Institut des
Risques
Industriels,
Assuranciels et
Financiers

AUDIT DU SYSTEME D'INFORMATION DE L'ENTREPRISE OLD RHUM

Présentation des recommandations

MASTER

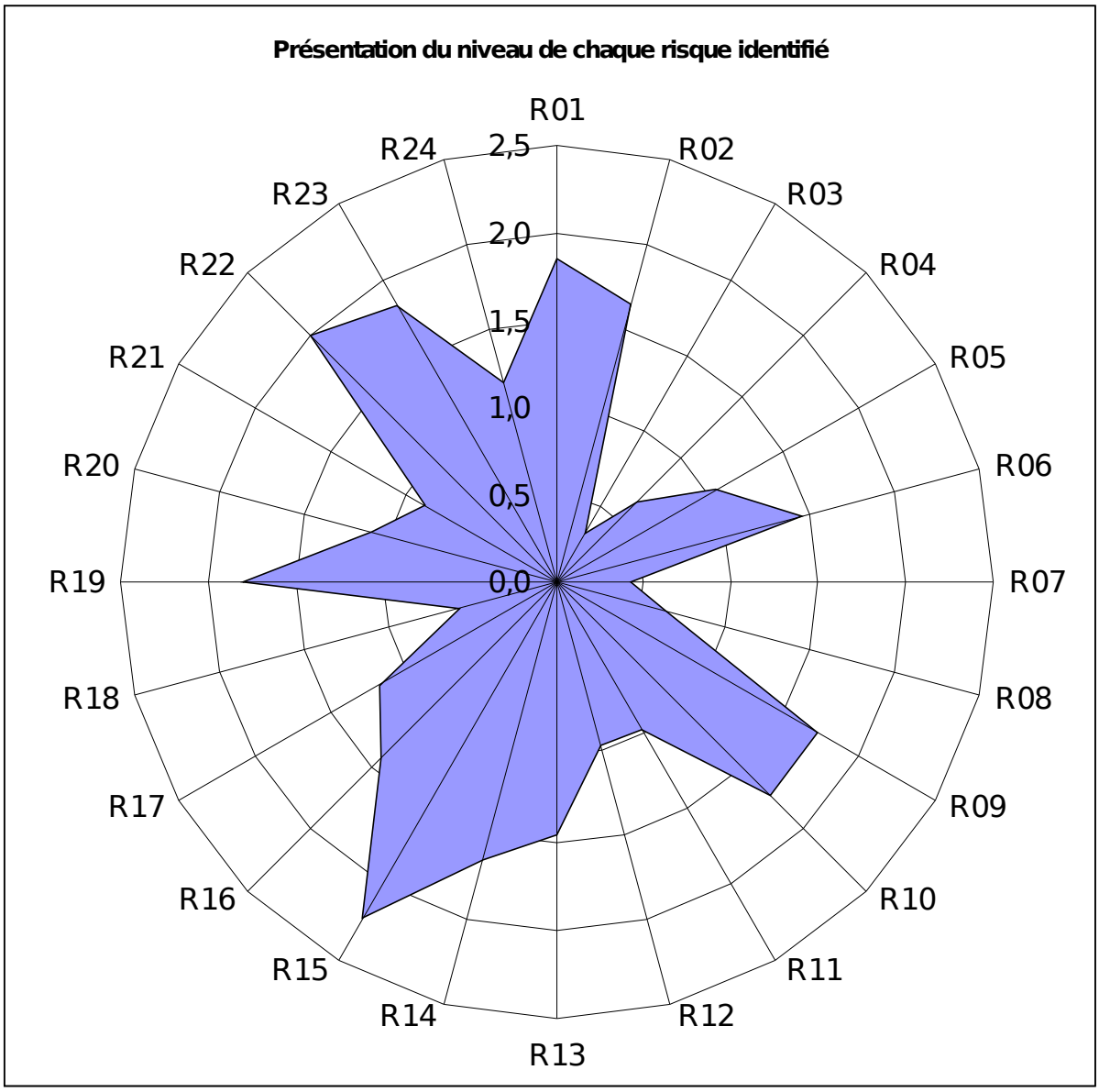
SÉCURITÉ DES SYSTÈMES D'INFORMATION

D. Bernaudeau
G. Fouquet
J. Vehent

L’audit effectué au sein de l’entreprise Old Rhum via la méthode EBIOS nous a permis de mettre en évidence un certain nombre de risques. Ces risques sont présentés dans le tableau ci-dessous :

R	Libellé
R01	Incendie non maîtrisé dans l’ensemble du bâtiment de production
R02	Dégâts des eaux dans la salle informatique - télécommunication rendant le matériel et les installations inutilisables
R03	Risque d'encrassage du matériel informatique
R04	Risque de détérioration du matériel informatique (choc électrique)
R05	Défaillance de la climatisation pouvant entraîner une surchauffe du matériel informatique
R06	Défaillance d'alimentation du matériel informatique
R07	Rupture des télécommunications
R08	Espionnage
R09	Perte de documents
R10	Disparition de matériels
R11	Divulgation interne
R12	Divulgation externe
R13	Matériel en panne
R14	Matériel défaillant
R15	Destruction du matériel informatique
R16	Opération de maintenance difficile
R17	Défaut d'intégrité dans le système de commande
R18	Installation de matériel d'espionnage
R19	Utilisation abusive des ressources informatique
R20	Introduction de virus dans le système informatique
R21	Modification du logiciel
R22	Consultation / Suppression de documents confidentiels
R23	Mise en péril du systeme (en se faisant passer pour quelqu'un d'autre)
R24	Absence/ disparition de preuves

La classification de ces risques selon les critères de disponibilité, intégrité, confidentialité, traçabilité et probabilité d’occurrence nous a permis d’obtenir la représentation suivante :



Note : si vous souhaitez plus d'informations sur la manière d'effectuer les calculs permettant l'obtention de cette classification, veuillez vous reporter au fichier excel joint.

La classification des risques détermine les risques les plus importants, et donc sur lesquels il convient d'intervenir. Ces risques sont regroupés dans le tableau suivant avec, cette fois, leurs valeurs de DICT.

Risque	Libellé	Disponibilité	Intégrité	Confidentialité	Traçabilité
R01	Incendie non maîtrisé dans l'ensemble du bâtiment de production	2	0	0	0
R06	Défaillance d'alimentation du matériel informatique	2	0	0	0
R09	Perte de documents	1	0	2	2

R10	Disparition de matériels	2	0	3	2
R13	Matériel en panne	2	0	0	0
R14	Matériel défaillant	1	1	0	0
R15	Destruction du matériel informatique	3	0	0	2
R16	Opération de maintenance difficile	1	0	0	0
R19	Utilisation abusive des ressources informatique	0	0	0	0
R22	Consultation / Suppression de documents confidentiels	0	3	3	2
R23	Mise en péril du systeme (en se faisant passer pour quelqu'un d'autre)	3	3	0	3
	SOMMES :	**17**	**7**	**8**	**11**

En faisant la somme de chaque critère, on détermine son importance pour l'ensemble de la sécurité du système. Dans le cas présent, le critère de disponibilité est extrêmement critique, c'est donc sur celui-ci que les premières actions devront être portée.
Vient ensuite le critère de la traçabilité puis les critères de confidentialité et d'intégrité. Sur ces deux derniers, la hiérarchisation des actions n'est pas très importante. Tant que les critères de disponibilité et de traçabilité sont réduit rapidement, on peut considérer que le plan d'action correspond aux besoins du système.

Recommandations

En matière de disponibilité…

1. Le système de protection incendie des locaux serveurs est clairement inadapté. Son déclenchement provoquerait la mise hors service immédiate de toute l'infrastructure serveur. En conséquence, il apparaît urgent de repenser ce système en utilisant, par exemple, un système d'extinction par gaz.

2. Old Rhum ne dispose pas d'infrastructure redondante. Le dysfonctionnement d'un système implique donc un arrêt du service hébergé par ce système pour une durée qui peut être longue. Nous recommandons à Old Rhum de doubler ses serveurs critiques au sein d'une architecture à haute disponibilité ou, à moindre coût, afin de pouvoir repartir en quelques heures a partir des sauvegardes sur un équipement vierge.

3. Dans l'état actuel des choses, la société Old Rhum devrait stopper son activité pour une durée indéterminée si l'environnement informatique venait à défaillir massivement. Afin d'assurer un niveau de sécurité supérieur, Old Rhum devrait démarrer la mise en place un Plan de Reprise d'Activité qui lui permettrait, en cas de sinistre, d'optimiser le temps de redémarrage.

4. Dans l’optique du PRA, il est important que Old Rhum négocie des contrats de mise à disposition de matériel si tout ou partie de son informatique été détruite. Ces contrats permettent généralement de disposer de matériel neuf pré-configuré en 4H, voir une journée. Toutefois, le coût d’un tel service est élevé, il faut donc localiser cela à des entités particulières au sein des groupes fonctionnels Direction/Vente et Production/Services généraux.

5. L’alimentation électrique est un critère déterminant qui doit être maîtrisé en interne de Old Rhum. Un système électrique redondant avec, si possible, un groupe électrogène est indispensable pour permettre la continuité d’activité en cas de panne EDF ou dysfonctionnement interne. Les systèmes onduleurs, à faible coût, permettent d’effectuer la bascule vers un générateur. Toutefois, ces derniers coûtent cher et ne doivent donc pas être dédiés à l’informatique. Il faut déployer ceci entre les différentes entités de Old Rhum.