DU CŒUR DE L'ÉTAT

Le Gouvernorat se raconte

Année 2 Cité du Vatican Numéro 2

TRIMESTRIEL AVRIL-JUIN 2025

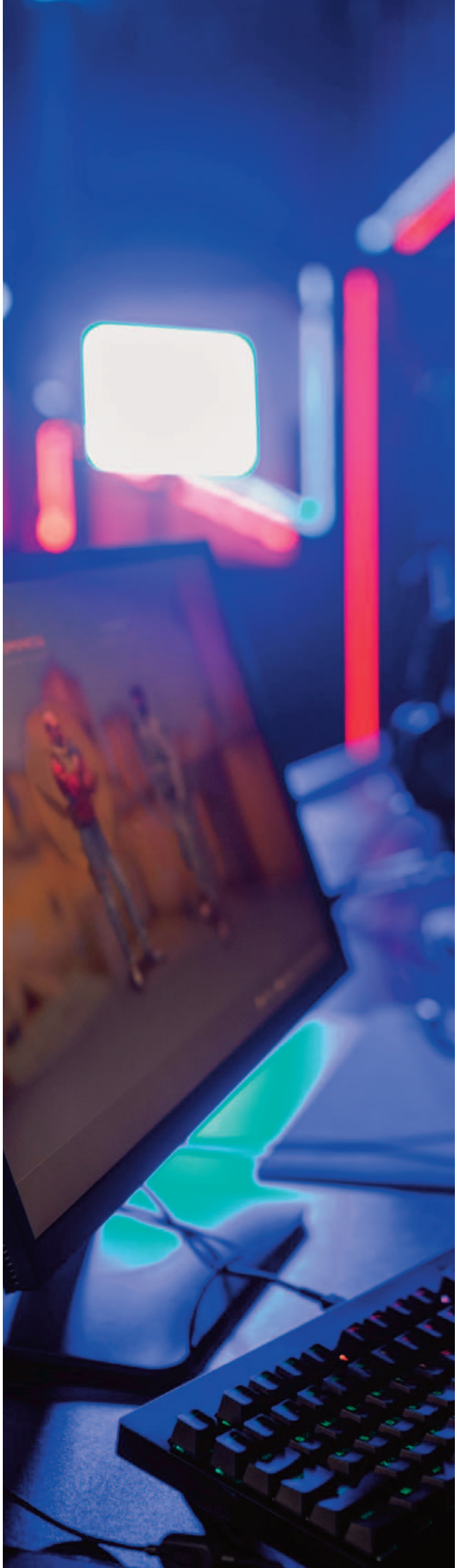
Publication du Gouvernorat de l'État
de la Cité du Vatican

Communication institutionnelle
00120 Cité du Vatican
(État de la Cité du Vatican)
Email: comunicazione@scv.va

Site internet: www.vaticanstate.va

X (Twitter): Governatorato_SCV
Instagram: Governatorato_SCV

Responsable éditorial : Nicola Gori
Éditeur : Gouvernorat de l'État de la Cité du Vatican



LA CYBERSÉCURITÉ EST L'AFFAIRE DE TOUS

Le choix de consacrer cette newsletter à la cybersécurité est né du désir d'offrir une sorte de vade-mecum pour s'orienter et se protéger au sein d'une réalité complexe et multiforme. Étant convaincus qu'à un niveau personnel, chacun porte une part de responsabilité en matière de sécurité informatique.
En effet, compte tenu de leurs implications, les questions liées à la cybersécurité vont bien au-delà des seuls aspects techniques. Elles concernent, entre autres, plusieurs dimensions : la gestion des risques, le droit, la communication, la vie privée, l'économie, etc.
Il est évident que la cybersécurité est un domaine très spécifique, qui mobilise des experts en informatique, en mathématiques ou en physique.
Cependant, elle fait désormais partie de notre quotidien, tout comme le monde numérique et, plus récemment, l'intelligence artificielle en font partie. La cybersécurité s'occupe de la protection des systèmes informatiques, des réseaux, des données et des dispositifs contre les menaces cybernétiques, les attaques et les violations de la vie privée. Elle vise à garantir la confidentialité et la disponibilité des ressources numériques, afin de prévenir les dommages et d'assurer protection et sécurité à toutes les activités dans l'environnement numérique.
Dans ce contexte, il est essentiel de prendre conscience qu'au sein du Gouvernorat, où l'on utilise des outils informatiques, chacun porte une part de responsabilité dans la protection de la structure.
Dans cette newsletter, on peut trouver quelques précautions utiles qu'un groupe d'experts du secteur suggère d'appliquer à notre relation quotidienne avec le monde cybernétique. Parmi les indications fondamentales, une attention particulière doit être portée aux demandes dont on ne connaît pas l'origine, aux

pièces jointes et aux supports USB potentiellement inactifs. En cas de doute, il est toujours bon de demander conseil et d'informer le responsable de la sécurité.
En effet, les attaques informatiques peuvent avoir des effets très négatifs sur l'intégrité de la structure numérique. Les cyberpirates visent à obtenir des avantages de nature financière, comme dans le cas des attaques par ransomware. Mais ils tendent aussi à obtenir des informations confidentielles qui produisent des effets sur les personnes. C'est le cas de données personnelles dérobées (par exemple : vol d'identité) et cédées à des organisations criminelles pour leurs propres objectifs.
De plus, une attaque subie par une entité institutionnelle peut également nuire à la confiance qu'on lui accorde ; ainsi, lorsqu'un site internet est frappé, il y a toujours une répercussion au niveau de son image.
Si l'on en arrive ensuite à la compromission de l'intégrité des systèmes informatiques, c'est parfois le fonctionnement même de l'organisation qui en pâtit. Les attaques peuvent aussi avoir des effets dévastateurs lorsque la cible est le système d'un hôpital ou d'un service de transport.
Pour toutes ces raisons, il est opportun d'être informé et conscient de sa responsabilité personnelle, afin de ne pas offrir d'occasion aux personnes malintentionnées.
C'est dans cet objectif que des conseils particulièrement intéressants et utiles sont proposés dans cette newsletter.

Nicola Gori

LA SÉCURITÉ AVANT TOUT

Le Gouvernorat de l'État de la Cité du Vatican a toujours placé la sécurité et la protection de ses systèmes informatiques au premier rang de ses priorités. Il s'agit d'un engagement qui a marqué la naissance et le développement du réseau Internet au sein de l'État et de ses systèmes d'exploitation.
Par ailleurs, les ressources investies dans la cybersécurité ne sont pas négligeables, car elles visent avant tout à protéger et à préserver l'image du Souverain Pontife, ainsi que l'usage quotidien des dispositifs numériques de la part de l'État à son service.
C'est dans cette perspective que la Direction des Services de Sécurité et de Protection civile du Gouvernorat a signé, le 18 juillet 2024, un Protocole d'entente avec l'Agence nationale pour la cybersécurité de la République italienne (Acn).
L'objectif était l'échange d'informations, les activités de formation et les projets de cybersécurité, afin de développer les capacités et les compétences techniques et scientifiques en matière de prévention des risques liés à la criminalité dans le cyberespace.
Il s'est agi d'une étape importante pour assurer une coopération plus vaste dans l'élaboration de programmes de formation dans le domaine de la cybersécurité.
Une attention particulière a été portée à l'échange d'informations, d'expériences et de procédures dans ce secteur, en vue de garantir la protection de l'espace cybernétique, tout en promouvant également des projets de recherche visant à accroître les capacités et les compétences techniques et scientifiques.
Il est évident que ce Protocole d'entente ne représente qu'une partie de l'effort du Gouvernorat pour garantir à l'ensemble de ses structures les piliers de la sécurité informatique : défense périmétrique, sécurité de l'information, gestion des identités et des accès (Iam), intégrité des données et disponibilité.
Malgré le fort investissement dans la cybersécurité, il est nécessaire de disposer non seulement de systèmes d'exploitation et de technologies, mais aussi de la collaboration de tous ceux qui font partie de la communauté de travail du Gouvernorat. C'est cela qui fait la différence et permet d'assurer un niveau de protection plus élevé.
Par conséquent, cette newsletter souhaite être une occasion d'apprendre et de retenir les bonnes pratiques qui empêchent d'offrir un espace dans lequel les criminels peuvent s'infiltrer.
C'est avec ce vœu que je souhaite à tous une bonne lecture.

Sœur Raffaella Petrini
Présidente du Gouvernorat de l'État de la Cité du Vatican

CYBERSÉCURITÉ : UNE VISION STRATÉGIQUE ENTRE TECHNOLOGIE, RÉSILIENCE ET CULTURE DE LA SÉCURITÉ

Dans un monde de plus en plus interconnecté, où la numérisation imprègne tous les secteurs, la cybersécurité n'est plus une problématique technique réservée aux services informatiques. Elle constitue désormais l'un des principaux défis stratégiques pour la protection des services, des données et des actifs numériques. Les cybermenaces, par leur capacité à frapper rapidement, à grande échelle et avec des impacts transversaux, exigent toujours plus une réponse systémique et permanente.
Dans le contexte actuel, il est nécessaire de développer une vision stratégique à long terme pour la protection de l'espace numérique. Cette vision doit reposer sur trois piliers fondamentaux :

- des infrastructures et des processus sécurisés ;
- des compétences techniques avancées ;
- une culture de la sécurité diffuse.

L'analyse de la situation actuelle montre que les infrastructures numériques – réseaux, centres de données, plateformes – sont aujourd'hui conçues pour garantir robustesse, continuité opérationnelle et fiabilité, tout en répondant à des exigences de maîtrise des coûts. Cependant, la rapide évolution des technologies et l'augmentation exponentielle des menaces imposent un modèle d'évolution continue. Il ne s'agit pas simplement de mettre à jour les appareils et les logiciels, mais de transformer l'ensemble du système en une infrastructure adaptative et intelligente, capable d'apprendre à partir des données et de réagir en temps réel. Dans cette perspective, l'adoption de modèles de Zero Trust architecture, la virtualisation des systèmes et l'intégration de l'intelligence artificielle dans les mécanismes de détection constituent des éléments clés d'une stratégie de défense avancée.
Traditionnellement, la cybersécurité s'est concentrée sur la protection du périmètre : pare-feux, antivirus, segmentation des réseaux. Or, cette approche n'est désormais plus suffisante. Les attaques ne se limitent plus à forcer les « portes d'entrée », mais exploitent aussi des vulnérabilités internes, les comportements humains et les dispositifs connectés.

Une stratégie moderne de cybersécurité doit donc inclure :

- Surveillance continue et threat intelligence : être capables d'analyser les flux de données en temps réel, d'identifier des schémas anormaux et d'anticiper les comportements malveillants.
- Réponse aux incidents et résilience opérationnelle : prédisposer des plans de réponse structurés aux incidents et garantir la continuité des activités, même en cas d'attaque.
- Cyberdissuasion : renforcer les capacités défensives pour dissuader les attaquants, notamment par le biais de coopérations internationales et de la cyber diplomacy.
- Protection end-to-end : assurer la sécurité à chaque étape du cycle de vie des données, de la collecte à la conservation, jusqu'à leur suppression.

Cette approche implique la transition d'une simple posture défensive vers une attitude proactive : identifier, évaluer et neutraliser les menaces avant qu'elles ne se transforment en incidents.
L'un des aspects les plus sous-estimés, mais décisifs, de la sécurité informatique est le facteur humain, souvent cité. Les statistiques confirment qu'un pourcentage significatif des cyberattaques réussies est dû à des erreurs humaines, des inat-

tentions ou un manque de formation. C'est pourquoi, parallèlement à l'innovation technologique, il est essentiel de promouvoir une culture de la sécurité impliquant tous les niveaux de l'organisation, des décideurs au sommet jusqu'aux utilisateurs finaux. Dans ce contexte, des initiatives telles que des programmes de formation continue pour l'ensemble du personnel, des campagnes de sensibilisation au phishing et à l'ingénierie sociale, des simulations d'attaques, ou encore des formations à la cyber hygiène, deviennent des outils fondamentaux pour bâtir un écosystème sécurisé.

On peut, par exemple, valoriser les cinq facteurs de la cyber hygiène au sein de sa propre structure professionnelle.

• Segmentation. Le réseau de données doit être segmenté en zones délimitées de manière à garantir la protection de l'ensemble du système et à rendre les points d'accès invulnérables aux attaques. Ce type de sécurité répond également aux besoins liés au télétravail. En cas de violation, la sécurité intrinsèque permettra de contenir l'incident sans compromettre le reste des activités.

• Chiffrement. Si les pare-feux et les protocoles d'accès sont violés et que les autres défenses échouent, le chiffrement garantit que toutes les données sensibles stockées deviennent inutilisables entre les mains des cybercriminels. Sans les clés pour les déchiffrer et les reconstituer, les données cryptées constituent un casse-tête difficile à résoudre. Une bonne hygiène informatique implique de chiffrer les fichiers et les données avant de les partager. Il en va de même pour le chiffrement du trafic réseau, lorsque cela est possible.

• Authentification à deux facteurs. La sécurité est de plus en plus liée à la personne : la reconnaissance faciale et les empreintes digitales en sont des exemples. Même la mise en place d'une authentification basique à deux facteurs peut s'avérer efficace pour bloquer une première vague de violations. Plus l'authentification devient personnelle, plus les réseaux seront sécurisés. En effet, il est bien plus compliqué de voler une empreinte digitale que de s'emparer d'un simple code PIN !

• Mises à jour constantes. Les malwares évoluent en devenant toujours plus sophistiqués, il est donc nécessaire d'être prêt à les contrer grâce aux mises à jour régulièrement publiées à cet effet.

• Principe du moindre privilège. Même si l'on a une confiance totale envers ses employés, cela ne signifie pas que tous ont besoin des mêmes niveaux d'accès. Une bonne pratique en matière de sécurité consiste à n'accorder à chaque utilisateur que les accès dont il a réellement besoin. En limitant au maximum l'accès aux données sensibles, on réduit les points de vulnérabilité.

Pour conclure, en regardant vers l'avenir, le concept à adopter n'est pas seulement celui de la cybersécurité, mais celui, plus large et ambitieux, de la cyber-résilience. Cela signifie :

• anticiper l'imprévisible,
• répondre avec flexibilité et rapidité aux événements critiques,
• rétablir les fonctions dans des délais certains,
• s'adapter et s'améliorer en permanence.

Dans le cyberespace, la résilience prime sur l'invulnérabilité.

La meilleure protection s'obtient en investissant dans la construction d'une identité numérique forte, fondée sur des infrastructures résilientes, des collaborateurs sensibilisés et une action stratégique multiniveau. Ce n'est qu'ainsi que l'on pourra relever les défis de la sécurité numérique d'aujourd'hui et de demain.

10 RÈGLES D'OR POUR ÊTRE EN LIGNE EN TOUTE SÉCURITÉ : COMMENT PROTÉGER SA VIE NUMÉRIQUE DES MENACES ET DES ESCROQUERIES

La sécurité en ligne est une préoccupation majeure à l'ère numérique. Protéger ses données et son identité en ligne est essentiel pour éviter les escroqueries, l'usurpation d'identité et les cyberattaques. Voici **dix règles essentielles** pour surfer en toute sécurité et réduire les risques.

1. Utiliser des mots de passe forts et uniques et favoriser l'utilisation de phrases de passe

Selon les lignes directrices du **National Institute of Standards and Technology (NIST)**, un mot de passe sécurisé doit comporter au moins **12 à 16 caractères**, des **lettres majuscules et minuscules, des chiffres et des caractères spéciaux**, et éviter les mots couramment utilisés. Il est conseillé d'utiliser un **gestionnaire de mots de passe** pour générer et stocker en toute sécurité les informations d'identification, en évitant de réutiliser le même mot de passe pour plusieurs comptes.

Dans le paysage de la sécurité informatique, l'adoption de phrases de passe s'avère être un choix de plus en plus recommandé et souhaitable. Contrairement aux mots de passe traditionnels, les phrases de passe représentent une chaîne de mots plus longue et plus articulée, conçue pour garantir un niveau de protection plus élevé dans les processus d'authentification.

Alors que les mots de passe classiques sont souvent limités à une séquence de seize caractères au maximum, une phrase de passe peut s'étendre à cent caractères ou plus. Sa structure, basée sur une combinaison de mots, de ponctuation et de lettres majuscules ou minuscules, la rend extrêmement résistante aux cyberattaques, tout en conservant un haut degré de mémorabilité pour l'utilisateur.

L'utilisation de phrases de passe renforce non seulement la sécurité contre les accès non autorisés, mais améliore également la facilité d'utilisation : contrairement aux séquences alphanumériques complexes des mots de passe traditionnels, les phrases de passe sont basées sur des phrases complètes, ce qui les rend plus intuitives et moins susceptibles d'être oubliées.

Ce type d'authentification est désormais largement utilisé dans des contextes qui exigent des normes de sécurité élevées, comme le cryptage des données et la protection des systèmes d'exploitation et des applications avancés. **La prise en charge** croissante des phrases de passe par de nombreuses plateformes informatiques souligne la nécessité d'une évolution des pratiques de protection des accès numériques, en mettant l'accent sur un équilibre entre la sécurité et la facilité d'utilisation.

2. Activer l'authentification multifactorielle (MFA)

L'authentification multifactorielle (MFA) ajoute un niveau de sécurité supplémentaire en exigeant plus d'une méthode de vérification pour accéder aux comptes. Outre les mots de passe, elle peut inclure des codes OTP envoyés par SMS ou par une application d'authentification, une authentification biométrique ou des clés de sécurité hardware, ce qui rend l'accès non autorisé plus difficile. Le **NIST recommande** d'utiliser des **applications d'authentification** ou des **clés physiques** plutôt que des SMS, qui peuvent être interceptés.

3. Se méfier des courriels et des messages suspects (Phishing)

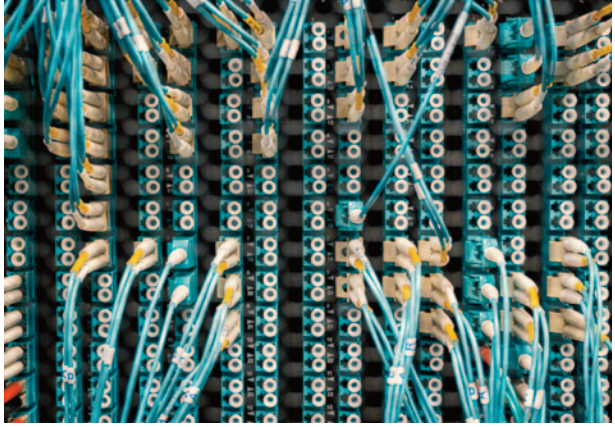
Les escroqueries par phishing visent à voler des informations sensibles en simulant des communications officielles. Il est important de ne pas cliquer sur des liens suspects et de toujours vérifier la source du message avant de saisir des données personnelles ou bancaires. Selon le **National Cybersecurity Centre (NCSC)**, plus de **90 % des cyberattaques** commencent par un courriel de phishing.

4. Mettre régulièrement à jour les appareils et les logiciels
Les mises à jour des systèmes et des applications contiennent souvent des correctifs de sécurité qui protègent les appareils contre les vulnérabilités connues. L'activation des mises à jour automatiques est une bonne pratique. Le **NIST** et d'autres organismes de sécurité recommandent d'appliquer immédiatement les patchs de sécurité délivrés afin d'éviter les attaques basées sur des « exploits » connus.

5. Protéger les données sensibles et la vie privée
Évitez de partager des informations personnelles ou financières sur des sites peu sûrs et limitez la quantité de données publiées sur les médias sociaux. Vous devriez revoir vos paramètres de confidentialité pour contrôler qui peut voir vos contenus. Le **Règlement général sur la protection des données (RGPD)** souligne l'importance de protéger les données personnelles pour éviter toute utilisation abusive.

6. Vérifier la sécurité des sites web
Avant de saisir des données sensibles sur un site web, assurez-vous qu'il utilise le protocole **HTTPS** et que le certificat SSL est valide. Les sites de confiance affichent l'icône d'un cadenas à côté de l'adresse dans la barre du navigateur. Selon le **Google Transparency Report**, les sites qui n'utilisent pas le protocole HTTPS sont plus sensibles aux écoutes et aux attaques de type « man-in-the-middle ».

7. Éviter les connexions Wi-Fi publiques non sécurisées
Les réseaux Wi-Fi ouverts sont souvent vulnérables aux attaques.



Si vous devez les utiliser, il est conseillé de ne surfer que sur des sites sécurisés et d'utiliser un **VPN (Virtual Private Network)** pour protéger les données transmises. Le **Federal Bureau of Investigation (FBI)** recommande d'éviter d'accéder à des comptes bancaires ou à des données sensibles via un réseau Wi-Fi public non protégé.

8. Attention aux pièces jointes et aux téléchargements
Les fichiers et les programmes téléchargés à partir de sources non fiables peuvent contenir des logiciels malveillants. Il est conseillé de vérifier la provenance des fichiers avant de les ouvrir et d'utiliser un **logiciel antivirus à jour**. Selon la **Cybersecurity and Infrastructure Security Agency (CISA)**, les pièces jointes au format .exe, .zip et .js sont parmi les vecteurs les plus courants de logiciels malveillants.

9. Vérifiez régulièrement ses comptes
Surveillez l'activité de vos comptes en ligne pour détecter tout accès suspect. Des services tels que **« Have I Been Pwned »** vous permettent de vérifier si vos informations d'identification ont été compromises lors de violations de données. Le **NCSC** suggère d'activer les notifications en cas d'accès non reconnu et de changer les mots de passe immédiatement en cas de suspicion de violation.

10. Utiliser des outils de sécurité fiables
L'utilisation d'un **antivirus à jour**, d'un **pare-feu actif** et d'un **VPN** permet de protéger les données contre les logiciels malveillants et les accès non autorisés. Il est important de choisir des outils de sécurité fiables provenant de fabricants reconnus. Le **NIST** recommande de toujours activer les fonctions de sécurité intégrées aux systèmes d'exploitation, telles que les pare-feu et le contrôle des accès.

Conclusion
Le respect de ces dix règles contribuera à **réduire le risque de cyberattaques** et à préserver la sécurité de votre identité numérique. La sensibilisation et la prudence sont les meilleures défenses contre les menaces qui pèsent sur les réseaux. La mise en œuvre de ces pratiques offre une protection efficace contre les menaces numériques.

RANSOMWARE : LA DERNIÈRE FRONTIÈRE DE L'EXTORSION NUMÉRIQUE ET COMMENT SE DÉFENDRE

Un matin, vous allumez votre ordinateur et vous êtes confronté à un message inquiétant qui s'affiche à l'écran :
« Vos fichiers ont été cryptés. Pour les récupérer, vous devez payer une rançon en crypto-monnaie dans les 72 heures ! »
Ce scénario dramatique est la réalité à laquelle de nombreuses entreprises et personnes sont confrontées quotidiennement à cause des ransomwares : l'une des menaces les plus dévastatrices dans le paysage de la cybersécurité.

Qu'est-ce qu'un ransomware ?
Un ransomware (*ransom* du vieux français ranson = rançon, et *ware* abréviation de logiciel) est une forme de logiciel malveillant conçu pour bloquer l'accès aux données d'un système par le biais du chiffrement. Les attaquants exigent ensuite une rançon, généralement en crypto-monnaies telles que Bitcoin, Ethereum ou autres, en échange de la clé de décryptage nécessaire pour récupérer les fichiers.
Il existe deux principaux types de ransomware:
- Locker Ransomware : il bloque l'accès à l'ensemble de l'appareil, le rendant inutilisable.
- Crypto Ransomware : il crypte des fichiers spécifiques, tels que des documents, des images et des bases de données, en laissant le système d'exploitation fonctionner pour permettre la communication avec les attaquants.

Comment les attaques se produisent-elles ?
Les attaques de ransomware se propagent par le biais de différentes techniques, notamment :
- Courriels de phishing : les attaquants envoient des courriels qui semblent provenir de sources fiables. Ces courriels contiennent des liens ou des pièces jointes infectés qui, lorsqu'ils sont cliqués ou ouverts, installent un ransomware sur l'appareil de la victime.
- Téléchargements à partir de sites web compromis : visiter des sites web dangereux ou télécharger des logiciels à partir de sources non fiables peut vous exposer à des logiciels malveillants cachés.
- Vulnérabilités des systèmes : Les pirates exploitent les failles de sécurité des logiciels ou des systèmes d'exploitation pour introduire le ransomware. Cela est particulièrement fréquent lorsque les mises à jour et les patchs ne sont pas appliqués.
- Dispositifs USB infectés : même les supports physiques, tels que les clés USB, peuvent être utilisés pour propager des ransomware.
- Attaques ciblées : les grandes entreprises sont souvent l'objectifs d'attaques ciblées, au cours desquelles les attaquants étudient le réseau et recherchent les points faibles avant de frapper.

Pourquoi les Ransomware sont-ils si dangereux ?
Les Ransomware sont dangereux pour plusieurs raisons :
- **Perte de données :** en l'absence de sauvegardes appropriées, les données cryptées peuvent être irrécupérables.
- **Impact économique :** le paiement de la rançon, les coûts de récupération et les temps d'arrêt peuvent entraîner d'énormes pertes financières.
- **Atteinte à la réputation :** pour les entreprises, une attaque par ransomware peut saper la confiance des clients et des partenaires.

- **Évolution constante :** les ransomware deviennent de plus en plus sophistiqués, ce qui les rend difficiles à prévenir.

Comment se défendre contre les ransomware

La prévention est la clé pour se protéger de cette menace. Voici quelques stratégies efficaces pour réduire le risque d'une attaque de ransomware :

- **Sauvegardes régulières :** sauvegardez régulièrement vos données sur des appareils externes ou des services cloud sécurisés. Veillez à ce que les sauvegardes soient isolées du réseau principal pour éviter qu'elles ne soient touchées lors d'une attaque.
- **Mises à jour et patchs :** gardez toujours votre système d'exploitation et vos logiciels à jour. De nombreux ransomwares exploitent des vulnérabilités connues qui peuvent être corrigées par des patchs rapides.
- **Formation du personnel :** pour les entreprises, il est essentiel de former les employés à reconnaître les courriels suspects et les autres techniques d'ingénierie sociale. Une formation régulière permet d'éviter les erreurs humaines.
- **Solutions de sécurité avancées :** Utilisez des logiciels antivirus, des pare-feux et des systèmes de détection d'intrusion pour surveiller et bloquer les activités suspectes. De nombreux outils comprennent également des protections spécifiques contre les ransomwares.
- **Authentification à deux facteurs (2FA) :** protéger les comptes par une authentification à deux facteurs afin de rendre l'accès aux systèmes de l'entreprise plus difficile pour les pirates.
- **Accès restreint :** appliquer le principe du privilège minimal, en n'accordant aux employés que l'accès aux ressources dont ils ont besoin pour leur travail. Cela permet de limiter les dommages potentiels en cas d'attaque.
- **Surveillance et audits réguliers :** pour les entreprises, la réalisation d'audits réguliers de la sécurité des systèmes peut aider à identifier les vulnérabilités avant qu'elles ne soient exploitées.
- **Plans d'intervention en cas d'incidents :** Préparer un plan détaillé sur la manière de répondre à une attaque de ransomware. Ce plan doit comprendre des instructions sur la manière d'isoler les systèmes infectés, de communiquer avec les parties affectées et d'entamer la récupération des données.

Que faire en cas d'attaque ?

En cas d'attaque par un ransomware, il est essentiel d'agir rapidement :

- **Isoler les systèmes infectés :** déconnecter immédiatement du réseau les appareils touchés afin d'éviter la propagation du malware.
- **Ne payez jamais la rançon !!!:** Payer ne garantit pas la récupération des données touchées et contribue à financer d'autres attaques.
- **Contactez les autorités :** signalez l'incident aux autorités chargées de l'application de la loi ou à d'autres organismes compétents.
- **Consulter des experts en cybersécurité :** des spécialistes du secteur peuvent aider à atténuer les dommages et à trouver des solutions pour restaurer les systèmes (par exemple : https://www.nomoreransom.org).

Conclusion

Les ransomwares sont l'une des menaces les plus importantes de l'ère numérique, mais avec les bonnes précautions, il est possible de réduire considérablement le risque d'être touché. Investir dans la formation de l'ensemble du personnel sur des thèmes tels que la sécurité de l'information, investir dans la technologie et le recrutement de personnel spécialisé en cybersécurité est aujourd'hui essentiel pour protéger les entreprises et les personnes. La cybersécurité ne doit pas être considérée comme un luxe, mais comme une nécessité fondamentale dans un monde de plus en plus connecté.

CYBERSÉCURITÉ ET SMART HOME : LA SÉCURITÉ DES APPAREILS CONNECTÉS ET LES NOUVELLES MENACES POUR LA VIE PRIVÉE

Introduction

La diffusion croissante de la technologie dans les maisons a radicalement transformé la façon dont nous interagissons avec notre environnement domestique. Allant des appareils connectés aux systèmes de sécurité avancés, le concept de « smart home – maison intelligente » a rendu nos maisons plus efficaces et plus confortables. Toutefois, l'intégration de ces dispositifs pose de nouveaux problèmes de cybersécurité et de protection de la vie privée qui ne peuvent être ignorés.

La vulnérabilité des dispositifs IdO

L'un des principaux risques concerne la vulnérabilité des appareils IdO (Internet des objets). Contrairement aux ordinateurs et aux smartphones, qui sont souvent équipés de solides mesures de sécurité, de nombreux appareils domestiques intelligents sont conçus avec des normes de protection minimales. Cela en fait des cibles faciles pour les pirates, qui peuvent accéder aux caméras de surveillance, aux thermostats et aux assistants vocaux pour compromettre la sécurité de la maison et la vie privée de l'utilisateur. Une fois qu'un appareil a été piraté, un pirate peut l'utiliser pour surveiller les activités de la maison, collecter des informations sensibles ou même prendre le contrôle d'autres appareils connectés au réseau.

Le manque de connaissance chez les utilisateurs

Un autre aspect critique est la sensibilisation des utilisateurs à la cybersécurité. De nombreux consommateurs achètent des appareils intelligents sans connaître les risques associés. Souvent, ils ne modifient pas leurs identifiants par défaut et ne mettent pas régulièrement à jour leurs logiciels, ce qui laisse des portes ouvertes aux pirates. Le fait de ne pas prêter attention à ces mesures de base augmente le risque de violations et d'intrusions. En outre, le trafic du réseau domestique est rarement surveillé par les utilisateurs, ce qui rend difficile la détection d'anomalies ou d'activités suspectes.

La protection des données personnelles

Outre les attaques directes contre les appareils, la protection des données personnelles suscite une inquiétude croissante. Les appareils intelligents collectent une quantité importante d'informations sur les utilisateurs, depuis les habitudes quotidiennes jusqu'aux données biométriques. Si ces informations tombent entre de mauvaises mains, elles peuvent être utilisées à des fins d'usurpation d'identité, de surveillance non autorisée ou même de profilage détaillé à des fins publicitaires. Certains fabricants ont des politiques opaques en matière de gestion des données, ce qui fait qu'il est difficile pour les utilisateurs de savoir comment et où leurs données sont stockées.

Les cyberattaques à grande échelle

Les cybermenaces ne se limitent pas aux utilisateurs individuels, mais peuvent avoir des conséquences à grande échelle. Les cybercriminels peuvent exploiter les appareils IdO pour créer des botnets, des réseaux d'appareils infectés qui sont utilisés pour des attaques à grande échelle, comme le Déni de service distribué (DDoS). Un exemple bien connu est l'attaque du botnet Mirai en 2016, qui a exploité des milliers d'appareils IdO vulnérables pour bloquer des services en ligne entiers. Cela montre qu'une gestion inadéquate de la cybersécurité à la maison peut également avoir des répercussions à l'échelle mondiale.

Solutions et responsabilités

Pour relever ces défis, les fabricants, les utilisateurs et les institutions doivent unir leurs efforts. Les fabricants devraient adopter des normes de sécurité plus strictes, mettre en œuvre un cryptage avancé et garantir des mises à jour automatiques des logiciels pour corriger les éventuelles vulnérabilités. Les utilisateurs, quant à eux, devraient adopter des pratiques de sécurité de base, telles que la modification des mots de passe par défaut, l'activation de l'authentification à deux facteurs et la surveillance régulière des appareils connectés.

Le rôle des réglementations

Au niveau législatif, des progrès ont été réalisés, avec des réglementations imposant des normes de sécurité minimales pour les appareils IdO. L'Union européenne, avec le GDPR, a mis l'accent sur la protection des données, mais l'évolution rapide de la technologie nécessite des mises à jour constantes des réglementations afin de garantir une sécurité adéquate. Il est fondamental que les entreprises soient tenues responsables de la protection des données des utilisateurs et que des mesures plus strictes soient prises pour prévenir d'éventuelles violations.

Conclusions

À une époque où la technologie est de plus en plus présente dans nos vies, assurer la sécurité des appareils connectés doit être une priorité. La maison intelligente offre de nombreux avantages en termes d'automatisation et de confort, mais sans mesures de protection adéquates, le risque de compromission est élevé. Seules une approche éclairée et l'adoption de solutions de sécurité avancées permettront de profiter pleinement des avantages de la technologie sans compromettre la vie privée et la sécurité numérique.

L'INGÉNIERIE SOCIALE : COMMENT LES CRIMINELS EXPLOITENT LES PERSONNES POUR PÉNÉTRER DANS LES SYSTÈMES

Une journée typique au travail… nous recevons un appel téléphonique urgent d'une personne qui se présente comme un technicien du service informatique. D'une manière extrêmement polie et courtoise, il nous informe qu'en raison d'un problème critique avec notre compte, nous devons confirmer certaines informations personnelles. En fournissant le mot de passe puis le token d'authentification, tout peut être résolu en toute sécurité et sans perte de temps. Le ton rassurant et calme de la conversation pourrait nous inciter à faire confiance et à coopérer, mais c'est précisément dans ce genre de situation que les cybercriminels frappent. Il s'agit d'un exemple classique d'ingénierie sociale.

Qu'est-ce que l'ingénierie sociale ?
L'ingénierie sociale est l'art de manipuler les gens pour obtenir l'accès à des informations ou à des systèmes protégés : au lieu d'essayer de percer des systèmes de sécurité informatique complexes, les criminels se concentrent sur une cible non technologique : l'être humain. Les cybercriminels exploitent des éléments tels que la confiance, la peur, la curiosité ou l'urgence de leurs victimes pour les inciter à effectuer des actions dommageables, comme cliquer sur un lien suspect, télécharger un fichier infecté ou révéler des informations d'identification confidentielles.

Quelques-unes des techniques d'ingénierie sociale les plus courantes :

1. Le phishing
Le phishing est probablement la technique d'ingénierie sociale la plus répandue. Il se manifeste par des courriels, des messages ou même des appels téléphoniques (appelés vishing : voice phishing) qui semblent provenir de sources fiables. Les criminels tentent d'inciter la victime à fournir des informations sensibles ou à télécharger des logiciels malveillants (malware).

2. Le pretexting
Dans ce cas, l'attaquant invente un prétexte, c'est-à-dire une histoire crédible, pour gagner la confiance de la victime. Par exemple, il peut se faire passer pour un employé du service des ressources humaines ou un prestataire de services.

3. Le baiting
Le baiting exploite la curiosité des gens. Un exemple classique est une clé USB laissée intentionnellement dans un lieu public, éventuellement avec une étiquette accrocheuse, telle que « Salaire de l'entreprise ». Une fois le dispositif connecté à l'ordinateur, le logiciel malveillant infecte le système.

4. Le tailgating
Cette technique se déroule dans le monde physique. Un criminel s'infiltre dans un bâtiment sécurisé en suivant simplement quelqu'un qui y a accès, peut-être en prétendant avoir oublié son badge.

Pourquoi l'ingénierie sociale est-elle si efficace ?
Le succès de l'ingénierie sociale repose sur un certain nombre de facteurs psychologiques :
- La confiance : les gens ont tendance à faire confiance à ceux qui se présentent de manière professionnelle ou autoritaire.
- L'urgence : la pression en ce qui concerne le temps conduit souvent les victimes à prendre des décisions impulsives.
- Les émotions : La peur ou la curiosité peuvent pousser les gens à agir sans réfléchir.

Comment se protéger ?
Se protéger de l'ingénierie sociale nécessite un mélange de prudence, de bonnes habitudes et d'outils de sécurité. Voici quelques conseils pratiques, axés sur le contexte professionnel :

1. Formation continue
La sensibilisation est la première étape. La participation régulière à des cours de formation sur la sécurité informatique peut faire toute la différence. Il ne s'agit pas nécessairement de cours com-

pliqués : même de simples sessions de remise à niveau sur la manière de reconnaître les techniques d'ingénierie sociale peuvent s'avérer utiles. En outre, la simulation périodique d'attaques (telles que de fausses tentatives de phishing) peut permettre de tester le niveau de préparation du personnel.

2. Politiques de vérification strictes
Ne fournissez jamais d'informations sensibles à une personne qui prend contact avec vous sans préavis, même si la demande semble légitime. Avant d'agir, il est préférable de prendre le temps de vérifier l'identité du demandeur. Par exemple, si un « technicien informatique » demande un mot de passe, il peut être utile d'appeler directement le service informatique en utilisant un numéro de téléphone officiel, plutôt que celui fourni par le prétendu technicien.

3. Culture de la sécurité
Il est essentiel de créer un environnement de travail dans lequel chacun se sent responsable de la sécurité. Il faut encourager le signalement de comportements ou de demandes suspects. Personne ne doit se sentir mal à l'aise en disant « cette demande semble étrange » ou en demandant un deuxième avis.

4. Protéger les appareils
Ne laissez jamais les ordinateurs portables, les smartphones ou les appareils de l'entreprise sans surveillance, en particulier dans les espaces partagés ou publics. Utilisez des verrous d'écran avec des mots de passe ou des codes PIN et veillez à ce que les appareils se verrouillent automatiquement après une période d'inactivité.

5. Authentification à deux facteurs (2FA)
Même si quelqu'un parvient à obtenir un mot de passe de connexion, l'authentification à deux facteurs ajoute un niveau de sécurité supplémentaire. Cet outil, qui exige une deuxième étape pour confirmer l'identité de l'utilisateur, est essentiel pour protéger les comptes d'entreprise.

6. Accès physique contrôlé
Veillez à ce que seules les personnes autorisées aient accès aux bureaux ou aux zones sensibles. Des systèmes tels que les badges personnels, les caméras de surveillance et les portes équipées de serrures électroniques sont des outils efficaces pour prévenir les intrusions physiques.

7. Attention aux signaux d'alarme
Faites attention aux détails. Les courriels contenant des fautes de grammaire, des demandes inhabituelles ou des expéditeurs inconnus sont souvent des signaux d'alarme. Avant de cliquer sur un lien ou de télécharger une pièce jointe, demandez-vous toujours si la demande a un sens. En cas de doute, mieux vaut ne pas prendre de risques.

8. Tests et audits périodiques
Effectuez régulièrement des audits de sécurité et des tests d'intrusion pour identifier les vulnérabilités dans les systèmes et les processus. Ces tests peuvent révéler des faiblesses qui pourraient autrement être exploitées par les cybercriminels.

Conclusion
L'ingénierie sociale est une menace insidieuse, mais pas invincible. Être conscient de la façon dont les criminels agissent et adopter de bonnes pratiques peut réduire considérablement les risques. Sur le lieu de travail, investir dans la formation des employés, promouvoir une culture de sécurité et utiliser les outils appropriés sont des étapes clés pour protéger les informations sensibles et les systèmes critiques. Souvent, la sécurité ne dépend pas seulement de la technologie, mais aussi de notre capacité à reconnaître les pièges.

LES MENACES INVISIBLES : LA CROISSANCE DES CYBERATTAQUES

Introduction

À l'ère numérique, les cybermenaces sont devenues un danger de plus en plus sophistiqué et difficile à détecter. Les organisations de tous les secteurs sont confrontées à des attaques visant les données sensibles, la continuité des activités et la réputation de l'entreprise. La multiplication de ces attaques entraîne non seulement des dommages économiques directs, mais aussi une perte de confiance de la part des clients et des partenaires. Cet article analyse les principales cybermenaces, les défis économiques qu'elles posent aux entreprises et les stratégies pour se défendre efficacement.

1. Les principales cybermenaces

Les cyberattaques sont en constante évolution et exploitent les vulnérabilités technologiques et humaines. Les menaces les plus répandues sont les suivantes :

- Ransomware : logiciel malveillant qui crypte les données de l'entreprise et en bloque l'accès jusqu'à ce qu'une rançon soit exigée.

- Phishing et Spear Phishing : courriels frauduleux visant à voler des informations d'identification et des données sensibles par le biais de l'ingénierie sociale.

- Attaques de type « Zero-Day » : elles exploitent des vulnérabilités encore inconnues dans les logiciels, visant à frapper la victime avant qu'elles ne soient corrigées par les fabricants.

- Logiciels malveillants et chevaux de Troie : programmes malveillants qui s'infiltrent dans les systèmes pour voler des informations ou permettre un accès non autorisé.

- Déni de service (DoS) et déni de service distribué (DDoS) : attaques qui surchargent les serveurs des entreprises, les rendant inaccessibles aux utilisateurs légitimes.

- Vol d'identifiants et violation de données : techniques d'attaque qui compromettent les identifiants de l'entreprise pour accéder à des systèmes confidentiels.

2. Les défis économiques pour les organisations

Les cyberattaques ne compromettent pas seulement les systèmes IT, elles ont aussi un impact économique important. Les principales conséquences sont les suivantes :

- Les coûts de récupération : les entreprises touchées doivent investir dans des expertises, la restauration des données et le renforcement des mesures de sécurité.

- Pénalités et poursuites judiciaires : des Réglementations telles que le GDPR prévoient de lourdes pénalités en cas de violation des données personnelles.

- Atteinte à la réputation : la perte de confiance des clients et des partenaires peut réduire considérablement la valeur du brand.

- Interruption des opérations : une attaque réussie peut paralyser les opérations commerciales pendant des jours ou des semaines, ce qui entraîne des pertes économiques importantes.

3. Stratégies de défense et solutions

Pour limiter les risques, les organisations doivent adopter une stratégie proactive en matière de cybersécurité. Voici quelques mesures clés :

- Formation et sensibilisation : la sensibilisation des employés aux cybermenaces réduit le risque d'attaques basées sur la tromperie humaine.

- Mise en place d'une authentification multifactorielle (MFA) : l'ajout d'un niveau de sécurité supplémentaire aux accès réduit le risque de compromission des comptes.

- **Mises à jour et patchs de sécurité :** maintenir les logiciels et les systèmes d'exploitation à jour pour se protéger contre les « exploit ».

- Sauvegardes régulières et chiffrées : faites des sauvegardes fréquentes et stockez-les dans des endroits sûrs pour garantir une récupération rapide en cas d'attaque.

- Surveillance continue et Threat intelligence : utiliser des outils avancés de détection des menaces pour repérer les comportements suspects et y réagir rapidement.

- Pare-feux et systèmes de prévention des intrusions (IDS/IPS) : protéger le réseau de l'entreprise contre les accès non autorisés et les attaques extérieures.

- Zero Trust Architecture : adopter un modèle de sécurité qui ne fait confiance à aucun accès et exige des vérifications constantes pour chaque transaction de données.

Conclusion

Les cyberattaques constituent une menace en constante évolution, qui a des répercussions importantes sur les entreprises en termes de sécurité et de coûts économiques. Adopter une approche proactive de la cybersécurité, investir dans la protection des données et former le personnel sont des étapes essentielles pour se défendre contre les menaces invisibles du monde numérique. Ce n'est qu'avec une stratégie intégrée et une vigilance constante que l'infrastructure de l'entreprise peut être protégée efficacement et que la résilience opérationnelle peut être assurée.

CYBERSÉCURITÉ DANS LES GOUVERNEMENTS : MENACES GLOBALES ET STRATÉGIES DE DÉFENSE

Ces dernières années, la numérisation a profondément transformé le fonctionnement des gouvernements, apportant de nouvelles opportunités mais aussi de nouvelles vulnérabilités. La cybersécurité est devenue un pilier fondamental de la stabilité nationale, les administrations publiques devant faire face à des cyberattaques de plus en plus sophistiquées et ciblées. La gestion des données sensibles, le contrôle des infrastructures critiques et la fourniture de services essentiels exposent les entités gouvernementales à des attaques cybernétiques aux répercussions géopolitiques, économiques et sociales.

Le coût des attaques informatiques dans le secteur public ne cesse d'augmenter, avec des études révélant un impact financier s'élevant à plusieurs milliards de dollars chaque année. Un exemple emblématique est celui du service de santé irlandais, paralysé en 2023 par une attaque par ransomware, ayant entraîné des dommages estimés à plus de cent millions d'euros. Des incidents de cette ampleur ne se limitent pas à des conséquences économiques, mais ils soulèvent également des enjeux cruciaux de confiance et de sécurité publique. Lorsque les données personnelles des citoyens sont compromises, le sentiment de vulnérabilité se diffuse rapidement, ébranlant la relation de confiance entre l'État et ses administrés.

La réputation d'un gouvernement peut être gravement compromise par une violation de la sécurité informatique. En 2020, une attaque contre les systèmes de santé norvégiens a exposé les données personnelles de près de trois millions de citoyens, entraînant une chute significative de l'adhésion aux services numériques publics. La crainte que les informations personnelles puissent être dérobées ou altérées freine l'innovation et entrave l'adoption des technologies numériques, avec des répercussions directes sur la modernisation de l'administration publique et de toute organisation gouvernementale.

Les stratégies de défense nécessitent une approche multiniveau, dans laquelle la prévention et la réponse aux incidents jouent un rôle déterminant. De nombreux systèmes utilisés par les organismes gouvernementaux sont technologiquement obsolètes, un facteur qui accroît considérablement le risque d'attaque. La modernisation des infrastructures informatiques doit ainsi devenir une priorité, accompagnée de politiques de sécurité strictes et de la formation continue du personnel. L'erreur humaine demeure en effet l'une des principales causes d'attaque informatique, rendant indispensables les programmes de sensibilisation et de simulation d'attaques pour renforcer les capacités de réaction face aux menaces.

La cybersécurité n'est pas uniquement un enjeu technique, mais une question de sécurité nationale. Les attaques contre des infrastructures critiques peuvent avoir des conséquences dévastatrices, comme l'a démontré l'affaire du Colonial Pipeline aux États-Unis, où une attaque informatique a interrompu l'approvisionnement en carburant de régions entières. La coopération internationale est essentielle pour faire face aux menaces à grande échelle, les cybercriminels opérant sans frontières. Le partage d'informations entre gouvernements et agences de sécurité permet d'anticiper les menaces et d'améliorer la résilience globale.

Le paysage de la cybersécurité gouvernementale est en constante évolution, avec des menaces qui s'adaptent rapidement aux nouvelles mesures de défense. Investir dans la protection des données et des infrastructures critiques n'est plus une option, mais une nécessité absolue pour garantir la stabilité et la sécurité des institutions. Dans un monde toujours plus interconnecté, protéger le cyberespace revient à protéger la démocratie elle-même.

Valerio Mercuri

LES JEUNES, ACTEURS DE L'ÉTHIQUE MONDIALE : CYBERDIPLOMATIE, DROIT, ÉCONOMIE ET TECHNOLOGIE DANS UN MONDE INTERCONNECTÉ

Comment distinguer un fait réel d'un deepfake ? Qui peut garantir qu'un algorithme ne manipule pas l'opinion publique ? Ces interrogations ont nourri le débat « Cyberdiplomatie, droit, économie et technologie dans un monde interconnecté – IA et avenir des institutions », organisé par la Direction des télécommunications et des services informatiques. À travers des présentations, des données et des études de cas concrets, étudiants et enseignants ont réfléchi à une problématique essentielle : dans un monde hyperconnecté, où l'intelligence artificielle (IA) peut créer ou effacer la vérité en quelques clics, l'éthique et le savoir constituent les seuls remparts contre la désinformation.

A et post-vérité : quand la technologie défie la perception

Au cœur du débat, l'impact juridique et économique de la cybercriminalité, ainsi que le rôle de l'intelligence artificielle dans la construction de la réalité. Les cyberattaques ne constituent pas uniquement une menace technologique : elles représentent un enchevêtrement de défis juridiques, de coûts économiques exponentiels et de risques en termes de réputation. Sur le plan juridique, les conflits de juridiction – tels que la tension entre le RGPD européen et le Cloud Act américain – compliquent la poursuite des délits numériques. Par ailleurs, l'absence de traités internationaux contraignants crée des zones d'ombre exploitées aussi bien par des groupes de hackers que par des États dits « voyous ».

Le coût économique est tout aussi préoccupant : selon des estimations récentes, la cybercriminalité coûte 8 000 milliards de dollars par an à l'économie mondiale — un chiffre appelé à croître avec l'avènement de l'informatique quantique et la multiplication des attaques contre les chaînes d'approvisionnement (supply chains). Des incidents comme l'attaque par ransomware contre Colonial Pipeline (2021), qui a paralysé l'acheminement de carburant aux États-Unis, ont engendré des pertes directes de 4,4 millions de dollars, sans compter les effets indirects de perte de confiance des consommateurs.

Des outils tels que les deepfakes vocaux ou les vidéos synthétiques menacent également de saper la confiance dans les institutions : en 2023, de faux enregistrements audio attribués à des responsables politiques ont provoqué des troubles sur les marchés financiers. Toutefois, l'IA peut aussi devenir une alliée : des algorithmes de fact-checking (vérification des faits) et des systèmes de détection de contenus manipulés offrent des perspectives concrètes de régulation. « Le problème, ce n'est pas la technologie, mais l'usage qu'on en fait ». « Il faut des règles claires : un deepfake utilisé dans un film relève de la création artistique ; utilisé pour manipuler une élection, c'est un crime ».

Sagesse numérique : pourquoi la connaissance constitue un patrimoine à protéger

Si les données sont le « nouveau pétrole », la capacité à les interpréter en constitue la véritable richesse et leur protection est le grand défi de notre époque. Les interventions ont mis en lumière le fait que les universités et les centres de recherche doivent former les jeunes non seulement à coder des algorithmes, mais aussi à réfléchir à leurs implications sociales. Un exemple ? Le Règlement général sur la protection des données (RGPD) européen, qui encadre strictement l'usage des données sensibles, découle d'une vision éthique : protéger les individus et pas seulement les infrastructures informatiques. « La sagesse numérique, c'est savoir trouver un équilibre entre l'innovation et les

droits ». Le cas Cambridge Analytica a été présenté comme emblématique d'un droit encore immature face à des vols de données qui ont influencé des campagnes électorales, tandis que des cyberattaques systémiques, parfois orchestrées par des États, ont eu des conséquences socio-économiques dramatiques.

Réputation et cybersécurité : replacer l'homme au centre

Aujourd'hui, la réputation d'un État ou d'une entreprise se joue en ligne. Des cyberattaques comme celle visant SolarWinds en 2020 — qui a compromis des données sensibles de plusieurs agences gouvernementales américaines — démontrent qu'un simple malware peut causer plus de dégâts qu'un missile. Mais la réponse ne peut pas être uniquement technologique : « Un pare-feu ne peut pas arrêter la manipulation de l'information ». De véritables stratégies holistiques sont nécessaires :

• Des plateformes numériques transparentes, capables de lutter contre la désinformation sans recourir à la censure ;
• Une éducation généralisée à la pensée critique, afin de reconnaître une fake news ;
• Une coopération et une législation internationales représentent la nouvelle frontière sur laquelle se concentrer.

Le rôle des jeunes : gardiens d'un avenir « humain »

En conclusion, un appel a été lancé aux natifs du numérique : « Nous sommes face à la première génération capable d'utiliser l'intelligence artificielle pour amplifier la connaissance et non pour diviser ». Les exemples concrets ne manquent pas : des start-up dirigées par des moins de 30 ans développent des outils permettant de vérifier les sources journalistiques, tandis que d'autres conçoivent des chatbots éthiques, programmés pour refuser de produire des discours de haine.

La rencontre a laissé des messages simples, mais urgents : à une époque où l'intelligence artificielle peut rendre le faux plus convaincant que le vrai, défendre la vérité devient une responsabilité collective. La cyberdiplomatie est essentielle pour atténuer les impacts politico-économiques aux conséquences sociales potentiellement dévastatrices.

Et ce sont les jeunes — forts de leur familiarité avec les technologies et de leur sensibilité aux valeurs — qui sont appelés à mener cette bataille silencieuse, à la réguler et à en faire une norme. Non pas avec des discours catastrophistes, mais à travers des choix quotidiens, concrets et technologiques : partager une information uniquement après l'avoir vérifiée, exiger des algorithmes transparents, défendre le savoir comme un bien commun. Car, comme le rappelle un proverbe adapté à l'ère numérique : « La vérité est comme l'eau : elle trouve toujours son chemin. Mais il faut quelqu'un pour nettoyer les berges ».

Valerio Mercuri