PRÉFET
DE LA RÉGION
NOUVELLE-AQUITAINE
Liberté
Égalité
Fraternité

RÉGION Nouvelle-Aquitaine

CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE
Nouvelle-Aquitaine

Mémo presse
Lundi 8 janvier 2024

Lundi 8 janvier 2024 : signature d'une convention de coopération pour intensifier l'action commune en matière de cybersécurité et faire de la Nouvelle-Aquitaine un territoire de confiance numérique

Étienne Guyot, préfet de la région Nouvelle-Aquitaine, **Alain Rousset**, président du Conseil régional de Nouvelle-Aquitaine**, et Mathieu Hazouard**, président du Campus régional de cybersécurité et de confiance Nouvelle-Aquitaine, **ont signé une convention de coopération ce lundi 8 janvier 2024 au Campus régional de cybersécurité et de confiance numérique Nouvelle-Aquitaine** (Campus cyber NA ci-après) **à Pessac**.

Cette convention a pour but d'**officialiser et de préciser le cadre de coopération entre les différents services de l'Etat, de la Région et du campus.**

Cette convention permettra de **partager un écosystème structuré et de confiance**, composé d'experts et de partenaires dans divers domaines, avec pour objectif la **mise en commun d'outils et le partage d'initiatives** en matière de formation, de recherche, de sensibilisation, de veille technologique, de financement et de prévention.

Elle vise à **intensifier l'action de prévention, d'anticipation et d'optimiser la prise en charge des victimes.**

Le Campus régional de cybersécurité et de confiance numérique Nouvelle-Aquitaine sur le site Ampéris à Pessac, bâtiment Colibri - Crédit : HOBO (Bordeaux)

1.3 // Contexte de la signature

Dans la lignée de la stratégie européenne de cybersécurité adoptée en décembre 2020 par la Commission européenne, la stratégie française de cybersécurité a été annoncée le 18 février 2021 par le Président de la République française. Son objectif est de garantir la **maîtrise des technologies critiques en matière de cybersécurité** par des acteurs français de confiance, et d'accélérer le développement de ce secteur économique, afin d'assurer et de renforcer de façon pérenne la sécurité des citoyens, des entreprises, des administrations et de l'ensemble des acteurs économiques. De plus, dans le cadre du plan de relance, l'Etat prévoit un **volet cybersécurité piloté par l'Agence nationale de sécurité des systèmes d'information (ANSSI)**. Si ce volet vise à profiter au plus grand nombre d'acteurs publics, une importance particulière est accordée aux collectivités territoriales et aux organismes au service du citoyen. Ainsi, des subventions sont proposées aux régions afin de favoriser la création d'équipes de proximité destinées à assister le tissu économique et social local.

Le Conseil régional de Nouvelle-Aquitaine a, pour sa part, très tôt affiché son ambition de **faire de la Nouvelle-Aquitaine un territoire de confiance numérique** : cet engagement s'est traduit par l'adoption en juillet 2020 d'une **feuille de route en matière de cybersécurité**. Le fil conducteur ayant conduit à l'élaboration et la mise en œuvre de la feuille de route régionale de cybersécurité pourrait se résumer ainsi :

« ***Pas de cybersécurité sans un climat de confiance, et pas de confiance numérique sans relations de proximité, entre les citoyens, les entreprises, les administrations et autres acteurs socio-économiques de la Nouvelle-Aquitaine*** ».

La **création d'un campus régional dédié à la cybersécurité** constitue le pilier central de l'ambition régionale en matière de cybersécurité et de confiance numérique et correspond à l'action 1 de la feuille de route. Il permettra la mise en cohérence de toutes les actions présentes et à venir et la mise en réseau des centres de ressources en cyber sécurité (CRC) territoriaux déjà initiés, suivant les recommandations de la Revue stratégique de cyberdéfense de février 2018. En fédérant les talents et les acteurs de la filière cybersécurité autour de projets innovants et collaboratifs, le Campus Cyber NA sera la vitrine à l'international de l'écosystème néo-aquitain en cybersécurité. Il aura pour vocation d'accélérer la mise en œuvre des ambitions régionales en matière de cybersécurité.

Pour assurer la pertinence de cette initiative et son ancrage fort dans le territoire, une **première brique opérationnelle** est développée, qui apporte un premier service aux entreprises et collectivités du territoire en prenant en charge la création et la mise en œuvre d'un **centre de réponse aux attaques informatiques (CSIRT pour Computer Security Incident Response Team)**. Ce service permettra la consolidation et la qualification des incidents dont il aura été saisi et la mise en relation de l'entité victime avec les organisations en charge de l'accompagner dans la résolution de l'incident (prestataires de solutions de sécurité informatique et services de police et gendarmerie).
Il fonctionne sous financement de l'État sous l'égide de l'agence nationale de la sécurité des systèmes d'information (ANSSI) à hauteur d'1M€ sur trois ans dans le cadre du Plan de relance, et du Conseil régional.

Inauguration du Campus régional de cybersécurité et de confiance numérique Nouvelle-Aquitaine le 7 juillet 2023 - Crédit Conseil régional de Nouvelle-Aquitaine - AA

Dans le cadre de sa compétence de développement économique qui la conduit à des missions de transformation et de sécurité numériques des entreprises, **la Région a conventionné** le 8 novembre 2021 pour 3 ans **avec le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN)** pour la création et l'exploitation du CSIRT en Nouvelle-Aquitaine. Le déploiement rapide de ce service et sa mise en relation avec des partenaires nationaux et européens (CERT-FR, Basque CyberSecurity Centre, par exemple) sera le garant de l'adhésion de l'ensemble de la communauté au projet de Campus, car celui-ci sera prioritairement développé sur une mission d'assistance, actuellement absente au niveau régional et revêtant un caractère d'intérêt général.

Par la suite, le Campus cyber NA pourra s'appuyer sur la connaissance de l'incidentologie régionale pour alimenter les formations proposées en son sein et s'assurer de la pertinence des projets d'innovations qu'il portera. Cette connaissance a vocation à être diffusée au sein de la filière régionale des entreprises cyber et à alimenter les centres territoriaux de ressources et les services de l'Etat, pour lesquels une connaissance précise de l'état de la menace est nécessaire.

Le positionnement territorial très fort du Campus et renforcé par ses relations opérationnelles avec des acteurs européens lui permettra également d'entraîner la communauté des entreprises néo-aquitaines dans des projets européens de grande envergure, nécessitant la plupart du temps la formation de consortium transnationaux. Le Campus Cyber NA a pour objectif de proposer un service de réponse à incident adapté à leurs contraintes aux acteurs de taille intermédiaire présents sur leur territoire. Ainsi, le CSIRT régional, service opérationnel du Campus Cyber NA, aura pour missions principales de proposer un service de réponse à incident de premier niveau aux acteurs de taille intermédiaire.

Son action consistera à :

- mettre en relation les victimes avec des prestataires régionaux et coordonner le suivi de la réponse de second niveau ;
- accompagner les victimes dans leur prise de contact avec les services judiciaires locaux et leur dépôt de plainte ;
- consolider les statistiques d'incidents cyber à l'échelle de la région.

Par ailleurs, les différents services déconcentrés de l'Etat, acteurs majeurs de la lutte contre la cybercriminalité et de la protection du patrimoine scientifique et technologique de la Nation, **ne sont que partiellement alertés des cyberattaques** survenant sur le territoire et conviennent de l'intérêt de parfaire l'accompagnement des victimes, de l'incident à sa résolution, en privilégiant le dépôt systématique de plainte quand les faits le justifient.

La **mise en place d'un équivalent cyber de « L'appel 17 »**, comme il est prévu dans la loi d'orientation et de programmation du ministère de l'Intérieur adoptée le 1er décembre 2022, **pourra donner lieu à une révision de la convention.**

2.3 // En conséquence de quoi, il a été convenu ce qui suit :

Article 1 // Objet de la convention

La Préfecture de région, le Conseil régional de Nouvelle-Aquitaine et le Campus cyber NA conviennent qu'il est de leur intérêt mutuel de **coopérer en matière de lutte contre la cybercriminalité**. L'objectif majeur de cette coopération est de **contribuer ensemble à accroître la sécurité numérique** du territoire régional, par **des actions concertées, un partage d'expérience et une montée en compétences mutuelle des parties.**

Cette coopération prend principalement la forme d'échange d'information entre les services préfectoraux et le Campus cyber NA, de partage de règles communes d'intervention et d'appui mutuel en matière de formation et de sensibilisation, sans que ces domaines soient exhaustifs.

La présente convention a pour objet de définir les modalités et les conditions par lesquelles la Préfecture de région, le Conseil régional et le Campus Cyber NA s'accordent sur le principe de cette coopération.

Article 2 // Mise en œuvre du dispositif

Article 2.1. - Interconnexion entre les parties

Les parties prenantes se transmettent mutuellement, en annexe à la présente, l'identité et/ou la fonction, ainsi que les **coordonnées téléphoniques et adresses de courrier électronique des points de contacts privilégiés** de chacune des parties chargés de réaliser les actions de coopération.

Chaque partie **notifiera à l'autre tout changement de coordonnées** de ces points de contact.

Article 2.2. - Schéma du dispositif

En tant que de besoin, les parties s'engagent à **répondre au mieux aux sollicitations entrant dans le cadre de la présente**. A cet effet, un lien direct peut être établi entre les parties dans les domaines qui relèvent de leurs compétences respectives.

La nature des faits justifiant l'activation de ce lien direct sera précisée par les parties au fur et à mesure de la présente collaboration, notamment lors des réunions de coordination tenues selon les modalités de l'article 4 des présentes.

Article 2.3. - Échanges d'informations

1/2. Échanges d'informations générales

Dans le cadre de la **veille générale** (sources ouvertes, retour d'expérience, partenariats, analyses de phénomènes…), les parties peuvent **échanger mutuellement** leurs connaissances dans le domaine de la cybersécurité et de la cybercriminalité, de manière générale ou directement en lien avec le territoire.

Ils pourront également partager des informations sur les expérimentations, les projets de recherche et de développement, les modifications réglementaires et législatives aux fins d'une meilleure connaissance de l'environnement de la cybersécurité, que ce soit au niveau régional, national ou européen.

Les services de l'État veilleront à informer le Campus Cyber NA des procédures de protection de la preuve numérique afin que ce dernier puisse les préconiser systématiquement en première intention dans le cas où les victimes de cyberattaque viendraient à entre en contact avec lui en tout premier lieu.

2/2. Échanges d'information lors d'un incident
De manière générale, le Campus Cyber NA peut être détenteur d'informations relatives à des attaques informatiques susceptibles d'avoir un impact important sur la sécurité collective et le maintien de l'ordre public, soit en raison de leur fréquence, soit en raison du territoire ou du secteur d'activité concerné. A ce titre, le Campus Cyber NA peut solliciter les conseils des services de l'État compétents, dans le respect du cadre juridique actuellement en vigueur, et notamment le Règlement général sur la protection des données (RGPD), et transmet les informations utiles à la maîtrise de la menace et la protection des victimes.

Le premier contact avec la victime d'une attaque cyber, qu'il soit établi auprès du Campus cyber NA ou auprès des forces de sécurité intérieure, permettra de diffuser les conseils d'urgence quant aux mesures nécessaires pour la préservation de la preuve numérique, et une première sensibilisation sur l'éventuelle judiciarisation de sa déclaration, si elle le souhaite, dans le cadre d'un dépôt de plainte.

Le Campus cyber NA informe les victimes qui s'adressent à lui de l'intérêt individuel et collectif du dépôt de plainte et les en informe des modalités. Dans le cadre de l'application du RGPD, le Campus cyber NA demandera systématiquement à la victime son consentement, en préalable à la transmission de l'intégralité des informations aux services de l'État. En cas de refus, les informations personnelles transmises seront pseudonymisées afin de permettre leur transmission d'une part, et une levée ultérieure de l'anonymat en cas de changement d'avis ou de dépôt de plainte

Réciproquement, lorsqu'un acte de cyber-malveillance est déclaré aux forces de sécurité intérieure, la victime est orientée vers les interlocuteurs du Campus Cyber NA, pour coordonner l'accompagnement et l'accès aux acteurs de la remédiation, prestataires labellisés au plan national par l'ANSSI et Cybermalveillance.

Le site du CSIRT du Campus Cyber NA fait apparaître deux schémas distincts de déclaration des incidents, en heures ouvrées et non ouvrées, selon le modèle suivant :

Le CSIRT traite sur le plan technique les incidents de cybersécurité concernant les organisations de Nouvelle-Aquitaine notamment en apportant une réponse technique aux victimes de cyber attaque.

Le CSIRT n'est pas un service de justice ou de police recevant des plaintes.

En dehors des heures ouvrées ou pour contacter les forces de l'ordre (7j/7, 24h/24), il est conseillé de composer le 17 ou contacter l'adresse cybermenaces-bordeaux@interieur.gouv.fr

Cf. un exemple de fiche de signalement en annexe ci-après.

Article 2.4. - Appui mutuel en matière de formation

Aux fins de **poursuivre la montée en compétence mutuelle des deux parties**, il est convenu que les parties s'apportent un appui en matière de formation. Cet appui peut prendre la forme d'invitations des spécialistes des services de l'État à intervenir lors de formations spécifiques. Parallèlement, le Campus Cyber NA peut proposer des formations permettant de consolider les connaissances et compétences desdits spécialistes.

Dès lors que les services de l'État sont sollicités par un tiers du territoire régional pour des avis relatifs à la cybersécurité, ils proposent au requérant de se mettre en relation avec le Campus Cyber NA, afin que ce dernier puisse apporter la réponse la plus adaptée en termes de formation ou de sensibilisation.

Article 2.5. - Entraînement et exercices

Dans le cadre de l'organisation et la **conduite d'exercice de gestion de crise cyber**, le Campus Cyber NA peut, en tant qu'organisateur ou contributeur, proposer, sans engagement de leur part, la participation des services de l'État, selon des modalités cohérentes avec le niveau et les objectifs de ces exercices (observation, conseil, participation active…).

Article 2.6. - Crise majeure

Dans le cadre de la gestion d'une crise majeure d'origine cyber, les **équipes du Campus cyber NA** pourront être associés à la coordination de l'action régionale **en lien avec l'ANSSI**, Agence nationale de sécurité des systèmes d'informations et rendront compte à la Préfecture de région.

Article 3 // Dispositions financières

La présente convention est établie à titre gratuit. **Chacune des parties supporte ses propres coûts**, qui pourraient éventuellement naître de l'exécution de la présente convention.

Article 4 // Pilotage et évaluation de la coopération

Les parties pourront échanger en tant que de besoin de manière collaborative afin d'identifier et de discriminer de manière objective l'ensemble des difficultés rencontrées par chacune d'entre elles dans l'exécution de la présente convention.

Cette convention donnera lieu à une réunion annuelle dans l'objectif de réaliser un **bilan** et de dresser les perspectives de la coopération entre les parties. Une réunion de coordination sera également organisée chaque semestre afin d'examiner les éventuelles difficultés et/ou bonnes pratiques de la coopération entre les parties, et de proposer les ajustements nécessaires. Lors de cette réunion de coordination semestrielle, les parties pourront inviter à participer des intervenants représentant les membres de l'association du Campus Cyber NA et les services de l'Etat compétents en matière de cybersécurité.

Article 5 // Confidentialité et communication

Les informations recueillies par le Campus Cyber NA auprès des victimes ou d'autres parties, peuvent présenter un caractère sensible qui nécessite la mise en place de mesures spécifiques de protection et une attention particulière lors des traitements effectués.

Certaines informations échangées dans le cadre de la présente convention peuvent recouvrir un caractère confidentiel et seront appelées « **informations confidentielles** » ci-après. Sans que l'énumération ci-après ne soit limitative :

(i) toute information écrite ou verbale quel qu'en soit le support, la forme ou la nature, concernant notamment ou des éléments relatifs aux marchés, clients, accords, actifs, procédures, marketing ou de nature technique, opérationnelle, industrielle, environnementale, scientifique, administrative, comptable, commerciale, économique, concurrentielle, sociale, managériale, organisationnelle, financière, fiscale, juridique et judiciaire, et relative directement ou indirectement à une partie et/ou ses sociétés affiliées/unités dont l'autre partie aurait connaissance dans le cadre de la présente convention ;

(ii) les travaux, études, rapports, synthèses, expertises, avis, opinions, correspondances, organigrammes, listes, savoir- faire ou tous autres documents de quelque forme, nature ou provenance que ce soit, qui font référence ou résultent des informations confidentielles définies au paragraphe (i) ci-dessus.

Chaque partie s'engage à tenir confidentielles les informations qu'elle recevra des autres parties et/ou de ses sociétés affiliées/unités, et services de l'Etat consultés, et notamment à ne pas divulguer ces informations à un tiers quelconque, autre que ses employés ou intervenants ayant besoin de les connaître, et de ne les utiliser qu'à l'effet d'exercer ses droits et de remplir ses obligations aux termes de la présente convention.

Nonobstant ce qui précède, l'obligation de confidentialité susvisée ne s'appliquera pas aux informations qui :
(i) seraient tombées ou tomberaient dans le domaine public indépendamment de la faute de la partie les ayant reçues ;
(ii) seraient développées à titre indépendant par la partie destinataire ;
(iii) seraient connues par la partie destinataire avant que la partie divulgatrice ne les lui communique ;
(iv) seraient légitimement reçues d'un tiers non soumis à une obligation de confidentialité ;
(v) seraient légitimement portées à la connaissance de la partie destinataire en l'absence d'une obligation de confidentialité ou d'un manquement à la présente convention ;
(vi) devraient être divulguées en vertu de la loi ou sur ordre d'une autorité publique, auquel cas elles ne devront être divulguées que dans la mesure requise et après en avoir prévenu par écrit l'autre partie.

Les obligations des parties à l'égard des informations confidentielles demeureront en vigueur pendant toute la durée de la convention et pendant une période de 5 ans après son expiration ou résiliation.

La partie destinataire devra restituer toutes les copies des documents et supports contenant des informations confidentielles, dès la fin de la convention, quelle qu'en soit la cause.

Chaque partie s'engage à faire respecter les obligations au titre de la présente convention par son personnel, ses intervenants ou tiers qui pourraient intervenir à quelque titre que ce soit dans le cadre de la convention.

Chaque partie reconnaît que seuls les employés, sociétés affiliées et contractants ayant besoin de connaître les informations confidentielles y auront accès, sous réserve que ces personnes aient accepté par écrit de respecter des obligations de confidentialité au moins équivalentes à celles exposées dans la présente convention.

Si une partie divulgue ou utilise des informations confidentielles en violation de la présente convention, l'autre partie pourra, nonobstant tout autre recours dont elle bénéficie, solliciter des mesures conservatoires afin d'interdire ces actions.

Aucune partie ne pourra faire mention ou usage du nom, de la dénomination, des marques et logos ou autres appellations, commerciales ou non, de l'autre partie, sans accord préalable et écrit de cette dernière. Les parties reconnaissent que la remise du logo de l'autre partie ne lui confère aucun droit de propriété sur ce logo et tout élément d'identification.

Pendant la durée de la présente convention, chacune des parties est autorisée à communiquer sur la présente convention ainsi que sur les actions entreprises dans le cadre de la présente convention.

Article 6 // Traitement des données à caractère personnel

Afin d'assurer le respect du Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre de circulation de ces données (« RGPD »), les parties s'engagent à respecter les dispositions applicables en matière de données personnelles dans le cadre de l'exécution de la présente convention.

Dans le cadre de l'exécution de cette convention, chaque partie doit être qualifiée de responsable de traitement indépendant de l'autre partie. A ce titre, chaque partie s'engage à traiter les données personnelles en conformité avec le RGPD et autres législations applicables, notamment en assurant la protection des droits des personnes concernées, en garantissant la sécurité et la confidentialité des données personnelles traitées, notamment par la mise en place de mesures internes organisationnelles et de sécurité et en assurant la licéité du traitement.

En tant que responsable de traitement indépendant, chaque partie restera intégralement et individuellement responsable des traitements des données personnelles qu'elle entreprend en vertu de cette convention, et en particulier à l'égard de toute demande d'indemnisation introduite par une personne qui a subi un préjudice matériel ou moral du fait d'une violation de la réglementation applicable.

Dans l'hypothèse où une partie serait amenée à traiter des données personnelles pour le compte de l'autre partie dans le cadre de la présente convention, elle l'en informera promptement. A cet égard, les parties s'approcheront en vue de compléter la présente convention afin que les traitements des données personnelles réalisés.

Article 7 // Responsabilité - Assurances

Chaque partie à la convention est responsable (a) des actions et omissions propres à son activité effectuées sous son contrôle et (b) du non-respect de la convention.

En conséquence, chaque partie est tenue de réparer, selon les règles de droit commun, les dommages causés à l'autre partie et aux tiers qui lui sont imputables.

Dans l'hypothèse où les intervenants d'une partie seraient amenés à se rendre dans les locaux de l'autre partie, cette partie se porte forte du respect par ses intervenants des règles en matière d'hygiène et de sécurité et le règlement intérieur applicables dans lesdits locaux.

Article 8 // Résiliation de la convention - Cas de force majeure

Chaque partie pourra résilier la convention en cas de manquement aux obligations contractuelles de l'autre partie, sous réserve d'une mise en demeure préalable restée infructueuse pendant une durée de 10 jours.

Aucune des parties ne sera responsable, ni ne sera considérée comme n'ayant pas respecté les dispositions de la convention, en cas de défaut d'exécution de ses obligations issues de la présente convention dû à un événement de force majeure, tel que ce terme est défini à l'art. 1218 du code civil. Dans une telle hypothèse, les parties conviennent de se rencontrer et de faire leur possible pour minimiser les conséquences de l'événement de la force majeure. Dès que l'empêchement dû à la force majeure cesserait, la partie affectée par un événement de force majeure reprendra l'exécution de ses obligations pour le reste du terme de la convention.

Article 9 // Droit applicable et litiges

La convention est régie par le droit français.

En cas de litige relatif à l'interprétation ou à l'exécution de la convention, les parties s'obligent à se rapprocher afin de parvenir à sa résolution amiable. Au cas où les parties ne parviendraient pas à trouver une solution amiable dans un délai de 30 jours, tout litige pouvant survenir à l'occasion de l'interprétation et/ou de l'exécution de la présente convention devra être soumis aux tribunaux compétents.

Article 10 // Durée de la convention - Avenants - Intégralité de l'accord

La convention entre **en vigueur le jour de sa signature** et est conclue pour **une durée initiale de 5 ans**, **renouvelable par tacite reconduction.**

Dans le cadre des réunions de coordination, les parties peuvent proposer des modifications de la présente convention.

Toute modification de l'une ou l'autre des clauses de la convention (hors annexe 1) devra faire l'objet d'un avenant écrit signé par les représentants dûment autorisés des parties.

La convention exprime l'intégralité de l'accord intervenu entre les parties. Elle annule et remplace tout accord ou contrat passé antérieurement, et tout autre acte de toute nature échangé à ce propos, qu'il ait été simplement soumis à l'attention de l'autre partie ou signé par les deux parties.

La convention contient 8 feuillets auxquels s’ajoutent deux annexes annexe. Elle est établie en trois exemplaires signés par les parties.

3.3 // Tendances des cybermenaces

Une cybermenace est un risque d'attaque de systèmes informatiques sur les infrastructures d'une compagnie, d'un État, d'une organisation privés ou publics. de son ou de ses systèmes d'information. Qu'ils soient isolés ou en réseaux et connectés ou non, les équipements visés peuvent être des ordinateurs, des serveurs, des imprimantes, des smartphones, des tablettes ou autre.

Quelles sont les principales motivations des attaquants ?

Les motivations des attaquants sont multiples. Les cyberattaques peuvent être catégorisées selon leurs finalités : la recherche de gains financiers, l'espionnage et la déstabilisation. Le Cert-Fr traite et porte une attention particulière à l'ensemble de ces catégories de menaces, puisqu'elles sont susceptibles d'affecter ses bénéficiaires des secteurs publics et privés, et plus généralement les intérêts fondamentaux de la Nation.

L'appât du gain
Les attaques à but lucratif visent à générer un gain financier de façon directe ou indirecte. Elles sont le plus souvent réalisées par des groupes de cybercriminels organisés. La cybercriminalité affecte un large panel d'entités qui se voient ciblées souvent de manière opportuniste par les attaquants. De par ses effets systémiques sur la société et en particulier lorsqu'elle porte atteinte aux intérêts de la Nation, la cybercriminalité fait l'objet d'un traitement par l'ANSSI.

Le pré-positionnement stratégique
Après être parvenu à infiltrer un système d'information, l'attaquant peut décider de s'y installer. C'est ce que l'on appelle le pré-positionnement. Généralement, cela précède une attaque de longue durée dont la finalité n'est pas clairement établie. Ce pré-positionnement peut permettre à l'attaquant de conduire dans un second temps des actions de sabotage ou d'espionnage.

L'espionnage
Les cyberattaques ayant une finalité de renseignement étatique ou économique sont le plus souvent réalisées en infiltrant les systèmes d'information d'une organisation ou d'un individu pour s'emparer des données qui y sont conservées et les exploiter.

L'objectif de telles opérations est de conserver un accès discret et durable au système infiltré afin de capter toute information stratégique d'intérêt. De fait, il faut parfois des années à une organisation pour s'apercevoir qu'elle a été victime d'espionnage.

Un certain nombre de secteurs industriels (armement, spatial, aéronautique, industrie pharmaceutique, énergie, etc.) ou encore certaines activités de l'État (économie, finances, affaires étrangères, défense, etc.) sont particulièrement exposés à ce type de menace.

La déstabilisation
Les opérations de déstabilisation peuvent prendre plusieurs formes.
Certaines opérations d'influence reposent sur la compromission de contenus légitimes (boîtes mails, sites internet) afin de pouvoir les utiliser lors de campagne de diffusion de fausses informations. Ces contenus peuvent être altérés volontairement et diffusés publiquement.

Pour les auteurs de ces opérations, il s'agit avant tout de modifier les perceptions d'une population ou de déstabiliser un acteur donné ou un processus démocratique.

Une cyberattaque peut également être un moyen de porter atteinte à l'image d'autrui. Si elles sont souvent le fait d'« hacktivistes », les attaques défigurant un site internet ou le saturant de connexions automatisées peuvent être commises par des concurrents, des employés mécontents, voire par des organisations étatiques afin de décrédibiliser leur cible.

Enfin, certaines cyberattaques peuvent prendre la forme d'actions de sabotage informatique qui consistent à rendre inopérant tout ou partie du système d'information (y compris les systèmes industriels) d'une organisation via une cyberattaque.

Certains attaquants cherchent à se prépositionner sur des systèmes d'informations stratégiques dans la longue durée. La finalité de ces intrusions est souvent peu claire, entre espionnage et préparation d'actions de sabotage.

Quelles sont les capacités et techniques des attaquants ?

Les attaques se limitent rarement à une seule technique et sont perpétrées par une large palette d'acteurs, de l'individu isolé aux organisations offensives étatiques.

Les acteurs cybercriminels, bien qu'animés par une recherche du meilleur ratio coût/bénéficie, peuvent parfois adopter des modes opératoires semblables à ceux d'acteurs soutenus par des gouvernements, en préparant minutieusement leurs opérations, en persistant sur les réseaux de leurs victimes pendant de longues périodes à la recherche de ressources d'intérêt et parfois en exploitant des vulnérabilités inconnues (0-Day). Par ailleurs, cette mise à disposition d'outils et services malveillants prêts à l'emploi peut profiter à d'autres types d'attaquants, notamment motivés idéologiquement tels que les hacktivistes.

Les attaquants étatiques peuvent avoir des capacités sophistiquées et développer des codes et des méthodes d'attaques très spécifiques. Ils s'inspirent également des méthodes cybercriminelles en s'appropriant des codes et outils traditionnellement utilisés par les attaquants cybercriminels tels que des rançongiciels. Pour se dissimuler, ils peuvent exploiter des outils légitimes présents sur les réseaux des victimes, échappant ainsi à la détection (selon la technique du living-off-the-land - LotL). Le développement de capacités offensives par des entreprises privées telles que NSO Group rend accessibles des capacités parfois de pointe à des acteurs n'ayant pas les moyens de les développer ou souhaitant maintenir une possibilité de déni plausible.

Afin de conduire leurs campagnes offensives, les attaquants peuvent utiliser plusieurs types d'attaques tels que :

<u>Les attaques sur la chaîne d'approvisionnement (supply chain attack) :</u>

Ce type d'attaque consiste à compromettre un tiers, comme un fournisseur de services logiciels ou un prestataire, afin de cibler la victime finale. Cette technique est éprouvée et exploitée par plusieurs acteurs étatiques et cybercriminels depuis au moins 2016. Cette méthode présente un risque de propagation rapide d'une attaque qui peut parfois concerner un secteur d'activité entier ou une zone géographique précise notamment lorsque l'attaque cible un fournisseur de logiciels largement répandus, une entreprise de service numérique (ESN) locale ou spécialisée dans un secteur d'activité particulier.

<u>Attaque par rançongiciel</u>
Les attaques de type « rançongiciel » (ransomware) ciblent tous types d'organisations, y compris les acteurs publics et les services gouvernementaux. Très répandus, les rançongiciels sont des logiciels malveillants qui chiffrent l'ensemble des données, outils et applications de la victime (fichiers, messagerie, SAP, etc.). Pour les récupérer, cette dernière se voit demander le paiement d'une rançon en échange de la clé de déchiffrement. Les cybercriminels exfiltrent parfois les données internes de leur cible avant l'attaque, afin d'augmenter leur pression en menaçant de les publier.

Attaques par point d'eau
L'attaque par point d'eau (watering hole) consiste à piéger un site internet légitime afin d'infecter les équipements informatiques des visiteurs. Elle peut aussi bien être employée contre des entreprises privées que des institutions travaillant sur des secteurs sensibles et qui disposent de systèmes informatiques hautement protégés et difficiles à attaquer.

Défiguration de sites internet
Ce type d'attaque peut viser tout type d'organisation et exploite souvent des vulnérabilités connues mais non corrigées, pour ajouter ou modifier des informations dans une page web à des fins de revendications. Ces opérations sont généralement revendiquées par des hacktivistes pour motifs politiques ou idéologiques, ou à des fins de défi technique entre attaquants.

Quels sont les profils des attaquants ?

Les auteurs de cyberattaques affichent des profils d'une grande diversité. Selon ces profils, les motivations varieront. L'ANSSI constate cependant une tendance à la collaboration entre certaines catégories d'attaquants aux objectifs proches.

États et agences de renseignement
Les États et agences de renseignements ont la capacité de réaliser une opération offensive de longue durée (ressources stables, procédures, etc.) et d'adapter leurs outils et méthodes à la typologie de la cible.

Organisations criminelles
Du fait de la prolifération des kits d'attaques facilement accessibles en ligne et d'une spécialisation de l'offre technique sur le darknet, les organisations criminelles mènent des opérations de plus en plus sophistiquées et organisées, à des fins lucratives ou de fraude.

Hacktivistes
Cette catégorie d'attaquant se distingue généralement par des attaques peu sophistiquées. L'objectif de ces individus est ainsi de véhiculer des messages et idéologies en ayant recours à différentes méthodes pour amplifier l'écho de leur action.

Entreprises spécialisées dans la vente de prestations et de services cyber-offensifs
Ces officines sont généralement dotées de capacités informatiques élevées sur le plan technique et proposent de véritables services de piratage à leurs clients. Plusieurs offres de services sont possibles : des outils clé en main, de l'expertise humaine ou encore des capacités telles que des méthodes d'exploitation de vulnérabilités 0-Day. Si ces services sont généralement réservés à des clients étatiques dans le cadre de la lutte contre le terrorisme et la criminalité organisée, ils peuvent être détournés à des fins d'espionnage stratégique et politique à l'encontre d'autres cibles telles que des journalistes, des défenseurs des droits de l'Homme et de hauts responsables ainsi que d'entreprises détenant des données à caractère personnel ou stratégiques.

Amateurs
Également appelés « script-kiddies », ces attaquants sont dotés de connaissances informatiques et motivés par une quête de reconnaissance sociale, d'amusement, de défi. Ils conduisent généralement des attaques basiques mais sont parfois à même d'utiliser les kits d'attaques proposés en ligne.

Menace interne
Cette typologie d'attaquant peut être guidée par un esprit de vengeance aigu ou un sentiment d'injustice. Il peut par exemple s'agir d'un salarié licencié ou encore d'un prestataire mécontent suite au non renouvellement d'un marché.

Source : https://cyber.gouv.fr

Le Campus cyber NA en chiffres
Le Campus cyber NA regroupe aujourd'hui 135 adhérents, représentant plus de 1 500 experts en cybersécurité.
Depuis avril 2023, le Centre régional de réponse à incident cyber (CRIC-NA), son service opérationnel, a traité **164 signalements** (2/3 entreprises, 1/3 public) dont :

- 27 défacements,
- 55 rançongiciels,
- 20 violation de données.
La moitié de ces incidents a été détecté par le Campus, lui permettant de prévenir la victime avant que les impacts ne soient irrémédiables.

Site Ampéris à Pessac - Crédit : HOBO

Annexe :

CSIRT Nouvelle-Aquitaine
FORMULAIRE DE DÉCLARATION D'UN INCIDENT DE SÉCURITÉ

1. *Type de déclaration*

Date de la déclaration :	jj /mm/aaaa	Déclaration	
		initiale	complémentaire
Nom de l'organisme effectuant la déclaration :			
Si entreprise, n° SIRET :			
Référence de la déclaration initiale fournie par le CSIRT (si connue de l'organisme)			

2. *Coordonnées de la personne effectuant la déclaration*

Nom :	Prénom :
Service :	Fonction :
Adresse postale :	Téléphone :
Adresse électronique fonctionnelle : (ex : contact@monadresse.com)	Adresse électronique :

3. Description de l'incident

Système d'information affecté :
Dénomination du système d'information :
Brève description du système d'information :

4. Incident constaté

Date à laquelle l'incident a été constaté :		jj/mm/aaaa
Date et heure estimées du début de l'incident :		jj/mm/aaaa hh : mm
Localisation des équipements du système d'in- formation affectés par l'incident :		
En cas d'attaque, état constaté ou présumé de l'attaque		activités préparatoires
		tentative d'attaque non aboutie
		attaque aboutie
Impacts sur la sécurité (constatés ou présumés)		disponibilité
		intégrité
		confidentialité
		disponibilité & intégrité
		disponibilité & confidentialité
		disponibilité & intégrité & confidentialité

Impacts sur les activités constatés ou présumés
Précisez les impacts sur les activités (exfiltration de données, destruction d'équipements, indisponibilité du système, etc.) et notamment la nature des données exfiltrées, les équipements affectés ou détruits par l'incident et les équipements visés en cas d'attaque.

Description des mesures prises et envisagées :		
Autres déclarations de l'incident (CNIL…)		
Accord pour transmission aux FSI	oui	non
Dépôt de plainte	☐ non envisagé	
	☐ envisagé	
	☐ effectué	

5. Observations complémentaires

Contacts presse :
Préfecture de la région Nouvelle-Aquitaine : Sophie Billa - 05 56 90 60 18 / pref-communication@gironde.gouv.fr

Conseil régional de Nouvelle-Aquitaine : Rachid Belhadj - 05 57 57 02 75 / presse@nouvelle-aquitaine.fr

Campus régional de cybersécurité et de confiance numérique : Guy Flament - 06 63 05 31 48 / contact@campuscyber-na.fr