



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

Troisième journée sur les technologies et standards de l'Internet

20 Octobre 2003

Normes utiles en sécurité réseau

GFSI



Hervé Schauer

Herve.Schauer@hsc.fr

- × Introduction
 - × IDMEF, ICAP, et les autres normes
- × Normes permettant la sécurisation et l'audit des réseaux
 - × ISO17799 / BS7799-1 : *Code of practice for information security management*
 - × BS7799-2 : *Information Security Management systems – Specification with guidance for use*
 - × ISO19011 : Lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental
- × Normes de journalisation des réseaux
 - × RFC3164 : *syslog*
 - × RFC3195 : *reliable delivery for syslog*
 - × Draft *syslog-sign*
- × Références et remerciements

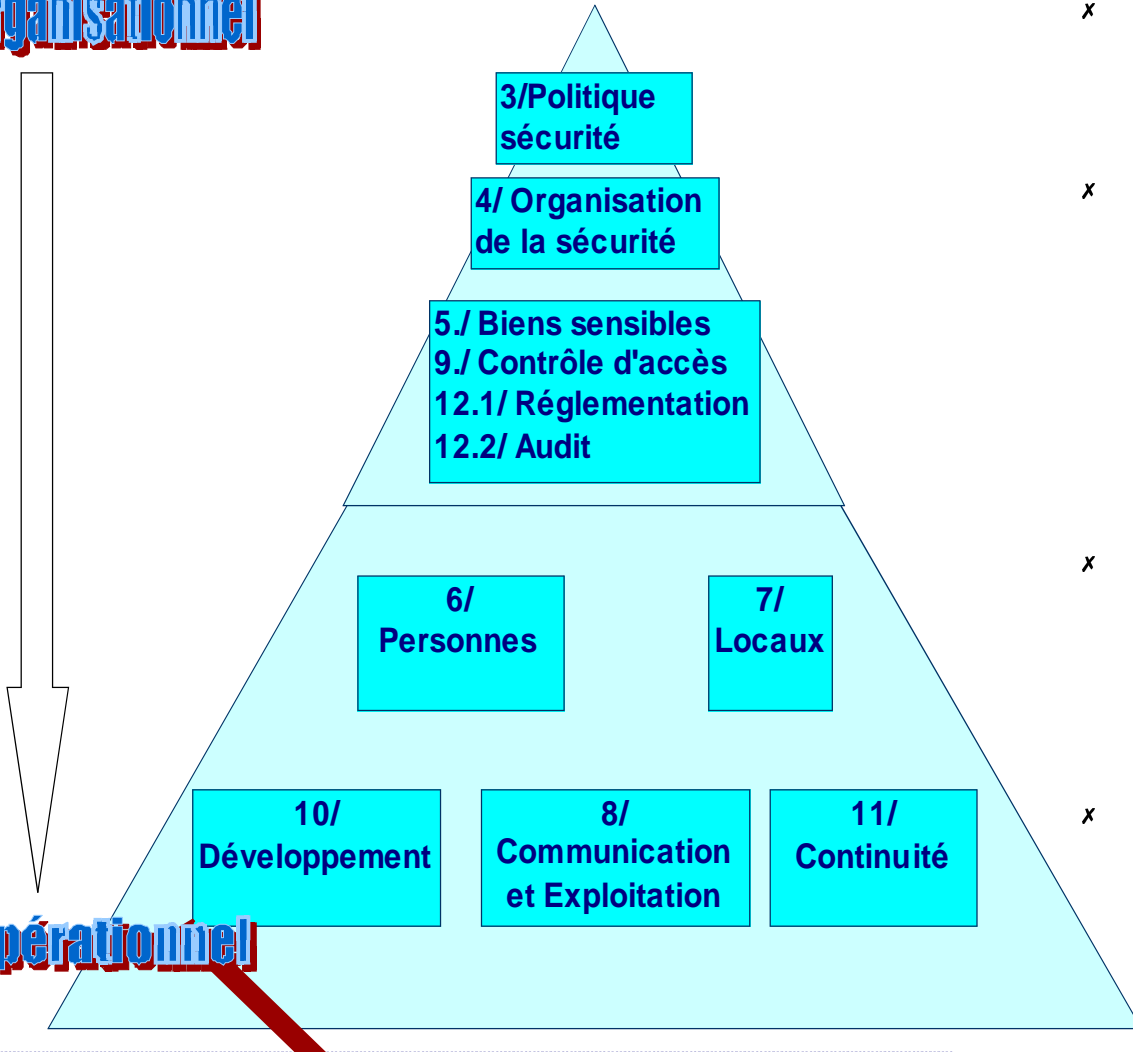
- × HSC est un cabinet de conseil et d'expertise en sécurité Internet
- × Objectif : donner un aperçu des normes qui nous sont utiles en sécurité Internet
 - × Focalisation sur les normes récentes
 - × Normes qui servent concrètement ou vont servir concrètement pour améliorer la sécurité des réseaux
 - × Vision limitée à notre expérience
 - × Introduction de normes ISO, utiles en sécurité, très loin du travail réalisé à l'IETF

- × Beaucoup de normes manquent dans cet aperçu
- × IDMEF (`draft-ietf-idwg-idmef-xml-10.txt`)
 - × Échanges de messages entre sondes et analyseurs de détection d'intrusion
 - × Aussi utile pour la journalisation
 - × Hervé Debar est auteur du draft
 - × Nombreuses implémentations notamment Prelude
 - × <http://www.prelude-ids.org/>
- × ICAP (RFC3507) Internet Content Adaptation Protocol
 - × Permet pour la distribution des données pour l'analyse de contenu
 - × Supporté dans plus de la moitié des *firewalls*, relais HTTP, anti-virus, etc
 - × Pour l'IESG devra être remplacé par une norme issue du groupe OPES

- × Les normes "anciennes" utilisées en sécurité incluent principalement :
 - × SSL/TLS, protocole principal pour la sécurité des échanges
 - × Exemple : SSLtunnel <http://www.hsc.fr/ressources/outils/ssl tunnel/>
 - × LDAP, utilisé en sécurité notamment pour construire des SSO (*Single Sign-On*)
 - × Identification, authentification et autorisation
 - × Radius
 - × X.509 & PKIX
 - × Kerberos
 - × IPsec, pour établir des liens point à point

- × ISO17799:2000
 - × Défini des objectifs et des recommandations concernant la sécurité de l'information
 - × Norme globale pour tout type d'organisme
- × Est complétée par BS7799-2, qui n'est pas prévue à l'ISO
- × Historique ISO17799
 - × Groupe britannique ayant produit BS7799:1995, puis BS7799-1:1999
 - × Soumis 2 fois en procédure *fast track* à l'ISO
 - × Adopté en Décembre 2000 dans des conditions particulières
 - × Actuellement en phase de révision depuis 2001

Organisationnel



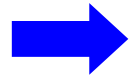
Opérationnel

- x Référence de bonnes pratiques
- x Chaque chapitre inclu des
 - x Objectifs de sécurité
 - x Mesures à mettre en œuvre
 - x Contrôles à effectuer
- x Chaque chapitre peut être consulté indépendamment des autres
- x Numéros = chapitres de la norme

- × Couvre toutes les thématiques
 - × Politique de sécurité
 - × Organisation de la sécurité
 - × Classification et contrôle du patrimoine informationnel
 - × L'insécurité issue des défaillances humaine
 - × La sécurité physique
 - × La gestion des opérations et des communications
 - × N'ignore pas Internet
 - × Ignore les réseaux sans fil
 - × Le contrôle d'accès
 - × Le développement
 - × La continuité d'activité
 - × La conformité à la réglementation

Exemples de biens sensibles

1/ Que protéger et pourquoi ?



Liste des biens sensibles

Permet de sélectionner ses mesures de sécurité sur la base d'une analyse de risques

Exemples de menaces

2/ De quoi les protéger ?

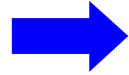


Liste des menaces

× Analyse de risque selon tout types de méthode y compris la sienne



3/ Quels sont les risques ?



Liste des impacts et probabilités

× Propose un référentiel commun international

× Positionnement de son organisme vis-à-vis des autres

Exemples de recommandations

4/ Comment protéger l'entreprise ?



Liste des contre-mesures

Permet une utilisation partielle comme règle ou guide interne

- × Norme anglo-britannique
 - × Une norme d'un pays européen a plus de valeur dans les autres qu'un document non-normatif
 - × Reprise par plusieurs pays comme norme
 - × Similaire à la norme ISO19011 en spécifique à la sécurité
- × Défini les exigences d'un système de management de la sécurité de l'information
 - × Règles de bonnes pratiques à suivre
 - × Applicable notamment pour la sécurité des réseaux
 - × Déclinables pour toutes les technologies et environnements
 - × Auditables et donc le suivi est contrôlable
- × Utilise le modèle PDCA : *Plan-Do-Check-Act*

- × Système de Management de la Sécurité de l'Information (SMSI)
 - × Définir une politique de sécurité et des objectifs en sécurité
 - × Appliquer la politique
 - × Atteindre les objectifs
 - × Contrôler que les objectifs ont été atteints
- × Permet une certification de l'organisme
 - × Certification dite "ISO17799" impossible : abus de marketing
 - × Certification des auditeurs par le BSI : BS7799 *Lead Auditor*

- × Annexe A
 - × Normative
 - × Contient les objectifs associés à chaque recommandation de sécurité listée dans ISO17799, et pour chaque objectif les mesures à mettre en place
 - × Proche de ce que les experts en sécurité font souvent
 - × Reste très général et indépendant des technologies
 - × Exemples :
 - × 8.5.1 : *A range of controls shall be implemented to achieve and maintain security in networks*
 - × 9.4.1 : *Users shall only have direct access to the services that they have been specifically authorized to use*
 - × 9.4.8 : *Shared networks shall have routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications*

ISO19011 : Audit des systèmes de management de la qualité

- × Norme d'audit, Octobre 2002, remplace ISO14010/14011/14012:1996
 - × Basé sur les concepts et le vocabulaire ISO9000:2000
 - × Conçue pour l'audit des systèmes de management de la **qualité** ou de management **environnemental**
 - × S'applique parfaitement aux audits de gestion de la **sécurité**, notamment aux audits de réseau et de sécurité réseaux, plates-formes, applications, etc
- × La norme ISO19011 défini
 - × Les principes de l'audit
 - × La gestion du processus de l'audit dans le temps
 - × Etablissement, mise en œuvre et revue du programme d'audit
 - × Le programme d'audit :
 - × Objectifs, Étendue, Responsabilités et ressources, Procédures
 - × L'organisation de l'audit
 - × Les qualités et connaissances requises

- × Référence de *syslog* : implémentation d'Unix BSD 4.2 depuis 1985
- × Normalisé en août 2001 par l'IETF
- × Ajout d'une normalisation du vocabulaire
 - × Equipement qui génère un message de journalisation : périphérique (*device*)
 - × Equipement qui reçoit un message et le retransmet à un autre équipement : relais (*relay*)
 - × Equipement qui reçoit un message et ne le retransmet pas : collecteur (*collector*) = serveur *syslog*
 - × Périphérique ou relais qui envoie un message : émetteur (*sender*)
 - × Relais ou collecteur qui reçoit un message : receptriceur (*receiver*)
 - × Principe : les émetteurs envoient des messages vers les récepteurs
- × Pour tout savoir sur le groupe *syslog* :
<http://www.employees.org/~lonvick/index.shtml>

- × Limitations de *syslog* dans le RFC3164
 - × Conservation d'UDP 514 uniquement
 - × Pas de fiabilité de délivrance de données
 - × Messages *syslog* peuvent arriver dans le désordre
 - × Sensibles aux attaques par usurpation d'adresses IP
- × Beaucoup d'implémentations propriétaires de *syslog* sur TCP
 - × Cisco PIX 4.3, *syslog-ng*, Kiwi *syslog*, Monitorware, etc
- × RFC3195
 - × Basé sur le RFC3080 : BEEP Blocks Extensible Exchange Protocol
 - × Le transport de BEEP sur TCP
 - × Deux profils de BEEP : RAW et COOKED
 - × Deux implémentations : SDSC-*syslog*, Adiscon Monitorware

- × BEEP (RFC3080) est un protocole d'échange de messages
 - × Entre hôtes
 - × Messages arbitraires de type MIME
 - × Souvent des messages texte structurés en XML
- × BEEP définit des canaux (*channels*) et des profils
 - × A chaque canal est associé un profil qui définit la syntaxe et la sémantique des messages échangés
 - × Trois profils sont prédéfinis
 - × Gestion des canaux
 - × Gestion de la sécurité du transport en se basant sur TLS
 - × Gestion de l'authentification des entités en utilisant SASL
 - × RFC3195 définit deux profils BEEP pour le transport de la journalisation
 - × RAW : format des messages identique au syslog du RFC3164
 - × COOKED : ajoute l'identification du rôle de l'émetteur et l'identification des relais et du niveau de sécurité durant le transit

- × Limitations de *syslog* dans le RFC3164
 - × Messages *syslog* envoyés en clair, interceptables voir modifiables
 - × Pas d'authentification entre émetteur et récepteur
 - × Déni de service relativement aisé
- × `draft-ietf-syslog-sign-12.txt`
 - × Ajoute des informations dans la partie MSG du protocole *syslog*
 - × Compatible avec les implémentations *syslog* ne supportant pas *syslog-sign*
 - × Indépendant de *syslog-reliable* (RFC3195)
 - × Implémenté dans *syslog-sec*, prévu dans SDSC-*syslog*
 - × <http://sourceforge.net/projects/syslog-sec/>
 - × Soumis comme draft IETF

- × Fonctionnalités de sécurité ajoutées au *syslog* (RFC3164) :
 - × Authentification de l'origine des messages
 - × Intégrité des messages
 - × Séquencement des messages
 - × Protection contre le rejeu
 - × Détection des messages manquants
- × Permet une mise en œuvre progressive émetteur par émetteur

- × Les normes principales sont des normes de sécurité et d'audit
 - × Ces normes sortent du cadre IETF
 - × Même lorsque le sujet est la sécurité Internet
 - × L'ensemble ISO17799 / BS7799-2 connaît du succès
 - × Répond à un besoin
- × Les normes de journalisation sont utiles au quotidien
 - × Un format standard de journaux aurait pu arriver 10 ans plus tôt
- × La sécurité repose sur le contrôle d'accès
 - × Sur Internet le contrôle d'accès ⇒
 - × Filtrage IP
 - × Analyse de contenu SMTP et HTTP
 - × Filtrage HTTP et XML

- × ISO17799:2000 : présentation générale, Groupe ISO17799, Clusif, 03/2003
 - × <http://www.hsc.fr/presse/publications.html.fr#ouvrages>
 - × <http://www.hsc.fr/~schauer/clusif/Presentation-ISO17799.pdf>
- × BS7799-2 : presentation générale, Groupe ISO17799, Clusif, à paraître en 2004
- × La journalisation, Frédéric Lavécot, HSC, 02/2003
 - × <http://www.hsc.fr/ressources/presentations/linux2003-a/>
- × *Universal Format for Logger Messages*, Jérôme Abela, HSC, 07/1997
 - × <http://www.hsc.fr/ressources/normalisation/ulm/>
- × XML-Logs, Nicolas Jombart, HSC, 10/2000
 - × <http://www.hsc.fr/ressources/presentations/xml-logs/>

- × Marie-Agnès Couwez et Pascal Lointier pour l'usage des schémas du document du Clusif
- × Alexandre Fernandez et Nicolas Jombart pour le cours *Lead Auditor* BS7799
- × Jean-Baptiste Marchand et Mercedes Fernández Vidal pour leur étude et expérimentation sur *syslog*
- × Alain Thivillon et Jean-Baptiste Marchand pour leur relecture