Glossaire

CYBERSÉCURITÉ

meritis

A

ARNAQUE (OU FRAUDE) AU PRÉSIDENT

Pratique consistant pour des escrocs à convaincre le collaborateur d'une entreprise d'effectuer en urgence un virement important à un tiers.

ATAWAD (ANY TIME, ANY WHERE, ANY DEVICE)

Capacité d'un usager en situation de mobilité à se connecter à un réseau sans contrainte de temps, de localisation ou de terminal.

AVEC

« Apportez Votre Équipement personnel de Communication ». Voir BYOD.

B

BOMBE PROGRAMMÉE, BOMBE LOGIQUE (LOGIC BOMB)

Logiciel malveillant conçu pour causer des dommages à un système informatique et qui est déclenché lorsque certaines conditions sont réunies.

Remarques : Certains virus contiennent une fonction de bombe logique : déclenchement à date fixe, déclenchement quand une adresse réticulaire (URL) particulière est renseignée dans le navigateur, etc.

Source : CLUSIF et OSSIR

C

CANULAR (HOAX)

Information vraie ou fausse, souvent transmise par messagerie électronique ou dans un forum, et incitant les destinataires à effectuer des opérations ou à prendre des initiatives, souvent dommageables.

Remarques : Il peut s'agir d'une fausse alerte aux virus,de chaîne de solidarité, pétitions, promesse de cadeaux, etc. Quelques canulars fréquents sont répertoriés sur des sites dédiés comme « Hoaxbuster » ou « Hoaxkiller ».

CHEVAL DE TROIE

Programme donnant l'impression d'avoir une fonction utile, mais qui possède par ailleurs une fonction cachée et potentiellement malveillante.

CHIFFREMENT DES DONNÉES

Technique rendant les données illisibles, sauf si une action spécifique (déchiffrement) est exercée pour en autoriser l'accès.

CLOUD ACT

Loi fédérale des États-Unis adoptée en 2018 sur la surveillance des données personnelles, notamment dans le cloud. Cette loi permet aux forces de l'ordre US de contraindre les fournisseurs de services américains à fournir les données demandées stockées sur des serveurs, qu'ils soient situés aux États-Unis ou dans des pays étrangers.

CODE D'EXPLOITATION (EXPLOIT)

Tout ou partie d'un programme permettant d'utiliser une vulnérabilité ou un ensemble de vulnérabilités d'un logiciel (du système ou d'une application) à des fins malveillantes.

Remarques : Les objectifs malveillants consistent souvent en une intrusion, une élévation de privilèges ou un déni de service. L'exploitation peut se faire directement à partir du système ciblé si l'utilisateur malveillant possède un accès physique (local exploit), ou à distance s'il s'y connecte (remote exploit).

Source : CLUSIF et OSSIR

C

CODE MALVEILLANT, LOGICIEL MALVEILLANT (MALICIOUS SOFTWARE, MALWARE)

Tout programme développé dans le but de nuire à ou au moyen d'un système informatique ou d'un réseau.

Remarques : Les virus ou les vers sont deux types de codes malveillants connus.

CYBERCRIMINALITÉ

Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes. d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

CYBERDÉFENSE

Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.

CYBERESPACE

Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.

CYBERSÉCURITÉ

État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense.

CYBERSQUATTING

Action malveillante qui consiste à faire enregistrer un nom de domaine dans le seul but de bloquer toute attribution ultérieure de ce nom au profit de titulaires plus naturels ou légitimes.

Un compte privilégié est un compte bénéficiant de droits d'accès étendus permettant à des utilisateurs malveillants de porter plus facilement ou plus gravement atteinte à la sécurité ou au fonctionnement du SIIV. Les comptes privilégiés sont par exemple des comptes d'administrateurs ou des comptes d'utilisateurs disposant de droits à fort impact métier dans une application.

Source : CLUSIF et OSSIR

D

DÉNI DE SERVICE

Action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu.

E

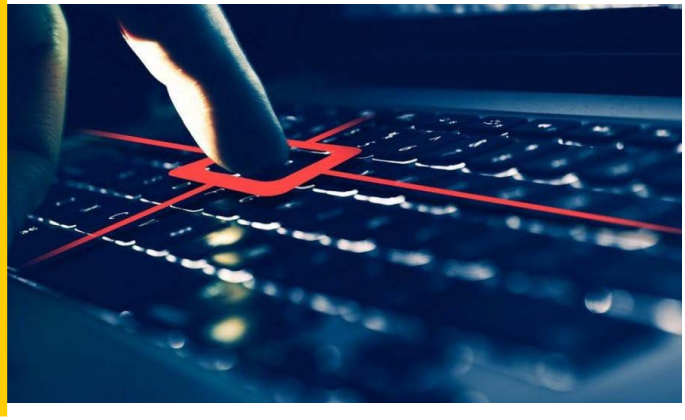
E-DISCOVERY

Loi américaine permettant l'investigation et l'instruction préalable au procès civil et commercial qui est essentielle pour toute action en justice aux États-Unis. Les demandes de communication qui sont faites à cette occasion auprès des entreprises peuvent concerner des milliers de courriers électroniques des salariés. Le refus d'obtempérer peut déboucher sur un jugement défavorable.

ESPIOGICIEL (SPYWARE)

Logiciel dont l'objectif est de collecter et de transmettre à des tiers des informations sur l'environnement sur lequel il est installé, sur les usages habituels des utilisateurs du système, à l'insu du propriétaire et de l'utilisateur.

H



[HAMEÇONNAGE]

Voir Phishing.

Source : CLUSIF et OSSIR

I

IAAS (INFRASTRUCTURE AS A SERVICE)

Infrastructures de datacenters où le client déploie son système d'information. Par exemple : Amazon Web Service, Google Cloud Platform, Microsoft Azure, etc.

INCIDENTS DE SÉCURITÉ

Un incident de sécurité est un événement qui porte atteinte à la disponibilité, la confidentialité ou l'intégrité d'un bien. Exemples : utilisation illégale d'un mot de passe, vol d'équipements informatiques, intrusion dans un fichier ou une application, etc.

INGÉNIERIE SOCIALE

Manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes.

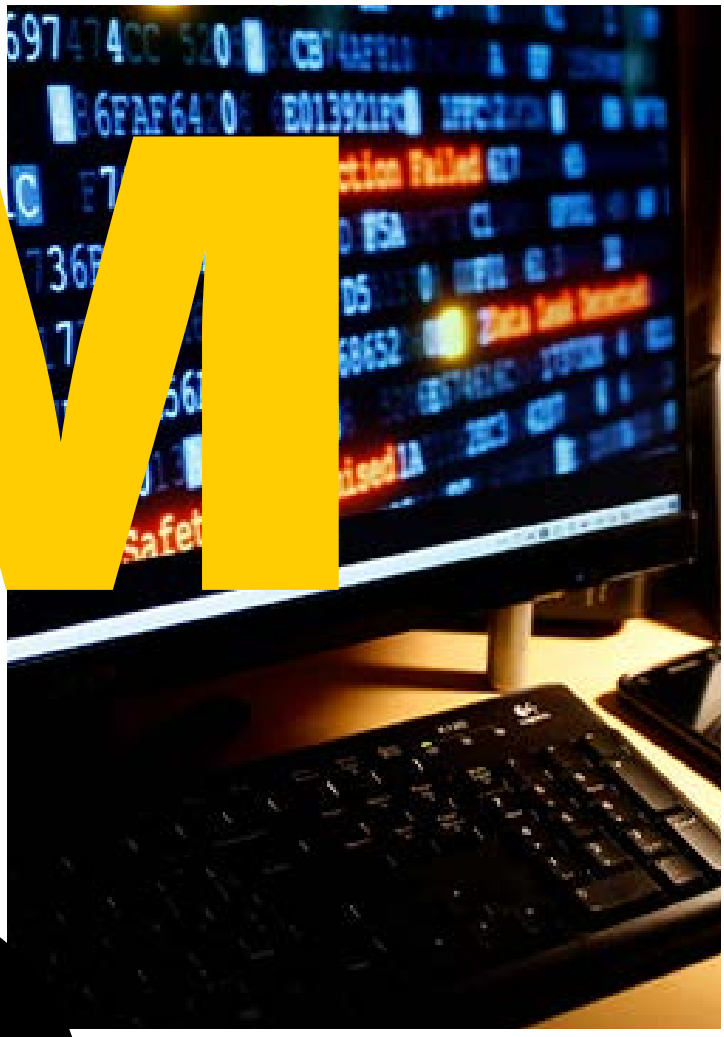
INTÉGRITÉ

Garantie que le système et l'information traitée ne sont modifiés que par une action volontaire et légitime.

INTRUSION

L'intrusion est le fait, pour une personne ou un objet, de pénétrer dans un espace (physique, logique, relationnel) défini où sa présence n'est pas souhaitée.

M



MÉTADONNÉE

Donnée servant à définir ou à décrire une autre donnée, quel que soit son support. Un exemple type est d'associer à une donnée la date à laquelle elle a été produite ou enregistrée, ou à une photo les coordonnées GPS du lieu où elle a été prise.

MFA

Multiple Factor Authentification, ou vérification en deux étapes, est une méthode par laquelle un utilisateur peut accéder à une ressource informatique (un ordinateur, un téléphone intelligent ou encore un site web) après avoir présenté deux preuves d'identité distinctes à un mécanisme d'authentification.

MOBIQUITÉ

Fusion des termes « mobilité » et « ubiquité ». Voir ATAWAD.

Source : CLUSIF et OSSIR

O

OUTILS DE DISSIMULATION D'ACTIVITÉ (ROOTKIT)

Tout programme ou ensemble de programmes permettant de dissimuler une activité, malveillante ou non, sur une machine. Par extension, tout programme ou ensemble de programmes permettant à une personne malveillante de maintenir un contrôle illégitime du système d'information en y dissimulant ses activités. Par extension, programme ou ensemble de programmes permettant de dissimuler une activité, malveillante ou non, sur une machine. L'activité dissimulée peut être une activité sur le système de fichiers (création, lecture, écriture), une activité réseau, une activité en mémoire. Pour cela, un rootkit peut travailler dans l'environnement de l'utilisateur, sans droits particuliers, ou en profondeur dans le système d'exploitation, nécessitant par conséquent des droits d'exécution élevés.

Remarques : L'installation de ces programmes nécessite que le système soit préalablement compromis (cheval de Troie, intrusion). Ces programmes modifient souvent les commandes usuelles de l'administrateur, afin de dissimuler toute trace de leur présence. Ils effectuent aussi fréquemment plusieurs opérations au niveau du noyau du système d'exploitation, comme l'installation de portes dérobées, la capture des frappes clavier, etc. Un outil de dissimulation d'activité n'a pas pour but d'offrir un accès quelconque à la machine hôte. En revanche, la plupart de ces outils malveillants embarquent des fonctionnalités de porte dérobée permettant à l'auteur un accès à distance et un maintien sur le système compromis.

Source : CLUSIF et OSSIR

P

PAAS (PLATFORM AS A SERVICE)

Plateforme intégrant les services techniques essentiels (envoi de courriel, stockage de données, puissance de calcul, etc.) où le client installe ses couches métier. Par exemple, stockage de données en ligne, hébergeur d'environnement web, etc.

PHISHING

Vol d'identités ou d'informations confidentielles par subterfuge. Un système d'authentification est simulé par un utilisateur malveillant qui essaie de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime.

PORTE DÉROBÉE

Accès dissimulé, soit logiciel soit matériel, qui permet à un utilisateur malveillant de se connecter à une machine de manière furtive.

R

RÉSEAUX DE MACHINES ZOMBIES (BOTNET)

Forme d'extorsion imposée par un code malveillant sur un utilisateur du système. Le terme « rançongiciel » (ou ransomware en anglais) est une contraction des mots « rançon » et « logiciel ». Il s'agit donc par définition d'un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon.

RENIFLEUR (SNIFFER)

Outil matériel ou logiciel dont l'objet est de capturer les trames transitant sur le réseau.

Remarques : Si les trames contiennent des données non chiffrées, un utilisateur malveillant peut aisément récupérer des données confidentielles, comme des mots de passe, des courriers électroniques, des contenus de pages internet, etc. L'utilisateur malveillant peut aussi, à partir des trames, récupérer des informations sur les systèmes échangeant les trames, comme le système d'exploitation ou les services employés.

RANÇONGICIEL

Un Botnet, autrement dit un réseau de bots (botnet : contraction de réseau de robots), est un réseau de machines compromises à la disposition d'un individu malveillant (le maître). Ce réseau est structuré de façon à permettre à son propriétaire de transmettre des ordres à tout ou partie des machines du botnet et de les actionner à sa guise. Remarques : Certains ensembles peuvent atteindre des nombres considérables de machines (plusieurs milliers). Celles-ci peuvent faire l'objet de commerce illicite ou d'actions malveillantes contre d'autres machines. Elles sont souvent pilotées par des commandes lancées à travers un canal de contrôle comme le service IRC (Internet Relay Chat).

RGPD (RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES)

Règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel.

Source : CLUSIF et OSSIR

S

SAAS (SOFTWARE AS A SERVICE)

Logiciel où le client assure la personnalisation de ses processus métier et de son identité visuelle. Par exemple, Microsoft Office 365, Salesforce, etc.

SHADOW IT

Solutions informatiques non connues des équipes informatiques et donc hors du périmètre de suivi, de protection et de contrôle.

SURFACE D'ATTAQUE

Somme des différents points faibles (les « vecteurs d'attaque ») par lesquels un utilisateur non autorisé (un « pirate ») pourrait potentiellement s'introduire dans un environnement logiciel et en soutirer des données.

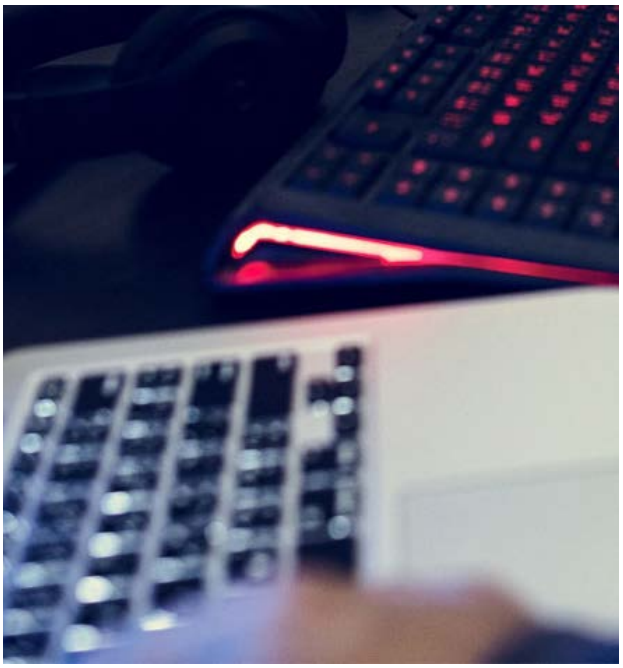
SYSTÈME D'INFORMATION

Ensemble des matériels contenant les informations nécessaires pour accomplir la mission de l'entreprise et des réseaux permettant leurs échanges.

T

TYPOSQUATTING

Action malveillante qui consiste à déposer un nom de domaine très proche d'un autre nom de domaine, dont seuls un ou deux caractères diffèrent.



Source : CLUSIF et OSSIR

U

USURPATION D'ADRESSE (ADDRESS SPOOFING)

Action malveillante qui consiste à utiliser délibérément l'adresse d'un autre système en lieu et place de la sienne.

Remarques : Il faut rapprocher cette action de l'usurpation d'identité, considérée comme un délit par le droit pénal français. L'idée est de faire passer son système d'information pour un autre. L'adresse usurpée peut être une adresse MAC (pour Medium Access Control), une adresse IP, une adresse de messagerie, etc.

UTILISATEURS PRIVILÉGIÉS

Dans un système, il existe en général des utilisateurs disposant de droits spéciaux leur permettant d'administrer le système.

V

VER (UN) (OU WORM)

Logiciel malveillant indépendant, cherchant à propager son code au plus grand nombre de cibles, puis de l'exécuter sur ces mêmes cibles. Il perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs.

Remarques : Les deux termes ver et virus sont relativement proches. Un ver est un virus qui se propage de manière quasi autonome (sans intervention humaine directe) via le réseau. Les vers sont donc une sous-catégorie de virus, dont le vecteur primaire de propagation reste le réseau.

VIRUS (UN)

Programme ou morceau de programme malveillant dont le but est de survivre sur un système informatique (ordinateur, serveur, appareil mobile, etc.) et, bien souvent, d'en atteindre ou d'en parasiter les ressources (données, mémoire, réseau). Le mode de survie peut prendre plusieurs formes : réplication, implantation au sein de programmes légitimes, persistance en mémoire, etc. Pour sa propagation, un virus utilise tous les moyens disponibles : messagerie, partage de fichiers, portes dérobées, page internet frauduleuse, clés USB.

VPN (VIRTUAL PRIVATE NETWORK)

Système permettant de créer un lien direct entre des ordinateurs distants

VULNÉRABILITÉ (VULNERABILITY)

Faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser.

Remarques : Une vulnérabilité peut être utilisée par un code d'exploitation et conduire à une intrusion dans le système.

Le talent d'aller plus loin

CONSEIL, PILOTAGE ET DÉVELOPPEMENT IT

Meritis est une société de conseil en transformation des Systèmes d'Information et Organisations.

➔ **Notre approche ?**
Accompagner nos clients sur l'ensemble de la chaîne de valeur : cadrage personnalisé, pilotage & développement applicatif pour les projets IT.

➔ **Notre mission ?**
Connecter les meilleurs talents au service de la transformation numérique pour donner un temps d'avance aux entreprises.

Nos +750 consultants vous accompagnent avec agilité dans tous vos projets de transformation digitale. Un seul objectif : vous emmener plus loin.

Meritis Cybersécurité

NOTRE EXPERTISE AU SERVICE DE VOTRE SECURITE !

Ransomware & malware (logiciels malveillants), **phishing** (hameçonnage par des fraudeurs) ou **intrusion au niveau du système d'information** (vol de données, usurpation d'identité , espionnage industriel) ; les sociétés sont toutes vulnérables face à ces menaces. Selon l'Autorité nationale de la sécurité des systèmes d'information (ANSSI), les **cyberattaques** ciblant des sociétés Françaises sont **de plus en plus nombreuses avec des pertes estimées à plusieurs millions d'euros.**

Pour répondre au plus près à vos besoins, nous avons composé une **équipe d'experts pluridisciplinaires** : RSSI, Consultant Cybersécurité, auditeur Cybersécurité, Risk Manager, Architecte Sécurité, Pentester ou encore experts DevSecOps

Quelques soient vos besoins, Meritis vous accompagne dans chaque étape de votre projet :

- ➔ **Analyse des menaces et des risques**
- ➔ **Détection des activités suspectes ou malveillantes**
- ➔ **Mise en place d'une stratégie cybersécurité**

EN SAVOIR PLUS

Nous contacter

Un projet, une question, vous souhaitez en savoir plus ?

Contactez-nous ! Nos équipes d'experts sont votre disposition pour répondre toutes vos questions.

NOUS CONTACTER **NOUS REJOINDRE**

meritis.fr