Ils font la cyber en Occitanie

Entretiens avec :
Orange
Cyber'Occ
Predicta Lab…

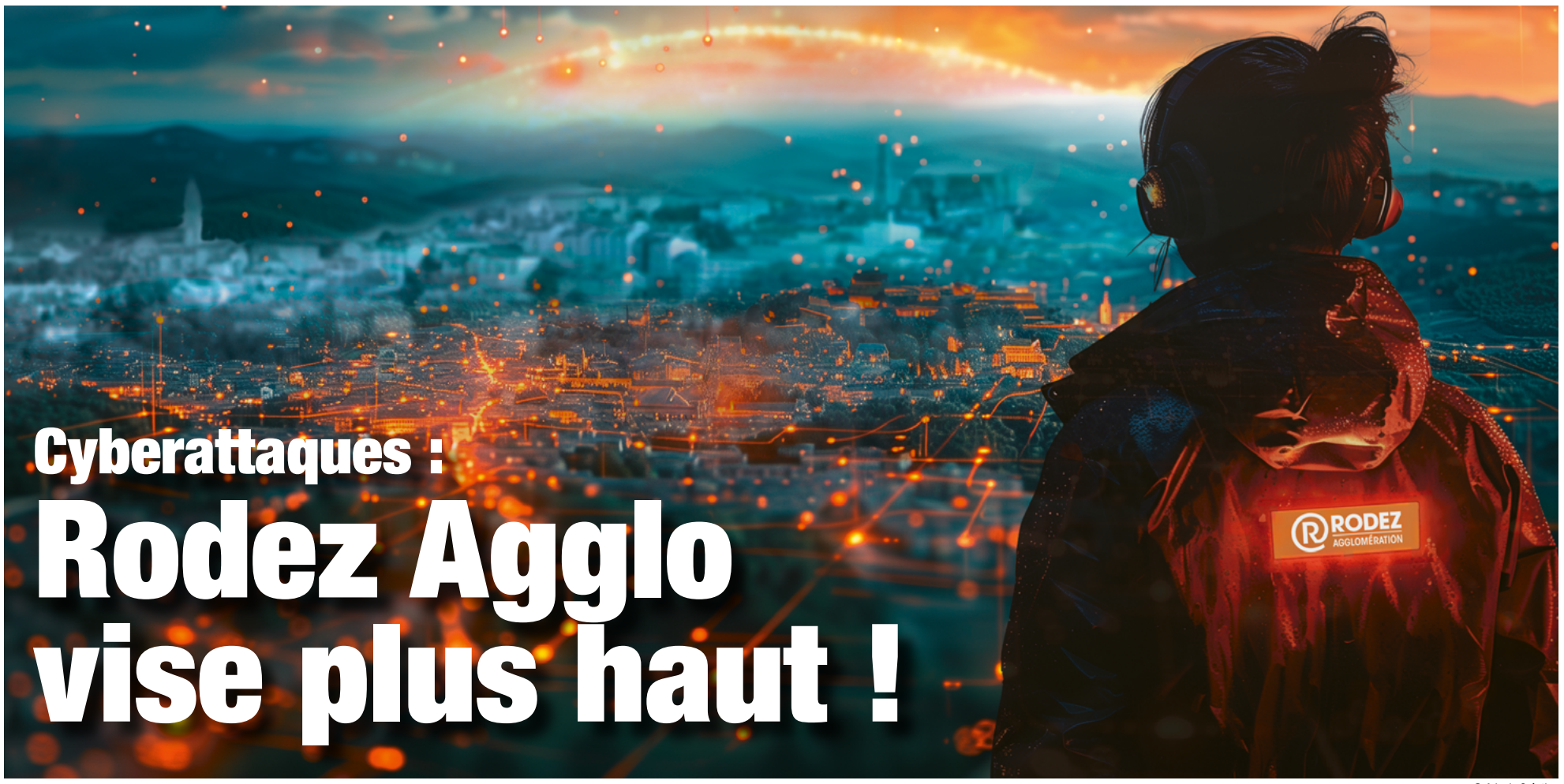
P. 2-3

le journal de la CYBER

Parlez-vous cyber ?
Quelques définitions **au fil des pages**

+ Malwares, spear phishing…
Les conseils de notre expert Ajyle
pour se protéger efficacement P. 3-4

#12* - Mai 2024



© Adonis Créative

Cyberattaques : Rodez Agglo vise plus haut !

ÉDITO

Le cyber-risque, un fléau économique et sociétal

© Rodez Agglomération

La nécessité de la fibre optique n'est plus à démontrer sur nos territoires riches d'entreprises et d'industries consommatrices d'une technologie en évolution constante. Cependant, le corollaire de la multiplication des usages - dématérialisation, partage d'informations, flux monétaires et financiers - est l'adaptation ultra-rapide et permanente de la cybercriminalité. Alors que nous trouvons tout à fait naturel de payer, de s'inscrire, de déclarer, de partager et d'échanger de gros volumes d'informations en ligne, nous devenons dans le même temps de plus en plus tributaires de la fiabilité des infrastructures supports de ces échanges. Les attaques ont augmenté de 400 % entre 2020 et 2023, et 42 % des collectivités sont exposées au cyber-risque. **L'interruption des activités et des services, la destruction de données et la perte financière sont parmi les premières conséquences d'une cyberattaque pour les collectivités.**
La protection contre tous les risques n'existe pas. C'est donc bien la prise de conscience du cyber-risque et de la défaillance des systèmes qui doit impérativement être au cœur de nos actions prophylactiques.
J'ai la responsabilité d'organiser la protection de l'agglomération de Rodez, c'est pourquoi j'ai voulu, en accueillant le CyberTour, proposer une journée d'information destinée aux entreprises et aux collectivités, mais aussi un module de formation pour ceux qui sont en charge de l'organisation numérique de nos collectivités.

Christian Teyssèdre
Président de l'agglomération, maire de Rodez

REGARDS CROISÉS

L'agglomération de Rodez accompagne, au sein de sa Maison de l'économie, des porteurs de projets et de jeunes entreprises. Comment aborde-t-elle avec eux la question de la cybersécurité ?

Nos équipes qui accompagnent les porteurs de projets et les jeunes entreprises abordent les questions de cybersécurité dès les premiers stades de leur réflexion et de leur développement. C'est essentiel pour les aider à se protéger contre les menaces numériques. Ces entrepreneurs sont parfois si concentrés sur leur projet, leur modèle économique, leur communication, leur stratégie, etc., qu'ils en oublient parfois les enjeux et les menaces du numérique.
Monique Bultel-Herment
Adjointe au maire de Rodez, vice-présidente de Rodez Agglomération

Notre mission principale est d'héberger et d'accompagner des entreprises au sein de notre incubateur, de notre pépinière et de notre hôtel d'entreprises. Elles on toutes leurs propres site et fonctionnement. En tant que collectivité, nous sommes des facilitateurs. En matière de cybersécurité, par exemple, nous avons mis à leur disposition le livre blanc de la BPI, nous leur conseillons de se rapprocher d'experts partenaires et les invitons à participer à des webinaires sur le sujet ou encore à des événements comme le CyberTour, qui fait étape à Rodez en mai.
Céline Marcilhac
Responsable de la pépinière d'entreprises

Le CyberTour, c'est une belle opportunité de découvrir l'actualité des dernières menaces et contre-mesures, et aussi de rencontrer les acteurs de la cybersécurité sur le territoire. Notre métier, c'est de digitaliser et centraliser sur une seule plateforme l'ensemble des machines et équipements de production de nos clients, qu'ils soient dans l'agroalimentaire, le traitement des déchets ou encore la métallurgie. Nous utilisons évidemment de nombreux outils numériques, pour le développement (éditeurs de code…), pour l'infrastructure (serveurs, bases de données…), et bien sûr pour le volet administratif et commercial. L'existence des menaces cyber nous contraint à une vigilance constante et à une pratique stricte *zero trust*. Comme tous les fournisseurs de services SaaS, nous sommes confrontés à des tentatives d'attaques contre lesquelles nous avons mis en place plusieurs outils de sécurité : des systèmes de double authentification, l'audit régulier des logs afin de vérifier qui s'y connecte et comment, des notifications en cas de comportement suspect, etc. La surveillance et la gestion de ces risques, c'est un métier à temps plein ! C'est pourquoi nous allons créer un poste dédié.
Sébastien Tachier
Cofondateur de la start-up Arkhale, au sein de la pépinière d'entreprises

De gauche à droite : Pascal Weitten (Arkhale), Monique Bultel-Herment (Rodez Agglomération), Sébastien Tachier et Loïc Sigaud (Arkhale), Céline Marcilhac (Rodez Agglomération).

Cyber TOUR

Vous avez dit CyberTour ?

Organisé par Projet X, ce **programme de conférences locales interactives au format TED** permet aux pros, experts et novices de partager leurs expériences autour de la cybersécurité. **Keynotes**, **tables rondes** et **ateliers** rassemblent des intervenants de premier plan pour offrir aux participants une compréhension approfondie des défis demain.

Cyber' VOC

Zero trust security (sécurité à confiance zéro) :
Modèle de sécurité qui n'accorde une confiance automatique à aucun utilisateur ou appareil, à l'intérieur ou à l'extérieur du réseau de l'organisation. Il nécessite une vérification continue de tous les utilisateurs et dispositifs tentant d'accéder aux ressources du système.

ORANGE CYBERDEFENSE, FORMER ET PROTÉGER À TOUS NIVEAUX

La filiale de l'opérateur télécom, acteur majeur de la cybersécurité en Europe, emploie 120 experts dans le Sud-Ouest. Entretien avec **Nicolas Brochot**, délégué régional Orange Occitanie.

© Orange

Quelle est la vision d'Orange concernant l'importance du CyberTour pour la communauté de la cybersécurité?

Orange est l'acteur de confiance qui donne à chacune et à chacun les clés d'un monde numérique responsable. Les défis en matière de cybersécurité sont nombreux et cet événement est une opportunité majeure pour sensibiliser les citoyens, les entreprises et les collectivités du territoire de l'Aveyron aux enjeux de la sécurité numérique. En tant qu'opérateur télécom, notre objectif est de permettre à tous de profiter des avantages du très haut débit tout en garantissant la protection et la confidentialité des données.

Comment Orange Cyberdefense répond-elle aux principaux défis de cybersécurité que le monde numérique affronte aujourd'hui ?

Dans un contexte de forte croissance des cyberattaques, Orange Cyberdefense a pour mission de venir au secours de nombreux clients qui sont victimes de hackers malintentionnés, avec demandes de rançons à la clé, et toujours plus expérimentés. Pour répondre localement à des besoins en forte croissance, Orange propose à ses clients un service sur mesure, avec des nouvelles offres de surveillance et de protection contre les menaces cyber, qui s'incarnent autour du Micro-SOC, une solution qui permet de protéger les postes de travail et les serveurs d'une entreprise. Son arsenal est complété par des offres innovantes en matière de gestion de crise, sécurité du cloud, environnements industriels et objets connectés, sans oublier des programmes de formation aux risques cyber. Orange a choisi de s'implanter en région car la majorité des attaques touche des TPE, PME et collectivités. Il est donc important d'être présent localement et d'analyser les besoins spécifiques de chacun.

> **La majorité des attaques touche des TPE, PME et collectivités. Il est donc important d'être présent localement.**

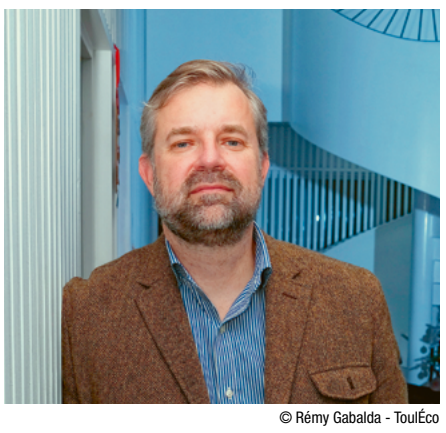
Quel rôle Orange Cyberdefense jouera-t-elle pour façonner l'avenir de la cybersécurité ?

L'évolution de la cybersécurité dans les années à venir pourrait inclure une augmentation des attaques basées sur l'intelligence artificielle. Avec la numérisation croissante des services publics, des entreprises et des infrastructures critiques, il est essentiel de garantir la protection des données sensibles et la continuité des activités. Orange Cyberdefense jouera un rôle-clé en développant des solutions de surveillance, de protection des données et de renforcement de la résilience des infrastructures critiques. La sensibilisation et la formation des acteurs des territoires seront prioritaires pour promouvoir la sécurité numérique. Orange Cyberdefense apportera des services pour aider les entreprises et les citoyens à adopter les bonnes pratiques en matière de cybersécurité.

www.orangecyberdefense.com/fr/

AJYLE, CATALYSEUR DE TRANSFORMATION NUMÉRIQUE ET SOCIÉTALE

La société Ajyle accompagne les organisations publiques et privées dans leur parcours de transition numérique. **Samuel Cette**, l'un de ses cofondateurs, nous dévoile son offre.



© Rémy Gabalda - ToulÉco

Quelles sont les spécificités d'Ajyle ?

Nous offrons des formations spécialisées, des conseils stratégiques et un accès à des compétences expertes *via* le modèle des salariés à temps partagé. En mettant l'accent sur l'IA, la cybersécurité et les technologies émergentes, nous dotons nos clients des outils et connaissances nécessaires pour naviguer dans un paysage numérique en constante évolution, donc instable.

> **La mesure de l'efficacité s'envisage, […] cela est unique, sur le suivi longitudinal des incidents de sécurité.**

Comment Ajyle intègre-t-elle les aspects de cybersécurité et de sécurité économique dans ses services de conseil et de formation ?

À travers des formations dédiées, des audits de sécurité et des conseils stratégiques pour renforcer la résilience des organisations face aux menaces numériques, à l'augmentation des attaques ciblées, à l'émergence de nouvelles formes de malwares.

Quelles motivations vous poussent à participer au CyberTour ?

En participant au CyberTour, Ajyle cherche à sensibiliser davantage les organisations aux enjeux de la cybersécurité, partager son expertise, raison pour laquelle nous axons nos interventions sur la transmission d'un message clair et la présentation de solutions concrètes pour y faire face.

Quelle approche adoptez-vous pour former et sensibiliser les organisations et leurs collaborateurs à la cybersécurité et à la sécurité économique ?

Notre approche repose sur des programmes obligatoirement sur mesure, des ateliers pratiques et des séminaires interactifs, conçus pour engager et acculturer les participants. La mesure de l'efficacité s'envisage, certes, à travers des évaluations avant et après formation, des retours d'expérience, mais surtout, et cela est unique, sur le suivi longitudinal des incidents de sécurité.

www.ajyle.fr

PREDICTA LAB, LA PUISSANCE DE L'OSINT

Baptiste Robert est un « hacker éthique » de renommée internationale. Il a cofondé Predicta Lab, une start-up toulousaine spécialisée dans le renseignement en sources ouvertes (OSINT).

Que propose Predicta Lab ?

Notre pôle technique développe des outils d'investigation et de protection des données, tandis que notre pôle d'analyse produit des rapports d'empreintes numériques qui permettent à notre clientèle d'évaluer son exposition en ligne et d'être accompagnée dans la réduction de cette exposition.

Pourquoi participer au CyberTour ?

Chez Predicta Lab, notre mission est de protéger les individus et les organisations contre les menaces numériques en exploitant la puissance de l'OSINT. Nous sommes engagés dans la sensibilisation et la formation à la protection des données. Par ailleurs, étant fièrement toulousains, nous sommes particulièrement enthousiastes à l'idée de participer à cette initiative dans la région Occitanie.

> **Nous sommes engagés dans la sensibilisation et la formation à la protection des données.**

© Predicta Lab

Quelles sont vos actualités ?

Je reviens tout juste de Washington, aux États-Unis, où j'ai représenté Predicta Lab aux côtés de la « CyberTaskForce ». Là-bas, j'ai pu rencontrer et échanger avec les départements de la Justice et de la Défense, ainsi qu'avec la Maison Blanche. Côté innovation, de nouvelles sources sont régulièrement ajoutées à Predicta Search, notre moteur de recherche d'empreinte numérique, et nos développeurs avancent sur Predicta Graph. Cette nouvelle solution de visualisation des données sera bientôt disponible !

www.predictalab.fr

© Christophe Fleury

« Le CyberTour est clairement une *place to be* »

L'ANSSI, agence française de référence en matière de sécurité du numérique, est en charge de promouvoir les bonnes pratiques envers les entités publiques comme privées. **Il faut que les actions de prévention en cybersécurité ruissellent sur le territoire**, et le CyberTour de l'Aveyron fait justement partie de ces actions. Les défis actuels auxquels la France est confrontée tournent autour de la sécurisation des J.O., mais également de la **mise en œuvre de la directive européenne NIS 2**, qui permettra de mieux sécuriser certains domaines, en complément des opérateurs de services essentiels (OSE) et des opérateurs d'importance vitale (OIV). La directive NIS 2 est un changement de paradigme : on passe de quelques centaines d'opérateurs régulés à quelques milliers, ce qui nécessite un passage à l'échelle aussi bien pour les prestataires que pour le régulateur (ANSSI). Cette directive rentrera en application courant octobre 2024 et fait l'objet de consultations vis-à-vis des associations d'élus comme des fédérations métiers.

Christophe Fleury
Délégué à la sécurité numérique pour l'Occitanie – Agence nationale de la sécurité des systèmes d'information (ANSSI)

cyber.gouv.fr/decouvrir-lanssi

Cyber' VOC

- **OSINT (Open Source Intelligence) :** Désigne la collecte et l'analyse d'informations issues de sources publiques pour le renseignement. C'est une pratique utilisée dans la cybersécurité, la sécurité nationale, le journalisme d'investigation et le secteur privé à partir de données issues de médias, de sites web, de bases de données publiques, de réseaux sociaux et d'autres plateformes en ligne.
- **Hacker éthique :** Professionnel de la cybersécurité qui utilise ses compétences pour détecter et corriger les vulnérabilités des systèmes informatiques de manière légale. Son objectif ? Améliorer la sécurité en identifiant les failles avant les cyberattaques. Il agit avec l'autorisation des propriétaires des systèmes.

CYBER'OCC, LA RÉPONSE RÉGIONALE

La Région Occitanie a lancé en 2022 Cyber'Occ, son centre régional dédié à la cybersécurité. Rencontre avec Marc Sztulman, conseiller régional délégué au numérique et président de Cyber'Occ.

© Région Occitanie – DR

Quel rôle joue Cyber'Occ en Occitanie en matière de cybersécurité ?

C'est d'abord un centre de réponse aux incidents (« CSIRT ») ou service d'urgence cyber public gratuit, que les entreprises, les associations et les collectivités peuvent appeler en cas de cyberattaque pour être conseillées. C'est aussi un centre de ressources et d'information, pour aider les acteurs économiques à se prémunir au mieux contre les cyber-risques, les inscrire dans une démarche *secure by design* s'ils développent des produits numériques, et également pour animer la filière cybersécurité en Occitanie : sensibilisation auprès des TPE, PME, associations, collectivités territoriales, organisations des partenariats avec l'ensemble des corps intermédiaires, ordres professionnels, syndicats, pour diffuser la culture de la cybersécurité auprès de leurs adhérents…

Quels sont les principaux objectifs de Cyber'Occ en participant au CyberTour ?

C'est une formidable occasion de faire connaître notre action dans nos 13 départements. Il faut que les acteurs économiques de la région connaissent notre service d'assistance et, s'ils sont malheureusement attaqués, aient le réflexe de faire appel à nous pour limiter les impacts. Ce service est ouvert depuis 1 an et joignable au 0 800 71 13 13.

> **« La volonté régionale, c'est de porter la cybersécurité auprès de tous les acteurs. »**

Comment le CyberTour s'inscrit-il dans la mission globale de Cyber'Occ ?

Trop souvent, on considère que la cybersécurité, c'est une question de métropole, de grands groupes, et que finalement, les acteurs plus petits ne sont pas concernés. Or, la volonté régionale, c'est de porter la cybersécurité auprès de tous les acteurs, car ils sont potentiellement tous victimes. Ainsi, ces événements s'inscrivent naturellement dans la mission globale de notre agence.

Quelles sont les perspectives d'avenir pour Cyber'Occ ?

Tout d'abord, nous allons avoir dans les prochains mois la labellisation « Campus Cyber ». Cette reconnaissance de notre travail s'accompagnera d'un enrichissement de notre offre de services, faisant de Cyber'Occ le véritable tiers de confiance en matière de cybersécurité dans notre région. Nous allons très rapidement ouvrir des Campus Cyber, dans le Sicoval et à Montpellier. Puis d'autres viendront à brève échéance.

Quels sont les défis spécifiques à la région Occitanie en matière de cybersécurité ?

Notre région connaît 2 types de défis, les défis classiques qui s'appliquent à toutes les régions et des défis particuliers, eu égard aux spécificités de notre tissu économique et notamment industriel. L'Occitanie est un grand centre de recherche et développement, et donc particulièrement ciblée en matière d'intelligence économique.

Comment voyez-vous l'évolution de la cybersécurité en Occitanie dans les années à venir ?

Il va y avoir une multiplication des attaques et, si on n'y prend pas garde, des effets de ces attaques. Notre rôle est de limiter tant les effets que le nombre d'attaques. Mais il faut savoir rester modeste. Il s'agit d'un combat infini. Comme le disait Platon, « Seuls les morts connaissent la fin de la guerre. »

www.cyberocc.com

DÉFINITIONS

CSIRT (*computer security Incident response team*)
Une équipe spécialisée dans la gestion des incidents de sécurité informatique. Il existe des CSIRT d'entreprise, sectorielles, gouvernementales, académiques, régionales, nationales…

CYBERSÉCURITÉ EN OCCITANIE : CHIFFRES-CLÉS

De 3 000 à 6 000
c'est le nombre de personnes mobilisées par la cybersécurité, qui devrait doubler dans les 2 ans.

150 millions d'euros
dédiés entre 2023 et 2027 au contrat de filière numérique, qui comprend de nombreuses actions destinées à la cybersécurité.

Près de 200 entreprises
régionales spécialisées en cybersécurité.

Une quarantaine d'universités, écoles et laboratoires
impliqués dans la région.

Source : laregion.fr

Dans le vaste univers de la cybersécurité, naviguer à travers les menaces peut s'avérer un défi. Quelques conseils pratiques de notre **expert Ajyle**.

#FAQ : MALWARES

COMMENT IDENTIFIER ET SE PROTÉGER CONTRE LES MALWARES ?

Les malwares, ou logiciels malveillants, sont conçus pour endommager ou infiltrer un système informatique. Ils peuvent se présenter sous forme de virus, de ransomwares ou de spywares.

LES BONNES PRATIQUES

1. INSTALLEZ UN ANTIVIRUS FIABLE ET METTEZ-LE À JOUR RÉGULIÈREMENT

POURQUOI C'EST IMPORTANT
Un logiciel antivirus joue un rôle crucial dans la détection et la neutralisation de logiciels malveillants qui pourraient infecter votre appareil. Un bon antivirus peut vous protéger contre une vaste gamme de menaces, y compris les virus, les logiciels espions, les ransomwares et d'autres formes de malwares.

COMMENT PROCÉDER
- Choisissez un logiciel antivirus réputé en vous basant sur des évaluations indépendantes et des critiques fiables. Prenez en compte les fonctionnalités offertes, la facilité d'utilisation et l'impact sur les performances de votre système.
- Activez les mises à jour automatiques pour votre antivirus afin de vous assurer qu'il est toujours actualisé avec les dernières définitions de virus et améliorations de fonctionnalités. Les menaces évoluant constamment, ce point est essentiel pour une protection efficace.
- Effectuez des analyses régulières pour détecter et supprimer les éventuels malwares présents sur votre appareil. Bien que la protection en temps réel soit essentielle, des analyses complètes périodiques peuvent révéler des menaces qui ont pu passer inaperçues.

© Adonis Créative

2. ÉVITEZ DE TÉLÉCHARGER DES FICHIERS OU DES LOGICIELS DEPUIS DES SITES WEB NON SÉCURISÉS

POURQUOI C'EST IMPORTANT
Les sites web non sécurisés peuvent héberger des logiciels malveillants déguisés en téléchargements légitimes. Télécharger et installer ces fichiers peut compromettre la sécurité de votre appareil.

COMMENT PROCÉDER
- Vérifiez la fiabilité des sources avant tout téléchargement. Privilégiez les sites officiels ou les plateformes de distribution reconnues.
- Recherchez des signes de sécurité, tels qu'une connexion HTTPS sécurisée (indiquée par un cadenas dans la barre d'adresse de votre navigateur), et lisez les avis d'autres utilisateurs si disponibles.
- Utilisez un logiciel antivirus avec protection web, qui peut vous avertir et vous protéger contre les téléchargements dangereux et les sites web malveillants.

3. GARDEZ VOTRE SYSTÈME D'EXPLOITATION ET VOS APPLICATIONS À JOUR

POURQUOI C'EST IMPORTANT
Les mises à jour de logiciels incluent souvent des correctifs pour les vulnérabilités de sécurité qui, si elles sont exploitées, peuvent permettre aux attaquants d'infiltrer ou de compromettre votre appareil. En maintenant votre système et vos applications à jour, vous minimisez le risque d'attaques.

COMMENT PROCÉDER
- Activez les mises à jour automatiques pour votre système d'exploitation et vos applications. Cela garantit que vous recevez et appliquez les correctifs de sécurité dès qu'ils sont disponibles.
- Vérifiez manuellement les mises à jour périodiquement, surtout pour les logiciels critiques ou ceux qui ne se mettent pas à jour automatiquement.
- Soyez attentif aux notifications de mise à jour de votre système ou de vos applications et n'ignorez pas les recommandations d'installation de mises à jour de sécurité.

(… suite)

LE SPEAR PHISHING

QUELQUES CONSEILS POUR SE PROTÉGER

Le numéro précédent du *Journal de la cyber* introduisait la notion de phishing. Zoom sur le spear phishing, qui a la particularité d'utiliser des informations spécifiques sur sa cible afin de paraître plus crédible. Pour ne pas tomber dans le panneau, suivez le guide !

QU'EST-CE QUE C'EST, AU JUSTE ?

Pour illustrer le spear phishing, cette forme de phishing qui cible des individus ou des organisations spécifiques avec des messages personnalisés pour augmenter leurs chances de succès, prenons quelques exemples d'attaques dont vous avez peut-être déjà entendu parler.

L'ATTAQUE CONTRE TV5 MONDE

En avril 2015, la chaîne de télévision mondiale basée en France a été victime d'une cyberattaque majeure. Bien que l'attaque elle-même ait été une combinaison de plusieurs techniques, elle a été précédée d'une campagne de spear phishing visant les employés. Comment ? Les cybercriminels ont utilisé des e-mails personnalisés pour obtenir les identifiants d'accès au réseau interne de la chaîne, ce qui a ensuite permis une attaque plus vaste qui a presque mis hors ligne la chaîne.

LE PIRATAGE DE LA CAMPAGNE PRÉSIDENTIELLE FRANÇAISE DE 2017

Pendant l'élection présidentielle française de 2017, l'équipe de campagne du parti d'Emmanuel Macron, En Marche !, a été ciblée par une série d'attaques de spear phishing sophistiquées. Les assaillants ont tenté d'obtenir l'accès aux comptes de messagerie personnels et professionnels des membres de l'équipe en utilisant des e-mails de phishing personnalisés. En a résulté la fuite de nombreux documents internes peu avant le jour du scrutin. L'équipe a pu identifier et contrer plusieurs de ces tentatives, limitant ainsi l'impact des attaques.

L'« ARNAQUE AU PRÉSIDENT »

De plus large envergure que le spear phishing traditionnel, l'« arnaque au président » mérite tout de même d'être mentionnée en raison de son approche hautement ciblée et personnalisée. Cette escroquerie implique des fraudeurs se faisant passer pour le PDG ou un haut dirigeant d'une entreprise contactant un employé par e-mail ou par téléphone pour lui demander de réaliser en urgence un virement financier. Plusieurs entreprises françaises ont été victimes de cette arnaque, perdant parfois des millions d'euros, à l'instar du groupe hôtelier Accor, de 2005 à 2006, qui en a significativement fait les frais.

LES ATTAQUES CONTRE LES HÔPITAUX

Les hôpitaux et les institutions de santé en France subissent régulièrement des cyberattaques, certaines au moyen de campagnes de spear phishing. Cela a été le cas en particulier pendant la crise du COVID-19. Les attaquants ont utilisé des e-mails prétendument envoyés par des organisations de santé officielles ou des fournisseurs de matériel médical pour inciter le personnel à cliquer sur des liens malveillants ou à divulguer des informations sensibles.

QUELLES SONT LES MESURES DE PRÉVENTION ?

La lutte contre le spear phishing, en raison de sa nature ciblée et sophistiquée, exige une approche multicouche qui combine la sensibilisation, la formation et l'adoption de technologies de sécurité avancées. Voici 6 mesures essentielles :

1. LA FORMATION ET LA SENSIBILISATION DE VOS EMPLOYÉS

- Des programmes de formation réguliers leur permettront de s'acculturer aux signes de spear phishing, tels que les demandes inattendues d'informations sensibles, les anomalies dans les adresses e-mail des expéditeurs et les liens ou pièces jointes suspects.
- Il peut être intéressant de compléter par des exercices de simulation de spear phishing pour tester leur vigilance et les former à réagir correctement face à des tentatives d'escroquerie.

2. LES SOLUTIONS DE SÉCURITÉ E-MAIL AVANCÉES

- Utilisez des filtres « anti-phishing », c'est-à-dire des solutions de filtrage des e-mails qui peuvent détecter et bloquer les tentatives de phishing, y compris les attaques sophistiquées de spear phishing.
- Vérifiez l'authenticité des e-mails et empêchez l'usurpation d'identité en mettant en place des protocoles comme DMARC, SPF et DKIM.

3. LES CONTRÔLES D'ACCÈS ET DE VÉRIFICATION

- Implémentez l'authentification multi-facteur (MFA) pour ajouter une couche de sécurité supplémentaire aux comptes, rendant plus difficile pour les attaquants l'accès aux systèmes, même s'ils obtiennent des informations d'identification.
- Adoptez le « principe du moindre privilège » : il consiste à limiter les accès aux informations et aux systèmes strictement aux nécessités opérationnelles. Cela permet de réduire l'impact potentiel d'une compromission.

4. LA MISE EN PLACE DE POLITIQUES DE SÉCURITÉ CLAIRES

- Établissez des protocoles stricts pour les transferts d'argent et les demandes financières urgentes, incluant des vérifications par plusieurs canaux de communication.
- Développez et communiquez des procédures claires pour signaler les tentatives de spear phishing et les incidents de sécurité.

5. LA SURVEILLANCE ET LA RÉPONSE AUX INCIDENTS

- Il existe des outils de détection des menaces capables de surveiller les réseaux et les systèmes en quête de signes d'activité suspecte, ce qui facilite une réponse rapide en cas d'attaque.
- Préparez des plans de réponse aux incidents de sécurité pour assurer une action coordonnée et efficace en cas de repérage d'une attaque de spear phishing réussie.

6. LES MISES À JOUR RÉGULIÈRES ET LE PATCH MANAGEMENT

Assurez-vous que tous les systèmes d'exploitation, logiciels et applications sont régulièrement mis à jour avec les derniers correctifs (patchs) de sécurité pour minimiser les vulnérabilités exploitables.

L'INFO EN +

Le phishing, cybermenace n° 1

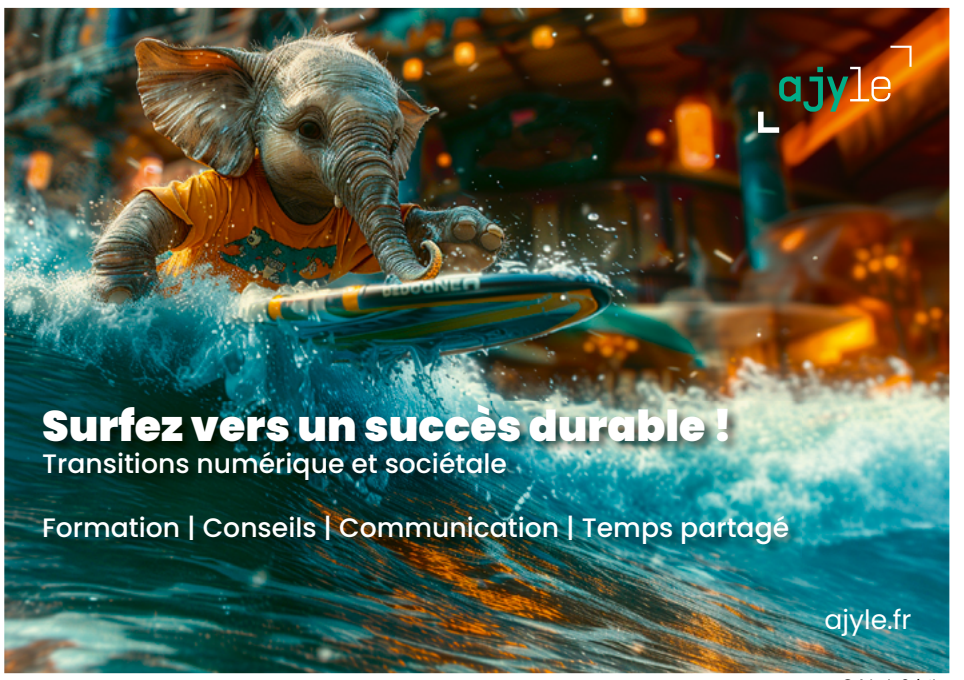
Selon le site www.cybermalveillance.gouv.fr, en 2023, près de **1,5 million de consultations** de ses contenus concernaient les principales formes de phishing, et **plus 50 000 particuliers et professionnels** ont recherché une assistance sur cette menace.

Le phishing occupe la **1re place** chez les particuliers, les collectivités et les administrations en termes de recherche d'assistance, et la 2e place chez les entreprises, juste derrière le piratage de compte.

5 entreprises sur 6

déclarent **ne pas disposer de moyens spécifiques** pour la sécurité de leur système d'information.

Source : BusinessDIT



© Adonis Créative

Le *Journal de la cyber* est édité par **Projet X** - N° 12 (* numéro bêta) – mai 2024
Directeur de la publication : Samuel Cette
Comité éditorial : Jean-Christophe Arguillère, Samuel Cette, Célie Cousinié, Ingrid Gautier, Martin Venzal
Rédaction, création graphique et maquette : Adonis Créative – **Impression :** Techni Print imprimerie

PEFC 10-31-1286 projet X Cyber TOUR