# Global Information Assurance Certification Paper

# Guide d'analyse de sécurité de solutions d'accès à distance

Christine Grassi
GSEC Practical Assignment
30 octobre 2003
Version 1.4b – Option 1

## ABSTRACT

Le travail à distance ou « télétravail » est un mode de fonctionnement de plus en plus utilisé par de nombreux employés (que ce soit par choix ou par obligation). Les départements informatiques de leur entreprise ont donc du mettre en place toutes les technologies leur permettant d'accéder aux réseaux internes de leur organisation de la manière la plus efficace qu'il soit. Mais l'efficacité n'est pas le seul aspect à prendre en compte dans le choix d'une technologie d'accès à distance. Dans la mesure où elles permettent d'ouvrir vers l'extérieur des systèmes auparavant inaccessibles, leur impact sur le niveau général de sécurité informatique de l'organisation doit lui aussi être étudié.

L'objectif de ce document est donc d'aider les décideurs qui ont à sélectionner une solution d'accès à distance au réseau local (LAN) et/ou étendu (WAN) de leur entreprise à évaluer le niveau général de sécurité implanté dans certaines de celles présentes sur le marché.

## 1. DESCRIPTION DU CONTEXTE

### 1.1 Le télétravail

De nos jours, il est de plus en plus fréquent que des solutions permettant le travail à distance soient implantées au sein des organisations.
Il s'agit d'une tendance qui est apparue il y a une vingtaine d'années :

> Le concept a émergé initialement dans les années 80, quand l'idée relativement simple de faire travailler les employés de chez eux a été mise en avant comme moyen d'augmenter la productivité, d'améliorer l'équilibre travail/vie personnelle, de retenir et d'attirer le personnel et de répondre à des problèmes de société comme la pollution atmosphérique et la congestion sur les routes.[1]

Avec le temps, ce mode de travail s'est fortement répandu dans les pays occidentaux. « Le nombre de télétravailleurs a doublé dans les trois dernières années pour atteindre 20 millions, selon une nouvelle étude publiée par le Bonn Empirica society for communication and technology research. »[2]

De même :

> D'après *Computer World*, le télétravail fait partie des applications d'Internet les plus prometteuses pour 2003. Selon l'International

[1] (AT&T)
[2] (Fiutak)

> Teleworkers Association Council (ITAC), les Etats-Unis compteraient déjà 28 millions de télétravailleurs et ce nombre devrait grimper de 6 millions par an au cours des trois prochaines années. Le Canadian Telework Association dénombre pour sa part 1.5 millions de canadiens et 200 000 québécois qui télétravaillent.[3]

Par conséquent, depuis plusieurs années, de très nombreuses entreprises en nouvelles technologies de l'information se sont mises à lancer sur le marché une pléthore de solutions permettant aux employés d'accéder à distance aux systèmes et/ou données hébergées au sein des réseaux LAN/WAN de leur organisation. Une des questions qui se posent alors est : toutes ces solutions fonctionnent-elles de façon sécuritaire ?

### 1.2 L'impact sur la sécurité : des préoccupations sérieuses

Toutes les organisations ne se sentent pas encore concernées par les questions entourant la sécurité informatique. Mais il s'agit d'une tendance qui tend de plus en plus à s'inverser. En effet :

> En 2001 les revenus globaux du marché, incluant les logiciels, le matériel et les services, ont bondi de 17 milliards de dollars à 45 milliards sur les trois dernières années, selon Brian Burke, analyste de recherche senior pour le service des produits de sécurité de l'IDC.[…] Les résultats de notre étude montre que la sécurité a été désignée comme la première des priorités en 2002. Et que la sécurité était aussi le seul budget des TI à augmenter en 2001.[4]

Or, le développement du télétravail place justement les entreprises devant de nombreuses questions de sécurité, dont voici quelques exemples :

- Le code en arrière de tous les produits d'accès à distance a-t-il été développé de façon à être exempt de tout problème de développement?
- Pourrais-je être sûr que seuls les individus dûment autorisés auront accès aux systèmes informatiques internes de mon organisation?
- Sera-t-il possible à un individu malveillant d'espionner les communications transitant entre un utilisateur légitime et mon réseau local ?
- Sera-t-il possible de garder une trace des opérations qui auront été faites sur mes systèmes internes à partir de ces accès distants?
- Sera-t-il possible de limiter les utilisations qui seront faites de ces accès distants?

Malheureusement les responsables en charge de la sélection d'une solution d'accès à distance n'ont pas toujours toutes les connaissances pour répondre à ces différentes questions, ni même la chance de disposer dans leur organisation d'un responsable de la sécurité qui sera en mesure de prendre en charge l'évaluation de ces produits.

---

[3] (Vachon)
[4] (Gaudin)

D'où l'intérêt de ce document : aider ces responsables à effectuer une première analyse générale du niveau de sécurité de certains produits présents sur le marché de l'accès à distance.

## 2. CADRE DE L'ANALYSE DE SÉCURITÉ

### 2.1 Les solutions d'accès à distance étudiées

Afin de clarifier la portée de ce document, il est important de préciser quelles sont les solutions d'accès à distance dont la sécurité pourra être analysée via ce guide.

Par solution d'accès à distance on entend une solution réseautique qui permet à un utilisateur physiquement situé en dehors des locaux hébergeant le LAN/WAN de son organisation d'y accéder. Par conséquent :

- Les solutions de type purement « accès à distance à un système unique » (« remote desktop software »), telles que « pcAnywhere » ou « VNC », ne font pas partie à proprement parlé de cette étude (bien que certains des critères de sécurité mis en avant dans ce guide pourraient être utilisés pour évaluer de telles solutions d'accès). En effet, nous avons souhaité nous concentrer sur des solutions pensées, dès leur début, pour permettre un accès de l'externe vers tout ou partie des ressources d'un WAN/LAN, et non pas des solutions d'accès initialement conçues pour permettre l'accès, souvent de l'interne, à un seul système.
- De même, les accès point à point (ex : ISDN) qui pourraient être établis entre deux LAN/WAN sont hors du cadre de cette analyse.
- Nous ne prendrons pas non plus en compte les solutions d'accès qui font appel, pour fonctionner, à un portail d'accueil géré par une entreprise tierce (qui renverrait ensuite le trafic vers le réseau LAN/WAN de l'entreprise cliente).
- Pour finir, nous sommes partis avec l'hypothèse que le système dont l'utilisateur se sert pour accéder au réseau de son entreprise est celui qui lui a été donné par cette même entreprise pour effectuer ses activités professionnelles. Ceci signifie par exemple qu'il ne peut s'agir d'une station en libre accès, placée dans un lieu public.

Ce guide est donc conçu prioritairement pour aider un gestionnaire à évaluer le niveau de sécurité général propre à une solution d'accès à distance de type :

- Accès VPN via l'utilisation d'un client logiciel;
- Solution d'accès RAS;
- Connexion distante via une technologie web (ex : accès VPN sans client logiciel);

## 2.2 Les limites du guide d'analyse de sécurité

Il est important aussi de préciser quelles sont les limites de ce guide en matière d'analyse de sécurité :

- Premièrement, nous ne cherchons pas à évaluer le niveau de sécurité inhérent à chaque élément de sécurité composant la solution (ex : la méthode de chiffrement). En effet, notre analyse de la sécurité n'ira pas jusqu'à étudier en détail le code d'une application, la solidité d'une fonction de chiffrement, etc.
  La portée de ce guide est plus macroscopique, dans le sens où l'objectif est uniquement d'évaluer le nombre et le type de composantes de sécurité qui ont été intégrées au sein de la solution d'accès et déterminer si ces composantes peuvent réellement la rendre plus sécuritaire (mais pas le niveau de fiabilité propre à chacune de ces composantes).
- Deuxièmement, ce guide n'est pas un guide d'audit de sécurité. Ce document est là pour aider un gestionnaire à évaluer le sérieux de la sécurité mise en place par un fabricant dans sa solution d'accès à distance. Mais :
  - Il ne fournit pas de méthodologie sur la façon d'obtenir une réponse aux différentes questions de sécurité posées. Cela est laissé au libre soin de la personne qui utilisera les grilles d'analyse (présentées à la section 3.3).
  - Il ne s'agit pas non plus d'un outil de certification : l'objectif de ce document est de fournir un certain nombre d'éléments d'analyse permettant d'obtenir une bonne indication du niveau général de sécurité. Mais il ne permet en aucun cas de fournir une certification des produits étudiés (que ce soit d'un point de vue fonctionnel, de sécurité, de gestion, etc.).
- Enfin, ce guide n'est pas là pour évaluer comment implanter de façon sécuritaire cette solution d'accès au sein d'une organisation. Il s'agit en effet d'une étape à envisager dans un deuxième temps, une fois qu'une solution d'accès aura été sélectionnée. Donc, de nombreux aspects ont été intentionnellement laissés de côté (bien qu'aussi importants que ceux relatifs au niveau de sécurité de la solution). Ex : la gestion de la configuration de l'application, la sécurisation de l'environnement réseau, le processus d'attribution des rôles et responsabilités, etc. A titre indicatif, certains de ces éléments sont listés dans la section 5. Mais ils ne sont mentionnés qu'à titre gracieux, comme des pistes d'analyse pour l'étape suivante.

## 2.3 Les critères d'analyse de la sécurité : la notion de risque

Afin de guider le décideur dans sa démarche d'analyse de sécurité, cette section fournit une définition du concept de risque.

En effet, lorsque l'on étudie la sécurité inhérente à un produit, on cherche en fait à déterminer quel impact sa mise en place sur un réseau aura sur le niveau général de risque technologique auquel fait déjà face l'entreprise hôte. En d'autres termes, et pour nous concentrer sur le sujet qui nous concerne : puisque l'introduction d'une solution d'accès à distance crée un chemin d'accès de l'externe vers des réseaux auparavant inaccessibles, les composantes de sécurité présentes dans cette même solution d'accès permettent-elles de limiter (et jusqu'à quel point?) l'augmentation des risques de sécurité premièrement générée ?

Or, pour pouvoir répondre à cette question, il est important de bien comprendre ce que l'on entend par un « risque ». Nous allons pour cela nous référer à la définition de l'IEEE (« Electrical and Electronics Engineers, Inc ») : « Un risque est caractérisé par la probabilité qu'un événement, un hasard, une menace ou une situation apparaissent ainsi que sa conséquence indésirable. »[5]

Pour compléter cette définition, nous allons aussi définir chacun des termes qui la constitue :

- La menace : une menace est un « événement potentiel et appréhendé, de probabilité non nulle, susceptible de porter atteinte à la sécurité informatique. »[6]
- La probabilité : la probabilité est une « grandeur numérique par laquelle on exprime le caractère aléatoire (possible et non certain) d'un événement, d'un phénomène et qui est égale au rapport du nombre des cas favorables à celui des cas possibles »[7]
- La conséquence : la conséquence est la « suite logique entraînée par un fait qui en est la cause ».[8]

Ce sont donc ces 4 éléments (risque, menace, probabilité et conséquence) qui seront utilisés au sein du guide d'analyse pour évaluer le niveau de sécurité des solutions.

[5] (Tsai)
[6] (Office québécois de la langue française)
[7] (Robert, p.472)
[8] (Le Petit Larousse Illustré en Couleur, p.261)

## 3. UTILISATION DU GUIDE D'ANALYSE DE SÉCURITÉ

### 3.1 Organisation du guide d'analyse

Afin d'être le plus simple possible, le processus d'analyse a été divisé en trois sections :

- Première section : analyse de la partie « cliente ».
  Il s'agit de l'étude de la partie logiciel éventuellement installée sur le système de l'utilisateur ainsi que des mécanismes qui lui permettent d'initier le processus d'accès à distance.

- Deuxième section : analyse de la partie « transport ».
  Il s'agit de l'étude de la portion logiciel chargée du transport des données entre le système de l'utilisateur et le réseau de l'organisation.
  Cette section traite autant des communications terrestres (via câbles) que de celles reposant sur une technologie sans-fil.

- Troisième section : analyse de la partie « système d'accès ».
  Il s'agit de l'étude de la partie logiciel installée sur le système placé à l'intérieur du réseau de l'organisation (DMZ ou LAN) et qui reçoit la communication distante en provenance de la machine de l'utilisateur.

### 3.2 Les domaines de sécurité pris en compte

Pour chacune de ces 3 sections, les éléments de sécurité étudiés se rapportent tous à l'un des domaines suivants :

- Faille de sécurité : par « faille de sécurité » on entend plus spécifiquement toutes les erreurs liées à une mauvaise programmation de l'application et qui permettraient à un individu non autorisé d'obtenir des accès et/ou des informations privilégiées, de perturber le bon fonctionnement de l'application ou de l'altérer (elle ou son contenu).
  Entre le 1er et le 30 septembre 2003, le site « Securityfocus » a publié plus de 180 failles de sécurité sur plus d'une centaine de produits différents. Avant d'utiliser un produit, il est donc important d'étudier son historique de sécurité. Car si vous ne le faites pas, soyez sûr que les pirates informatiques, eux, le feront!

- Droits d'accès à l'application : par « droits d'accès » on entend le « droit accordé à une personne ou à toute autre entité d'avoir accès à des données ou programmes déterminés et de les exploiter d'une façon particulière ».[9]
  Après qu'un administrateur a installé et configuré une application, il est important de savoir s'il sera ensuite possible à un individu de changer les paramètres préalablement établis (par exemple pour rendre l'application

[9] (Office québécois de la langue française)

moins sécuritaire ou obtenir des informations/accès qui ne lui sont pas destinés).

- Relations avec les composantes tierces : par « composante tierce » on entend tous les éléments logiciels directement nécessaires au bon fonctionnement de l'application mais qui lui sont à l'origine indépendants (ex : système d'exploitation, navigateur web, serveur web, etc.). En effet, « les vulnérabilités qui peuvent être présentes dans le noyau du système d'exploitation d'un serveur monofonctionnel peuvent elles aussi complètement miner sa sécurité. »[10]

  Si l'application a besoin pour fonctionner de telles composantes, il est important de s'assurer que la gestion de leur sécurité sera elle aussi prise en charge par l'application. Car il est inutile de disposer d'une technologie parfaitement sécuritaire si elle repose pour fonctionner sur un élément qui, lui, ne l'est pas.

- Administration centralisée : par « administration centralisée » on entend l'accès à une interface unique physiquement installée sur un seul système et qui permet de gérer la configuration et l'utilisation qui est faite de l'application à laquelle elle est liée.
  En effet, pour garder un contrôle sur une application d'accès à distance, il est nécessaire que son administrateur dispose d'une interface lui permettant notamment :

  - D'enregistrer puis de stocker un certain nombre d'informations privilégiées sur l'utilisation qui est faite de l'application et sur son fonctionnement. En effet :

    > […] les journaux d'audit, l'analyse du matériel et les journaux d'activités de sécurité devraient être passés en revue régulièrement ; c'est un processus très demandant en temps et cela seul permet d'alerter l'administrateur des violations et menaces de sécurité une fois qu'elles se sont produites.[11]

  - De reconfigurer l'application dès que nécessaire;
  - D'imposer à tous les utilisateurs des règles strictes d'utilisation de l'application. Ainsi :

    > Sans méthode d'application, l'efficacité de la politique de sécurité est mise en question. […] Sans moyens d'application, l'administrateur met en jeu la sécurité du réseau de son entreprise en faisant confiance aux utilisateurs distants des VPN pour se conformer volontairement à cette politique. Puisque le périmètre réseau sécuritaire est étendu pour atteindre le client VPN, la politique de sécurité doit être imposée en « temps réel »

[10] (Steinberg)
[11] (Stines)

pour protéger l'intégrité à la fois du client VPN et du réseau de l'entreprise.[12]

Il est à noter qu'il est important aussi de s'attacher à la façon dont l'accès aussi bien aux informations d'audit qu'à l'interface d'administration est limité et contrôlé.

- Authentification : par « authentification » on entend le processus qui permet de vérifier qu'un individu est bien celui qu'il affirme être. « L'authentification d'un utilisateur est un élément critique d'une politique de sécurité.».[13]

  Il est critique de s'assurer que les utilisateurs sont ceux qu'ils prétendent être - en particulier lorsque vous n'avez aucun contrôle sur les ordinateurs à partir desquels les utilisateurs effectuent leur accès (le VPN SSL), et que vous ne pouvez pas vous fier à l'adresse IP de l'ordinateur de l'utilisateur (ou aucune autre information qui lui serait reliée) comme preuve de l'identité de l'utilisateur. [14]

  Sans mécanisme d'authentification, n'importe quel individu pouvant bénéficier d'un accès Internet ou téléphonique pourrait accéder au réseau LAN/WAN de l'organisation ayant mis en place une solution d'accès à distance.

- Chiffrement des données : par « chiffrement » on entend une « opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale. »[15]
  Lorsque les données transitent entre le système de l'utilisateur et le réseau local de l'entreprise, si elles ne sont pas convenablement chiffrées n'importe quel individu pouvant se placer sur le chemin de transit pourra les capturer et/ou les modifier.

Le tableau ci-dessous présente les domaines de sécurité étudiés dans chacune des 3 sections du processus d'analyse :

| | Partie « client » | Partie « transport » | Partie « accès » |
|---|---|---|---|
| Failles de sécurité | **X** | | **X** |
| Administration centralisée | | | **X** |
| Droits d'accès à l'application | **X** | | |
| Relations avec des composantes tierces | **X** | | **X** |
| Authentification | **X** | **X** | **X** |
| Chiffrement des données | | **X** | |

[12] (Stines)
[13] (North American Electric Reliability Council)
[14] (Steinberg)
[15] (Office québécois de la langue française)

## 3.3 Comment remplir le guide d'analyse de sécurité ?

L'utilisation de ce guide d'analyse se fait en 4 étapes :

***Étape 1 : récolter toutes les informations/contact nécessaires***

Le décideur doit commencer par réunir toute la documentation et les contacts nécessaires sur la solution d'accès à distance dont il souhaite évaluer le niveau général de sécurité.

***Étape 2 : personnaliser les outils d'analyse***

Dans la section 2.3, nous avons décrit ce qu'était la notion de risque et quel était son rôle. Maintenant il est nécessaire de lui associer un système de quantification, c'est à dire une échelle de mesure permettant de définir les différents niveaux de risque que l'introduction d'une solution d'accès à distance peut faire courir à l'entreprise.

- Pour cela, il est nécessaire de remplir les deux tableaux suivants : « Tableau de définition du niveau de probabilité » et « Tableau de définition du niveau d'impact d'une conséquence » (puisque, comme nous l'avons vu plus haut, la probabilité et l'impact d'une conséquence influencent le niveau général de risque).

| NIVEAU DE PROBABILITÉ | DÉFINITION |
|---|---|
| FAIBLE | |
| MOYEN | |
| ÉLEVÉ | |

- Tableau de définition du niveau de probabilité (à remplir) -

| IMPACT D'UNE CONSÉQUENCE | DÉFINITION |
|---|---|
| FAIBLE | |
| MOYEN | |
| ÉLEVÉ | |

- Tableau de définition du niveau d'impact d'une conséquence (à remplir) -

Pour faciliter ce travail, une échelle de valeurs est déjà proposée pour les deux tableaux, soit « faible », « moyen » et « élevée ». Il est évidemment possible d'y substituer tout autre système de gradation.
Le travail qui reste à effectuer est de trouver une définition pour chacun de ces niveaux. Aucune définition n'a été fournie à l'avance car chacune doit être adaptée aux caractéristiques de l'entreprise.
En effet, toutes les entreprises n'ont ni les mêmes impératifs ni les mêmes craintes en matière de sécurité. Par exemple, une même faille de sécurité peut avoir des impacts complètements différents pour deux entreprises. Voyons l'exemple suivant :

- L'entreprise A est une entreprise qui propose des produits de vente par correspondance (pas de système d'achat en ligne) et héberge

sur un serveur interne des informations personnelles sur tous ses clients. Cette entreprise portera une grande attention à la protection de la confidentialité et de l'intégrité des données hébergées sur ce système.

- L'entreprise B est une entreprise de transport dont les systèmes informatiques gèrent le bon fonctionnement de véhicules utilisés par le grand public. Cette entreprise sera donc surtout sensible aux questions de disponibilité et d'intégrité de ses systèmes.

La classification de leurs besoins de sécurité n'est donc pas la même.
De plus, si un individu non autorisé parvient à accéder à distance au réseau de ces deux entreprises, les actions qu'il pourrait y commettre n'auraient pas forcément le même impact. S'il rendait inopérant un des systèmes internes de ces deux entreprises pour quelques heures, les perturbations seraient sans doute jugées minimes pour l'entreprise A alors que l'entreprise B ferait face à un problème critique pouvant mettre en danger la vie d'individus.
Voilà pourquoi les deux tableaux présentés ci-dessous ont été laissés incomplets : afin de coller le plus possible aux réalités de son organisation en matière de sécurité, c'est au décideur de définir lui-même le contenu des deux échelles de valeurs « probabilité » et « conséquence » (en se basant sur les besoins de son organisation et sur la façon dont la solution d'accès à distance sera utilisée).

- Prendre connaissance ensuite du « tableau d'évaluation du niveau de risque » : ce tableau permet de faire la synthèse des résultats issus de l'analyse des deux tableaux précédents (probabilités et conséquences). Il permet de déduire le résultat final de chaque test, c'est à dire le niveau de risque lié au non-respect de l'élément de sécurité étudié.
  Les données qui le composent sont inspirées des tableaux d'évaluation du risque présents dans les documents « Rank your findings according to risk »[16] et « GNSA Study Guide »[17].

| | | CONSÉQUENCE | | |
|---|---|---|---|---|
| | | FAIBLE | MOYEN | ÉLEVÉ |
| PROBABILITÉ | FAIBLE | FAIBLE | FAIBLE | FAIB LE |
| | MOYEN | FAIBLE | MOYEN | MOYEN |
| | ÉLEVÉ | MOYEN | MOYEN | ÉLEVÉ |

- Tableau d'évaluation du niveau de risque -

A titre indicatif, il existe de nombreuses méthodologies d'analyse de risque sur le marché et parmi celles-ci plusieurs sont d'une grande efficacité.
Par conséquent, celle présentée dans ce document n'est pas forcément la meilleure « dans l'absolu ».

[16] (Sans Institute, p.39)
[17] (Anderson, Baccam, Grill, Grundschober, Madeiros, Meshram et Schaller)

Mais, si les concepts de « menace », « probabilité » et « conséquence » et les niveaux de gradation « faible », « moyen » et « élevé » ont été choisis c'est en raison de leur relative simplicité; simplicité qui permet de bien coller aux objectifs de cette étude (qui ne prétend pas être aussi pointue et détaillée qu'un audit de sécurité).
D'ailleurs, le choix d'une méthodologie d'évaluation des risques implique toujours une certaine part de subjectivité de la part de la personne qui la met en place, comme le souligne l'ISACA (Information Systems Audit and Control Association) :

> Un auditeur en systèmes d'information peut choisir parmi de nombreuses méthodologies d'analyse de risque disponibles, certaines informatisées d'autres non. Elles vont de la simple classification « élevée », « moyen » et « faible », en fonction du jugement de l'auditeur en SI, à celles utilisant des calculs complexes et apparemment scientifiques qui fournissent une quantification numérique du risque. L'auditeur en SI devrait définir le niveau de complexité et de détail approprié à l'organisation à auditer. […] Toutes les méthodologies d'analyse de risque reposent à un moment donné de leur processus sur des jugements subjectifs (par exemple lors de l'assignation de facteurs de pondération aux différents paramètres). [18]

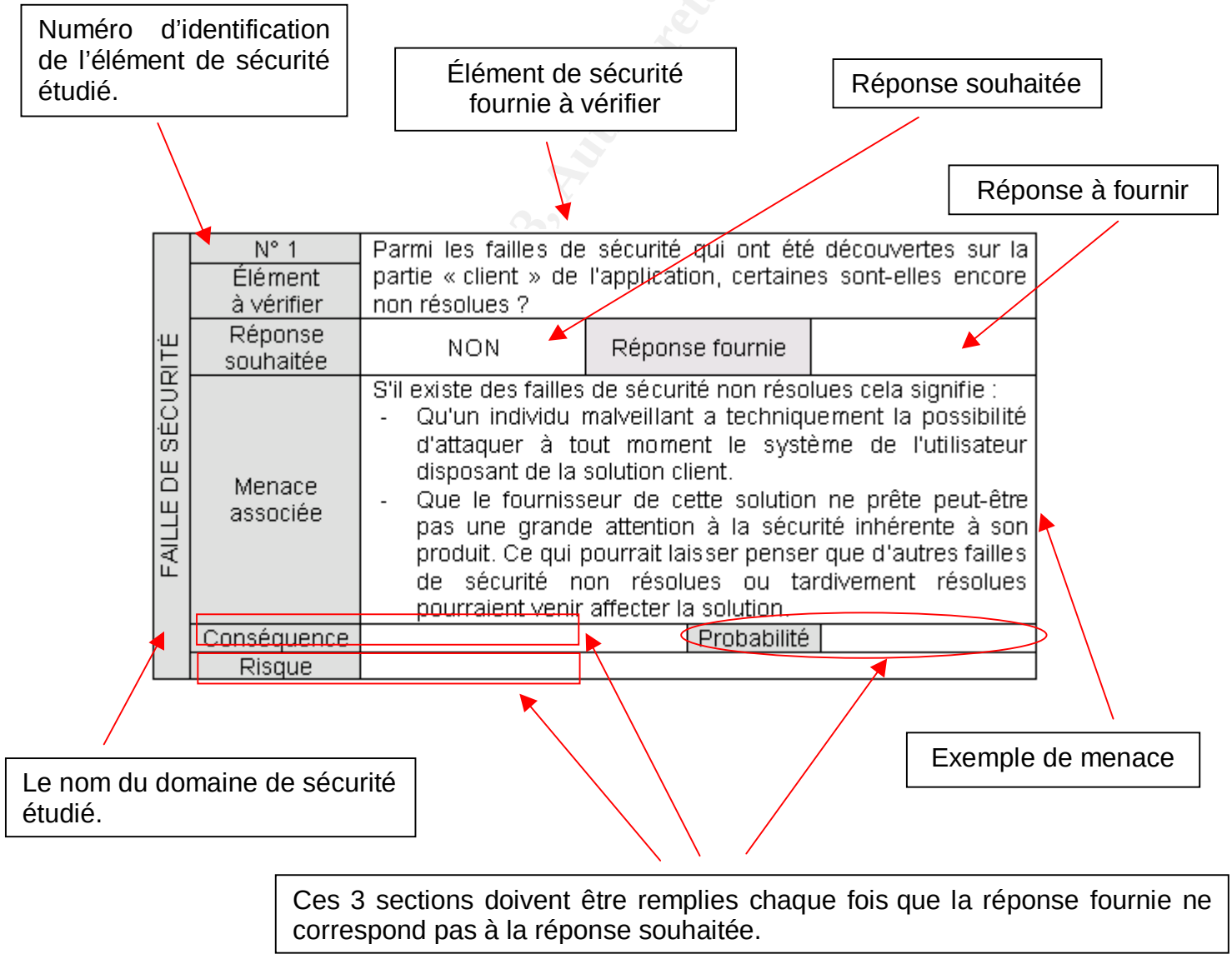
### *Étape 3 : remplir chaque grille d'analyse*

Chacune des trois sections présentées dans la partie 3.1 (« client », « transport » et « système d'accès ») est constituée d'une série de grilles d'analyse. Chaque grille contient une question de sécurité.
Une fois que le gestionnaire aura personnalisé sa méthode d'évaluation du risque, il pourra alors s'en servir pour remplir chacune de ces grilles.
Chaque grille d'analyse est divisée en 9 parties (voir schéma ci-dessous) :

- Numéro d'identification de la grille : permet, lorsque nécessaire, de l'identifier (voir étape 4);
- Nom du domaine de sécurité : la liste des noms de domaine de sécurité étudiés est définie à la section 3.2;
- Élément à vérifier : cette partie contient la question de sécurité à laquelle le gestionnaire doit répondre;
- Menace : cette partie présente un exemple de menace (c'est à dire de problème) qui pourrait survenir en cas de non-respect de l'élément de sécurité mentionné dans la section « élément à vérifier ». Ceci est fourni pour aider le gestionnaire dans son travail d'évaluation du niveau de risque;
- Réponse fournie : le gestionnaire marquera dans cet espace la réponse à la question posée (« oui » ou « non »).

[18] (Information Systems Audit and Control Association)

- Réponse souhaitée : comme son nom l'indique, cette partie contient la réponse qui devrait idéalement être fournie par le gestionnaire. Si la réponse fournie par le gestionnaire (et inscrit dans l'espace « réponse fournie ») correspond effectivement à celle qui est indiquée dans la section « réponse souhaitée », un risque est évité et il n'est donc pas la peine de remplir les sections « Conséquence », « Probabilité » et « Risque ».
- « Conséquence », « Probabilité » et « Risque » : ces 3 sections sont à remplir par le gestionnaire chaque fois que la réponse fournie ne correspond pas à la réponse souhaitée. Dans ce cas là :
    - Dans les cases « Conséquence » et « Probabilité » : le gestionnaire doit inscrire « faible », « moyen » ou « élevé », en fonction de sa propre évaluation (à l'aide des tableaux présentés à la section 3.3);
    - Dans la case « Risque » : le gestionnaire doit inscrire « faible », « moyen » ou « élevé », en fonction des valeurs qu'il a marquées dans les champs « Conséquence » et « Probabilité »;



### *Étape 4 : évaluer les résultats obtenus*

Une fois que toutes les grilles de sécurité auront été remplies et que tous les niveaux de risque nécessaires auront été définis, le gestionnaire aura une bonne idée du niveau général de sécurité propre à la solution analysée.
A titre de support, afin de l'aider dans cette dernière étape, voici en plus une classification des éléments de sécurité étudiés :

| Évaluation | Numéro de la grille d'analyse correspondante |
|---|---|
| Si la réponse fournie à un des éléments de sécurité suivants n'est pas satisfaisante (c'est à dire qu'elle entraîne un risque de sécurité, qu'il soit faible, moyen ou élevé), la solution d'accès à distance doit être rejetée.<br>En effet, tous ces éléments sont à considérer comme cruciaux et aucune solution d'accès à distance ne peut s'en passer. | n°1, n°5, n°6, n°8, n°10, n°12, n°15, n°16, n°17, n°21, n°22, n°23, n°25, n°29 |
| Si la réponse fournie à un des éléments de sécurité suivants n'est pas satisfaisante (c'est à dire qu'elle entraîne un risque de sécurité, qu'il soit faible, moyen ou élevé), le gestionnaire doit évaluer s'il est possible de mettre en place une solution additionnelle indépendante pour compenser les faiblesses de sécurité identifiées.<br>Dans le cas contraire, il devra rejeter la solution d'accès à distance.<br>En effet, tous ces éléments sont à considérer comme cruciaux et il est nécessaire de disposer au moins d'une solution de compensation. | n°3, n°7, n°13, n°18, n°27, n°28 |
| Si la réponse fournie à un des éléments de sécurité suivants n'est pas satisfaisante (c'est à dire qu'elle entraîne un risque de sécurité, qu'il soit faible, moyen ou élevé), le gestionnaire doit évaluer s'il peut mettre en place une solution additionnelle indépendante pour compenser les faiblesses de sécurité identifiée.<br>Dans le cas contraire, le gestionnaire devra évaluer si les risques engendrés peuvent ou non être supportés par l'entreprise.<br>En effet, tous ces éléments de sécurité ne sont pas forcément cruciaux, mais du fait même qu'ils engendrent un risque, ils ne peuvent être ignorés. | n°2, n°4, n°9, n°11, n°14, n°19, n°20, n°24, n°26, n°30 |

## 4. LE GUIDE D'ANALYSE DE SÉCURITÉ

4.1 Analyse de la section « partie client » (le système d'accès de l'utilisateur)

| | | | | |
|---|---|---|---|---|
| FAILLE DE SÉCURITÉ | N° 1 | Parmi les failles de sécurité qui ont été découvertes sur la partie « client » de l'application, certaines sont-elles encore non résolues ? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | NON | Réponse fournie | |
| | Menace associée | S'il existe des failles de sécurité non résolues cela signifie :<br>- Qu'un individu malveillant a techniquement la possibilité d'attaquer à tout moment le système de l'utilisateur disposant de la solution client.<br>- Que le fournisseur de cette solution ne prête peut-être pas une grande attention à la sécurité inhérente à son produit. Ce qui pourrait laisser penser que d'autres failles de sécurité non résolues ou tardivement résolues pourraient venir affecter la solution. | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

| | | | | |
|---|---|---|---|---|
| DROITS D'ACCÈS | N° 2 | Est-il possible d'empêcher l'utilisateur de librement reconfigurer la partie « client » de l'application ? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI | Réponse fournie | |
| | Menace associée | Si un utilisateur peut modifier la configuration de la partie « client » il pourrait éventuellement, en changeant des paramètres de sécurité mis en place par l'administrateur, introduire (inconsciemment ou non) des faiblesses de sécurité. | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

| | | | | |
|---|---|---|---|---|
| COMPOSANTES TIERCES | N° 3 | Si la partie « client » fait appel pour fonctionner à une technologie tierce : si cette composante tierce peut stocker certaines des données d'affaire accédées à distance, un mécanisme est-il en place pour supprimer automatiquement ces données à la fin de l'utilisation de l'accès distant ? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI | Réponse fournie | |
| | Menace associée | Si la composante tierce peut conserver en mémoire cache des données d'affaire accédées lors de la connexion distante, un individu mal intentionné qui accéderait à la partie « client » de l'application pourrait accéder par la même occasion à des données possiblement confidentielles. | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

| | | |
|---|---|---|
| AUTHENTIFICATION | N° 4 | Est-il possible d'utiliser un système d'authentification à deux facteurs? |
| | Élément à vérifier | |
| | Réponse souhaitée | OUI<br>A titre de justification :<br>Une recommandation importante est qu'une authentification forte à deux facteurs (comme un mot de passe à utilisation unique, un jeton SecurID de RSA, etc.) soit utilisée chaque fois qu'un VPN SSL est implanté. Dans le cas de VPN SSL, une authentification forte est encore plus essentielle qu'avec les VPN IPSEC, dans la mesure où les VPN SSL seront souvent activés dans des endroits où des individus inconnus pourront voir l'utilisateur entrer ses informations d'identification/authentification.[19] |
| | Réponse fournie | |
| | Menace associée | Si le système d'authentification n'utilise qu'un seul facteur (ex : quelque chose que l'on sait, comme un mot de passe), cela simplifie les étapes nécessaires à un pirate pour dérober cette information et utiliser ensuite illégitimement l'accès. |
| | Conséquence | Probabilité |
| | Risque | |

[19] (Steinberg)

| | | | | |
|---|---|---|---|---|
| AUTHENTIFICATION | N° 5 | En cas de réponse négative à la question n°4 : pour activer l'application, l'utilisateur peut-il être forcé de créer un mot de passe complexe (8 caractères, utilisation de lettres, chiffres et caractères complexes) ? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI<br>A titre de justification :<br>Une bonne sécurité commence toujours avec une politique de mots de passe consistante. Même si les utilisateurs peuvent s'en plaindre, que la direction puisse s'opposer à vous, imposer une politique de mots de passe forte est quelque chose pour laquelle vous devez vous battre car la plupart des autres éléments de sécurité deviennent discutables si des mots de passe faibles sont autorisés. [20] | | |
| | Réponse fournie | | | |
| | Menace associée | Si un utilisateur n'est pas contraint de créer un mot de passe complexe, il sera tenté d'en utiliser un simple. Or, un mot de passe simple pourra souvent être facilement découvert par un individu malveillant. | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

| | | | | |
|---|---|---|---|---|
| AUTHENTIFICATION | N° 6 | En cas de réponse négative à la question n°4 : pour activer l'application, l'utilisateur peut-il être forcé de changer son mot de passe sur une base régulière ? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI<br>A titre de justification : « Un âge maximum sur les mots de passe empêche qu'un mot de passe compromis soit utilisé trop longtemps. »[21] | | |
| | Réponse fournie | | | |
| | Menace associée | Si un mot de passe n'est pas ou peu changé : un pirate qui aurait réussi à en découvrir la forme chiffrée (forme sous laquelle les mots de passe sont souvent stockés et/ou transportés) pourra prendre tout le temps nécessaire pour le déchiffrer. Il pourra ensuite utiliser à son tour l'accès correspondant (en disposant aussi du nom du compte). | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

[20] (Cole, Fossen, Northcutt, Pomeranz, p.1237)
[21] (Cole, Fossen, Northcutt, Pomeranz, p.1237)

| | | | | |
|---|---|---|---|---|
| AUTHENTIFICATION | N° 7 | En cas de réponse négative à la question n°4 : l'utilisateur a-t-il la possibilité de pré-enregistrer ses informations d'identification et d'authentification (nom d'usager et mot de passe) ? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | NON<br>A titre de justification :<br>En accord avec le State Data Security Executive order 01.01.1983.18 , les logiciels applicatifs ne doivent pas être configurés pour se « souvenir » des numéros de téléphone des modems réseau ou des mots de passe d'accès réseau (par exemple sur l'écran Windows de connexion réseau modem, l'option "Se souvenir du not de passe" ne doit pas être sélectionnée). [22] | | |
| | Réponse fournie | | | |
| | Menace associée | Si cette fonctionnalité est offerte, l'utilisateur pourrait être tenté de l'utiliser. Or, si ces informations d'accès étaient enregistrées n'importe quel individu malveillant parvenant à s'installer devant le système client pourrait activer sans difficulté la solution d'accès. | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

| | | | | |
|---|---|---|---|---|
| AUTHENTIFICATION | N° 8 | En cas de réponse négative à la question n°4 : la solution d'accès distant dispose-t-elle d'un système d'authentification personnel? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI | Réponse fournie | |
| | Menace associée | Si la solution d'accès distant ne dispose pas d'un système d'authentification personnel et utilise celui d'un autre système existant (ex. : le système interne bureautique), un individu qui parviendrait à voler le mot de passe d'un des employés de l'entreprise (disposant aussi d'un droit d'accès distant) pourrait par la suite accéder n'importe quand et de n'importe où au réseau de l'entreprise, sans qu'il ne soit facile de le repérer. | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

[22] (Maryland Department of Health and Mental Hygiene)

| | | | | |
|---|---|---|---|---|
| AUTHENTIFICATION | N° 9 | Est-il possible d'utiliser un système de restriction des adresses IP sources ? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI | Réponse fournie | |
| | Menace associée | Sans cela, n'importe quel individu possédant un accès Internet/téléphonique (et éventuellement l'application « cliente » correspondante) pourrait tenter de se connecter au système d'accès à distance (et deviner ensuite un nom de compte et un mot de passe valides pour entrer sur le LAN/WAN de l'entreprise).<br>Il est toutefois à noter que cette solution de restriction des adresses IP sources n'est pas toujours applicable, comme par exemple lorsque les utilisateurs ont besoin de se connecter de n'importe où (par exemple, aussi bien de chez eux que d'un hôtel). | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

| | | | | |
|---|---|---|---|---|
| AUTHENTIFICATION | N° 10 | Pour activer l'application, l'utilisateur doit-il fournir un nom d'utilisateur ? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI<br>A titre de justification :<br>En effet, l'authentification et l'autorisation sont les deux faces de la même médaille. D'un côté, vous ne pouvez pas autoriser l'accès à un objet si vous ne savez pas qui est la personne qui demande cet accès, et vous ne pouvez pas savoir qui est cette personne sans l'avoir préalablement authentifié.[23] | | |
| | Réponse fournie | | | |
| | Menace associée | Si l'utilisateur n'a pas besoin de fournir beaucoup d'informations pour activer l'application d'accès à distance, un individu malveillant aura moins d'effort à fournir pour l'activer lui aussi (et ainsi accéder sans autorisation au réseau de l'entreprise). | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

[23] (Cole, Fossen, Northcutt, Pomeranz, p.1177)

| | | |
|---|---|---|
| AUTHENTIFICATION | N° 11 | Pour activer l'application, l'utilisateur est-il contraint de ne pas dépasser un nombre maximum d'erreurs d'authentification (sous peine de perdre temporairement la possibilité de s'authentifier auprès de l'application) ? |
| | Élément à vérifier | |
| | Réponse souhaitée | OUI<br>A titre de justification :<br>Si un pirate informatique tente d'utiliser un programme qui permet de deviner un mot de passe, alors les comptes devraient être bloqués de façon temporaire pour empêcher que de trop nombreux essais ne soient effectués. [24] |
| | Réponse fournie | |
| | Menace associée | Sans ce mécanisme un individu malveillant pourra facilement tenter une attaque de force brutale (« brute force ») sur le mot de passe (en essayant toutes les combinaisons possibles ), et ce sans être importuné. |
| | Conséquence | Probabilité |
| | Risque | |

| | | |
|---|---|---|
| AUTHENTIFICATION | N° 12 | Un système de délai ("time-out") est-il disponible pour couper la communication après un certain temps d'inactivité ? |
| | Élément à vérifier | |
| | Réponse souhaitée | OUI<br>A titre de justification :<br>Pour diminuer l'exposition du réseau de l'entreprise, les utilisateurs d'un VPN devraient être empêchés d'ouvrir une session VPN vers le réseau de leur bureau, puis de la laisser active. Ceci est particulièrement important pour les utilisateurs distants qui se connectent via un accès Internet, en raison de la nature continuellement active de la connexion. La politique de sécurité devrait adresser le problème du temps de connexion aux sessions VPN des clients VPN, et imposer qu'une session soit coupée après qu'une certaine période prédéterminée de temps d'inactivité se soit écoulée.[25] |
| | Réponse fournie | |
| | Menace associée | Dans le cas contraire, si l'utilisateur laissait son système d'accès sans surveillance un long moment et sans couper sa connexion distante, un individu malveillant pourrait s'en emparer et utiliser sans autorisation cette connexion encore active pour pénétrer sur le réseau de l'entreprise |
| | Conséquence | Probabilité |
| | Risque | |

[24] (Cole, Fossen, Northcutt, Pomeranz, p.1238)
[25] (Stines)

## 4.2 Analyse de la section « partie transport »

a. Transport via des câbles

| | | |
|---|---|---|
| CHIFFREMENT DES DONNÉES | N° 13 | Une fonctionnalité de chiffrement des données en transit est-elle disponible ? |
| | Élément à vérifier | |
| | Réponse souhaitée | OUI<br>A titre de justification :<br>La cryptographie est une question vitale pour la sécurité de l'information. Une des principaux objectifs de la cryptographie est d'aider à se protéger des personnes qui cherchent à écouter le trafic réseau. L'idée est que communiquer, quelque soit le type de média utilisé, présente le risque inhérent qu'une tierce partie non autorisée puisse écouter la communication, et nous voulons miniser ce risque. Donc, dans sa forme la plus basique, la cryptographie déforme du texte d'une façon telle qu'aucune personne interceptant le message ne pourra le comprendre. [26] |
| | Réponse fournie | |
| | Menace associée | Si aucune solution de chiffrement n'est en place, un individu malveillant pourrait capturer et/ou modifier les informations en transit entre l'utilisateur et le réseau de l'entreprise. |
| | Conséquence | Probabilité |
| | Risque | |

[26] (Cole, Fossen, Northcutt, Pomeranz, p.884)

| | | | | |
|---|---|---|---|---|
| CHIFFREMENT DES DONNÉES | N° 14 | Si la réponse à la question n°13 est positive : le système de chiffrement en place fait-il appel à un système à clefs publiques (au minimum lors des phases initiales de communication, pour l'échange d'une clef privée) ? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI<br>A titre de justification : « Cela étant dit, le plus gros problème avec les clefs privées est lié à la gestion de leur création et de leur échange afin d'éviter qu'elles ne soient compromises. » [27]<br>« Les problèmes de gestion associés avec les clefs symétriques sont tellement accablants qu'ils excluent virtuellement d'eux-mêmes leur utilisation dans le domaine des échanges commerciaux. » [28] | | |
| | Réponse fournie | | | |
| | Menace associée | Si le système utilise uniquement un système à clef privée (clé unique), un individu malveillant pourrait parvenir à s'en emparer lors du processus initial obligatoire d'échange et rendre ainsi inutile tout le système de chiffrement utilisé par la suite. | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

| | | | | |
|---|---|---|---|---|
| CHIFFREMENT DES DONNÉES | N° 15 | Si la réponse à la question n°13 est positive : la clef de chiffrement utilisée est-elle d'une longueur officiellement et publiquement reconnue comme sécuritaire ? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI | Réponse fournie | |
| | Menace associée | Avec certaines longueurs de clef (ex : 56 bits), il est techniquement possible pour un individu malveillant de décoder dans un délai raisonnable le message chiffré. | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

[27] (Cole, Fossen, Northcutt, Pomeranz, p. 913)
[28] (Cole, Fossen, Northcutt, Pomeranz, p. 914)

| | | | | |
|---|---|---|---|---|
| CHIFFREMENT DES DONNÉES | N° 16 | Parmi les algorithmes de chiffrement qui peuvent être utilisés, en existe-t-il au moins un qui soit officiellement et publiquement reconnu comme étant un algorithme rendant réellement tout message intercepté indéchiffrable (dans un délai raisonnable)? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI | Réponse fournie | |
| | Menace associée | Lorsque certains algorithmes de chiffrement, désormais qualifiés de faibles, sont utilisés, un individu malveillant qui voudrait déchiffrer les données en transit pourrait y parvenir dans un délai raisonnable (ex : DES). | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

| | | | | |
|---|---|---|---|---|
| CHIFFREMENT DES DONNÉES | N° 17 | L'algorithme utilisé par le fabricant pour créer la fonction de chiffrement fait-il appel à des technologies standards reconnues (plutôt que développé à l'interne) ? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI<br>A titre de justification :<br>Ne croyez jamais dans un algorithme cryptographique secret ou propriétaire (même si vous travaillez pour la National Security Agency américaine). L'algorithme pourrait être éventuellement découvert, et puisque le fait de découvrir un algorithme rend très facile le fait de déchiffrer un message sans connaître la clef appropriée, toutes les communications chiffrées avec cet algorithme seraient compromises. [29] | | |
| | Réponse fournie | | | |
| | Menace associée | S'il n'a pas été auparavant publié et testé par de nombreux experts internationaux en cryptographie, rien n'assure que le code développé en interne ne contient pas de très nombreuses failles de sécurité. Or, dans ce cas là, tout le système de chiffrement ne servirait à rien et les données sensées être protégées pourraient être facilement exposées. | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

[29] (Cole, Fossen, Northcutt, Pomeranz, p.889)

b. Transport via une technologie sans-fil

| | | |
|---|---|---|
| CHIFFREMENT DES DONNÉES | N° 18 | Une solution WEP (au minimum) peut-elle être activée pour chiffrer les communications lors de leur transport ? |
| | Élément à vérifier | |
| | Réponse souhaitée | OUI<br>A titre de justification :<br>L'écoute électronique est très facile dans un environnement sans fil fréquence radio. Les données envoyées via le chemin des ondes radio peuvent être interceptées par n'importe qui équipé d'un système conçu à cet effet et qui écoute sur la même fréquence.[30]<br><br>Wired Equivalent Privacy, ou WEP, a été conçu dans le but d'empêcher l'écoute électronique et les accès non autorisés à un réseau sans fil. Il fonctionne en utilisant une clef secrète pour chiffrer les paquets entre un point d'accès et un équipement sans fil. De plus, un contrôle d'intégrité est effectué pour s'assurer que les données n'ont pas été modifiées en transit. [31] |
| | Réponse fournie | |
| | Menace associée | Si aucune solution de chiffrement n'est en place, un individu malveillant pourrait sans effort capturer les informations en transit entre l'utilisateur et le réseau de l'entreprise. |
| | Conséquence | Probabilité |
| | Risque | |

| | | |
|---|---|---|
| CHIFFREMENT DES DONNÉES | N° 19 | Les adresses MAC des systèmes pouvant utiliser le lien sans fil peuvent-elles être restreintes ? |
| | Élément à vérifier | |
| | Réponse souhaitée | OUI<br>A titre de justification :<br>« En général, c'est une bonne idée de configurer un réseau en utilisant une authentification basée sur les adresse MAC, un chiffrement WEP et des SSID silencieux . » |
| | Réponse fournie | |
| | Menace associée | Dans le cas contraire, un individu non autorisé pourrait utiliser sans problème son propre système pour tenter d'accéder à distance via le lien sans fil au réseau LAN/WAN de l'entreprise. |
| | Conséquence | Probabilité |
| | Risque | |

[30] (Cole, Fossen, Northcutt, Pomeranz,A-40)
[31] (Cole, Fossen, Northcutt, Pomeranz,A-59)

| | | | | |
|---|---|---|---|---|
| AUTHENTIFICATION | N° 20 | La fonctionnalité de « broadcast » SSID peut-elle être désactivée ? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI<br>A titre de justification :<br>Le SSID est un identifiant attaché à tous les paquets qui traversent le réseau local sans fil. Le SSID fonctionne comme un mot de passe nécessaire pour rejoindre le réseau local sans fil. Les SSID sont généralement diffusés de façon généralisée par les points d'accès et ne devraient pas être considérés comme « secrets ». [32]<br><br>Configurer le point d'accès pour qu'il ne diffuse pas le SSID. Ceci permet de désactiver le signal balise du point d'accès et de le configurer pour ignorer les requêtes anonymes pour un SSID. [33] | | |
| | Réponse fournie | | | |
| | Menace associée | Si le numéro de SSID est librement diffusé par le point d'accès un utilisateur non autorisé pourrait s'en emparer pour s'associer librement à ce point d'accès et tenter ensuite de l'utiliser pour entrer sur le réseau de l'organisation en arrière. | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

### 4.3 Analyse de la section « système d'accès »

| | | | | |
|---|---|---|---|---|
| FAILLES DE SÉCURITÉ | N° 21 | Parmi les failles de sécurité qui ont été découvertes sur la partie « système d'accès» de l'application, certaines sont-elles encore non résolues ? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | NON | Réponse fournie | |
| | Menace associée | S'il existe des failles de sécurité non résolues cela signifie :<br>- Qu'un individu malveillant a techniquement la possibilité d'attaquer à tout moment le serveur disposant de la partie « système d'accès ».<br>- Que le fournisseur de cette solution cliente ne prête peut-être pas une grande attention à la sécurité inhérente à son produit. Ce qui pourrait laisser penser que d'autres failles de sécurité non résolues ou tardivement résolues pourraient venir affecter la solution. | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

[32] (Cole, Fossen, Northcutt, Pomeranz, p. A-58)
[33] (Cole, Fossen, Northcutt, Pomeranz, p. A-63)

| | | |
|---|---|---|
| ADMINISTRATION CENTRALISÉE | N° 22 | Une fonctionnalité d'audit est-elle disponible pour étudier l'utilisation qui est faite de la solution d'accès (idéalement en temps réel ) ? |
| | Élément à vérifier | |
| | Réponse souhaitée | OUI<br>A titre de justification :<br>Surveillez les tentatives de connexion infructueuses et les connexions réussies durant des heures d'affaire inhabituelles. […] Si votre équipement pour les connexions modem offre cette possibilité, vous devriez conserver un journal d'activités de tous les numéros d'identification des appelants ainsi que du nom d'utilisateur de l'appelant, de l'heure de connexion, et de la durée de connexion. [34] |
| | Réponse fournie | |
| | Menace associée | S'il n'est pas possible de savoir ce que font les utilisateurs lorsqu'ils accèdent à distance au réseau de l'entreprise :<br>- Ils pourraient effectuer des actions en désaccord avec les consignes de sécurité mises en place dans l'organisation (sans que l'administrateur ne puisse le savoir);<br>- Des usurpations d'identité pourraient être commises (sans que l'administrateur ne puisse le savoir); |
| | Conséquence | Probabilité |
| | Risque | |

| | | | | |
|---|---|---|---|---|
| ADMINISTRATION CENTRALISÉE | N° 23 | Le mécanisme d'audit permet-il de différencier les actions de chacun des utilisateurs ? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI | Réponse fournie | |
| | Menace associée | Dans le cas contraire, si des d'opérations illicites étaient effectuées sur ou via le système d'accès, il serait impossible de savoir quel est l'utilisateur qui en est responsable (ou au minimum à quel compte associer ces opérations, en cas d'usurpation d'identité). | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

[34] (Stasiak)

| | | | | |
|---|---|---|---|---|
| ADMINISTRATION CENTRALISÉE | N° 24 | Est-il possible de configurer une liste d'événements dont l'apparition déclencherait une alerte pouvant être envoyée dans l'instant à un administrateur (ex : via pagette)? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI | Réponse fournie | |
| | Menace associée | Dans le cas contraire, l'organisation ne pourrait pas réagir rapidement en cas d'apparition d'un incident de sécurité (ex : tentative d'utilisation de commandes illicites). | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

| | | | | |
|---|---|---|---|---|
| AUTHENTIFICATION | N° 25 | L'accès à la console d'administration est-il protégé par : une authentification à deux facteurs ou au moins un nom d'utilisateur ainsi qu'un mot de passe complexe (8 caractères, avec lettres, chiffres et caractères complexes), à changer régulièrement, un mécanisme pour couper le processus d'authentification après un certain nombre d'erreurs d'authentification ou un certain délai d'inactivité et, si la console peut être accédée à distance, un canal chiffré (ex : accès https pour une interface web)? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI<br>A titre de justification :<br>La condition la plus basique en matière de sécurité web est probablement la confidentialité des communications. C'est à dire que des tierces parties ne devraient pas pouvoir capturer le trafic généré par une conversation entre les navigateurs et les serveurs.[35]<br>Pour la justification des autres points, voir les grilles n° 4, 5, 6, 10, 11 et 12. | | |
| | Réponse fournie | | | |
| | Menace associée | Si jamais la communication n'est pas chiffrée ou que le processus d'authentification est faible, il serait très facile pour un individu non autorisé d'espionner la communication ou de tenter de deviner le mot de passe d'accès. | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

[35] (Cole, Fossen, Northcutt, Pomeranz, p. 551)

| | | | | |
|---|---|---|---|---|
| AUTHENTIFICATION | N° 26 | S'il existe plusieurs administrateurs de la solution, peuvent-ils tous disposer d'un compte personnalisé? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI | Réponse fournie | |
| | Menace associée | Dans le cas contraire, un des administrateurs pourrait effectuer des opérations illégitimes sans qu'il ne soit possible de lui attribuer personnellement ces actions. | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

| | | | | |
|---|---|---|---|---|
| COMPOSANTES | N° 27 | Si le serveur a besoin pour fonctionner d'une composante/logiciel tierce (ex : serveur web, tel que « IIS ») : le fabricant a-t-il pris soin de fournir une version bastionnée de cette composante ? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI | Réponse fournie | |
| | Menace associée | Dans le cas contraire, le travail de bastionnage :<br>- Ne sera jamais fait;<br>- Sera fait à l'interne, par l'entreprise qui met en place la solution d'accès. Or, puisque que cette dernière ne dispose pas toujours de l'expertise technique nécessaire pour effectuer un tel travail ou de suffisamment d'informations sur le fonctionnement de l'application d'accès à distance, il se pourrait que le travail de bastionnage ne soit pas effectué de façon satisfaisante;<br>Dans les deux cas, ceci signifie que toute la sécurité mise en place au niveau de l'application pourrait être contrecarrée par la conservation d'une faille de sécurité dans une des composantes tierces. | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

| | | | | |
|---|---|---|---|---|
| COMPOSANTES | N° 28 | En cas de réponse positive à la question 27 : ce travail de bastionnage a-t-il été validé par une organisation tierce reconnue ? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI | Réponse fournie | |
| | Menace associée | En l'absence de certification par une organisation tierce experte dans ce genre d'activités, il se peut que le travail de bastionnage ait été mal effectué et ne serve donc à rien. | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

| COMPOSANTES | | | | |
|---|---|---|---|---|
| | N° 29 | Un utilisateur normal a-t-il la possibilité d'accéder au système d'exploitation en arrière de la solution d'accès (par exemple via cette même solution d'accès à distance)? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | NON | Réponse fournie | |
| | Menace associée | S'il disposait d'un tel accès, il pourrait tenter de l'utiliser pour contourner ou reconfigurer les règles de sécurité/filtrage en place dans l'application. | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

| COMPOSANTES | | | | |
|---|---|---|---|---|
| | N° 30 | Avant de s'activer, l'application d'accès à distance peut-elle être configurée pour vérifier la pré-activation sur le système de l'utilisateur de certains éléments de sécurité additionnels (ex : un pare-feu personnel, un anti-virus)? | | |
| | Élément à vérifier | | | |
| | Réponse souhaitée | OUI | Réponse fournie | |
| | Menace associée | Dans le cas contraire, l'utilisateur pourrait alors accéder au réseau de son organisation avec un système dont le niveau général de sécurité n'est pas satisfaisant (ex : présence de cheveux de Troie, de vers, etc.) et éventuellement mettre en danger ce réseau. | | |
| | Conséquence | | Probabilité | |
| | Risque | | | |

## 5. LES MESURES COMPLÉMENTAIRES

Le travail d'analyse de sécurité propre à ce guide est à présent terminé. Toutefois, cette section est là pour rappeler qu'aussi sécuritaire qu'elle soit, une technologie est toujours implantée au sein d'un réseau et d'une organisation particulière. Ceci signifie que la technologie :

- Va être utilisée dans un réseau qui dispose déjà de forces mais aussi, vraisemblablement, de faiblesses de sécurité, dont certaines pourraient impacter le fonctionnement a priori sécuritaire de la nouvelle solution;
- Va être gérée en fonction des pratiques d'utilisation de l'organisation, qui pourraient, elles aussi, entraîner une baisse du niveau initial de sécurité de la nouvelle solution.

Par conséquent, lorsqu'une nouvelle technologie est implantée, il est important non seulement d'étudier son propre niveau de sécurité (d'où le rôle de ce guide d'analyse) mais aussi celui de l'environnement réseau au sein duquel elle sera implantée et des pratiques de gestion qui l'entoureront. L'obkectif est de s'assurer que ces éléments répondent eux aussi à de hauts standards de sécurité.
Car il ne faut pas oublier que « l'environnement d'un système informatique est aussi critique que son composant le plus critique et aussi vulnérable que son composant le plus vulnérable. » [36]

Donc, puisqu'il n'est pas souhaitable que ce guide donne l'illusion qu'une fois la sécurité propre à la solution d'accès étudiée, tout le travail de sécurité est fait, voici quelques exemples des éléments qui seraient à étudier dans un second temps (une fois la solution d'accès à distance sélectionnée) :

- Sécurité physique :
  - L'accès physique aux locaux hébergeant les équipements impliqués dans la solution d'accès à distance a-t-il été sécurisé?
  - L'accès physique aux équipements impliqués dans la solution d'accès à distance a-t-il été sécurisé?
- Sécurité logique :
  - Tous les logiciels impliqués dans la solution d'accès à distance pourront-ils être continuellement tenus à jour (ex : le système d'exploitation) ?
  - Concernant la partie cliente :
    - Que la solution soit installée sur un poste de travail ou un équipement de type « palm », une solution de pare-feu personnelle est-elle en place (lorsque techniquement faisable) ?
    - L'utilisateur peut-il modifier la configuration de son pare-feu?

[36] (North American Electric Reliability Council)

- Le « split-tunneling » est-il bloqué ?
- La partie cliente est-elle protégée par un anti-virus à jour ?
- La sécurité du système d'exploitation du poste de travail a-t-elle été renforcée ?

- Concernant l'entrée sur le réseau local de l'entreprise :
  - Un équipement spécialisé de filtrage a-t-il été mis en place (ex : un pare-feu) ?
  - Ce dernier a-t-il été configuré de la façon la plus restrictive possible ?
- Concernant la partie serveur :
  - Le système supportant l'application d'accès à distance a-t-il été installé sur une portion appropriée du réseau (dans le réseau local ? dans une DMZ ? directement sur l'Internet ?)
  - Le serveur est-il protégé par un anti-virus à jour ?
  - Le serveur est-il dédié à la gestion de l'accès à distance ou supporte-t-il d'autres applications et fonctions ?

- Gestion de la sécurité :
  - Un responsable de cette solution d'accès à distance a-t-il été désigné?
  - Les administrateurs réseau devant travailler avec cette solution ont-ils reçu une formation adéquate (y compris sur les aspects de gestion sécuritaire) ?
  - Sont-ils rapidement informés de toutes les nouvelles failles de sécurité pouvant impacter un des éléments de la solution d'accès à distance ?
  - Un ensemble de procédures et politiques régulant l'utilisation au sein de l'entreprise de la solution d'accès à distance est-il en place ?
  - Un ensemble de procédures définissant les mesures d'installation et de maintenance de la solution d'accès à distance est-il en place (ex : configuration initiale standard des parties client et serveur, gestion des mises à jour, des sauvegardes, fréquence de vérification des logs, des audit de la configuration, etc.).
  - Les utilisateurs ont-ils été sensibilisés aux bonnes et mauvaises pratiques de sécurité propres à l'utilisation de cette technologie d'accès à distance ?

## CONCLUSION

Actuellement, les besoins d'accès à distance aux réseaux LAN/WAN des organisations sont de plus en plus importants et variés. Mais il n'est pas toujours facile pour un gestionnaire qui a la charge de sélectionner la technologie à implanter de savoir si cette dernière possède tous les éléments de sécurité informatique nécessaires, afin de ne pas mettre en danger le réseau interne ainsi accédé.
Donc, ce présent guide est fourni comme un outil de support à la décision : il est là pour aider le gestionnaire à se poser les bonnes questions et évaluer adéquatement le niveau de sécurité offert dans certaines des solutions d'accès à distance.

Toutefois, comme cela est précisé un peu plus haut, entre l'étape de sélection du produit d'accès à distance et son implantation définitive et fonctionnelle au sein d'une entreprise, de nombreuses autres tâches de sécurité devront être effectuées (ex : définition des processus de gestion et de séparation des pouvoirs, mise en place d'une architecture réseau sécuritaire, attribution rigoureuse des droits d'accès, etc.). Car la sécurité d'une entreprise ne repose pas uniquement sur l'utilisation de quelques produits, mais plutôt sur la mise en place de tout un ensemble de composantes organisationnelles, opérationnelles et techniques permettant à une organisation de prévenir, surveiller et réagir de façon optimale à tous les risques liés à l'utilisation de technologies informatiques.

Malheureusement, de nombreuses organisations ne se sont pas encore penchées sur ces aspects. J'espère alors que le bref aperçu que j'ai pu donner à travers ce document des différents éléments de sécurité à prendre en compte dans l'étude d'une simple solution d'accès à distance apportera sa pierre au travail de sensibilisation en matière de sécurité informatique et aidera les organisation à s'assurer que les processus et outils qu'elles utilisent leur permettent de toujours traiter les questions de sécurité avec toute la rigueur nécessaire.

## RÉFÉRENCES


[1] AT&T. « Remote working in the Net-Centric Organization ». 14 juillet 2003. URL:http://www.business.att.com/content/whitepaper/remote_working_net-centric_org.pdf

[2] Fiutak, Martin. « Teleworking on the increase in Europe ». 8 octobre 2002 http://news.zdnet.co.uk/business/management/0,39020654,2123557,00.htm

[3] Vachon, Isabelle. « Le travail parmi les tendances 2003 ». 31 janvier 2003 http://www.infometre.cefrio.qc.ca/loupe/sistech/0103.asp#8

[4] Gaudin, Sharon. « Study shows security market doubling by 2006 ». 6 février 2003
http://itmanagement.earthweb.com/secu/article.php/1580541

[5] Tsai, Wei-Tek. « Risk-based testing ».
http://asusrl.eas.asu.edu/est/content/statistic/Risk-basedTesting.pdf

[6] Office québécois de la langue française. « Le grand dictionnaire terminologique ». 1997.
http://www.granddictionnaire.com/btml/fra/r_motclef/index1024_1.asp

[7] Robert, Paul. Dictionnaire alphabétique et analogique de la langue Française, tome cinquième. Paris : Société du nouveau littré, 1966. 472

[8] Le Petit Larousse Illustré en Couleur. Tournai : Larousse. 1995. 261

[9] Office québécois de la langue française. « Le grand dictionnaire terminologique ». 1997.
http://www.granddictionnaire.com/btml/fra/r_motclef/index1024_1.asp

[10] Steinberg, Joseph. « SSL VPN security : secure remote access from any web browser ». 16 mai 2003.
http://www.sans.org/rr/papers/20/whale.php

[11] Stines, Michael. « Remote Access VPN – Security concerns and policy enforcement ». 2003.
http://www.giac.org/practical/GSEC/Mike_Stines_GSEC.pdf

[12] Stines, Michael. « Remote Access VPN – Security concerns and policy enforcement ». 2003.
http://www.giac.org/practical/GSEC/Mike_Stines_GSEC.pdf

[13] North American Electric Reliability Council. « Security guidelines for the electricity sector : securing remote access to electronic control and protection systems ». Version 1.0. 10 juin 2003
http://www.esisac.com/publicdocs/Guides/secguide_pcs_final.pdf

[14] Steinberg, Joseph. « SSL VPN security : secure remote access from any web browser ». 16 mai 2003. http://www.sans.org/rr/papers/20/whale.php

[15] Office québécois de la langue française. « Le grand dictionnaire terminologique ». 2003.
http://www.granddictionnaire.com/btml/fra/r_motclef/index1024_1.asp

[16] SANS Institute. Track 7 – Auditing networks, perimeters and systems, volume « 7.2 Auditing the perimeters : auditing networks and firewalls », version 1.0. 2002. 39.

[17] Anderson, Gary. Baccam, Tanya. Grill, Bob. Grundschober, Stéphane. Madeiros, Steve. Meshram, Tapan. Schaller, Jeff. « GNSA Study Guide ». 18 juillet 2003. http://www.giac.org/gsna_study_guide_v12.pdf

[18] Information Systems Audit and Control Association. « Use of risk assessment in Audit Planning ». Document # 050.010.030. 2000
http://www.isaca.org/Template.cfm?Section=Standards,_Guidelines_and_Procedures1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=6587

[19] Steinberg, Joseph. « SSL VPN security : secure remote access from any web browser ». 16 mai 2003.
http://www.sans.org/rr/papers/20/whale.php

[20] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security essentials with CISSP CBK, version 2.1, volume two. United States of America : Sans Press. Février 2003. 1237

[21] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security essentials with CISSP CBK, version 2.1, volume two. United States of America : Sans Press. Février 2003 1237

[22] Maryland Department of Health and Mental Hygiene. « Standard operating procedures (SOPs) for the use of laptops/portables & off-site data processing equipment ». Version 1. Mars 1999.
http://www.dhmh.state.md.us/policies/laptop.htm

[23] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security essentials with CISSP CBK, version 2.1, volume two. United States of America : Sans Press. Février 2003.1177

[24] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security essentials with CISSP CBK, version 2.1, volume two. United States of America : Sans Press. Février 2003.1238

[25] Stines, Michael. « Remote Access VPN – Security concerns and policy enforcement ». 2003.
http://www.giac.org/practical/GSEC/Mike_Stines_GSEC.pdf

[26] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security essentials with CISSP CBK, version 2.1, volume two. United States of America : Sans Press. Février 2003. 884

[27] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security essentials with CISSP CBK, version 2.1, volume two. United States of America : Sans Press. Février 2003. 913

[28] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security essentials with CISSP CBK, version 2.1, volume two. United States of America : Sans Press. Février 2003. 914

[29] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security essentials with CISSP CBK, version 2.1, volume two. United States of America : Sans Press. Février 2003. 889

[30] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security essentials with CISSP CBK, version 2.1, volume two. United States of America : Sans Press. Février 2003. A-40

[31] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security essentials with CISSP CBK, version 2.1, volume two. United States of America : Sans Press. Février 2003. A-59

[32] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security essentials with CISSP CBK, version 2.1, volume two. United States of America : Sans Press. Février 2003. A-58

[33] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security essentials with CISSP CBK, version 2.1, volume two. United States of America : Sans Press. Février 2003. A-63

[34] Stasiak, Ken. « Remote access white paper ». 2001.
http://www.sans.org/rr/paper.php?id=476

[35] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security essentials with CISSP CBK, version 2.1, volume two. United States of America : Sans Press. Février 2003. 551

[36] North American Electric Reliability Council. « Security guidelines for the electricity sector : securing remote access to electronic control and protection systems ». Version 1.0. 10 juin 2003
http://www.esisac.com/publicdocs/Guides/secguide_pcs_final.pdf

Last Updated: May 28th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Stockholm 2017 | Stockholm, Sweden | May 29, 2017 - Jun 03, 2017 | Live Event |
| SANS San Francisco Summer 2017 | San Francisco, CA | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| SANS Houston 2017 | Houston, TX | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Security Operations Center Summit & Training | Washington, DC | Jun 05, 2017 - Jun 12, 2017 | Live Event |
| Community SANS Ottawa SEC401 | Ottawa, ON | Jun 05, 2017 - Jun 10, 2017 | Community SANS |
| SANS Charlotte 2017 | Charlotte, NC | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | vLive |
| Community SANS Portland SEC401 | Portland, OR | Jun 12, 2017 - Jun 17, 2017 | Community SANS |
| SANS Secure Europe 2017 | Amsterdam, Netherlands | Jun 12, 2017 - Jun 20, 2017 | Live Event |
| SANS Rocky Mountain 2017 | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Minneapolis 2017 | Minneapolis, MN | Jun 19, 2017 - Jun 24, 2017 | Live Event |
| SANS Columbia, MD 2017 | Columbia, MD | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Cyber Defence Canberra 2017 | Canberra, Australia | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| SANS Paris 2017 | Paris, France | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS London July 2017 | London, United Kingdom | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| Cyber Defence Japan 2017 | Tokyo, Japan | Jul 05, 2017 - Jul 15, 2017 | Live Event |
| SANS Cyber Defence Singapore 2017 | Singapore, Singapore | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Minneapolis SEC401 | Minneapolis, MN | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Los Angeles - Long Beach 2017 | Long Beach, CA | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Phoenix SEC401 | Phoenix, AZ | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Munich Summer 2017 | Munich, Germany | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Mentor Session - SEC401 | Ventura, CA | Jul 12, 2017 - Sep 13, 2017 | Mentor |
| Mentor Session - SEC401 | Macon, GA | Jul 12, 2017 - Aug 23, 2017 | Mentor |
| Community SANS Atlanta SEC401 | Atlanta, GA | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| Community SANS Colorado Springs SEC401 | Colorado Springs, CO | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style | Washington, DC | Jul 24, 2017 - Jul 29, 2017 | vLive |
| Community SANS Charleston SEC401 | Charleston, SC | Jul 24, 2017 - Jul 29, 2017 | Community SANS |
| Community SANS Fort Lauderdale SEC401 | Fort Lauderdale, FL | Jul 31, 2017 - Aug 05, 2017 | Community SANS |
| SANS San Antonio 2017 | San Antonio, TX | Aug 06, 2017 - Aug 11, 2017 | Live Event |
| SANS Prague 2017 | Prague, Czech Republic | Aug 07, 2017 - Aug 12, 2017 | Live Event |