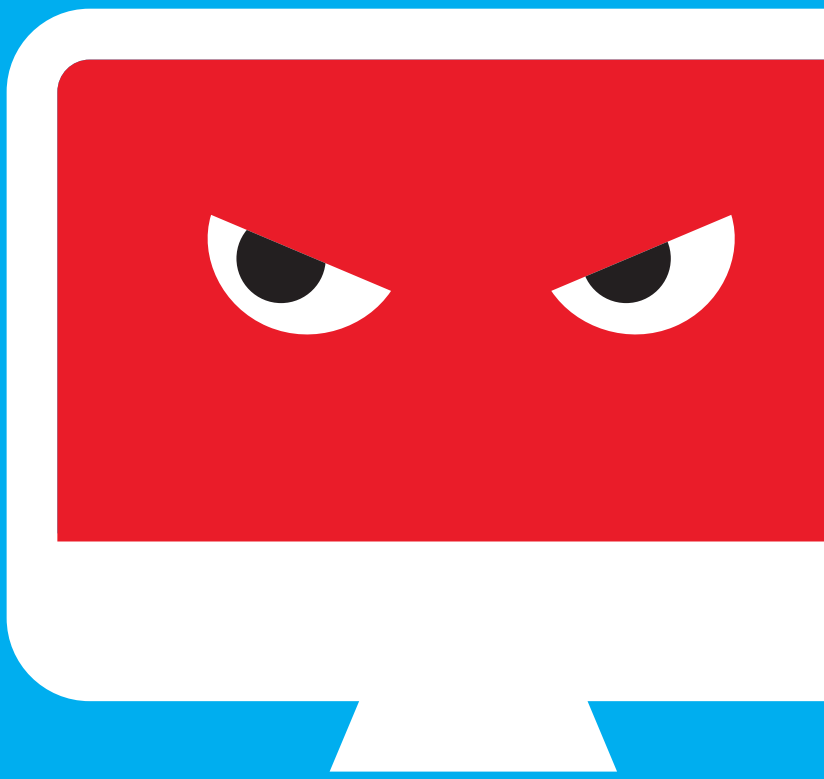
Cybersécurité, la Gironde contre attaque !

Le 29 janvier 2021
conférences, tables-rondes et hackathon



gironde.fr/cybersecurite

gironde numerique
Le numérique au service des Girondins

Gironde
LE DÉPARTEMENT

Le monde d'après se construira avec et par le numérique !

La crise sanitaire que nous traversons bouscule en profondeur nos habitudes. Elle nous impose de réinventer nos façons de vivre, d'étudier et de travailler, de nous informer et de nous divertir, mais aussi de maintenir le lien avec nos proches.

Alors que la distanciation physique devenait la règle, la place centrale qu'occupe le numérique dans nos sociétés s'est révélée comme une évidence. A défaut d'être reconnu par la loi comme un service public obligatoire, au même titre que l'eau potable ou l'électricité, le Département de la Gironde est pleinement mobilisé pour garantir l'accès au numérique pour tous et partout.

Lancé dès 2018, le plan Gironde Haut Méga doit nous permettre de relever ce défi de taille en raccordant l'ensemble du territoire girondin à la fibre optique d'ici 2024. Et au-delà de la construction des infrastructures, le Département soutient des actions de médiation numérique pour accompagner les publics les plus éloignés vers ces nouveaux usages.

Comme toute révolution de cette ampleur, le numérique induit de nouvelles menaces auxquelles nous devons nous préparer. Pour cette seconde édition de l'évènement cybersécurité, nous avons fait le choix de mettre l'accent sur le télétravail dont l'essor est devenu une réalité pour beaucoup de travailleurs comme pour leurs organisations.

Au travers de témoignages et de bonnes pratiques, nous vous proposons de bâtir des systèmes plus résilients, à même d'anticiper et de nous prémunir d'attaques de plus en plus fréquentes et sophistiquées contre nos organisations.

Ensemble, organisons la contre-attaque girondine !

Jean-Luc GLEYZE
Président du Département de la Gironde

Des clés pour décrypter et agir

La crise sanitaire a largement bouleversé nos habitudes professionnelles et mis à rude épreuve nos facultés d'adaptation.
L'usage d'internet a augmenté de près de 30 % pendant le premier confinement, 20 % lors du second. Cette augmentation des usages correspond notamment à un accroissement du télétravail et donc à l'ouverture plus grande depuis l'extérieur des systèmes d'information. Ainsi, le terrain de jeu des hackers s'est agrandi.

En 2020, notre Département de la Gironde n'a pas échappé à ce phénomène et a dû parer à de nombreuses attaques informatiques en tout genre :

- 2 141 100 984 connexions bloquées (sources de risques de piratage),
- 5 102 attaques contrées, soit 20 % d'augmentation enregistrés dès le premier confinement,
- 30 426 malwares neutralisés.

Pour cette édition 2021 de notre événement cybersécurité, nous traiterons plus particulièrement des menaces informatiques liées au télétravail et des bonnes pratiques à mettre en place.

Au cours des tables-rondes et des conférences, les intervenants vous apporteront les clés nécessaires pour aborder sereinement les évolutions qui s'imposent à nos organisations.

À l'occasion d'un hackathon, des élèves ingénieurs répondront aux défis d'un scénario d'attaque-défense et tenteront de pirater un système construit spécifiquement pour l'occasion.

Ce scénario aura vocation à mesurer leur habileté et à sensibiliser un public plus large aux risques concrets de la cybercriminalité et aux moyens de s'en prémunir.

Matthieu ROUVEYRE
Vice-Président du Conseil départemental de la Gironde,
chargé de la Citoyenneté, des Relations avec les Usagers,
de la Communication et des Accès Numériques.

Sommaire

Programme de la journée 6

Les intervenants 8

Les participants au hackathon 11

Le Glossaire 15

Les informations pratiques 19

Programme de la journée

8h45

Début du Hackathon

14 h 15

Conférence :

Cybersécurité et télétravail :
acteurs, enjeux, bilan de l'année 2020, chiffres clefs, impact COVID/télétravail

Intervenant :
Cyril BRAS

15 h 15

Zoom sur le Hackathon

15 h 25

Table ronde 1 :

Cybersécurité et télétravail :
les menaces et risques ?

Intervenants :
Winston DELBEY
Delphine RIDER
Eric FREYSSINET
Paul BOUSQUET

16 h 25

Zoom sur le Hackathon

16 h 35

Table ronde 2 :
Cybersécurité et télétravail : les bonnes pratiques ? Comment améliorer sa cybersécurité ?

Intervenants :
Pascal MOREL
Olivier GRALL
Valérie BRUNET

17 h 35

Remise des prix Hackathon

Merci aux animatrices :

Laëtitia LANGELLA et **Orianne DUPONT**

Les intervenants

Commissaire Paul BOUSQUET

Commissaire Divisionnaire, en poste à la Direction Interrégionale de Police Judiciaire de Bordeaux.
Il dirige la division des affaires économiques et financières, composée d'une trentaine d'enquêteurs spécialisés, et notamment d'un groupe de lutte contre la cybercriminalité.

La Police Judiciaire est en charge de la lutte contre la criminalité organisée et la grande délinquance financière. La lutte contre la cybercriminalité entre à ce titre dans ses domaines de compétence, et notamment les affaires de piratage, d'escroquerie ou d'extorsion commis par le moyen des nouvelles technologies.

Afin de renforcer la prévention de cette criminalité et de sensibiliser les entreprises, grandes ou petites, à la cybersécurité, la PJ de Bordeaux a également mis en place depuis 2018 un réseau de prévention des cybermenaces, composé de réservistes locaux et nationaux et de professionnels partenaires.

Cyril BRAS

Sa carrière en informatique débute en 2000. Il occupe successivement des fonctions d'administrateur système et réseaux (France Telecom), de chargé d'études NTIC (CCI de Nîmes) puis intègre la fonction publique d'état au CNRS. Il y assure pendant 12 ans, les fonctions de responsable informatique et de chargé de sécurité des systèmes d'information dans deux laboratoires de recherche à Caen (GIP Cyceron) puis à Grenoble (CERMAV).

En 2018, à la faveur d'un détachement, il rejoint la fonction publique territoriale en qualité de RSSI auprès de Grenoble Alpes Metropole. Il constitue en 2020, un réseau de RSSI de collectivités territoriales afin de partager des informations et améliorer la résilience face aux cyberattaques.

Il apprécie particulièrement de partager ses connaissances, raison pour laquelle il est enseignant vacataire en Cybersécurité auprès de l'Université Grenoble Alpes. Il intervient aussi pour le CNFPT sur la région Auvergne Rhône Alpes afin de sensibiliser aux enjeux liés à la Cybersécurité les agents de différentes collectivités.

Enfin, il est auditeur IHEDN/INHESJ de la 2ème session nationale « Cybersécurité et Souveraineté numérique » et a intégré en octobre 2020 l'INCRT (Institut National de Cybersécurité et de Résilience des Territoires) en qualité de vice-président.

Colonel Éric FREYSSINET

Chef du Pôle national de lutte contre les cybermenaces – Direction Générale de la Gendarmerie Nationale - Officier supérieur de gendarmerie, spécialiste en investigation numérique, coordinateur d'enquêtes criminelles liées aux technologies numériques, enseignant invité, chercheur associé. Spécialités : investigation numérique, investigation sur les réseaux, coopération policière internationale, formation, cybermenaces, transformation numérique.

Olivier GRALL

Délégué à la sécurité numérique de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour la région Nouvelle Aquitaine. Il a intégré en Septembre 2018 le dispositif d'action territoriale qui permet à l'Agence d'agir au plus près des acteurs économiques et des collectivités locales. Il était auparavant Ingénieur en investigation numérique au sein de la division réponse de l'ANSSI. Il est également membre du comité Directeur de l'AFSIN (Association Francophone des spécialistes de l'investigation numérique) et a dirigé pendant 7 ans la Branche Francaise de la Société MSAB qui équipe les forces de l'ordre en solutions d'analyse de téléphones mobiles.

Véronique BRUNET

Actuellement déléguée à la sécurité du numérique de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour la région Bourgogne Franche-Comté, Véronique Brunet représente l'ANSSI en région auprès des institutions et du tissu économique local.

Diplômée en linguistique, en ingénierie de la formation et en cybersécurité, elle est à l'origine du MOOC SecNumacadémie qu'elle a développé pour l'Agence de 2015 à 2018. Auparavant, elle a dirigé une PME dans le domaine des arts graphiques durant 15 ans en région Bourgogne-Franche-Comté.

Winston DELBEY

TEHTRIS CERT, consultant senior responsable de l'activité de réponse aux incidents cyber

Après un début de carrière dans l'informatique et sur de larges périmètres internationaux à fort enjeux de disponibilités et de confidentialités, Winston a concouru à la sécurisation de systèmes d'information et systèmes d'armes au profit du Ministère des Armées.

Il s'est ensuite spécialisé dans la recherche d'attaquants sophistiqués (type APT) et à la mise en œuvre de réponses permettant de reprendre le contrôle de système d'information compromis.

Pascal MOREL

Ingénieur en informatique de formation, Responsable Informatique et Télécommunications en charge de la cybersécurité dans une entreprise de production et de négoce de vins et délégué de la CdC Médullienne.

« Comme dans toute chose, pour une cyberattaque, il y a un avant, un pendant et un après. Si vous n'avez connu que la 1ère phase, cela signifie que vous avez été à la fois prudent, prévoyant et chanceux. Si vous êtes dans la 2nde ou la 3ème phase, cela signifie que, bientôt, vous allez investir dans la 1ère phase, confirmant que la vie n'est qu'un éternel recommencement »

Delphine RIDER

RSSI du Service Départemental d'Incendie et de Secours de Seine-et-Marne, membre d'un réseau de RSSI des collectivités territoriales (communes, départements, sdis, régions, métropoles, etc.).

Les participants au hackathon

L'ENSEIRB-MATMECA

L'ENSEIRB-MATMECA propose six formations d'ingénieurs spécialistes de haut niveau reconnues par le monde industriel et couvrant le domaine du numérique au sens large : l'électronique, l'informatique, le calcul haute performance et la modélisation mathématique et mécanique, les télécommunications et les réseaux.

Ces thématiques sont au cœur des enjeux sociétaux et répondent à de fortes demandes des entreprises : transport intelligent, intelligence artificielle, technologiques numériques au service de la santé et du bien-être, objets connectés, cyber sécurité, etc.

Pour ce dernier domaine, une option de l'école est labélisée « SecNumEdu » par l'Agence Nationale de la Sécurité des Systèmes d'Information. Afin de mieux préparer nos élèves-ingénieurs à cette problématique, l'école dispose d'une plate-forme d'entraînement à la cyber sécurité. Par ailleurs, l'école a mis en place un parcours « ingénieur-docteur » destiné aux élèves-ingénieurs intéressés par la recherche scientifique et ses applications.

Le Master Cryptologie et Sécurité Informatique (CSI) de l'Université de Bordeaux

Le Master Cryptologie et Sécurité Informatique (CSI) de l'Université de Bordeaux forme des experts (BAC+5) en cryptologie et en sécurité informatique pour des problématiques privées ou gouvernementales. À l'interface entre les mathématiques et l'informatique, nous faisons en sorte que tous nos étudiants aient des bases communes dans les deux domaines afin d'affronter la sécurité sous les aspects les plus pratiques ainsi que les plus théoriques.

École d'ingénierie informatique (EPSI) et Web Internationale School

L'EPSI est la première école d'informatique en France à avoir été créée par des professionnels, et première à avoir obtenu le titre niveau I RNCP (Bac +5 certifié par l'État).
Résolument engagée auprès des entreprises, l'EPSI accompagne le développement des compétences informatiques depuis plus de 55 ans et forment des experts en informatique et en système d'information.
Face à l'évidence de la transformation digitale des entreprises et du contrôle du numérique sur tous les secteurs d'innovation des industries et des services, l'EPSI est à l'initiative de la création de l'école WIS.
WIS se donne pour mission de former des professionnels du web et du digital business, capables d'accompagner le développement des compétences des entreprises, de mener à bien la digitalisation des processus-métiers et d'assurer la transformation digitale des organisations, en France et à l'International.

CESI – École d'ingénieur

CESI École d'Ingénieurs Campus Bordeaux permet à chaque élève ingénieur·e de construire un parcours personnalisé dont il est acteur, grâce à une école en cinq ans, sous statut étudiant.
Il s'agit d'une formation d'ingénieur·e en cinq ans, accessible après un bac S, STI2D ou STL.
Cette offre de formation comprend :

- Un cycle préparatoire intégré
- Un choix d'orientation parmi deux spécialités : Généraliste ou Informatique
- Des parcours étudiants
- Des formations d'ingénieur·e·s en formation continue pour adultes
- Des spécialisations post bac +5 avec 12 Mastères spécialisés®

EPITECH

L'école référence de l'expertise informatique forme depuis 20 ans les experts qui dessinent le monde de demain. Epitech est une école en 5 ans spécialisée dès la première année sur la programmation et les nouvelles technologies.

▶ Une école accessible à toutes et à tous dès 18 ans
▶ Avec une pédagogie active unique qui forge les personnalités
▶ À travers un écosystème international
▶ Epitech : un passeport pour des carrières à fort impact

100 % d'employabilité à la fin du cursus dans tous secteurs : jeux vidéos, sécurité, logiciels, mobiles…
Transformez votre passion en métier.

YNOV Campus

Le numérique, en se déployant sur l'ensemble des secteurs et des fonctions, entraîne de profondes mutations des métiers, des savoir-faire et des compétences. Conscient de cet enjeu, Bordeaux Ynov Campus, pôle d'enseignement supérieur à l'ADN digital, forme près de 1 200 étudiants chaque année.

Bordeaux Ynov Campus dispense 6 Bachelors et 18 Mastères en phase avec le marché en constante évolution dans les 6 différents grands pôles disciplinaires que sont l'informatique, l'animation 3D et jeux vidéo, la création et le design, le marketing et la communication, la robotique et l'ingénierie systèmes ainsi que l'audiovisuel. Cette multitude de parcours de formation, des plus créatifs aux plus techniques, ont tous en commun le digital, les nouvelles technologies et sont axés sur la professionnalisation.

Ils ont participé à la réalisation du hackathon

Beware Cyberlabs

Beware Cyberlabs est une société spécialisée dans les solutions de cybersécurité. Elle a en particulier développé une plateforme de formation et d'entraînement permettant de mettre ses utilisateurs en situation réelle avec une configuration représentative de celle qu'ils connaissent. Ils peuvent ainsi améliorer leurs compétences et leur maîtrise de différentes technologies par la pratique, en jouant de multiples scénarios pouvant comprendre des situations d'attaque et des situations de défense.
La société possède un centre de formation dans ses locaux bordelais et propose environ une trentaine de modules de sensibilisation, formation et entraînement.

Elle a aussi développé une solution de cyberdéception pour leurrer les hackers.

www.beware-cyberlabs.eu

Cabinet Thierry Meyer Consultants

Créé en nom propre en 2005 et basé à Bordeaux, Thierry Meyer Consultants est un cabinet de conseil, d'audit et d'expertise technique spécialisé en sécurité des Systèmes d'Information.

Les prestations menées par le cabinet ont pour objectif d'évaluer et d'adapter le niveau de sécurité du système d'informations de ses clients. Le cabinet fournit également un accompagnement d'urgence en cas d'incident.

Toutes les missions réalisées sont personnalisées, couvertes par un accord de confidentialité, et conduites dans le respect de l'état de l'art, et en accord avec les bonnes pratiques, normes et méthodes françaises et internationales.

Les interventions des consultants du cabinet sont destinées à des clients professionnels, de tailles (TPE, PME, Grands comptes…) et secteurs d'activité (Services, Aéronautique, Industrie, Médical…) très variés.

Le Glossaire

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. 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 (Trojan Horse) : Programme donnant l'impression d'avoir une fonction utile, mais qui possède par ailleurs une fonction cachée et potentiellement malveillante. La fonction cachée exploite parfois les autorisations légitimes d'une entité du système qui invoque ce programme. Elle peut par exemple permettre la collecte frauduleuse, la falsification ou la destruction de données.

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

Compte privilégié : 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.

Confidentialité : Propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.

Contournement de la politique de sécurité : Toute action ayant pour conséquence la mise en échec des règles ou des mécanismes de sécurité mis en place.

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.

Cybersécurité : État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptible 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.

Défiguration, barbouillage (defacement) : Résultat d'une activité malveillante qui a modifié l'apparence ou le contenu d'un serveur internet, et a donc violé l'intégrité des pages en les altérant. Cette action malveillante est souvent accompagnée de revendications.

Déni de service (Denial of Service, DoS) : Action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu. Cette action n'est pas nécessairement malveillante. Elle peut aussi traduire un mauvais dimensionnement du service, incapable de fournir la réponse à une forte demande. Si l'action est lancée depuis plusieurs sources, il est fréquent de parler de Déni de Service Distribué (DDoS).

Élévation de privilège (privilege escalation) : Obtention de privilège supérieur par exploitation d'une vulnérabilité. Par exemple, si un utilisateur local accède à des droits normalement réservés à l'administrateur, il y a élévation de privilège. Une élévation de privilège est souvent recherchée par une personne malveillante lorsqu'elle a réussi à s'introduire sur un système d'information en usurpant l'identité d'un utilisateur légitime.

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.

Exécution de code arbitraire à distance : Mise en œuvre de commandes à distance sur un ordinateur, à l'insu de son utilisateur légitime.

Faille : Vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.

Hameçonnage ciblé (spearphishing) : Cette attaque repose généralement sur une usurpation de l'identité de l'expéditeur, et procède par ingénierie sociale forte afin de lier l'objet du courriel et le corps du message à l'activité de la personne ou de l'organisation ciblée. Généralement, le courriel usurpe l'identité d'une personne morale (établissement financier, service public, concurrent…) ou d'une personne physique (collègue de travail, famille, ami…) dans le but de duper le destinataire qu'il invite à ouvrir une pièce jointe malveillante ou à suivre un lien vers un site Web malveillant. Une fois cette première machine contaminée, l'attaquant en prend le contrôle pour manœuvrer au sein du système d'information de l'organisation constituant la véritable cible (on parle ici « d'infiltration »). Une fois ses cibles atteintes, il recherchera les informations qu'il s'efforcera de capter le plus discrètement possible (on parle alors ici « d'exfiltration ») soit en une seule fois, en profitant d'une période de moindre surveillance du système (la nuit, durant les vacances scolaires, lors d'un pont…).

Hameçonnage, filoutage (Phishing) : Vol d'identités ou d'informations

confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime. Les sites sont reproduits, après avoir été aspirés. L'utilisateur est souvent invité à visiter le site frauduleux par un courrier électronique.

Ingénierie sociale (Social Engineering) : Manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes.
Il s'agit, pour les personnes malveillantes usant de ces méthodes, d'exploiter le facteur humain, qui peut être considéré dans certains cas comme un maillon faible de la sécurité du système d'information.

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.

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. 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.
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.

Pare-feu (Firewall) : Un pare-feu (ou garde-barrière), est un outil permettant de protéger un ordinateur connecté à un réseau ou à l'internet. Il protège d'attaques externes (filtrage entrant) et souvent de connexions illégitimes à destination de l'extérieur (filtrage sortant) initialisées par des programmes ou des personnes.

Porte dérobée (Backdoor) : Accès dissimulé, soit logiciel soit matériel, qui permet à un utilisateur malveillant de se connecter à une machine de manière furtive. Une porte dérobée peut également être la cause d'une mise en œuvre incorrecte d'un protocole.

Pourriel, polluriel (spam) : Tout courrier électronique non sollicité par le destinataire. Le courrier est souvent envoyé simultanément à un très grand nombre d'adresses électroniques. Les produits les plus vantés sont les services pornographiques, la spéculation boursière, des médicaments, le crédit financier, etc.
Rançongiciel (Ransomware) : 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. Pour y parvenir, le rançongiciel va empêcher l'utilisateur d'accéder à ses données (fichiers clients, comptabilité, factures, devis, plans, photographies, messages, etc.), par exemple en les chiffrant, puis lui indiquer les instructions utiles au paiement de la rançon.

Réseaux de machines zombies (Botnet) : 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.

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. 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.

Ver (Worm) : Un ver (ou worm) est un 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.

Virus : Un virus est 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…

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.

Les informations pratiques

Réagissez !

#LaGirondeContreAttaque #Cybersecurite
sur Twitter @gironde

L'évènement se tiendra en 100% distanciel
et sera retransmis sur Gironde.fr/cybersecurité
Un replay sera disponible à l'issue
de l'événement

Pour participer aux activités Beekast :

1. Connectez-vous à internet (Wi-Fi, 4G)

2. Ouvrez votre navigateur favori (Chrome, Safari...)

3. Dans votre barre URL, tapez: www.beekast.live

4. Saisissez le code session : cyber33 et cliquez sur « Participez »

5. Une fois connecté une notification, en haut de votre écran, vous indiquera qu'une ou plusieurs activités sont désormais accessibles. Puis il vous suffit donc de cliquer sur «répondre» pour y participer. Si toutefois vous ne l'apercevez pas, pas de panique. Il vous suffit de cliquer sur l'onglet «activité». Ainsi vous verrez l'ensemble des activités qui sont à votre disposition et il suffira de cliquer dessus pour y participer.

gironde.fr/cybersecurite

gironde numerique
Le numérique au service des Girondins

Gironde
LE DÉPARTEMENT