G²C Club R2GS

Vers une gouvernance sécurité plus mobilisatrice pour l'ensemble de l'entreprise

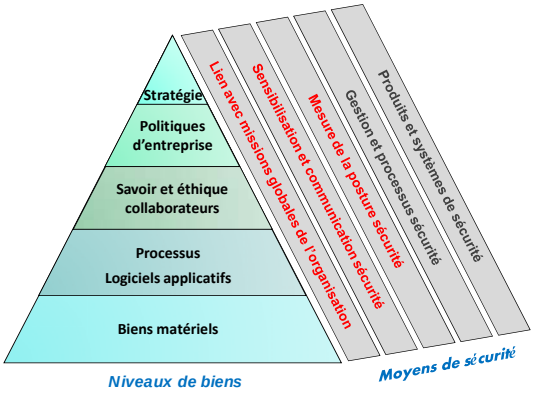
Gérard GAUDIN
(Consultant indépendant – G²C)

Le 2 décembre 2013

SOMMAIRE

1. Le rôle clé du top management dans l'existence de la SSI

Stand-by en SSI de moins en moins efficace



2. L'implication de l'ensemble des membres de l'entreprise est essentielle pour une Cyber défense efficace

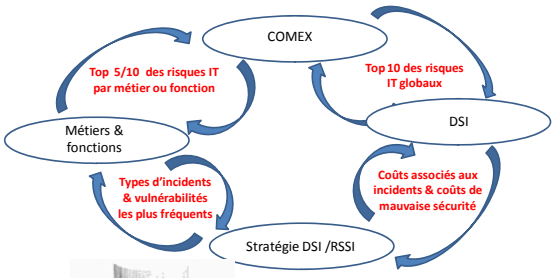
- Accroissement et évolution constante des menaces avec un *rôle clé des utilisateurs* (concernés dans *70 %* des incidents de sécurité de nature malveillante)
- La plupart des attaques sont le résultat de groupes organisés avec des objectifs précis
- L'usage croissant de ressources IT externes ou personnelles engendrent de nouveaux défis

Les processus et outils de sécurité sont ***plus efficaces quand*** :

- Mesures priorisées, liées aux risques réels et constamment supervisées
- Chaque utilisateur comprend son rôle et ses responsabilités dans le SMSI et s'engage à s'y conformer pour garantir la pérennité de l'entreprise

3. Adapter la représentation du risque IT à chaque niveau

Et impliquer le top management dans la supervision des risques



Basé sur une « intelligence de la menace » (standard ETSI ISG ISI sur les indicateurs)

4. Le besoin d'indicateurs opérationnels partagés

Le rôle de pivot essentiel d'un standard à ce sujet

- Lien précis développé entre incidents/vulnérabilités/non-conformités, et :
  - ✓ Profils de risques IT (en route vers un RoI fiable en SSI)
  - ✓ Points de repère des référentiels généraux (pour évaluer les niveaux de conformité et d'assurance des politiques, et les progrès humains)
- Prise de décision sur la base de chiffres fiables (avec possibilité de benchmarking de la posture sécurité)
- *Réconcilier 2 populations* aux intérêts souvent divergents (gouvernance/experts techniques terrain) = analyses croisées *« Threat intelligence/efficacité technique actuelle »*
- Meilleure utilisation et mise en perspective des apports des différents outils techniques et des équipes opérationnelles en SSI

5. Une potentialité essentielle pour se benchmarker

Faisabilité de la démarche prouvée par G²C sur la base d'un panel international d'entreprises dans 4 pays

	Etat de l'art (par mois)	Ecart pays	Niveau de dispersion	Degré d'imprécision (1)	Périmètre de l'indicateur	Source (s)	Périodicité
IEX_PHI.1	33 entreprises (3)	Oui (uniquement Fr & All)	100 % par rapport à l'état de l'art (entre -70 % et +50 %)	1	(2)	ENISA + chiffres complémentaires sur hypothèse (4)	Trimestriel
IEX_DOS.1	0.008 attaque DDoS	Non	30 % par rapport à l'état de l'art (entre -50 % et +50 %)	1	Par site Web	CERT Fond de 15	Annuel + affinage trimestriel
IEX MLW.4	1,5 malware installé avec succès sur des serveurs (5)	Non	20 % par rapport à l'état de l'art (entre -15 % et +65 %)	3	Par environ Honeypot 10.000 serveurs	CERT Fond de 15	Annuel + affinage trimestriel
VCF UAC.3	6 comptes non confirmés	Non	50 % par rapport à l'état de l'art (entre -50 % et +40 %)	3	Par bases de données ou par application	Fond de 15	Trimestriel

6. Apports travaux du réseau européen des Club R2GS

Travaux au sein du réseau et lien avec entités de standardisation