



EDITORIAL

EDITORIAL	p1
AGENDA	p1
ACTUALITES	p2
ZOOM	p3
➤ La communication de crise	
L'ESSENTIEL	p5
➤ Le contrôle d'accès physique	
VEILLE	p7
➤ HDCP ou High Definition Content Protection	

Lutter contre le risque informatique, pragmatisme ou méthodologie ?

Le pragmatisme, qualité indéniable liée à la vision réaliste d'une situation est souvent opposé à une démarche plus rigoureuse basée sur une méthodologie. Dans la réalisation de projet, la perception de la réalité opérationnelle, pragmatique par essence, apporte un résultat probant en un minimum de temps.

Concernant la sécurité des systèmes d'information, le pragmatisme permet de prendre rapidement des actions face à une situation particulière de risque. Alors pourquoi se lancer dans une démarche méthodologique complexe lorsque l'utilisateur des moyens informatiques vous répond « j'ai besoin de tout, tout le temps » ou « je ne sais pas, ce n'est pas moi le spécialiste » ou encore « nous n'avons pas de budget pour ça, fait au mieux » ?

Les métiers de l'informatique, apportent les solutions nécessaires, les outils, aux acteurs cœur de métier de l'entreprise. Ce sont ces derniers les propriétaires de l'information gérée. Ils sont les seuls à connaître avec exactitude la valeur de leurs informations.

Sécuriser un réseau, mettre en place un plan de reprise d'activité sont des projets dont l'importance est liée à la valeur de l'information gérée. Est-il pragmatique de mettre en place un plan de reprise d'activité si celui ne répond ni au besoin métier, ni aux situations de risques pouvant survenir ? La qualité de gestion de la sécurité des systèmes d'information est directement liée à la maturité organisationnelle de l'entreprise. En effet, comment identifier les processus métiers critiques s'ils ne sont pas définis ? À défaut, la fonction sécurité informatique devra évaluer le degré de criticité de telle ou telle application, sans que la criticité des processus métiers supportés ne soit évaluée.

La gestion du risque informatique par une approche méthodologique gagne de plus en plus de terrain, le développement des diverses normes ISO et la disponibilité de nombreuses méthodes tel MEHARI, EBIOS parmi d'autres sont là pour en témoigner.

AGENDA

HACK.LU 2008 - 22 au 24 octobre 2008

Du 22 au 24 octobre 2008, se déroule la conférence annuelle Hack.lu. Dédiée à la sécurité informatique, elle présente les nouveaux vecteurs et techniques d'attaque.

➤ Plus d'infos : <http://hack.lu/index.php/hl/>

La Lutte Informatique Offensive, 3 février 2009 séminaire SOGETI.

La Lutte Informatique Offensive (LIO) porte sur les moyens d'attaquer les SI afin d'en prendre le contrôle, d'en extraire des informations confidentielles ou encore de les mettre hors d'état de fonctionner.

➤ Plus d'infos : <http://esec.fr>

Conférence SMSI et ISO 27001 - 23 octobre 2008

Après sa conférence sur les Plans de Continuités d'Activité de septembre, Le CLUSIF organise une nouvelle conférence sur les SMSI et la norme ISO 27001.

➤ Plus d'infos : <http://clusif.asso.fr>



ACTUALITÉS

Cyber surveillance du salarié

La Cyber surveillance du salarié dans l'entreprise est un sujet délicat. Un nouvel arrêté de la Cour de Cassation renforce les droits des employeurs. La Chambre sociale de la Cour de Cassation vient en effet de juger le 9 juillet 2008 que « les connexions établies par un salarié sur des sites Internet pendant son temps de travail grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail

sont présumées avoir un caractère professionnel, de sorte que l'employeur peut les rechercher aux fins de les identifier, hors de sa présence » : connexion Internet, fichiers, mels... Tous professionnels ! Cet arrêt généralise donc le droit d'accès de l'employeur sur l'historique de navigation de chaque salarié, ainsi que son pouvoir quasi inquisitoire de rechercher si le salarié a effectivement fait une utilisation

raisonnable de la connexion mise à sa disposition.

Pour en savoir plus :

<http://www.droit-technologie.org/actuality-1153/cybersurveillance-du-salarie-dans-l-entreprise-connexion-internet-fi.html>



Nouvelle norme ISO 27799:2008 publiée

« Avec l'utilisation croissante des technologies sans fil et de l'Internet dans les prestations de soins et du fait de l'accroissement des échanges électroniques d'informations personnelles de santé entre professionnels de la santé, une gestion efficace de la sécurité des technologies de l'information dans le domaine de la santé est un impératif des plus urgents qui justifie clairement

l'utilité de l'adoption d'une référence commune en la matière », peut-on lire dans le communiqué de l'Iso. Il rappelle que la nouvelle norme est complémentaire à l'ISO/CEI 27002:2005 (Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour la gestion de la sécurité de l'information), et plus généralement à la famille ISO 27000, qui encadre la

sécurisation des systèmes d'information. Du même ordre une norme ISO 27011 est en cours de réalisation pour la branche télécom.

Pour en savoir plus :

<http://www.iso.org/iso/fr/home.htm>



Un appareil photo des services secrets du Royaume Uni, vendu sur eBay

Un internaute Américain a acheté un appareil photo via le site de vente aux enchères américain eBay. Il y découvre des dossiers ultra-sensibles sur Al-Qaeda avec des identités, des photos, des empreintes digitales et des archives contenues dans la mémoire de l'appareil photo numérique.

Parmi les documents, des photos de missiles et roquettes prétendument fournies par l'Iran aux Irakiens. Plus sympathique encore, un fichier sur le système informatique du Mi6 à Londres.

Des informations qui valent des millions entre de mauvaises mains et qui ont été acquises pour 17 £.

L'acquéreur a été remercié d'une bien étrange manière. Il a contacté la police qui a tout simplement pris son avertissement comme une plaisanterie. Quelques jours plus tard, les services secrets ont débarqué à son domicile. L'appareil photo et l'ordinateur familial ont été saisis. Coût de l'opération, 1.000 £ de frais pour la famille avec interdiction d'en parler aux médias.

Après les affaires des deux dossiers top secret de sept pages oubliés dans le train par un espion anglais, et l'affaire d'une clé USB Secret Défense OTAN découverte dans une bibliothèque de Stockholm, le Mi6 est sérieusement touché.

Pour en savoir plus :

<http://www.thesun.co.uk/sol/homepage/news/article1749217.ece>



Loi pour le chiffrement des données personnelles : L'état du Massachusetts se lance

Dès 2009, les sociétés ou résidents de l'état du Massachusetts des États-Unis devront chiffrer toutes les données personnelles stockées sur des supports « mobiles » (laptop, clefs USB, PDA?, téléphones). La règle sera la même lors du transfert sur un réseau sans fil, de type WiFi, ou sur Internet.

Pour les entreprises, il est demandé à ce qu'elles renforcent d'une façon générale leurs mesures de sécurité,

Le Massachusetts a également adapté une loi rentrant en application ce mois-ci concernant le chiffrement obligatoire des messages électroniques contenant des données personnelles.

Pour en savoir plus :

<http://www.mofo.com/news/updates/bull-etins/14495.html>

http://blog.baselinemaq.com/bottom_line/content/security/nevada_deadline_on_email_encryption_looming.html
<http://www.leg.state.nv.us/Nrs/NRS-597.html#NRS597Sec970>



ZOOM

La Communication de Crise

Un article dans la presse, un produit défectueux nécessitant un rappel, un sinistre sur un site de production sont des exemples où la machine médiatique s'emballa. Dès lors rentre en jeu la communication de crise. C'est un concept que toute entreprise doit assimiler, l'improvisation n'étant pas de mise. Cet article décrit un exemple d'organisation possible de la communication de crise où chacun pourra reprendre des idées applicables à son contexte d'entreprise.

Les acteurs de la communication

Le rôle de chacun des acteurs de la communication de crise doit être établi lors de l'élaboration du Plan de Communication de Crise.

La direction de la communication en situation de crise :

Elle a pour rôle de piloter la communication de crise et de maintenir cette communication en condition opérationnelle. Pour cela, elle participe à la cellule de crise décisionnelle pluridisciplinaire.

La cellule de veille interne/externe :

Elle doit identifier sans délai l'information disponible en interne ou en externe. La cellule de veille interne utilise la communication reçue par les collaborateurs comme outil de pilotage. Elle doit permettre à la cellule de crise décisionnelle de répondre au mieux aux interrogations des collaborateurs. Pour sa part, la cellule de veille externe doit réagir aux informations diffusées par les médias.

La Task Force communication :

Elle assure la coordination entre la cellule de crise décisionnelle et les équipes métier.

Les collaborateurs de la communication :

Ils sont chargés de rédiger les messages, à partir des éléments communiqués par les métiers, qui seront validés par la direction.

Le groupe de coordination :

Il est chargé du pilotage du déploiement du dispositif de crise, de remonter toutes difficultés/anomalies au décisionnel de crise et de consolider les informations émanant des opérationnels pour les remonter au décisionnel de crise.

Cette organisation dépend fortement de la taille et du contexte de l'entreprise.

Les principes et les stratégies de communication

Les principes de base liés à la communication de crise sont les suivants :

- définir au préalable la communication à tenir en cas d'atteinte à l'image de l'Établissement ou du Groupe ;

- engager le processus de communication lors de la survenance d'un sinistre ;
- veiller à diffuser une communication précise, concertée et organisée à chaque niveau ;
- éviter de créer la confusion et d'engendrer des rumeurs ;
- être le plus transparent possible ;
- éviter les contestations et les remises en cause ;
- veiller à s'enquérir auprès des collaborateurs de leur état moral, les rassurer, les informer et les mobiliser ;
- créer un climat d'empathie et renforcer la cohésion ;
- se faire assister de spécialistes des situations d'urgence (le cas échéant) ;
- prévenir et gérer les éventuelles défaillances humaines.

Les stratégies de communication se doivent d'être adaptées aux différents types d'acteur.

Ensemble des collaborateurs :

L'ensemble des collaborateurs doit prendre les réflexes suivants pour toute communication avec un tiers :

- différencier ce qui relève de l'information habituelle - opérationnelle - de l'information de crise ;
- dans ce dernier cas dirigé vers l'interlocuteur le plus adapté ;
- répondre aux questions d'ordre opérationnel, si elles n'impliquent pas de fournir de données relatives à la crise ;
- ne pas répondre aux questions dont la réponse donne une information sur la gravité de la crise ou sur les modalités de traitement mises en œuvre.

Décisionnel de Crise :

Son rôle est d'occuper le terrain médiatique, pour cela il est utile de :

- définir un planning de communication volontariste :
 - ne pas laisser la place à des sources d'informations non maîtrisées (non officielles) ;
 - communiquer rapidement afin de ne pas être obligé de communiquer en mode défensif ;
 - renouveler l'information dès que cela est possible, sinon informer qu'il n'y a pas de changement par

rapport au communiqué précédent.

- informer les collaborateurs au moins deux fois par jour.

Une identification des populations cibles homogènes en fonction de leurs attentes et/ou besoins est à réaliser.

Un 1^{er} macromaillage pourrait regrouper les catégories suivantes : les contrôleurs, les fonctionnels, les tiers ayant un lien avec la société, les tiers diffus.

Il convient ensuite de détailler par cible unitaire, (définir la priorité en fonction de la nature du sinistre :

- instances publiques/parapubliques (administration fiscale, administration sociale, institution sanitaire, inspection du travail, DDTE, CRAM, ministère de la Justice/tribunaux, ministère des Finances, ministère des Affaires étrangères, chambre des notaires, huissiers, chambre de commerce et d'industrie, mairie, préfecture, député) ;
- médias (presse, TV...) ;
- collaborateurs ;
- familles des collaborateurs (en cas de dommages corporels et/ou psychologiques) ;
- maison mère éventuelle ;
- clients finaux ;
- clients des prestations essentielles assurées pour le compte de tiers ;
- autorités de tutelle éventuelles ;
- secours (pompiers, SAMU...) ;
- préfecture de police, gendarmerie, renseignements généraux ;
- fournisseurs (électricité, gaz, eau, climatisation, La Poste) ;
- prestataires de services essentiels ;
- partenaires (apporteurs d'affaires, prescripteurs...) ;
- partenaires sociaux ;
- avocats, conseils ;
- assureurs, réassureurs, experts ;
- voisinage immédiat.

À chacune des cibles doit correspondre un type de porte-parole : généralistes et/ou spécialistes.

En amont, le degré de validation nécessaire avant diffusion de l'information sera établi en fonction du profil.

L'assurance d'une diffusion cohérente de l'information délivrée entre les différentes cibles doit être prise.



Afin de garantir que l'image de la société ne sera pas écornée, il est opportun de :

- délivrer une information objective, vérifiable, fiable, ne prêtant pas à argumentation ;
- diffuser un discours simple, compréhensible et court ;
- communiquer sur la défense des intérêts des différentes « victimes » de la crise (victimes, sécurité du personnel et des riverains, clients, porteurs d'obligations...)
- ne pas communiquer sur la défense des intérêts particuliers de la société ;
- ne pas minimiser un problème ;
- communiquer jusqu'à ce que les bénéficiaires demandent un arrêt de la communication.

Répondre à une interview peut s'avérer périlleux, pour une efficacité optimum il convient de respecter les règles suivantes :

- répondre à toutes les questions ;
- accepter de dire que l'on ne sait pas immédiatement répondre à une question (réponse d'attente) ;
- dans ce cas, prendre rendez-vous pour répondre ultérieurement, rechercher la réponse et répondre précisément, à la date fixée ;
- identifier les interlocuteurs et la structure les employant ;
- rester courtois en toute circonstance ;
- planifier la réunion de communication suivante ;
- laisser les porte-paroles techniques répondre aux questions techniques ;
- assurer la communication globale par les porte-paroles généralistes ;
- informer prioritairement les collaborateurs sur tout autre public.

La communication relative aux victimes nécessite une attention particulière, dans ce cadre il est important de :

- assurer l'avancement des contacts avec les familles des victimes ;
- réserver la primeur de l'information concernant les victimes aux proches ;
- définir les démarches à mettre en œuvre ;
- s'assurer de leur caractère pragmatique et non symbolique ;
- décomposer les démarches en aides psychologiques et aides matérielles.

La communication institutionnelle :

Il s'agit de la communication générale et concertée à destination de l'environnement de l'entreprise (publics externes et internes). Elle est assumée par les représentants de la Direction Générale et ses porte-parole et destinée à des « cibles » génériques : clientèles, fournisseurs, la Profession (autorités de tutelle, marchés, analystes financiers, concurrents...). Il est important de communiquer un message générique interne et/ou externe dans le ¼ d'heure suivant la déclaration d'état de crise.

D'autre part, il convient de ne pas privilégier un contact unique pour les médias.

La communication commerciale et opérationnelle :

Cette partie de la communication de crise a en charge d'informer les partenaires habituels ou les collaborateurs par l'intermédiaire de personnes habilitées. Cela dans le but de répondre aux clients et fournisseurs sur leurs opérations en cours en utilisant des messages orientés suivant l'activité et la situation opérationnelle du moment.

La communication sociale et interne :

Il s'agit d'une communication spécifique à destination des collaborateurs et de leurs instances représentatives. Celle-ci doit être prise en charge par la Direction des Ressources Humaines.

Une communication bien maîtrisée est essentielle pour la sauvegarde de l'image de l'entreprise.

➤ Les outils de la communication

En amont, le Plan de Communication de Crise :

Il a pour objet de dresser la liste des actions de communication de crise à entreprendre, et de définir le plan d'action permettant d'atteindre cette cible.

Annuaire PCA/PRA :

En fonction de la nature du sinistre, le système d'information peut se trouver indisponible temporairement. Il conviendra donc de maintenir un

annuaire PCA/PRA accessible par la cellule de crise décisionnelle.

Serveur vocal :

Ce dispositif peut être utilisé comme moyen d'activation du PCA. En effet, les collaborateurs mobilisés en cas de crise pourront appeler un numéro coloré pour recevoir les consignes émises par la cellule de crise décisionnelle.

Intranet / Internet PCA :

Un Intranet peut permettre de centraliser les informations générales relatives à la crise à destination des collaborateurs (liste des numéros de téléphone utiles, consignes PCA...). Celui-ci pourra être mise à jour durant la crise afin d'affiner le dispositif de reprise.

Un site Internet peut servir, par exemple, à centraliser les communiqués de presse.

Call Center ou centre d'appel :

La constitution d'un centre d'appel peut se révéler utile dans le cas, par exemple, d'un incident impactant de près ou de loin la population civile. Celui-ci devra être organisé en plusieurs domaines :

- un centre d'appel traitant toutes les questions relatives à l'administration du personnel (paye, congé...)
- un centre d'appel traitant toutes les questions relatives à la continuité des activités (vers quel site se replier ? quand se replier ? quelle équipe ? matin/après-midi ?...)
- un centre d'appel à l'écoute des angoisses des collaborateurs. Il serait en liaison avec une cellule de soutien psychologique ;
- un centre d'appel à l'écoute des clients potentiels de l'entreprise.

Téléphonie mobile :

Il pourra être nécessaire de mettre à disposition des téléphones mobiles afin de pallier une éventuelle défaillance du réseau téléphonique.

➤ Pour aller plus loin :

- <http://www.communication-sensible.com/portail/> : Le magazine de la communication de crise sensible et de la gestion de crise édité par l'Observatoire International des Crises.
- <http://www.prim.net/> : Le portail de la prévention des risques majeurs.

Encore récemment, lors de l'incendie accidentel de trois camions dans une navette ferroviaire circulant dans le tunnel sous la Manche, nous avons pu constater qu'une communication de crise bien préparée et maîtrisée est primordiale pour la sauvegarde de l'image d'une entreprise. Par exemple, le délai de réouverture du service annoncé des les premières heures du sinistre a été respecté, point positif d'une communication de crise réaliste.

Rappelons enfin qu'il existe trois stratégies de communication possible : la reconnaissance, la contre-attaque ou le refus. Dans tous les cas, il faut observer le principe de réalité, pas de décalage trop important entre le communicant et son discours ainsi que le principe de cohérence : pas de changement de version ou d'arguments contradictoires.

L'ESSENTIEL

Contrôle d'accès physique

Il est utilisé tous les jours, et pourtant nous y prêtons peu attention. Les systèmes de contrôle d'accès sont omniprésents et leur utilisation est quotidienne. La liste (non exhaustive) suivante rappelle les lieux où on les retrouve le plus fréquemment : immeubles, parkings, locaux d'entreprises, transports en commun, autoroutes, remontées mécaniques, véhicules, ... Cet article aborde les thèmes de l'architecture de ces dispositifs, les types de lecteurs/capteurs utilisés (sans contact, biométrie, ...), les technologies mises en jeu ainsi que les concepts de sécurité

Architecture

Les systèmes de contrôle d'accès fonctionnent de manière soit autonome soit centralisée. Les systèmes centralisés sont fréquemment utilisés dans les entreprises où le nombre d'accès à gérer est important. A contrario, un hall d'immeuble n'a typiquement qu'un seul et unique accès. Ces systèmes sont composés de différents éléments et agissent le plus souvent sur des portes, des barrières, des ascenseurs, des tourniquets, des sas.

Éléments

Les systèmes de contrôle d'accès sont constitués des éléments suivant :

- des lecteurs et/ou capteurs ;
- des contrôleurs ;
- un logiciel de gestion.

Lecteurs et Capteurs

Les lecteurs/capteurs sont les interfaces manipulées par les utilisateurs. Leur rôle se limite à la lecture des informations nécessaires pour accéder à une zone (hall d'entrée, bureaux, salle informatique, ...), ils peuvent être de différentes natures: lecteurs de proximité, de cartes, biométriques, claviers numériques... .

Les types de lecteurs et capteurs sont un moyen de contrôler les individus. Leur nature n'affecte ni le fonctionnement, ni l'architecture des systèmes de contrôle d'accès.

Contrôleurs

Les contrôleurs sont des cartes électroniques qui gèrent les accès proprement dits. Ils reçoivent les informations des lecteurs/capteurs et pilotent les gâches électriques des portes. Ils peuvent également remonter des alarmes au logiciel de gestion lorsqu'une porte est forcée par exemple. Ces cartes sont constituées d'une mémoire qui stocke toutes les informations nécessaires au contrôle : les comptes utilisateurs, les zones ainsi que les droits d'accès associés (en fonction des comptes), un calendrier (contenant les dates des week-ends, des jours fériés, ...) ainsi qu'une horloge. En fonction des différents paramètres, le contrôleur va autoriser ou non l'ouverture de l'accès.

Logiciels de gestion

Le logiciel de gestion gère une base de donnée contenant les utilisateurs, les différentes zones définies (accueil, bureaux, salle informatique, sous-sol, ..), les accès à contrôler, les informations de monitoring (les remontées d'alarme, les rapports), Ces logiciels sont propriétaires, et les fonctionnalités qu'ils proposent dépendent des constructeurs/éditeurs. Certains gèrent uniquement les bases de données et la création de badges par exemple, d'autres permettent de visualiser en temps réel l'état des accès contrôlés, d'avoir une représentation 3D du bâtiment,

Ces logiciels gèrent en amont toutes les configurations des contrôleurs et les mettent à jour, sur le même principe des répliques de base de données. C'est par ce biais que les utilisateurs, les zones, les calendriers et autres paramètres sont configurés, et sont ensuite stockés en local sur chacun des contrôleurs.

Topologie

L'architecture réseau des systèmes de contrôle d'accès est relativement simple. La base est constituée de contrôleurs connectés entre eux sur une topologie de type bus. Chaque contrôleur est connecté à un lecteur et/ou capteur, ainsi qu'à la gâche électrique des portes à contrôler (au minimum).

L'ordinateur de gestion est quant à lui connecté au premier contrôleur, lequel est connecté à un second contrôleur, et ainsi de suite. De la même manière que les réseaux de type 10BaseX, le dernier contrôleur est configuré comme un 'bouchon' (terminologie pour le coaxial). En parallèle, un circuit électrique stabilisé est chargé d'alimenter les contrôleurs. Ces derniers fournissent le courant aux lecteurs/capteurs et aux autres composants (comme une gâche électrique, une sirène, ...). Ces réseaux d'alimentation sont indépendants du réseau électrique des bâtiments, et sont placés dans des boîtiers spécifiques.

Lorsque deux contrôleurs consécutifs sont séparés par une distance trop importante, la liaison peut être sans fil, en utilisant des modules radio spécialisés.

Pour assurer la continuité du réseau sur des sites plus éloignés, les contrôleurs peuvent utiliser des liaisons modems ou GSM. Pour effectuer les mises à jour et/ou les changements de configuration. En revanche, les logiciels de monitoring doivent impérativement rester connectés.

Les systèmes de contrôle d'accès peuvent être étendus et devenir une extension des solutions de gestion des identités (ou IAM - Identity Access Management). Il est ainsi possible, à partir d'une base de données de référence, de gérer les ressources humaines, le contrôle d'accès réseau, le contrôle d'accès physique, les comptes de cantine ... De cette manière, un seul référentiel des identités est utilisé pour une gestion centralisée du personnel, le contrôle d'accès physique compris.

Technologies

Bien que les systèmes de contrôle d'accès soient propriétaires et très peu documentés, ils utilisent toutefois des technologies largement inspirées des réseaux locaux industriels et domotiques.

Réseau

La connexion entre la plateforme de gestion et le premier contrôleur peut être de différents types: RS-232, RS-485, USB ou TPC/IP.

Lecteur et capteurs

Voici une liste non exhaustive des types de lecteurs et capteurs qui peuvent être utilisés:

- Les lecteurs de proximité RFID ;
- Les lecteurs de cartes ;
- Les lecteurs biométriques;
- Les claviers ;
- Les capteurs d'ouvertures de porte ;
- Les capteurs de présence;
- Les capteurs boutons poussoir.

Il faut noter que des lecteurs et/ou capteurs peuvent être couplés afin de rendre plus sûre/complexe l'identification: par exemple le couplage d'un lecteur de proximité avec un lecteur biométrique, ou encore un lecteur de proximité muni d'un clavier numérique,

Chaque type de lecteur ou capteur présente des avantages et inconvénients à prendre en compte pour le déploiement. Le couple sécurité/facilité d'emploi détermine le type de lecteur



et/ou capteur à utiliser. Par exemple, les lecteurs de proximité sont simples et rapides d'utilisation, contrairement à des capteurs biométriques, mais au détriment de la sécurité (les technologies RFID présentent certains risques (cf § Sécurité).

Sécurité

La sécurité fournie par ces dispositifs paraît intéressante. En effet, elle est dissuasive : comment un individu non autorisé pourrait franchir une porte fermée où il faut présenter un badge, son index et un code, et ce, sur des capteurs de nature différente. De plus, forcer la porte est à exclure puisque les capteurs d'ouvertures remontent une alarme en temps réel (via la plateforme de gestion, via une sirène, ...). Cependant, même si le système de contrôle d'accès peut être configuré de manière très sécurisée, il reste souvent basique dans les entreprises, notamment pour des raisons de sûreté des personnels. Quoi qu'il en soit, le niveau de sécurité doit être proportionnel à la valeur du bien à protéger.

La sécurité des locaux d'une entreprise repose donc sur ces dispositifs de contrôle d'accès. Mais qu'en est-il de la sécurité de ces systèmes ?

Les vecteurs d'attaques à considérer sont les éléments constitutifs du système :

- l'ordinateur de gestion ;
- le réseau d'interconnexion des contrôleurs ;
- les lecteurs et les capteurs ;
- les contrôleurs ;
- le réseau d'alimentation stabilisé.

L'ordinateur de gestion apparaît comme une cible de premier choix. En effet, celui-ci offre à un attaquant le contrôle total du système: créer un badge avec des droits VIP, modifier ou s'attribuer des droits plus étendus, verrouiller ou déverrouiller certain accès, ... Il est donc impératif que cette plateforme soit isolée de tout réseau, qu'elle soit durcie, et que l'accès physique soit restreint.

Un autre vecteur est l'attaque du réseau d'interconnexion des contrôleurs. L'attaquant se branche sur le bus RS-485, et écoute le réseau à l'aide d'un outil de monitoring. La difficulté est que les protocoles de communications sont

propriétaires et très peu documentés. Cependant, si les communications utilisent le réseau LAN de l'entreprise, les risques augmentent sensiblement (à priori, les modules ne supportent pas de chiffrement), au même titre que les modules sans fil.

L'attaque sur les lecteurs dépend du type de ceux-ci. S'il s'agit de lecteurs de proximité (RFID), il est possible, avec un minimum de matériel et de temps, d'usurper un badge existant, ou encore de mener une attaque par relais. S'il s'agit de lecteur biométrique, cela se complique, mais reste faisable. Tout d'abord, on peut citer les techniques d'usurpation, qui consistent à récupérer une empreinte puis de la rejouer (ne marche que sous certaines conditions : la non-vérification de la chaleur émise par ex.). Autre possibilité : attaquer le lecteur lui-même. En le démontant, il est possible de contourner le contrôle au niveau électronique en effectuant un court-circuit. Cela dit, les probabilités de l'endommager ne sont pas négligeables, et la discrétion de l'attaquant est mise à mal.

Les claviers de types digicodes peuvent être mis en défaut par une révélation des touches utilisées. Cependant, retrouver la combinaison par brute force peut s'avérer très long et délicat (étant donné qu'il faut être devant le lecteur...). La compromission par le biais électronique reste également possible, au même titre que les lecteurs biométriques.

Les cartes magnétiques peuvent être contournées à l'aide de matériel 'home made' assez basique. En effet, la duplication peut être envisagée avec l'émission d'un signal (contenu dans un fichier WAV par exemple) au travers d'un petit montage électronique (un amplificateur et un solénoïde en guise d'antenne). Cette faiblesse provient des mécanismes des lecteurs de badges magnétiques. Les cartes à puces peuvent être plus complexes, mais des attaques restent possibles, selon le type de cartes utilisées et la sécurité qu'elles embarquent.

Un vecteur intéressant est celui des contrôleurs. En effet, ces contrôleurs possèdent des ports console (interfaces RS-232) afin de les administrer

localement. Avec un câble série et un terminal, il est possible d'accéder à la configuration du contrôleur. Toutefois un mot de passe est requis, mais n'y a t'il pas de fortes chance pour ce soit celui par défaut (souvent donné dans la documentation) ? De plus, en écoutant le trafic il est possible de retrouver ce mot de passe (aucun chiffrement n'est utilisé pour les communications). Enfin, les contrôleurs étant reliés sur un même bus, un attaquant peut 'jouer' avec tous les accès des bâtiments contrôlés par ce réseau. Une fois entré dans la configuration, on peut envisager d'ouvrir ou fermer n'importe quel accès, créer, modifier ou supprimer des profils utilisateurs, etc. Le niveau d'interaction est le même qu'à partir de la station d'administration.

Pour lutter contre ce problème, les boîtiers peuvent (et doivent !) intégrer des alarmes anti-intrusion (souvent sous la forme de modules supplémentaires), et être confinés dans des boîtiers fermés à clé.

Un autre vecteur est le réseau d'alimentation dédié. Selon la configuration, les gâches électriques des portes sont maintenues par une tension de 12 ou 24 volts. En coupant l'alimentation, la gâche est libérée et la porte peut être ouverte. Cela dit, l'effet inverse (le maintien à l'état fermé) est également possible, au détriment de la sûreté des personnels dans certains cas.

Une autre possibilité ne faisant pas partie des éléments de l'infrastructure : la génération d'une impulsion électromagnétique (d'environ 5 Mégawatts) ; cela peut provoquer un choc puis un redémarrage du contrôleur et libérer la gâche quelques instants. La puissance énoncée (5 Mégawatts) permet d'avoir une portée d'environ 70 cm, ce qui est suffisant pour couvrir les systèmes électroniques situés autour de l'accès. Une protection possible est d'utiliser des cages de Faraday afin d'isoler les contrôleurs.

Pour aller plus loin :

Les aspects juridiques de la biométrie
<http://www.cnil.fr/index.php?id=2013>

La principale faiblesse des contrôles d'accès physique reste les lecteurs de type RFID et magnétiques, sur lesquels existent diverses attaques opérationnelles. Cependant, l'ensemble des solutions semble très satisfaisant en matière de sécurité, et les fonctionnalités offertes par les stations de gestion permettent une surveillance fine des événements. Le couplage de différents capteurs pour contrôler les accès sensibles reste la meilleure solution. Les contrôleurs ainsi que la station de gestion doivent impérativement être hors de portée de tout individu non autorisé, et il est recommandé de placer des systèmes de vidéo surveillance au niveau de leurs accès.

VEILLE

HDCP ou High Definition Content Protection

L'évolution des modes de consommation de contenus audiovisuels et du tout numérique a amené les professionnels de ce secteur à rechercher différents modes de protection de ces médias. Dans un premier temps est apparu le Digital Right Management (DRM), prévu pour protéger les contenus eux-mêmes puis a émergé une protection propriétaire nommée HDCP. Celle-ci est conçue pour protéger la chaîne de diffusion du dit contenu au travers d'un mécanisme complet d'authentification, de chiffrement des données et de révocation de certificat utilisé au quotidien.

Qu'est-ce que l'HDCP et quel est son rôle ?

La protection HDCP (High Definition Content protection) a été créée par le « Digital Content Protection » (DCP) filiale d'Intel. Le but de cette protection est de pouvoir sécuriser dans son intégralité la chaîne de transmission des contenus audiovisuels haute définition et éviter leurs duplications par écoute.

Le principe est que tout élément de la chaîne de diffusion HD (Haute Définition), doit être certifié et authentifié HDCP afin que le flux soit distribué au format HD. Dans le cas contraire, il sera au mieux diffusé dans une résolution inférieure « SD », au pire non visualisable.

Le HDCP n'est actif que sur des interfaces de type DVI (Digital Virtual Interface), HDMI (High-Definition Multimedia Interface) ou DisplayPort. Donc, si le flux est diffusé via une interface analogique il ne sera pas protégé par le HDCP.

- Ainsi le HDCP repose sur trois principes :
- l'authentification, servant à déterminer que tous les différents éléments de la chaîne (source, répéteur, diffuseur) sont bien compatibles HDCP
 - le chiffrement des données pour protéger le contenu diffusé ;
 - le processus de révocation empêchant les éléments non conformes d'accéder à ces flux.

Pour mémoire, à l'heure actuelle cette protection est essentiellement utilisée sur les disques Blu-ray.

L'authentification.

Chaque élément de la chaîne de diffusion qu'il soit source (lecteur blu-ray, disque blu-ray, console de jeu), répéteur (amplificateur), ou diffuseur (télévision, projecteur) embarque un ou plusieurs émetteurs ou récepteurs.

Un émetteur HDCP est un élément capable de chiffrer est de transmettre un signal HDCP au travers d'une ou plusieurs interfaces.

Un récepteur HDCP est un élément capable de recevoir et de déchiffrer le contenu d'un signal HDCP.

Un répéteur quant à lui doit être capable de déchiffrer un flux HDCP émis par une source HDCP, de le chiffrer à nouveau et de le retransmettre aux éléments récepteurs de la chaîne.

La figure suivante (figure 1) présente les différents éléments d'une chaîne HDCP.

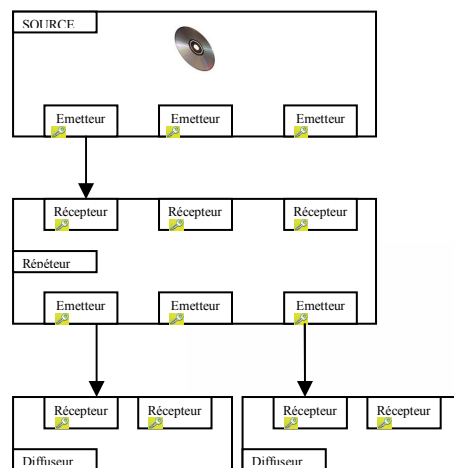


Figure 1- les différents éléments d'une chaîne HDCP.

Chaque émetteur/récepteur HDCP se voit allouer 40 clefs uniques de 56 bits chacune. Ces clefs sont les clefs privées de l'élément, elles sont fournies par l'organisme DCP. En outre, chaque émetteur/récepteur HDCP possède un identifiant nommé KSV (Key Selection Vector) fourni lui aussi par le DCP. Il s'agit d'une clef de 40 bits (1 bit pour chacune des clefs privées) dont 20 sont fixés à zéro et 20 à un.

L'authentification des tiers se fait à l'aide d'un protocole de cryptage asymétrique. Le schéma suivant (figure 2) illustre la première partie de cette authentification. Une source « S » initie la transaction à l'aide d'un message contenant son KSV (KSVS) ainsi qu'un code pseudo aléatoire (PSAS, Pseudo Aléatoire Source) de 64 bits générés via la fonction de cryptage du module HDCP émetteur. À la réception de ce message, le module récepteur « R » de l'équipement tiers envoie une réponse contenant son propre KSV (KSVR). La source « S » vérifie alors que le KSVR n'est pas révoqué et que cette clé est bien constituée de 20 zéros et 20 un.

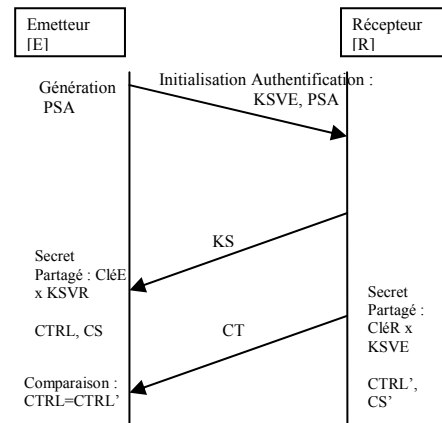


Figure 2-authentification.

À ce stade, chaque élément dispose du KSV de l'élément tiers. À partir de ce vecteur, ils vont, à l'aide d'une de leurs clefs privées calculer un « secret partagé ». Grâce à cette valeur et au code pseudo aléatoire, est calculée une clé de session « CS », partagée, de 56 bits, ainsi qu'une valeur de contrôle « Ctrl ». Cette dernière indique à l'élément tiers que la transaction est terminée. La source compare alors la valeur de contrôle reçue à celle calculée par elle-même. Si les deux valeurs sont identiques, l'authentification est alors considérée comme étant valide.

Le chiffrement des données.

Le chiffrement de la session se fait à l'aide de la clef partagée « CS » calculée précédemment lors de la phase d'authentification. Par la suite, tout au long de la session, un message d'information est envoyé, toutes les 2 secondes, par l'élément HDCP récepteur afin de valider le fait que les deux éléments HDCP sont correctement synchronisés et que l'équipement recevant les flux arrive bien à décoder ces derniers.

Le chiffrement des données, quant à lui, est effectué par la source de façon relativement simple. Pour chaque pixel (d'une taille de 24 bits) envoyé, un code pseudo aléatoire d'une taille identique est généré à l'aide du module HDCP embarqué. Ce pixel subit alors une opération appelée « Ou exclusif » (XOR). Le résultat de cette opération est transmis par la source en utilisant un

algorithme de codage mis au point par Silicon Image : TMDS (Transition Minimized Differential Signaling). Celui-ci est conçu pour la transmission des données à haute vitesse, et la correction d'erreur. L'opération inverse est réalisée à la réception du flux.

La révocation

La protection HDCP prévoit le fait qu'une ou des clefs privées puissent être compromises. Dans ce cas, le KSV correspondant est déclaré comme étant non valide. L'équipement possédant le KSV révoqué ne pourra plus s'authentifier auprès des sources. Il ne sera donc plus en mesure de délivrer le flux HD convenablement.

Les mises à jour des listes de KSV révoquées se font typiquement via le contenu audiovisuel des médiums tels que les Blu-ray discs.

Ce système fonctionne donc par le biais d'une liste négative (blacklist). D'après les travaux des spécialistes en cryptanalyse, un certain nombre de faiblesses dans le fonctionnement de HDCP ont été mises à jour. Ainsi, l'analyse du fonctionnement de 40 éléments HDCP permettrait d'obtenir suffisamment d'information pour générer des certificats valides non officiels.

Dans ce cas, l'utilisation de liste de type blacklist devient inutile, et source de problème. Une solution possible, serait de passer dans un mode de fonctionnement de liste blanche (whitelist), ou seul les constructeurs certifiés HDCP seraient référencés et

donc autorisés à diffuser ou à recevoir du contenu HDCP. Bien sûr ce genre de liste a des limitations par exemple l'intégration de nouveaux acteurs sur le marché.

La liste des KSVs révoqués est donc maintenue par le « DCP ». Elle est transmise, signée à l'aide d'une signature digitale DSA permettant d'authentifier et de garantir son authenticité, aux presseurs de disques Blu-ray ou HDDVD. Ceux-ci ont pour responsabilité de l'intégrer dans chacun des disques en cours de fabrication. Les disques deviennent alors les vecteurs de propagation lors de la mise à jour des équipements HD sur lesquels ils seront utilisés.

Cette protection ne s'applique, pour l'instant, que lors de la lecture d'un média enregistré sur un support Blu-ray ou HDDVD et nécessite un lecteur HD pour être mise en œuvre, car c'est bien le lecteur associé au support HD qui forme « l'autorité validante » de la chaîne, et ceci uniquement pour la durée de la diffusion du contenu.

Au quotidien.

IL ne peut pas y avoir de protection HDCP mise en œuvre, sans source certifiée HDCP. C'est la source qui valide la chaîne HDCP jusqu'au diffuseur.

Dans le cas où la source n'est pas certifiée HDCP les flux seront diffusés au maximum de ce que le support peut fournir, peu importe que les éléments se trouvant entre la source et le diffuseur soient compatibles HDCP. Dans le cas

contraire (source embarquant un émetteur HDCP), si la chaîne de diffusion n'est pas entièrement compatible HDCP, le signal sera soit altéré à l'aide d'un downscaling (l'image et le son seront émis avec une définition plus faible) soit il ne sera tout simplement pas diffusé.

Actuellement, tous les diffuseurs estampillés HDready ou FullHD devraient être compatibles avec la protection HDCP, ce qui représente environ 99% de la production actuelle de télévision.

Le problème risque de se poser pour les plateformes informatiques telles que les PC multimédias où seules les générations récentes de carte sont compatibles HDCP. En effet, les constructeurs de carte vidéo ne proposent des cartes et des pilotes compatibles HDCP que depuis moins de deux ans.

Néanmoins, cette protection peut être maintenant facilement outrepassée sur plateforme PC à l'aide de logiciels spécialisés dans le contournement de protection vidéo, ce qui permet à des cartes vidéo Haute Définition non compatibles HDCP de diffuser le contenu HD au meilleur de sa résolution.

Pour aller plus loin :

- <http://www.digital-cp.com/>
- Scott Crosby, Ian Golberg, Robert Johnson, Dawn Song et David Wagner dont les résultats : « "A Cryptanalysis of the High-bandwidth Digital Content Protection System" », 5 novembre 2001

Il est certain que ce système a été conçu et réfléchi de manière commerciale et non pas dans l'objectif de créer un coffre totalement inviolable. En effet, le but de cette protection est d'empêcher la reproduction (à la manière d'une copie de VHS) ou la multidiffusion d'une œuvre fixée sur un support Blu-ray ou HDDVD. De ce point de vue, l'objectif est atteint jusqu'à un certain point : la protection des disques Blu-ray a déjà été contournée et bon nombre de contenus HD se trouvent maintenant en téléchargement illégal sur internet.



Réagissez aux articles de la newsletter sur le blog de l'ESEC :
<http://esec.fr.sogeti.com/blog>

Inscription à la Newsletter : newsletter-subscribe@esec.fr.sogeti.com
Désinscription : newsletter-unsubscribe@esec.fr.sogeti.com

Agence ESEC
Sogeti Infrastructures Services
6-8 rue Duret 75016 Paris - France
Tél. : +33 (0)1 58 44 26 79
Site : <http://esec.fr.sogeti.com>
Mail : esec@esec.fr.sogeti.com

Société par Actions Simplifiées au capital de 15 999 790 € - RCS Paris 479 942 583
Conformément à la loi « Informatique et libertés » du 6 janvier 1978, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser au directeur de l'agence ESEC.

Sogeti ne peut être tenue pour responsable en cas avéré de détournement des liens communiqués à titre d'illustration dans ses propos.

Cette newsletter a été réalisée par des consultants sécurité de l'agence **ESEC**.

Responsable de la publication : Edouard **JEANSON**

Auteurs :

- Loïc **FREIXAS**
- Loïc **CORNET**
- Alexandre **LAFFONT**

Rédacteur en chef : Nicolas **VINCENT**

Relecteur(s) : François-René **HAMELIN**

