Deloitte.

Cyber Sécurité

Faire face aux menaces

Définir sa stratégie et faire face aux menaces d'une cyber attaque

Cloud, objets connectés, transformation digitale… Pour se protéger, les organisations doivent adapter leur programme de cyber sécurité en fonction de leurs évolutions stratégiques et opérationnelles et de leur environnement externe. Il faut non seulement anticiper les risques mais surtout être capables de détecter les incidents et d'y réagir efficacement.

Définir sa stratégie et sa gouvernance

- Auditer vos acquis, évaluer le niveau de maturité de votre dispositif et votre système de management de la continuité d'activité
- Former et évaluer les compétences techniques de vos collaborateurs
- Coacher vos équipes mêlant experts et représentants des fonctions clés de l'entreprise

Détecter les attaques et menaces
Protéger ses systèmes d'information

- Détecter les vulnérabilités
- Protéger ses applications et ses outils métiers
- Mettre en place une Data Privacy et conformité aux réglementations
- Gérer les identités et les accès

Réagir et gérer les situations de crise

- Intervenir lors d'investigations et réponses aux incidents cyber
- Accompagner et coacher le RSSI
- Préparer conjointement les équipes mêlant experts et représentants des fonctions clés de l'entreprise

Axes de réflexion pour être proactif afin d'imposer une cyber sécurité adaptée à son organisation ?

- Quels sont parmi les actifs sensibles et critiques de l'entreprise, ceux qui sont portés par le SI ? (pour chaque produit, pour chaque programme, dans toutes les phases de vie du produit, de la conception au retrait de service, et en conséquence, pour chaque métier)
- Qui a intérêt à vous « attaquer », et dans quels buts ? Identification et pondération des risques.
- Quel est l'impact de valeur au regard du risque ?
- Quelles sont les vulnérabilités principales (organisationnelles, humaines, techniques, juridiques, contractuelles…) ?
- Quelles sont les priorités de protection ? (mesures techniques, organisationnelles, humaines, etc.)
- Comment les décline-t-on en projets concrets ? Avez-vous une stratégie cyber cohérente et ordonnée ?
- Quelle efficience de ces mesures de sécurité ?

Comprendre les impacts et impliquer l'ensemble des parties prenantes

La vigilance s'accroît sur tous les sujets de cyber sécurité. La mise en place des actions pour se protéger devient un enjeu majeur pour les sociétés. Les réglementations, autant françaises qu'internationales, convergent au cœur de l'actualité.

Dans le climat actuel caractérisé par l'importance du digital, le disruptif et la rapidité de l'innovation, chaque entreprise est désormais une entreprise technologique. Dans ce contexte, celle-ci se doit de redéfinir ses systèmes cœurs pour rester compétitive. Du point de vue de la cyber sécurité, cela a pour effet d'introduire de nouvelles vulnérabilités et faiblesses.

Un enjeu majeur pour l'ensemble des parties prenantes de votre entreprise

Aucune organisation ne peut prédire ou empêcher une attaque. En revanche, elle peut renforcer sa résilience face aux menaces et limiter les dommages causés par une attaque. Elle doit rester constamment en alerte et se tenir prête.

Face à l'émergence d'attaques très ciblées et d'un contexte réglementaire fort, la gestion du risque devient un enjeu majeur pour les entreprises. Il est indispensable d'identifier les niveaux d'exposition de l'ensemble des métiers pour mettre en place les actions de prévention adéquates.

L'augmentation du nombre de données personnelles générées par l'IoT accroît le risque de fuite de données

Le monde qui nous entoure est de plus en plus parsemé de capteurs connectés. L'Internet of Things (IoT) se développe à grande vitesse dans de nombreux domaines : véhicules, machines, wearables, éoliennes... Gartner prévoit 21 milliards d'objets connectés en 2020.

Collecter toujours plus de données, et de surcroît plus de données personnelles, accroît le risque de fuite de données. Les organisations devront décider ce qui peut relever de l'IoT et ce qui est trop sensible pour l'être.

Les entreprises qui étudient les opportunités d'utiliser les technologies pour promouvoir le bien doivent également considérer de potentiels impacts négatifs. De plus, les organisations sont souvent habituées à se protéger contre les menaces qui pèsent sur le cœur de leur métier, mais sont moins enclines à comprendre ce qui les menace dans le domaine de la responsabilité sociale.

C'est pourquoi elles doivent s'efforcer de mettre à jour les différents scénarios de menaces, leurs politiques de protection des données privées, ainsi que leurs politiques de gestion des risques cyber.

Le **« secure by design »** implique des spécialistes de la cyber sécurité tout au long du processus de développement. Devant la multitude d'informations à traiter, les plateformes autonomes offrent la possibilité de gérer dynamiquement les ressources qui s'intègrent et s'orchestrent dans le développement et le fonctionnement des solutions IT. Toutes les opérations IT traditionnelles sont candidates pour cette automatisation. La configuration autonome est le fait de provisionner et déployer de manière autonome non seulement les ressources du data center, serveur, réseau et stockage mais également la configuration des applications, des données, des plateformes, des profils utilisateurs, de la sécurité. Les équipes IT sont ensuite immédiatement productives. L'optimisation autonome s'attache à réallouer dynamiquement les ressources et charges entre les environnements. La surveillance autonome maintient les environnements en bonnes conditions et permet d'anticiper les problèmes et d'empêcher les erreurs, les incidents et les coupures.

Notre expertise

Nous vous accompagnons sur tout le processus de lutte contre les cyberattaques, en élaborant avec vous un programme de sécurité efficace.

Continuité d'activité

Connaître les risques cyber au sein de son organisation pour mieux les maîtriser.
Procéder à des exercices de simulation de cyberattaques pour pouvoir mieux y faire face.
Mise en place d'un plan de continuité d'activité capable de répondre à l'ensemble des enjeux métiers et IT de l'organisation.

IAM

Gestion des identités et des accès
Appliquer de bout en bout une approche centrée sur les activités qui garantit et rationalise la gestion des identités dans une optique d'économie de coûts, de productivité et de réduction des risques.

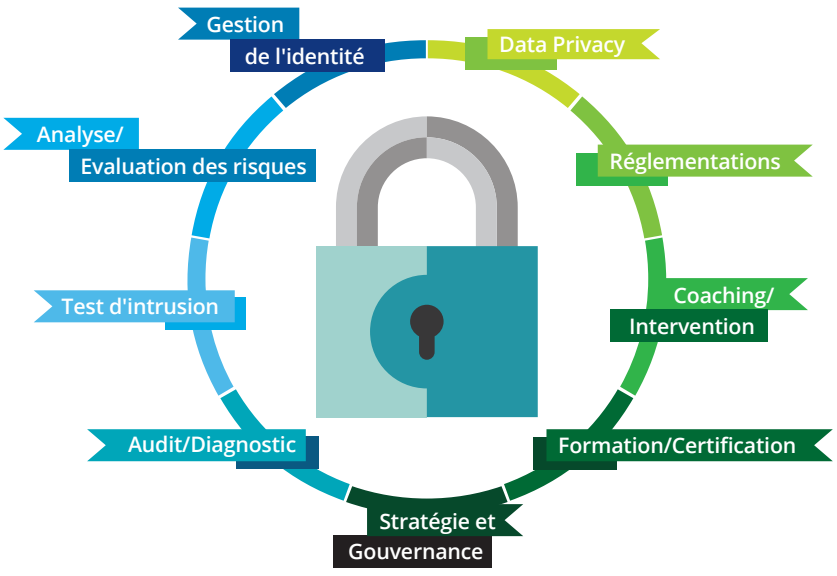
Diagnostic

Identifier son exposition aux risques de cyberattaques
Une analyse régulière des cyberattaques donne un diagnostic objectif sur les défaillances potentielles du contrôle interne. Ces tests d'intrusion s'effectuent de façon adaptée, en fonction de cadres de référence.

Formation

En 2014, Deloitte s'est rapproché de la société Hervé Schauer Consultants (HSC), société pionnière de la sécurité informatique en France, qui a permis de renforcer ses effectifs et son savoir-faire en sécurité des systèmes d'information.

Ce rapprochement avec la société HSC nous permet de nous positionner en leader français de la formation en SSI avec le plus large programme du marché (43 formations différentes proposées).



Stratégie et gouvernance

Etablir des procédures adéquates pour garantir un programme solide de lutte contre les cyberattaques
Nous vous assistons dans l'élaboration de procédures sur l'ensemble de la mise en place du dispositif de cyber sécurité : de la mise en place de la politique de contrôle (coaching des RSSI, préparation conjointe des équipes mêlant experts et représentants des fonctions clés de l'entreprise...) à la réalisation de procédures spécifiques (dispositif d'alerte interne, politiques et procédures en matière de protection des données personnelles...).

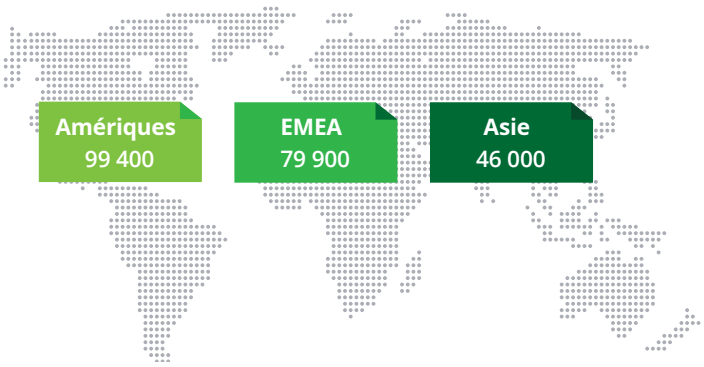
Tests d'intrusion

En s'appuyant sur des outils à la pointe de la technologie, des moyens humains et logistiques dimensionnés en fonction des besoins, les équipes du DLab assurent une réactivité optimale et un service immédiat pour diagnostiquer, superviser, analyser et sécuriser les environnements de leurs clients, qu'il s'agisse de sécurité ou de maîtrise des données.

Nous organisons des conduites de tests d'intrusion, mesure de l'exposition au risque de malveillance externe, contrôle permanent des vulnérabilités sur les infrastructures externes et internes.

Deloitte, un leader mondial à vos côtés

Plus de 225 000 collaborateurs dans plus de 150 pays



Une offre pluridisciplinaire

… au service de toutes les organisations

… dans tous les secteurs d'activité, avec notamment une organisation par secteur d'activité stratégique (Energie & Ressources, Secteur Public, Sciences de la vie & Santé…)

Un interlocuteur unique

Pour chaque client, un associé responsable est garant de :

- la qualité de service
- la remontée d'informations adaptées
- l'accès aux meilleures ressources
- la maîtrise des budgets
- la gestion des conflits d'intérêts
- la gestion de la collégialité (audit)

De plus, il a autorité sur le réseau mondial.

Deloitte est classé numéro 1 mondial des services de conseil en cyber sécurité par Gartner pour la 4e année consécutive*

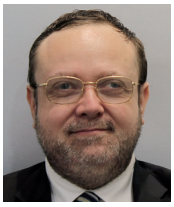
- **Une équipe d'experts :** Deloitte France compte aujourd'hui plus de **100 experts spécialisés** en audits de sécurité qui interviennent régulièrement auprès des plus grands comptes
- **Une expertise reconnue :** en matière de systèmes d'information, au travers de nombreuses missions d'audit et de conseil et par la certification de nos équipes
- **Une réelle indépendance :** vis-à-vis des constructeurs et des éditeurs contribuant à l'objectivité de nos prestations
- **Des outils optimisés :** acquis et développés par nos équipes techniques, ces derniers nous permettent d'obtenir des résultats pertinents et d'optimiser au mieux nos délais d'intervention. Les investigations humaines restent cependant une priorité pour garantir le succès et la pertinence des audits
- **DLab, un laboratoire sécurisé :** nos équipes s'appuient sur ce laboratoire, répondant aux exigences de l'ANSSI, dédié à la conduite des missions d'audit de sécurité et de tests d'intrusion. Il nous permet de garantir la sécurité et la confidentialité des informations, ainsi que la traçabilité des actions effectuées

* Source : Gartner – Gartner Market Insight - Security Consulting Services, Taxonomy Update 2.0, Jacqueline Heng, 04, March 2016

Contacts

Michael Bittan
Associé
Leader des activités
Cyber Risk Services
mbittan@deloitte.fr

Alain Robic
Associé
Cyber Risk Services
Responsable du secteur
Aerospace & Defense
arobic@deloitte.fr



Hervé Schauer
Associé
Cyber Risk Services
Directeur général HSC
hschauer@deloitte.fr

Deloitte.