II

ÉVÉNEMENTS TRAITÉS PAR LES CSIRT TERRITORIAUX

A
SYNTHÈSE SUR LES ÉVÉNEMENTS TRAITÉS

En 2024, les CSIRT territoriaux ont traité 1387 événements de sécurité composés de 658 incidents et 729 signalements. Parmi ces incidents, les CSIRT territoriaux ont accompagné le traitement de 136 entités victimes de rançongiciels.

1387 ÉVÉNEMENTS DE SÉCURITÉ TRAITÉS PAR LES CSIRT TERRITORIAUX EN 2024

658 INCIDENTS TRAITÉS PAR LES CSIRT TERRITORIAUX EN 2024 DONT 136 ATTAQUES PAR RANÇONGICIEL

La taxonomie utilisée par les CSIRT territoriaux pour classer les événements de sécurité est disponible en annexe page 43. Elle précise la nature pour chaque type d'événement de sécurité c'est-à-dire si c'est un signalement ou un incident.

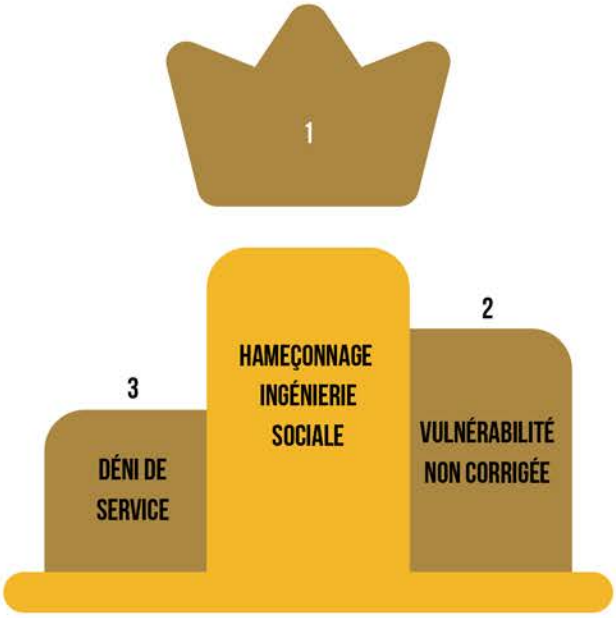
UN ÉVÉNEMENT DE SÉCURITÉ EST UN INCIDENT OU UN SIGNALEMENT PORTÉ À LA CONNAISSANCE DES CSIRT TERRITORIAUX ET QUI A DONNÉ LIEU À UN TRAITEMENT PAR LES ÉQUIPES OPÉRATIONNELLES.

UN SIGNALEMENT EST UN ÉVÉNEMENT DE SÉCURITÉ QUI CARACTÉRISE UN COMPORTEMENT ANORMAL OU INATTENDU D'UN SI POUVANT AVOIR UN CARACTÈRE MALVEILLANT OU OUVRIR LA VOIE À DES USAGES NÉFASTES À L'ENCONTRE D'UN SYSTÈME D'INFORMATION (EX. UN MESSAGE D'HAMEÇONNAGE, UNE VULNÉRABILITÉ NON CORRIGÉE SUR UN SYSTÈME EXPOSÉ SUR INTERNET, ETC.).

ENFIN, UN INCIDENT EST UN ÉVÉNEMENT DE SÉCURITÉ OÙ LES CSIRT TERRITORIAUX SONT EN MESURE DE CONFIRMER QU'UN ACTEUR MALVEILLANT A CONDUIT DES ACTIONS MALVEILLANTES AVEC SUCCÈS SUR UN SYSTÈME D'INFORMATION (EX. ATTAQUES PAR RANÇONGICIEL)

B
SIGNALEMENTS DE SÉCURITÉ

TOP 3 DES SIGNALEMENTS LES PLUS RENCONTRÉS

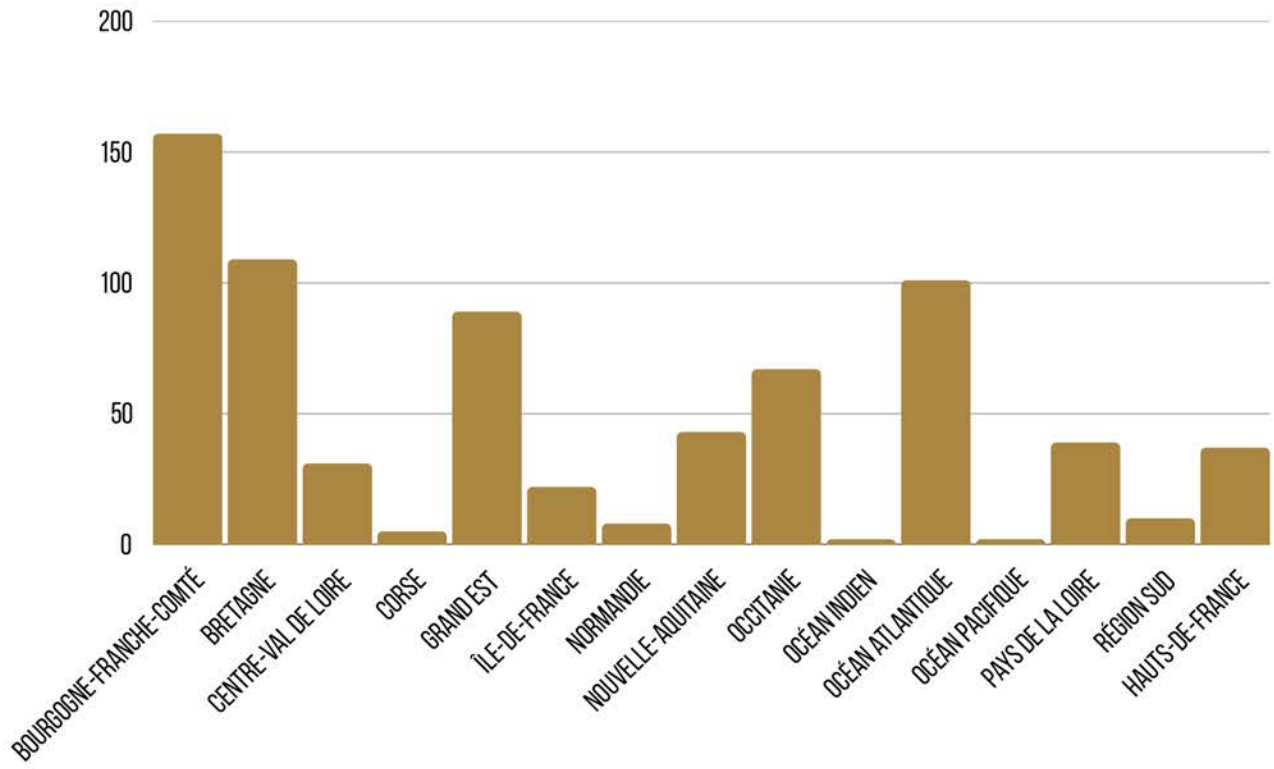


CES 3 TYPES DE SIGNALEMENTS REPRÉSENTENT PLUS DE 90% DES SIGNALEMENTS TRAITÉS PAR LES CSIRT TERRITORIAUX

Ces événements de sécurité pourraient être considérés comme moins importants. Ils sont toutefois potentiellement le germe d'incidents plus graves avec l'objectif en tant que défenseur d'arrêter un attaquant dans le déroulé de son action malveillante.

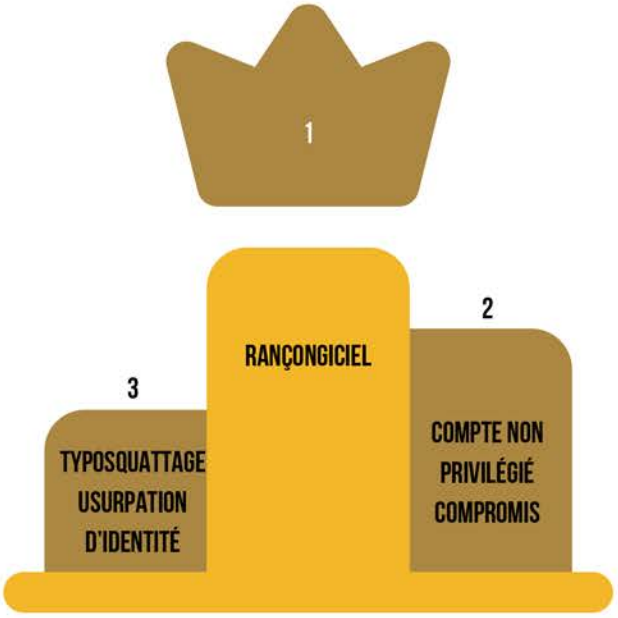
Par exemple, un compte de messagerie compromis à la suite d'un hameçonnage ou une vulnérabilité critique non corrigée sur un serveur exposé sont des vecteurs d'incidents pouvant être très graves. Leur résolution préventive diminue drastiquement les risques.

NOMBRE DE SIGNALEMENTS TRAITÉS PAR LES CSIRT TERRITORIAUX EN 2024



C
INCIDENTS DE SÉCURITÉ

TOP 3 DES INCIDENTS LES PLUS RENCONTRÉS

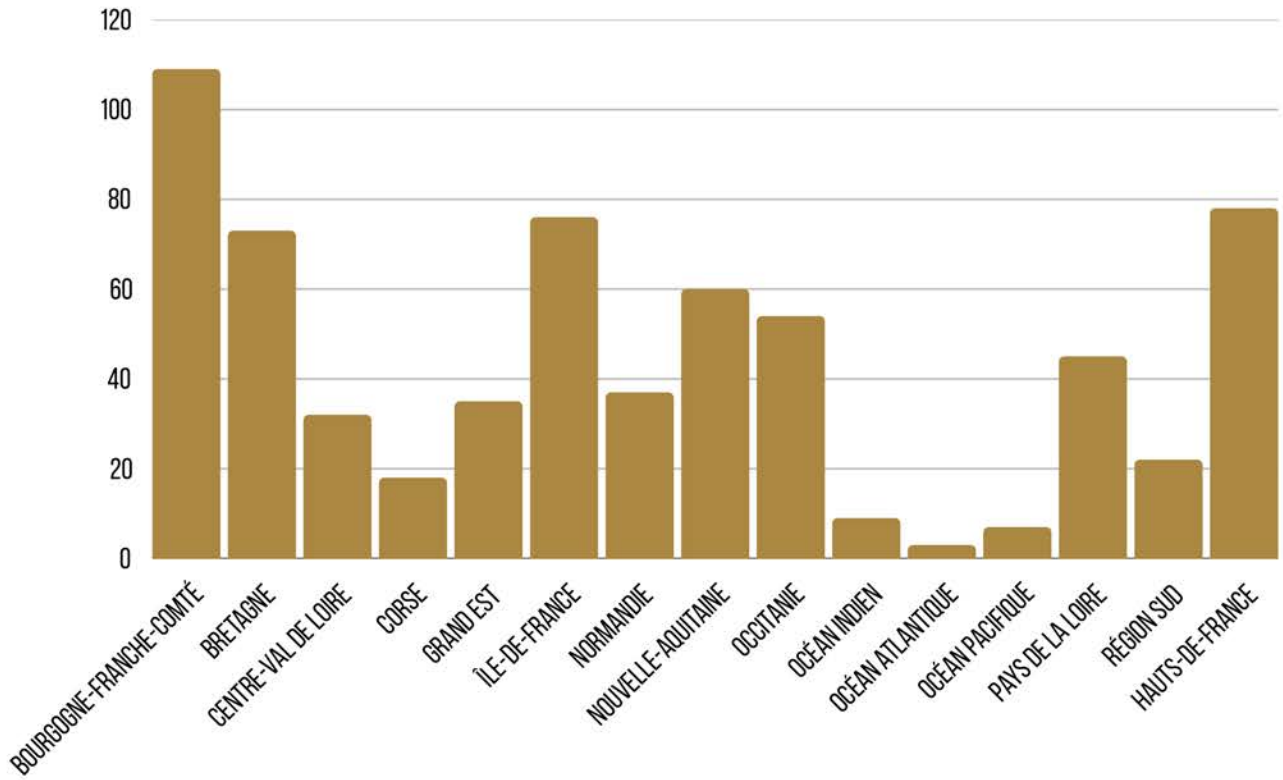


CES 3 TYPES D'INCIDENTS REPRÉSENTENT PLUS DE 50% DES INCIDENTS TRAITÉS PAR LES CSIRT TERRITORIAUX

Ces événements de sécurité matérialisent des incidents conduisant à des compromissions avérées de systèmes d'information. Il s'agit du cœur de métier des CSIRT territoriaux.

Parmi ces incidents, on distingue les incidents qui affectent très fortement le fonctionnement des SI comme les attaques par rançongiciel et des incidents de moindre envergure mais tout aussi importants à traiter.

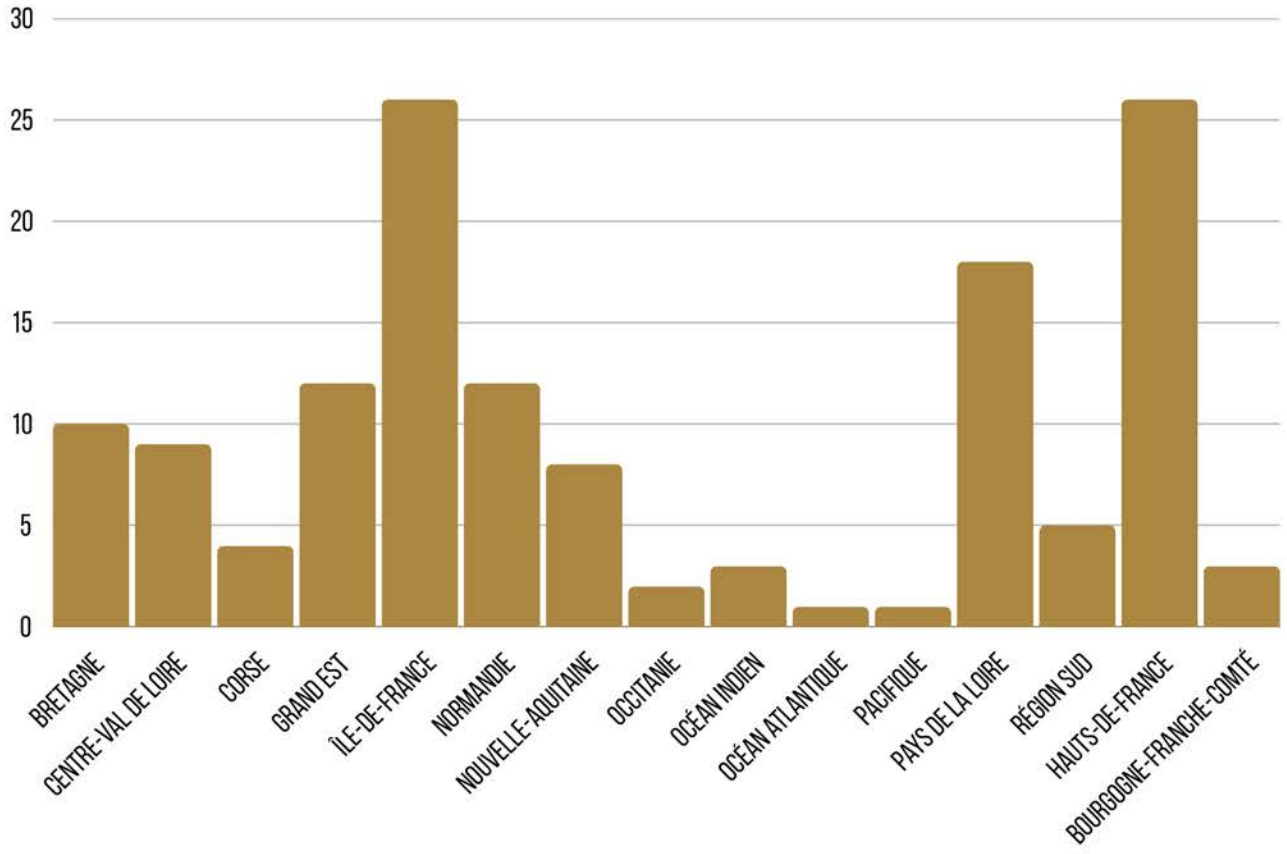
NOMBRE D'INCIDENTS TRAITÉS PAR LES CSIRT TERRITORIAUX EN 2024



D
ATTAQUES RANÇONGICIEL

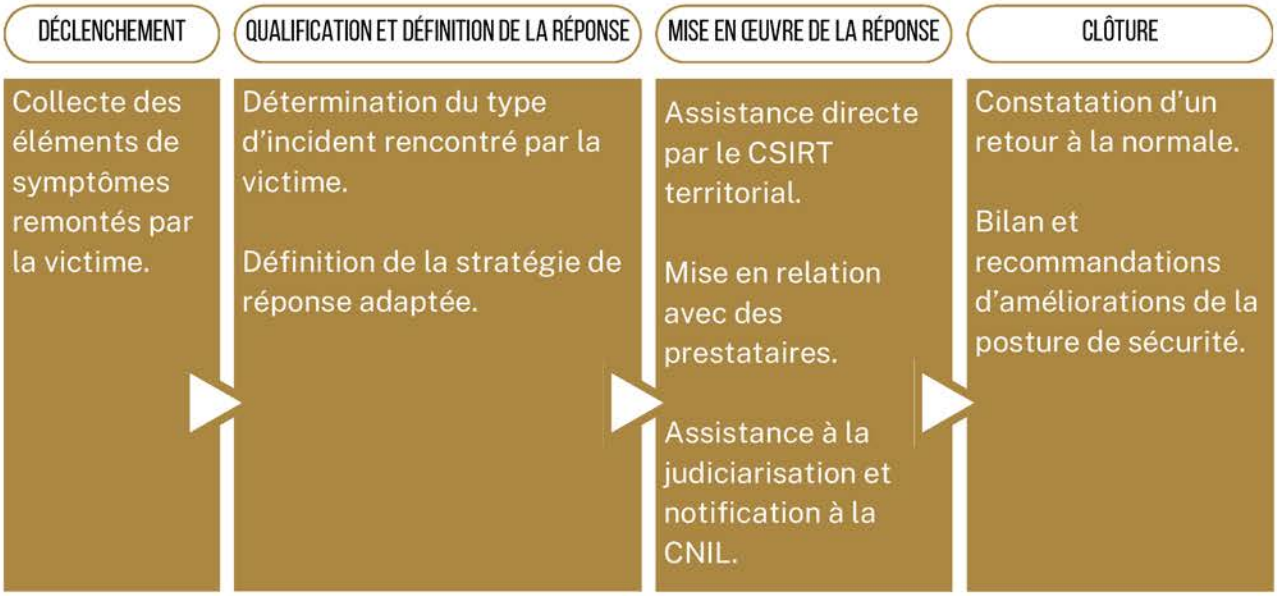
Les CSIRT territoriaux ont accompagné 136 entités victimes de rançongiciels en 2024 avec une répartition comme suit :

NOMBRE D'ATTAQUES RANÇONGICIEL TRAITÉS PAR TERRRITOIRE EN 2024



E
PROCESSUS DE TRAITEMENT DES INCIDENTS

Une assistance par un CSIRT territorial pour un incident se déroule comme suit :



Il s'agit d'un accompagnement de bout en bout de l'appel initial jusqu'à la résolution finale de l'incident. La durée de traitement ou de résolution d'un incident dépend du type d'incident rencontré. Pour les incidents les plus simples, le traitement est très rapide en 2 ou 3 jours ouvrés. Pour les incidents les plus graves, comme les rançongiciels, la durée de traitement d'un incident se compte en semaines voire en mois.

L'accompagnement des CSIRT territoriaux sur les cas de rançongiciels permet aux victimes de s'appuyer sur des tiers de confiance en capacité de les conseiller sur de nombreux aspects d'une gestion de crise cyber. Sur un aspect juridique, l'accompagnement permet aux victimes d'être informé sur leurs obligations face à un incident de sécurité. Cet aspect peut être crucial car par exemple les assurances cyber imposent le respect scrupuleux des délais légaux de 72h pour la notification auprès de la CNIL et du dépôt de plainte pour bénéficier de l'assurance.

Le niveau d'accompagnement des CSIRT territoriaux auprès des bénéficiaires est variable suivant l'origine de la sollicitation d'une part s'il s'agit d'une demande d'assistance par la victime elle-même ou s'il s'agit d'une action proactive des CSIRT territoriaux et d'autre part la maturité en cybersécurité de la victime.

Lorsqu'une entité est mentionnée dans les revendications de groupes criminels ou signalée par un partenaire, les CSIRT territoriaux peuvent être amenés à la contacter directement.

Les CSIRT territoriaux peuvent parfois faire face à des défis pour établir une relation de confiance avec les victimes lors d'un incident, notamment lorsqu'ils prennent l'initiative d'une action proactive.

L'ACCOMPAGNEMENT PAR UN CSIRT TERRITORIAL PERMET DE STRUCTURER LES ACTIONS POUR RÉPONDRE EFFICACEMENT À UN INCIDENT

Le risque le plus important face à un incident de sécurité est de réaliser une remédiation incomplète sans compréhension du mode opératoire utilisé par l'attaquant lui laissant le champ de réitérer ses actions malveillantes. Les opérations d'investigations numériques sont ainsi cruciales car elles permettent de reconstituer la chronologie de l'attaque c'est-à-dire les actions réalisées par l'attaquant sur le système d'information et le vecteur d'intrusion initial. Les actions de remédiation peuvent ainsi prendre en compte les vulnérabilités par lesquelles l'attaquant a pu s'introduire dans le système d'information en les corrigeant, assurant une protection durable de la victime.

Dans les situations où les victimes n'ont plus aucune sauvegarde, leur serveur de sauvegarde ayant lui aussi été chiffré, il existe une solution de la dernière chance encore trop souvent méconnue de la part des victimes de cyberattaques : la récupération de données par des laboratoires spécialisés. Les CSIRT territoriaux peuvent ainsi mettre en relation des victimes de cyberattaques avec ces laboratoires pour recouvrer leurs données de manière éthique sans le paiement de la rançon. Les chances de succès ne sont pas totalement garanties mais dans de nombreux cas, ces opérations de récupération fonctionnent.

Parmi les incidents largement rencontrés, l'arnaque au changement de RIB est une escroquerie courante où un fraudeur se fait passer pour un créancier légitime pour inciter la victime à effectuer un virement sur un compte bancaire frauduleux. Cette arnaque peut avoir des conséquences financières graves, car les recours auprès des banques sont souvent inefficaces si ils ne sont pas menés très rapidement au moment de la survenue de l'incident. Cette fraude est le plus souvent permise suite à la compromission d'un compte de messagerie d'un utilisateur de l'organisation. Ce type d'incident souligne l'importance de la protection des comptes de messagerie.

LORS D'UNE ATTAQUE PAR RANÇONGICIEL, LES CRIMINELS NE CHIFFRENT EN RÉALITÉ QU'UNE PETITE PARTIE DES DONNÉES, EN CIBLANT DES SECTIONS SPÉCIFIQUES DES FICHIERS. CETTE MÉTHODE LEUR PERMET DE GAGNER DU TEMPS TOUT EN RENDANT LES FICHIERS INACCESSIBLES, MÊME SI LA MAJORITÉ DES DONNÉES SONT EN RÉALITÉ INTACTES.

DES LABORATOIRES EXPERTS EN RÉCUPÉRATION DE DONNÉES PEUVENT AINSI SOUVENT RESTAURER CES FICHIERS EN SE CONCENTRANT SUR LES PARTIES NON CHIFFRÉES. CETTE APPROCHE PERMET AUX VICTIMES DE RÉCUPÉRER LEURS INFORMATIONS SANS PAYER DE RANÇON, OFFRANT AINSI UNE SOLUTION ÉTHIQUE QUI ÉVITE DE FINANCER DES ACTIVITÉS CRIMINELLES.

RANSOMWARE.LIVE

F
IMPACT DE L'ACCOMPAGNEMENT DES CSIRT TERRITORIAUX

Les coûts directs liés aux cyberattaques pour des collectivités locales de taille moyenne sont de l'ordre de 50 k€ à 60 k€ en coûts directs (prestations d'investigations et de remédiation) d'après les retours d'expériences suite à des incidents avérés. Les coûts indirects de dégradation de la qualité des services publics sont difficiles à évaluer mais bien réels (ex. interruption de la délivrance des titres d'identité, impacts sur les services de périscolaire ou de gestion des EHPAD communaux etc.) sans compter l'impact psychologique et les conséquences à plus long terme sur les équipes des collectivités locales concernées. De nombreux témoignages confirment des conséquences encore visibles d'une cyberattaque plus de 12 mois après la survenue de l'incident.

COÛT MOYEN D'UNE CYBERATTAQUE POUR UNE COLLECTIVITÉ DE TAILLE MOYENNE 50 K€ À 60 K€ EN COÛTS DIRECTS

Concernant les entreprises, les coûts sont souvent répartis souvent comme suit : environ 20% pour les coûts directs (prestations d'investigations et de remédiation) et environ 80% pour les pertes d'exploitation associées au sinistre. D'après les assureurs, le coût moyen d'une cyberattaque pour les PME / ETI est de l'ordre de 150 k€ (Source : étude LUCY, édition 2024, collection AMRAE) pouvant largement fragiliser la santé financière de ces entités. Un assureur spécialisé en cybersécurité indique que la perte moyenne pour les cas de fraude est de 55 k€ et pour les cas de rançongiciel, le coût moyen monte à plusieurs centaines de milliers d'euros.

COÛT MOYEN D'UNE CYBERATTAQUE POUR UNE PME – ETI 150 K€ COMPOSÉ DE 20% DE COÛTS DIRECTS ET DE 80% DE PERTES D'EXPLOITATION

L'intervention des CSIRT territoriaux dans l'accompagnement sur la réponse à incidents permet de limiter les impacts d'une attaque en cours pour les incidents les moins graves et les signalements, et évite qu'ils ne dégénèrent en incident plus graves (ex. compromission de compte, hameçonnage, fraude ou tentative de fraude, etc.).

Pour les incidents les plus graves, et les cas de rançongiciel en particulier, l'accompagnement apporté permet aux victimes de répondre de manière efficace et rapide à un incident limitant sérieusement les pertes d'exploitation qui constituent le coût principal des attaques.

L'action des CSIRT territoriaux a donc un impact significatif. On peut prendre par exemple le cas d'une entreprise bretonne de 300 salariés au moment de la survenue de la cyberattaque dont l'accompagnement par le CSIRT régional breton a permis de relancer ses activités 15 jours après la survenue du sinistre en partant d'une situation initiale dramatique pour la victime, avec le chiffrement complet des données et serveurs applicatifs de l'entreprise et en l'absence de sauvegarde saine.

G
COLLABORATION ET PARTAGE D'INFORMATIONS SUR LE TRAITEMENT D'INCIDENTS

Les CSIRT territoriaux collaborent au quotidien sur les signalements et incidents dont ils ont connaissance. Les échanges se déroulent sur un canal dédié de la messagerie gouvernementale Tchap. Des réunions sont également organisées de manière bi-hebdomadaire sur le pilotage des activités des CSIRT territoriaux avec le CERT-FR.

3 CSIRT territoriaux ont rejoint l'InterCERT France au cours de l'année 2024. L'InterCERT France a pour mission d'incarner la voix commune des CERT français, de promouvoir et d'accompagner leur développement, de développer les échanges opérationnels et d'animer la communauté de confiance des CERT. Une des forces de la communauté de l'InterCERT France est la collaboration opérationnelle au travers d'une plateforme d'échanges sécurisées.

JULIEN MOUSQUETON A DÉVELOPPÉ UN SITE NOMMÉ RANSOMWARE.LIVE QUI COLLECTE ET RECENSE LES REVENDICATIONS DES ATTAQUES DES GROUPES CRIMINELS DE RANÇONGICIELS SUR LEUR SITE WEB. LE CSIRT BRETON A DÉVELOPPÉ UN OUTIL D'ALERTE GRÂCE À L'API OFFERTE PAR LE SITE RANSOMWARE.LIVE CONSISTANT CONCRÈTEMENT À ENVOYER DES MAILS EN TEMPS RÉEL POUR CHAQUE PUBLICATION DES GROUPES CRIMINELS AFFECTANT UNE ENTITÉ FRANÇAISE. CES ALERTES SONT PARTAGÉES À LA COMMUNAUTÉ DE TOUS LES CSIRT TERRITORIAUX.

Ils collaborent sur des incidents de manière bilatérale ou multilatérale. Par exemple, le CSIRT Bretagne et le CSIRT Hauts de France ont collaboré en mai 2024 sur une attaque rançongiciel d'une victime prétendument bretonne revendiquée par le groupe criminel 8Base. Après qualification de l'incident, le CSIRT breton a pu identifier que la victime réelle de l'attaque était située dans les Hauts de France. Les CSIRT breton et des Hauts de France ont ensuite collaboré sur le traitement de cet incident avec les éléments recueillis initialement par le CSIRT breton au profit de la victime réelle située dans les Hauts de France.

Sur les incidents d'attaque par chaine d'approvisionnement ou les attaques en déni de service impliquant de nombreuses victimes réparties sur tout le territoire dans un temps donné, les CSIRT territoriaux se partagent en temps réel les informations. Des actions coordonnées sur un incident peuvent être montées le cas échéant.

L'ANSSI a proposé d'intégrer les CSIRT territoriaux lors de la refonte de sa plateforme téléphonique opérationnelle avec la mise en œuvre du numéro court 32 18. Un serveur vocal interactif a notamment été déployé au printemps 2024 en amont de la cérémonie d'ouverture des Jeux Olympiques de Paris 2024.

Les CSIRT territoriaux métropolitains ont été intégrés à ce déploiement, d'une part en heures ouvrables où les appelants au 32 18 peuvent être redirigés vers les CSIRT territoriaux, et d'autre part en heures non ouvrées des CSIRT territoriaux avec une redirection vers la permanence opérationnelle du CERT-FR ouvert 24 heures sur 24.

Ainsi, du 1er juillet au 31 décembre 2024, 52 appels ont été transférés en heures ouvrables du CERT-FR vers les CSIRT territoriaux métropolitains actuellement déployés sur ce service.