Réunion plénière – Architrave, Strasbourg

Le 4 octobre 2019

CACES® - Cybersécurité

Compte rendu

http://association-pari.org/

Nombre de participants ***: 64.***

Réunion ouverte à ***13 h 45.***

Compte rendu et présentations sont complémentaires. Suivre les liens intégrés à ce document.

Sommaire

Le Président Henri KRUTH souhaite la bienvenue aux participants.

I. Les réformes des CACES®, évolution pour 2020

Denis SCHNEIDER ; « CARSAT »

Consulter le diaporama.

I.1. Historique

L'augmentation constante des accidents liés à l'utilisation d'engins mobiles automoteurs et d'engins de levage a conduit, au début des années 2000, la CNAMTS à élaborer le dispositif CACES® « Certificat d'Aptitude à la Conduite En Sécurité ». Les recommandations qui en ont résulté, préconisant une formation ET une évaluation, sont destinées à prévenir les risques d'accidents, souvent graves, occasionnés par ces engins.

Le CACES® n'est pas obligatoire, ce n'est qu'une recommandation. Cependant, la circulaire de 1998 précise qu'il *« constitue un bon moyen pour le chef d'établissement de se conformer aux obligations en matière de contrôle des connaissances et du savoir-faire de l'opérateur pour la conduite en sécurité ».* Donc le CACES® n'est pas obligatoire, mais il est reconnu par le Ministère chargé du travail ! Par ailleurs, l'évolution du nombre de CACES® délivré (plus de 800.000 en 2018) confirme le succès du CACES®.

I.1. L'évolution pour 2020

Face à l'évolution des équipements et compte tenu de l'hétérogénéité des pratiques des organismes testeurs certifiés, malgré une sinistralité maîtrisée et restée stable depuis 20 ans, la rénovation du CACES® devenait nécessaire. Les objectifs sont d'améliorer le niveau de formation des conducteurs, pour intégrer de nouvelles familles d'équipements et tenir compte des activités hors production, pour centraliser la gestion des certificats et, enfin, pour prendre en compte l'anti-endommagement des réseaux. Il y avait également la nécessité d'harmoniser la mise en œuvre des évaluations pratiques, car il en existe une grande variété, autant que d'organismes de formation.

Il faut privilégier la formation à l'acquisition des connaissances dans les conditions de travail dans l'entreprise. Le CACES® n'est que l'évaluation des compétences et la formation à l'utilisation des équipements de travail doit être renouvelée aussi souvent que nécessaire. Les nouvelles recommandations insistent sur l'obligation de formation **adaptée à l'équipement que doit utiliser le salarié**.

Elles ne prennent en compte que les engins les plus courants, sinon pour les engins « non classiques » il sert seulement de base. Par contre il est toujours nécessaire de faire une formation adaptée et une évaluation complémentaire.

Les 6 recommandations anciennes ont été remplacées (R.482, R.487, R.4873, R.486, R.489 et R.490) et 2 nouvelles recommandations ont été créées (R.484 relative aux « ponts roulants et portiques » et R.485 pour les « chariots gerbeurs à conducteur accompagnant ».

Le nouveau CACES® est valable pendant 5 ans pour les chariots, pour les nacelles, pour les ponts roulants et les gerbeurs, et pendant 10 ans pour les engins de chantier. Par contre, pour les grues (mobiles, à tour et de chargement, il est possible de prolonger la validité du CACES® initial de 5 ans en passant avec succès une nouvelle évaluation théorique et si l'employeur atteste que le salarié a réalisé, durant ces 5 premières années, au minimum 50 jours de conduite par an de l'équipement concerné.

Les tests théoriques et pratiques doivent être effectués uniquement en langue française, il y a donc nécessité absolue de la maîtriser !

Certaines recommandations sont encore en cours d'évolution, par conséquent, de façon à toujours disposer de la dernière version, il est conseillé de consulter les sites Web plutôt que de télécharger les documents. La majorité des informations intéressantes se trouvent dans les annexes… On y retrouve notamment les engins concernés, les options par rapport aux équipements, les équipements représentatifs pour la réalisation des tests CACES® ainsi que les procédures de test et moyens requis pour que les organismes puissent faire des formations adaptées avec les appareils et les conditions de travail effectives.

Les textes sont consultables sur le site « AMELI.fr » via l'outil :

Recherche de recommandations par secteur d'activité ou CNT

La rénovation du système s'accompagnera de la mise en place d'une Base de données et le Forum Aux Questions sera reconduit.

Q.: Avec les entreprises étrangères, comment solutionner le problème de la langue ?

R.: il n'y a d'équivalence entre les dispositifs des pays de l'UE. La délivrance de l'autorisation de conduite reste de la responsabilité de l'employeur, il n'y a pas de solution pour les employés ne maîtrisant pas le français. L'employeur doit vérifier à quoi correspondent les documents d'autorisation en possession des conducteurs étrangers, quelle a été leur formation, etc.

Q.: Comment fait-on pour les chariots gerbeurs qui lèvent à plus de 1,2 m sans déplacement du chariot ?

R.: La réponse se trouve dans le contenu des évaluations.

Pour le CACES®, les conducteurs doivent être évalués sur la thématique « avec » déplacement du chariot, sinon il faut faire une autorisation de conduite en réalisant la formation dans les conditions d'utilisation réelles de l'entreprise.

II. La Cybersécurité, prévention et lutte contre la cybercriminalité

Major Denis MÉREAU ; DIPJ-Strasbourg.

***Consulter le diaporama*.**

Organigramme de la Police : en tuyau d'orgues.

La DIPJ, Direction Interrégionale de la Police Judiciaire de Strasbourg fait partie de la DCPJ, Direction Centrale de la Police Judiciaire.

Les LIONS (Laboratoires d'investigation opérationnelle numérique) ont la possibilité d'analyser TOUT ce qui est numérique, des réseaux aux drones…

II.1. La cybercriminalité

Elle consiste essentiellement à nuire via la correspondance électronique, par exemple… la « *mailveillance* », tous les moyens sont bons pour pirater un ordinateur, que ce soit celui d'un particulier ou le réseau interne d'une entreprise.

Il faut absolument avoir conscience que les risques sont importants pour tous. N'importe qui peut être attaqué sans s'en rendre contre, un clic peut suffire pour subir des dommages qui peuvent atteindre des millions d'euros. Les conséquences peuvent être catastrophiques pouvant mener l'entreprise à la faillite suite à un piratage. Récemment deux entreprises alsaciennes ont été victimes de ces arnaques.

Or par la prévention, en prenant quelques précautions souvent simples, on peut éviter les pièges. Il faut avant tout être très vigilant.

Les chiffres présentés dans le diaporama montrent l'importance de ces arnaques, mais ce ne sont que les cas déclarés par les victimes… la réalité est à coup sûr bien pire.

Si vous êtes victime d'une escroquerie au président et que vous avez viré l'argent :

Réagir très vite, contacter la DIPJ (voir les coordonnées en fin de présentation) :

en 24 h on peut récupérer les fonds et limiter les dégâts,

entre 24 et 48 heures il reste quelques chances,

au-delà les pertes sont très difficilement récupérables !

Surtout, ne rien effacer ni supprimer dans l'ordinateur, car il faut absolument garder les traces, entre autres les fichiers « .log », qui permettront à la PJ de faire des recherches rapides et efficaces. Continuer le dialogue pour récupérer un maximum d'informations.

Si l'enquête et les recherches aboutissent, cela prendra ensuite plusieurs semaines, voire quelques mois et une vingtaine d'informaticiens, pour récupérer les fichiers cryptés !

II.2. Les attaques

Les principaux types d'attaques peuvent prendre des formes variées, mais on peut les résumer en deux principaux types :

Les harponnages ou hameçonnages, « phishing » et « spear-phishing » consistent pour le pirate, à envoyer un message contenant un lien ou une pièce jointe avenants ou techniques, demandant par exemple une mise à jour des données personnelles.

Cela permet au cybercriminel de récupérer des identifiants dont il peut faire usage ensuite. Les envois de « phishing » ne visent pas une personne en particulier, c'est un envoi en masse contrairement au « spear-phishing » qui lui, est ciblé sur une personne ou une entreprise.

L'infection par un logiciel malveillant, un cheval de Troie, « malware, ransonware, cryptolocker… ». Elle se produit lors de l'ouverture d'une pièce jointe (photo) ou d'un lien d'un message reçu, entraînant le cryptage de l'ensemble des données contenues dans l'ordinateur. Dans une entreprise le réseau interne est ensuite contaminé de proche en proche. L'accès à toutes les données est alors bloqué. La victime, particulier ou entreprise est alors sommée de payer une rançon en « bitcoins » pour les récupérer. Quatre cents serveurs ont été cryptés en un week-end pour une seule entreprise Alsacienne !

Dans le cas des escroqueries et du chantage, mais pas lors d'un « ransomware », c'est souvent l'engrenage infernal, il faut payer toujours plus !

Concrètement ces attaques peuvent prendre les formes suivantes :

- ***Les clés USB trouvées par terre***, elles sont à considérer comme systématiquement piégées !

  Le cybercriminel joue sur la curiosité naturelle de l'être humain.

  Lorsque la clé est branchée sur l'ordinateur une photo, d'apparence inoffensive, apparaît… en quelques secondes l'ordinateur est piraté ! Souvent, le virus s'installe dès qu'on branche la clé et, même si la victime est prise d'un doute et l'enlève immédiatement, il est trop tard le virus est déjà transféré et actif (fichier « Helper.exe » dans l'exemple de la vidéo). Les pirates peuvent alors sortir en clair tous les mots de passe du PC (compte en banque…). Souvent la victime n'a rien remarqué et ne sait pas que son ordinateur est infecté.

Une clé trouvée ne doit jamais être branchée sur un ordinateur !

- ***Les Mots de passe :*** on ne donne jamais ses mots de passe ou son code de CB à quiconque, car il faut être conscient que le collègue peut aussi être délinquant informatique ! Pour se souvenir des mots de passe, il vaut mieux les avoir sur un papier en sécurité, et non affiché sur l'écran dans un fichier informatique, les risques de récupération sont beaucoup moins grands.

  Les mots de passe génériques (utilisés par tous dans l'entreprise) doivent être bannis. Dans certains cas le « hacker » peut être un responsable informatique qui se venge.

- ***Les Achats en ligne*** **:** le « hacker » qui a piraté l'ordinateur enregistre en direct tout ce qui a été et est tapé sur le clavier de l'ordinateur, il peut donc récupérer tous les identifiants et mots de passe et peut s'en servir à sa guise.

- ***Les Applications web à accès sécurisé, réseaux sociaux, etc. :***

  Pour accéder, le pirate essaie le plus simple : en « login » le prénom ou le nom et, comme mot de passe, une date de naissance. Ce sont les habitudes les plus fréquentes de la plupart des gens pour pouvoir retenir ces données.

  La prévention consiste à ne pas rien dévoiler sur le Web, réseaux sociaux et autres, de sa vie privée, de ses photos personnelles… de même pour les entreprises être prudent avec les sites de présentation pour ne pas y fournir d'informations sensibles.

  Pour sauvegarder toutes les données personnelles critiques, utiliser des disques durs externes de sauvegarde « à froid », c'est-à-dire branchés uniquement pour la sauvegarde, ne pas laisser ces disques connectés en permanence. Éviter les sauvegardes de données critiques sur des sites en réseau sur internet. Mettre en place des sauvegardes protégées, c'est coûteux certes, mais il faut évaluer l'aspect bénéfice-risque.

- ***Les Courriels, « Mails » avec liens ou pièces jointes :***

  95 % des « ransomware » arrivent par des pièces jointes :

on n'ouvre pas les pièces jointes envoyées par un inconnu !

Des entreprises ont été piégées et toutes sont potentiellement vulnérables. À titre d'exemple le réseau interne du CHU de Montpellier a été crypté par une pièce jointe ouverte sans méfiance.

En cas de demande de rançon, ne jamais payer ! malgré les promesses du pirate ; dans la majorité des cas les données ne seront pas décryptées, souvent les escrocs effacent tout et si, exceptionnellement, le pirate est bienveillant, on n'est jamais sûr qu'il n'ait pas laissé un autre virus masqué. Courriels d'inconnus avec pièces jointes ou lien :

avant de cliquer tourner sept fois le doigt autour de la souris

- ***L'Arnaque au président*** **:** ce sont les Faux ordres de virement (F.O.VI.), le pirate se fait passer pour un dirigeant de l'entreprise ou une personne de haut rang hiérarchique… Il demande d'effectuer un virement urgent, pour profiter de conditions particulièrement favorables et opportunistes et il y a urgence. Cela nécessite pour le pirate une préparation longue et rigoureuse, mais les sommes récupérées en valent la peine. Plusieurs entreprises alsaciennes en ont été victimes. Pour l'une les fonds ont été récupérés, pour l'autre la réaction de la comptable qui a eu un doute a osé déranger le Directeur pour lui demander s'il était bien l'auteur de l'ordre : elle a bloqué l'arnaque et empêché le pire.

  Même en étant prudente, avec une longue expérience, une entreprise peut être piégée, un clic suffit. Il faut mettre des garde fous, attendre sans réagir, téléphoner au donneur d'ordre (le vrai). Sur les sites Web de présentation, ne pas dévoiler de données critiques pouvant être susceptibles d'intéresser ou d'aider les arnaqueurs.

- ***La Gestion des personnels, stagiaires, anciens salariés :***

  Dans une Société A, des employés partis à la concurrence dans l'entreprise B continuaient à utiliser les anciens mots de passe restés actifs chez A ! Ils ont pu y pirater toutes les informations intéressantes et confidentielles et entraîner la faillite de A…

  Quand un salarié part de l'entreprise, après son départ, bloquer ses accès personnels, changer les mots de passe… on ne peut présager de son comportement futur, surtout s'il part à la concurrence.

  Lors d'embauche de stagiaires être prudent, on ne sait pas *a priori* de quoi il est capable. Ainsi dans un hôpital, un stagiaire en informatique avait récupéré les données des ordinateurs de ses collègues, ce de façon invisible et, parmi elles, il y avait des données médicales de patients.

- ***Le « WI-FI »***

  Se méfier des « Wi-Fi » externes (Macdo, bars branchés ou autre…) on peut se trouver connecté via un PC de « hacker » qui opère masqué à distance !

  L'entreprise tourne avec un réseau interne en « Wi-Fi », elle doit s'assurer qu'il est bien sécurisé de façon à ce qu'un appareil pirate ne puisse pas se connecter.

  Attention aux « objets connectés » : tout est sécurisé dans l'entreprise, c'est parfait on est confiant, mais… attention aux périphériques, les imprimantes en particulier. Tous ces appareils connectés via le « Wi-Fi » sont des fenêtres ouvertes au piratage, de véritables passoires sans aucune protection, et elles le resteront, car les sécuriser correctement coûterait beaucoup trop cher.

  Un père de famille a été accusé d'entretenir un site de pédopornographie, il est arrêté, auditionné… or on ne trouvait rien sur son ordinateur et il clamait son innocence ! Avant que l'on ne découvre le vrai criminel… qui avait pris le contrôle du réfrigérateur de sa victime et s'en servait pour diffuser ses données pédopornographiques ! Ce dernier a été découvert car les diffusions continuaient alors que sa victime était arrêtée et l'ordinateur aux mains de la police. Les conséquences pour la victime ont été terribles, arrêté dans sa famille, encadré de la police devant les voisins… Depuis cette affaire des précautions sont prises par les enquêteurs.

  En 2015 les escrocs se sont branchés sur les freins d'une voiture connectée, avec tous les risques que cela peut engendrer.

  Dans un casino c'est le thermomètre d'un aquarium qui a servi de cible.

  Idem pour les téléphones : 206 applications Google ont été supprimées car elles étaient infectées par des « Malwares ». Quinze millions de connexions avaient été réalisées !

  « WhatsApp » a reconnu une faille en 2019, il était infecté par un logiciel espion.

Le « Bluetooth » est moins risqué que le « Wi-Fi ». La plus faible distance de connexion le protège relativement.

D'une façon générale, ne pas mélanger les données privées, trop personnelles, avec les données publiques ou de travail et éviter les diffusions sur le Web.

- ***Les Réseaux sociaux***

  Pourquoi publier sa vie privée ? il ne faut pas mélanger vie privée et vie publique !

  Les données personnelles photos, identités, adresses, sont autant de tentations pour les cybercriminels, ils peuvent les exploiter à leur guise, les réseaux sociaux sont des points d'entrée et de contact relativement faciles pour les escrocs. Très fréquente, « l'escroquerie à l'amour » en direct sur le Web. Si vous acceptez le faux amoureux ou la fausse amoureuse dans vos amis Facebook par exemple, et que vous vous filmez devant votre webcam, alors tout est enregistré par l'escroc ! Ensuite demande de rançon… escalade au paiement…

  La solution consiste à ne jamais payer quel que soit la demande, ami dans le besoin (ce n'est pas l'ami !), chantage… tant pis si les données sont diffusées, le chantage s'arrêtera de lui-même et tout sera vite oublié !

II.3. Les solutions

Si malheur vous arrive, prévenir la DIPJ de Strasbourg :

Il est bien clair que la justice ne peut pas suivre. Tout d'abord pour des questions de coût, récupérer une rançon demande des engagements importants en moyens et en personnels de milliers d'euros, qui ne peuvent pas être immobilisés pour récupérer de petites rançons.

Le gendarme court toujours derrière le voleur qui a systématiquement un train d'avance, la Police est bloquée par les frontières, pas les escrocs ! Dans beaucoup de pays on ne peut rien obtenir et, même avec l'Allemagne pourtant proche aussi bien géographiquement qu'idéologiquement, c'est compliqué d'obtenir les informations nécessaires aux enquêtes.

Le pire des virus c'est Vous par un clic malencontreux !

Le meilleur anti-virus c'est Vous, par votre prudence !

II.4. Questions-réponses

Q.: Est-ce que cela intéresse vos services de connaître toutes les attaques qu'on décèle, faut-il toutes vous les adresser ?

R.: Bientôt le « Projet Thésée » permettra de porter plainte directement en ligne.

Cela simplifiera les démarches pour les victimes et permettra de faire des recoupements qui ne sont pas encore possible actuellement.

Q.: Dans nos professions nous sommes en contact avec des clients potentiels dont on ne connaît rien ! comment peut-on se protéger ?

R.: Il n'y a que la prudence et un antivirus à jour et efficace qui puisse vous protéger. Rien d'autre.

Q.: Y a-t-il une éducation possible pour les particuliers ?

R.: Non ! Rien n'est prévu et les gens ignorent complètement ce à quoi ils peuvent être exposés, ils ignorent totalement les risques.

Q.: Il existe des coffres-forts à mots de passe. Sont-ils efficaces ?

R.: Oui, ils sont généralement sûrs.

Q.: Les antivirus gratuits sont-ils fiables ?

R.: Il est difficile de répondre à cette question car en fait les antivirus payants proposent des options complémentaires. Les antivirus gratuits sont aussi efficaces en général.

Q.: Dans un piratage ciblé, avec une adresse fictive visiblement, le pirate disait avoir eu des vidéos compromettantes. Avez-vous des retours avec la même adresse que qui a contacté l'entreprise ou la personne ?

R.: On peut se faire passer pour n'importe qui en faisant apparaître une adresse fictive et le pirate en change systématiquement, c'est donc difficile à suivre. Mais il faut rechercher derrière, la date de création du message ou du site.

Q.: Les « Cloud » sont-ils sécurisés ?

R.: Ce type de stockage est en très forte augmentation.

Une précaution élémentaire consiste à crypter les données que l'on dépose sur ces serveurs. L'idéal serait que ces sites effectuent un stockage des données divisées en paquets sur plusieurs serveurs séparés physiquement, ce type de stockage est bien sécurisé.

Les interventions étant terminées Henri remercie nos intervenants pour leurs très intéressantes présentations.

III. Info PARI

Henri nous donne rendez-vous pour l'Assemblée générale qui aura lieu le 13 décembre à Duppigheim comme à l'habitude, le menu sera :

BAECKEHOFFA et VACHERIN GLACÉ !

À bientôt donc…

La réunion est terminée à 16 h 10

Le 16/10/2019

Le secrétaire, Jean DUCRET