Cybersécurité : un enjeu majeur

Le numérique occupe une place prépondérante dans le fonctionnement des organisations, situation qui suscite un intérêt croissant des cybercriminels dont les techniques ne cessent de s'améliorer.

Il faut savoir qu'ils s'attaquent aussi bien aux grandes entreprises qu'aux services de santé ou aux associations. Dans ce contexte, quels sont les risques pour notre réseau et comment y faire face ? Ce grand angle a pour objectif de vous livrer les clés qui vous permettront d'assurer votre cybersécurité et de vous aider à sensibiliser vos Ogec.

L'édito

Jean-François Deboudt
Président du GTSI (Groupe de Travail sur les Systèmes d'Information)

> *Paradoxalement, là où le numérique et très impliqué, les risques de fraudes ou d'attaques se multiplient*

Cybersécurité : le numérique et ses paradoxes

La cybersécurité est un sujet d'actualité permanent. Nous sommes effectivement de plus en plus plongés dans un monde "numérique", monde qui apporte du confort et du service, qui devient indispensable voire même de plus en plus indispensable dans nos vies quotidiennes. Et paradoxalement, là où le numérique est très impliqué, les risques de fraude ou d'attaques de toutes natures se multiplient. C'est donc la sécurité et la continuité de nos activités qui sont en jeu ! Dans un autre domaine digital, si les réseaux sociaux représentent un excellent outil de communication, ils sont aussi capables de générer des comportements dangereux voire criminels. Autre paradoxe lié à la consommation d'énergie : en étant omniprésent, le numérique devient très énergivore. La technologie numérique est de plus en plus pointue et de moins en moins abordable pour la plupart des utilisateurs. Encore un paradoxe qui questionne. Mais quand on analyse les principales causes des incidents de sécurité dans les entreprises, les deux premières concernent l'utilisation d'outils non qualifiés et des vulnérabilités connues non traitées. Il y a de vrais défauts technologiques "surprises", mais on observe qu'une bonne partie des causes sont identifiables. Ce constat est plutôt rassurant car il appelle à la responsabilité individuelle de chacun au bon usage du numérique. La "sobriété numérique" ou "green-IT" est une démarche dont le but est de minimiser l'impact environnemental du numérique. La proposition de l'ADEME est plus large : elle propose à chacun de "profiter du numérique tout en gardant le contrôle" et d'avoir un regard de gestion sur ses réels besoins.

ISI Day 2023

Nous vous informons qu'ISI day, la journée dédiée au numérique organisée par la Fédération nationale des Ogec aura lieu le 4 avril 2023 et aura pour thème la **sobriété numérique.** Cette journée sera exclusivement diffusée en ligne.

Règle d'or pour une sécurité informatique sans faille et efficace : ne plus se laisser surprendre !

Les récits médiatiques de cyber-attaques dont ont été victimes de nombreux organismes (entreprises, hôpitaux, services municipaux, établissements scolaires, etc.) rappellent que les malveillances informatiques sont désormais l'affaire de tous. La question n'est plus de savoir si cela va m'arriver mais quand et comment. Ce dossier spécial a été conçu pour vous aider à décrypter les enjeux d'un système d'information bien sécurisé et vous éclairer sur les principaux risques, de l'hameçonnage au rançongiciel, afin de vous permettre de contrer, par des mesures simples, des pièges de mieux en mieux élaborés. Au hit-parade des cyber-risques qui peuvent toucher les établissements scolaires, on trouve le rançongiciel (ransomware ou encore cryptolocker) qui profite de failles internes pour paralyser les systèmes informatiques.

Prise d'otage de vos données sensibles

Tout commence par un e-mail d'apparence authentique, adressé par un expéditeur à priori fiable et dont le contenu joue sur la vraisemblance et l'urgence. Par exemple, l'interruption imminente d'un service auquel vous avez souscrit (service bancaire, énergie ou abonnement...) si les informations de paiement ne sont pas mises à jour dans les plus brefs délais. C'est la stratégie de l'hameçonnage (ou phishing). Votre vigilance étant affaiblie, vous suivez un lien ou téléchargez une pièce jointe. Mais un logiciel malveillant s'active sur votre ordinateur et peut s'étendre à tout le réseau informatique pour en crypter les données et les rendre inaccessibles. Dans certains cas, des

© Adobe Stock

informations sensibles (RIB des familles, données médicales...) sont siphonnées pour être revendues via des réseaux clandestins. Les pirates exigent alors une rançon pour ne pas les dévoiler et vous trans-mettre une clé de déchiffrement. Les spécialistes conseillent de ne pas céder au chantage car rien ne vous garantit qu'ils tiendront parole, et vous pourriez même passer pour une cible facile.

Partager les mesures de prudence

Le premier enjeu est d'identifier les données dites sensibles de votre établissement et de vous assurer qu'elles sont régulièrement sauvegardées sur une durée suffisamment longue, via plusieurs copies sur

des supports différents, dont un hors ligne, pour faciliter leur récupération et la reprise d'activité en cas de piratage. Puis, face à la sophistication croissante des scénarios d'attaque, l'autre enjeu est de sensibiliser vos équipes aux bons réflexes comme celui d'identifier un message frauduleux. Enfin, votre établissement doit se doter à minima des compétences nécessaires et les renforcer en continu pour mettre en œuvre les mesures techniques incontournables de sécurisation de votre système d'information : mise à jour régulière des logiciels (systèmes d'exploitation, navigateurs internet, lecteurs PDF...), déploiement de solutions antivirus avancées, cloisonnement des réseaux privés (administratif, pédagogique...) et accès visiteurs (wifi notamment), sécurisation de vos accès à internet (pare-feu), suppression des clés USB, etc.

Encourager la culture de la cybersécurité

En cas d'attaque sur un poste, chaque utilisateur doit appliquer un protocole connu d'avance. D'où la pertinence d'élaborer une charte informatique qui détaille les règles d'utilisation du numérique, les bonnes pratiques en cas de cyber-attaque et encourage ainsi une culture de la cybersécurité. Par exemple, dans le cas d'un rançongiciel, l'ordinateur doit impérativement être déconnecté du réseau (câblé et/ou wifi) et ne pas être éteint au risque de détruire des preuves. Il faut enfin alerter le responsable informatique ou le prestataire externe.

> Les responsables informatiques déplorent le manque de fondamentaux chez des utilisateurs souvent trop confiants dans la sécurité des systèmes et persuadés que cela n'arrive qu'aux autres. Or, la cyberprudence sera une responsabilité collective en 2023.

Article rédigé par Olivier Valentin, responsable communication et animation du réseau Fédération des Ogec Ile-de-France

Éviter le pire ? C'est possible en prenant des initiatives préventives qui permettent d'assurer une meilleure sécurité

Même si les cas de cyber-attaques sont de plus en plus médiatisés et que ces agressions touchent aussi bien des entreprises du CAC 40 que des organismes de santé publique, nous avons toujours le sentiment que ces attaques n'arrivent qu'aux autres et que nous nous sentons suffisamment protégés pour les éviter. Malheureusement, ces événements arrivent aussi dans nos établissements...

Mme Germouty, cheffe d'établissement du lycée GTP-Sup partage avec nous son expérience.

À quel moment avez-vous su que votre établissement était victime d'une cyber-attaque ?

Un jour, mon collaborateur du collège, avec qui nous partageons l'infrastructure informatique, m'a contactée à mon domicile pour m'informer qu'il était avec notre responsable informatique car en voulant utiliser son ordinateur, il s'est retrouvé face à un écran noir. Nous étions en train de subir une attaque informatique de type "rançongiciel" qui avait débuté vers 4h du matin. Nous avons vite été confrontés à la problématique suivante : qui peut nous aider face à cette situation ? Nous avons eu la chance de réussir à joindre le responsable du second degré au sein de la direction diocésaine de Vendée qui connaissait une entreprise spécialisée dans la récupération de données informatiques.

Que s'est-il passé ensuite ?

La suite fut d'informer la communauté éducative quant à la situation et aux incidences qui allaient suivre : plus d'accès aux outils informatiques ni à internet. Environ 600 postes au sein du collège et du lycée étaient concernés et se ont retrouvés bloqués pendant plusieurs semaines. Seuls les postes de l'administration ont pu être remis en route avec l'aide de nos partenaires informatiques.

Avez-vous pu reprendre vos activités rapidement ?

Nos données ont été partiellement récupérées quelques semaines plus tard seulement. Nous avons mis plusieurs mois avant de pouvoir retrouver un mode de travail normal car nous avons dû revoir notre infrastructure réseau et prendre de nouvelles dispositions de sécurisation :

- Doublage des pare-feux
- Mise en place d'une sauvegarde immuable

Mme Germouty
Cheffe d'établissement du lycée GTP-Sup - UFA Notre Dame - CFP Les Abeilles

> *« Nous avons mis plusieurs mois avant de pouvoir retrouver un mode de travail normal [...]*

• Solution de protection antiphishing/antispam
• Interdiction d'utiliser des clés USB
• Restriction d'accès aux emails non professionnels via les ordinateurs de l'établissement
• Restriction d'accès à notre réseau wifi pour tous les appareils extérieurs à l'établissement (proposition d'une connexion wifi dédiée)

Qu'est-ce que cette attaque a changé dans votre manière de fonctionner ?

Six mois plus tard, nous avons pris la décision de faire un audit de notre nouvelle structure pour, à la fois sécuriser les responsables, prendre de nouvelles habitudes de travail et communiquer sur les risques

"cyber" à l'ensemble des acteurs de la communauté.

Avez-vous une idée de l'impact financier que cette attaque peut avoir sur votre Ogec ?

Nous estimons à plusieurs dizaines de milliers d'euros l'impact de cette cyberattaque. Nous n'étions pas assurés à l'époque et nous ne pouvions malheureusement plus l'être à court terme.

Avez-vous su d'où venait cette attaque ?

La société qui nous a accompagnés a pu remonter à l'origine de l'attaque qui provenait de "hackers" originaires des pays de l'Europe de l'Est. On nous a expliqué qu'ils ciblaient principalement les serveurs avec une grosse activité. Ils se sont introduits via un accès extérieur insuffisamment sécurisé.

Conlusion

Nous vous remercions infiniment pour votre précieux témoignage qui touchera l'ensemble de nos lecteurs, membres du réseau des Ogec, et les sensibilisera à la menace permanente qui planne chaque jour au-dessus de nos structures, et particulièrement celles de nos Ogec. Vous leur rappelez qu'il est plus qu'important d'agir en amont et de mettre en place des actions préventives, même si ce n'est pas toujours dans notre culture. Nous avons tendance à minimiser les risques jusqu'à ce que l'on en devienne une victime. Il est donc important d'agir aujourd'hui et de prendre les mesures nécessaires pour éviter ces types d'attaques qui se multiplient par milliers actuellement.

Les conséquences d'une cyberattaque sont lourdes et touchent tous les domaines de l'activité d'une structure. Sur le plan matériel, humain et financier, la remise en service ne se fait pas du jour au lendemain mais prend plusieurs mois, voire plusieurs années : agissez !

Témoignage de Céline Germouty, cheffe d'établissement du Lycées GTP-Sup - UFA Notre Dame - CFP Les Abeilles
Propos reccueillis et rédigés par Anthony Mortier, responsable du pôle numérique de l'Uradel

Cyberattaques : quels sont les conseils pour vous prémunir d'un piratage ?

Hameçonnage, rançongiciel et piratage de comptes constituent le top trois des attaques auprès des collectivités. Autant de techniques qu'il convient de bien comprendre et de faire connaître à tous les utilisateurs pour mieux les appréhender. Cette meilleure connaissance des risques cyber et des attaques permet de les prévenir et de former les utilisateurs aux gestes clés de sécurité.

Pour vous protéger contre le hameçonnage, soyez vigilant lorsque vous recevez des emails ou des messages provenant de personnes ou d'entreprises que vous ne connaissez pas ou qui vous demandent des informations personnelles ou financières. Ne cliquez jamais sur des liens ou des téléchargements douteux dans les emails ou les messages que vous recevez. Si vous êtes incertain, vérifiez l'adresse du site web avant de cliquer sur le lien. Utilisez un logiciel de sécurité qui inclut une protection contre le hameçonnage et qui met à jour régulièrement ses définitions de virus. Soyez attentif aux fautes d'orthographe et aux erreurs de grammaire dans les emails et les messages que vous recevez, car cela peut être un signe que le message est frauduleux. Utilisez des mots de passe forts et uniques pour chaque compte, et changez-les régulièrement. Utilisez également un gestionnaire de mots de passe pour vous aider à gérer vos mots de passe de manière sécurisée. Ne transmettez jamais vos informations personnelles ou financières par email ou sur des sites web non sécurisés. En suivant ces consignes, vous devriez être en mesure de vous protéger efficacement contre le hameçonnage et de maintenir la sécurité de vos informations sensibles.

Le hameçonnage est la cyberattaque la plus propagée, mais en quoi cela consiste-t-il ?

Le hameçonnage, également appelé *phishing*, est une technique utilisée par les cyber-criminels pour tenter de voler des informations sensibles, comme des mots de passe ou des numéros de carte de crédit, en se faisant passer pour une entreprise ou un individu de confiance.

© Adobe Stock

Article rédigé par Frédéric Hul, DSI de la Fédération nationale des Ogec

Le rançonnage, également appelé rançongiciel, est une forme de cyberattaque qui vise à verrouiller ou à rendre inaccessible votre ordinateur ou vos données, jusqu'à ce que vous payiez une rançon. Nous vous présentons ci-dessous quelques étapes que nous vous recommandons de suivre pour vous protéger contre le rançonnage : 1. Utilisez un logiciel de sécurité qui inclut une protection contre les logiciels de rançon et qui met à jour régulièrement ses définitions de virus. 2. Sauvegardez régulièrement vos données importantes, de manière à pouvoir les récupérer en cas de perte ou de corruption. 3. Soyez vigilant lorsque vous naviguez sur le web et évitez de cliquer

sur des liens ou de télécharger des fichiers de sources douteuses. 4. Ne cliquez jamais sur un lien dans un email ou un message qui vous demande de payer une rançon ou qui vous avertit qu'un problème a été détecté sur votre ordinateur. 5. Soyez attentif aux fautes d'orthographe et aux erreurs de grammaire dans les emails et les messages que vous recevez, car cela peut être un signe que le message est frauduleux. 6. Ne payez jamais la rançon demandée. Même si vous payez, il n'y a aucune garantie que vous récupériez vos données ou que le logiciel de rançon soit désinstallé de votre ordinateur. En suivant ces 6 étapes, vous devriez être en mesure de vous protéger contre le rançonnage et de maintenir la sécurité de vos données. Si vous êtes victime d'une attaque de rançonnage, il est fortement recommandé de contacter immédiatement votre fournisseur de logiciel de sécurité ou un professionnel de l'informatique pour obtenir de l'aide. **INFO CLIN D'OEIL :** cet article a été rédigé en utilisant l'application ChatGPT, qui défraye la chronique. ChatGTP est une intelligence artificielle qui dépasse les assistants personnels actuels comme Siri, Google Assistant, Amazon Alexa, etc.) car il collecte et croise des milliards de données accessibles publiquement sur Internet et les restitue au demandeur de façon pertinente et structurée. Attention toutefois, il convient de bien vérifier les réponses qu'il vous soumet, notamment sur nos sujets.

En suivant ces étapes, vous devriez être en mesure de vous protéger et de maintenir la sécurité de vos données. Si vous êtes victime d'une attaque, il est recommandé de contacter immédiatement votre fournisseur de logiciel de sécurité et votre responsable informatique.

Article rédigé par ChatGPT

Plan de reprise d'activité : une précaution indispensable pour anticiper les impacts liés à une cyberattaque

Quelle que soit la taille de votre établissement, il est nécessaire d'envisager et de mettre en place une solution de secours en cas de sinistre subi au niveau de votre infrastructure informatique. En effet, une cyberattaque ou une panne majeure peut s'avérer fatale pour votre établissement en cas de perte majeure de fichiers ou de destruction de votre matériel. Un plan de reprise d'activité vous permettra de faire face à ce type de déconvenues.

Qu'est-ce qu'un PRA (plan de reprise d'activité) ?

Un plan de reprise comprend l'ensemble des procédures et des durées d'interventions nécessaires pour redémarrer votre activité après un incident informatique majeur. Ce type de catastrophe comprend les cataclysmes naturels, les incendies (local ou chez votre hébergeur[1]), les attaques informatiques (encore plus fréquentes aujourd'hui), les vols, les défaillances technologiques... soit tout ce qui peut détruire vos données et outils informatiques et qui peut être plus ou moins prévisible. Ce plan est une sécurité pour la gestion des Ogec, mais n'est pas un plan standardisé. Chaque plan s'adapte aux besoins et aux spécificités de votre établissement. Avoir le plan idéal signifie définir avec votre prestataire informatique ou votre responsable informatique, les données les plus importantes et les dangers possibles.

Comment s'y prendre ?

Pour vous aider à prioriser les données à récupérer en cas de sinistre, le registre de traitement peut vous être utile. Mis en place en 2018 dans le cadre du

© Adobe Stock

[1] *Rappellez-vous OVH en 2021*

RGPD, il vous permet de cartographier et d'obtenir une vision détaillée de tous les traitements réalisés au sein de votre structure, de toutes les données manipulées, les différents intervenants... Vous pourrez ensuite réfléchir aux incidents possibles pour chaque support et aux actions à mener en amont pour limiter l'impact de ces incidents sur vos activités (sécuriser un local contre le vol, présence d'extincteur, sauvegardes régulières...). Enfin, le plan de reprise d'activité est constitué de la démarche générale et des étapes à suivre pour remettre en route l'activité (notamment dans le cadre d'une reprise progressive). Pour qu'il soit efficace, votre PRA doit prévoir d'identifier et d'impliquer les ressources humaines concernées (internes et externes) pour remettre sur pied votre système d'information.

L'importance des sauvegardes

La sauvegarde de vos données est la condition de réussite de votre plan de reprise d'activité. Les systèmes d'information sont de plus en plus complexes et hybrides (applications locales, services dans le Cloud), mais nous vous conseillons vivement d'effectuer en parallèle vos propres sauvegardes et ce, pour l'ensemble de vos données, y compris celles hébergées par votre prestataire ou par une solution Cloud. Aucune entreprise n'est en effet à l'abri d'un sinistre destructeur. Concernant les services hébergés dans le Cloud, il est préférable de choisir un hébergement redondant sur un autre site géographique, de telle sorte que l'autre serveur puisse prendre le relais en cas d'incident. Concernant les applications et les données locales, nous vous conseillons d'appliquer la règle du "3-2-1" qui vous permettra d'augmenter le nombre de sauvegardes que vous conservez et de diversifier les lieux où elles sont stockées.

> L'hébergement et le rythme de sauvegarde sont des éléments importants à ne pas négliger, pour vous prémunir en cas de perte de données innattendue.

Qu'est-ce que la règle du 3-2-1 ?

Cette règle stipule que vous disposez de 3 copies de données dont 2 sont stockées sur des supports différents et au moins une est stockée hors site ou sur le Cloud (ou à minima sur un bâtiment non connexe de celui hébergeant vos serveurs). Concernant le rythme des sauvegardes, il est conseillé, à minima, d'avoir une sauvegarde quotidienne pour les données dites "vivantes" (qui changent régulièrement) avec un système de roulement (hebdomadaire, mensuel, annuel). Cette politique de sauvegarde doit donc être formalisée et doit compléter votre PRA.

À noter : l'application ISI Data vous aide à répertorier votre activité numérique

ISI Data est une application accessible depuis votre espace Isidoor. Simple et intuitive, elle vous permettra de maintenir votre conformité RGPD, de détecter vos failles de sécurité et de gérer votre parc informatique. Elle vous permettra également de bien tenir à jour votre registre de traitement et d'indiquer l'état des sauvegardes pour chaque source de données identifiée ainsi que les précautions prises pour les sécuriser.

Article corédigé par Anthony Mortier, responsable du pôle numérique de l'Uradel, et Frédéric Hul, DSI de la Fédération nationale des Ogec

Cybersécurité : tous utilisateurs, tous concernés ! Comment sensibiliser pour mieux agir ?

Ces dernières années, le pays a été la cible de très nombreuses cyberattaques. Si une prise de cons-cience collective commence à s'opérer, il reste encore beaucoup à faire pour atteindre un bon niveau de sécurité et démystifier ce sujet. Obscure pour certains, anxiogène pour d'autres, la cybersécurité est en-core trop souvent perçue comme une contrainte et comme un sujet uniquement technique.

Il suffit d'une seule intrusion dans un système informatique pour entraîner la perturbation des services, voire l'arrêt total de l'activité, une atteinte à l'image et à la réputation de l'établissement scolaire, ou encore une rupture de la confiance numérique entre votre établissement et ses parties prenantes. Un seul clic sur un lien malveillant, le téléchargement d'une pièce jointe infectée ou la réutilisation d'un mot de passe tombé entre de mauvaises mains, peuvent ainsi avoir de graves conséquences. Une cyberattaque est souvent le fait d'une négligence humaine. Il suffit parfois d'une simple erreur pour rendre toute une organisation vulnérable. Si chaque membre de la communauté éducative en est conscient, alors chacun, à son niveau, peut être acteur d'une politique *cyber* et contribuer à protéger son établissement scolaire, notamment en adaptant son comportement.

Pour garantir un niveau de vigilance constant de la part de vos utilisateurs et développer une culture *cyber*, il devient nécessaire de diffuser ces recommandations via des campagnes de communication et de sensibilisation récurrentes. Divers outils ainsi que des ressources documentaires sont aujourd'hui disponibles sur le site Cybermalveillance.gouv que vous retrouverez également dans l'espace documentaire d'ISI Data. D'autre part, nous vous proposons de tester vos connaissances depuis votre espace Isidoor : dans la rubrique formation, un quiz pédagogique vous permettra d'évaluer votre niveau général de cyber-prudence. Des exercices vous permettront de vous aider à renforcer votre vigilance dans les domaines tels que la sécurité de l'information au travail, les usages et les risques liés à l'utilisation des messageries électroniques et d'Internet, la e-réputation et les réseaux sociaux, ou encore la mobilité et la sécurité à domicile. Des vidéos pédagogiques réalisées par les instances de la sécurité informatique en France (c'est-à-dire par le site de référence cybermalveillance.gouv, par l'Anssi ou encore la Cnil), viennent illustrer chaque thématique. Ces ressources vous aideront à sensibiliser vos utilisateurs et vous permettront de renforcer votre cybersécurité.

Pour bien commencer : rendez-vous dans l'espace formation d'Isidoor pour tester vos connaissances et corriger vos usages numériques. C'est un premier par vers la cyberbienveillance en vue de renforcer la cybersécurité de votre établissement.

Article rédigé par Frédéric Hul, DSI de la Fédération nationale des Ogec