SEC105 - Architectures et bonnes pratiques de la sécurité des réseaux, des systèmes, des données et des applications

PEI Millau – Concepteur Architecte Informatique (toutes spécialités)

Objectif : Comprendre le fonctionnement et les vulnérabilités, configurer, exploiter, superviser les exigences de sécurité, expliquer DICT, la différence avec la sureté de fonctionnement, mettre en place les mesures de base sur tout système, OS.

Thème : *Sécurité de base des matériels et systèmes d'exploitation – Partie 2 -* ***Virtualisation & cloud***

Préambule

Les technologies dites de « virtualisation » ont connu un essor important ces dernières années, lié notamment au développement de nouveaux usages comme l'informatique en nuage (cloud computing).

Virtualiser un ensemble de serveurs est devenu aujourd'hui relativement aisé, et de nombreuses entreprises ont choisi de « virtualiser » leurs serveurs pour faire des économies de place, d'énergie et de budget.

- Mais les risques associés à l'utilisation de ces nouvelles technologies sont-ils systématiquement pris en compte ?
- Les conséquences de la virtualisation sont-elles correctement comprises et acceptées ?

Rappels

« Virtualiser » un objet informatique, ou le rendre virtuel, signifie le faire apparaître sous son seul aspect fonctionnel, indépendamment de la structure physique et logique sous-jacente.

Le périmètre couvert ici peut se résumer à deux cas :

- la **virtualisation de la couche matérielle** destinée à permettre l'exécution du système (en particulier d'un système d'exploitation) sans qu'il ait à se soucier de la réalité physique sur laquelle il s'appuie. Dans le cas présent, il s'agit bien de « matériel virtualisé », c'est-à-dire de matériel rendu virtuel pour le système d'exploitation qui l'emploie, et non pas d'un « système d'exploitation virtuel » comme on peut souvent le lire ;
- la **virtualisation d'un système d'exploitation** au profit de certaines applications pour que ces dernières puissent fonctionner sur ce dernier alors que cela n'était pas prévu initialement ou pour renforcer l'isolation entre applications.

Périmètre

Dans le cas présent, nous ne retiendrons donc que la virtualisation ne s'applique qu'à deux niveaux :

- le **niveau applicatif**, dès lors que la solution de virtualisation cible une application et lui présente une couche d'abstraction correspondant à son environnement d'exécution. Une machine virtuelle Java (JVM) met par exemple en œuvre une virtualisation au niveau applicatif. Des applications Java développées à un haut niveau s'y exécutent et font abstraction de tout détail de plus bas niveau comme la nature du système d'exploitation ou du matériel sur lequel l'exécution a réellement lieu ;
- le **niveau système**, si la solution de virtualisation vise un système d'exploitation et lui présente une couche d'abstraction correspondant à un environnement matériel compatible. On trouve ainsi des solutions de virtualisation qui permettent de faire tourner simultanément plusieurs systèmes d'exploitation sur une même machine.

De même, le cadre méthodologique pour la virtualisation ici présenté est le même que présenté dans les UE précédentes : complète, cloisonnée, etc.

Risques liés à la virtualisation – avant propos

Le guide ANSSI *« Problématiques de sécurité associées à la virtualisation des systèmes d'information »* **précise qu'on peut identifier les risques comme suit :**

- Risques « classiques » : ceux déjà présents sans virtualisation
- Risques « nouveaux » ou « additionnels » : tous les risques venant s'ajouter du fait de l'utilisation de la virtualisation.

Ainsi, il est recommandé de s'interroger systématiquement de la manière suivante pour identifier les risques :

- Risques pouvant toucher le/les systèmes
- Risques portants sur la couche d'abstraction
- Risques induits par la combinaison des deux.

Risques

RISQUE 1 :
Risque accru de compromission des systèmes

Finalité : *Prise de contrôle par un acteur malveillant d'une brique utilisée dans le système virtualisé.*

Méthode : *Compromission * d'un système invité depuis un autre système invité, ou du système hôte depuis un système invité.*

Conséquence : *Fuite de données, altération du système, perturbations pouvant aller jusqu'à l'indisponibilité.*

Contre mesure :

- **Diminuer au maximum la surface d'attaque :** Défense en profondeur des systèmes invités et hôtes, mise à jour régulière
- **Sauvegardes / PRA * :** procédures à mettre en place

* *Prise de contrôle par un acteur malveillant d'une brique utilisée dans le système virtualisé*
* *Plan de reprise d'activités*

Risques

RISQUE 2 :
Accroissement du risque d'indisponibilité

Finalité : *Indisponibilité d'un ou plusieurs services.*

Méthode : *Pas forcément de compromission, mais utilisation intensives des ressources.*

Conséquence : *Indisponibilité d'un ou de plusieurs services invités sur un système.*

Contre mesure :

- **Idem risque 1**
- **Répartition des systèmes invités, machines dédiés aux systèmes critiques**

Risques

RISQUE 3 :
Fuite d'information par manque de cloisonnement

Finalité : *Accès frauduleux à des informations, altération de l'intégrité des données.*

Méthode : *Compromission de mécanismes de la couche d'abstraction « partagés » (ex. réseau).*

Conséquence : *Impact sur la confidentialité ou l'intégrité de données*

Contre mesure :

- **Limitation des périphériques partagés par la couche d'abstraction** (ex. autant de cartes réseaux que d'hôtes)
- **Utilisation de composantes de cloisonnement adaptés, et fonctionnels** (ex. I/OMMU)
- **Retour à un mode non virtualisé pour les systèmes sensibles**

Risques

RISQUE 4 :
Complexification de l'administration et de la mise en œuvre

Finalité : *Usurpation d'identité, perte de confidentialité/intégrité, manque de traçabilité des opérations de maintenance.*

Méthode : *Aucune*

Constat : *Plus d'éléments, administration « cohérente » rendue plus difficile, erreurs liées à l'automatisation trop importante, erreurs de configuration*

Conséquence : Diverses, mais liées à des erreurs ou manque de traçabilité induite par la complexité

Contre mesure :

- **Conscience du risque et moyens adéquat**
- **Travail de sécurisation des interfaces de gestion**
- **Traçabilité accrue**

Risques

RISQUE 5 :
Complexification de la supervision

Finalité : *Manque d'efficacité ou de cohérence dans la supervision.*

Méthode : *Aucune*

Constat : *Paradoxe entre la nécessité de cloisonnement des machines virtuelles et le souhait d'une vision d'ensemble lors des opérations de supervision*

Conséquence : Gouvernance des systèmes diminuée

Contre mesure :

- *Impose que le personnel opérant les moyens de supervision soit autorisé à accéder aux informations du niveau de sensibilité le plus élevé des données traitées.*

Risques

RISQUE 6 :
Prolifération non souhaitée des données et des systèmes

Finalité : *La localisation précise d'une donnée complexifiée ; difficile d'empêcher la copie frauduleuse.*

Méthode : *Aucune*

Constat : *La virtualisation rend les systèmes invités moins adhérents aux équipements. Leur migration sur différentes machines est donc possible, et la plupart du temps souhaitée.*

Conséquence : Risques de copie non maîtrisée (non-respect des licences logicielles) des instances, perte, vol, modification ou perte de maîtrise des versions logicielles des instances (régression) importants.

Contre mesure :

- Aucune, si ce n'est d'intégrer ce risque et de mettre en œuvre une politique adaptée.

Risques

RISQUE 7 :
Incapacité à gérer voire à comprendre les erreurs

Finalité : *Accroissement de la complexité à identifier les erreurs.*

Méthode : *Aucune*

Constat : *Les problèmes de fonctionnement et les erreurs peuvent être complexes à gérer techniquement dans une architecture s'appuyant sur une solution de virtualisation*

Conséquence : Manque d'efficacité dans le traitement des incidents / erreurs

Contre mesure :

- Mettre en place une centralisation et une corrélation des journaux sur l'ensemble des systèmes.

Risques

RISQUE 8 :
Investigations post incident plus difficiles

Finalité : *Accroissement de la complexité à investiguer sur des incidents.*

Méthode : *Aucune*

Constat : *L'optimisation de la mémoire vive des systèmes invités rend l'investigation plus délicate*

Conséquence : Manque d'efficacité dans le traitement des incidents à postériori

Contre mesure :

- Seule la connaissance précise du mode de fonctionnement des solutions de virtualisation permettra de retenir celles qui gèrent le plus rigoureusement les accès mémoire et facilitent des investigations post incidents

Recommandations

R1	La politique de sécurité du système faisant l'objet d'une démarche de virtualisation doit être mise à jour pour qu'y soient inclus certains items spécifiques à la technologie de virtualisation employée.
R2	Un processus de veille des vulnérabilités propres aux technologies de virtualisation utilisées au sein de l'organisme doit être mis en place.
R3	Réduire la surface d'attaque de la solution de virtualisation.
R4	Concevoir une architecture respectant le principe de cloisonnement.
R5	Utiliser des matériels gérant le cloisonnement.
R6	Mettre à jour le plan de reprise ou de continuité d'activité.
R7	Dédier une équipe d'administration à la solution de virtualisation distincte de celle des systèmes invités.
R8	Prévoir une équipe d'administration des machines virtuelles (systèmes invités) indépendante de l'équipe d'administration de la solution de virtualisation.
R9	Former les équipes d'administration, d'audit et de supervision aux techniques de virtualisation.

Règles de contrôle : checklist recommandée

☐	L'architecture de la solution de virtualisation a été conçue en prenant en compte les éléments suivants : • le niveau d'exigences en termes de sécurité d'une machine physique doit être au moins égal au niveau d'exigences du système invité ayant le besoin de sécurité le plus élevé ; • une atteinte en intégrité d'un des systèmes invités sur une machine physique peut porter atteinte à la sécurité de tous ses systèmes invités ; • le risque d'indisponibilité d'une application est plus élevé si elle est hébergée sur une machine virtuelle ; • la migration non voulue des systèmes invités, de leurs applications et des données qu'elles traitent, d'une machine physique à une autre peut conduire à une circulation non souhaitée des données sur le réseau ;
☐	Les systèmes invités présents sur une même machine physique manipulent des données qui ont une sensibilité similaire ;
☐	Les systèmes invités présents sur une même machine physique appartiennent originellement à une même zone de confiance (Réseau d'entreprise interne, de production, de recherche et développement, etc.) ;

Règles de contrôle : checklist recommandée

☐	Une carte réseau physique est utilisée par groupe de systèmes invités qui manipulent des données de même sensibilité, en particulier si aucun autre moyen complémentaire de protection des flux (tel le chiffrement) n'est prévu par ailleurs ;
☐	L'utilisation des ressources (processeur, mémoire, espace disque) par chaque machine virtuelle est limitée afin qu'aucune d'elles ne puisse monopoliser le système hôte au détriment des autres ;
☐	Des règles strictes, précises et cohérentes concernant la migration manuelle ou automatique des systèmes invités, de leurs applications et des données traitées entre différentes machines physiques sont établies ;
☐	Un réseau est dédié pour l'administration et la supervision des systèmes hôtes en s'appuyant sur des moyens réseau (cartes réseau, commutateurs) distincts de ceux utilisés par les systèmes invités ;
☐	Les postes dédiés à l'administration et à la supervision des machines virtuelles sont correctement sécurisés. En particulier, ils ne permettent pas l'accès à Internet ;
☐	Les administrateurs des machines hôtes doivent s'authentifier nominativement, et leurs actions sont journalisées ;

Règles de contrôle : checklist recommandée

☐	Tous les éléments d'authentification (mots de passe, certificats) par défaut ont été supprimés ou modifiés ;
☐	La solution de virtualisation gère de manière adéquate le cloisonnement des données, y compris vis à vis des périphériques, par la mise en œuvre, entre autres, d'une IOMMU (*Input/Output Memory Management Unit*);
☐	La solution de virtualisation ne diminue pas le niveau de sécurité intrinsèque des systèmes invités. Par exemple, elle ne doit pas leur donner accès à des fonctionnalités matérielles sur lesquelles reposent certains de leurs mécanismes de sécurité ;
☐	Les systèmes hôtes et les systèmes invités sont impérativement sécurisés, notamment en durcissant les systèmes d'exploitation et en maîtrisant leur configuration. Ceci impose une gestion rigoureuse des supports d'installation et des mises à jour ;
☐	Les politiques et moyens techniques de mise à jour des systèmes invités, du système hôte et de la solution de virtualisation sont clairement définis, en particulier les mécanismes appliquant et contrôlant les mises à jour de sécurité des systèmes s'ils accèdent à Internet ou sont accessibles depuis Internet ;

Règles de contrôle : checklist recommandée

☐	La solution de virtualisation a été évaluée d'un point de vue de la sécurité. Les mécanismes de cloisonnement entre les machines virtuelles font partie de la cible de sécurité s'il s'agit d'une certification ;
☐	L'ensemble des matériels, des systèmes et des couches de virtualisation est supervisé. Cela impose au minimum la journalisation des informations de virtualisation, la synchronisation temporelle des machines hôtes, des systèmes invités et des éléments actifs du réseau afin de pouvoir corréler les journaux ;
☐	La politique de sécurité existante prend bien en compte tous les points spécifiques à la solution de virtualisation mise en place ;
☐	Des administrateurs réseau et système sont formés aux techniques de la virtualisation. Les administrateurs de la solution de virtualisation sont choisis parmi les plus expérimentés ;
☐	Les administrateurs des machines hôtes et ceux des systèmes invités sont distincts ;

Règles de contrôle : checklist recommandée

☐	Le personnel assurant l'administration et la supervision fait si possible l'objet d'une enquête de sécurité (voire, en fonction du contexte, d'une habilitation à accéder à des données de niveau de classification supérieur à celui des données traitées par les systèmes qu'il administre et/ou supervise) ;
☐	Les machines virtuelles sont créées et administrées en respectant des procédures rigoureuses. Ces procédures empêchent la prolifération non maîtrisée des images représentant les machines virtuelles et la copie ou le vol de ces images. Elles permettent de gérer la mise à jour de sécurité de ces images afin de garantir l'exécution des machines virtuelles dans leur version la plus à jour.

Voir aussi (si applicable)

Recommandations de sécurité pour les architectures basées sur VMware vSphere ESXi

NOTE TECHNIQUE

RECOMMANDATIONS DE SÉCURITÉ POUR LES ARCHITECTURES BASÉES SUR VMWARE VSPHERE ESXI

Et le Cloud ?

Quels enjeux supplémentaires liés à l'activité du Cloud ? (d'un point de vue du fournisseur de service)

Et le Cloud ?

Problématiques :

- Intégration de nombreux niveaux de privilège induit par l'octroi de droits à l'usager
- Automatisation à outrance (Allocation dynamique d'environnement, de ressources etc…)
- Supervision complexifié (comment superviser quelque chose qui évolue en permanence ?)
- Quel niveau de confiance pour les usagers ?
- Transfert de certains éléments d'infrastructure au client ? Quel impact pour le cloisonnement ?

Et le Cloud ?

Bibliographie recommandée :

- SecNumCloud évolue et passe à l'heure du RGPD
- Le référentiel général de sécurité version 2.0 :
  - les documents
  - Le texte
- Prestataires de services de confiance qualifiés Critères d'évaluation de la conformité au règlement eIDAS
- Prestataires de services d'informatique en nuage (SecNumCloud) référentiel d'exigences