REVUE DE PRESSE

➢ voir à la fin de cette revue de presse le Dossier de presse du Forum Cybersécurité et Numérique

le Journal du Palais
Réseau Légalnet

La cybersécurité a son forum en BFC

Région BFC. Le premier Forum cybersécurité et numérique à portée régionale aura lieu à l'IUT de Dijon, le 24 janvier de 8 h 30 à 17 h avec 19 intervenants et plusieurs thématiques, dont l'IA.

Lecture **3 min**

Partager :

Publié le **14 janvier 2025** • **Frédéric Chevalier**

Quelque 300 visiteurs sont attendus au Forum cybersécurité et numérique à Dijon. Un rendez-vous qui s'adresse à l'ensemble des professionnels de la cybersécurité et du numérique, qu'ils soient experts, utilisateurs, ou décideurs, issus du secteur privé comme du secteur public. Cet évènement qui réunira les acteurs clés de la filière en Bourgogne Franche-Comté, est coorganisé par La French Tech Bourgogne Franche-Comté, le Centre régional de la cybersécurité (CSIRT) BFC, créé le 24 février 2022 et l'Agence nationale de la sécurité des systèmes d'information (Anssi).

Il est soutenu par la Région BFC, la préfecture de BFC, Dijon Métropole et l'Agence régionale du numérique et de l'intelligence artificielle (ARNia), ainsi que par le Medef, l'IUT Dijon Auxerre Nevers et la CCI BFC. Cette rencontre sera ouverte par Marie-Hélène Juillard-Randrian, conseillère municipale à la ville de Dijon et vice-présidente de Dijon métropole et Philippe Rouiller, délégué à la transformation numérique Région Bourgogne Franche-Comté. Elle verra intervenir Sébastien Morey, directeur du CSIRT BFC, Silvère Denis, directeur délégué de la French Tech BFC et Serge Durand ex vice-président d'Airbus qui évoquera les enjeux économique, étatique et individuel de la cybersécurité. Pour le reste du programme ; des tables rondes sur différentes thématiques : le numérique dans la santé, l'IA dans les entreprises, les directions informatiques face aux cybermenaces et les moyens d'action des RSSI au sein de leurs organisations ; des ateliers ; des conférences et des rendez-vous BtoB devraient permettre aux visiteurs d'échanger avec des professionnels, d'assister à des démonstrations, se renseigner sur les dernières innovations et ainsi de

renforcer leur résilience face aux cyberattaques. *« Le Forum régional de la cybersécurité s'adresse à tous les décideurs en entreprises, en collectivités ou associations. Il a pour objectif de créer un espace d'échanges et de solutions autour d'une thématique cruciale. La sécurité des données, des infrastructures, des usages est aujourd'hui plus que jamais incontournable pour assurer la continuité des activités et des services publics au bénéfice de tous »*, conclut Patrick Molinoz, président ARNia.

Auteur : Frédéric Chevallier

Lien : https://journal-du-palais.fr/au-sommaire/entreprises/la-cybersecurite-a-son-forum-en-bfc

Du 20 au 26 janvier 2025 - N° 4951

2€

le Journal du Palais

L'HEBDOMADAIRE RÉGIONAL D'INFORMATION ÉCONOMIQUE ET JURIDIQUE – (96e année)

RÉSEAU LÉGALNET BOURGOGNE FRANCHE-COMTÉ

JDP

Le portrait du Journal du Palais

Côté cordes

Gaël Chevalier est propriétaire d'un magasin de sport et fait partie des meilleurs cordeurs professionnels au monde. Il est aussi le seul Français présent aux tournois du Grand Chelem de Roland-Garros et de l'US Open. *Page 24*

Université régionale : la fin d'un rêve

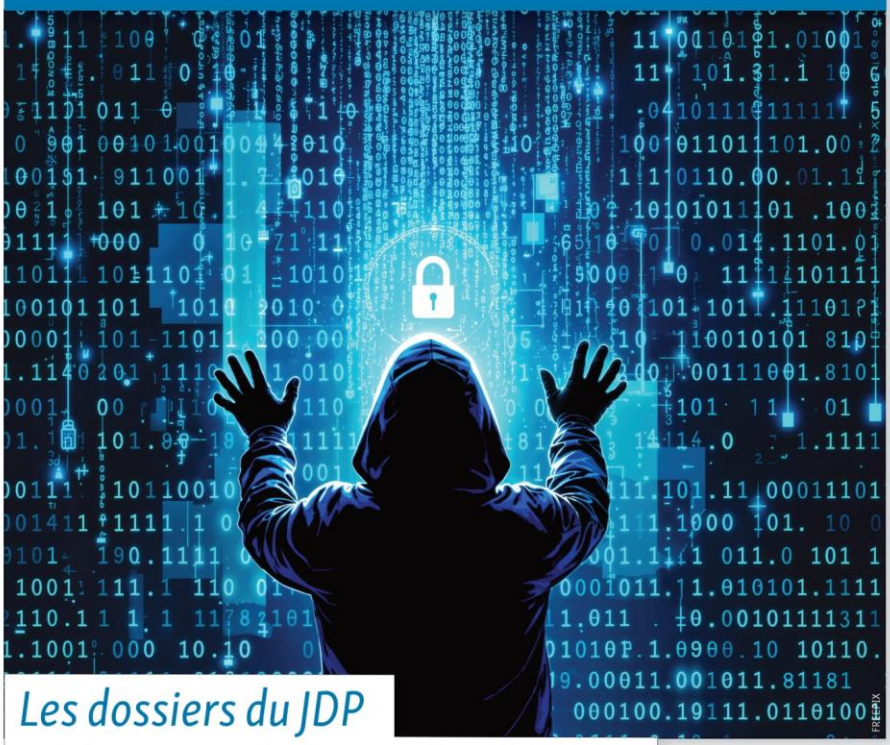
Avec la création, au 1er janvier, des deux EPE, (Université Bourgogne Europe en Côte-d'Or et Université Marie et Louis Pasteur en Franche-Comté), le rêve d'une grande université régionale, né il y a plus de 20 ans, s'éloigne définitivement. *Page 3*

« Dijon Bourgogne » : une marque est née

Cette plateforme de marques a vocation à mobiliser les agences (DBE, DBI, DBT&C) et, grâce à un réseau d'ambassadeurs, faire rayonner la métropole dijonnaise en France, en Europe et à l'international. *Page 6*

7 pages d'annonces légales
Lire les pages 17 à 23

CYBERSÉCURITÉ



Les dossiers du JDP

Vendredi 24 janvier aura lieu à l'IUT de Dijon le premier Forum cybersécurité et numérique à portée régionale co-organisé par l'Agence nationale de la sécurité des systèmes d'information (Anssi), le Centre régional de cybersécurité BFC (CSIRT-BFC) et la French Tech BFC, l'écosystème des acteurs qui œuvrent collectivement pour l'innovation et le développement économique des startups et entreprises de la Tech de Bourgogne-Franche-Comté. « *La sécurité des données, des infrastructures, des usages est aujourd'hui plus que jamais incontournable pour assurer la continuité des activités et des services publics au bénéfice de tous* », détaille Patrick Molinoz, président de l'ARNia (Agence régionale du numérique et de l'intelligence artificielle).

À cette occasion, ce dossier spécial fait le point sur la nécessité d'organiser sa cybersécurité avec les acteurs du secteur en BFC, que l'on soit une TPE, une collectivité locale, en milieu rural ou en ville. Comment détecter une cyberattaque ? Comment s'en prémunir ? Quels sont les bons interlocuteurs à contacter ? Bonne nouvelle : les ressources locales sont là !

Pages 7 à 15

Le ministre Marc Ferracci à Montbard. Page 5

R 28302 - 4951 - 2€

WWW.JOURNAL-DU-PALAIS.FR EST HABILITÉ PAR ARRÊTÉ PRÉFECTORAL À PUBLIER LES ANNONCES JUDICIAIRES ET LÉGALES POUR LES DÉPARTEMENTS DE LA CÔTE-D'OR ET DE L'YONNE

Vendredi 24 janvier aura lieu à l'IUT de Dijon le premier Forum cybersécurité et numérique à portée régionale co-organisé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le Centre régional de cybersécurité BFC (CSIRT-BFC) et la French Tech BFC, l'écosystème des acteurs qui œuvrent collectivement pour l'innovation et le développement économique des startups et entreprises de la Tech de Bourgogne-Franche-Comté. À cette occasion, ce dossier spécial fait le point sur la nécessité d'organiser sa cybersécurité avec les acteurs du secteur en BFC, que l'on soit une TPE, une collectivité locale, en milieu rural ou en ville. Bonne nouvelle : les ressources locales sont là !

SOMMAIRE

CYBERATTAQUES : PERSONNE N'EST À L'ABRI

En juillet 2024 était publié le premier rapport annuel sur la cybercriminalité commandé par le ministre de l'Intérieur d'alors, Gérald Darmanin, avec des chiffres éloquents : 278.703 infractions liées au numérique avaient été enregistrées par les forces de sécurité intérieures en 2023 (en augmentation de 9 % par rapport à 2022 selon le Service statistique ministériel de la sécurité intérieure, SSMSI), dont 59 % constituées par des atteintes « numériques » aux biens (escroqueries, arnaques en ligne), 34 % par des atteintes « numériques » à la personne, 5 % par des atteintes aux institutions. En 2023, le CSIRT-BFC (Centre régional de cybersécurité BFC, opéré par l'ARNia, l'Agence régionale du numérique et de l'intelligence artificielle) dévoilait une typologie des cyberattaques recensées par ses services : 40 % concernait des TPE/PME/ETI ; 23 % des collectivités locales et 10% des établissements de santé. Avec une nouveauté par rapport à l'origine des cyberattaques : personne n'est plus à l'abri, de la plus petite collectivité locale à la moindre TPE. « *Historiquement les cyberattaques étaient plutôt de type étatique*, retrace Jean-Félix Chevassu, directeur d'offre cybersécurité chez Adista (télécoms, cloud et cybersécurité). *Pour faire des cyberattaques, il fallait un certain niveau technique. N'importe qui ne pouvait pas être un hacker malveillant. Il y a une quinzaine d'années, c'était surtout les services d'espionnage qui s'attaquaient à d'autres États pour déstabiliser une organisation étatique ou s'attaquer à l'image d'un pays. Maintenant, les cyberattaques se sont démocratisées avec des outils disponibles sur le web qui permettent très facilement, sans niveau technique important, de déstabiliser une entreprise avec une attaque automatisée pour quelques euros* ». La conclusion s'impose d'elle-même : toute entité est potentiellement une victime, comme le confirme Serge Durand, ex-vice-président du groupe Airbus et « *observateur attentif* » de la cybersécurité dont il a pu vivre les prémices dès le début des années 2000 avec l'apparition des BlackBerry permettant la communication en mode push. « *Les connexions sont alors devenues beaucoup plus ouvertes donc forcément plus dangereuses. J'ai eu des exemples dans les forums cybersécurité auxquels je participe régulièrement. Les témoignages de victimes de cyberattaques émanent souvent des PME où le patron est sursollicité et où il n'a pas le temps ou les compétences pour prendre en compte le problème. Il faut que chaque chef d'entreprise y compris des petites comprenne pourtant que l'enjeu cyber est extrêmement important. Nous sommes dans un monde hyper relié, n'importe qui peut attaquer n'importe quelle entreprise. Chaque individu est une cible potentielle. Regardez le nombre de mails de phishing que l'on reçoit même si on a des actions préventives !* »

LES OIV PROTÉGÉS

En France, la réglementation a imposé, il y a presque 20 ans, une protection des opérateurs jugés stratégiques par l'État, comme l'écrit l'ANSSI (Agence nationale de la sécurité des systèmes d'information) sur son site internet : « *En 2006, le dispositif Secteur d'activité d'importance vitale (SAIV) est mis en place afin de protéger les opérateurs jugés indispensables à la survie de la nation contre les actes malveillants (terrorisme, sabotage, cyberattaque) et les risques naturels, technologiques, sanitaires… Ces opérateurs identifiés par les différents ministères*

> **« HISTORIQUEMENT LES CYBERATTAQUES ÉTAIENT PLUTÔT DE TYPE ÉTATIQUE. AUJOURD'HUI, CES DERNIÈRES SE SONT DÉMOCRATISÉES AVEC DES OUTILS DISPONIBLES SUR LE WEB NE NÉCESSITANT PAS DE NIVEAU TECHNIQUE IMPORTANT »**
>
> *JEAN-FÉLIX CHEVASSU, DIRECTEUR D'OFFRE CYBERSÉCURITÉ CHEZ ADISTA.*

278.703

atteintes numériques enregistrées en 2023 (+40 % en 5 ans).

59 %

d'atteintes aux biens.

34,5 %

d'atteintes aux personnes.

6 %

d'atteintes aux institutions et à l'ordre public.

Les chiffres clés 2023 de la la cybersécurité

Sources : Service statistique ministériel de la sécurité intérieure, Office Anti-Cybercriminalité de la police nationale, Unité Nationale Cyber de la gendarmerie nationale, section J3 du parquet.

FREEPIK

de tutelle seront désignés par arrêté "Opérateurs d'importance vitale" (OIV). Fin 2013, pour faire face à l'augmentation en quantité et en sophistication des attaques informatiques, l'article 22 de la loi de programmation militaire vient compléter ce dispositif en ajoutant une nouvelle pierre à l'édifice, imposant aux OIV le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent : les systèmes d'information d'importance vitale (SIIV). » Deux dispositifs viennent compléter l'arsenal de défense contre les hackers : les directives Sécurité des réseaux et de l'information, dites « directives Nis » (Network and Information System Security) 1 et 2 dont l'objectif est d'assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne. Nis 1 a été adoptée le 6 juillet 2016 et transposée en France le 26 février 2018 ; son périmètre d'application est étendu par Nis 2 (publiée le 27 décembre 2022 au Journal Officiel de l'Union européenne) qui amènera aussi les États membres à renforcer leur coopération en matière de gestion de crise cyber. « *À l'échelle nationale, Nis 2 s'appliquera à des milliers d'entités appartenant à plus de dix-huit secteurs qui seront désormais régulés,* détaille Yves Verhoeven, sous-directeur stratégie de l'ANSSI sur le site de l'organisme. *Environ 600 types d'entités différentes seront concernés, parmi eux des administrations de toutes tailles et des entreprises allant des PME aux groupes du CAC 40.* » Mais qu'en est-il des plus petits opérateurs dont on a vu qu'ils constituent le gros des victimes de cyberattaques ?

TOUT LE MONDE EST VISÉ

Si l'ANSSI note globalement une meilleure connaissance par l'écosystème économique et par les collectivités locales de l'existence de la menace cyber, les plus modestes (TPE notamment), ne pensent pas être des proies suffisamment intéressantes pour les cyberattaques dont l'immense majorité relève du rançongiciel. Et c'est une erreur, s'alarme Jean-Félix Chevassu : « *Curieusement beaucoup de chefs d'entreprise aujourd'hui n'ont pas encore pris conscience qu'ils sont potentiellement une cible. Parce qu'ils se disent : "pourquoi je serai attaqué moi ? Je n'intéresse personne, je n'ai pas de données qui valent beaucoup d'argent." Ils n'ont pas compris que les attaquants maintenant réclament comme rançons de tous petits montants. L'attaque est menée par des robots (botnets), qui scannent en permanence toutes les failles possibles exposées sur internet. Or une entreprise est forcément exposée sur internet, parce qu'elle a un accès au web, un site web, un serveur de messagerie, un serveur de fichiers… toutes ces connexions vers l'extérieur présentent autant de moyens nouveaux pour que des petites et des moyennes entreprises soient attaquées.* »

Le problème est celui de la détection de la cyberattaque car on s'en aperçoit lorsqu'il est déjà trop tard : « *Bien souvent, le cybercriminel amène des éléments de preuve, de fuite de données sensibles,* poursuit Jean-Félix Chevassu. *Ça peut être des secrets de fabrication, des données personnelles des collaborateurs de l'entreprise ou des clients, des données contractuelles, des bases clients, des bases de produits, des bases de prix, ce genre de choses. La détection intervient un peu tard, puisque on est là devant le fait accompli alors que le cybercriminel réclame une rançon pour restituer les données et ne pas les mettre en vente sur le darkweb. Bien souvent, mais ce n'est pas systématique, le système d'information du client a été aussi chiffré. C'est ce qu'on appelle le cryptolockage : les serveurs ne démarrent plus, le parc informatique du client n'est plus opératif* ». Avec des conséquences parfois dramatiques dont un forum comme celui du 24 janvier permet à l'auditoire de mesurer l'ampleur.

JUSQU'À LA FAILLITE

« *C'est l'intérêt de tels rendez-vous,* soutient Serge Durand : *souvent le chef d'entreprise qui y assiste tombe de l'armoire et se dit : "ce n'est pas possible, j'ai autant de risques, c'est aussi intrusif la cyberattaque ?" Oui, c'est aussi intrusif. Ce qui les choque aussi, ce sont les témoignages de ceux qui ont été cyberattaqués : je peux vous dire que la leçon est largement apprise à leurs dépens si ce n'est qu'ils ont quelquefois fait faillite.* » « *Il faut prendre aujourd'hui en compte qu'une attaque, c'est presque aussi dramatique qu'un incendie,* reprend Sébastien Morey, directeur du Centre régional de cybersécurité de Bourgogne-Franche-Comté (CSIRT-BFC). *Revenir à la normale peut prendre des semaines ou des mois. Ça veut dire que pendant ce temps-là, il n'y a plus de chiffre d'affaires, il n'y a plus de ventes parce qu'on ne fabrique plus. Si une entreprise a de la trésorerie elle pourra sûrement s'en sortir. Si c'est un peu plus compliqué, elle va être malmenée. Il y aura sûrement des impacts sur les salariés, des primes prévues seront annulées…* ». « *C'est très perturbant,* soutient encore Jean-Félix Chevassu. *C'est un peu comme un cambriolage chez soi, on a l'impression d'avoir été violé dans son quotidien. C'est très difficile. Ce qui est anxiogène, c'est aussi toute la période de réponse à incident, de reconstruction : là, il y a un investissement énorme en temps pour retrouver les informations, recréer les systèmes, refaire toutes les configurations pour que ça refonctionne. Ce qui entraîne forcément une perte d'exploitation, une perte de chiffre d'affaires… et explique que de petits acteurs ne peuvent plus exercer leur activité parce que forcément leurs charges sont toujours là, ils doivent toujours payer leurs loyers, leurs employés mais ils n'ont plus de revenu parce qu'ils sont incapables de reprendre leur production sauf à faire des choses à la main comme on a vu dans les hôpitaux, mais ce n'est pas tenable dans le temps pour une activité industrielle. Il y a une pression énorme puisque pendant tout ce temps les collaborateurs ne peuvent plus travailler. Donc une grosse angoisse de perdre leur travail, de perdre leurs clients, de perdre leurs partenaires, tout leur écosystème…* ».

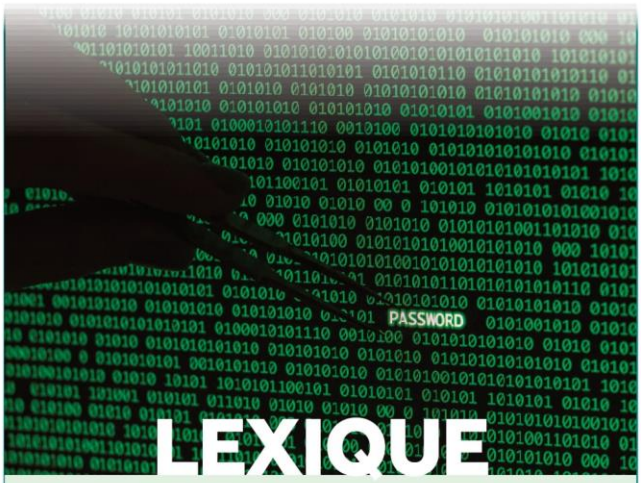
STRATÉGIE D'ENTREPRISE

On aura compris la nécessité d'une véritable politique de cybersécurité au sein des entreprises de toutes dimensions, comme dans les collectivités locales. « *Aujourd'hui, on ne peut pas ne pas prendre en compte cette problématique alors que l'on en parle partout, que les entreprises sont aussi au courant à travers leurs organisations patronales, le Medef, la CPME, les chambres de commerce… font beaucoup d'informations là-dessus. On sait que ça coûte de l'argent. Mais ne plus prendre en compte ce sujet, ce n'est pas trop normal en 2025* », soutient Sébastien Morey. Serge Durand va plus loin en évoquant une obligation de chaque chef d'entreprise à cet égard : « *Le dirigeant doit avoir la conscience des risques qu'il fait prendre à son entreprise en n'ayant pas une politique extrêmement sévère en termes de cybersécurité. La première des choses, est de mettre en place la politique cyber, choisir son responsable des systèmes d'information et ensuite mettre en place cette politique. Et moi je suis pour la sévérité, c'est-à-dire qu'il faut des règles ! Car sinon on est trop dépendant de négligences internes.* » Jean-Félix Chevassu évoque lui la nécessité d'envisager la cybersécurité comme partie pernante de la stratégie des entreprises : « *C'est un projet qui doit être mené par le dirigeant au même titre que son plan de financement, son plan de développement et tous les projets stratégiques d'entreprise parce qu'il en va de la survie des sociétés et des collaborateurs dans leur métier. Et ce projet entreprise n'est pas que technique, il est aussi sur les processus. Exemple : un collaborateur s'en va. Je dois suivre un processus tel que : détruire son mot de passe, récupérer son matériel, vérifier qu'il ne parte pas avec des données de l'entreprise.* » Pour être efficace, il importe aussi que l'ensemble des personnels soit impliqué, au travers de plans de formation qui prennent parfois des visages très simples, comme l'explique Jean-Félix Chevassu : « *90% des cyberattaques proviennent de phishing. Savoir déceler que la connexion qu'on me demande n'est pas une vraie connexion et que notre mot de passe est en train d'être volé, ça empêche déjà 90 % des attaques. Si dans un deuxième temps, on met également un système de double authentification, on réduit encore plus le nombre de cyberattaques.* »

L'IA, POISON ET ANTIDOTE

L'irruption de l'intelligence artificielle vient encore complexifier l'écosystème de la cybersécurité : l'IA permet en effet, en un temps record, de créer de nouveaux logiciels malveillants. Mais, et c'est la bonne nouvelle, sa capacité à traiter de manière extrêmement rapide un nombre incommensurable de données lui permet de scanner très vite des comportements anormaux et opérer de la détection comportementale. Une IA entraînée à connaître le mode de fonctionnement des collaborateurs (horaires habituels de connexion, systèmes utilisés, sites visités…) détectera en effet en temps réel toute déviance des schémas habituels des fonctionnements. Si l'entreprise ou la collectivité locale a prévu, grâce à son responsable sécurité (interne ou non) un système de déconnexion immédiat, une attaque en cours est ainsi rapidement circonscrite. Une cyberattaque laissant des traces, une IA qui en a connaissance sera aussi plus à même d'en reconnaître les prémices, et d'anticiper des cyberattaques menées en parallèle. Bref, une alliée à se faire d'urgence pour sécuriser les systèmes d'informations : « *Cette technologie,* conclut Jean-Félix Chevassu, *est comme la pharmacopée : elle peut être à la fois le poison et l'antidote* ».

Emmanuelle de Jesus



LEXIQUE

Cyberattaque

Ensemble coordonné d'actions qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité. L'ANSSI identifie quatre grandes familles de cybermenaces : la cybercriminalité à visée lucrative, l'espionnage, la déstabilisation et le sabotage. Selon la motivation de l'attaquant et le mode opératoire adopté, chaque cyberattaque pourra être associée à l'une de ces menaces.

OIV

Personne morale publique ou privée qui gère ou utilise des établissements ou des ouvrages dont la destruction ou même l'indisponibilité obéreraient gravement le potentiel militaire, la force économique, la sécurité, voire la capacité de survie d'un État, ou mettraient en danger sa population.

Rançongiciel

Les rançongiciels ou ransomwares sont des logiciels malveillants qui bloquent l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclament à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.

ANSSI

L'Agence nationale de la sécurité des systèmes d'information est l'héritière d'une longue série d'organismes chargés d'assurer la sécurité des informations sensibles notamment de l'État : la Direction technique des chiffres créée en 1943 à Alger ; le Service central technique des chiffres, qui lui a succédé à Paris en 1951 ; le Service central du chiffre et de la sécurité des télécommunications, créé en 1977 ; le Service central de la sécurité des systèmes d'information en 1986 ; la Direction centrale de la sécurité des systèmes d'information créée par le décret n° 2001-693 du 31 juillet 2001 au sein du Secrétariat général de la défense nationale. Le décret n° 2009-834 du 7 juillet 2009 créant l'Agence nationale de la sécurité des systèmes d'information donne à cette agence, en plus de la sécurité des systèmes d'informations de l'État, une mission de conseil et de soutien aux administrations et aux opérateurs d'importance vitale, ainsi que celle de contribuer à la sécurité de la société de l'information, notamment en participant à la recherche et au développement des technologies de sécurité et à leur promotion. L'ANSSI bénéficie de l'expertise d'un comité stratégique constitué de responsables de haut niveau de l'administration. La mission de ce comité est de proposer la stratégie de l'État en la matière. Son directeur général, Vincent Strubel, a été nommé par décret en date du 4 janvier 2023.

« LA SOUVERAINETÉ EST CRUCIALE »

Entretien avec Patrick Molinoz, président de l'ARNia.
Crédit photo : Édouard Barra.

***Le Journal du Palais*. Pouvez-vous nous rappeler l'enjeu de la cybersécurité, pour les entreprises et les collectivités locales, ainsi que les structures type CHU par exemple ?**

Patrick Molinoz. Tout d'abord il faut rappeler que la cybersécurité est un des principaux défis de la numérisation de la société. J'aime rappeler que l'univers numérique devrait être pensé comme le monde « physique » : il n'y a ni liberté, ni démocratie, ni croissance pour les citoyens dans le monde « physique » sans sécurité. C'est la même chose avec le numérique.

Il est donc nécessaire de protéger les données collectées et les systèmes qui les traitent pour permettre le fonctionnement normal, et sain, de leur activité.

La question n'est pas de savoir « si » une cyberattaque aura lieu, puisqu'il est certain qu'elle aura lieu, mais « comment » s'en protéger... une des spécificités de la cybercriminalité est que les attaques sont de plus en plus « tous azimuts ». En Bourgogne Franche-Comté comme ailleurs de nombreuses entités, de toutes tailles, publiques et privées, sont victimes d'attaques informatiques chaque année.

Les collectivités, les entreprises les citoyens eux-mêmes produisent et/ou collectent des données qui intéressent une multitude de tiers malveillants. Les cybercriminels peuvent chercher à exploiter des données volées pour leur intérêt propre (espionnage économique ou technologique...), à s'en servir comme « monnaie d'échange » (extorsion, chantage) ou même dans le cadre d'opérations de déstabilisation politique (influencer des processus électoraux...) et économique (déstabilisation macroéconomique).

Si la majorité des cyberattaques a pour but l'extorsion via des rançongiciels (programmes qui rendent inutilisables les données par leur propriétaire) ou la fraude bancaire (principalement des demandes de changement de coordonnées bancaires pour le paiement des factures) l'argent n'est pas tout... Au-delà des dommages financiers il faut se protéger de la paralysie... il est donc vital (au sens propre parfois) de garantir la poursuite du fonctionnement des entités attaquées et singulièrement des services publics. Ainsi en ce qui concerne les CHU il faut évidemment garantir la continuité des soins des patients, même avec un système d'information dégradé, et protéger les données de santé.

Quel est le bilan des premières années d'existence du CSIRT-BFC ?

Le CSIRT-BFC, mis en œuvre par l'Agence Régionale du Numérique et de l'intelligence artificielle (ARNia) pour le compte de la région, est opérationnel depuis 2022, grâce au financement de l'ANSSI (Agence nationale de la sécurité des systèmes d'information).

Le nombre de sollicitations augmente régulièrement. Entre 2023 et 2024, l'évolution est de + 61%. Le CSIRT-BFC s'adresse aux entreprises, établissements publics, collectivités et associations.

Au-delà de la réponse aux incidents, le CSIRT-BFC joue plusieurs rôles : la sensibilisation (près de 40 interventions en 2024), la détection de vulnérabilités (2.200 sites ont été analysés en 2024) et l'animation de la filière.

Notre rôle est essentiel car sans nous, il n'existe pas de structure au service des entreprises et collectivités de taille intermédiaire. Nous sommes à ce propos préoccupés pour l'avenir car l'ANSSI n'envisage plus de financer les CSIRT... or il n'y a que deux solutions pour ne pas abandonner les PME et les collectivités : soit l'ANSSI s'en occupe directement, soit elle poursuit son soutien aux CSIRT régionaux. La présidente de la région est mobilisée sur ce sujet.

Quels sont les enjeux de ce Forum consacré à la cybersécurité en BFC ?

Le Forum Cybersécurité et Numérique est le fruit de la mobilisation de la filière (French Tech BFC), de l'ANSSI et de l'ARNia. Evénement régional il est un rendez-vous majeur pour les acteurs de la filière cybersécurité en Bourgogne Franche-Comté.

À destination de tous les décideurs - en entreprises, en collectivités ou dans les associations – le Forum a pour objectif d'augmenter la sensibilisation à cette thématique devenue cruciale et de mettre en relation des fournisseurs régionaux d'offres de cybersécurité avec des entités demandeuses. En Bourgogne Franche Comté la question de la cybersécurité est ainsi placée au cœur des enjeux stratégiques tant pour le secteur public que privé.

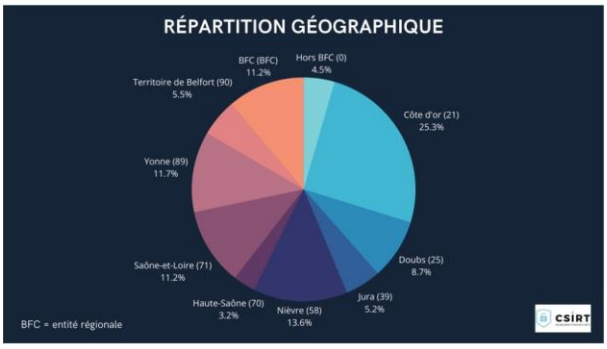
Quel arsenal juridique pour protéger les entreprises vis-à-vis des réglementations étrangères notamment concernant la protection des données ? Faut-il pour les administrations et les collectivités locales une obligation d'utilisation de suites bureautiques et d'hébergement français ?

Les législateurs, français comme européens, mènent des travaux de réglementations autour de ces sujets. Le Règlement général sur la protection des données (RGPD) a été l'une des premières pierres. Nous allons devoir mettre en place la directive européenne relative à la sécurité des réseaux et des informations (NIS 2) qui impactera les entreprises et les administrations publiques. Cette dernière oblige les organisations à appliquer des règles renforcées en matière de cybersécurité.

Pour les fournisseurs de solutions numériques, le règlement européen Cyber Resilient Act poursuit le même objectif en matière de logiciel et de matériel.

Enfin la souveraineté est cruciale. Et elle ne se limite pas à la question des logiciels mais concerne aussi l'hébergement des données (qui doit être français ou européen) voire, la problématique des matériels et composants eux-mêmes. Pour que la souveraineté numérique ne soit pas qu'un slogan, il faut à la fois des champions européens et un « small business act numérique ».

Propos recueillis par Emmanuelle de Jesus



LA CYBERSÉCURITÉ S'OFFRE UN FORUM À DIJON

C'est le premier Forum cybersécurité et numérique à portée régionale et il aura lieu rue Edgar Faure à Dijon, dans l'enceinte de l'IUT Dijon-Auxerre-Nevers, le 24 janvier de 8 h 30 à 17 h. Les thématiques abordées sont : les cybermenaces gérées par les directions informatiques, la cybersécurité vue par les RSSI, le numérique dans la santé et l'IA dans les entreprises. Quelque **300 visiteurs** sont attendus pour un rendez-vous qui s'adresse à l'ensemble des professionnels de la cybersécurité et du numérique, qu'ils soient experts, utilisateurs, ou décideurs, issus du secteur privé comme du secteur public. Cet évènement qui réunira les acteurs clés de la filière en Bourgogne Franche-Comté, est coorganisé par La French Tech Bourgogne Franche-Comté, le Centre régional de la cybersécurité de Bourgogne Franche-Comté (CSIRT-BFC), créé le 24 février 2022 et l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

« Le Forum régional de la cybersécurité s'adresse à tous les décideurs en entreprises, en collectivités ou associations. Il a pour objectif de créer un espace d'échanges et de solutions autour d'une thématique cruciale. La sécurité des données, des infrastructures, des usages est aujourd'hui plus que jamais incontournable pour assurer la continuité des activités et des services publics au bénéfice de tous », conclut **Patrick Molinoz, président de l'ARNia.**

Au programme :

◆ **Silvère Denis**, direceur délégué de La French Tech BFC, présentera les différentes actions en région.

◆ **Sébastien Morey,** directeur du CSIRT-BFC évoquera les missions du CSIRT-BFC de l'aide à la remédiation en cas de cyberattaques à l'animation de la filière cyber régionale.

◆ **Serge Durand**, ex-vice-président d'Airbus égrènera les enjeux économique, étatique et individuel de la cybersécurité.

◆ **Véronique Brunet,** déléguée à la sécurité du numérique BFC, détaillera la directive NIS2 et ses impacts.

◆ **Christophe Levallet**, spécialiste SIC à la Gendarmerie nationale parlera de la sécurisation des entreprises et des datacenters.

◆ Côté atelier, **Davis Dussort,** dirigeant de Sérénitique, interrogera notamment les participants sur la disponibilité, la résilience et la sécurité des systèmes qui soutiennent leur organisation.

◆ **Des tables-rondes** aborderont les prochaines évolutions numériques pour la prise en charge des patients, des cas concrets d'apport de l'IA dans les entreprises, les directions informatiques face aux cybermenaces et les moyens d'action des RSSI au sein de leurs organisations.

◆ **Des rendez-vous BtoB** devraient permettre aux visiteurs d'échanger avec des professionnels, d'assister à des démonstrations, se renseigner sur les dernières innovations et ainsi renforcer leur résilience face aux cyberattaques. ❐

Frédéric Chevalier

TÉMOIGNAGE : LE CAS PARTICULIER DES UNIVERSITÉS

◆ Pascal Chatonnay est enseignant chercheur à l'Université Marie et Louis Pasteur (UMLP, ex-université de Franche-Comté). Il enseigne au sein du département MMI (Métiers du Multimédia et de l'Internet) à Montbéliard, il est également Référent enseignement de défense et sécurité intérieure (REDS) et depuis un an est Responsable de la sécurité des systèmes d'information (RSSI) de l'UMLP. Il intervient sur le salon cybersécurité et numérique de Dijon sur une table ronde portant sur la sécurisation du système d'information et les moyens d'action des RSSI au sein de leurs organisations. *« Pour nos missions de RSSI, le cadre universitaire présente des particularités uniques de par les différents publics qu'il héberge. Nous avons d'un côté les enseignants-chercheurs qui réalisent des expérimentations complexes aux frontières de la sécurité et qui s'accommodent mal d'un dispositif de sécurité informatique trop contraignant. Pour eux, il s'agit de trouver le juste milieu entre verrouillage total du système et ouverture sans limite. De l'autre côté, se trouvent les étudiants qui viennent avec leurs propres machines, qui peuvent être contaminées, et qui se raccordent au réseau ».* Face à ses différentes usagers de l'université, les solutions techniques (filtres, pare-feu, routeurs, antivirus…) ne suffisent pas, il est nécessaire de faire évoluer les pratiques des utilisateurs *« d'autant que concernant les chercheurs, leurs recherches de pointes peuvent être la cible de pirates ou d'espions »*, explique Pascal Chatonnay ajoutant que la sensibilisation constitue une très grande partie de son travail : *« Nous avons en moyenne une fois par semaine une alerte pour un matériel compromis ou exposé à des attaques. Nous donnons des conseils aux étudiants sur la façon de décontaminer leurs appareils, les PC mais aussi les portables qui contiennent beaucoup de secrets, et sur les bons réflexes à adopter. Côté enseignants-chercheurs, nous les alertons également sur les risques liés à leurs déplacements à l'étranger, sur les dangers des wifi-fi publics, sur la nécessité d'utiliser un VPN crypté de bout en bout, sur la sécurité des mots de passe ou encore sur la bonne utilisation du Bluetooth… Cette sensibilisation de nos publics est plutôt efficace, nous recevons beaucoup d'appels sur de potentielles menaces après une intervention de nos services, mais les réflexes et bonnes résolutions s'émoussent vite : les piqûres de rappel sont indispensables, c'est un travail de longue haleine ».*

Propos recueillis par F. C.

DES SOLUTIONS LOCALES ET FRANÇAISES

La cybersécurité est devenue une problématique majeure pour les entreprises et les collectivités, en particulier face à l'augmentation exponentielle des cyberattaques. Récemment, on note que les géants Kiabi (prêt-à-porter) et Free (opérateur de téléphonie mobile) ont été pris pour cible. Localement, c'est la communauté de communes de Nuits-Saint-Georges qui subissait un piratage informatique en mars 2024 – malgré le renforcement de son système de sécurité suite à une attaque subie en 2019. Aujourd'hui, il n'est plus seulement question de vigilance et d'équipement : il faut s'entourer des bonnes compétences pour parvenir à se protéger efficacement. « *Il faut se faire aider parce que malheureusement la plupart des entreprises ont créé un système d'information en achetant un équipement réseau, des serveurs, des choses comme ça, mais sans vraiment en avoir une connaissance accrue,* constate Sébastien Morey, responsable du CSIRT-BFC. *Quand on veut sécuriser son système par défaut, il faut de la compétence, il faut des gens qui savent le faire. Ces compétences sont bien plus présentes localement aujourd'hui qu'elles ne l'étaient en 2022* ».

« *On a dans nos structures adhérentes des fournisseurs, que ce soient les start up ou des offreurs de solutions, qui eux-mêmes portent des solutions de cybersécurité,* témoigne Silvère Denis, directeur délégué de la French Tech Bourgogne Franche-Comté. *Notre objectif, c'est de faire en sorte que ces solutions soient connues, développées, et adoptées par tous. C'est aussi pour cela qu'on participe à l'organisation de ce Forum Cybersécurité* ». Car c'est peut-être ici que se situe l'enjeu principal du secteur : acculturer les entreprises et les collectivités locales de toutes tailles à ces problématiques grandissantes. « *Les entreprises de la French Tech ont des solutions technologiques, donc le sujet de la cybersécurité est souvent pris en main dès le démarrage. C'est surtout pour les autres secteurs économiques, où toutes les entreprises font aujourd'hui face à des évolutions technologiques importantes, notamment l'IA, une véritable révolution industrielle. Ces entreprises intègrent de plus en plus d'outils et gèrent de plus en plus de données, mais en face elles ont besoin de se structurer et de*

> **« QUAND ON VEUT SÉCURISER SON SYSTÈME PAR DÉFAUT, IL FAUT DE LA COMPÉTENCE, IL FAUT DES GENS QUI SAVENT LE FAIRE »**
>
> SÉBASTIEN MOREY, RESPONSABLE CSIRT-BFC.
> CRÉDIT PHOTO : ÉDOUARD BARRA.


FREEPIX

monter en compétences pour pouvoir être suffisamment armées pour faire face à ces nouvelles menaces. Le vrai enjeu c'est de pouvoir bien identifier et s'entourer des bons partenaires ».

RÉAGIR EN CAS D'ATTAQUES

« *Je pense que de plus en plus de monde est conscient des enjeux stratégiques et du besoin de sécuriser,* observe Silvère Denis. *Mais de toute façon, le risque zéro n'existe pas* ». Alors que faut-il faire en cas de menaces ou d'intrusion ? « *Au moment où l'attaque arrive, si l'entreprise est bien préparée, elle a déjà la liste des personnes qu'elle doit contacter* », précise Sébastien Morey. Il peut s'agir de prestataires extérieurs, de spécialistes internes, ou directement du centre régional de cybersécurité. « *Quand on parle de cyberattaques, il faut bien comprendre qu'il existe au moins 25 catégories différentes, et en fonction, on n'agit pas toujours de la même façon,* poursuit le responsable du CSIRT-BFC. *Si on prend le cas le plus compliqué où on a un chiffrement des données, les actions doivent être prises le plus rapidement possible : on déconnecte les éléments du réseau, mais on n'éteint pas tout électriquement car on pourrait perdre des éléments de preuve ou des informations qui pourraient aider les spécialistes à déchiffrer plus facilement* ». Ensuite, un plan d'action de reprise d'activité est engagé, avec la mise en place d'une cellule de crise. « *On fait souvent intervenir des acteurs de la région pour aider les entreprises touchées qui, généralement, n'ont pas les moyens de tout faire seules,* explique Sébastien Morey. *Et puis, sur des cas très graves, on est obligés de partir d'un système d'information totalement vierge, puis remonter les serveurs et les postes de travail un par un. Quand on réintègre une machine au réseau, on s'assure qu'elle n'est pas vérolée et on la sécurise. Quand on a quatre machines, ça va,* poursuit-il, *mais imaginez le cas d'un hôpital avec 1.000 serveurs et 5.000 postes, ça prend un temps énorme ! On ne peut pas le faire seul, il faut se faire aider* ». « *On a aujourd'hui des solutions locales ou françaises qui peuvent répondre aux besoins de l'ensemble des acteurs pour se protéger sur le volet cybersécurité* », rappelle Silvère Denis. On note, entre autres, en Bourgogne Franche-Comté, des structures telles que Proxim Cybersolutions (expert en cybersécurité à destination des TPE/PME, collectivités en zone rurale - 89), C2iP (accompagnement DSI/RSSI/DPO - 21), Fcnet (solutions télécom, hébergement local, cybersécurité, réseaux - 25), 3S Sécurité (cybersécurité - 21), N-CyberExpertise (Consultant en cybersécurité accompagnant les TPE/PME - 58), Cybergogne (démocratise l'accès à des solutions de cybersécurité avancées, spécifiquement pour les petites entreprises, collectivités locales et organisations en Bourgogne - 21) ou encore H4ckrz (spécialiste de la cybersécurité offensive - 71). « *Ces entreprises répondent à pas mal de normes, de critères et de certifications dans différents domaines* », certifie le directeur délégué de la French Tech BFC. ❐

Killian Roblot

« NOTRE OBJECTIF, C'EST DE FAIRE EN SORTE QUE LES SOLUTIONS PORTÉES PAR NOS START-UP LOCALES SOIENT CONNUES, DÉVELOPPÉES, ET ADOPTÉES PAR TOUS. C'EST AUSSI POUR CELA QU'ON PARTICIPE À L'ORGANISATION DE CE FORUM CYBERSÉCURITÉ »

SILVÈRE DENIS, DIRECTEUR DÉLÉGUÉ DE LA FRENCH TECH BFC.
CRÉDIT PHOTO : DAVID CESBRON/LA FRENCH TECH BFC.


FREEPIX

RÉPONDRE EFFICACEMENT AUX INCIDENTS

AU service des entreprises et des collectivités de toutes tailles, la startup cybertech Sekoia.io propose des solutions SaaS (« Software as a Service » ou « logiciel en tant que service ») visant à détecter et répondre aux incidents de sécurité. « *Pour ce faire, on propose des solutions qui sont basées sur le renseignement cyber ou la "cyber threat intelligence" : pour être capable de détecter des menaces, on étudie les attaquants pour repérer les infrastructures et les serveurs qu'ils vont utiliser*, explique Martial Outrey, vice-président en charge des alliances chez Sekoia.io. *On est donc une équipe de chercheurs qui fait des investigations pour identifier les traces d'attaquants et répondre aux menaces grâce aux éléments techniques en notre possession* ». Avec des solutions hébergées dans le cloud, Sekoia.io peut démultiplier ses capacités de détection et de réponse, « *ça facilite beaucoup les choses et on peut davantage automatiser* ». Dans les faits, la startup se sert des sécurités déjà mises en place par ses clients (antivirus, proxys…) pour en agréger les données et parvenir à aller plus loin. « *L'idée c'est de rationaliser tous les outils déjà déployés, de les piloter, sans mettre à la poubelle l'existant, car il a évidemment un intérêt*, précise Martial Outrey. *On apporte une vision à 360 aux clients, qui sont donc en mesure de détecter et corréler des signaux faibles qui viennent de différentes parties de son système d'information* ».

« ON APPORTE UNE VISION À 360 AUX CLIENTS, QUI SONT DONC EN MESURE DE DÉTECTER ET CORRÉLER DES SIGNAUX FAIBLES QUI VIENNENT DE DIFFÉRENTES PARTIES DE SON SYSTÈME D'INFORMATION »

MARTIAL OUTREY, VICE-PRÉSIDENT EN CHARGE DES ALLIANCES CHEZ SEKOIA.IO.

CRÉDIT PHOTO : DR

FREEPIX

UN MARCHÉ QUI SE DÉMOCRATISE

« *Depuis moins de cinq ans, on observe une tendance sur le marché des SMB (Small-to-Medium Sized Business, traduisible par TPE/PME, Ndlr) qui sont soit contraints par la force des choses, soit prennent conscience de la nécessité d'investir dans leur cybersécurité*, témoigne Martial Outrey. *Aujourd'hui le marché se transforme beaucoup : l'accès à la sécurisation des infrastructures des entreprises, des administrations et des collectivités passe par des sociétés de services qui vont opérer au quotidien en temps réel la cybersécurité de ces structures* ». Ainsi, face à un manque de moyens pour attirer des profils qualifiés très recherchés, de plus en plus d'administrations – même modestes – sont en mesure d'accéder à des services de cybersécurité en faisant appel à des prestataires de services. On note les principaux que sont Orange Cyberdéfense, Atos, Thales ou Capgemini, parfois clients de Sekoia.io. « *Il faut aussi garder en tête que le marché se transforme car des réglementations sont mises en place*, rappelle Martial Outrey. *Les très grandes entreprises françaises ont été réglementées il y a à peu près dix ans par la LPM, la loi de programmation militaire, qui oblige un certain nombre de grandes entreprises à se conformer à des règles de sécurité. En France, on a l'avantage d'agir par la réglementation, elle entraîne le marché. Ça a été le cas pour les grandes entreprises, mais on voit aujourd'hui que ça commence aussi à avoir une incidence claire sur le marché SMB – notamment depuis l'entrée en vigueur de nouvelles directives européennes* (Nis 1 et 2, Ndlr), *encore balbutiantes* »

Killian Roblot

« TOUTES LES MENACES PEUVENT VENIR DE L'IA »

Entretien avec Marion Kemps Houver, responsable du développement IA chez JustAI, cabinet de conseil et d'ingénierie en intelligence artificielle.

***Le Journal du Palais*. Quelle est la place de l'intelligence artificielle dans le domaine de la cybersécurité ? Comment est-elle concrètement utilisée ?**

Marion Kemps Houver. L'IA et la cybersécurité sont liées depuis un moment déjà, mais comme cela fait partie de notre quotidien, on n'y fait pas forcément attention. On peut par exemple utiliser les systèmes d'intelligence artificielle pour détecter les intrusions ou les comportements anormaux avec des pares-feux intelligents. De plus en plus d'entreprises intègrent l'IA dans leur cybersécurité, que ce soit pour détecter ces comportements étranges ou des intrusions sur un réseau. Il y a aussi des choses qui existent depuis longtemps qui permettent de vérifier que c'est un humain et non une machine qui essaie d'intégrer ou pirater un système.

Lorsqu'une attaque est en cours, l'IA reste utile : elle permet de détecter des patterns inhabituels et d'étudier les activités suspectes ou les extractions de données pour « prédire la suite ». On peut alors plus facilement cibler où est l'attaque et réagir plus rapidement.

Concrètement, il existe des logiciels d'intelligence artificielle très efficaces : il y a notamment Darktrace qui permet d'identifier des comportements anormaux sur un réseau – le logiciel peut par exemple s'appuyer sur des algorithmes d'apprentissage automatique pour détecter si je me connecte sur mon espace de travail en dehors de mes heures habituelles, et ainsi lancer une alerte si l'activité est suspecte.

L'Intelligence artificielle est également utilisée du côté des cyberattaquants, est-elle davantage leur alliée que la nôtre ?

Je dirais que c'est à peu près 50/50 : l'IA permet par exemple de sécuriser et de mieux reconnaître les attaques de type phishing (ou hameçonnage, Ndlr), mais de l'autre côté, elle sera aussi capable de créer des pièges plus crédibles pour l'humain. Toutes les cybermenaces peuvent venir de l'intelligence artificielle : elle permet de contextualiser les éléments et de reproduire ce qui existe déjà pour intégrer le réseau d'une entreprise. Il existe par exemple une application qui, en 30 secondes, permet d'enregistrer une voix et la reproduire en différentes langues ou lui faire dire des choses qu'elle n'aurait jamais dites. D'où la vigilance qu'il faut avoir au quotidien par rapport aux fake news ou ce genre de choses qui peuvent entraîner de nombreuses problématiques dans le monde professionnel et personnel. Il faut savoir s'en protéger, mais aussi apprendre à l'utiliser et comprendre comment cela fonctionne.

La première chose que je demande quand j'interviens en entreprise c'est « Est-ce que vous utilisez ChatGPT ? Si c'est le cas, est-ce que vous l'avez bien configuré pour ne pas que vos données entraînent le modèle ? » C'est une vérification importante à mettre en œuvre pour la sécurité des données de l'entreprise. Si vous avez une recette spécifique et que vous souhaitez l'améliorer avec ChatGPT sans le configurer pour protéger vos données, cette recette sera disponible aux yeux de tous car elle entrera dans le catalogue des informations utilisées par le modèle, mais c'est aussi valable pour des informations plus sensibles.

Nous, au niveau de notre cybersécurité, quand on déploie un modèle on le met sur un GPU - un petit processeur - où toutes les données de l'entreprise sont hébergées en local (plutôt qu'en réseau), garantissant une certaine sécurité. Pour prédire les attaques et pour la souveraineté de nos données en France, il vaut mieux qu'il y ait des serveurs qu'on utilise depuis chez nous : c'est ce vers quoi se dirigent de plus en plus de sociétés.

Pour les petites entreprises, TPE/PME, et les collectivités, l'intelligence artificielle constitue aujourd'hui un danger bien plus grand qu'avant, c'est clair. Mais aujourd'hui, ces structures n'ont pas des fonds assez importants, ça reste des questions de moyens. Malheureusement, pour se protéger, il faut avoir de l'argent, et ce malgré les différents financements qui existent...

Quelle est alors la solution pour ces petites structures ?

Le vrai problème c'est quand on se dit que ce genre d'attaque n'arrive jamais et donc on ne met pas en place de système de cyberdéfense. En avoir un, ce n'est pas non plus la garantie que rien ne se passera, mais c'est une sécurité supplémentaire. Il y a toujours une marge d'erreur, il faut toujours être vigilant.

Selon moi, chaque entreprise ayant des données spécifiques, il faut parvenir à adapter les logiciels en fonction des besoins. En réalité, c'est un accompagnement qu'il faut faire, pas simplement se dire « j'achète mon logiciel et c'est bon je suis protégé ». Il faut partir d'un diagnostic complet pour que cette solution soit pertinente : chacun a des contraintes ou des problématiques différentes.

Il y aussi un besoin d'acculturation. La sensibilisation est importante – c'est par exemple le cas dans le cadre de ce Forum de la Cybersécurité. Malheureusement, il y a encore des PME pour lesquelles l'informatique passe au second plan, mais aujourd'hui, sans ordinateur, on ne travaille plus : se protéger est une nécessité.

Propos recueillis par Killian Roblot

LES USAGES CRIMINELS DE L'INTELLIGENCE ARTIFICIELLE EN 2023

◆ Les progrès de l'Intelligence Artificielle (IA) et son usage par les cyberdélinquants représentent aujourd'hui, comme pour les années à venir, un défi majeur pour les forces de sécurité intérieure.

Depuis l'avènement des larges modèles de langage sur lesquels s'appuie l'IA générative, nombreuses sont les opportunités d'imposture que ce soit dans le domaine de l'image, de l'audio ou du texte.

Et l'espace cyber ne manque pas à l'appel puisqu'il y est possible de générer, modifier ou optimiser des maliciels ou encore de réaliser des campagnes d'hameçonnage.

L'IA offre ainsi la possibilité d'améliorer les campagnes de phishing non seulement en générant de nouvelles techniques mais aussi en démultipliant les cibles potentielles notamment par du multilinguisme.

Ces techniques, réservées à une criminalité organisée il y a quelques années, sont aujourd'hui à la portée du délinquant d'opportunité sans compétence ni budget importants.

L'IA, c'est encore la possibilité de gérer des réseaux de machines zombies (botnets) et d'augmenter l'efficience des attaques de type DDoS par exemple en adaptant les schémas d'attaques aux mesures de sécurité mises en place sur les systèmes d'information visés.

Parmi les enjeux à fort impact, le phénomène des deepfakes, au regard de la célérité et de la diversité des développements, est à prendre en compte dès à présent par les forces de sécurité intérieure.

Toujours plus réalistes, ces impostures accrois-sent considérablement l'efficacité des faux ordres de virement, la vraisemblance des théories complotistes ou encore des atteintes à l'identité numérique.

Source : rapport annuel sur la cybercriminalité 2024. Ministère de l'Intérieur et des Outre-Mer.

Auteurs : Frédéric Chevallier / Emmanuelle de Jesus / Kilian Roblot

Lien : https://journal-du-palais.fr/le-kiosque/

ICI 12/13 Bourgogne
Réalisation C.Meunier, R.Augier, C.Clerc
Durée : 2 minutes
https://www.france.tv/france-3/bourgogne-franche-comte/ici-12-13-bourgogne/6843250-emission-du-vendredi-24-janvier-2025.html

ICI 19/20 Bourgogne
Réalisation C.Meunier, R.Augier, C.Clerc
Durée : 2 minutes
https://www.france.tv/france-3/bourgogne-franche-comte/ici-19-20-bourgogne/6843238-emission-du-vendredi-24-janvier-2025.html

ici Bourgogne

Les infos de 07h00 du samedi 25 janvier 2025

Le 25 janvier 2025

5 min

https://www.francebleu.fr/archives/emissions/le-journal-de-07h00-fb-bourgogne/2025?pageCursor=MA%3D%3D

Reportage réalisé par Stéphanie PERENON
Durée : 1 minute 34

LE BIEN PUBLIC

Bourgogne-Franche-Comté

Comment se protéger contre les cyberattaques en recrudescence

Avec l'utilisation toujours plus massive du numérique, les systèmes et données des entreprises ou des établissements publics n'ont jamais été aussi menacés par les cyberattaques. En Bourgogne-Franche-Comté, le centre régional de cybersécurité (CSIRT) apporte des solutions préventives et curatives à ces problématiques.

Juliette Boffy - Hier à 17:00 | mis à jour hier à 17:32 - Temps de lecture : 4 min

« Les cyberattaques ne font qu'augmenter et cela ne risque pas de s'arrêter », lance Sébastien Morey, responsable du CSIRT (*Computer security incident response team*) de Bourgogne-Franche-Comté (BFC), à l'occasion du forum régional Cybersécurité et numérique de Dijon , qui se tenait vendredi 24 janvier au sein de l'IUT (Institut universitaire de technologie).

Le numérique, déjà omniprésent dans nos vies, et l'arrivée de l'intelligence artificielle, ne font que démultiplier d'année en année les actes malveillants provenant de cyberattaquants. En 2023, le dispositif Cybermalveillance.gouv.fr a rapporté une augmentation des faux ordres de virement de 63 %, des défigurations de sites internet de 61 %, et des inaccessibilités de serveurs d'entreprise de 41 %.

---

*Extrait du média **Le Bien Public,** le 26 janvier 2025*
Auteur : Juliette Boffy
Lien : https://www.bienpublic.com/economie/2025/01/26/comment-se-proteger-contre-les-cyberattaques-en-recrudescence

Cybersécurité : une prise de conscience collective est nécessaire

Les acteurs de la cybersécurité en Bourgogne-Franche-Comté ont tenu leur premier forum à Dijon, histoire de rappeler l'urgence d'une prise de conscience collective de la menace et découvrir la filière numérique locale dédiée à la prévention et la protection.

Fred JIMENEZ - Aujourd'hui à 12:32 | mis à jour aujourd'hui à 12:33 - Temps de lecture : 3 min

Le sujet est suffisamment grave pour justifier une union sacrée. Celle du centre régional de cybersécurité (CSIRT) , de l'Agence nationale de la sécurité des systèmes d'information (Anssi) et de la French tech de Bourgogne-Franche-Comté qui organisaient le premier Forum régional cybersécurité et numérique, ce vendredi 24 janvier, à l'IUT de Dijon.

*Extrait du média **L'Est Républicain**, le 27 janvier 2025*
Auteur : Fred Jimenez
Lien : https://www.estrepublicain.fr/economie/2025/01/27/cybersecurite-une-prise-de-conscience-collective-est-necessaire

la gazette
des communes • des départements • des régions

Les centres régionaux de cybersécurité en quête de financements

Publié le 27/01/2025 • Par Gabriel Thierry • dans : France

Face à la menace de cyberattaques, l'agence nationale de sécurité des systèmes informatiques (Anssi) s'appuie sur un réseau de douze entités territoriales.
Anssi

Avec la fin annoncée de la subvention de l'Etat, les structures territoriales d'assistance informatique, dont le douzième centre vient d'être inauguré en Corse, doivent trouver leur équilibre financier.

Et de douze ! En avril 2024, l'inauguration du centre régional de réponse aux incidents informatiques CyberCorsica, un CSIRT – Computer Security Incident Response Team, selon son acronyme en anglais – porte à une douzaine le nombre de ces structures régionales en métropole.

Il en existe également deux en outre-mer, le premier pour l'Atlantique, le second pour l'île de La Réunion. L'Auvergne – Rhône-Alpes est désormais la seule collectivité régionale sans structure de ce type. En 2021, l'Agence nationale de la sécurité des systèmes d'information (Anssi) avait soutenu le lancement de ces CSIRT territoriaux, financés, pour leurs débuts, par le plan de relance. Autant de structures sur lesquelles le cyber-pompier français, qui se voit en chef d'orchestre, compte s'appuyer.

*Extrait du média **La Gazette des Communes,** le 27 janvier 2025*
Auteur : Gabriel Thierry
Lien : https://www.lagazettedescommunes.com/965962/les-centres-regionaux-de-cybersecurite-en-quete-de-financements/

LE JOURNAL DU CENTRE

Cyberattaques : les entreprises et collectivités de la Nièvre ne sont pas épargnées

Le premier forum régional cybersécurité et numérique était organisé le 24 janvier à Dijon. L'occasion de découvrir les solutions pour se protéger des risques qui ne font que croître. En 2024, 177 entreprises ou collectivités, cyberattaquées, ont appelé le centre régional de réponse aux cyberattaques.

C'est une première en Bourgogne-Franche-Comté : le centre régional de réponse aux cyberattaques (le CSIRT), l'Agence nationale de la sécurité des systèmes d'information (Anssi) et la French Tech ont organisé le 24 janvier à Dijon un forum régional cybersécurité et numérique. L'objectif : mobiliser les entreprises et les collectivités autour de ce risque et les inciter à se saisir des moyens existant pour se défendre.

*Extrait du média **Le Journal du Centre**, le 27 janvier 2025*
Auteur : Alexandra Caccivio
Lien : https://www.lejdc.fr/dijon-21000/economie/cyberattaques-les-entreprises-et-collectivites-de-la-nievre-ne-sont-pas-epargnees_14631128/

LE JOURNAL DU CENTRE

L'usage de l'IA bouleverse l'activité des entreprises

L'intelligence artificielle entre peu à peu dans les entreprises pour venir soutenir l'activité. Des applications comme Dicte-ai peuvent permettre de gagner énormément de temps pour les entreprises.

C'est un des autres sujets abordés lors du forum régional cybersécurité et numérique : l'intelligence artificielle entre peu à peu dans les entreprises pour venir soutenir l'activité. « Cela fait longtemps qu'elle est utilisée dans les usines, par exemple pour la détection des défauts en sortie de chaîne (...) ou pour faire de la maintenance prédictive », relève Marion Kemps Houver, responsable développement dans la start-up Just IA.

*Extrait du média **Le Journal du Centre**, le 27 janvier 2025*
Auteur : Alexandra Caccivio
Lien : https://www.lejdc.fr/dijon-21000/economie/lusage-de-lia-bouleverse-lactivite-des-entreprises_14631130/

le Journal du Palais
Réseau Légalnet

Cybersécurité : nul n'est à l'abri !

Région BFC. Près de 300 acteurs étaient rassemblés vendredi 24 janvier à l'IUT Dijon-Auxerre-Nevers pour assister au premier Forum régional Cybersécurité et Numérique .

L'objectif de cette rencontre était notamment de créer un moment de confiance autour de la problématique de la protection des données des entreprises, collectivités et associations en rappelant que *« la cybersécurité est un des principaux défis de la numérisation de la société »*, souligne Patrick Molinoz, président de l'Agence régionale du numérique et de l'intelligence artificielle (ARNia) qui anime le CSIRT territorial. *« J'aime rappeler que l'univers numérique devrait être pensé comme le monde "physique" : il n'y a ni liberté, ni démocratie, ni croissance pour les citoyens dans le monde "physique" sans sécurité. C'est la même chose avec le numérique. Il faut donc protéger les données collectées et les systèmes qui les traitent pour permettre le fonctionnement normal, et sain, de leur activité. »*

L'évènement co-organisé par le CSIRT Bourgogne-Franche-Comté, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et la French Tech Bourgogne-Franche-Comté, a permis aux participants de s'informer et de rencontrer les entreprises de la filière cybersécurité venues présenter leurs savoir-faire et offres de services.

Des Appels Au CSIRT En Hausse De 61 %

« À l'heure où les attaquants se saisissent de toutes les opportunités, notamment pour mener des attaques à des fins d'extorsion financière, les entreprises, les établissements publics et les collectivités doivent impérativement hisser leur niveau de cybersécurité, précise Véronique Brunet, déléguée de l'ANSSI en Bourgogne Franche-Comté. Parmi les premières choses à mettre en place il y a la création de sauvegardes sur disques durs déconnectés du réseau et la création de mots de passe complexes et cryptés, notamment sur les messageries. Ces deux précautions permettent de réduire les failles de sécurité et de se reconstruire plus vite en cas d'attaque ». *« Ce forum constitue également une opportunité essentielle pour renforcer la collaboration entre acteurs économiques, collectivités, fournisseurs de solutions en cybersécurité et start-up innovantes locales »*, ajoute Silvère Denis, directeur délégué de la French Tech Bourgogne Franche-Comté. *« N'attendez pas d'être attaqué et de subir de graves préjudices pour nous contacter. Le CSIRT-BFC n'est pas uniquement le pompier de la cybersécurité, c'est aussi votre allié au quotidien pour vous aider à protéger votre système d'information contre les cyberattaques, détecter les menaces dès leur apparition et réduire l'impact et la durée entre le piratage informatique et le rétablissement normal de votre activité »*, défend

Sébastien Morey, responsable du centre régional de cybersécurité Bourgogne Franche-Comté, tout en rappellant que *« nul n'est à l'abri ! »*. Le CISRT BFC a reçu en 2024, 404 sollicitations contre 250 en 2023, soit 61 % d'augmentation. Dans le détail, 40 % de ces appels sont des demandes d'information, 44 % des incidents, 16 % des alertes (actions de prévention à destination des bénéficiaires, par exemple détection de vulnérabilités). Par ailleurs, 47 % des sollicitations concernent des communes et des communautés urbaines, d'agglomération et de communes, 18 % des établissements publics et 20 % des entreprises (TPE, PME, ETI). Les sollicitations les plus fréquentes concernent la fraude bancaire, les faux sites marchands, les rançongiciels et l'hameçonnage (phishing). *« Au-delà de la réponse aux incidents, le CSIRT-BFC joue plusieurs rôles : la sensibilisation, les alertes comme des détections de vulnérabilités et l'animation de la filière à l'instar de ce Forum Cybersécurité et Numérique »*, complète Sébastien Morey. *« Ce forum apparaît aussi comme un révélateur de l'émergence en BFC d'une véritable filière de la cybersécurité, souligne Silvère Denis, directeur délégué de la French Tech BFC. Les entreprises de la French Tech BFC sont parfaitement positionnées pour offrir des réponses fiables et efficaces aux défis croissants de cybersécurité auxquels font face les entreprises et les collectivités de notre territoire. En collaboration avec le CSIRT Bourgogne Franche-Comté, nous avons notamment permis la création d'un annuaire régional des prestataires en cybersécurité, regroupant 50 sociétés qualifiées pour accompagner les acteurs locaux dans leur montée en résilience face aux cybermenaces »*.

Auteur : Frédéric Chevalier

Lien : https://journal-du-palais.fr/au-sommaire/entreprises/cybersecurite-nul-n-est-a-l-abri

Au cœur des territoires
Côte d'Or

28 janvier 2025

Près de 300 acteurs ont assisté au premier Forum régional Cybersécurité et Numérique qui s'est déroulé à Dijon. L'occasion pour différents experts de la Bourgogne-Franche-Comté et d'autres régions de partager leurs connaissances et rappeler les défis à relever pour contrer les cybermenaces.

Communiqué :

Le premier Forum régional Cybersécurité et Numérique s'est tenu à Dijon. L'objectif de cette rencontre était notamment de créer un moment de confiance autour de la problématique de la protection des données des entreprises, établissements publics et collectivités en rappelant que « la cybersécurité est un des principaux défis de la numérisation de la société », comme l'a souligné Patrick MOLINOZ, Président de l'Agence Régionale du Numérique et de l'intelligence artificielle (ARNia) qui anime le CSIRT territorial. « J'aime rappeler que
l'univers numérique devrait être pensé comme le monde « physique » : il n'y a ni liberté, ni démocratie, ni croissance pour les citoyens dans le monde « physique » sans sécurité. C'est la même chose avec le numérique. Il faut donc protéger les données collectées et les systèmes qui les traitent pour permettre le fonctionnement normal et sain, de leur activité. »

« À l'heure où les attaquants se saisissent de toutes les opportunités, notamment pour mener des attaques à des fins d'extorsion financière, les entreprises, les établissements publics et les collectivités doivent impérativement hisser leur niveau de cybersécurité » a précisé Véronique BRUNET, déléguée de l'ANSSI en Bourgogne-Franche-Comté.
« Dans un contexte où les cyberattaques se multiplient et touchent tous les secteurs, ce forum constitue une opportunité essentielle pour renforcer la collaboration entre acteurs économiques, collectivités, fournisseurs de solutions en cybersécurité et start-up innovantes locales » a déclaré Silvère DENIS, Directeur délégué de la French Tech Bourgogne-Franche-Comté, lors de son allocution.

Hausse de 61% des sollicitations en 1 an : la mission du CSIRT territorial reste indispensable

Le Forum a été l'occasion pour le CSIRT Bourgogne-Franche-Comté, par la voix de son responsable, Sébastien MOREY, de dresser le bilan des actions du centre régional de cybersécurité menées depuis 2023 pour sensibiliser les acteurs publics comme privés – nul n'est à l'abri a-t-il alerté - à la nécessité d'anticiper les cyberattaques qui ne cessent de progresser, touchant toutes les entités publiques et privées quelle qu'en soit la taille :

« N'attendez pas d'être attaqué et de subir de graves préjudices pour nous contacter. Le CSIRT-BFC n'est pas uniquement le 15 de la cybersécurité, c'est aussi votre allié au quotidien (numéro gratuit accessible 24/24, 7/7) pour vous aider à protéger votre système d'information contre les cyberattaques, détecter les menaces dès leur apparition et réduire l'impact et la durée entre le piratage informatique et le rétablissement normal de votre activité ».

Les chiffres du bilan de l'année 2024 et la progression par rapport à 2023 suffisent à eux-mêmes pour redire la nécessité de l'action du centre régional de cybersécurité créé en 2022 grâce au financement de l'ANSSI :

* 404 sollicitations reçues par le CSIRT en 2024 contre 250 en 2023 soit 61% d'augmentation. Ces 404 sollicitations correspondent à 4621 entités alertées ou impactées, une sollicitation du CSIRT pouvant être faite pour plusieurs établissements (les filiales d'une entreprise par exemple) :
- 40% sont des demandes d'information, 44% des incidents et 16% des alertes (actions de prévention à destination des bénéficiaires, par exemple détection de vulnérabilités).
- 47% sont des communes et des communautés urbaines, d'agglomération et de communes, 18% des établissements publics et 20% des entreprises (TPE, PME, ETI).
- les sollicitations les plus fréquentes concernent la fraude bancaire, les faux sites marchands, les rançongiciels et l'hameçonnage (phishing).

« Le constat est que le Centre régional de cybersécurité est mieux connu aujourd'hui et les entreprises le sollicitent de plus en plus depuis 2024 », explique Sébastien MOREY. Au-delà de la réponse aux incidents, le CSIRT-BFC joue plusieurs rôles : la sensibilisation, les alertes comme des détections de vulnérabilités et l'animation de la filière à l'instar de ce Forum Cybersécurité et Numérique. » L'occasion de rappeler les quatre grandes missions du CSIRT de Bourgogne-Franche-Comté à destination des établissements publics, collectivités territoriales, PME /ETI et associations :

1/REMEDIER : via un numéro unique régional [0970 609 909], le CSIRT-BFC prend en charge la demande des acteurs régionaux victimes d'une cyberattaque en les orientant vers des prestataires pour la remédiation, vers les forces de l'ordre (Gendarmerie, Police) pour le dépôt de plainte, vers la CNIL en cas de violation de données à caractère personnel et vers l'ANSSI pour le suivi de l'incidentologie.

2/ ALERTER lorsque des vulnérabilités sont détectées, sur la fin des supports logiciels, sur les fuites de données. Actuellement le CSIRT supervise 2200 entités en effectuant 2 millions de scans/an. Quant aux fuites de données, grâce au service baptisé cyberleaks (soumis au consentement du bénéficiaire), il analyse plus de 5000 bases de fuites sur le darkweb.

3/ SENSIBILISER les acteurs de la région sur les thématiques de la cybersécurité (menaces, risques, comment s'en protéger, bonnes pratiques) via l'information, les rencontres de la filière, des webinaires, le cybermois en octobre.

• En 2024 le CSIRT Bourgogne-Franche-Comté a réalisé plus de 45 actions de sensibilisation et d'information (37 de sensibilisation et 8 webinaires). La sensibilisation est constante via des articles en accès libre sur le site web (https://www.csirt-bfc.fr/) qui reçoit 40.000 visites/an et la diffusion d'informations via Linkedin.

• Il a développé plusieurs outils gratuits : analyse de courriels douteux, fin de supports des logiciels, test de la robustesse des mots de passe.

4/ ANIMER : Forum régional annuel, rencontres et annuaire des prestataires en cybersécurité en BFC https://www.csirt-bfc.fr/cyber-en-bfc/ : référencement de 50 sociétés par domaine d'intervention, qualification (ANSSI, Expert Cyber, ISO…), zone géographique d'intervention, horaires d'ouverture…

Auteur : Nadège Hubert

Lien : https://www.echodescommunes.fr/actualite_5329_un-forum-dadia-a-la-cybersacurita.html

Paroles d'élus

Cybersécurité

Lundi 27 janvier 2025

Au Forum régional Cybersécurité et Numérique avec Silvère Denis

Mobilisation générale en région Bourgogne-Franche-Comté. Le 24 janvier dernier, plus de 400 participants, acteurs publics et privés, étaient réunis à Dijon pour le premier Forum régional Cybersécurité et Numérique. Un succès dû sans aucun doute à la formule choisie et à l'implantation des trois organisateurs : le CSIRT régional, l'ANSSI et la French Tech BFC.

Des inscriptions stoppées rapidement

Il ne fallait pas arriver en retard ce vendredi matin à l'IUT de Dijon. L'amphi, plein à craquer, a peut-être rappelé aux plus nostalgiques ou aux plus assidus leurs années d'études et certains cours magistraux. Cette première édition du Forum régional Cybersécurité et Numérique a donc rempli son objectif de mobilisation. Notons au passage que les inscriptions ont été stoppées six jours avant… Mais qu'est-ce qui explique un tel engouement ?

Une grande diversité de profils

Pour Silvère Denis, Directeur délégué de La French Tech Bourgogne, le sujet, de plus en plus prégnant ces dernières années, y est pour beaucoup : ***"Nous avons une grande diversité de profils : des entreprises du secteur, des acteurs publics, des administrations et des étudiants."*** Côté contenu, le programme est riche afin de permettre de découvrir de nouvelles solutions et d'échanger avec des experts du domaine.

Un programme particulièrement riche

"Nous avons des témoignages et des retours d'expérience en amphithéâtre, ainsi que des éléments de contexte sur les évolutions réglementaires, nous précise le Directeur délégué de La French Tech Bourgogne, car les enjeux autour de la cybersécurité sont de plus en plus importants. En parallèle, tout au long de la journée, les participants peuvent découvrir des solutions innovantes, ***rencontrer des experts et assister à des démonstrations technologiques***."

Une French Tech dynamique

À la question de savoir si la French Tech se porte bien en Bourgogne-Franche-Comté, Silvère Denis nous le confirme : ***"Elle se porte très bien ! Elle est en plein développement et en pleine dynamique. Aujourd'hui, nous rassemblons près de 400 organisations issues de divers secteurs et nous les fédérons autour d'événements réguliers.*** Ces rencontres sont essentielles, car elles permettent de mettre en lumière les entreprises et les solutions existantes sur le territoire. Outre ce forum cybersécurité, nous organisons également d'autres événements dans l'année, comme le French Tech Connect avec la Direction Générale des Achats de l'État, ainsi qu'une journée dédiée à la défense avec le ministère des Armées."

La question du recrutement

Choisir l'IUT de Dijon n'est bien sûr pas anodin. Le recrutement est un enjeu majeur pour les entreprises de la French Tech. C'est même un défi prioritaire, poursuit Silvère Denis. ***"Nos entreprises, en forte croissance, doivent identifier de nouveaux talents pour poursuivre leur développement***. Nous avons mis en place plusieurs dispositifs, notamment School Corner, qui vise à renforcer les liens entre les écoles, les universités et les entreprises. Ce type d'événement est aussi une opportunité précieuse pour les étudiants en fin d'études, en recherche de stages, d'alternances ou même de CDI."

Auteur : Valentin Goethals
Lien : https://parolesdelus.com/actualites/au-forum-regional-cybersecurite-et-numerique-avec-silvere-denis/

DOSSIER DE PRESSE
sous embargo jusqu'au 24 janvier 2025 à 12h

Dijon, le 24 janvier 2025

Forum régional Cybersécurité et Numérique le 24 janvier 2025 à Dijon

Le CSIRT-BFC (centre régional de cybersécurité), l'Agence nationale de la sécurité des systèmes d'information et la French Tech de Bourgogne-Franche-Comté unissent leurs efforts et compétences pour aider les entreprises, établissements publics et collectivités à augmenter leur résilience face aux cybermenaces.

Près de 300 acteurs étaient rassemblés aujourd'hui à l'IUT Dijon-Auxerre-Nevers pour assister au **premier Forum régional Cybersécurité et Numérique** autour d'experts de la Bourgogne-Franche-Comté et d'autres régions venues partager leurs connaissances et rappeler les défis à relever pour contrer les cybermenaces.

L'objectif de cette rencontre était notamment de créer un moment de confiance autour de la problématique de la protection des données des entreprises, établissements publics et collectivités en rappelant que « la cybersécurité est un des principaux défis de la numérisation de la société », comme l'a souligné **Patrick MOLINOZ**, Président de l'Agence Régionale du Numérique et de l'intelligence artificielle (ARNia) qui anime le CSIRT territorial. « J'aime rappeler que l'univers numérique devrait être pensé comme le monde « physique » : il n'y a ni liberté, ni démocratie, ni croissance pour les citoyens dans le monde « physique » sans sécurité. C'est la même chose avec le numérique. Il faut donc protéger les données collectées et les systèmes qui les traitent pour permettre le fonctionnement normal et sain, de leur activité. »

L'évènement de ce 24 janvier, co-organisé par le CSIRT Bourgogne-Franche-Comté, l' Agence nationale de la sécurité des systèmes d'information (ANSSI) () et la French Tech Bourgogne-Franche-Comté, a permis aux participants de s'informer et de rencontrer (rendez-vous BtoB et espaces d'exposition) les entreprises de la filière cybersécurité venues présenter leurs savoir-faire et offres de services.

« À l'heure où les attaquants se saisissent de toutes les opportunités, notamment pour mener des attaques à des fins d'extorsion financière, les entreprises, les établissements publics et les collectivités doivent impérativement hisser leur niveau de cybersécurité » a précisé **Véronique BRUNET**, déléguée de l'ANSSI en Bourgogne-Franche-Comté.

« Dans un contexte où les cyberattaques se multiplient et touchent tous les secteurs, ce forum constitue une opportunité essentielle pour renforcer la collaboration entre acteurs économiques, collectivités, fournisseurs de solutions en cybersécurité et start-up innovantes locales » a déclaré **Silvère DENIS**, Directeur délégué de la French Tech Bourgogne-Franche-Comté, lors de son allocution.

Hausse de 61% des sollicitations en 1 an : la mission du CSIRT territorial reste indispensable

Le Forum a été l'occasion pour le CSIRT Bourgogne-Franche-Comté, par la voix de son responsable, **Sébastien MOREY**, de dresser le bilan des actions du centre régional de cybersécurité menées depuis 2023 pour sensibiliser les acteurs publics comme privés – nul n'est à l'abri a-t-il alerté - à la nécessité d'anticiper les cyberattaques qui ne cessent de progresser, touchant toutes les entités publiques et privées quelle qu'en soit la taille :

« N'attendez pas d'être attaqué et de subir de graves préjudices pour nous contacter. Le CSIRT-BFC n'est pas uniquement le 15 de la cybersécurité, c'est aussi votre allié au quotidien (numéro gratuit accessible 24/24, 7/7) pour vous aider à protéger votre système d'information contre les cyberattaques, détecter les menaces dès leur apparition et réduire l'impact et la durée entre le piratage informatique et le rétablissement normal de votre activité ».

Les chiffres du bilan de l'année 2024 et la progression par rapport à 2023 suffisent à eux-mêmes pour redire la nécessité de l'action du centre régional de cybersécurité créé en 2022 grâce au financement de l'ANSSI :

➜ **404 sollicitations reçues par le CSIRT en 2024** contre 250 en 2023 soit **61% d'augmentation**. Ces 404 sollicitations correspondent à 4621 entités alertées ou impactées, une sollicitation du CSIRT pouvant être faite pour plusieurs établissements (les filiales d'une entreprise par exemple) :

- 40% sont des demandes d'information, **44% des incidents** et 16% des alertes (actions de prévention à destination des bénéficiaires, par exemple détection de vulnérabilités).
- **47% sont des communes et des communautés urbaines, d'agglomération et de communes**, 18% des établissements publics et 20% des entreprises (TPE, PME, ETI).
- les sollicitations les plus fréquentes concernent la fraude bancaire, les faux sites marchands, les rançongiciels et l'hameçonnage (phishing).

Concernant l'état de la menace en France voir à la fin de ce communiqué quelques éléments du panorama établi en 2024 par l'association InterCERT France dont fait partie le CSIRT-BFC depuis février 2024.

L'InterCERT France est une association loi 1901 qui constitue la première communauté de CSIRT en France.
Son objectif est de renforcer la capacité de chaque membre à détecter et à répondre aux incidents de sécurité impactant son périmètre. L'échange d'expérience et le partage d'informations concourent ainsi à la réalisation de cet objectif.
Le CSIRT-BFC a intégré l'InterCERT France dans des objectifs de coopération et de renforcement de sa capacité à détecter et à répondre à ses bénéficiaires.

« Le constat est que le Centre régional de cybersécurité est mieux connu aujourd'hui et les entreprises le sollicitent de plus en plus depuis 2024 », explique **Sébastien MOREY**. Au-delà de la réponse aux incidents, le CSIRT-BFC joue plusieurs rôles : la sensibilisation, les alertes comme des détections de vulnérabilités et l'animation de la filière à l'instar de ce Forum Cybersécurité et Numérique. » L'occasion de rappeler les quatre grandes missions du CSIRT de Bourgogne-Franche-Comté à destination des établissements publics, collectivités territoriales, PME /ETI et associations :

➜ REMEDIER : via un numéro unique régional [0970 609 909], le CSIRT-BFC prend en charge la demande des acteurs régionaux victimes d'une cyberattaque en les orientant vers des prestataires pour la remédiation, vers les forces de l'ordre (Gendarmerie, Police) pour le dépôt de plainte, vers la CNIL en cas de violation de données à caractère personnel et vers l'ANSSI pour le suivi de l'incidentologie.

➜ ALERTER lorsque des vulnérabilités sont détectées, sur la fin des supports logiciels, sur les fuites de données. Actuellement le CSIRT supervise **2200 entités en effectuant 2 millions de scans/an**. Quant aux fuites de données, grâce au service baptisé cyberleaks (soumis au consentement du bénéficiaire), **il analyse plus de 5000 bases de fuites sur le darkweb.**

➜ SENSIBILISER les acteurs de la région sur les thématiques de la cybersécurité (menaces, risques, comment s'en protéger, bonnes pratiques) via l'information, les rencontres de la filière, des webinaires, le cybermois en octobre.

- En 2024 le CSIRT Bourgogne-Franche-Comté a réalisé **plus de 45 actions de sensibilisation et d'information** (37 de sensibilisation et 8 webinaires). La sensibilisation est constante via des articles en accès libre sur le site web (https://www.csirt-bfc.fr/) qui reçoit 40.000 visites/an et la diffusion d'informations via Linkedin.
- Il a développé plusieurs outils gratuits : analyse de courriels douteux, fin de supports des logiciels, test de la robustesse des mots de passe.

➜ ANIMER : Forum régional annuel, rencontres et **annuaire des prestataires en cybersécurité en BFC** https://www.csirt-bfc.fr/cyber-en-bfc/ : référencement de 50 sociétés par domaine d'intervention, qualification (ANSSI, Expert Cyber, ISO…), zone géographique d'intervention, horaires d'ouverture…

En 2025 le CSIRT-BFC continuera à développer des nouveaux services dans le but d'aider ses bénéficiaires à avoir une première vision de leurs systèmes d'information. Des échanges sont prévus avec des acteurs du monde de l'entreprise comme les organisations syndicales ou les têtes de filières.
Le CSIRT-BFC travaillera à la montée en compétence des entreprises numériques de la région en les incitant à obtenir des certifications, qualifications ou labels. Par ailleurs, il continuera d'échanger avec l'enseignement supérieur (universités, écoles) qui forme les futurs experts dans le domaine de la cybersécurité.

Une collaboration renforcée entre le CSIRT et les adhérents de la French Tech en Bourgogne-Franche-Comté

« Les entreprises de la French Tech BFC sont parfaitement positionnées pour offrir des réponses fiables et efficaces aux défis croissants de cybersécurité auxquels font face les entreprises et les collectivités de notre territoire, souligne **Silvère DENIS**, Directeur délégué de la French Tech BFC. En collaboration avec le CSIRT Bourgogne-Franche-Comté, nous avons

notamment permis la création d'un annuaire régional des prestataires en cybersécurité, regroupant 50 sociétés qualifiées pour accompagner les acteurs locaux dans leur montée en résilience face aux cybermenaces. »

La French Tech Bourgogne-Franche-Comté abordera les événements clés 2025 pour accompagner ses adhérents notamment dans leur développement commercial. Tout au long de l'année, les adhérents de la French Tech BFC pourront participer à des moments d'échange dont Le French Tech Connect, un événement incontournable pour les entreprises numériques de se connecter avec les acteurs économiques et les administrations publiques.
Organisé dans le cadre du programme « Je Choisis la French Tech », cette initiative entend mettre davantage les innovations de la French Tech au service des grandes transformations du pays. Il s'agit d'encourager les institutions et les entreprises du territoire à choisir les solutions de la French Tech. L'objectif est de doubler la commande publique et les achats des grands groupes auprès des start-up, des entreprises innovantes et numériques françaises.

Quelques chiffres sur l'état de la menace en France en 2024 (source : association InterCERT France)

- Les attaques sont opportunistes dans 75% des cas, c'est-à-dire qu'elles ne visaient pas spécifiquement l'entité attaquée. Il s'agit de campagnes menées sur un très grand nombre d'entités et qui touchent leurs cibles quand celles-ci sont vulnérables.
- L'argent est la principale motivation des attaques.
- Le chiffrement de données est assez rare mais il est souvent accompagné d'une exfiltration des données. Cela permet à l'attaquant d'avoir deux arguments pour le paiement d'une rançon : la clé de déchiffrement des données et la non-divulgation.
- Certains domaines comme la défense ou l'aérospatial sont victimes de cyber-espionnage.
- 27 jours est le nombre moyen de jours qui s'écoule entre l'intrusion et la détection.

CSIRT Bourgogne-Franche-Comté

Soutenu par RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité — RÉGION BOURGOGNE FRANCHE COMTÉ

A propos de l'ARNia

Créée en 2008, L'ARNia (Agence Régionale du Numérique et de l'intelligence artificielle) apporte à ses 1.850 adhérents de Bourgogne-Franche-Comté les solutions quotidiennes aux évolutions/contraintes des usages numériques.
Elle propose une plateforme d'outils numériques ainsi que des prestations intellectuelles, incluant du conseil, des audits et un accompagnement personnalisé. Cette plateforme à destination des organismes publics (collectivités, syndicats, associations…) permet d'accéder à la modernisation de l'administration, au développement numérique des territoires et à l'amélioration des services publics.

A propos de la French Tech Bourgogne-Franche-Comté

La French Tech Bourgogne-Franche-Comté est un écosystème dynamique dédié à l'innovation et à l'entrepreneuriat technologique au cœur d'une région riche en savoir-faire. Représentant un réseau d'entrepreneurs, de startups, d'investisseurs et de partenaires, elle s'engage à favoriser le développement économique et numérique à l'échelle locale et nationale. Grâce à un ancrage territorial fort, la French Tech Bourgogne-Franche-Comté soutient les initiatives innovantes, encourage la collaboration entre les acteurs publics et privés, et promeut les talents qui façonnent les solutions de demain.

A propos de l'Agence nationale de la sécurité des systèmes d'information

L'ANSSI a été créée par le décret n°2009-834 du 7 juillet 2009 sous la forme d'un service à compétence nationale. L'agence est l'autorité nationale en matière de cybersécurité et de cyberdéfense. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale (SGDSN), sous l'autorité du Premier ministre.

Contacts Presse

Pour le CSIRT Bourgogne-Franche-Comté / L'ARNia :
Véronique Massé, attachée de presse, v.masse@isee-communication.fr, 06 23 92 26 35
Isabelle Provaux, Responsable Communication de l'ARNia, iprovaux@arnia-bfc.fr, 06 43 47 45 86

Pour l'Agence nationale de la sécurité des systèmes d'information (ANSSI) :
Roxane Rosell, Cheffe adjointe du bureau Médias/Relations Presse, presse@ssi.gouv.fr, 06 49 21 63 80

Pour la French Tech Bourgogne-Franche-Comté :
Silvère Denis, Directeur délégué, contact@lafrenchtechbfc.fr, 06 70 69 41 24