Guide sur la Cybercriminalité

Perplexe face à la Cybercriminalité ? Alors, sans attendre, procurez-vous ce guide de l'Exera. Il vous fera toucher du doigt les dangers potentiels et surtout vous aidera à mieux définir les parades.

L'Exera fait partie des trop rares associations dans le monde industriel à avoir des commissions prolifiques. L'une d'elles, la Commission Technique Automates Programmables et Superviseurs, vient, assistée de l'Institut Prisme, de publier un Guide sur la cybercriminalité, qui est une sorte d'introduction et une sensibilisation aux risques « informatiques » dans les systèmes de contrôle/commande.

Il présente différents risques « informatiques » encourus sur un système de contrôle/commande. Pour une grande majorité, ces risques sont issus de l'introduction dans le monde du contrôle/commande de l'informatique de traitement « grand public » en particulier par le biais de l'ouverture « TCP/IP » et du rapprochement vers le système d'information de l'entreprise.

Seulement, les solutions proposées pour l'informatique de traitement ne conviennent pas ou ne s'appliquent pas directement au monde du contrôle/commande. Ce Guide y pallie et propose quelques voies d'analyse des risques et quelques stratégies de défense.

Si le sujet vous paraît important, et, à l'heure des premiers virus qui infectent les systèmes de contrôle/commande, ce serait de l'inconscience de penser le contraire, procurez-vous ce Guide auprès de l'Exera. Il reste véritablement un document de référence. Nous l'avons lu en avant-première, et en exclusivité en voici quelques extraits - www.exera.com.

1. Exigences de performances différentes	
IT	**IC**
Non Temps Réel	Temps Réel
Réponse fiable	Temps de réponse critique
Messages longs & peu fréquents	Messages courts et fréquents
Délais de réponse acceptés	Délais de réponse critiques
Exemple : La mise en œuvre de procédés de chiffrement n'est pas généralisable en raison du temps de réponse requis en IC	
2. Besoins de disponibilité différents	
IT	**IC**
Exploitation programmée	Exploitation continue
Défaut occasionnel admis	Arrêt interdit
Beta test admis *in situ*	Test avant exploitation
Intervention sur appel « user »	Reconfiguration automatique

EXTRAITS

La cyber-sécurité

La majorité de l'industrie utilise de nos jours des moyens informatiques basés sur les systèmes d'exploitation communs tels que Windows ou Unix (à un degré moindre) ; ceci a été fait parce que l'utilisation des systèmes d'exploitation communs est rentable. Le développement et l'utilisation des normes fournissent le même coût pour des solutions sécuritaires. Développer des solutions uniques pour chaque compagnie est cher et rend l'interopérabilité et le partage d'information difficiles. Les constructeurs, en particulier, supportent fortement les normes, car celles-ci permettent à des constructeurs de développer les systèmes qui peuvent être déployés à tous les clients avec seulement des variations mineures de configuration. Ceci a comme conséquence des économies lors des études.

…

A l'exception des domaines critiques tels que le nucléaire, la pharmacie, l'agroalimentaire, la conduite des réseaux électriques, la distribution d'eau… la sensibilisation à la sécurité informatique reste faible. Alors que dans le domaine des Technologies de l'Information et de la Communication (TIC), la conscience des enjeux sécuritaires existe, dans le monde des automatismes cette conscience est faible.

Les systèmes actuels sont un mélange de technologies de l'information (IT) et de contrôle industriel (IC). Cependant, il existe plusieurs raisons pour ne pas appliquer aveuglément les techniques de l'informatique générale.

.....

Stratégie d'analyse et de défense

Le rapport ANSI/ISA-TR99.00.02–2004, propose une approche cohérente pour définir, mettre en œuvre et suivre l'exécution de programmes d'action relatifs à la cyber-sécurité dans les systèmes d'automatisme ou de contrôle des procédés.

Il s'adresse aux utilisateurs, fabricants, fournisseurs et responsables de la sécurité de tels systèmes.

Les trois points majeurs préconisés par ce rapport sont :

– identifier les risques et estimer les conséquences (risk analysis),

– mise en place d'un cycle de vie de la sécurité,

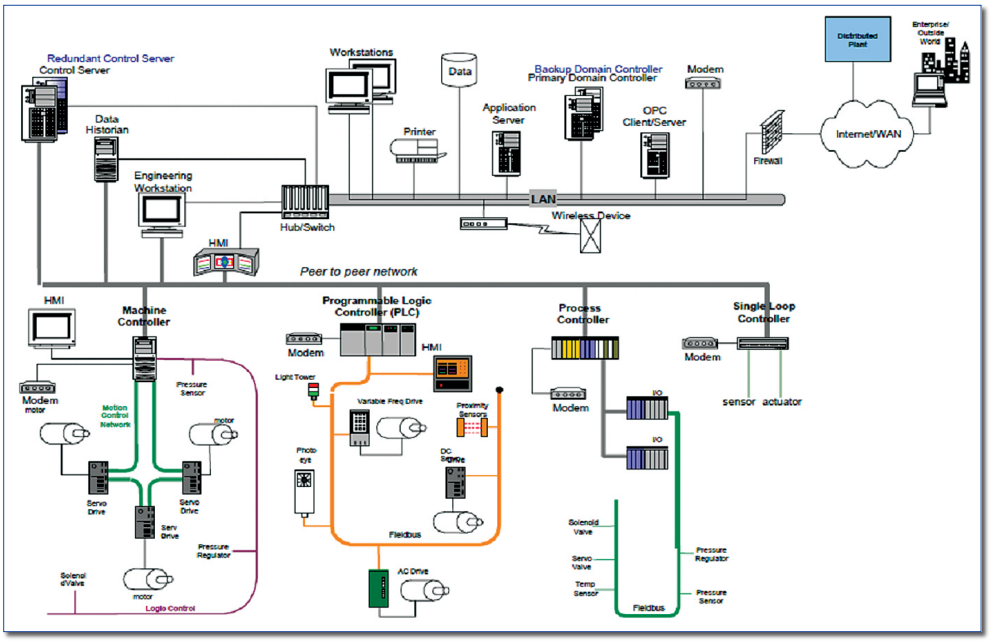


Figure 1 - Plan-type d'un système identifiant les connexions entre composants et les points d'ouverture externe.

– mise en place d'un processus de validation et de surveillance.

Le rapport formule des recommandations relativement indépendantes des technologies décrites dans le document précédent :
– Se tenir en permanence informé des évolutions technologiques et de l'état de l'art du marché,
– La sécurité est partout, de la conception à l'exploitation, et se superpose au cycle de vie du système (ou s'y intègre),
– La sécurité concerne tous les acteurs : donneurs d'ordres, exploitants, maîtres d'ouvrage, sous-traitants, sociétés de service.
…
Le document développe une proposition de méthode d'analyse basée sur l'examen physique de la structure du système et sur l'identification des points d'ouverture externe, ainsi que sur une évaluation quantitative de la probabilité du risque d'agression et du niveau de criticité des conséquences pouvant en résulter.
Il préconise par exemple d'établir un schéma détaillé du système mettant en évidence toutes les liaisons internes et externes entre équipements constitutifs (Figure 1).

.....

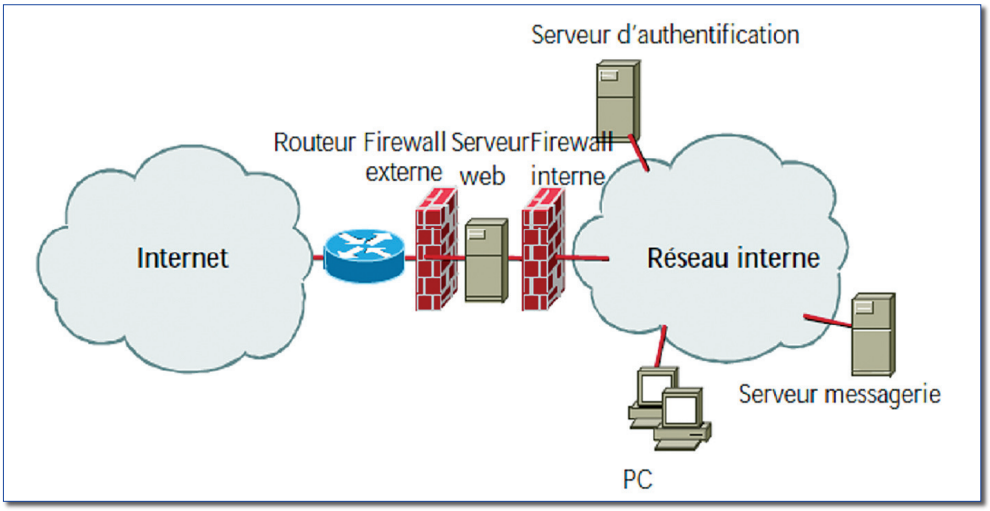
Les bonnes pratiques

Voilà encore quelques années, instaurer la sécurité c'était simplement installer un pare-feu. Mais même alors, c'était voir un peu juste. Pour établir un périmètre de sécurité, il ne suffit pas d'utiliser des pare-feux et de détecter des intrusions. Le pare-feu n'est qu'une composante du périmètre de sécurité, lequel n'est qu'un élément de la sécurité.
On a souvent besoin d'installer des services qui doivent communiquer directement avec le réseau extérieur et dans ces cas-là, un firewall pur et dur devient un vrai casse-tête. On parle alors de DMZ (Zone démilitarisée), sorte de purgatoire un peu protégé dans lequel les serveurs publics jouissent d'une relative sécurité derrière un barrage filtrant, mais non protégés par un firewall plus strict, dont le rôle reste de protéger la partie privée du réseau.
En fait, une DMZ est identique à une sécurité réseau IP classique à la différence qu'elle intègre, entre autres, un ou plusieurs serveurs applicatifs et la rupture protocolaire ; il s'agit en fait d'un deuxième réseau local. Une DMZ accentue les contrôles réseaux et applicatifs (qui ne sont pas les mêmes que dans la sécurité réseau IP classique). Le but est d'empêcher un hacker d'arriver à franchir le 2e niveau de sécurité ; des alertes seront déclenchées avant qu'il ne parvienne à ce niveau.
En aucun cas, un process initié par l'extérieur ne pourra écrire directement sur une machine du réseau « commande ». Par ce biais, une étanchéité optimale du réseau « commande » est définie et appliquée. La réciproque est également vraie (du réseau « commande » vers l'extérieur).

.....

Définition des zones de sécurité - Notion de « conduit »

Un « conduit » désigne une zone de sécurité spécifique à des moyens de communication entre



Architecture de sécurité avec double fortification pour serveur web.

éléments de l'architecture. Un conduit protège la sécurité des canaux de communication qu'il contient, comme un fourreau protège un câble. Conceptuellement analogues à des tuyaux contenant les moyens de communication, soit internes (à l'intérieur d'une zone), soit externes (avec l'extérieur).

Le plus souvent un conduit est matérialisé par un réseau de communication et les composants qui le supportent : connectique, câblage, routeurs, commutateurs, stations de gestion ou de maintenance du réseau… Les conduits peuvent regrouper des techniques de communication différentes et comporter plusieurs « canaux de communication » utilisant le même support physique (par exemple : sur un réseau de terrain peuvent cohabiter un trafic cyclique de données de contrôle de procédé et un ou plusieurs trafics de messagerie d'observation, configuration et réglage, chacun des canaux ayant des exigences et vulnérabilités différentes vis-à-vis de la sécurité).

.....

Bâtir un programme de gestion de la cyber-sécurité

Mettre en place un programme de gestion de la « cyber-sécurité » dans une entreprise n'est pas une tâche facile : Par où commencer ? Dites-moi ce que je dois faire ? sont les questions initiales les plus fréquemment posées. En raison du nombre important de contextes différents (système nouveau ou amélioration de systèmes existants, diversité et niveau de maturité des technologies et des intervenants), il n'existe malheureusement pas de recette unique. En fait, la réponse ne peut être que relative et doit s'intégrer dans la politique générale de l'entreprise. La sécurité parfaite est un idéal et une solution de compromis est à rechercher en considérant le coût du développement face au coût des conséquences des risques potentiels.

.....

Etablissement d'un système de gestion de la cyber-sécurité

Ce système constitue la structure d'accueil de l'ensemble de la politique et des actions collectives au niveau d'une société. Au fur et à mesure de la réalisation de ces actions le niveau de maturité de cyber-sécurité s'accroît. Le modèle « Plan-Do-Check-Act » est généralement adopté pour produire les résultats escomptés de sécurité de l'information. Les différentes actions sont :

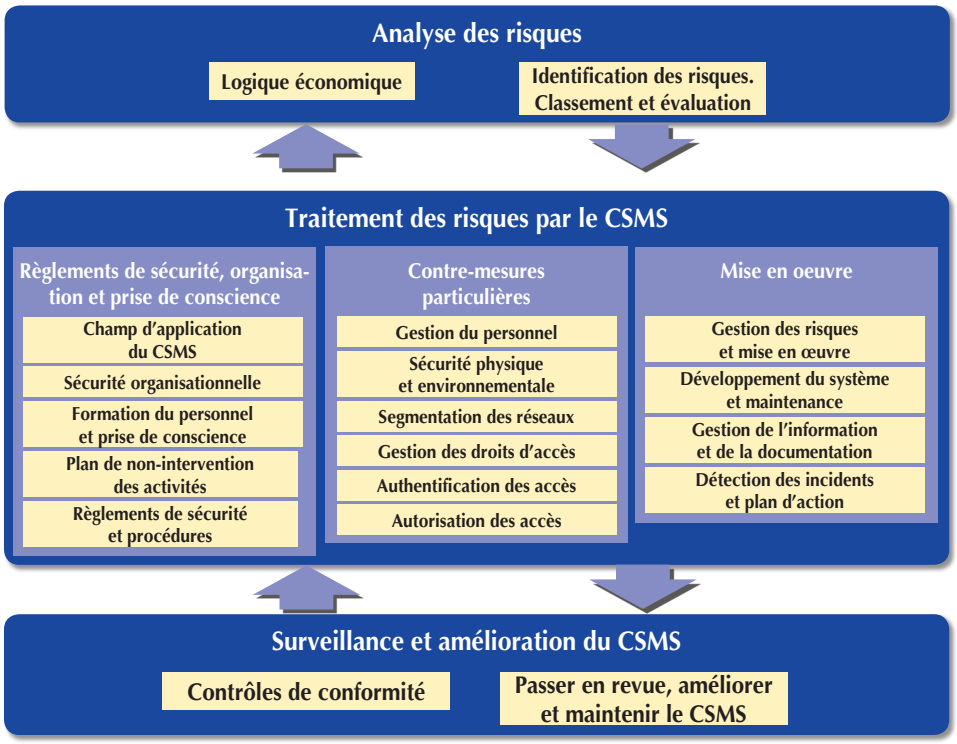
***Planification** : Etablissement des limites du système et de la politique de la société, identification, classification et évaluation des risques, développement d'un plan stratégique d'action continue.*

***Réalisation** : Mise en place, exploitation et maintenance du système, y compris l'organisation transversale, la sécurité physique, les contrôles d'accès, les procédures de traitement des incidents, la gestion des communications, de l'exploitation et de la documentation.*

***Vérification** : Surveillance, évaluation et mesures d'efficacité du système. Elaboration des rapports et revues périodiques de résultat.*

***Action** : Organisation des actions correctives et préventives. Réalisation des actions de maintenance et de maintien à niveau technologique. Ces dernières actions sont des actions permanentes pour maintenir le niveau de protection.*

Les différents éléments constitutifs d'un système de cyber-sécurité sont regroupés dans le shéma ci-contre.



Elément d'un CSMS.

.....

Certifications

Parce que la sécurité n'est plus aujourd'hui une option, beaucoup d'entreprises mettent en place leur système de cyber-sécurité. Pour s'assurer un niveau optimal de sécurité du système et de la bonne formation du personnel responsable de ce système de cyber-sécurité, un audit externe est nécessaire. Afin de pouvoir juger des éventuels écarts par rapport à une norme de cyber-sécurité, la certification s'impose. De plus, la certification est une garantie du maintien dans le temps du niveau de sécurité acquis. Elle fait l'objet d'un audit externe.

Actuellement, il existe de nombreuses certifications dans le domaine de la sécurité informatique. Par contre, dans le domaine de la cyber-sécurité des systèmes de contrôle/commande, peu de choses existent à ce jour. ■