Bilan Cert-IST 2015 des failles et attaques

1) Introduction

Comme chaque année, le Cert-IST fait un bilan de l'année écoulée afin de mettre en évidence les tendances sur l'évolution des attaques et d'aider les acteurs à mieux se protéger.

Nous présentons tout d'abord un rétrospective des événements les plus marquants de l'année 2015 (cf. chapitre 2).

Nous donnons ensuite un récapitulatif des productions du Cert-IST au cours de cette année (cf. chapitre 3).

La conclusion (cf. chapitre 4) effectue une synthèse du paysage actuel de la cyber-menace et des challenges auxquels l'entreprise doit faire face.

Nota : Les encadrés bleus insérés tout au long du bilan correspondent à des articles ou des annonces qui ont été publiés au cours de l'année dans le bulletin mensuel du Cert-IST.

➢ A propos du Cert-IST

Le Cert-IST (**C**omputer **E**mergency **R**esponse **T**eam - **I**ndustrie, **S**ervices et **T**ertiaire) est un centre d'alerte et de réaction aux attaques informatiques destiné aux entreprises. Créé en 1999, il aide ses adhérents à identifier les menaces en analysant quotidiennement les nouvelles vulnérabilités, leurs criticités et les moyens de protection pour y répondre. En cas d'incident de sécurité touchant l'un de ses adhérents, le Cert-IST peut apporter son aide dans l'investigation de cet incident et permettre une remise en service opérationnelle et sécurisée.

2) Les événements les plus marquants de 2015

2.1 Les attaques visant le logiciel Adobe Flash

De nombreuses vulnérabilités ont été découvertes dans Adobe Flash, et ce composant a fait l'objet de multiples attaques au cours de l'année 2015. Nous avons effectivement publié cette année pour ce composant 18 avis et 5 DG (sur un total de 12 DG).
Le cabinet d'expertise Recorded Future a publié un rapport comportant l'analyse d'une centaine « d'exploits kit » : il indique que les vulnérabilités Flash sont des points d'intrusion dans 8 cas sur 10, devant Internet Explorer.

Cette situation a amené de nombreux acteurs du web à agir pour l'abandon de Flash :

- Mozilla a bloqué par défaut les contenus Flash,
- Alex Stamos, le chef de sécurité de Facebook, a demandé à Adobe, via un tweet de donner une date de fin de vie pour le plugin,
- YouTube a abandonné Flash pour HTML5.

On peut noter aussi que le plugin Java, un autre composant qui a eu la vedette en termes d'attaques ces dernières années, semble également être sur la sellette.
Alors que de nombreux navigateur bloquaient ce plugin depuis déjà plusieurs mois, Oracle a en effet annoncé sa disparation et appelé à utiliser à sa place Java Web Start.

L'évolution des navigateurs vers un abandon des plugins se confirme donc.

Extrait de la Une du bulletin Cert-IST de janvier 2015

Plusieurs nouvelles vulnérabilités dans le composant Flash ont été découvertes fin janvier à l'occasion d'attaques 0-day. Nous détaillons cet événement dans notre rubrique « Attaques du mois ». Cette situation rappelle celles vues en 2010 (multiples attaques PDF et Flash), puis en 2012 (attaques Java), et montre une nouvelle fois que le poste de travail de l'utilisateur est exposé à un risque élevé d'attaques lors de sa navigation sur Internet.

Extrait de la Une du bulletin Cert-IST de juin 2015

Une fois de plus des attaques ont visé le logiciel Adobe Flash Player. Ce composant est désormais en tête des logiciels les plus dangereux sur le poste de travail.

Extrait de la rubrique «Attaques du mois» du bulletin Cert-IST de juin 2015

Les attaques contre Flash ne sont pas nouvelles : elles ont régulièrement fait l'objet de Dangers Potentiels ou de messages Vuln-coord au cours de ces dernières années, mais elles passent maintenant en tête devant des logiciels comme Java ou Adobe (pdf) Reader qui sont désormais moins souvent agressés. Ce phénomène amène à se poser la question : faut-il garder Flash ou l'interdire lors de la navigation sur Internet ? Le journaliste Brian Kreb a tenté une expérience (cf. son article intitulé « A Month Without Adobe Flash Player ») et il conclut que Flash ne lui a manqué que 2 fois : si on ne peut pas l'interdire, il faudrait donc désactiver Flash la plupart du temps et ne le réactiver que lorsque c'est strictement nécessaire par exemple avec un mécanisme comme le « Click to play ».

2.2 La sécurité offensive dévoilée : le cas « Hacking-Team »

Le secteur de la sécurité offensive se développe depuis plusieurs années (cf. les bilans des années précédentes). Dans un premier temps, il a été découvert que les états étaient actifs dans ce secteur, et l'on pouvait craindre que des sociétés privées envahissent ce marché. L'actualité de 2015 a confirmé cette inquiétude.

Suite au piratage de la société Hacking-team, les données dérobées ont mis en lumière le développement d'outils offensifs ainsi que l'existence d'un marché des 0-days.
Hacking-team achetait effectivement des 0-days à plusieurs fournisseurs appelés « 0-day brokers ».

Au-delà de la poignée de « 0-day brokers » mis en évidence à cette occasion, on a vu aussi l'apparition de nouveaux brokers.

La société zerodium.com (fondée par le créateur de VUPEN) a été lancée en 2015 et a annoncé avoir acheté une attaque 0-day contre IOS pour 1 million de dollars.

Début 2016, l'explosion du nombre de brokers continue : 2 ou 3 annonces de nouvelles sociétés de ce type ont été publiées. Il est possible d'imaginer une uberisation de la sécurité informatique où des individus vendraient des failles qu'ils auraient découvertes.
On passerait d'un modèle de vente de prestation d'audit (modèle classique), à un modèle de vente de failles découvertes par des particuliers (modèle uberisé ou collaboratif).

Extrait de la Une du bulletin Cert-IST de juillet 2015

La très controversée société italienne de sécurité offensive « Hacking Team » s'est faite pirater début juillet, et 400 Go de données volées chez eux ont ensuite été rendues publiques. L'exploration de ces données (correspondance mail, code source d'outils d'attaques, etc.) suscite de nombreux articles de presse qui mettent en pleine lumière des phénomènes que l'on connaissait en fait déjà.

Que retenir parmi ces annonces ?
- Tout le monde peut se faire pirater !
- Le marché des 0-day est florissant (voir cet article, ainsi que ce mail de Hacking Team) et les failles se vendent biens (ex. 45 000 dollars pour une faille Flash),
- La sécurité offensive intéresse beaucoup les états, qu'il s'agisse de pays démocratiques (avec des utilisations a priori légitimes, voir par exemple ces échanges supposés avec le FBI) ou des pays totalitaires (dans le but de traquer les opposants).

2.3 Dridex et Crypto-Locker : des nuisances très bien orchestrées

Les entreprises ont été attaquées cette années par les vagues d'infections Crypto-Locker (en début d'année) puis Dridex (à partir du mois de juin).

Ces malwares utilisent la technique d'attaque basique, largement utilisée dans les années 1990, d'envois d'email piégés pour infecter le poste des utilisateurs qui ouvrent la pièce jointe ou se rendent sur le site web pointé par le mail.

Les observateurs ont noté le retour des macros virus qui avaient quasiment disparus (cf. une brève de notre bulletin du mois de juin).

Bien qu'elles soient moins sophistiquées techniquement que les attaques de cyber-espionnage, de type APT, ces attaques ont été très efficaces et ont apparemment provoqué des dégâts car elles sont très bien orchestrées et les antivirus ne les détectent pas immédiatement.

Comme les messages de Dridex étaient souvent des factures relatives à des commandes, il est probable que ces attaques ciblaient principalement les entreprises. Celles-ci étant probablement plus à même de payer les rançons demandées pour récupérer des documents précieux.

On peut noter la difficulté pour démanteler ces gangs : une grande campagne de « take-down » a été lancée contre Dridex en septembre 2015 avec un résultat mitigé car les vagues d'infection ont continué.

Les entreprises ont semblée bien démunies pour faire face à ces attaques, et il est intéressant de noter que certaines d'entre elles ont utilisé des IOC pour mettre en place des règles de blocage des flux réseaux.

Cela nous interroge sur l'inefficacité des moyens de protection actuels et sur leur évolution.

VulnCoord-2015.020 : Spam massif DRIDEX/DYREZA et Macro Office malveillantes
Extrait de la rubrique «Attaques du mois» du bulletin Cert-IST de juin 2015

Autre événement important pour le mois de juin 2015 : le lundi 8 juin 2015 une vague de mails malveillants visant la France est apparue. Il s'agit de mails rédigés en français à propos de factures en cours avec un fichier « .doc » (ou « .zip ») attaché. Lorsque ce fichier est ouvert, il affiche un message du type « veuillez autoriser les macros pour visualiser ce fichier ». Si la victime le fait, une macro malveillanes se déclenche : elle télécharge et installe sur le poste un malware bancaire de la famille de « Dridex ».

Bien que très classique, ce schéma d'attaque illustre des problèmes bien réels :

- Les antivirus ne détectent pas l'attaque et les procédures de désinfections sont difficiles à mettre au point. La réinstallation complète des postes infectés et alors souvent la solution la plus sûre.
- Après avoir presque disparu, les virus macros (les macros malveillantes) font leur retour avec succès. Nous parlons de ce phénomène dans un des articles de ce bulletin.

Enfin, il faut noter que les cyber-criminels qui montent ces attaques sont bien organisés. Par exemple, le malware Dridex qui infecte le poste, utilise pour dialoguer avec son serveur C&C un serveur de rebond (un proxy) installé sur des équipements de type « routeurs personnels » compromis (voir cet article pour plus de détails). Il est ainsi plus difficile de neutraliser cette infrastructure réseau.

2.4 TV5-Monde : L'essor des attaques par sabotage

Cette attaque subie au début du mois d'avril par TV5-Monde a été très médiatisée. Cependant, très peu d'éléments techniques ont été diffusés sur l'attaque, ce qui a laissé la place à beaucoup de spéculations, en particulier sur les auteurs. Le soupçon s'est porté d'abord vers les Islamistes puis ensuite sur des russes.

Cet évènement est une illustration « à la française » de l'attaque subie par Sony fin 2014, et il a montré :

- l'importance des dégâts que peut faire une attaque informatique,
- que toutes les entreprises sont potentiellement exposées à ce type d'attaques,
- que les entreprises doivent envisager la possibilité d'être la cible d'attaques provoquant la destruction complète de leur système d'information (écrasement du MBR de toutes les machines infectées).

La Une du bulletin Cert-IST d'avril 2015

La cyber-attaque subie début avril par TV5-Monde ressemble à un sabotage informatique. Aucun détail technique n'a été publié officiellement et on ne peut que spéculer sur la nature réelle de cet incident. Mais visiblement plusieurs serveurs internes ont été brutalement mis hors service (les serveurs d'encodage vidéo, les serveurs de messagerie ont tous les 2 été cités dans la presse). On peut alors se demander si les pirates n'auraient pas installé sur tous les postes Windows affectés un logiciel de destruction du poste (un « Wiper »). Cette technique a déjà été vue dans les incidents Sony Pictures Entertainment (novembre 2014 aux USA, voir notre article sur ce sujet) ou DarkSeoul (mars 2013 en Corée du Sud) ou encore Aramco (août 2012 en Arabie saoudite). Elle semble de plus en plus courante et doit donc être considérée comme un risque tout à fait probable en cas d'intrusion au sein du système informatique. L'US-CERT a publié fin 2013 la note ST13-003 pour prendre en compte ce risque (et aussi, fin 2014, l'alerte TA14-353A suite à l'incident Sony). Les recommandations formulées sont très nombreuses. Pour faire face à ce type de risque, les mesures prioritaires nous semblent :

- Limiter la propagation de l'intrusion en cloisonnant les réseaux et en limitant les comptes ayant les privilèges administrateur.
- Disposer de procédures de reprise après incident pour les serveurs d'infrastructure et s'assurer que le cas d'une attaque informatique volontaire à bien été pris en compte (par exemple un système RAID ne protège pas contre un écrasement volontaire des disques).

Nota : Pour plus d'information sur ces malwares de type « Wiper », on pourra par exemple consulter cette analyse du CERT-FR (sur le malware Sony) ou cette étude d'IBM (recensement des « Wipers » connus).

2.5 Vol de données : de plus en plus de cas médiatisés

Il y a eu de très nombreux cas de vol de données personnelles dans l'actualité 2015 :

- En début d'années plusieurs cas de vols de données de santé, via des attaques contre des mutuelles (cf. attaque qui a visé la société Anthem et qui pourrait avoir entraîné le vol de données personnelles de 80 millions de clients) ou des établissements de santé (laboratoires, hôpitaux, ..)
- Au mois de juin une agence américaine, l'Office of Personnel Management (OPM), a fait l'objet d'une cyberattaque ayant eu pour conséquence le vol de données confidentielles concernant plus de 20 millions de fonctionnaires américains.
- Au mois d'août c'est le site de rencontres extraconjugales « Ashley Madison » qui a fait l'objet d'une attaque également remarquable par son ampleur (10 Go de données compressées, liées à 33 millions de comptes), et par le caractère intime des informations divulguées.
- En plus de ces attaque d'envergure de nombreux vols de données personnels ont été divulgués au long de l'année : Morgan Stanley, 000Webhost , VTech, etc…

Bien que ces attaques soient très différentes et que certaines soient plus préoccupantes que d'autres, elles mettent en lumière les faiblesses de systèmes contenant de nombreuses données confidentielles.

Il semble que les attaques se déplacent vers des cibles moins protégées mais tout aussi lucrative, et visent désormais davantage les données personnelles et les identités numériques que les informations bancaires.

2.6 Vulnérabilités dans les anti-virus : tous vulnérables ?

En 2014, les ingénieurs en sécurité de Google ont lancé le programme « Project Zero », afin de détecter les failles Zero-Day et de réduire le nombre de failles critiques sur Internet. Puis, en 2015 plusieurs chercheurs de ce projet ont concentré leurs efforts sur des produits de sécurité (antivirus et plus généralement les outils de type end-point protection).

Et à ce jour des vulnérabilités ont été découvertes dans plusieurs antivirus de Kaspersky, ESET, Avast, Sophos, ainsi que dans des équipements FireEye.

La perfection n'étant pas de ce monde, il n'est pas surprenant qu'en cherchant des vulnérabilités dans ces produits, on en découvre, et le nombre de vulnérabilité étant à l'arrivée relativement limité, cela ne remet pas en cause à ce stade leur fiabilité.

Par leur travail, les équipes de « Project Zero », ont participé à l'amélioration de la sécurité de ces produits.

2.7 SCADA, voitures connectées et Internet des objets : des cibles pour les attaques futures

L'actualité de l'année 2015 a montré :

- qu'il était a priori possible de **hacker un avion**.

  En début d'année, des annonces ont affirmé qu'il était possible de hacker un avion via le réseau Wi-Fi destiné aux passager. Puis les experts ont dit que la séparation des réseaux « vol » et « divertissement » rendait ces attaques impossibles. En fin d'année, le directeur de l'Agence européenne de la sécurité aérienne (AESA) a déclaré que l'aviation était vulnérable à la cybercriminalité.

- que l'on pouvait **prendre le contrôle de certaines voitures.**

  Au mois de juillet, deux experts en sécurité ont effectivement pu prendre le contrôle d'une automobile à distance, via Internet, en exploitant une vulnérabilité d'un module multimédia embarqué dans les Jeep cherokee de Fiat Chrysler.

- que la sécurité des systèmes informatiques des **Aéroports** était bien trop faible pour des installations aussi critiques.

  Au mois de juin, la compagnie aérienne polonaise, LOT, a dû annuler plusieurs de vols suite à une attaque informatique ciblant son système gérant les opérations au sol.
  A la fin du mois d'octobre, lors de la conférence Hackito Ergo Sum 2015, un chercheur a fait un retour sur un audit qu'il a réalisé sur la sécurité d'un des plus grands aéroports internationaux de l'Union européenne. Son équipe a trouvé près de 60 vulnérabilités, dont certaines très critiques !
  Nota : Au début de l'année 2016 une attaque du principal aéroport d'Ukraine a confirmé cette menace.

- que les **Equipements médicaux** étaient également menacé par des cybers attaques.

  Lors de la conférence Hack.lu 2015, Marie Moe (une ancienne responsable du Cert Norvégien) a fait une présentation sur la sécurité des pacemakers pour alerter non seulement la population, mais aussi les constructeurs d'équipements dans le domaine médical sur les problématiques de sécurité qui commencent à se multiplier.

  A la conférence Derbycon 2015 deux chercheurs en sécurité (Scott Erven et Mark Collao) ont présenté de nombreuses vulnérabilités qu'ils ont découvert dans différents équipements médicaux (appareils d'anesthésie, équipements de cardiologie, systèmes d'injection, stimulateurs cardiaques, …).

Extrait de la rubrique «Attaques du mois» du bulletin Cert-IST d'août 2015

Comme mentionné dans notre Une, au mois d'août il a également été signalé plusieurs cas de vulnérabilités permettant des attaques de voitures connectées (vulnérabilités des voitures Tesla, prise de contrôle à distance d'un Jeep, vulnérabilité des antivols électroniques MegKamos Crypto). Le cas le plus préoccupant est celui de l'attaque contre les Jeep Cherokee présentée à la conférence Blackhat USA. Les auteurs ont en effet montré qu'ils avaient pris le contrôle d'une jeep à travers Internet et qu'ils l'avaient faite sortir de la route. Fiat Chrysler a lancé suite à cela un rappel affectant 1,4 millions de véhicules de la marque. Dans le domaine des objets connectés, on peut noter aussi qu'aux Etats-Unis une pompe à perfusion a été interdite pour cause de vulnérabilités critiques.

L'informatique est partout et les attaques impactent nos vraies vies : l'informatique est de plus en plus un composant central de la vie courante. Au-delà de l'intrusion visible dans notre vie (BYOD, traçage) il est aussi omniprésent, plus discrètement, dans les systèmes d'automatismes (péages, informatique embarquée, …) et dans des systèmes critiques (aéroports, usines, réseaux de distribution d'énergies, etc…). Les attaques informatiques sur ces systèmes, nous impactent alors dans notre quotidien. Ce n'est plus une intrusion ou une panne informatique, mais toute une région qui est privée d'électricité par exemple.

A ce jour ces attaques sont encore à un stade de « prototypes » et il y a une prise de conscience de la nécessité impérative à sécuriser tous ces équipements critiques.

En 2015 un décret a défini des obligations pour les opérateurs d'importance vitale (OIV), et il y aura probablement bientôt des mesures législatives contraignant les fabricants d'objets connecté à prendre en compte la sécurité. Il pourrait y avoir dans le futur des normes de sécurité « cyber », tout comme aujourd'hui il y a des normes de sécurité physiques pour de nombreux objets (comme les jouets par exemple).

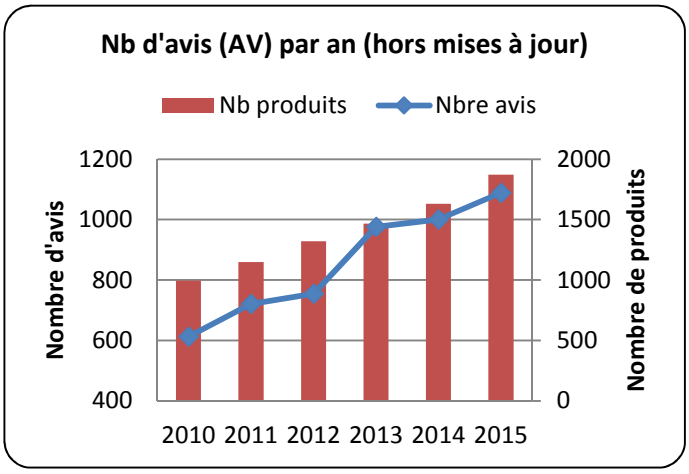
3) La production du Cert-IST en 2015

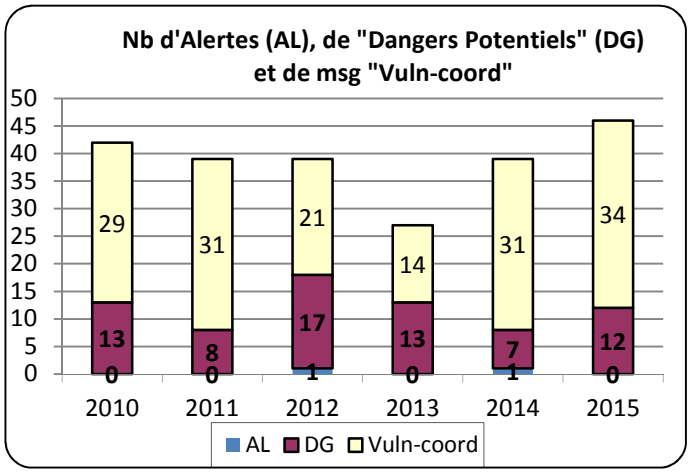
3.1 Veille sur les vulnérabilités et des menaces

Dans le cadre de son activité de veille sur les vulnérabilités et les menaces, le Cert-IST suit de façon continue, différentes sources d'informations (annonces constructeurs, blogs sécurité, mailing-lists, échanges privés entre CERTs, etc.) afin d'être informé des nouvelles vulnérabilités. Ces informations sont analysées quotidiennement pour fournir à nos adhérents des informations triées, qualifiées et priorisées. Le Cert-IST émet ainsi plusieurs types de publications :

- Les **Avis de sécurité** : ils décrivent les nouvelles vulnérabilités découvertes dans les produits suivis par le Cert-IST. Ces avis sont enrichis de façon continue avec des mises à jour mineures ou majeures. Ces dernières correspondent typiquement au cas où des programmes d'attaques – des "exploits" – sont publiés.
- Des **Alertes**, des **Dangers Potentiels** et des **messages "Vuln-coord"**. Les Alertes du Cert-IST sont utilisées pour les menaces majeures nécessitant un traitement prioritaire. L'émission d'une alerte est un événement rare : par exemple le Cert-IST a émis en 2014 une alerte sur la vulnérabilité Shellshock. Les Dangers Potentiels décrivent des menaces significatives mais non encore imminentes (ou d'une gravité modérée) pour lesquelles le Cert-IST recommande des mesures de protection spécifiques. Les messages "Vuln-coord" enfin, sont des informations de coordination qui attirent l'attention sur des vulnérabilités particulières mais d'une dangerosité immédiate plus faible. Ces 3 catégories complémentaires sont axées sur les risques d'attaques alors que les avis de sécurité répertorient eux de façon systématique toutes les vulnérabilités (quelle que soit leurs probabilités d'être utilisées dans des attaques).

Les graphiques ci-dessous montrent la production du Cert-IST au cours des dernières années.





Ainsi, en 2015, le Cert-IST a publié :

- **1 088 avis de sécurité**, suivis de façon continue au cours de l'année avec 3 069 mises à jour mineures et 159 mises à jour majeures. Le nombre d'avis est en augmentation constante depuis plusieurs années (cf. la courbe ci-dessus), avec une augmentation de +12% par rapport à 2014. Cette augmentation continue montre que la découverte de vulnérabilités est un phénomène en constante augmentation. Le maintien du niveau de sécurité passe donc forcément par une application régulière des correctifs de sécurité sur ces produits. Au 31/12/2015 le Cert-IST suivait les vulnérabilités concernant 1 871 produits et 14 762 versions de produits.

- **0 Alerte, 12 Dangers Potentiels et 34 messages "Vuln-coord"**. En 2015 aucune alerte n'a été émise. Le nombre de dangers Potentiels a quant à lui, augmenté pour passer de 7 à 12 (dont 5 sur le produit Adobe Flash Player), et le nombre de messages Vuln-coord est passé de 31 à 34.

3.2 Veille technologique

En plus de la veille sur les vulnérabilités, le Cert-IST publie également des bulletins de veille technologique :

- Un bulletin quotidien de veille média recense les articles les plus intéressants parus sur Internet sur un ensemble de sites francophones et anglophones traitant de sécurité.
- Un bulletin mensuel de veille SCADA présente une synthèse de l'actualité sur la sécurité des systèmes industriels.
- Un bulletin mensuel généraliste donne une synthèse de l'actualité du mois (en termes d'avis et d'attaques) et traite de sujets d'actualité au travers d'articles rédigés par le Cert-IST.

4) Conclusions

Les entreprises doivent encore et toujours composer avec une situation de plus en plus complexe.

Les constats figurant dans notre bilan 2014 restent toujours d'actualité :

- l'informatique a une place de plus en plus centrale dans la vie quotidienne, aussi bien sur le plan professionnel que sur le plan personnel ; pour mémoire, la thématique du FORUM Cert-IST 2015 a été « La transformation digitale et la sécurité ».
- l'évolution des technologies pousse à disperser l'information (avec par exemple le développement du Cloud et du BYOD) et cherche à rendre toujours plus facile l'accès à cette information.

D'autre part, le risque d'intrusion a augmenté de façon importante au cours des dernières années.

De nouveaux attaquants, visant spécifiquement les entreprises (cyber-espionnage, cyber-sabotage, ramsomware) ont été identifiés.

2015 confirme cette montée du risque :

- Les attaques sont plus fréquentes en particulier le vol de données de grande ampleur et les ramsonwares.
- Le "cyber" est devenu un enjeu stratégique pour les états ; en France, le décret concernant les obligations des Opérateurs d'Importance Vitales (OIV) est paru en 2015.
- Les Systèmes industriels, les voitures connectées et l'Internet des Objets sont devenus des cibles très prisées des attaquants et de nombreuses vulnérabilités concernant ces domaines sont découvertes.

Pour s'adapter à cette situation, l'entreprise a besoin tout d'abord d'être tenue au courant des menaces et de leurs évolutions. Le Cert-IST, au travers de son activité de veille technologique et de ses bilans, lui donne une vision argumentée de la menace.

Face à la montée du risque, chaque entreprise doit aussi :

- évaluer son exposition à ce type d'attaques,
- renforcer ses défenses,
- développer sa capacité de détection et de réaction aux intrusions : collecte des logs, supervision de sécurité et recherche active des attaques, à l'aide notamment d'IOC (Indicators Of Compromise).

Le Cert-IST travaille actuellement à la mise en place d'un nouveau service autour des IOCs.

Fin du document