tendance… L'objectif est que ça ne se reproduise pas.

Parmi les erreurs les plus fréquentes, les entreprises sous-estiment encore trop souvent les conséquences d'une attaque et les risques : « on traitera quand ça arrivera… » Pourtant 117 339 attaques seraient recensées chaque jour. On constate globalement une mauvaise estimation des risques, la destruction des preuves, une absence de plan de réponse à incident, de gestion de crise et de prise en compte de la réponse à incident dans les PCA, ou encore une mauvaise gestion de la e-réputation et de la communication. Pourtant, quand on subit un crash c'est violent, parfois même comme un accident de voiture.

Un certain nombre de bonnes pratiques doivent être mises en place au sein des organisations, comme la définition d'un plan de réponse à incident, la constitution d'une équipe dédiée, la définition d'un corpus documentaire, la préservation des preuves… Un plan de communication doit également être mis en œuvre. Il est essentiel d'identifier une autorité centrale en charge de cette communication, avec les médias par exemple. L'entreprise doit être impliquée en la matière, car « mieux elle va maitriser sa communication, mieux elle va gérer sa sortie de crise ». Enfin, en cas de gestion de crise, elle devra mettre en place une cellule de « war room », mais aussi gérer les relations avec les différents organismes et autorités concernés (CNIL, ANSSI…).

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

Source : http://www.globalsecuritymag.fr/Reponse-sur-incident-des-enjeux,20151001,56316.html