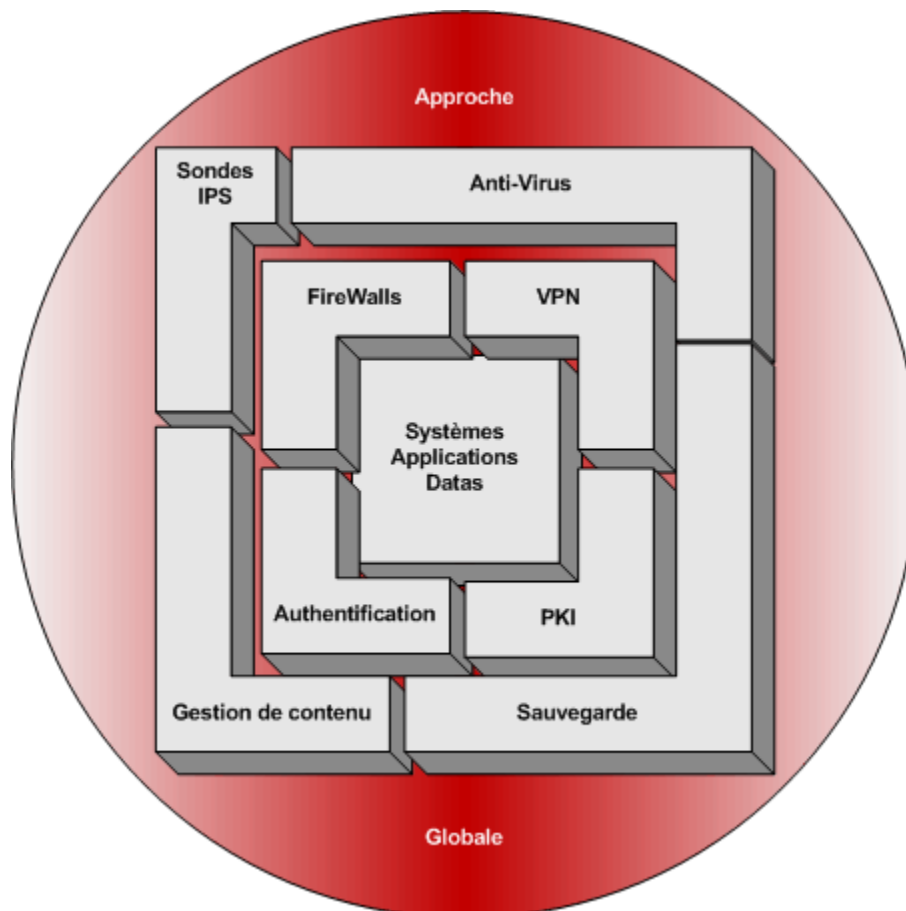


Audits Sécurité

Des architectures complexes...

L'avènement d'Internet et le développement des applications Intranet/Extranet ont permis aux entreprises d'accroître leur compétitivité par l'ouverture de leurs systèmes à leurs clients, partenaires et collaborateurs.

Cette nécessité d'ouverture a conduit à l'exposition croissante des systèmes et données internes aux accès malveillants, tant depuis l'extérieur que depuis l'intérieur de l'entreprise. Les risques inhérents à ces communications ont nécessité l'intégration d'éléments de sécurité spécifiques et complémentaires donnant naissance à des architectures de plus en plus complexes.



Adresse :

8, Rue de la Chapelle
95510 Vienne en Arthies

Téléphone :

00 33 1 34 78 10 15

Télécopieur :

00 33 1 34 78.10.20



Nécessité d'une approche globale

Les différents éléments physiques et logiques impliqués dans la sécurisation des accès, systèmes et données, tout comme les méthodes de travail utilisées au sein de l'entreprise, impactent l'ensemble du système d'information.

Ainsi, bien que celle-ci constitue un premier niveau de protection, la sécurité effective d'un système ne résulte pas seulement de sa protection périmétrique (FireWall, VPN, Content Management, CRM), mais de l'interaction des éléments suivants:

- **Sécurité physique** : Méthodes et protections d'accès physique aux locaux et systèmes, Redondance de disques, de serveurs...
- **Sécurité logique** : Configuration des systèmes d'exploitation (clients et serveurs), configuration des applications mises à disposition, niveau d'authentification requis, procédures d'exploitation, supervision...
- **Sécurité des données** : Configuration des systèmes anti-virus, chiffrement, intégrité, sauvegarde...
- **Sécurité périmétrique** : FireWall, VPN, Authentification d'accès au réseau, détection d'intrusion, gestion de contenu (filtrage)...

Le maillon le plus faible détermine le niveau de sécurité global.

Aussi, de par la complexité des interactions possibles et pour une efficacité maximum, Janus Consulting adopte une approche globale, méthodique et transversale, en quatre phases.

Un audit en quatre phases

Afin de fournir un état exhaustif de la sécurité globale du système à auditer, Janus Consulting applique la méthodologie suivante :

Phase d'interview et de recensement technique,

Phase d'analyse, constitution du diagramme d'interaction des systèmes,

Phase de tests techniques, scans de ports, identification et classement des vulnérabilités découvertes,

Phase de formalisation, Rédaction d'un rapport exhaustif.

Adresse :

8, Rue de la Chapelle
95510 Vienne en Arthies

Téléphone :

00 33 1 34 78 10 15

Télécopieur :

00 33 1 34 78.10.20

451 776 264 RCS Pontoise

N° TVA Intracommunautaire : FR87451776264

APE : 721Z Siret : 451 776 264 00025

<http://www.janus-consulting.fr>



Interviews

La première phase de l'audit consiste à interviewer le Responsable de la Sécurité des Systèmes d'Information, le ou les techniciens chargés de la maintenance et de l'exploitation du système, des utilisateurs représentatifs.

Ces entretiens ont pour but d'obtenir une vision objective sur:

- La politique de sécurité de l'entreprise,
- La sécurité des procédures d'exploitation du ou des systèmes,
- Le niveau de décalage entre la réalité d'exploitation et le niveau de sécurité auquel prétend l'entreprise.

Collecte et Analyse des configurations

Lors de cette phase, Janus Consulting établit un recensement complet des éléments participants à la sécurité physique, logique, données, périmétrique, et collecte l'ensemble des configurations systèmes et matériels impliqués dans la sécurité à l'aide d'outils adaptés.

Une analyse est ensuite réalisée afin de :

- Déterminer la cohérence des configurations collectées, politique anti-Virale, serveur Web, FTP, Règles de FireWall etc.
- Déterminer les niveaux de correctifs appliqués et les besoins de mise à jour,
- Etablir un diagramme d'interaction des différents éléments impliqués,
- Extraire les éléments les plus exposés afin d'en tester la vulnérabilité à l'aide d'outils spécifiques.

Scans de vulnérabilité

Dans le cas d'un audit de sécurité, la simple analyse de l'information collectée peut s'avérer insuffisante. Aussi, afin de corroborer les informations relevées, Janus Consulting procède à deux scans réseaux (non intrusifs), réalisés par les deux outils les plus performants, l'un du marché, l'autre « underground ».

Ces deux outils combinés permettent de détecter plus de 2000 types de vulnérabilités sur plus de 300 applications et 20 systèmes d'exploitation. Les méthodes employées permettent également de fournir une représentation graphique exhaustive de ce qui est visible de l'extérieur.

Les méthodes employées sont :

AXFR : Détermination du Start of Authority du domaine DNS scanné (SOA), et obtention de l'ensemble des enregistrements Name Server (NS) du domaine.

Adresse :

8, Rue de la Chapelle
95510 Vienne en Arthies

Téléphone :

00 33 1 34 78 10 15

Télécopieur :

00 33 1 34 78.10.20

451 776 264 RCS Pontoise

N° TVA Intracommunautaire : FR87451776264

APE : 721Z Siret : 451 776 264 00025

<http://www.janus-consulting.fr>



FQDN brute force : Utilisation d'un dictionnaire de plus de 100 noms hosts communs (www, mail...) puis concaténation avec le nom de domaine afin de découvrir l'ensemble des systèmes déclarés sur la zone publique.

IP brute force : Utilisation de l'adresse IP trouvée afin de déterminer le netblock correspondant, ce qui permet de vérifier l'appartenance de la machine au domaine.

Scan IP TCP UDP : 65534 ports RFC 1700 IANA, ce qui permet d'identifier chaque type de service actif sur la machine cible et d'en tester la vulnérabilité,

Scan des ports « Dead Host » : Ce qui permet de détecter l'existence de machines qui ne répondraient pas, un firewall par exemple,

Scan des adresses privées RFC 1918 : Ceci permet d'établir le NAT (translation d'adresse) utilisé, et permet d'avancer plus loin dans l'investigation du réseau interne à partir de l'extérieur,

Classification des résultats en 5 niveaux :

- **Niveau 1** : Des informations peuvent être obtenues,
- **Niveau 2** : Des informations précises peuvent être collectées comme la version d'OS du système cible,
- **Niveau 3** : Présence de vulnérabilités directement exploitables comme la lecture partielle de certains fichiers ou arborescences, la sensibilité à certaines attaques de type « Buffer Overflow » ou « Denial of Service »
- **Niveau 4** : Modification possible de fichiers, présence de listes utilisateurs lisibles ou « Backdoors » exploitables.
- **Niveau 5** : Accès en modification au système troyen détecté, prise de contrôle à distance possible.

Formalisation des résultats

Une fois la phase d'analyse terminée, un rapport complet vous est remis. Ce rapport contient :

- Une présentation du contexte de notre audit,
- Une expression écrite de vos besoins,
- Un descriptif des méthodes et outils d'analyse utilisés,
- Une formalisation précise de l'état de la sécurité du système analysé, reprenant les comptes rendus d'interviews, le diagramme d'accès et le rapport de scan,
- Un classement exhaustif des vulnérabilités découvertes sur 5 niveaux,
- La liste des correctifs, mises à jour d'OS, et modifications de procédures à apporter classées selon 5 niveaux d'urgence,
- Des préconisations de modification d'architecture ou/et d'intégration de nouveaux services susceptibles d'accroître sensiblement la sécurité.

Ainsi, vous disposez d'un document complet vous fournissant un bilan précis de l'état de votre sécurité et vous permettant d'engager immédiatement les actions correctives nécessaires.

Options

Adresse :
8, Rue de la Chapelle
95510 Vienne en Arthies

Téléphone :
00 33 1 34 78 10 15

Télécopieur :
00 33 1 34 78.10.20

451 776 264 RCS Pontoise
N° TVA Intracommunautaire : FR87451776264
APE : 721Z Siret : 451 776 264 00025
<http://www.janus-consulting.fr>



L'expérience de Janus Consulting acquise au fil de nombreuses missions et la formation permanente de nos collaborateurs aux nouvelles technologies, nous permettent de vous accompagner dans la suite logique de cet audit en vous proposant :

- La mise en place des correctifs,
- Le pilotage ou/et réalisation des modifications d'architecture,
- Des tests intrusifs et, le cas échéant, exploitations des vulnérabilités pour évaluation de risques,
- L'aide à la mise en place d'une nouvelle politique de sécurité,
- Une formation complémentaire de vos équipes.

Adresse :

8, Rue de la Chapelle
95510 Vienne en Arthies

Téléphone :

00 33 1 34 78 10 15

Télécopieur :

00 33 1 34 78.10.20

451 776 264 RCS Pontoise
N° TVA Intracommunautaire : FR87451776264
APE : 721Z Siret : 451 776 264 00025
<http://www.janus-consulting.fr>