LA LETTRE D'INFORMATION

N°14 *Direction de la Sécurité Économique en Zone Paris*

EDITO

Cette lettre d'information s'inscrit dans la préparation du salon international de l'aéronautique et de l'espace (SIAE) du Bourget. L'accent, teinté d'actualité, sera mis sur la protection de vos activités au sens large car le contexte ultra-concurrentiel et les opportunités commerciales du secteur aérien et spatial font de l'édition 2017 du SIAE un moment plus propice que jamais au risque de captation d'informations.

Certes, toutes les entreprises du portefeuille ne participeront pas au SIAE, mais les principes énoncés se veulent applicables en d'autres lieux et ou circonstances.

Naturellement, les équipes de la DSEZP sont également à vos côtés pour vous accompagner sur des thématiques protection plus précises et en fonction de vos besoins. Pour cela, l'équipe sensibilisation est à même de délivrer son message de manière très ciblée et en langue anglaise.

Enfin, l'actualité cyber étant encore une fois très dense, vous trouverez, outre l'article cyber, un flash info lié à l'attaque wannacry.

Le directeur de la DSEZP

INTELLIGENCE ECONOMIQUE

Le salon professionnel, risques et opportunités.

Les défis relevés chaque jour par les entreprises du secteur de l'aéronautique et du spatial pour s'adapter à ce secteur en constante évolution, où la concurrence est exacerbée, les obligent à innover, et à présenter ces innovations. Un salon professionnel de renommée internationale comme le SIAE est donc une opportunité pour exposer son matériel, montrer son savoir-faire et présenter ses services. Cependant, c'est aussi un lieu particulièrement propice à la captation d'informations sensibles. **Ce paradoxe peut être exploité et maitrisé en l'observant sous le prisme de l'intelligence économique**.

Pour introduire ces idées, quelques chiffres sur le SIAE 2015 :

- 2300 exposants de 48 pays ;
- 296 délégations officielles et 350 000 visiteurs ;
- 7100 rdv d'affaires et 4300 journalistes ;
- le GIFAS réalise 80% de son CA (58 Mds d'euros) à l'export et représente 364 sociétés du secteur.

Ces lieux d'exposition sont ainsi de formidables lieux d'affaire et de partenariat technologique. Il est donc essentiel de prendre en compte dans la réflexion globale de votre activité sur le salon, en dehors de l'activité commerciale, les 3 piliers de l'intelligence économique que sont la **veille, l'influence et la sécurité économique**.

En effet, en plus d'une veille régulière tout au long de l'année, le salon est l'occasion de réaliser une **veille technologique et stratégique** importante à un moment clé pour le secteur d'activité. De fait, identifier les éléments mis en avant par la concurrence pour les prospections et les négociations menées permet d'en savoir plus sur sa stratégie commerciale.

Le salon est aussi un formidable lieu **d'influence**. L'ensemble des acteurs importants y sont présents : presse spécialisée, sites internet influents, organismes de certification et de contrôle, délégations étrangères, décideurs politiques. Dans ce contexte, il peut sembler intéressant de suivre la lutte d'influence qui s'est engagée dans le domaine des lanceurs spatiaux entre les nouveaux entrants et les acteurs historiques.

Enfin, et comme il a été indiqué précédemment, les salons professionnels sont des lieux privilégiés pour **capter de l'information technique ou commerciale** par des moyens techniques (interceptions de données/communications, prises de vues…) ou humains (questions intrusives, approche en dehors du salon…). Il est plus que jamais important de prendre la mesure de cette menace et d'assurer une surveillance constante de votre environnement et de vos équipements (cf. « Réflexes salons », page 4).

Les nombreuses opportunités commerciales, technologiques et stratégiques qu'offre un salon professionnel international ne doivent pas faire oublier la nécessité de protéger l'information. Il est donc important de **préparer** sérieusement toute participation à un salon professionnel, bien **en amont**, afin **d'anticiper** au mieux **les risques et les opportunités**.

CYBER

Les salons

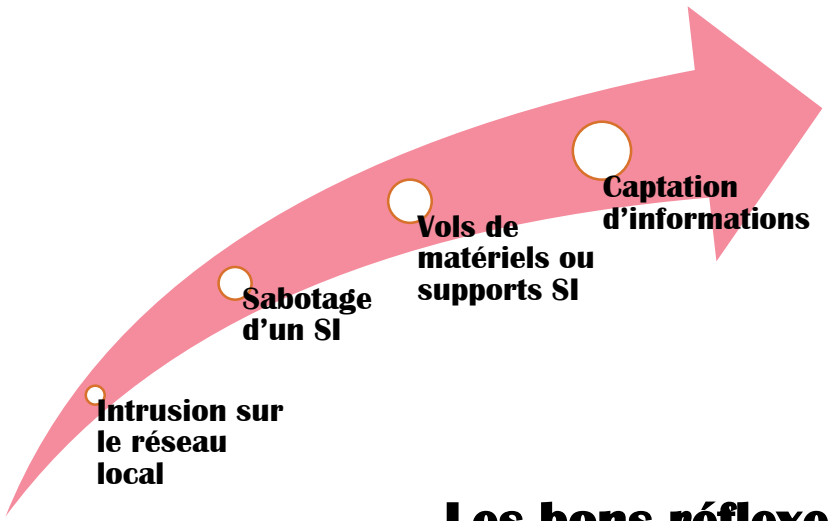
Quels risques sur les salons?

Un salon est perçu différemment, selon ce que chacun vient y chercher.

Néanmoins, il demeure une vérité communément admise : un salon d'armement ou autre est une forme d'intrusion consentie et une source d'informations pour la concurrence. Et dans le domaine cyber cette vérité se vérifie tout autant.

Il s'agit ici de faire un point des menaces principales et vous donner les conseils qui permettront d'en minimiser les conséquences.

Menaces



Les bons réflexes

AVANT

- **Préparer un matériel dédié**
- **Préparer un Plan de Continuité des Activités Informatiques**
- **Adopter un mot de passe durci**
- **Équiper chaque matériel de capacités de chiffrement (VPN, chiffrement données DD)**
- **N'amener sur le salon que les data indispensables**

PENDANT

- **Ne pas se connecter sur les bornes wifi libre accès sans protection**
- **Ne jamais laisser son matériel sans surveillance**
- **Ne jamais brancher des supports inconnus (utiliser un USB *blocker*)**
- **Etre attentif à l'orientation de vos écrans (utiliser un filtre écran)**

APRES

- **Sauvegarder ses données**
- **Changer de mot de passe**
- **Reformater les postes**

Pour toute question supplémentaire veuillez contacter :
dpsd-dsezp-ssi.cds.fct@intradef.gouv.fr

CYBER — FLASH Attaque cyber WANNACRY/WANNACRYPT

La vague d'attaques cyber du 13 mai a fait grand bruit car elle est d'une ampleur rarement constatée. Cela étant, la cinématique n'est pas novatrice. Elle consiste, malheureusement, en l'exploitation combinée de systèmes d'information non tenus à jour et d'un défaut de sensibilisation ou d'attention d'utilisateurs qui ont contribué à ce résultat.

Processus d'attaque :

- les modes d'attaque sont polymorphes (diffusion d'un mail piégé, clé USB infectée etc.) et reposent sur la propagation d'un ver informatique ;
- le ver se propage sur le réseau en exploitant une vulnérabilité du protocole SMB (voir ci-dessous) et chiffre les disques durs des stations et des serveurs touchés ;
- à ce stade, si vous n'avez pas de sauvegarde de vos données, la situation devient critique.

Cibles potentielles :

- toute machine sous environnement *Windows* obsolète (ex SCADA, réseau isolé etc.).

Actions à mener :

- rappel sur l'emploi des messageries (réfléchir avant de cliquer) ;
- faire des sauvegardes régulières de ses données ;
- tenir son système d'information à jour ;
- bloquer le protocole SMB 1.0 sur chaque machine ou par *group policy objects (*GPO).

En complément :

Cette attaque repose sur l'exploitation d'une vulnérabilité connue de *Windows*. *Microsoft* a sorti un correctif le MS17-010 sur ses versions encore soutenues (*Windows7*, *Windows10* et versions serveur soutenues) et le correctif KB4012598 pour les versions qui ne sont plus soutenues

Bulletin de l'ANSSI sur internet : **CERT2017-2017-ALE-010**

Le protocole SMB :

Server message block (SMB) est le protocole de *Microsoft* (architecture client /serveur) utilisé pour le partage de fichiers et d'imprimantes en réseau sur son système d'exploitation *Windows*.
Trois versions ont été élaborées à ce jour mais la plus ancienne (version 1) est activée par défaut dans *Windows10*.

Pour toute question supplémentaire veuillez contacter :
dpsd-dsezp-ssi.cds.fct@intradef.gouv.fr

PROTECTION

Usurpations d'identité

Les récentes affaires d'usurpation d'identité à des fins de détournement de fonds, doivent inciter les entreprises à se prémunir de ce risque souvent associé à la criminalité organisée. Des procédures simples peuvent ici suffire à écarter la menace :

- **vérification** de la qualité de l'appelant (rappel sur un numéro) ;
- procédure de la **double validation** pour l'engagement de fonds (services financiers et direction).

Sensibilisations

La DSEZP possède en son sein une équipe dédiée aux sensibilisations. Outre une prestation qui peut concerner vos collaborateurs sur les aspects protection du secret et/ou d'information stratégique, il est également possible d'effectuer une sensibilisation plus courte (15 min) ciblée sur les risques salons.

Réflexes salons

Il s'agit ici d'être vigilant durant toute la période du salon (**montage**, pendant le salon et **démontage**), et d'acquérir un certain nombre de réflexes :

- **identifier** (nom, prénom, société…) les personnes présentes sur vos stands (via badge, carte de visite…) ;
- **ne pas traiter d'informations sensibles/stratégiques dans les lieux publics** (transport, hôtel, restaurant…) et sur des réseaux non sécurisés (réseau Wifi tiers, SMS, appel non sécurisé…) ;
- **sécuriser et surveiller son matériel** tout au long du salon (ordinateur portable, maquette, matériel de démonstration…) ;
- **faire remonter tout incident** (individu au comportement suspect, vol de matériel, question intrusive…) à votre correspondant DRSD sur place.

Le conseil SOPHIA

Les procédures d'habilitation nécessitent encore parfois l'envoi des informations sous CD-ROM. Cet envoi doit se faire selon des procédures clairement définies et listées ci-dessous ; toute erreur pouvant entrainer du retard dans le traitement.

Rappel sur l'identification des CD-ROM :

Les informations présentes sur la pochette du CDROM seront :

- la mention « DIFFUSION RESTREINTE » ;
- le nom de la société ;
- le nom et l'adresse de l'établissement demandeur ;
- le code SE de l'établissement demandeur ;
- le N° de téléphone de l'émetteur du CDROM (en cas de problème) ;
- l'adresse de messagerie de l'émetteur du CDROM (en cas de problème).

Les informations présentes OBLIGATOIREMENT sur la face du CD :

- la mention « DIFFUSION RESTREINTE » ;
- le nom et l'adresse de l'établissement demandeur ;
- le code SE de l'établissement demandeur ;
- le N° de téléphone de l'émetteur du CDROM, (en cas de problème) ;
- l'adresse de messagerie de l'émetteur du CDROM, (en cas de problème).

Le CDROM dans sa pochette sera introduit dans une double enveloppe :

- l'enveloppe interne comportera la mention « DIFFUSION RESTREINTE » et comportera la mention « **à l'attention du DRSD/CNHD** ».
- l'enveloppe externe comportera l'adresse postale du CNHD :

Ministère de la Défense
CS 21 623 - Case 44
60 boulevard du général Martial VALIN
75509 PARIS CEDEX 15