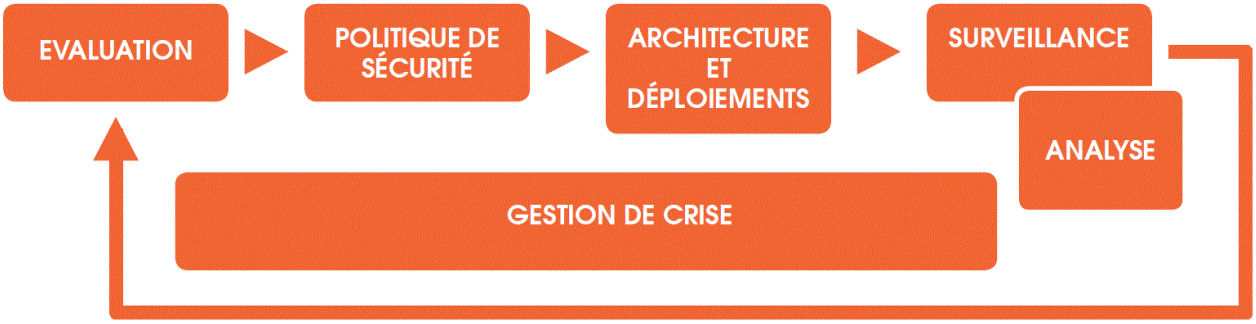
Approche systémique recommandée par SOGETI.



La démarche systémique de cybersécurité (cf. figure) s'inscrit dans une approche par les risques, qui permet d'accroître sur tous les fronts, de manière cohérente, la cybersécurité de l'entreprise. Elle résulte d'une approche de progrès bouclée comprenant, outre une bonne « hygiène informatique » :

- une évaluation de la sécurité réelle de l'entreprise, menée à l'aide d'audits organisationnels et techniques et de tests d'intrusion, permettant d'identifier les faiblesses, d'évaluer le niveau de maturité de la sécurité de l'entreprise et de définir des plans d'amélioration ;
- une analyse de risques sérieuse, une politique de sécurité, une gouvernance appropriée, une organisation solide et des collaborateurs sensibilisés ou formés ;
- une architecture informatique robuste et le déploiement d'outils de sécurité adaptés, correctement administrés et opérés ;
- une surveillance permanente du système d'information assurant le maintien en condition de sécurité et permettant de détecter au plus vite les incidents ;
- une analyse détaillée des événements intervenant dans le système afin de réagir rapidement en cas d'attaque ;
- une capacité de gestion de crise organisée et éprouvée permettant de réduire l'impact des agressions et de minimiser les dommages pour l'entreprise.

80% des attaques informatiques sont bloquées par une hygiène informatique sérieuse et de bonnes mesures de sécurité préventives. 19% des attaques sont parées à l'aide de dispositifs proactifs de surveillance et de détection des agressions. Quant au 1% des attaques restantes, les plus sophistiquées, il est impossible de s'en prémunir à coup sûr mais l'entreprise peut considérablement limiter leur impact si elle s'est dotée d'une sécurité en profondeur et s'est bien préparée à gérer la crise.

(Source : SOGETI, pleinement propriétaire des droits du texte et de l'image ci-dessus.)