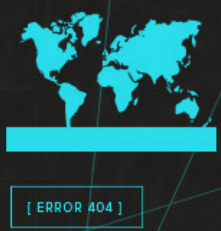
ARMIS®

L'ÉTAT DE
CYBERGUERRE

RAPPORT ARMIS SUR L'ÉTAT DE CYBERGUERRE ET LES TENDANCES : 2022-2023

RECENSE LES IMPRESSIONS DE PROFESSIONNELS DE LA SÉCURITÉ ET DE L'INFORMATIQUE DU MONDE ENTIER EN MATIÈRE DE PRÉPARATION ET DE DÉPENSES LIÉES À LA CYBERSÉCURITÉ



Les personnes interrogées affirment que les organisations manquent de préparation pour faire face à la cyberguerre, qu'il n'existe pas de réponse unique aux attaques par rançongiciel et que les dépenses liées à la cybersécurité sont en hausse.

AVANT-PROPOS PAR NADIR IZRAEL

CTO ET COFONDATEUR, ARMIS

Armis a le plaisir de partager avec vous les résultats de son étude et de son analyse du marché mondial de la cyberguerre. Nous espérons que vous trouverez le contenu de ce rapport mondial, ainsi que celui des rapports régionaux qui l'accompagnent intéressant et utile.

Commençons par clarifier le contexte dans lequel nous évoluons aujourd'hui : **les plus éminents analystes**[1] prévoient que d'ici 2025, les cybercriminels disposeront d'environnements de technologies opérationnelles (OT) armés pour réussir à blesser ou tuer des êtres humains. Même si ce constat peut sembler extrême, cela vient étayer une tendance propre à la cyberguerre, caractérisée par le fait que les cybercriminels passent de la reconnaissance et de l'espionnage à l'application cinétique des outils de cyberguerre. De telles cyberarmes cinétiques ont déjà été découvertes, bien qu'aucune n'ait été spécifiquement déployée à des fins létales. Par exemple, en 2017, le logiciel malveillant Triton, capable de **cibler et de désactiver**[2] les contrôleurs des systèmes instrumentés de sécurité (SIS) d'une usine pétrochimique d'Arabie saoudite a été découvert, ce qui aurait pu contribuer à une catastrophe à l'échelle de l'usine si le problème n'avait pas été identifié à temps. De plus, en **février 2021**[3], un hacker a tenté d'empoisonner l'eau d'un bâtiment de service de distribution d'une petite ville américaine de l'État de Floride via un accès à distance. Des attaques par rançongiciel contre le secteur des services de santé ont déjà **entraîné des décès**[4]. L'impact potentiel des cyberattaques, qu'il soit intentionnel ou non, est donc évident.

Si les cybermenaces cinétiques sont le futur de la course aux cyberarmes, les cyberarmes ne sont pas un nouveau concept. Le monde a pu avoir un aperçu du cyberarsenal de la **National Security Agency**[5] (NSA) en 2016 suite aux **fuites organisées par le groupe des Shadow Brokers**[6], qui ont exposé certaines des cyberarmes les plus puissantes et les moins détectables de la planète. Le cyberarsenal qui a fuité, qui comprenait la vulnérabilité EternalBlue, est devenu le socle de certaines des attaques les plus étendues de l'histoire, notamment NotPetya et WannaCry.

Le développement de ces cyberarmes a également accéléré l'émergence d'un secteur à part entière connu sous le nom de « marché zero-day », une association obscure de chercheurs, de courtiers et de sites Web qui cherchent à tirer profit des attaques zero-day. Bien que personne ne connaisse le montant exact que représente ce marché dans son ensemble, des listes de prix disponibles au public ont révélé que le prix d'une attaque « zéro-clic » fonctionnelle était de **2,5 millions pour Android et de 2 millions pour iOS**[7].

Ce paysage continue d'évoluer de manière significative et a radicalement changé au cours des cinq dernières années, notamment après l'invasion de l'Ukraine par la Russie en février 2022. Il est donc impératif que les chefs d'entreprise et les responsables informatiques comprennent l'évolution du paysage des menaces afin d'améliorer leur posture de cybersécurité et de pouvoir se défendre contre ces attaques. C'est ce qui a motivé l'élaboration du **Rapport Armis sur l'état de cyberguerre et les tendances : 2022-2023**[8]. Pour préparer ce rapport, Armis a commandé une étude exclusive menée auprès de 6 021 professionnels de la sécurité et de l'informatique dans des entreprises de plus de cent collaborateurs aux États-Unis, au Royaume-Uni, en Espagne, au Portugal, en France, en Italie, en Allemagne, en Autriche, en Suisse, en Australie, à Singapour, au Japon, aux Pays-Bas ainsi qu'au Danemark. Par ailleurs, Armis a utilisé les données de sa plateforme primée Asset Intelligence and Security Platform pour analyser les résultats de l'enquête par rapport aux tendances des données du monde réel. Les questions posées portaient notamment sur les points suivants :

- Pensez-vous que votre organisation est bien préparée face à la cyberguerre ?
- Avez-vous confiance dans la capacité du gouvernement de votre pays à faire face à une cyberguerre ?
- Quelle est la politique de votre organisation en matière de paiement des rançons en cas d'attaque par rançongiciel ?
- Quelles sont les pratiques de cybersécurité mises en œuvre au sein de votre organisation ?

Les réponses à ces questions ainsi qu'à d'autres ont été utilisées pour recenser les impressions des professionnels de la sécurité et de l'informatique au niveau mondial, régional et national, au cas par cas, afin de faire un bilan sur les tendances suivantes. Examinons de plus près les résultats et leur incidence sur la manière dont les organisations peuvent améliorer leur posture de cybersécurité pour se défendre contre les attaques liées à la cyberguerre.

CYBERGUERRE

\si.bɛʁ.gɛʁ\

NOM :

L'utilisation de cyberattaques, provoquant des dommages comparables à ceux d'une guerre réelle et/ou perturbant des systèmes ou des services vitaux. Les objectifs recherchés peuvent être l'espionnage, le sabotage, la propagande, la manipulation de l'opinion publique, l'intimidation ou l'interruption de services essentiels.

TABLE DES MATIÈRES

LES ORGANISATIONS SONT-ELLES BIEN PRÉPARÉES À AFFRONTER LA TEMPÊTE QU'EST LA CYBERGUERRE ?

Principaux résultats du rapport mondial.

Selon l'enquête réalisée par Armis, un tiers (33 %) des organisations mondiales ne prennent pas au sérieux la menace de la cyberguerre. Ces organisations se disent indifférentes ou peu préoccupées par l'impact de la cyberguerre sur leur organisation dans son ensemble, laissant potentiellement des failles de sécurité ouvertes. De plus, les tensions géopolitiques croissantes engendrées par la guerre en Ukraine ont rendu la menace d'une cyberguerre beaucoup plus plausible. Plus de 64 % des professionnels de la sécurité et de l'informatique interrogés par Armis sont d'accord sur le fait que la guerre en Ukraine a augmenté la menace d'une cyberguerre, et plus de la moitié (54 %) des personnes interrogées qui sont les seuls décideurs en matière de sécurité informatique ont déclaré qu'ils ont été confrontés à une augmentation des menaces sur leur réseau entre mai et octobre 2022 comparativement aux six mois précédents. Dans ces conditions, il n'est pas surprenant que 45 % des personnes interrogées déclarent avoir dû signaler un acte de cyberguerre aux autorités.

CADRES DIRIGEANTS INTERROGÉS :

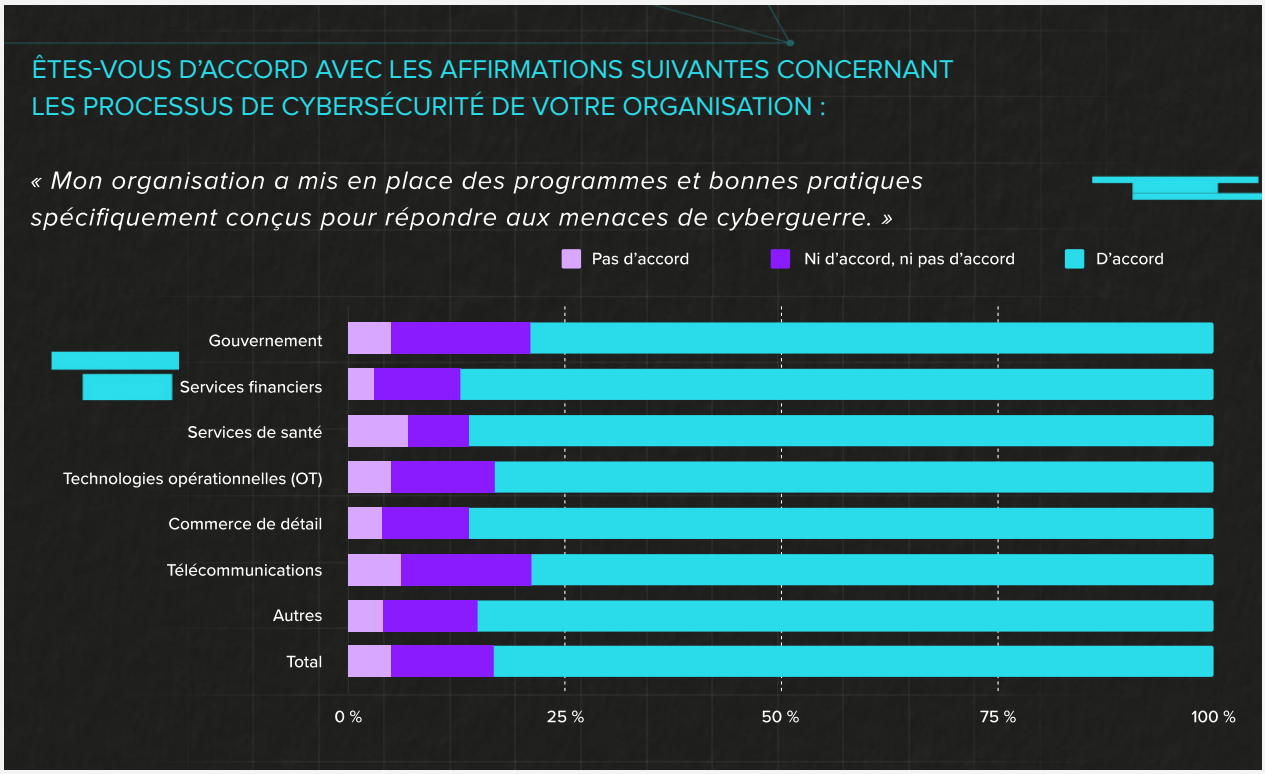
Avez-vous été confronté à plus ou moins de menaces, le cas échéant, sur votre réseau au cours des six derniers mois par rapport aux six mois précédents ?

SECTEURS VERTICAUX	SECTEUR INDUSTRIEL	PLUS	AUTANT	MOINS	S/O	JE NE SAIS PAS
Gouvernement	Gouvernement, autorité locale, agence du secteur public	**39 %**	44 %	14 %	3 %	
Services financiers	Services financiers et assurances	**20 %**	70 %	10 %		
Services de santé	Médical, services de santé, industrie pharmaceutique	**26 %**	52 %	20 %	2 %	
Technologies opérationnelles (OT)	Automobile	**43 %**	33 %	24 %		
	Distribution, logistique, transport	**30 %**	48 %	19 %	4 %	
	Agroalimentaire	**44 %**	44 %	11 %		
	Fabrication, ingénierie	**40 %**	30 %	8 %	22 %	
	Pétrole, gaz, exploitation minière, construction, agriculture	**30 %**	50 %	15 %	5 %	
	Transport	**32 %**	36 %	18 %	14 %	
	Fournisseurs : Eau et électricité	**15 %**	62 %	15 %	8 %	
Total OT		**37 %**	35 %	12 %	16 %	
Autres	Organismes de bienfaisance, à but non lucratif	**29 %**	29 %	14 %	29 %	
	Autre (veuillez préciser)	**33 %**	43 %	5 %	10 %	10 %
	Technologie	**42 %**	25 %	30 %	2 %	1 %
Total Autre		**42 %**	25 %	29 %	2 %	1 %
Commerce de détail	Services de commerce de détail/de gros	**42 %**	40 %	15 %	3 %	
Télécommunications	Télécommunications, câble, satellite	**44 %**	38 %	18 %		
Total		**40 %**	31 %	22 %	6 %	0,5 %

Les données exclusives de la plateforme Armis Asset Intelligence & Security, recueillies entre le 1er juin 2022 et le 30 novembre 2022, ont confirmé que les tendances évoquées ci-dessus n'ont pas ralenti, mais se sont plutôt aggravées. Les menaces contre la clientèle internationale d'Armis ont augmenté de 15 % entre septembre et novembre par rapport au trimestre précédent. En outre, Armis a identifié que les menaces visant des organisations essentielles représentent le pourcentage le plus élevé, les établissements de santé se plaçant au deuxième rang des entreprises les plus ciblées par rapport aux autres secteurs d'activité.

une cible privilégiée, étant donné leur importance pour la sécurité nationale et économique.

La détérioration du paysage des menaces a eu un impact tangible sur les projets de transformation numérique à l'échelle mondiale, ralentissant l'innovation dans le monde entier. Plus de la moitié (55 %) des personnes interrogées déclarent que leur organisation a mis en pause ou arrêté ses projets de transformation numérique en raison de ces menaces. Ce pourcentage est encore plus élevé dans certains pays, notamment en Australie (79 %), aux États-Unis (67 %), à Singapour (63 %), au Royaume-Uni (57 %) et au Danemark (56 %).



Si tous les secteurs sont exposés à des cyberattaques, les infrastructures essentielles, les services de santé et les agences gouvernementales sortent du lot et constituent des cibles de premier choix pour les États-nations. Les services de santé sont particulièrement attrayants en raison de l'étendue de la surface d'attaque et de l'effet qu'une attaque pourrait avoir sur les processus stratégiques, ainsi que sur la santé et la sécurité des patients. Les agences gouvernementales sont attractives en raison des données qu'elles stockent. Quant aux infrastructures essentielles, elles continuent d'être

Compte tenu de l'inquiétude suscitée par la menace croissante de la cyberguerre et du coût moyen d'une violation de données qui s'élève à **9,44 millions de dollars américains**[9] aux États-Unis et à 4,35 millions de dollars américains dans le monde, il n'est pas étonnant que les analystes du secteur **prévoient**[10] que les dépenses mondiales en matière de sécurité et de gestion des risques augmenteront de 11,3 % en 2023. Les modèles de travail à distance et de travail hybride, la transition des réseaux privés virtuels (VPN) vers l'accès au réseau zéro confiance (ZTNA) et le passage à l'informatique basée dans le Cloud sont autant

de facteurs qui contribuent à cette situation, mais cela peut en réalité se résumer par une surface d'attaque en constante expansion, associée à une prépondérance de pays capables de développer des cyberarmes sophistiquées. En fin de compte, les organisations numériques et véritablement connectées peuvent-elles se permettre de ne pas augmenter leurs dépenses liées à la cybersécurité ?

Malgré le risque que la cyberguerre ait un impact sur les organisations, la cyberdéfense et la résilience contre de telles attaques restent faibles. De plus en plus d'États-nations se sont détournés des infrastructures essentielles pour s'attaquer à des entités commerciales de toutes formes et de toutes tailles. Ironie du sort : cette étude a révélé que près d'un quart (24 %) des organisations mondiales ne se sentaient pas suffisamment bien préparées à affronter la menace de la cyberguerre. Pourtant, l'élément de sécurité qui revient le moins souvent dans les réponses des professionnels de la sécurité et de l'informatique est la prévention d'une attaque par un État-nation. De plus, même pour les organisations qui sont prêtes à investir dans un programme de cybersécurité solide (les tendances en matière de dépenses seront abordées plus tard dans ce rapport), il est toujours difficile de trouver des personnes capables de remplir les fonctions de cybersécurité et possédant les compétences nécessaires pour surveiller efficacement les technologies et les logiciels associés. Le nombre d'emplois à pourvoir dans le domaine de la cybersécurité **a augmenté de 350 %**[11] entre 2013 et 2021, passant d'un million à 3,5 millions. Selon les prédictions, ce chiffre sera le même en 2025.

QUELS SONT LES SECTEURS LES PLUS VULNÉRABLES ?

MENACES SUR LES INFRASTRUCTURES ESSENTIELLES

Avec le conflit en Ukraine qui se prolonge dans la durée, en 2022, les agences internationales ont émis de nombreuses alertes concernant des cyberopérations malveillantes de la part de la Russie visant les infrastructures essentielles. Il convient de souligner que Industroyer2 et InController/PipeDream sont des outils d'attaque modulaires destinés aux technologies opérationnelles (OT) dans tous les secteurs d'activité et comprennent des systèmes de contrôle et d'acquisition de données (SCADA), des systèmes de contrôle distribués (DCS), des unités terminales distantes (RTU) et des environnements opérationnels d'automates programmables industriels (PLC).

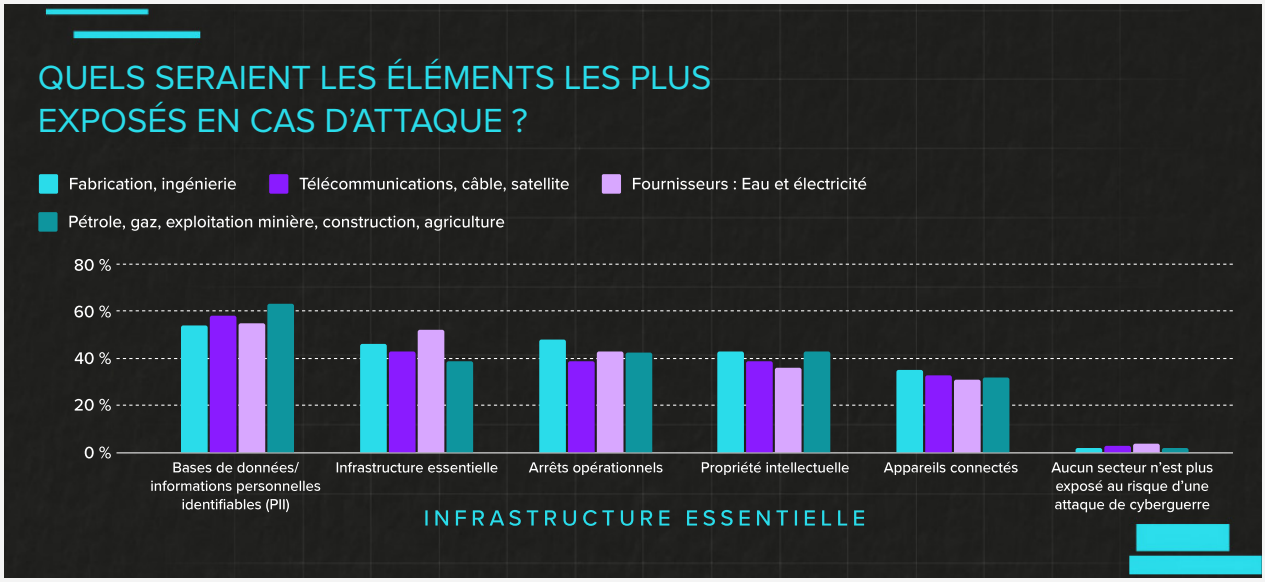
En mai 2021, l'infrastructure de **Colonial Pipeline**[12], qui contrôle près de la moitié de l'essence, du kérosène et du diesel circulant le long de la côte Est des États-Unis, est victime d'une attaque par rançongiciel au niveau informatique, ce qui affecte ses opérations OT. Le piratage de Colonial Pipeline est la plus grande cyberattaque contre une infrastructure essentielle aux États-Unis rendue publique à ce jour. Après s'être entretenu avec le Federal Bureau of Investigation (FBI), le ministère américain de l'Énergie (DOE), le ministère de la Sécurité intérieure (DHS) et la Cybersecurity and Infrastructure Security Agency (CISA), Colonial Pipeline a pris la décision difficile de payer la rançon en cryptomonnaie demandée par les pirates de DarkSide.

L'entreprise a estimé que payer pour obtenir la clé de décryptage était le meilleur moyen de remettre rapidement le pipeline en service. Environ un mois plus tard, le FBI a pu récupérer la majeure partie de la rançon en saisissant les bitcoins appartenant aux pirates.

La cyberguerre entre les États-nations ne se limite pas aux pays limitrophes ou aux participants actifs dans le conflit. Les cybercriminels peuvent viser d'autres pays pour un grand nombre de raisons, liées (par exemple, la fourniture d'armes) ou non au conflit. En 2021, les États-Unis ont lancé des accusations officielles contre Nobelium, un acteur étatique des services de renseignement russes, pour avoir piraté SolarWinds avec l'intention d'infiltrer les réseaux gouvernementaux des États-Unis et de l'UE. L'attaque de Nobelium a modifié le paysage des menaces pour pratiquement tous les secteurs. En octobre 2022, le groupe de hackers prorusse Killnet a lancé **des dizaines d'attaques DDoS**[13] visant l'industrie aéronautique américaine et a proclamé que toutes les infrastructures essentielles américaines allaient subir une attaque persistante.

Les chefs d'entreprise n'ont pas pu ignorer la nouvelle de ces attaques continues et croissantes relevant de la cyberguerre, ni les efforts de sensibilisation des organisations publiques et privées. Selon le Rapport Armis sur l'état de cyberguerre et les tendances : 2022-2023, 74 % des responsables d'infrastructures OT essentielles interrogés à l'échelle mondiale rapportent que les conseils d'administration de leurs entreprises travaillent à modifier la culture organisationnelle en matière de cybersécurité en réponse à la menace d'une cyberguerre.

Si l'on examine les secteurs les plus couramment associés à une infrastructure essentielle (voir le tableau ci-dessous), la convergence de l'informatique et des technologies opérationnelles (OT) dans l'industrie 4.0 ressort clairement des réponses. Nous avons demandé aux participants de choisir les trois éléments les plus exposés en cas de cyberguerre. Dans chaque secteur, les bases de données et les informations personnelles identifiables (PII) sont arrivées en première position. L'infrastructure essentielle (équipement physique et usines), les temps d'arrêt opérationnels et la propriété intellectuelle arrivent en milieu de liste des domaines à risque. Les appareils connectés étant les moins préoccupants dans les secteurs avec des infrastructures essentielles.



Ces réponses révèlent un large spectre de préoccupations autour des environnements IT[14], OT[15] et de systèmes de contrôle industriel (ICS)[16], ce qui n'est pas surprenant étant donné la convergence récente et rapide de ces systèmes autrefois disparates. Dans les infrastructures essentielles, la plupart des environnements ICS et OT datent d'il y a des dizaines d'années et sont toujours sécurisés en grande partie par des méthodes traditionnelles basées sur la conception du réseau et l'accès basé sur des rôles. Plus ces environnements sont interconnectés et automatisés, plus la surface d'attaque s'étend jusqu'à la jonction entre les réseaux existants et des équipements qui n'ont jamais été prévus pour se connecter à ces réseaux.

C'est cette jonction d'équipements connectés qui pousse Armis à mener des recherches sur les vulnérabilités de sécurité afin d'aider à sensibiliser aux vulnérabilités et aux attaques qui touchent les infrastructures essentielles. En mars 2022, l'équipe de recherche d'Armis a dévoilé au public trois vulnérabilités zero-day susceptibles d'affecter plus de 20 millions d'appareils APC Smart-UPS (onduleurs intelligents), qui fournissent une alimentation de secours aux équipements stratégiques au sein des centres de données, des installations industrielles, des hôpitaux, etc. Ces vulnérabilités, communément appelées TLStorm[17], permettent aux cybercriminels de désactiver, de perturber et de détruire ces appareils UPS et les équipements qui y sont rattachés. En les exploitant, un cybercriminel peut utiliser les appareils UPS comme des armes. Il peut, par exemple, altérer la tension au point que les appareils prennent feu. Ces vulnérabilités surviennent dans les systèmes cyberphysiques qui relient les mondes numériques et physiques. Il est donc d'autant plus important de les identifier puisqu'elles confèrent aux cyberattaques la possibilité d'avoir de vraies conséquences sur l'infrastructure, de mettre des vies en danger et/ou d'entraîner la destruction physique de l'infrastructure ciblée.

MENACES SUR LES SERVICES DE SANTÉ

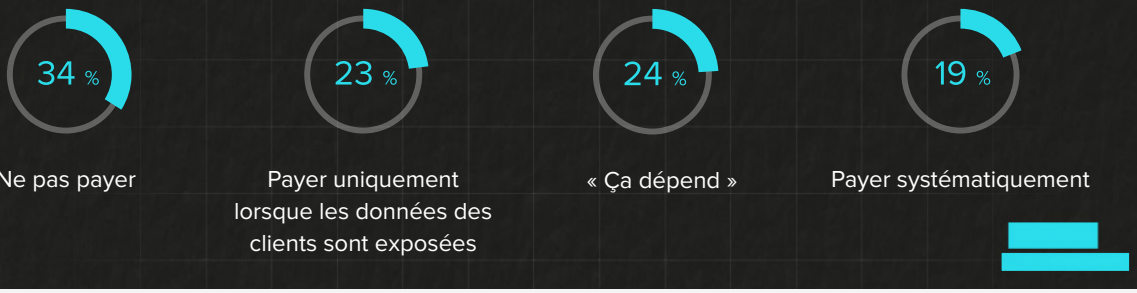
Le secteur des services de santé est d'une importance capitale pour les citoyens de chaque nation. Il est vital pour le bon fonctionnement de toute société et joue un rôle central dans le développement de tout État moderne. Au vu des conséquences concrètes et potentiellement mortelles qui découlent de la mise en péril de la sécurité des patients, les services de santé restent une cible privilégiée par les acteurs malveillants. Par exemple, en octobre 2022, CommonSpirit Health[18] a subi une importante attaque par rançongiciel sur un système sur lequel reposaient 140 hôpitaux et plus de 1 000 sites de soins dans plusieurs villes des États-Unis. À la fin de l'année 2022, cette attaque touchait encore près de 20 millions d'Américains dans 21 États et, par conséquent, le personnel de santé devait prodiguer des soins sans les dossiers médicaux de leurs patients. Bien entendu, c'est une façon très dangereuse de gérer les services de santé. À cause de cela, un enfant de trois ans originaire de l'Iowa a reçu une surdose d'analgésiques. Il a heureusement survécu. Plus tôt en 2020, une cyberattaque beaucoup moins importante contre un hôpital allemand à Düsseldorf[19] a entraîné une panne de réseau et la nécessité de transférer les patients vers d'autres hôpitaux, entraînant la mort d'un patient.

Non seulement les attaques contre les services de santé peuvent être mortelles, mais elles sont aussi extrêmement coûteuses pour les systèmes de santé qui ont déjà des budgets serrés et qui essaient encore de sortir la tête de l'eau après la pandémie de COVID-19. Les directeurs informatiques du secteur des services de santé[20] ont du mal à retenir les talents de haut niveau dans les domaines de la technologie et de la sécurité, car les travailleurs à distance cherchent à percevoir des revenus plus élevés en travaillant dans d'autres secteurs. Cette pénurie de personnel qualifié intervient à un moment critique pour les organismes de santé, qui demeure l'un des secteurs les plus ciblés par la cyberguerre et la cybercriminalité. (Selon IBM, le coût moyen d'une violation dans le secteur des services de santé atteindrait actuellement 10,1 millions de dollars américains[21], soit plus que les 9,44 millions de dollars estimés pour l'ensemble des secteurs.) Lorsque le système de santé public irlandais, appelé Health Service Executive[22], a été attaqué par le rançongiciel Conti en 2021, il a fallu passer à des processus papier, ce qui a entraîné l'annulation de 80 % des rendez-vous des patients et environ 600 millions de dollars américains de frais pour la remise en état et le remplacement des systèmes.

Selon cette étude, 72 % des personnes interrogées responsables de l'informatique dans les secteurs des services de santé, du médical et l'industrie pharmaceutique rapportent que les conseils d'administration de leurs entreprises travaillent à modifier la culture de leur organisation en matière de cybersécurité en réponse à la menace de la cyberguerre. Cette tendance s'explique par la prévalence et la cadence régulière des cyberattaques dans le secteur des services de santé : 45 % des personnes du secteur interrogées

IMPORTANT

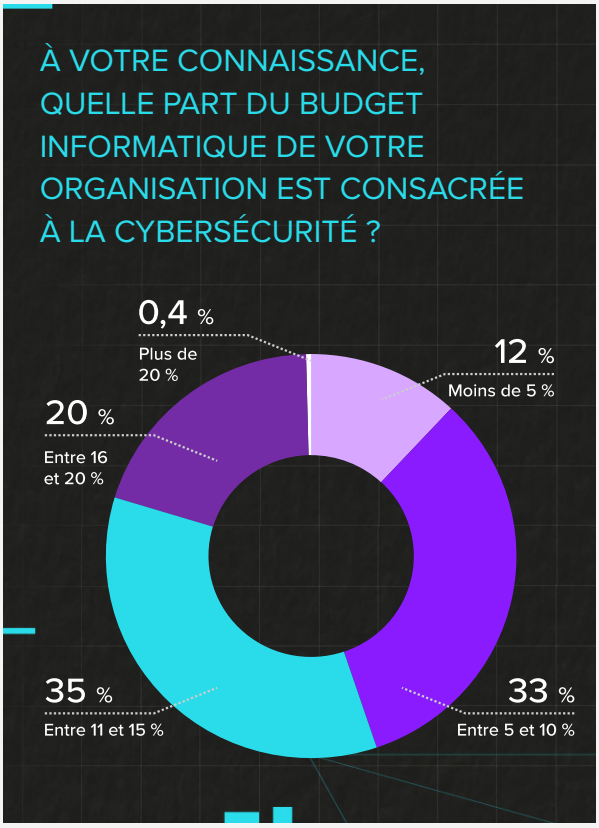
Les organismes de santé mondiaux interrogés par Armis ont indiqué que leur politique en matière de paiement des rançons en cas d'attaque par rançongiciel est la suivante :



ont indiqué qu'elles avaient constaté le même nombre de menaces sur leur réseau entre mai et octobre 2022 par rapport aux six mois précédents, tandis que 28 % ont déclaré avoir été confrontées à davantage de menaces sur les mêmes périodes. En outre, les participants ont indiqué qu'ils étaient assez ou très préoccupés par l'impact de la cyberguerre sur leur organisation dans son ensemble (70 %), sur l'infrastructure essentielle de leur entreprise (72 %) et sur les services de leur entreprise (68 %).

Malgré cela, les dépenses de cybersécurité des organismes de santé restent faibles par rapport à celles des autres secteurs d'activité dans le monde. Près de la moitié (45 %) des entreprises du secteur des services de santé consacrent moins de 10 % de leur budget IT à la cybersécurité. En moyenne, les personnes du secteur des services de santé interrogées ont indiqué qu'elles consacraient environ 11 % du budget IT de leur entreprise à la cybersécurité, certaines y consacrant entre 11 à 15 % (35 %) ou 16 à 20 % (20 %), et un petit nombre 20 % du budget ou plus (moins de 1 %).

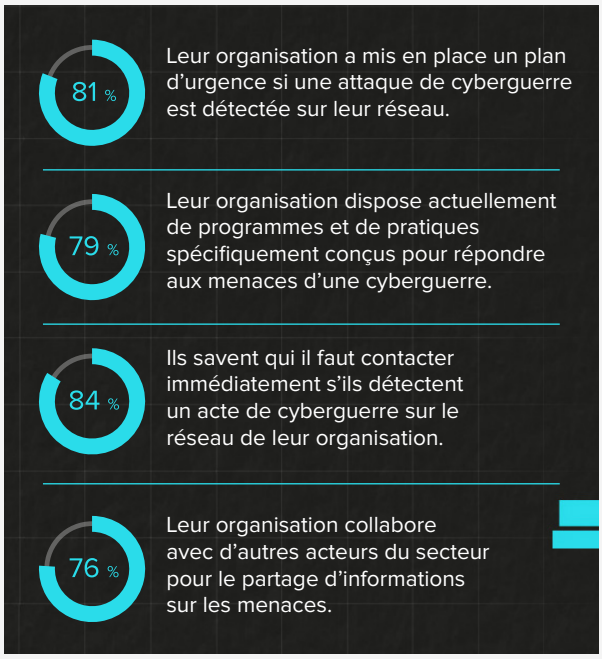
Alors que les technologiques informatiques pour les services de santé continuent de progresser et de transformer numériquement les soins aux patients, l'innovation peut résoudre certains des principaux défis auxquels le secteur des services de santé est confronté, tels que la pénurie de personnel, l'augmentation des coûts et les problèmes de conformité. Toutefois, 55 % des personnes interrogées ont déclaré que la menace de la cyberguerre était susceptible de ralentir ce processus de transformation numérique. Cela peut avoir un impact considérable sur la vie des patients, car les avantages de la transformation numérique risquent de ne pas être pleinement exploités si elle est ralentie par des cyberattaques. Si la transformation numérique n'est pas adoptée en gardant la cybersécurité au premier plan,



ces nouveaux projets pourraient être détournés. Prenons, par exemple, les systèmes de tubes pneumatiques (PTS). Ces systèmes sont utilisés dans plus de **80 % des hôpitaux en Amérique du Nord[23]** et dans plus de 3 000 hôpitaux à travers le monde. Ils permettent d'automatiser la logistique et le transport des matériaux dans les hôpitaux grâce à un réseau de tubes pneumatiques. Ces systèmes jouent un rôle crucial dans les soins aux patients et sont utilisés presque 100 % du temps. En 2021, les chercheurs d'Armis ont identifié neuf vulnérabilités dans ces appareils, baptisées **PwnedPiper[24]**, qui, si elles sont utilisées par des cybercriminels, pourraient permettre à un pirate non authentifié de prendre le contrôle total d'un hôpital afin de déployer une attaque sophistiquée par rançongiciel ou de divulguer des informations médicales sensibles.

MENACES SUR LES AGENCES GOUVERNEMENTALES

Les équipements sont le dénominateur commun au sein de notre monde numérique moderne et toujours plus fragmenté. Aucune entité ne dispose de plus de ressources (personnes, appareils ou logiciels) que les agences gouvernementales et les personnes qu'elles cherchent à servir et à protéger. Malgré ce qui s'est passé ces dernières années, les personnes interrogées au niveau mondial appartenant au secteur public semblent confiantes lorsqu'il s'agit de la gestion de la cyberguerre :



Cette confiance accrue provient peut-être du fait que les alliances mondiales partagent davantage de renseignements. Les nations de l'alliance Five Eye[25] (Australie, Canada, Nouvelle-Zélande, Royaume-Uni et États-Unis) partagent désormais de manière proactive leurs ressources en matière de renseignement afin de renforcer leur posture de sécurité globale, notamment en ce qui concerne la protection des équipements. Plus intéressant encore, si l'un de ces pays était amené à entrer dans un conflit lié à la cyberguerre, 63 % des personnes interrogées au niveau mondial ont déclaré qu'elles seraient favorables à la création d'une ligue de cyberdéfense.

Cette démonstration massive de la confiance des agences est également mise en évidence dans la mesure où l'enquête révèle que 9 personnes interrogées sur 10 (90 %) appartenant à une agence gouvernementale ont confiance dans la capacité de leur pays d'origine à se protéger contre la cyberguerre. Cependant, lorsque des violations sont détectées, 55 % des personnes interrogées au niveau mondial pensent que leurs agences gouvernementales sont incapables de faire face aux impacts négatifs des activités des cybercriminels et de les corriger. Cela n'aurait pas pu être plus vrai en avril 2022, lorsque les pirates du groupe russe du rançongiciel connu sous le nom de Conti **se sont attaqués au gouvernement du Costa Rica[26]**. Leur attaque brutale a complètement bloqué les systèmes fiscaux du pays, provoquant des ravages sur les exportations et retardant les paiements des travailleurs locaux. Durant cette attaque, Conti a réussi à divulguer **97 % des données volées[27]**. En mai 2022, la situation s'était tellement détériorée que le gouvernement du Costa Rica n'a eu d'autres choix que de déclarer l'état d'urgence.

Aux États-Unis, les agences gouvernementales, les institutions et les systèmes éducatifs ont ressenti les répercussions mondiales des groupes impliqués dans la cyberguerre. Au plus fort de la pandémie de 2020 aux États-Unis, 79 attaques par rançongiciel ont été menées contre des agences gouvernementales. On estime que ces agences auraient perdu environ **18,8 milliards de dollars[28]** à cause des frais de récupération et des temps d'arrêt. Suite à cela, le gouvernement américain a lancé une offensive au troisième trimestre de l'année 2021 afin de réduire le volume global de rançongiciels avec le site Web **StopRansomware.gov[29]**. Il reste à espérer que, grâce à des partenariats public-privé, les agences gouvernementales, comme celles des États-Unis, pourront commencer à mieux se protéger contre les rançongiciels, mieux les détecter et mieux corriger les dégâts causés par ces logiciels.

IMPORTANT

Les organisations gouvernementales sont, tous secteurs confondus, le secteur le moins susceptible de payer une rançon en cas d'attaque par rançongiciel, avec 43 % des personnes interrogées déclarant que la politique de leur organisation est de ne jamais payer (chiffre nettement supérieur à la moyenne mondiale (26 %) du nombre de personnes interrogées dont l'organisation a pour politique de ne jamais payer).

QUELLES SONT LES TENDANCES EN MATIÈRE DE CYBERSÉCURITÉ DANS LE MONDE ?

IL N'EXISTE PAS DE RÉPONSE UNIQUE AUX ATTAQUES PAR RANÇONGICIEL

Nombreux sont ceux qui prennent les attaques par rançongiciel pour des actions visant uniquement à voler des données sensibles. Cependant, il s'avère que la plupart des organisations sont des cibles faciles et les cybercriminels sont des opportunistes. Après tout, il est beaucoup plus efficace et rentable d'extorquer une rançon de plusieurs millions de dollars à ces entreprises en échange de l'accès à leurs opérations que d'exfiltrer et de vendre des centaines de milliers de données individuelles sur le marché noir.

Que le rançongiciel soit déployé par des États-nations ou des cybercriminels, l'anatomie d'une attaque par rançongiciel reste à peu près la même. L'attaque commence par l'entrée dans l'environnement, qui peut se faire via un site Web compromis, une attaque par hameçonnage ou une attaque ciblée. Une fois à l'intérieur, les cybercriminels se déplacent latéralement dans le réseau, en élevant leurs privilèges et en se frayant un chemin dans le réseau. Grâce à des tunnels, les cybercriminels établissent une connexion de commande et de contrôle qui aboutit à l'exfiltration des données d'une organisation et au démarrage d'un rançongiciel qui crypte ces données sur le système cible.

DarkSide est un groupe de cybercriminels d'Europe de l'Est qui a développé REvil, un outil d'attaque par rançongiciel qui était à l'origine une variante de GandCrab et qui est l'une des plateformes de Ransomware-as-a-Service (RaaS) les plus connues grâce à l'attaque contre Colonial Pipeline de 2021 que nous avons mentionnée plus haut. Ce groupe a fait sa première apparition en avril 2019 et a eu une forte activité jusqu'en octobre 2021, lorsque les serveurs de REvil ont été piratés puis mis hors ligne dans le cadre d'une opération menée par plusieurs pays. Jusque-là, DarkSide fournissait ses logiciels malveillants à des « affiliés » et partageait la rançon avec les clients menant les attaques. Outre le logiciel malveillant lui-même, DarkSide fournissait le mécanisme de décryptage (qui est toujours considéré comme l'un des systèmes de décryptage les plus sophistiqués de toutes les familles de logiciels malveillants), l'infrastructure pour les chats du darknet, les sites dédiés aux fuites sur le darknet et des services de blanchiment d'argent. Avec l'aide de courtiers d'accès initial,

IMPORTANT

Qui paye, et qui ne paye pas ?

Un peu plus de trois professionnels de l'informatique interrogés sur 10 (31 %) travaillant au sein d'une entreprise de plus de 500 collaborateurs ont déclaré que la politique de leur organisation en matière de paiement des rançons en cas d'attaque par rançongiciel était de ne jamais payer, tandis que plus d'un cinquième (23 %) des professionnels de l'informatique interrogés dans une entreprise comptant entre 100 et 249 collaborateurs ont dit la même chose. Ces réponses changent selon les pays : près de la moitié (47 %) des professionnels de l'informatique interrogés travaillant aux États-Unis ont déclaré que la politique de leur entreprise en matière de paiement des rançons en cas d'attaque par rançongiciel était de payer systématiquement, contre seulement 1 sur 14 (7 %) au Japon.

une nouvelle catégorie de cybercriminels qui vendent l'accès à un réseau compromis, les affiliés accèdent à un réseau cible, lancent la charge utile de REvil et négocient une rançon avec l'organisation concernée en échange de la récupération des données cryptées.

Comme si la prolifération des rançongiciels et la progression du marché du zero-day ne suffisaient pas, le secrétaire général d'Interpol, Jurgen Stock, a déclaré en mai 2022 qu'il craignait que des cyberarmes développées par des États se retrouvent sur le darknet au cours des deux prochaines années. « C'est un problème majeur dans le monde physique, les armes utilisées sur le champ de bataille seront utilisées par les organisations criminelles de demain », a déclaré Stock lors d'un panel **modéré par CNBC**[30] durant le Forum économique mondial de Davos, en Suisse.

Lorsqu'on a demandé aux personnes interrogées dans le cadre de cette enquête quelle était la politique de leur organisation en matière de paiement des rançons en cas d'attaque par rançongiciel, les professionnels de l'informatique du monde entier étaient divisés. 24 % des personnes interrogées ont indiqué que leur organisation payait systématiquement, 31 % ont déclaré que leur organisation payait uniquement lorsque les données des clients étaient exposées, 26 % ont révélé que l'organisation ne payait jamais, et 19 % que cela dépendait.

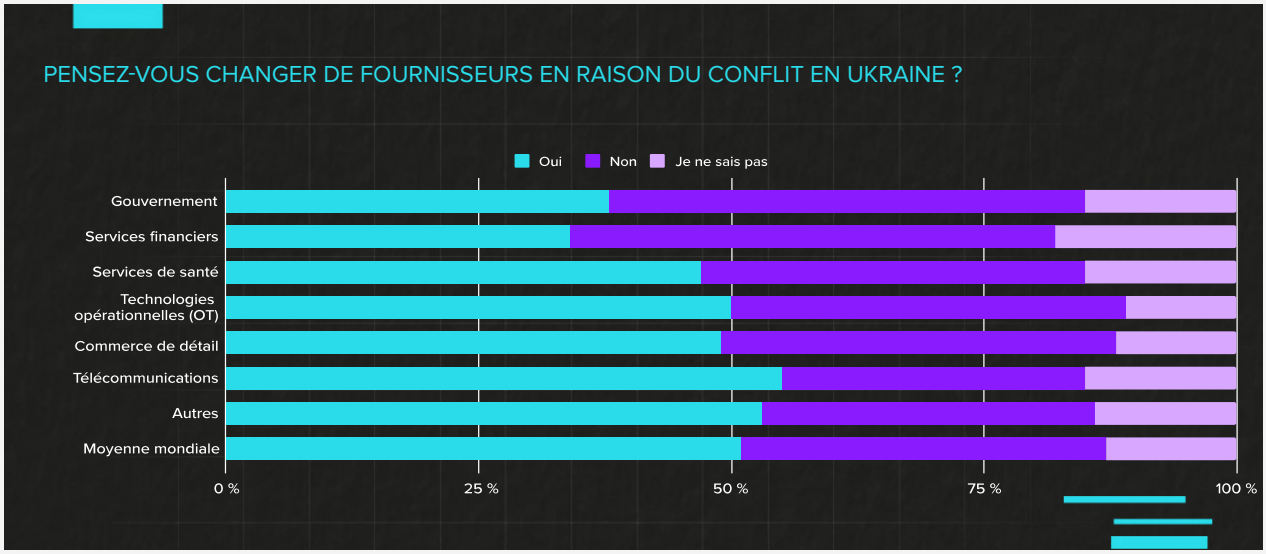
LES DÉPENSES LIÉES À LA CYBERSÉCURITÉ CONTINUENT D'AUGMENTER

Si vous vous demandez dans quoi les entreprises vont dépenser leur budget IT, vous ne serez pas surpris d'apprendre qu'elles prévoient d'augmenter leurs dépenses dans les services de cyberdéfense, de résilience et de protection.

Un peu plus des trois quarts (76 %) des professionnels de l'informatique interrogés ont affirmé que les conseils d'administration de leurs entreprises travaillaient à modifier la culture de leur organisation en matière de cybersécurité en réponse à la menace de la cyberguerre. Il s'agit d'un point important, car la surveillance exercée par le conseil d'administration était rarement assurée auparavant, et ces personnes assument désormais une responsabilité partagée dans l'amélioration de la posture de cybersécurité d'une organisation.

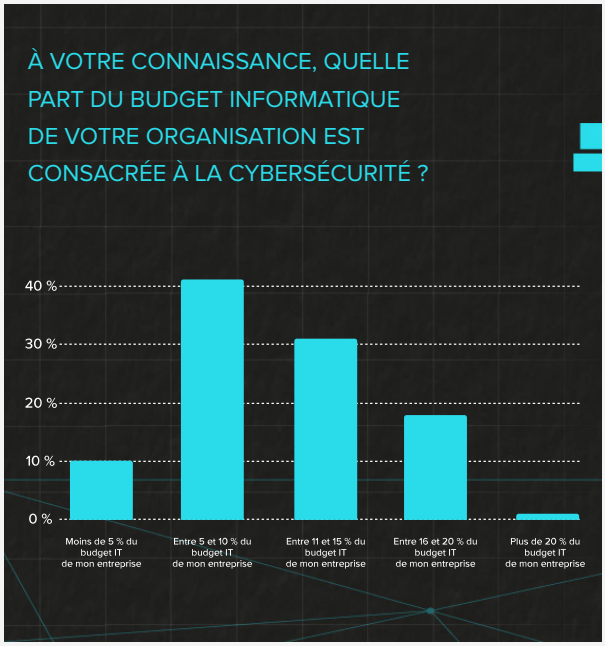
Dans ce contexte, un peu plus de la moitié (51 %) des personnes interrogées au niveau mondial ont déclaré qu'elles reconsidéraient leurs fournisseurs en raison du conflit en Ukraine et qu'elles prévoyaient que leur organisation intègre de nouveaux fournisseurs de cybersécurité ou de services de sécurité gérés (MSSP) immédiatement (31 %) ou au cours des six prochains mois (29 %). Il est essentiel que les fournisseurs soient conscients des tendances en matière de dépenses et sachent où les organisations ont le plus besoin de leurs services, afin de leur fournir les bonnes solutions.

> *« La pénurie de compétences dans le domaine de la cybersécurité reste un problème majeur, car le manque d'effectifs accroît la demande de services ou de solutions, ce qui s'inscrit parfaitement dans les capacités stratégiques des partenaires. La pénurie de compétences fait du marché de la cybersécurité un marché porteur, notamment pour les MSSP et les partenaires qui cherchent à réduire les risques de répercussions sur leur activité en développant des services internes pour de meilleurs rendements. »*
>
> **TIM MACKIE**
> VP WORLDWIDE CHANNEL, ARMIS



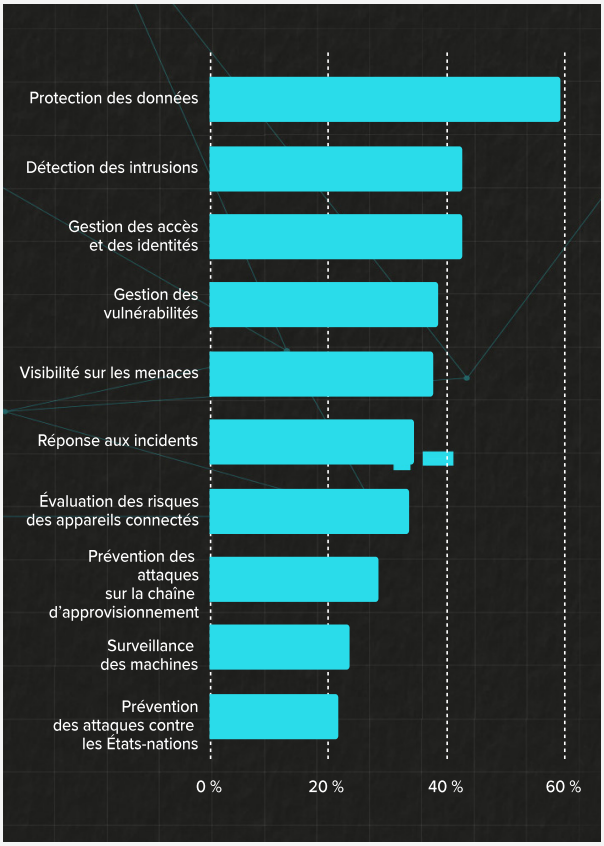
En examinant les données recueillies, il ressort que près de 4 professionnels de l'informatique sur 5 (78 %) ont déclaré à propos des événements mondiaux récents soudains et en cours (tels que la pandémie, le conflit en Ukraine, etc.), qu'il était probable que leur entreprise investisse une plus grande part de son budget dans la cybersécurité, et près de 2 sur 5 personnes interrogées (37 %) pensent que c'est très probable. Alors, combien les organisations dépensent-elles, et sur quoi portent ces investissements ? Cette enquête a révélé qu'à l'échelle mondiale, le pourcentage moyen des budgets IT alloué à la cybersécurité était de 11 %, et se décomposait comme suit :

Parmi les organisations qui dépensent le plus,



37 % ont déclaré qu'il était très probable qu'elles augmentent bientôt leurs investissements, et 41 % que c'était assez probable. Cependant, les entreprises qui investissent moins sont moins susceptibles d'augmenter leurs dépenses prochainement.

Voici les réponses obtenues au niveau mondial lorsqu'il a été demandé aux personnes interrogées de classer les éléments de sécurité par ordre de priorité absolue :



Plus de 2 professionnels de l'informatique interrogés sur 5 (42 %) prévoient que leur organisation investira immédiatement dans la gestion des vulnérabilités[31], tandis que près de 3 sur 10 (28 %) prévoient de le faire au cours des six prochains mois. En ce qui concerne les investissements dans la gestion des équipements[32], 37 % des personnes interrogées ont indiqué que leurs entreprises réaliseraient des investissements immédiatement, et 30 % ont déclaré qu'elles le feraient au cours des six prochains mois.

Non seulement les entreprises investissent dans des solutions de cybersécurité, mais elles adoptent également des principes qui donnent la priorité à la cybersécurité dans toute l'organisation et investissent dans la formation à la cybersécurité. Un tiers (33 %) des professionnels de l'informatique interrogés prévoient que leurs organisations adopteront immédiatement des modèles « Zero Trust[33] », tandis que 28 % déclarent que cela sera fait au cours des six prochains mois. En ce qui concerne la formation à la cybersécurité, 41 % des personnes interrogées au niveau mondial ont indiqué que leur organisation allait investir immédiatement dans une formation avancée à la cybersécurité, tandis que 46 % ont déclaré qu'elles investiraient au cours de l'année prochaine. Seules 4 % des organisations ont déclaré qu'elles ne prendraient aucune mesure pour améliorer la formation en matière de cybersécurité.

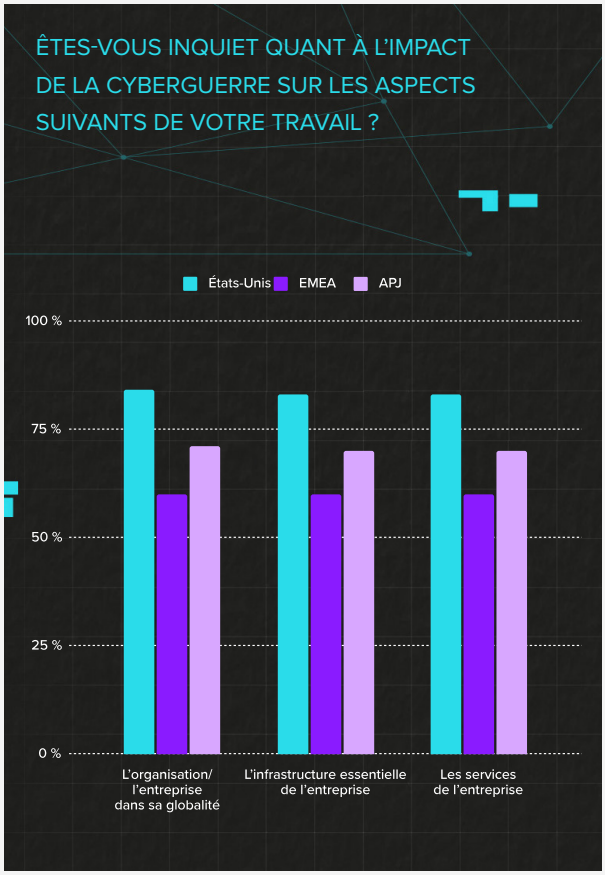
> *« Les équipes de sécurité ont incontestablement besoin d'un degré élevé de visibilité contextuelle sur l'ensemble du paysage d'exploitation technologique si elles souhaitent être efficaces. Le niveau de visibilité dont bénéficient les équipes de sécurité grâce aux technologies modernes aide les CISO et leurs équipes à identifier les opportunités réelles, dans le contexte de l'entreprise et sur la base de données, pour éliminer de l'environnement les anciennes solutions concurrentes et toutes les dépenses connexes. »*
>
> **CURTIS SIMPSON**
> RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (CISO)
> CHEZ ARMIS

QUELLES SONT LES DIFFÉRENCES RÉGIONALES (ÉTATS-UNIS, EMEA ET APJ) QUI RESSORTENT ?

Outre les tendances mondiales mises en évidence ci-dessus, des différences régionales sont également apparues en comparant les réponses des États-Unis, de la région EMEA et de la région APJ (Australie, Japon, Singapour). Par exemple :

INQUIÉTUDES QUANT À L'IMPACT DE LA CYBERGUERRE

Nous avons invité les participants originaires des États-Unis, de la région EMEA et de la région APJ à indiquer leur degré d'inquiétude quant à l'impact de la cyberguerre sur divers aspects de leur travail. Pour la région EMEA, les personnes interrogées ont fait part d'une inquiétude moindre que celle de leurs homologues de la région APJ, qui sont plus inquiets, et ils sont également nettement moins inquiets que les professionnels de l'informatique aux États-Unis, qui ont le niveau d'inquiétude le plus élevé.



ACTIVITÉ DÉCOULANT DES MENACES ET NOMBRE DE VIOLATIONS SUBIES

- D'après l'enquête, les professionnels de l'informatique de la région APJ sont ceux qui ont subi le moins de violations de cybersécurité, avec 53 % des personnes interrogées appartenant à cette région indiquant que leur entreprise a subi une violation de cybersécurité ou plus. À titre de comparaison, près de 3 personnes interrogées sur 5 (58 %) dans la région EMEA et 7 sur 10 (73 %) aux États-Unis ont indiqué que leur entreprise avait subi une violation de cybersécurité ou plus.
- Les organisations américaines ont également connu la plus forte augmentation du nombre de menaces au cours des derniers mois (45 %) par rapport à leurs homologues de la région APJ (36 %) et EMEA (25 %).

CONFIANCE DANS LA PRÉPARATION DE L'ORGANISATION

Les personnes interrogées aux États-Unis sont les plus convaincues que leur entreprise a alloué un budget suffisant pour les programmes, le personnel et les processus de cybersécurité avec près de 9 personnes interrogées sur 10 (88 %) qui ont exprimé leur confiance, contre 78 % dans la région APJ et 76 % dans la région EMEA. En outre, 90 % des personnes interrogées aux États-Unis ont indiqué que les collaborateurs de leur organisation savent à qui s'adresser s'ils remarquaient une cyberactivité suspecte, contre 4 sur 5 (82 %) pour ceux basés dans les régions EMEA ou APJ.

LES PRATIQUES DE SÉCURITÉ DÉJÀ MISES EN ŒUVRE

- Lorsqu'il s'agit d'investir dans une assurance cybersécurité, les entreprises américaines sont les plus susceptibles d'avoir investi (45 %), suivies par la région APJ (37 %) et enfin par la région EMEA (31 %).
- En ce qui concerne l'importance de la formation des collaborateurs, les trois régions ont donné des réponses similaires : États-Unis (51 %), EMEA (49 %) et APJ (45 %).
- Quant à la création d'une culture d'entreprise axée sur la sécurité, 44 % des personnes interrogées aux États-Unis ont indiqué que leur entreprise avait une culture qui mettait la sécurité au premier plan, contre 37 % des personnes interrogées dans la région EMEA et 33 % dans la région APJ.
- La région États-Unis est la plus susceptible d'avoir mis en œuvre un cadre de gestion des cyber-risques (43 %), tandis que seulement 34 % des personnes interrogées dans la région APJ et 31 % dans la région EMEA déclarent avoir mis en œuvre un tel cadre.

SÉCURISATION DES DONNÉES SENSIBLES ET TRAVAIL INTELLIGENT

On a demandé aux personnes interrogées si elles étaient d'accord avec une liste d'affirmations :

- *« Mon organisation détient des données sensibles, il y a des réglementations que nous devons suivre, et nous voulons minimiser toute répercussion négative liée à un événement de sécurité. »*
  - » D'accord : 91 % aux États-Unis, 84 % dans la région APJ et 83 % dans la région EMEA.
- *« La question de la sécurité informatique est devenue plus importante pour les employés avec l'adoption du travail intelligent. »*
  - » D'accord : 91 % aux États-Unis, 85 % dans la région APJ, 81 % dans la région EMEA.

ANALYSE PAYS PAR PAYS

Si vous souhaitez en savoir plus sur les différences régionales décrites ci-dessus, l'équipe d'Armis a préparé une analyse unique pays par pays, particulièrement pertinente pour les nations et territoires étudiés dans le cadre de ce rapport.

Pour lire ces rapports nationaux individuels, qui sont disponibles en anglais, en français et dans d'autres langues, allez sur https://www.armis.com/cyberwarfare.

1. **États-Unis**
2. **Royaume-Uni**
3. **France**
4. **DACH** (Autriche, Suisse, Allemagne)
5. **Péninsule ibérique**
6. **Italie**
7. **Danemark**
8. **Pays-Bas**
9. **APJ** (Australie, Japon, Singapour)

CONCLUSION

Pourquoi ces résultats sont-ils importants et que peut faire votre organisation pour se protéger ?

Les responsables de l'informatique et de la sécurité admettent qu'ils ne prennent pas la menace de la cyberguerre au sérieux, qu'ils ne se sentent pas suffisamment préparés pour y faire face et que l'élément de sécurité le moins important à leurs yeux est la prévention des attaques d'États-nations. En outre, ils constatent une augmentation des menaces liées à la cyberguerre suite à la guerre en Ukraine, comme en témoigne la hausse des menaces sur leurs réseaux entre mai 2022 et octobre 2022 par rapport aux six mois précédents. En plus de ne pas prendre au sérieux la hausse d'activité, ces dirigeants laissent la menace de la cyberguerre avoir un impact sur l'innovation, et admettent avoir mis en pause ou arrêté des projets de transformation numérique en conséquence. Il est clair que ces menaces ne doivent pas être ignorées et qu'il faut les aborder de front pour pouvoir se défendre.

Comme indiqué précédemment dans ce rapport, 37 % des personnes interrogées qui dépensent déjà le plus en matière de cybersécurité ont indiqué être très susceptibles d'augmenter leurs investissements prochainement, et 41 % qu'elles étaient plutôt susceptibles de les augmenter. Plus de 2 professionnels de la sécurité et de l'informatique interrogés sur 5 (42 %) prévoient que leur organisation investira immédiatement dans la **gestion des vulnérabilités**[34], tandis que près de 3 sur 10 (28 %) prévoient de le faire au cours des six prochains mois. En ce qui concerne les investissements dans la **gestion des équipements**[35], 37 % des personnes interrogées ont indiqué que leurs entreprises réaliseraient des investissements immédiatement, et 30 % ont déclaré qu'elles le feraient au cours des six prochains mois.

Les conséquences d'une attaque du réseau sur les opérations et la réputation d'une organisation sont les mêmes, qu'elle soit le fait d'un État-nation ou de cybercriminels. En outre, les réseaux supportant le télétravail et le BYOD (« apportez votre propre appareil »), les vulnérabilités des réseaux privés virtuels et les erreurs de configuration sur les protocoles sont en passe de devenir les points d'entrée les plus courants pour les cybercriminels. Ce phénomène a été exacerbé par la pandémie, et en 2021, les attaques par rançongiciel ont **presque doublé**[36] au niveau mondial.

La mise en place des outils adéquats et d'un plan de réponse aux incidents (IR) n'est que la première étape. En testant régulièrement ce plan, vous pourrez identifier de manière proactive les faiblesses de votre stratégie de cybersécurité et renforcer vos défenses afin de protéger les données sensibles des entreprises et des consommateurs. Sans compter que cela peut permettre aux organisations d'économiser des millions de dollars quant aux coûts des violations de données.

Armis recommande à toutes les organisations de prendre les mesures suivantes :

- Quels que soient les outils et les techniques qu'elles choisissent de mettre en place, nombreuses sont les organisations qui auront besoin d'aide pour atténuer les répercussions d'une attaque en exécutant un plan de réponse aux incidents. Une organisation a souvent intérêt à faire appel à une équipe spécialisée dans la réponse aux incidents afin de réduire les coûts et d'accélérer la réponse aux incidents.
- Une fois une attaque détectée, il est impératif d'en minimiser l'impact. Le cloisonnement ou l'isolement reste les stratégies prédominantes au sein de la plupart des organisations. Il existe diverses techniques d'isolation, et la plupart des outils de détection des points de terminaison et de réponse aux incidents disposent d'une fonctionnalité d'isolation sur

l'appareil. Cela permet aux intervenants en cas d'incident d'isoler les machines individuelles impactées du reste du réseau.

- De plus, avoir une bonne stratégie et un bon processus de sauvegarde constitue également une première ligne de défense contre les attaques des États-nations et des cybercriminels. Les organisations doivent s'assurer que la solution qu'elles choisissent peut résister aux attaques et qu'elle inclut une surveillance et un contrôle d'intégrité continus.
- Une organisation cyber-résiliente devra également investir dans des formations de sensibilisation à la sécurité pour ses collaborateurs. Assurez-vous que les collaborateurs sont formés régulièrement à l'identification des e-mails malveillants et mettez en place des mécanismes de signalement faciles à utiliser.

Il est essentiel que les organisations partent du principe que les tentatives d'attaques aboutiront, qu'elles soient le fait d'un État-nation ou de cybercriminels. En effet, les acteurs malveillants n'ont besoin que d'une seule tentative réussie d'accès au réseau d'une organisation, tandis que les équipes informatiques et de sécurité doivent être capables de se défendre 100 % du temps pour empêcher ces attaques.

Alors, que peuvent faire les organisations pour se protéger ? La détection précoce et la surveillance continue sont le meilleur moyen d'améliorer la posture de sécurité et de corriger rapidement les problèmes. Après tout, vous ne pouvez pas corriger un problème dont vous n'avez pas connaissance et vous ne pouvez pas protéger un équipement sur lequel vous n'avez pas de visibilité. **C'est là qu'Armis peut vous aider.**

PLATEFORME ARMIS ASSET INTELLIGENCE

La **plateforme Armis Asset Intelligence** offre une visibilité unifiée sur les équipements et la sécurité, sur tous les types d'équipements, y compris IT (technologies de l'information), IoT (Internet des objets), OT (technologies opérationnelles), IoMT (Internet des objets médicaux), Cloud, et IoT cellulaire, managés et non managés. Déployée sous forme de plateforme SaaS (software-as-a-service) sans agent, la solution Armis s'intègre facilement dans les piles informatiques et de sécurité existantes afin de fournir rapidement les renseignements contextuels nécessaires à l'amélioration de votre posture de sécurité, sans perturber les opérations ou les flux de travail en cours. Armis aide ses clients à se protéger contre les risques opérationnels et les cyber-risques invisibles, gagner en efficacité, optimiser l'utilisation des ressources et à innover en toute sécurité avec de nouvelles technologies afin de développer leur activité, que la menace soit liée à la cyberguerre ou autre.

Pour demander une démonstration personnalisée. d'Armis, consultez la page : armis.com/demo.

Pour approfondir les résultats du rapport Armis sur l'état de cyberguerre et les tendances : 2022-2023 à l'échelle mondiale, consultez la page : **armis.com/cyberwarfare.**

DONNÉES DÉMOGRAPHIQUES DU RAPPORT

Pour préparer ce rapport, Armis a commandé une étude réalisée avec Censuswide auprès de 6 021 professionnels de la sécurité et de l'informatique dans des entreprises de plus de cent collaborateurs aux États-Unis, au Royaume-Uni, en Espagne, au Portugal, en France, en Italie, en Allemagne, en Autriche, en Suisse, en Australie, à Singapour, au Japon, aux Pays-Bas ainsi qu'au Danemark. Les réponses ont été recueillies entre le 22 septembre 2022 et le 5 octobre 2022.

PERSONNES INTERROGÉES PAR PAYS	
Australie	511
Autriche	100
Danemark	50
France	501
Allemagne	501
Italie	500
Japon	501
Pays-Bas	52
Portugal	251
Singapour	501
Espagne	500
Suisse	50
Royaume-Uni	1003
États-Unis	1000

PERSONNES INTERROGÉES PAR POSTE/RÔLE	
Directeur informatique (CIO)	432
Responsable de la sécurité des systèmes d'information (CISO)	241
Directeur de la technologie (CTO)	530
Technicien support informatique	229
Administrateur de bases de données	457
Analyste sécurité informatique	392
Chef de projet IT	1831
Administrateur réseau	394
Architecte réseau	260
Autres	346
Analyste système	493
Développeur Web	416

PERSONNES INTERROGÉES PAR SECTEUR D'ACTIVITÉ	
Gouvernement, autorité locale, agence du secteur public	369
Services financiers et assurances	120
Médical, services de santé, industrie pharmaceutique	255
OT (automobile, distribution, logistique et transport, agro-alimentaire, fabrication, pétrole, gaz, construction, exploitation minière, agriculture, transport)	1415
Technologies et autre	3133
Commerce de détail et vente en gros	295
Télécommunications	434

NOTES DE FIN DE DOCUMENT

1. https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we
2. https://www.csoonline.com/article/3654833/u-s-charges-russian-government-agents-for-cyber-attacks-on-critical-infrastructure.html
3. https://www.wired.com/story/oldsmar-florida-water-utility-hack/
4. https://www.washingtonpost.com/politics/2021/10/01/ransomware-attack-might-have-caused-another-death/
5. https://www.nsa.gov/
6. https://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html
7. https://arstechnica.com/information-technology/2019/09/for-the-first-time-ever-android-0days-cost-more-than-ios-exploits/
8. https://www.armis.com/cyberwarfare/
9. https://www.ibm.com/reports/data-breach
10. https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i
11. https://www.einpresswire.com/article/556075599/cybersecurity-jobs-report-3-5-million-openings-through-2025
12. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html
13. https://www.darkreading.com/attacks-breaches/us-airports-cyberattack-crosshairs-pro-russian-group-killnet
14. https://www.armis.com/cybersecurity-asset-management/
15. https://www.armis.com/ot-device-security/
16. https://www.armis.com/ics-risk-assessment/
17. https://www.armis.com/research/tlstorm/
18. https://www.healthcaredive.com/news/commonspirit-health-ransomware-cyberattack/634011/
19. https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies
20. https://www.beckershospitalreview.com/healthcare-information-technology/a-war-for-talent-cios-detail-the-challenges-of-retaining-health-it-professionals.html
21. https://www.ibm.com/reports/data-breach
22. https://www.bankinfosecurity.com/irish-ransomware-attack-recovery-cost-estimate-600-million-a-16931
23. https://www.swisslog-healthcare.com/-/media/swisslog-healthcare/documents/products-and-services/transport/translogic-pts/pts-513-swisslog-healthcare-delivers-unmatched-innovation.
24. https://www.armis.com/research/pwnedpiper/
25. https://www.zdnet.com/article/five-eyes-advisory-warns-more-malicious-russian-cyber-activity-incoming/
26. https://www.bleepingcomputer.com/news/security/how-conti-ransomware-hacked-and-encrypted-the-costa-rican-government/
27. https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/
28. https://www.americancityandcounty.com/2021/03/22/report-ransomware-attacks-cost-local-and-state-governments-over-18-billion-in-2020/
29. http://stopransomware.gov
30. https://www.cnbc.com/2022/05/23/military-cyberweapons-could-become-available-on-dark-web-interpol.html
31. https://www.armis.com/avm/

32. https://www.armis.com/armis-asset-management/
33. https://www.armis.com/zero-trust/
34. https://www.armis.com/avm/
35. https://www.armis.com/armis-asset-management/
36. https://www.securitymagazine.com/articles/97166-ransomware-attacks-nearly-doubled-in-2021#:~:text=Ransomware%20attacks%20rose%20by%2092.7,nation%2Dstate%20cyberattacks%20and%20more.

L'ÉTAT DE
CYBERGUERRE

À PROPOS D'ARMIS

Armis, leader de la sécurité et de la visibilité sur les équipements, fournit la première plateforme d'intelligence des équipements unifiée du secteur, conçue pour gérer la nouvelle surface d'attaque étendue que créent les équipements connectés. Les sociétés classées au Fortune 100 font confiance à notre protection continue et en temps réel pour voir tous les équipements managés, non managés dans des environnements IT, Cloud, IoT, IoT des appareils médicaux (IoMT), des technologies opérationnelles (OT), des systèmes de contrôle industriel (ICS) et la 5G, le tout avec un contexte complet. Armis offre une gestion passive des cyberéquipements, la gestion des risques et la mise en application automatisée. Armis est une société privée dont le siège social est situé en Californie.

armis.com

info@armis.com

20230110-1

ARMIS®