notos

SÉCURITÉ DES SYSTÈMES D'INFORMATION

Perfectionnez la sécurité
de votre informatique

NOTOS ET LA SÉCURITÉ INFORMATIQUE DES PME/PMI

La Sécurité des Systèmes d'Information, menacée en permanence, est devenue un enjeu majeur de la pérennité d'une entreprise.
Il ne s'écoule pas un mois sans que la presse ne relate un événement majeur lié à la sécurité (virus ou vers, piratage de données confidentielles, espionnage industriel…).

La Sécurité ne consiste pas seulement à mettre en place un pare-feu et un antivirus.
Selon les experts, nombre de malveillances proviennent de l'intérieur de l'entreprise. Il est donc essentiel de protéger durablement chacun des serveurs et de se doter de plans efficaces permettant de continuer ou de reprendre rapidement l'activité en cas de sinistre.

À Propos de NoToS

NoToS a été créé par Dominique GAYTE, **expert en iSeries (AS/400)** et **spécialiste des Systèmes d'Information**.

NoToS conseille et accompagne les services Informatique des PME/ PMI dans toutes les démarches liées à la Sécurité.

QUELLES SONT LES DOMAINES D'INTERVENTIONS DE NOTOS ?

NoToS propose les services suivants pour perfectionner la Sécurité de votre informatique :

- **La formation**, pour vous sensibiliser aux risques et apprendre à les prévenir
- **Les audits**, pour avoir une idée claire sur votre situation à un instant donné
- **La définition d'un Plan Sécurité** complet, pour définir une stratégie claire
- **La fourniture et l'installation de matériels et de logiciels adaptés à vos besoins** (antivirus, pare-feu logiciel, matériel ou à base de Linux, détection d'intrusion…).

Dominique GAYTE

Dominique GAYTE, fondateur de NoToS, intervient sur l'Informatique des PME/PMI depuis près de 20 ans.
Il est **expert en IBM AS/400** et en ses successeurs iSeries et i5.
Il est titulaire d'un Doctorat en sciences et d'un DESS en Informatique. Il a publié plusieurs ouvrages aux éditions Eyrolles sur l'IBMi (AS400).
Fort de ces diverses compétences, il s'est orienté vers la Sécurité des Systèmes d'Information.
Il est désormais certifié par IBM sur plusieurs technologies.

LES FORMATIONS PROPOSÉES PAR NOTOS

Mise en oeuvre d'un Single Sign On (SSO) à base d'EIM avec un IBM i (AS/400)

Durée : 3 jours (à adapter selon les besoins)
Public : informaticiens
Objectifs : donner aux participants une bonne connaissance des mécanismes d'EIM sur IBM i et Active Directory
Programme :

- SSO avec Kerberos et EIM
- Les besoins de l'entreprise en termes de SSO
- La solution : Kerberos et EIM
    - Authentification (Principes)
    - Autorisations
    - Domaine (Organisation)
    - Identity Mapping (Principes et Exemples)
    - Kerberos (Norme, Mécanisme et Jeton)
    - LDAP (Principe, Annuaires LDAP, Utilisation)
    - Exemples
- Configuration de Microsoft Active Directory
    - Domaine
    - Organisation
    - Kerberos
    - Connexion
    - Comptes
    - Sécurité
    - Stratégie de Groupe
    - Forêts
    - Unités d'organisation
- Configuration de Network Authentication Service (NAS) et d'EIM
- iSeries Navigator et commandes QSH
- Configuration des postes de travail avec iSeries Access for Windows
- Configuration des applications supportant l'architecture EIM
- iSeries Access : iSeries Navigator, PC5250, transfert de fichiers.
- NetServer et le partage de fichiers Microsoft
- Accès base de données : Pilote IBM ODBC
- Accès Web : IBM HTTP Server et Microsoft Internet Explorer
- Configuration EIM incluant plusieurs System i
- Travaux pratiques
- Etude de différents scénarios (selon les besoins)
- Conclusions

Sécurité des IBM i (AS/400)

Durée : 3 jours (à adapter selon vos besoins)
Public : informaticiens
Objectifs : donner aux participants une bonne connaissances des principes de Sécurité de l'IBM i (AS/400) et de son réseau. Identifier les points faibles sur les serveurs de production et définir les méthodes à appliquer pour renforcer la Sécurité
Programme :

Introduction
L'OS/400
    - Principes
    - Valeurs système
Les profils utilisateur
    - Droits spéciaux, privés & publics
    - Groupes
    - Mots de passe
Les objets
    - Listes d'autorisation
DB2/400
    - SQL
    - Fichiers logiques
L'IFS
    - Commandes de gestions
    - Les droits
    - Les virus
Les réseaux
    - iSeries Acces for Windows (Client Access Express)
    - ODBC, transfert de fichiers, émulation écran
    - iSeries Navigator (Operation Navigator)
    - Serveurs IP
Les fonctions d'audit
Les sauvegardes
    - Les commandes
    - Ce qui n'est pas sauvegardé
    - Les impressions
    - Restauration
Les fichiers spool
Les points d'exit
Divers
Conclusions

Mise en oeuvre de SSL sur IBM i (AS/400)

Durée : 3 à 5 jours (à adapter selon vos besoins)
Public : informaticiens
Objectifs : donner aux participants une bonne connaissance des principes du protocole SSL sur IBM i.
Programme :

Introduction
Les cryptages
SSL et TLS
Digital Certificate Manager (DCM)
Autorité de certification
    - Locale
    - Officielles
Magasins de certificats
    - IBM i
    - Client Access
    - Windows
SSL et les serveurs Web
    - Configuration
    - Tests
SSL et Client Access
    - Configuration
    - PC5250
    - Navigator
    - Transfert de fichiers
    - Tests
    - Déploiement sur les postes clients
TELNET entre IBM i
    - Configuration du serveur
    - Configuration du client
FTP
    - FTPS
    - Problématique SFTP
Le serveur d'administration
Autres logiciels
    - SMTP
Conclusions

Pourquoi se former avec NoToS ?

NoToS vous propose des formations adaptées à vos besoins. Nous pouvons également imaginer des **formations sur mesure,** dans vos locaux.

Les formations sont proposées essentiellement en intra entreprise afin de coller au mieux à votre environnement..

La valeur ajoutée de NoToS

Notre grande **expérience de la formation** associée à de **solides compétences techniques** vous garantissent la satisfaction de vos collaborateurs

LES AUTRES PRESTRATIONS DE NOTOS

Analyse des risques

Avant de mettre en place une **politique globale de Sécurité**, nous procédons à une **Analyse des risques**.

La **méthode MEHARI**, conçue par le CLUSIF, ou EBIOS, recommandée par la DCSSI, permet d'évaluer les risques et d'en définir les conséquences.

Un Plan Stratégique est établi afin de définir la stratégie générale de Sécurité et de garantir la cohérence des actions définies.

Un Plan Opérationnel assurera la mise en place de cette stratégie au niveau des différentes entités identifiées.

Cette étude demande une forte implication des dirigeants de l'entreprise. Elle prend en compte la totalité de la problématique sécuritaire et conduit à faire des choix stratégiques qui guideront les préventions à mettre en place.

Des chartes, telles que la **Charte de Management de la Sécurité**, et que la **Charte de l'utilisateur**, seront établies afin de définir le comportement de chacun.

Qu'est-ce que le risque informatique ?

3 causes :

- Accident
- Erreur
- Malveillance

3 conséquences :

- Disponibilité
- Intégrité
- Confidentialité

L'analyse des risques permet de mesurer les potentialités et les impacts de chaque risque afin de définir clairement la politique Sécurité de l'entreprise.

Audit

Etes vous surs de la Sécurité mise en place pour votre Système d'Information : réseau, serveurs, postes de travail, interconnexion avec Internet… ?

Un audit permet d'avoir une **situation claire de votre existant**. Il peut prendre en compte tous les aspects de la Sécurité :

- Sauvegardes/restaurations
- Solutions de secours à chaud ou à froid
- Niveau de protection des serveurs
- Architecture réseau
- Firewall
- Interconnexion avec Internet VPN
- Les postes client
- Documentation des tâches essentielles
- Gestion des mots de passe
- Analyse des plans Sécurité existants
- Analyse des sinistres récents

Cet audit peut être **exhaustif**, pour avoir une vision complète du niveau de Sécurité de votre Système d'Information, ou **rapide** afin de définir les éventuelles lacunes à corriger rapidement.

iSeries et Sécurité

L'AS/400 est reconnu comme un serveur extrêmement robuste sur le plan de la Sécurité. Cette reconnaissance est largement justifiée.

Toutefois, **la Sécurité est souvent gérée par les applications, héritage des architectures centralisées des années 80 et 90. Avec l'ouverture de l'AS/400 aux réseaux, cette organisation ne suffit plus à protéger efficacement les données**.

Ainsi, dans certains cas, la base de données est directement accessible via de nombreux moyens : ODBC, Client Access Express, Operation Navigator, FTP…

Si la protection est uniquement gérée par les applications, il est probable que certains utilisateurs mal intentionnés puisse accéder directement aux fichiers (celui de la paye, par exemple).

De même, **on trouve encore aujourd'hui des serveurs dont le niveau de Sécurité est resté à 20 qui est en fait un niveau de forte insécurité.** L'AS/400 dispose de tous les mécanismes qui permettant de protéger efficacement vos applications et vos données, mais encore faut il le configurer convenablement en fonction de votre organisation et de vos attentes en matière de Sécurité.

Matériels et logiciels

La Sécurité des réseaux informatiques s'appuie généralement sur la mise en œuvre de matériels et de logiciels

Deux types de solutions ont étés retenus par NoToS :

- **partenariats avec des éditeurs et des constructeurs** afin de proposer des produits commerciaux. Il s'agit, notamment de Symantec et d'IBM
- **distribution de logiciels du monde libre** lorsque ces solutions ont un sens dans votre contexte. Linux, par exemple, peut s'avérer un excellent pare-feu si vos équipes y sont préparées.

CONTACT

04 67 86 09 08
Dominique GAYTE, gérant
dgayte@notos.fr

www.notos.fr

Centre de développement et de formation
2, Esplanade du Pic Saint-Loup
34160 BEAULIEU

Siège Administratif
32, Chemin de Notre Dame
34160 BEAULIEU

04 67 86 09 08

IBM Partenaire Commercial

zend Solution Partner