CYBERATTAQUES

LA PRISE DE CONSCIENCE N'EST PLUS UNE OPTION

CYBERATTAQUES

LA PRISE DE CONSCIENCE N'EST PLUS UNE OPTION

CHAPITRE 1 – LE SCÉNARIO

1.1 La transformation numérique et ses pièges 05
1.2 Les cyberattaques : des « fissures » psychologiques et technologiques 08
1.3 La guerre : non seulement sur le front, mais aussi dans le cyberespace 11
1.4 Au-delà du phishing et des malwares 13
1.5 À l'ère du numérique, la sécurité n'est pas une option 16

CHAPITRE 2 – LA FORMATION

2.1 Une mesure de sécurité nécessaire 19
2.2 Le rôle de la formation 22
2.3 Méthodologie efficace 25
2.4 Formation continue 28
2.5 Participation à la formation 31
2.6 Gamification 34
2.7 Engagement 36

CHAPITRE 3 - CYBER GURU

3.1 La plateforme de sensibilisation à la sécurité 37
3.2 Cyber Guru Awareness 40
3.3 Cyber Guru Phishing 42
3.4 Cyber Guru Channel 45

RÉSUMÉ ANALYTIQUE

La croissance exponentielle des cyberattaques réussies contre des individus et des organisations, dont la cause originelle peut être attribuée à une erreur humaine, a définitivement levé tout doute quant au maillon faible de la chaîne de défense de chaque organisation.

LA TENDANCE DES CYBERATTAQUES EST À LA HAUSSE, RAPIDE ET CONTINUE.

LA CYBERSÉCURITÉ EST UN PROBLÈME TRANSVERSAL QUI CONCERNE L'ENSEMBLE DU PAYS ET QUI TOUCHE INDIFFÉREMMENT LES INDIVIDUS ET LES ORGANISATIONS DE TOUT TYPE

Le facteur humain, rendu encore plus vulnérable par l'effet pandémique, est aujourd'hui le **principal vecteur** utilisé par la **cybercriminalité** pour s'insinuer au sein des organisations, avec des stratégies offensives de plus en plus sophistiquées.
Ce sont précisément les utilisateurs, avec leurs comportements inadaptés à la complexité du défi, qui laissent inconsciemment le champ libre aux attaquants.

La tendance était déjà très marquée avant la pandémie. Si l'on part de 2020 en analysant les différents rapports qui concernent l'état de la cybersécurité, tant au niveau italien qu'au niveau mondial, la tendance qui émerge est que la **croissance des cyberattaques** semble **imparable** et que parmi les différentes techniques d'attaque utilisées, celles qui se caractérisent par une plus grande croissance s'appuient principalement sur le facteur humain. Une confirmation supplémentaire que la grande majorité des cyberattaques ont une matrice humaine, attribuable à une action incorrecte de la part d'un utilisateur.

L'irruption dans le scénario économique et social de la pandémie de coronavirus n'a fait qu'exacerber cette situation, augmentant le nombre d'attaques. Ces dernières années, l'action des cybercriminels s'est de plus en plus concentrée sur les individus qui, face au phénomène pandémique et à ses principales conséquences, comme le recours massif au smart working, se sont avérés beaucoup plus vulnérables que les organisations n'auraient pu l'imaginer.

La **presse** abonde **de cyberattaques** réussies, qui ont touché des organisations de tous les secteurs et de toutes les tailles. Des marques prestigieuses et d'autres moins connues ont vu leurs activités de production bloquées et leur réputation compromise. Même le vieux refrain souvent cité par de nombreuses PME : « nous ne sommes pas attractifs pour un hacker » a été démenti par les faits.

Il s'agit d'une véritable **cyberguerre**. Une guerre asymétrique qui voit les **attaquants** dans une **position** d' **avantage incontestable**, d'autant plus que la première ligne de défense est constituée de civils sans défense qui, dans la plupart des cas, ne se rendent pas compte qu'ils sont attaqués.

Ces dernières années, les **capacités de défense** au niveau technologique ont sans aucun doute augmenté, mais l'efficacité de ces investissements est constamment réduite à néant, en vertu de la théorie du **maillon faible** selon laquelle la « **force globale d'une chaîne est déterminée par son maillon le plus faible** ». Lorsque le maillon faible, comme dans ce cas, est représenté par les utilisateurs qui interagissent avec les technologies numériques et avec le réseau internet, il apparaît clairement que les investissements technologiques ne sont plus suffisants pour arrêter les attaques.

La seule façon de recréer une symétrie entre attaquants et défenseurs, c'est d'**investir** sur la **«première ligne de défense»**, c'est-à-dire sur les **utilisateurs numériques**. Chaque organisation doit mettre en place **des programmes de sensibilisation à la cybersécurité efficaces** et **innovants**. Mais la guerre ne pourra être gagnée que si ces investissements démontrent toute leur efficacité sur le plan de la formation, avec des programmes capables d'influer concrètement sur les comportements humains.

Ces dernières années, les investissements souvent insuffisants réalisés dans ce domaine ont été davantage motivés par la nécessité d'atteindre un degré minimum de conformité réglementaire que d'atteindre des objectifs de protection efficaces contre les cyberattaques.

Par ailleurs, tous les principaux cadres et réglementations qui font explicitement référence à la cybersécurité (par exemple RGPD, NIST, Directive NIS, AGID […]) ont mis en évidence la question de la formation des utilisateurs finaux, tout en laissant une large marge d'interprétation aux organisations pour déterminer ce qui était nécessaire pour atteindre la conformité à ces exigences.

Un espace si vaste que les initiatives mises en œuvre se sont avérées fonctionnelles par rapport à la nécessité de se conformer aux réglementations, mais absolument inefficaces par rapport à l'objectif réel : **accroître la protection des individus** et des **organisations** contre le cyberrisque.

LE CYBER-RISQUE EST L'UN DES RISQUES LES PLUS IMPORTANTS AUXQUELS LES ENTREPRISES SERONT CONFRONTÉES D'ICI LES ANNÉES À VENIR.

LES CYBERATTAQUES S'APPUIENT DE PLUS EN PLUS SUR LA COMPOSANTE HUMAINE, VÉRITABLE MAILLON FAIBLE DE LA CHAÎNE DE DÉFENSE.

Pour ces raisons, il est donc essentiel de lancer des **programmes de sensibilisation à la cybersécurité efficaces** et **innovants**, capables d' **influencer** les **comportements humains** et de faire des utilisateurs la première ligne de défense des organisations.

C'EST DEPUIS LE DÉBUT LA MISSION SPÉCIFIQUE DE CYBER GURU : CONSTRUIRE UNE PLATEFORME DE SENSIBILISATION À LA CYBERSÉCURITÉ POUVANT CONCRÈTEMENT AIDER SES CLIENTS À RENFORCER LE MAILLON FAIBLE DE LA CHAÎNE DE LA CYBERSÉCURITÉ.

LA PLATEFORME CYBER GURU A ÉTÉ RÉALISÉE ET CONTINUELLEMENT MISE EN ŒUVRE, UTILISANT LES TECHNOLOGIES, PROCESSUS DE PRODUCTION ET MÉTHODOLOGIES PÉDAGOGIQUES LES PLUS AVANCÉS POUR ASSURER UNE IMPLICATION MAXIMALE DES UTILISATEURS ET ATTEINDRE L'OBJECTIF PRINCIPAL D'UN PROGRAMME DE SENSIBILISATION À LA SÉCURITÉ : LA PROTECTION DES CYBERRISQUES.

1. LE SCÉNARIO

1.1 LA TRANSFORMATION NUMÉRIQUE ET SES PIÈGES

RÉSUMÉ

Nous pouvons dire que 2021 a structuré le bouleversement social et économique déclenché par la pandémie, l'année précédente, le transformant en une situation d'alerte chronique sur tous les fronts.
La transformation numérique forcée intervenue en 2020 et gérée de **manière urgente est** devenue **une réalité consolidée** à laquelle la collectivité doit faire face, pour le meilleur et pour le pire. L'une des conséquences les plus évidentes a été la croissance des cyberattaques, qui ont survolé la vague de l'année précédente en continuant à exploiter les vulnérabilités psychologiques, ainsi que l'écart entre le processus de numérisation accéléré et la sensibilisation des utilisateurs aux cybermenaces, qui n'est toujours pas comblé.

CES DEUX DERNIÈRES ANNÉES QUE NOUS AVONS VÉCUES RESTERONT SANS AUCUN DOUTE DANS LES LIVRES D'HISTOIRE COMME LES ANNÉES DE LA **PANDÉMIE DE COVID 19** ET DE TOUTES LES TRANSFORMATIONS CAPITALES QUE LA COMMUNAUTÉ A CONNUES PAR LA SUITE.

AUX PREMIÈRES PLACES, IL Y A LE **REPOSITIONNEMENT** DE **NOTRE VIE** SUR LE WEB. SI, AVANT LA COVID, SEULE UNE PARTIE DE CELLE-CI SE CONFRONTAIT QUOTIDIENNEMENT AU RÉSEAU, AUJOURD'HUI, ON PEUT DIRE QUE LE WEB GÈRE LA PLUPART DE NOS JOURNÉES.

Du travail, à l'école, aux relations sociales, au shopping, à l'information. Aujourd'hui, on ne peut plus se passer du web dans toutes ses déclinaisons. Cela a été une occasion parfaite pour tous ceux qui font de **l'arnaque informatique** leur métier et ainsi les **attaques de pirates** sont devenues une **réalité très répandue** et tout aussi dangereuse.

Au point d'être qualifiée d'« **arme la plus dangereuse au monde** » par **JP Morgan** à l'occasion de son International Council qui s'est tenu en décembre dernier, et d'être identifiée comme « la plus grande menace pour la stabilité financière, avec le changement climatique », par Christine Lagarde, lors de la conférence annuelle du European Systemic Risk Board (ESRB). Des affirmations qui tirent la sonnette d'alarme et qui sont malheureusement confirmées par les données.

Selon le **rapport Clusit** 2022 sur la **cybersécurité**, au cours des 4 dernières années, la moyenne mensuelle des attaques graves dans le monde est passée de 130 à 171, entraînant une croissance dramatique des pertes qui sont passées de 1 000 milliards de dollars en 2020 à 6 000 milliards en 2021, avec un taux d'aggravation annuel à 2 chiffres et une valeur égale à 4 fois le PIB italien.

Une escalade due principalement à **l'utilisation massive** du **smart working** qui, dans l'urgence, est devenu dans de nombreuses situations un nouveau mode de travail, mais aussi à l'adoption de plus en plus fréquente de l'enseignement à distance et des méthodes de formation en ligne et, surtout, au recours à des plateformes de collaboration sociale et de divertissement numérique.

Un signe incontestable de cette transformation rapide se trouve également dans la **croissance** des **achats en ligne** qui, selon les données du rapport de Salesforce Shopping Index, pour le premier trimestre 2021, a connu une **augmentation globale de** 58 % sur une base annuelle contre 17 % au premier trimestre 2020.

NOUS VOUS RAPPELONS QUE DANS LE **COMMERCE EN LIGNE**, DES MÉTHODES DE PAIEMENT TELLES QUE LES CARTES DE CRÉDIT ENTRENT EN JEU, DONT LES DONNÉES SONT PARTICULIÈREMENT ATTRAYANTES POUR LES **CYBERCRIMINELS**. CONFIRMANT LA NUMÉRISATION ACCRUE DE LA SOCIÉTÉ, NOUS NE POUVONS PAS NE PAS SOULIGNER ÉGALEMENT L'AUGMENTATION CONSIDÉRABLE DE L'UTILISATION DE LA BANDE PASSANTE. AU COURS DES PREMIERS MOIS DE LA PANDÉMIE, DE NOMBREUX OPÉRATEURS DE SERVICES DE RÉSEAU ONT ENREGISTRÉ DES AUGMENTATIONS TELLES QU'ILS CRAIGNAIENT DES SCÉNARIOS CATASTROPHE SUR LA RÉSISTANCE D'INTERNET.

Avec l'Italie comme protagoniste, enregistrant une hausse de 78 % qui la place au premier rang en Europe et au quatrième rang dans le monde, après le Canada, les Pays-Bas et le Royaume-Uni. Un **saut technologique** qui a sans aucun doute représenté et représente une grande opportunité sur la voie de l'innovation mais qui, en revanche, peut réserver des atterrissages brusques sinon traumatisants.

Le fait est que tout cela s'est produit sans une croissance correspondante de la **culture numérique** et donc sans une véritable capacité des utilisateurs à profiter des technologies numériques et du réseau internet en toute sécurité. Une absence de conscience des menaces provenant du monde numérique, qui n'a pas encore été comblée et qui continue donc à offrir de grandes opportunités aux entreprises cybercriminelles.

1.2 **LES CYBERATTAQUES°:** PDES «°FISSURES°» PSYCHOLOGIQUES ET TECHNOLOGIQUES

RÉSUMÉ

La **situation particulière** générée par la **pandémie** est à l'origine de la **croissance** des **cyberattaques** qui a commencé en 2020 et s'est poursuivie en 2021. De ce point de vue, il faut tenir compte à la fois des **vulnérabilités technologiques**, liées au smart working, à l'augmentation de toutes les activités en ligne et à l'utilisation de nouveaux outils digitaux tels que les codes QR, et des vulnérabilités **psychologiques**, liées aux **états d'urgence** continus et à la situation de distanciation sociale. Deux « fissures » importantes dans lesquelles le crime s'est facilement infiltré, entraînant des attaques qui ont eu un impact considérable sur de nombreuses organisations. La presse n'a eu cesse de relater des cas emblématiques relatifs à des organisations de tout type et de toute dimension, qui ont vu leur capacité à opérer sur des périodes plus ou moins longues, avec toutes les conséquences, économiques et d'image, qu'un arrêt de ce type peut entraîner.

LA **PANDÉMIE** DE **COVID-19** A EU UN **EFFET PERTURBATEUR** NON SEULEMENT SUR LE PLAN ÉCONOMIQUE ET SOCIAL, MAIS AUSSI SUR **L'ACCÉLÉRATION** DES **CYBERATTAQUES** CLASSÉES COMME **GRAVES**.

Une tendance déjà fortement enregistrée en 2020 et qui a connu une forte hausse en 2021. Le rapport Clusit, dévoilé en début d'année, parle de cas graves en hausse et d'une Europe de plus en plus au centre des attaques des cybercriminels : + 22 % contre 16 % en 2020 et 11 % en 2019.

L'augmentation quantitative s'ajoute à l'augmentation qualitative car les **dommages** sont beaucoup plus **graves** pour les **entreprises affectées**. En général, au cours des quatre années 2018-2021, le nombre d'attaques graves analysées par le Clusit a augmenté de 32 % et parmi les catégories les plus touchées, il y a les services publics (15 %) suivi par les TIC et les cibles multiples.

Selon les données sur la **gravité des attaques**, celles de niveau critique représentaient 32 %, de haut niveau 47 %, de niveau moyen 19 % et de bas niveau seulement 2 %.
Sur l'ensemble des données, la gravité critique et élevée des attaques a donc atteint 80 %, contre 56 % l'année précédente.

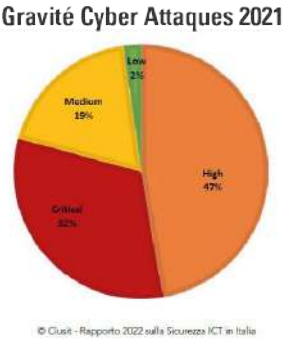
En outre, une récente étude produite par IBM Security, **Cost of a Data Breach Report 2021**, a montré que les attaques contre la cybersécurité ont entraîné, au cours de l'année qui vient de s'achever, les coûts les plus élevés jamais associés aux violations de données au cours des 17 années d'histoire du rapport, avec une moyenne de 4,24 millions de dollars par incident. Bref, si la tendance devait se poursuivre ainsi, les perspectives ne seraient certainement pas roses.

LES PRINCIPAUX **MOTEURS** DE L'ACCÉLÉRATION DES **CYBERATTAQUES SONT** TOUJOURS ANCRÉS DANS LES TRANSFORMATIONS INDUITES PAR LA PANDÉMIE. L'UN DE CES MOTEURS EST DE TYPE **PSYCHOLOGIQUE** LIÉ À L'EFFET SUR LA PSYCHÉ HUMAINE DE LA SITUATION D'URGENCE, L'AUTRE DE TYPE **TECHNOLOGIQUE** IMPUTABLE À L'APPLICATION MASSIVE DE FORMES DE TÉLÉTRAVAIL ET À L'UTILISATION ACCRUE DU RÉSEAU POUR LES ACTIVITÉS QUOTIDIENNES.

Le **niveau psychologique** a généré des états d'anxiété et de peur typiques des urgences, avec la **perte** des **repères traditionnels**, la recherche obsessionnelle de nouvelles et d'informations et la difficulté de discerner entre les informations vraies et fausses, difficulté soulignée également en raison des techniques avancées de construction des **Fake News**.

En s'appuyant sur ces états anxieux beaucoup plus répandus dans la population qu'à l'époque pré-covid, on a multiplié les **campagnes** de **phishing** qui ont eu pour objet les thèmes du Covid dans toutes ses déclinaisons : les différentes variantes du virus, le pass sanitaire et toutes les informations, souvent alarmistes, qui ont tourné autour de la pandémie.

L'utilisateur s'est ensuite trouvé plus isolé et plus enclin à perdre ses repères habituels au sein de l'entreprise ou de l'organisation, difficiles à retrouver avec la seule utilisation des outils de collaboration sociale.
En outre, dans le contexte spécifique généré par la pandémie, les espaces domestiques ont souvent été et sont encore partagés avec d'autres membres de la famille qui opèrent de la même manière, à la fois pour des raisons professionnelles et pour des raisons éducatives, créant ainsi des conditions critiques du point de vue de la sécurité informatique.



LE PARTAGE DES APPAREILS, DU RÉSEAU, MAIS AUSSI L'ACTION INCONSCIENTE DUE À DES PHÉNOMÈNES INDUITS PAR LA DISTRACTION, DEVIENNENT DES ÉLÉMENTS QUI JOUENT AU PROFIT DE LA CRIMINALITÉ.

Étant donné que le **maillon faible** est toujours le **comportement humain**, dans une situation d'alerte sanitaire généralisée, l'attention aux bons comportements à tenir en ligne a été pénalisée, ouvrant ainsi les portes aux **cybercriminels** qui, en tant que connaisseurs raffinés de la psyché humaine, **se glissent précisément dans** les **fissures** des **émotions**.

À cela s'ajoute le **niveau technologique**: le smart working repose sur une architecture complexe qui fait souvent appel aux appareils privés de l'utilisateur, moins sécurisés par définition et dotés de configurations matérielles.
Là encore, c'est le facteur humain qui inquiète le plus, car l'écart qui existe entre la **rapidité** du **processus** de **transformation numérique** et celle de **l'adaptation** des personnes à cette nouvelle dimension socio-économique reste, aujourd'hui encore, à l'avantage de la cybercriminalité.

Il suffit de penser aux **risques qui sont apparus** avec l'augmentation massive de l'utilisation des **codes QR**, de plus en plus souvent utilisés pour résoudre des problèmes liés aux restrictions pandémiques ou pour fournir des services plus innovants et efficaces.

Un outil qui, comme toute technologie, peut grandement faciliter la vie de tous les jours, mais qui doit être « manipulé » avec soin car il peut **cacher des pièges dangereux**, tels que des **logiciels malveillants** ou **des sites frauduleux**. Le fait que la majorité des utilisateurs soient mal informés sur les aspects opaques des QR codes, et des outils numériques en général, offre facilement un boulevard aux hackers toujours à la recherche de nouveaux moyens d'accéder à leur crime favori.

1.3 **LA GUERRE :** PAS SEULEMENT SUR LE FRONT MAIS AUSSI DANS LE CYBERESPACE

RÉSUMÉ

Pour compliquer cette situation déjà dramatique s'est ajoutée, au début de cette année, la **guerre** en **Ukraine**, qui a ouvert de nouveaux scénarios sur le front de la **cybersécurité**. À côté de la guerre traditionnelle, celle faite avec les armes à feu et les obus, on est en train de mener une autre **guerre**, la **cybernétique**, faite avec un autre type d'armes et qui a de fortes répercussions au niveau mondial. Mais les effets ne sont pas encore quantifiables et se verront probablement dans quelques mois, voire des années.

Selon CheckPoint , **les attaques** contre les services de l'État et l'Armée depuis le début des hostilités ont déjà augmenté de 21 % dans le monde.
Un signe indubitable de la façon dont le conflit russo-ukrainien est à tous égards un conflit global et pas seulement confiné dans l'espace géographique des deux pays protagonistes.

Dans ce scénario, aucun pays européen ne peut être rassuré, étant donné les nombreuses **voix institutionnelles** qui ont récemment lancé un **cri d'alarme** sur la vulnérabilité informatique de leurs pays en indiquant la cyberguerre comme l'un des plus grands risques qui peuvent nous impliquer.

Les cas d'attaques de pirates exploitant les **craintes** de la **guerre** en cours sont de plus en plus fréquents. Les entreprises manufacturières européennes ont été les premières visées par les hackers, victimes de cette guerre et ciblées par une campagne de phishing avec pour objet **«Supplier Survey : Effect of supply chain from the Ukraine/Russia conflict»**. Dans l'e-mail, les pirates, sous une fausse identité, ont exhorté les destinataires à remplir un formulaire joint, contenant manifestement des logiciels malveillants, pour signaler tout retard et plan de sauvegarde.

Un terrain fertile qui exploite les craintes provoquées par la guerre et les lourds impacts d'approvisionnement. Sans parler des différentes vagues de spam et de phishing, dans lesquelles les **cybercriminels** se faisant passer pour des **agences humanitaires** ou des **institutions ukrainiennes**, ont fait circuler en Europe et aux États-Unis des campagnes de charité et de collecte de fonds, dans le seul but de voler de l'argent.

Mais ces quelques exemples dont nous avons parlé ne sont certainement pas une représentation exhaustive d'une situation dynamique et en mouvement continu qui pourrait conduire à des bouleversements du scénario géopolitique, financier, des équilibres économiques, ce qui aura certainement des conséquences sur la cybersécurité, mais dont les effets se verront probablement dans quelques mois, peut-être des années.

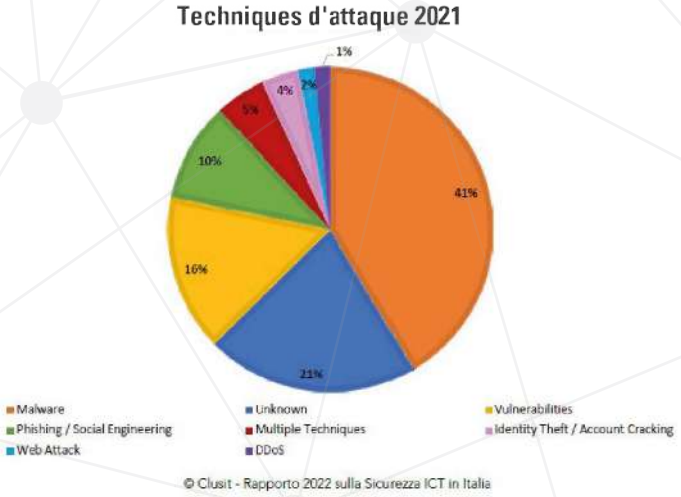
L'AGENCE POUR LA **CYBERSÉCURITÉ NATIONALE** EN ITALIE A SURENCHÉRI EN AVERTISSANT LES ENTREPRISES DE **L'URGENCE** DE « PROCÉDER À UNE ANALYSE DES RISQUES DÉCOULANT DES **SOLUTIONS** DE **SÉCURITÉ INFORMATIQUE** UTILISÉES ET D'ENVISAGER L'APPLICATION DE STRATÉGIES DE DIVERSIFICATION APPROPRIÉES EN CE QUI CONCERNE, NOTAMMENT : ANTIVIRUS, WEB APPLICATION, PARE-FEU, PROTECTION DU COURRIER ÉLECTRONIQUE, PROTECTION DES SERVICES CLOUD, SERVICES DE SÉCURITÉ GÉRÉS ».

1.4 AU-DELÀ DU PHISHING ET DES MALWARES

RÉSUMÉ

Si la plupart des projecteurs continuent d'être braqués sur les malwares et, bien sûr, le phishing, nous avons déjà dit que toutes les autres formes d'attaques liées à la variété des « fissures », ou vulnérabilités, dans lesquelles les criminels parviennent à se faufiler pour nuire ou extorquer des données ou de l'argent aux particuliers et aux entreprises, ont littéralement explosé au cours de l'année écoulée. Parmi celles-ci, il y a sans aucun doute celle liée à **l'intelligence artificielle et l'IoT (internet of things), Internet des objets.**

CE QUI RESSORT DE L'ANALYSE DES NOUVEAUX MODES D'ATTAQUE EN 2021, C'EST QUE LES CYBERCRIMINELS **SONT DE** PLUS EN PLUS **SOPHISTIQUÉS** ET CAPABLES DE SE METTRE EN RÉSEAU AVEC LA CRIMINALITÉ ORGANISÉE. PAR CONSÉQUENT, LES **MENACES** SONT DEVENUES DE PLUS EN PLUS SOURNOISES ET DIFFICILES À DÉTECTER ET DE PLUS EN PLUS CONCENTRÉES SUR L'EXPLOITATION DE TOUS LES POINTS D'ENTRÉE JUGÉS PLUS FAIBLES, Y COMPRIS LES INDIVIDUS.



Le **rapport Clusit** 2021 montre que plus de la moitié des cibles touchées ont été victimes de logiciels malveillants et de leurs vulnérabilités. Essentiellement, les cybercriminels se sont principalement appuyés sur **l'efficacité** des **logiciels malveillants**, désormais fabriqués industriellement à des coûts de plus en plus bas, et sur l'exploitation de tout maillon faible pouvant représenter une opportunité pour leurs objectifs.

Dans cette optique, le **développement rapide** des **technologies numériques** et des applications utilisant l'intelligence artificielle, sans aucun doute une opportunité importante pour toute l'humanité, ne peut pas passer inaperçu. Jusqu'à il y a quelques années, si nous avions vu notre meilleur ami parler au réfrigérateur, nous aurions pensé appeler un médecin ou lui conseiller de prendre des vacances, alors qu'aujourd' hui cela nous semble la chose la plus normale au monde. Oui, parce que nos actions quotidiennes sont de plus en plus liées à des outils d'intelligence artificielle qui remplacent l'homme non seulement dans les actions mais aussi dans la pensée. Il est parfois difficile de savoir où finit l'un et où commence l'autre.

SMART CITY, SMART BUILDING, SMART OFFICE, SMART HOME, SMART DEVICE, SMART WEARABLES, LE FUTUR DE L'HUMANITÉ OCCIDENTALE SEMBLE DÉSORMAIS IRRÉVERSIBLEMENT ENGAGÉ VERS LE RENDEMENT MAXIMUM AVEC LE MOINDRE EFFORT.

Nous parlons d'une révolution qui concerne les personnes dans leur dimension individuelle mais aussi dans leur dimension professionnelle. En fait, l'adoption de systèmes IoT ne cesse de croître aussi dans les organisations, en particulier dans l'automatisation des bâtiments, le secteur automobile et les soins de santé.

Il s'agit d'un **processus** en **constante évolution** qui ouvre la voie à une infinité d'applications possibles et qui, surtout lorsque le réseau 5G sera largement répandu, gérera notre vie dans la plupart de ses aspects. Une perspective pour beaucoup fascinante mais qui comporte aussi de grands risques.

Sans entrer dans le fond des implications que tout cela peut avoir sur le fonctionnement de notre esprit, il faut sans aucun doute souligner le **risque** de **sécurité** qui est **proportionnel** à **l'utilisation** de la connexion à Internet. Aussi parce que les appareils intelligents sont souvent, notamment par rapport aux ordinateurs et aux smartphones, beaucoup moins évolués du point de vue des défenses technologiques et pourraient être utilisés comme une sorte de cheval de Troie pour infiltrer les réseaux. En bref, les proies parfaites pour les cybercriminels.

Au cours des cinq dernières années, les **cyberattaques** liées à l'IoT ont été **multipliées par 70**, précisément parce que la plupart (environ 76 %) des différents outils communiquent avec le réseau sur des canaux non cryptés, devenant ainsi l'objet de vulnérabilités qui font la joie des pirates.

IL SUFFIT DE PENSER QUE CES SYSTÈMES D'INTELLIGENCE ARTIFICIELLE SONT SOUVENT INTÉGRÉS AVEC DES SYSTÈMES DE COMMERCE ÉLECTRONIQUE ET PAR CONSÉQUENT AVEC DES MOYENS DE PAIEMENT, TELS QUE LES CARTES DE CRÉDIT OU LES SUPPORTS NUMÉRIQUES. C'EST UNE BELLE OPPORTUNITÉ POUR LES ESCROCS À LA RECHERCHE DE PROFITS.

Selon une étude menée par **Kaspersky**, 89 % des propriétaires d'appareils IoT expriment des doutes quant à leur sécurité en ligne. L'une des préoccupations les plus courantes est d'être espionné par les cybercriminels à l'aide de **caméras** et de **microphones**, ou de recevoir une demande de rançon à la suite du blocage de l'un des appareils, ou d'infecter l'ensemble du réseau domestique.

Des préoccupations absolument fondées tant pour les milieux de vie que pour les milieux de travail, d'autant plus que la diffusion de l'IoT connaît une croissance irréversible.
Selon certains analystes, d'ici 2025, plus de 30 milliards de connexions IoT devraient être présentes dans le monde. Avec ces chiffres, chaque personne disposera en moyenne de 4 appareils interconnectés. La connaissance des outils pour se prémunir contre ces risques est donc primordiale

LA SENSIBILISATION ET LA BONNE FORMATION AUX RISQUES NUMÉRIQUES RESTENT LES DEUX ARMES LES PLUS EFFICACES.

1.5 **À L'ÈRE DU NUMÉRIQUE, LA SÉCURITÉ N'EST PAS UNE OPTION**

RÉSUMÉ

Il est désormais évident que la vie « telle qu'elle était », dont beaucoup ont la nostalgie, ne reviendra peut-être plus et que les effets que la pandémie a provoqués deviendront structurels. La confiance que nous avions exprimée l'année dernière dans la fin de l'urgence doit probablement être réduite. En effet, nous nous sommes rendus compte que **l'urgence** sous toutes ses formes est en train de devenir la **nouvelle norme** et que **nous devrons nous adapter** le plus **rapidement** possible aux transformations sociales et professionnelles que la crise sanitaire nous a imposées. Pour cette raison, il est nécessaire d'agir avec décision sur le **facteur humain**, le véritable maillon faible du système défensif, avec des programmes de formation efficaces de sensibilisation à la cyber-sécurité, une mesure désormais incontournable pour la **sécurité** des **individus** et des **organisations**.

LE **SMART WORKING** PREND UNE **CONNOTATION STRUCTURELLE**, TOUT COMME LE COMMERCE ÉLECTRONIQUE, L'ENSEIGNEMENT À DISTANCE ET LES DIFFÉRENTES PLATES-FORMES DE FORMATION, LES SERVICES AUX CITOYENS DE LA PART DE L'ADMINISTRATION PUBLIQUE ET DES SOCIÉTÉS QUI FOURNISSENT DES SERVICES PUBLICS.

SI, D'UNE PART, LA **TRANSFORMATION NUMÉRIQUE** REPRÉSENTE UNE GRANDE OPPORTUNITÉ D'INNOVATION ET DE **MODERNISATION**, D'AUTRE PART, ELLE IMPLIQUE INÉVITABLEMENT UNE **AUGMENTATION** DES **RISQUES** POUR LA **SÉCURITÉ**.

Pour aggraver les choses, il y a le fait que les nouveaux modes d'attaque, comme nous l'avons vu, sont de plus en plus sophistiqués, l'ingénierie sociale de plus en plus raffinée et souvent les cybercriminels n'agissent plus de manière autonome mais se mettent en réseau avec d'autres « collègues » ou même avec le crime organisé, provoquant des effets très nocifs, surtout pour les entreprises.

En bref, si l'avenir de notre vie et de notre entreprise ne peut pas se passer du numérique, cela signifie que la **gestion** des **données**, leur **utilisation correcte** et leur **protection** seront de plus en plus au cœur de tout investissement d'entreprise.

Une tendance qui a heureusement été reprise par **l'Europe** et qui s'est traduite par un engagement à soutenir les **États membres** dans leur transition vers la **numérisation**. Dans ce scénario, il est important de réaliser que tous les pays de la Communauté européenne n'ont pas le même niveau de numérisation, comme le montre l'édition 2021 de l'indice de numérisation de l'économie et de la société (Desi).

Dans les pays où le niveau de numérisation est le plus faible, il ressort que la population âgée de 16 à 74 ans possède des compétences numériques de base et que seulement 22 % ont des compétences numériques supérieures à celles de base.

Selon le rapport, l'Italie, parmi les pays d'Europe où le niveau de numérisation est faible, « doit faire face à d'importantes lacunes dans les compétences numériques de base et avancées qui risquent de se traduire par l'exclusion numérique d'une partie importante de la population et de limiter la capacité d'innovation des entreprises ».

Les choix mis en œuvre pour le meilleur placement des 48,1 milliards que, dans le cas spécifique, le gouvernement italien a décidé d'affecter à ce secteur à travers le **PNRR**, dans lequel la **cybersécurité** occupe une place centrale et stratégique, seront donc déterminants.

D'autant que les études publiées jusqu'à présent sur le thème de la transition numérique indiquent que l'évolution du traitement des données et de leur sécurité sera la clé de la relance économique. En bref, l'innovation numérique, en plus d'être très attrayante, est essentielle pour l'entreprise du futur, mais son développement augmente également son côté obscur, à savoir le risque de cyberattaques.

Le seul moyen de se protéger est une formation adéquate en entreprise qui permet à tous les employés d'arriver préparés au rendez-vous avec cette nouvelle vague de numérisation en évitant les clics erronés et irréversibles.

Pour cela, il est nécessaire d'agir avec décision sur le facteur humain, le véritable maillon faible du système défensif. L'action sur le facteur humain et par conséquent les programmes de formation de sensibilisation au cyberrisque, doivent être considérés comme une mesure de sécurité nécessaire.

De nombreuses organisations ont au fil du temps **activé cesprogrammes** dans le seul but de démontrer la conformité aux différentes réglementations qui prévoient, dans leurs normes, la **formation** du **personnel** ; dans de nombreux cas, cela a signifié une attention insuffisante à l'efficacité réelle des **parcours de formation**. Mais les deux dernières années nous ont montré sans équivoque que cette attitude est vouée à l'échec et qu'à l'avenir il faudra surtout se soucier de leur efficacité.

Les programmes devront être en mesure de transformer concrètement les attitudes et les comportements des utilisateurs face à la cybermenace.

DONC, DANS LE CHOIX DU PARCOURS DE SENSIBILISATION À LA CYBERSÉCURITÉ, LES ORGANISATIONS DEVRAIENT TENIR COMPTE DE CERTAINES VARIABLES FONDAMENTALES TELLES QUE L'EFFICACITÉ, LES MÉTHODES PÉDAGOGIQUES UTILISÉES, LES TECHNIQUES D'IMPLICATION UTILISÉES, LES TECHNIQUES DE MISE À JOUR À DIFFÉRENTS NIVEAUX DE SENSIBILISATION, ET ENFIN LES « LANGUES » MULTIMÉDIA UTILISÉES.

2. LA FORMATION
2.1 UNE MESURE DE SÉCURITÉ NÉCESSAIRE

RÉSUMÉ
Toutes les organisations qui veulent tirer parti de ce processus de transformation numérique désormais imparable doivent investir dans le facteur humain avec des programmes de formation avancés et efficaces, capables de transformer concrètement le comportement des utilisateurs, en les adaptant au niveau de la menace qui ne cesse de croître et d'évoluer. Nous sommes confrontés à un défi asymétrique qui voit les attaquants dans une position d'avantage incontestable. Pour rétablir la symétrie dans ce défi, il est nécessaire de s'appuyer sur le facteur humain qui, dans la cybersécurité, joue un rôle décisif.

LE DÉVELOPPEMENT DE LA SOCIÉTÉ NUMÉRIQUE, AVEC SES RISQUES, OBLIGENT TOUTES LES ORGANISATIONS À INVESTIR DE MANIÈRE CONSTANTE DANS LE FACTEUR HUMAIN, NOTAMMENT AU NIVEAU DE LA SENSIBILISATION DES PERSONNES. UN INVESTISSEMENT DEVENU NÉCESSAIRE POUR COMBLER LE FOSSÉ CULTUREL QUE LES EFFETS PANDÉMIQUES ET LA TRANSFORMATION NUMÉRIQUE RAPIDE ONT CREUSÉ.

Le **problème** ne concerne pas seulement les personnes les moins habituées à l'utilisation des technologies numériques, mais aussi les **nouvelles générations** et les **«millennials»**.
Les nouvelles générations, malgré une propension naturelle à utiliser les technologies, adoptent très souvent une posture numérique similaire à celle des « utilisateurs non avertis », sans capacité à reconnaître les cyberrisques derrière leurs actions.

Nous avons été habitués ces dernières années à considérer la **cybersécurité** comme un sujet **technologique**, qui ne concernait que les spécialistes. L'idée de base est que quelque part dans notre organisation il y a toujours quelqu'un qui s'occupe de la cybersécurité et que c'est plus que suffisant. Face à une cyberattaque, nous sommes amenés à penser que le problème n'est lié qu'à l'expertise de cette équipe de spécialistes.

De plus, la cybersécurité a toujours été perçue comme quelque chose qui ne concernait que la dimension professionnelle de notre existence. Rien qui nous concerne directement. Le préjugé a toujours été le même : **«Pourquoi un hacker devrait-il s'intéresser à moi en tant qu'individu ?»**. Au cours des dernières années, nous avons vécu tout cela avec une certaine « légèreté » : une conviction qui a concerné non seulement le comportement des utilisateurs, mais aussi, et c'est encore plus préoccupant, celui des fonctions de gestion. Aujourd'hui, il est clair que la cybersécurité est un problème transversal qui touche tout le monde et affecte indifféremment les individus et les organisations de toutes sortes.

Un **défi asymétrique** qui voit les attaquants dans une position d'avantage incontestable, d'autant plus que la première ligne de défense est constituée de personnes « sans défense » qui n'ont pas la conscience des menaces et des contre-mesures nécessaires. Dans certains cas, les utilisateurs subissent des attaques sans même s'en rendre compte. Suivant la théorie du maillon faible, selon laquelle la force globale d'une chaîne est déterminée par son maillon le plus faible, on peut dire que l'efficacité de ces investissements est aujourd'hui extrêmement réduite par la faiblesse du facteur humain.

AU FIL DES ANS, LES ORGANISATIONS SE SONT SURTOUT PRÉOCCUPÉES DE DÉVELOPPER DES CAPACITÉS DE DÉFENSE AU NIVEAU TECHNOLOGIQUE, ET CES DÉFENSES ONT SANS AUCUN DOUTE AUGMENTÉ.

La présence sur le terrain d'un maillon aussi vulnérable, comme celui représenté par les **utilisateurs** qui **interagissent** avec les **technologies numériques** et avec le réseau Internet, nous redonne le sens de la façon dont ce défi est déséquilibré en faveur des attaquants.

Afin de ramener la symétrie dans ce défi, dont l'issue est autrement déjà marquée, il est nécessaire que les utilisateurs **prennent conscience**, puis, par conséquent, puissent mûrir des attitudes et adapter leurs comportements par rapport aux risques cybernétiques.
Un processus continu fait non seulement d'acquisition de connaissances théoriques, mais aussi d' **entraînement** de certaines caractéristiques défensives humaines, telles que la **perception** du **danger** et la **promptitude**.

Un processus qui, d'une part, doit être considéré comme une mesure de sécurité nécessaire, d'autre part, doit être conçu et gouverné selon les critères typiques de la formation axée sur le développement des ressources humaines. Pour sensibiliser les gens, des **programmes de formation avancés** sont nécessaires, basés sur des méthodes innovantes de formation continue, d'entraînement et d'engagement.
Des plateformes de formation capables de minimiser l'impact sur les fonctions de gestion de la formation et de cybersécurité. Ce n'est que de cette façon qu'il sera possible de suivre l'évolution constante des stratégies d'attaque, qui deviennent de plus en plus sophistiquées, et surtout qui se révèlent capables de s'adapter à la mutation constante des scénarios. Il faut aussi considérer la nécessité de guider **l'apprentissage cognitif** de manière appropriée, sans surcharger le système cognitif de l'apprenant qui, ne l'oublions pas, est une personne extrêmement engagée et ne peut consacrer à la formation que quelques « miettes » de son attention.

DANS LA CYBERSÉCURITÉ, LE FACTEUR HUMAIN JOUE UN RÔLE DÉCISIF !

2.2 LE RÔLE DE LA FORMATION

RÉSUMÉ

La seule façon de renforcer les capacités de défense des organisations contre la **cybercriminalité est d'investir de manière significative** et **constante** sur la **«première ligne de défense»**, c'est-à-dire sur les **personnes**. Il sera donc nécessaire d'impliquer toute la main-d'œuvre dans un **parcours de formation** qui permette à tous de faire un usage toujours plus conscient des technologies numériques, des outils sociaux et des ressources présentes sur le web.

Un parcours de croissance qui permet d'acquérir un niveau de connaissance partagé et qui stimule certaines caractéristiques défensives humaines telles que **l'attention**, la **promptitude** et la **réactivité**.

Imaginons une ville médiévale fortifiée qui se prépare à résister à un siège. Pensez à une poignée de soldats engagés à renforcer sans cesse les défenses périmétriques de la ville, tandis que la plupart des habitants continuent d'entrer et de sortir des fortifications en laissant les portes ouvertes, et entre eux, certains creusent même des tunnels de l'intérieur vers l'extérieur, pour garantir des voies d'accès privilégiées vers certaines zones de la campagne environnante.

Il semble absurde de ne l'imaginer que parce que les habitants d'une ville médiévale étaient parfaitement conscients du risque individuel et collectif qu'un tel comportement produirait.
À moins d'être un conspirateur à la solde de l'ennemi, aucun citoyen n'aurait jamais songé à affaiblir le système de défense de sa ville par un comportement « à risque ».

En revanche, dans la **réalité numérique**, de tels comportements sont courants et se produisent dans un climat de totale **inconscience**, sans réelle perception du **niveau** de **risque** déterminé par ces comportements.

À PARTIR DE CE CADRE, LA CERTITUDE QUE LA SEULE FAÇON DE RECRÉER UNE SYMÉTRIE DANS L'ÉTERNEL DÉFI ENTRE ATTAQUANTS ET DÉFENSEURS CONSISTE EN UN INVESTISSEMENT IMPORTANT ET CONSTANT DANS LA PREMIÈRE LIGNE DE DÉFENSE, C'EST-À-DIRE SUR LES GENS, LES UTILISATEURS DES TECHNOLOGIES NUMÉRIQUES.

Nous avons déjà souligné que la matrice humaine peut être trouvée dans la plupart des attaques, même celles apparemment plus technologiques. Les vecteurs de déclenchement les plus courants peuvent être attribués à des erreurs de comportement de la part des utilisateurs concernant :

• LA GESTION DES APPAREILS NUMÉRIQUES ;

• L'INTERACTION AVEC LA MESSAGERIE, À PARTIR DU COURRIER ÉLECTRONIQUE;

• L'UTILISATION DES IDENTIFIANTS DE CONNEXION ET, EN PARTICULIER, DES MOTS DE PASSE ;

• LA FAIBLE ATTENTION ACCORDÉE À LA VALEUR DE LA VIE PRIVÉE ET DES INFORMATIONS CRITIQUES ;

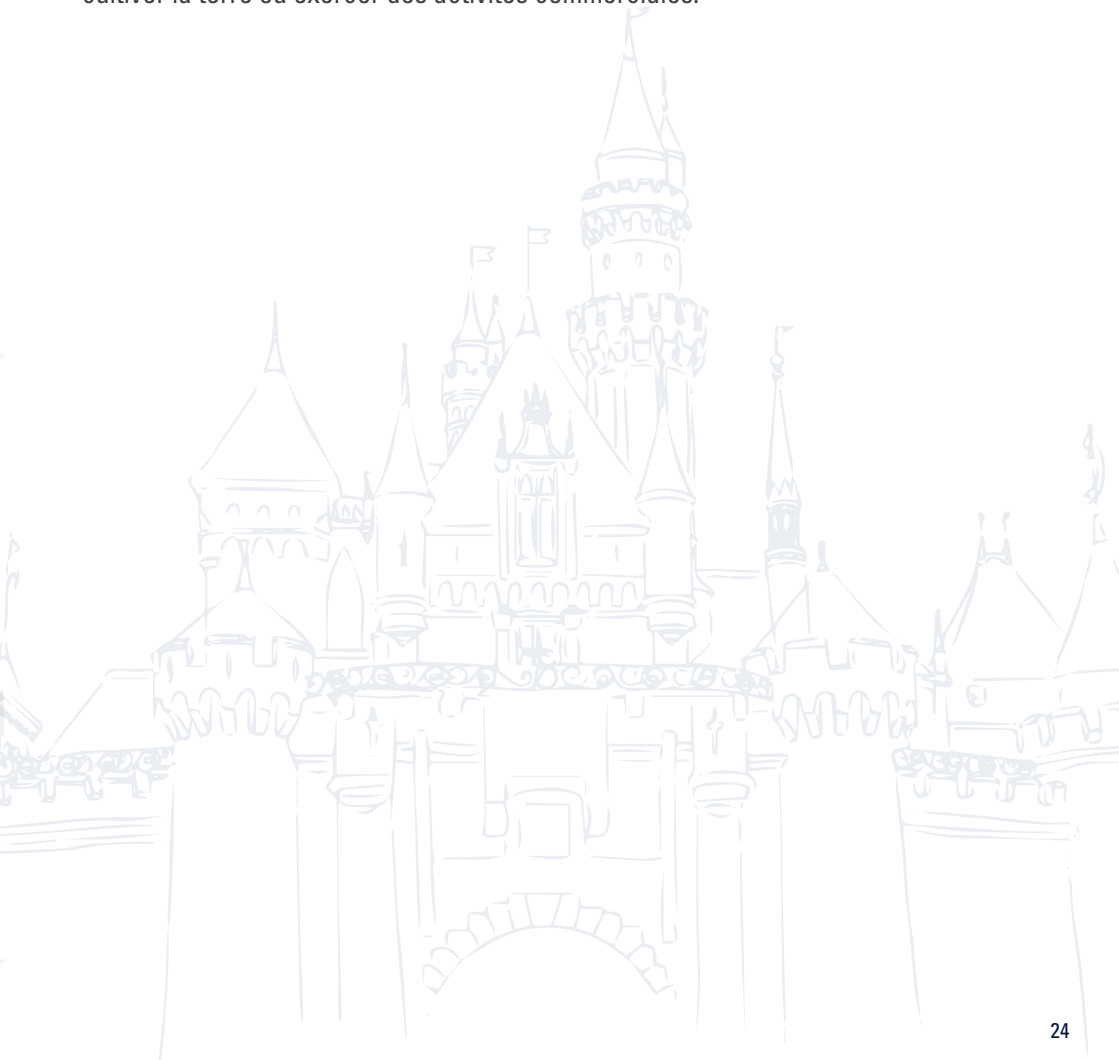
• L'ATTITUDE AVEC LAQUELLE ILS NAVIGUENT SUR LE RÉSEAU INTERNET ET AVEC LAQUELLE LES RESSOURCES DU WEB SONT APPROCHÉES.

Pour lutter efficacement contre les cyber-risques, toute organisation, publique ou privée, devra impliquer l'ensemble de la main-d'œuvre, quel que soit son rôle et ses compétences, dans un parcours de formation permettant à chacun de faire un usage toujours plus conscient des technologies numériques, des outils sociaux et des ressources présentes sur le web.

Un **parcours** de **croissance** qui permet d'acquérir un niveau de **connaissance partagé** et qui stimule certaines caractéristiques défensives humaines telles que **l'attention**, la **promptitude** et la **réactivité**.

La **prise de conscience** du **risque** conduit à réagir de manière plus appropriée face aux dangers connus, mais aussi à avoir une **attitude défensive correcte** face à des **menaces potentielles** encore inconnues, une attitude qui dans le monde Cyber est absolument nécessaire pour **l'évolution rapide** des techniques d'attaque.

La conscience est également nécessaire pour éviter qu'une attitude extrêmement défensive face à une perception irrationnelle du risque ne produise des comportements qui affectent négativement la productivité de l'individu et de l'organisation. Même dans la cité médiévale, il fallait quitter les fortifications pour cultiver la terre ou exercer des activités commerciales.



2.3 **MÉTHODOLOGIE EFFICACE**

RÉSUMÉ

Un programme de formation qui vise à transformer les comportements individuels doit être fondé sur une méthodologie efficace, mettant en évidence des résultats tangibles sur les processus d'apprentissage.
Une méthodologie qui n'est pas exclusivement axée sur l'aspect des connaissances, mais qui est capable d'intégrer des parcours expérientiels et inductifs dans le processus de formation. Ce mélange de composants permettra de développer non seulement les connaissances, mais aussi la perception du risque et la préparation, en créant une génération d'utilisateurs conscients, capables d'interagir correctement dans la sphère numérique, tant dans leur dimension individuelle que dans leur dimension professionnelle.

UN PROGRAMME DE FORMATION À LA CYBERSÉCURITÉ DOIT REPOSER SUR UNE **MÉTHODOLOGIE EFFICACE**, ORIENTÉE VERS UN RÉSULTAT **PARTICULIÈREMENT DIFFICILE**, COMME CELUI DE TRANSFORMER LES COMPORTEMENTS HUMAINS. LA RÉALISATION DE CE RÉSULTAT EST ÉTROITEMENT LIÉE À LA CAPACITÉ D'ACTION TOUT AUSSI EFFICACE SUR LES PROCESSUS D'APPRENTISSAGE, À LA FOIS SUR LES PROCESSUS D'APPRENTISSAGE LES PLUS STRICTEMENT DIDACTIQUES ET SUR CEUX LIÉS À L'ACTIVITÉ DE FOND ENVERS LA CYBERSÉCURITÉ, TOUS DEUX NÉCESSAIRES POUR PRODUIRE UN CHANGEMENT DURABLE DANS LE COMPORTEMENT.

La formation doit contribuer à développer la **perception correcte** du **cyber-risque**, en **réalignant** la **sphère rationnelle** sur la sphère **émotionnelle**, car aujourd'hui, dans la plupart des cas, les dimensions objective et subjective ne sont pas équilibrées. De la part des utilisateurs numériques, il y a en général une profonde **sous-estimation** du **cyber-risque**, ou au contraire, précisément en raison de l'absence d'une bonne compréhension du phénomène, des attitudes de blocage peuvent être générées à l'égard des processus incontestables de transformation numérique.

Un **utilisateur conscient** est un utilisateur qui a une compréhension claire des menaces du réseau et une perception correcte du cyberrisque, et qui a donc acquis une posture numérique adéquate. Un utilisateur conscient est aussi celui qui parvient à comprendre comment le thème de la conscience concerne à la fois sa dimension privée et sa dimension professionnelle, et à mûrir la capacité de maintenir autant que possible ces deux dimensions distinctes, car aujourd'hui ces deux dimensions ont souvent tendance à se chevaucher.

Une **méthodologie efficace** doit éviter les erreurs qui, au cours des dernières années, ont empêché les initiatives de sensibilisation à la cybersécurité de créer le climat d'engagement nécessaire, condition essentielle pour obtenir des résultats tangibles sur la voie de la réduction des risques. Des erreurs souvent inhérentes aux méthodes de formation traditionnelles et qui dans ce contexte spécifique, étant un sujet imaginé comme particulièrement difficile, peuvent prendre une plus grande importance.

Parmi les **perceptions erronées** les plus répandues sur le thème de la sensibilisation à la cybersécurité, on trouve :

- LA SENSIBILISATION À LA CYBERSÉCURITÉ EST UNE DISCIPLINE TECHNIQUE QUI A L'AMBITION ILLUSOIRE DE TRANSFORMER LES UTILISATEURS EN SPÉCIALISTES DU SECTEUR OU EN UNE SORTE DE SHERLOCK HOLMES MODERNES CAPABLES DE FAIRE DES ENQUÊTES SOPHISTIQUÉES ;

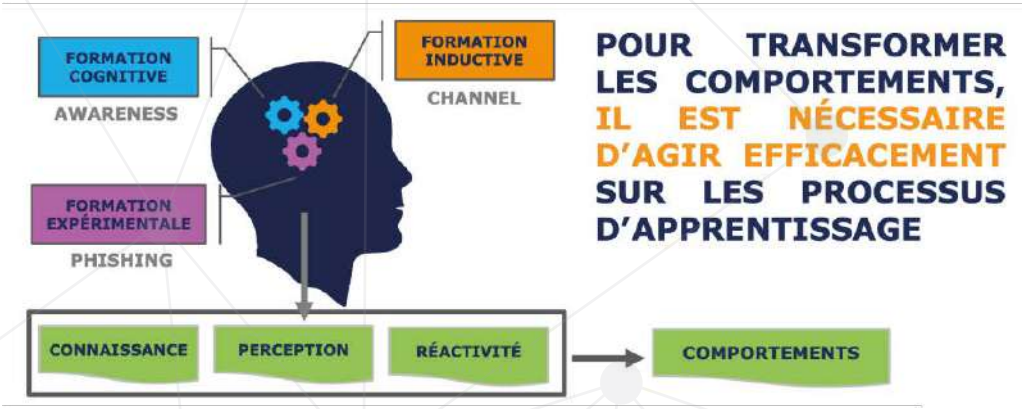
- LA CYBERSÉCURITÉ CONCERNE EXCLUSIVEMENT LA DIMENSION PROFESSIONNELLE DE L'INDIVIDU ET DONC SON RÔLE AU SEIN DE L'ORGANISATION.

- LA SENSIBILISATION À LA CYBERSÉCURITÉ A POUR SEUL BUT DE PRÉVENIR L'ORGANISATION FACE AUX PROCESSUS D'AUDIT LIÉS À DES RÉGLEMENTATIONS OBSCURES, ET A UNE IMPLICATION EXÉCUTOIRE ;

- LA SENSIBILISATION À LA CYBERSÉCURITÉ EST UNE FORMATION IMPOSÉE QUI NE PRODUIT PAS DE RÉSULTATS UTILES, POUR L'INDIVIDU ET POUR L'ORGANISATION ;

- LA SENSIBILISATION À LA CYBERSÉCURITÉ TRAITE DES ARGUMENTS THÉORIQUES QUI NE TROUVENT AUCUNE RÉPONSE PRATIQUE DANS LA DIMENSION PRIVÉE ET PROFESSIONNELLE DE L'INDIVIDU.

La sensibilisation à la **cybersécurité** is, est en fait une discipline transversale, à caractère populaire, qui permet de développer les compétences nécessaires pour agir en toute sécurité dans la sphère numérique, que ce soit dans la sphère privée, en se protégeant soi-même et son réseau social, ou dans la sphère professionnelle, en protégeant son rôle et ses responsabilités d'entreprise, son organisation et l'ensemble de l'écosystème dont l'organisation fait partie (clients, fournisseurs, partenaires […]).



Pour obtenir des résultats concrets, les programmes de sensibilisation à la cybersécurité ne peuvent pas se limiter à fournir des notions, mais doivent s'articuler dans des parcours à caractère expérientiel et inductif, en suivant des approches **«learning by doing»** et **«learning by example»**.

En combinant des approches pédagogiques avec d'autres à caractère expérientiel et inductif, on obtient une mixité significative capable d'agir positivement sur les connaissances, la perception du danger et l'état de préparation, conditionnant les attitudes et les comportements.

S'il est assez facile d'imaginer une **formation didactique**, il est plus difficile de penser à une formation expérientielle et inductive. Dans le cas de l'apprentissage par l'expérience, l'utilisateur devra expérimenter des situations typiques d'attaque, comme c'est le cas dans le cas de l'attaque de phishing, devenant la cible de simulations capables de reproduire l'expérience réelle. Dans le cas de la formation inductive, elle devra être menée dans des situations réelles, à travers une narration efficace qui produise un processus d'identification, au point de ressentir la menace de manière plus concrète que ce à quoi ils sont habitués.

2.4 **FORMATION CONTINUE**

RÉSUMÉ

Compte tenu des caractéristiques et du contexte spécifique de la thématique, un programme de formation, pour être efficace, doit se développer selon un modèle de formation continue, que nous pourrions métaphoriquement définir de type « homéopathique », caractérisé donc par des micro-interventions, diluées dans le temps. Une formation capable d'agir non seulement au niveau cognitif, mais aussi au niveau de la perception, permettant ainsi à l'utilisateur de développer une véritable aptitude à reconnaître les menaces de la dimension numérique, un peu comme cela se produit par rapport aux menaces de la vie réelle.

DANS LE CONTEXTE HISTORIQUE ACTUEL, UN PROGRAMME DE SENSIBILISATION À LA CYBERSÉCURITÉ, POUR ÊTRE EFFICACE, DOIT ÊTRE DÉVELOPPÉ SELON UN MODÈLE DE FORMATION CONTINUE, CONFORME AU PROCESSUS DE TRANSFORMATION NUMÉRIQUE ET D'ÉVOLUTION DES CYBERATTAQUES, QUI PROGRESSE SANS CESSE.

Afin de soutenir un modèle de formation continue, sans nuire clairement à la productivité de l'individu et des équipes de travail, il sera essentiel de procéder à des micro-interventions, organisées de façon régulière.

Le principe de base est que les organisations doivent habituer leur personnel à investir régulièrement une partie de leur temps (bien que compatible avec leurs activités et avec la nécessité de ne pas surcharger le système cognitif) pour prévenir ce qui est déjà aujourd'hui le risque le plus important pour leur sécurité individuelle et, par conséquent, pour la sécurité de l'ensemble de l'organisation.

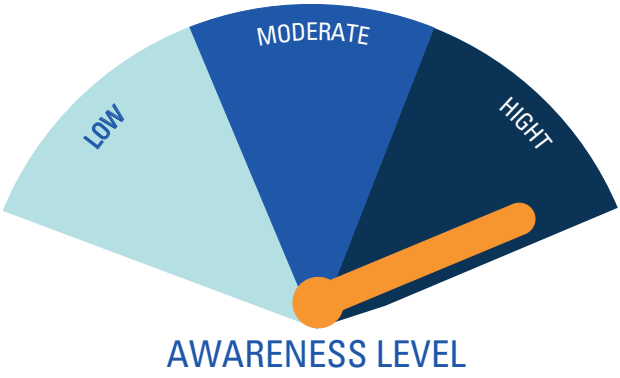
IL EST DONC FONDAMENTAL QU'UNE VRAIE CONSCIENCE DU NIVEAU DE RISQUE SOIT ACQUISE. PARCE QUE LE CYBERRISQUE PEUT, D'UNE PART, TRANSFORMER LA VIE D'UN INDIVIDU EN UN VÉRITABLE CAUCHEMAR ET, D'AUTRE PART, REMETTRE EN QUESTION LA SURVIE MÊME DE L'ORGANISATION.

Aujourd'hui, la cybersécurité n'est plus un problème technologique, mais un sérieux problème commercial, et le risque de cybersécurité doit donc également être interprété différemment des années précédentes.

MAIS QUEL EST LE LIEN ENTRE LA FORMATION CONTINUE ET LA FORMATION EFFICACE ?

Pourquoi un modèle de formation continue devrait-il être plus efficace qu'un modèle de formation caractérisé par des approches plus « concentrées », plus intenses, et donc plus simples à organiser, à gérer et à suivre ?
Avant de répondre à cette question, il faut faire un constat : dans cette étude approfondie, la formation en salle n'est pas prise en considération, car elle est jugée moins efficace dans le domaine professionnel, et parce que les événements survenus à partir de 2020, ont en effet montré que pour traiter des problèmes de ce type, il n'existe que l'option de l'enseignement à distance, sous toutes ses formes.

Pour revenir aux deux questions précédentes, il est essentiel de souligner à nouveau l'objectif réel et concret de la formation dans le domaine de la cybersécurité : **sensibiliser aux cybermenaces** pour transformer le comportement de tous les individus, en particulier de ceux qui n'ont aucune connaissance ou spécialisation dans le domaine de la cybersécurité, considéré depuis toujours comme un domaine technologique.



Pour transformer les comportements des utilisateurs numériques en les adaptant au niveau actuel et futur des menaces, il ne suffit pas d'agir avec un modèle didactique, mais il est également nécessaire d'avoir une incidence sur la perception.

L'utilisateur doit développer une véritable **aptitude à reconnaître les dangers**, en développant un certain niveau de résilience, afin que cette sorte d'instinct puisse s'adapter constamment aux évolutions continues des stratégies d'attaque.
Au niveau numérique, nous devons donc aider les utilisateurs à développer ce niveau de perception du danger, qui dans la vie de tous les jours nous sauve des nombreuses menaces qui nous entourent.

Pour ces raisons, une **formation intensive** et **concentrée** ne peut que générer un effet éphémère, avec une efficacité concrète seulement dans l'immédiat, mais qui, de par sa nature, tend inévitablement à se disperser dans le temps.
Utiliser au contraire une approche de caractère « homéopathique », avec de petites interventions diluées dans le temps, permet de maintenir la dimension perceptive à un niveau adéquat, et permet de mettre à jour également la dimension conceptuelle, en la maintenant toujours en ligne avec les développements de la thématique. Alors que les cybermenaces changent constamment, prenant des formes toujours plus sophistiquées, qui les différencient de leur forme originelle, il est essentiel de continuer à instiller de petites doses du « vaccin » chez les personnes, pour les immuniser contre toutes leurs multiples formes.

MAIS QUELLE EST UNE PART DE TEMPS ACCEPTABLE À CONSACRER À CE TYPE DE FORMATION ?

QUEL EST LE POINT D'ÉQUILIBRE ENTRE LE RÉSULTAT OBTENU ET L'IMPACT PRODUIT ?

L'expérience acquise nous a montré comment une occupation de temps allant de 20 à 30 minutes par mois, avec une modularité qui permet de diviser cet engagement en sessions de formation auto-consistantes qui ne dépassent pas 10 minutes, est compatible avec tout type d'exigence de travail, en éliminant tout blocage potentiel dû à une surcharge de type cognitif.

De nombreux cours intensifs et ciblés, tels que celui sur la sécurité au travail (loi 81/2008) ou les cours liés à l'introduction du RGPD (Règlement général sur la protection des données), ont produit au fil des ans une sorte de refus de la part de tous les employés : une erreur à éviter absolument.
Dans le paragraphe suivant, nous verrons comment un modèle de formation continue, bien qu'ayant un faible impact sur la main-d'œuvre, doit dans tous les cas être soutenu par des techniques d'implication de l'utilisateur, qui doit se sentir motivé pour participer en raison de la qualité du contenu reçu et les avantages obtenus.

2.5 **PARTICIPATION À LA FORMATION**

RÉSUMÉ

Un **cours efficace** doit être extrêmement **engageant** et donc non perçu selon une simple logique « obligatoire ». L'implication dépend fortement des langages et des formats, mais aussi de la capacité à transmettre le bénéfice de caractère individuel que le participant obtient, une sorte de retour sur investissement significatif par rapport à son engagement. Cela ne signifie pas qu'une telle formation ne puisse pas être classée comme obligatoire, mais l'éventuelle obligation ne devra jamais être utilisée comme alternative à l'utilisation de critères efficaces d'« engagement ».

UN PROGRAMME QUI VEUT ÊTRE EFFICACE DOIT ÊTRE ENGAGEANT ENVERS LE PARTICIPANT, ET DÉVELOPPER EN LUI UN NIVEAU SUFFISANT D'« ENGAGEMENT ». POUR IMPLIQUER L'UTILISATEUR SUR UNE THÉMATIQUE APPAREMMENT « HOSTILE », CONSIDÉRÉE À TORT COMME UNE EXCLUSIVITÉ DU PERSONNEL SPÉCIALISÉ, IL FAUT SURMONTER LE PRÉJUDICE INSIDIEUX DE CELUI QUI, N'ÉTANT PAS UN TECHNICIEN, NE PARVIENT PAS À EN PERCEVOIR LA MOTIVATION.

La première chose à prendre en compte est le langage et les formes d'expression utilisés. Nous sommes habitués à concevoir la formation en entreprise comme quelque chose qui doit être caractérisé par la « lourdeur » des contenus et des formes d'expression.

En nous basant sur les canons de la formation traditionnelle, nous courrions le risque, sur une thématique dont l'objet est les cybermenaces et les conséquences qu'elles peuvent engendrer, de dépasser l'alarmisme et le technicisme, et d'induire une situation de rejet.

POUR ATTEINDRE L'OBJECTIF DE LA SENSIBILISATION À LA CYBERSÉCURITÉ, LE **LANGAGE UTILISÉ** DOIT DONC **ÊTRE HAUTEMENT INFORMATIF, COMPRÉHENSIBLE** , PAR TOUS. UN LANGAGE QUI EXPLIQUE CLAIREMENT QU'IL NE S'AGIT PAS D'UNE MATIÈRE À CARACTÈRE TECHNIQUE, MAIS D'UNE **MATIÈRE** QUI **CONCERNE LA VIE QUOTIDIENNE** ET TOUTE PERSONNE AYANT UNE INTERACTION AVEC LA SPHÈRE NUMÉRIQUE.

Tout effet barrière préventif doit s'effondrer dès le début pour laisser place à une perception claire de l'utilité de l'intervention de formation et de la possibilité de pouvoir en bénéficier pleinement, quelles que soient ses compétences.

Les formes d'expression doivent inévitablement s'inspirer des principes de l'apprentissage multimédia et se caractériser par une grande interactivité. L'aspect moderne et captivant ne doit jamais être « alourdi » par une utilisation excessive d'animations, qui doivent être maintenues en équilibre avec l'élément humain. La fonction de coaching continuera donc à être interprétée par l'élément humain pour favoriser le processus d'identification basé sur le canon enseignant/élève.

La sensibilisation à la cybersécurité est un investissement sur le facteur humain, et cette connotation doit également se refléter dans le programme de formation. L'interactivité prend une importance concrète dans la logique d'une alternance continue entre de courts contenus de formation et des tests d'apprentissage, qui servent à renforcer la compréhension du contenu, en suivant la logique de l'exemption universitaire, plutôt que la logique de l'examen final. Une autre forme d'implication est liée au bénéfice que l'on obtient d'une formation, de ce que l'on peut appeler le « levier individuel ».

Il est essentiel que le participant comprenne dès la première leçon que le principal avantage de la sensibilisation à la cybersécurité s'adresse à l'individu et à son réseau social, avant même son organisation. Cette conviction atténuera le caractère imposant de la formation elle-même et l'idée qu'elle n'est requise que pour protéger l'organisation d'éventuelles conséquences.

Ce n'est qu'en percevant ce type d'avantage que l'implication sera totale et que l'incitation à maintenir son niveau de sensibilisation aux cyberattaques sera automatique. Ce sentiment d'implication spontanée sera davantage perçu si le processus d'identification est renforcé par la référence continue à des cas et des situations réels, dans lesquels il est facile de se reconnaître.

Souvent, au démarrage d'un parcours de ce type, la question qui revient le plus souvent aux managers internes est de savoir si cette formation doit être qualifiée d'obligatoire ou s'il s'agit avant tout de privilégier l'implication des personnes. Honnêtement, il n'y a pas de réponse unique à cette question, car chaque organisation a sa propre dynamique.

Il ne fait aucun doute que le maximum d'efficacité est obtenu en combinant ces deux types de leviers : celui de l'obligation et celui de l'implication.

S'IL EST VRAI QUE L'OBLIGATION D'UN PROGRAMME DE FORMATION POURRAIT ÊTRE PERÇUE NÉGATIVEMENT COMME UNE IMPOSITION, IL EST ÉGALEMENT VRAI, ET L'EXPÉRIENCE ACQUISE LE CONFIRME, QUE LE MANQUE D'OBLIGATION POURRAIT ÊTRE LU COMME SYNONYME DE « PEU IMPORTANT ».
C'EST POURQUOI LE MAXIMUM D'EFFICACITÉ EST ATTEINT LORSQUE LES OBLIGATIONS ET LA PARTICIPATION COEXISTENT DE MANIÈRE ÉQUILIBRÉE.

2.6 **LUDIFICATION**

RÉSUMÉ

Le jeu est peut-être le plus puissant des éléments qui génèrent une implication dans la formation en entreprise. Formes de ludification individuelle, avec la délivrance de reconnaissances virtuelles, et de groupe, avec le développement d'une compétition vertueuse entre différentes équipes, renforcent les processus d'apprentissage et agissent également positivement sur le jeu d'équipe.

QUE LE JEU SOIT UN OUTIL QUI FACILITE LES PROCESSUS D'APPRENTISSAGE EST UNE CHOSE CONNUE DEPUIS LONGTEMPS, TOUT COMME IL EXISTE UNE ÉVIDENCE QUE LES TECHNIQUES DE LUDIFICATION APPLIQUÉES À LA FORMATION COMMERCIALE AUGMENTENT L'EFFICACITÉ DE LA FORMATION ELLE-MÊME, EN AGISSANT POSITIVEMENT AUSSI BIEN SUR LA PARTICIPATION D'UN POINT DE VUE QUANTITATIF QUE QUALITATIF. C'EST D'AUTANT PLUS VRAI QUAND ON PARLE DE FORMATION À DISTANCE.

Les **techniques** de **ludification**, en ajoutant des éléments de motivation, renforcent le niveau d'implication par rapport au parcours de formation, qui, comme nous l'avons vu, représente une étape fondamentale pour obtenir un résultat efficace.

La ludification peut agir **au niveau individuel**, grâce à des éléments de gratification virtuels, tels que l'acquisition de badges, médailles, coupes, […], qui marquent toutes les étapes importantes du parcours de formation et récompensent l'engagement du participant. La ludification peut également agir **au niveau du groupe**, en s'appuyant sur le sentiment d'appartenance et le jeu d'équipe.

Appartenir à une équipe, et en ce sens activer le mécanisme de compétition vertueuse avec d'autres équipes, génère des niveaux élevés d'implication et une plus grande capacité à développer des processus omniprésents de communication interne.

LES TECHNIQUES DE LUDIFICATION, ET DONC LA CAPACITÉ DE CONVERTIR LE NIVEAU D'UTILISATION DU PARCOURS DE FORMATION EN SCORE, AIDENT LES PARTICIPANTS ET LES SUPERVISEURS À COMPRENDRE IMMÉDIATEMENT LES PROGRÈS RÉALISÉS DANS L'APPRENTISSAGE, ET FOURNIT DES ÉLÉMENTS CONCRETS POUR EFFECTUER UNE ÉVALUATION DES RÉSULTATS.

2.7 **ENGAGEMENT**

RÉSUMÉ

Le niveau d'engagement au sein de l'organisation et l'attention du top management sont des facteurs décisifs, surtout par rapport à une initiative qui se caractérise par sa transversalité et par la criticité du thème traité.

DANS LE DOMAINE DE LA FORMATION EN ENTREPRISE, L'EFFICACITÉ EST CLAIREMENT FAVORISÉE AUSSI DU NIVEAU D'ENGAGEMENT ET D'IMPLICATION DES STRUCTURES DE L'ENTREPRISE.
L'ATTENTION DU TOP MANAGEMENT SUR UNE INITIATIVE AUSSI TRANSVERSALE DEVIENT UN FACTEUR CRITIQUE DE SUCCÈS DE CETTE INITIATIVE.

Nous avons déjà souligné que le cyberrisque est en fait un risque commercial comme les autres, et il est donc évident que la réduction de la menace de ce risque doit être un objectif de l'ensemble de l'organisation et non une exclusivité des départements informatiques/SEC.

L'implication des structures de RH, de la Communication Interne, avec l'activation de tous les canaux de communication, comme par exemple le réseau Intranet, devient fondamentale pour favoriser le succès de l'initiative et pour la faire avancer dans le temps.

L'EXPÉRIENCE A MONTRÉ QUE LORSQUE L'ENGAGEMENT VA AU NIVEAU DIT « C », TOUTES LES BARRIÈRES QUI STOPPENT LA PARTICIPATION ET L'IMPLICATION SONT BRISÉES ET L'EFFICACITÉ DE LA FORMATION AUGMENTE CONSIDÉRABLEMENT.

3. CYBER GURU
3.1 LA PLATEFORME DE SÉCURITÉ

RÉSUMÉ
Cyber Guru est la première ligne de solutions de sensibilisation à la cybersécurité conçue pour augmenter le niveau de sécurité des individus et des entreprises, en agissant efficacement sur le facteur humain. Une plateforme capable d'agir efficacement sur le facteur humain grâce à une méthodologie innovante qui améliore les processus d'apprentissage.

LA PLATEFORME CYBER GURU, CONÇUE EN ITALIE, SE BASE SUR DES MÉTHODOLOGIES DE FORMATION QUI SONT LE FRUIT D'UN TRAVAIL MULTIDISCIPLINAIRE, QUI A ÉGALEMENT BÉNÉFICIÉ DE LA COLLABORATION DU DÉPARTEMENT DES SCIENCES DE LA FORMATION DE L'UNIVERSITÉ DE ROME TROIS.

Toutes les solutions de la plateforme Cyber Guru permettent d'atteindre deux grands objectifs :

- ACCROÎTRE LA SENSIBILISATION DES INDIVIDUS AUX RISQUES ENCOURUS DANS L'INTERACTION AVEC LES TECHNOLOGIES NUMÉRIQUES ET INTERNET ;
- INFLUENCER LES COMPORTEMENTS DES INDIVIDUS, AFIN DE LES ADAPTER AUX BESOINS DE PROTECTION DES ENTREPRISES ET AUX DÉFIS POSÉS PAR L'ÉVOLUTION DE LA CYBERCRIMINALITÉ.

Pour atteindre ces objectifs, la conception et le développement des plateformes ont suivi des lignes méthodologiques précises, qui prennent en compte la nécessité d'agir efficacement sur les processus d'apprentissage.

LA MÉTHODOLOGIE REPOSE SUR 3 NIVEAUX DE FORMATION :

FORMATION PÉDAGOGIQUE

APPRENTISSAGE EXPÉRIMENTAL

FORMATION INDUCTIVE

EN OUTRE, LA MÉTHODOLOGIE, QUI EST À LA BASE DE CYBER GURU, PREND EN COMPTE DEUX AUTRES ASPECTS DÉTERMINANTS :

- Un processus de formation continue, constitué de micro-interventions effectuées avec constance et régularité ;
- L'implication de l'utilisateur dans ce processus, en faisant comprendre à l'utilisateur lui-même que l'objectif principal du processus est sa protection, en tant qu'individu inséré dans un contexte social de plus en plus interconnecté.

TOUT CELA SERT À DÉVELOPPER, EN PERMANENCE ET PROGRESSIVEMENT, TROIS CARACTÉRISTIQUES QUI AFFECTENT LES COMPORTEMENTS HUMAINS LORSQUE LES PERSONNES SONT MENACÉES, GÉNÉRANT L'ATTITUDE À RÉAGIR CORRECTEMENT POUR SE PROTÉGER ET PROTÉGER SA PROPRE ORGANISATION :

CONNAISSANCES
ACTION RATIONNELLE

PERCEPTION
ACTION INSTINCTIVE

RÉACTIVITÉ
ACTION IMMÉDIATE

3.2 CYBER GURU AWARENESS

RÉSUMÉ

Cyber Guru Awareness est un système d'e-learning intégré innovant qui permet d'impliquer toute l'organisation dans un parcours de formation basé sur une méthodologie de formation continue et sur l'application de techniques de jeu à l'ensemble du parcours de formation.

Cyber Guru Awareness est conçu pour impliquer toute l'organisation dans un parcours d'apprentissage éducatif et stimulant, qui se caractérise par son approche de « libération constante et progressive » et par certaines caractéristiques particulières :

- MODULES DE FORMATION AUTOCONSISTANTS AVEC ACTIVATION MENSUELLE ;
- ENGAGEMENT HEBDOMADAIRE MINIMAL, COMPATIBLE AVEC TOUTES LES FONCTIONS ;
- MICRO-LEÇONS VIDÉO EN FORMAT MULTIMÉDIA ;
- UTILISATION D'ACTEURS PROFESSIONNELS AYANT DES FONCTIONS DE COACH ;
- LANGAGE HAUTEMENT ABORDABLE ;
- APPROCHE INTERACTIVE AVEC ALTERNANCE CONTINUE ENTRE LES MICRO LEÇONS ET LES TESTS ;
- TEST D'ÉVALUATION À RÉPONSES MULTIPLES ;
- MÉTHODOLOGIE DE LUDIFICATION, AVEC ORGANISATION EN ÉQUIPE ;
- PLATEFORME MULTILINGUE ;
- CONTENU ADDITIONNEL ET CONSTAMMENT MIS À JOUR.

La **formation Cyber Guru Awareness** se compose de **modules de formation** auto-cohérents, chacun dédié à un sujet précis, avec une activation mensuelle pour une durée de 12/24/36 **mois**.
Chaque module se compose à son tour de **3 courtes leçons vidéo** de 5 **minutes chacune**, chacune liée à un **test** d'apprentissage avec **des questions** à **choix multiples.**
La leçon vidéo, avec **l'acteur en tant que coach**, représente l'élément de base du parcours de formation qui permet, avec la ludification, d'impliquer activement l'utilisateur dans ce parcours.

Les mécanismes de ludification sont structurés pour créer le plus haut niveau d'implication de l'individu et de l'organisation, en favorisant l'activation des processus de communication interne, y compris dans une logique de **«team building»**.

LA LUDIFICATION EST STRUCTURÉE :

- **SOUS FORME INDIVIDUELLE** , AVEC L'ATTRIBUTION DE MÉDAILLES ET COUPES VIRTUELLES QUI RÉCOMPENSENT LA PARTICIPATION DE L'UTILISATEUR, ÉGALEMENT DU POINT DE VUE QUALITATIF ;
- **SOUS FORME AGRÉGÉE**, AVEC UNE ORGANISATION EN ÉQUIPE QUI PERMET DE GÉNÉRER UNE COMPÉTITION VERTUEUSE ENTRE DIFFÉRENTES ÉQUIPES, UN MÉCANISME PARTICULIÈREMENT MOTIVANT QUI S'APPUIE SUR LES LOGIQUES D'APPARTENANCE.

Cyber Guru Awareness, afin d'augmenter l'engagement de l'utilisateur, sans faire peser de fardeau sur ceux qui sont en charge de la formation, met à disposition une fonction automatique de Student Caring, qui s'occupe de stimuler la participation, à travers des notifications ponctuelles.

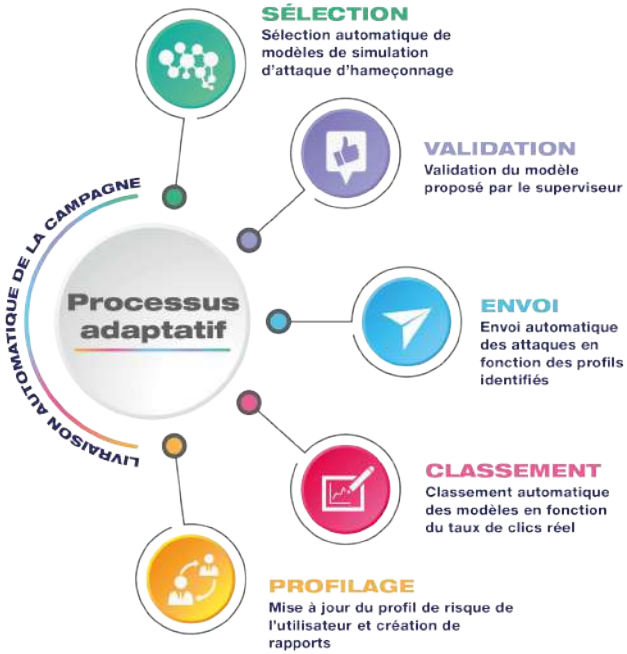
3.3 CYBER GURU PHISHING

RÉSUMÉ

Cyber Guru Phishing est une plateforme de formation anti-phishing innovante, basée sur une méthodologie d'apprentissage par l'expérience. L'objectif de Cyber Guru Phishing est de maximiser l'efficacité de la formation vis-à-vis du risque de Phishing : perception du danger, réactivité face à l'attaque, conscience de la menace.

CYBER GURU PHISHING A ÉTÉ CONÇU POUR FORMER LE PERSONNEL À RÉSISTER AUX ATTAQUES DE PHISHING, PAR LE BIAIS DE CAMPAGNES D'ATTAQUES SIMULÉES, PERSONNALISÉES SUR LA BASE DU PROFIL COMPORTEMENTAL DE L'UTILISATEUR INDIVIDUEL, GRÂCE À L'UTILISATION D'UN PROCESSUS D'INTELLIGENCE ARTIFICIELLE.

Grâce à son approche adaptative, Cyber Guru Phishing peut être considéré comme un véritable « coach personnel » à la fonction anti-phishing.



Les campagnes de simulation reproduisent l'expérience réelle et les stratégies d'attaque adoptées par les cybercriminels. Les algorithmes d'apprentissage utilisés par la plateforme sont capables de sélectionner les modèles d'attaque, sur la base d'un critère d'efficacité maximale de la formation.

À chaque campagne, le moteur adaptatif choisit les nouveaux modèles en fonction du profil utilisateur, augmentant par exemple le niveau de difficulté des attaques, pour les utilisateurs classés comme « forts ».

La plate-forme suit le schéma de fonctionnement suivant :

1. À CHAQUE CAMPAGNE, LA PLATEFORME SÉLECTIONNE AUTOMATIQUEMENT LES MODÈLES D'ATTAQUE ET LES REND DISPONIBLES POUR L'APPROBATION.

2. LA PLATEFORME DISTRIBUE LES ATTAQUES SELON UN SCHÉMA PERSONNALISÉ ET AVEC UN MÉCANISME QUI ÉVITE LE PHÉNOMÈNE DU BOUCHE À OREILLE.

3. TOUTE PERSONNE QUI TOMBE DANS LA TROMPERIE EST EXPOSÉE À UN ENTRAÎNEMENT SPÉCIALISÉ PAR RAPPORT À L'ATTAQUE SUBIE, RENFORÇANT AINSI LA MÉTHODE D'APPRENTISSAGE EXPÉRIENTIEL.

4. LES EFFETS DE CHAQUE CAMPAGNE PERMETTENT DE VALORISER LES INDICATEURS DE RISQUES SURVEILLÉS PAR LA PLATEFORME, DÉTERMINANT LA PRÉPARATION ET LA DIFFUSION DE LA CAMPAGNE SUIVANTE.

5. OUTRE LE CLASSEMENT DES UTILISATEURS EN « FAIBLES », « INTERMÉDIAIRES » ET « FORTS », LA PLATEFORME PERMET DE VALORISER ÉGALEMENT LA CATÉGORIE DÉFINIE DES « DEFENDER », C'EST-À-DIRE DE CEUX QUI, EN PLUS DE NE PAS TOMBER DANS LA TROMPERIE, RECONNAISSENT L'ATTAQUE ET LE SIGNALENT.

6. TOUS LES INDICATEURS ALIMENTENT EN TEMPS RÉEL LA FONCTION DE REPORTING, UTILISABLE VIA UN TABLEAU DE BORD AVANCÉ.

Le reporting ne se limite pas à exposer le taux de clics d'une campagne, mais met à disposition des rapports et des indicateurs qui expriment une carte claire du risque et de l'efficacité réelle du parcours entrepris.

L'apprentissage expérientiel, réalisé grâce au Cyber Guru Phishing, s'avère particulièrement efficace pour réduire le risque de Phishing, augmentant constamment le niveau de résistance aux cyberattaques de l'ensemble de l'organisation et réduisant avec une égale régularité le nombre d'utilisateurs classés comme « faible ».

Cette méthodologie d'apprentissage est soutenue par les caractéristiques de la plateforme, en particulier son niveau d'automatisation, qui minimise l'impact sur les équipes de cybersécurité.

3.4 CYBER GURU CHANNEL

RÉSUMÉ

Cyber Guru Channel est un parcours de formation vidéo basé sur une méthodologie inductive, réalisé avec des techniques de production avancées, typiques des séries télévisées , et avec un storytelling immersif, conçu pour immerger l'utilisateur dans des situations réelles qui reproduisent les conséquences d'une cyber-attaque générée par un comportement humain incorrect.

La méthodologie inductive mise en œuvre par Cyber Guru Channel est basée sur l'immersion de l'utilisateur dans une situation réelle et sur un processus d'auto-identification avec la cybermenace, qui prend une forme concrète et donc possible.

L'utilisateur prend conscience non pas à travers une notion, mais à travers une narration, qui agit d'abord sur la perception du danger, puis sur l'élément notionnel.

L'élément conceptuel est « induit » par la narration elle-même, et renforcé par le matériel d'approfondissement mis à la disposition de l'utilisateur.

Les vidéos de la plateforme Cyber Guru Channel sont réalisées avec des techniques de production avancées et avec une narration particulièrement engageante.

Dans ce parcours de formation particulier, où la clé de la compréhension réside dans l'implication dans une histoire, l'utilisateur est en outre soutenu par la disponibilité, au sein de la plate-forme, du matériel d'approfondissement nécessaire, qui fournit les supports théoriques nécessaires pour accroître son niveau de sensibilisation à la menace au cœur de l'histoire.

CYBER GURU CHANNEL PRÉVOIT :

- **PLUSIEURS FORMATS VIDÉO AVEC DIFFÉRENTES NARRATIONS ;**
- **UNE DOCUMENTATION DÉTAILLÉE POUR CHAQUE ÉPISODE ;**

- **INTÉGRATION AVEC LE MÉCANISME DE GAMIFICATION ;**

- **FONCTIONS DE STUDENT CARING, POUR MOTIVER LA PARTICIPATION ;**

- **UN REPORTING AVANCÉ SUR LE NIVEAU D'UTILISATION**

Le niveau d'engagement généré par Cyber Guru Channel est très élevé et devient donc un tremplin pour d'autres parcours de formation visant à la sensibilisation à la cybersécurité et pour des activités de communication interne visant à la diffusion de la culture de la cybersécurité dans l'organisation.

Les vidéos de formation, intégrées à la plateforme Cyber Guru, sont enrichies de tous ses composants de contrôle d'accès, d'engagement et de surveillance de cette plateforme.


Cyber
Guru

WWW.CYBERGURU.IT