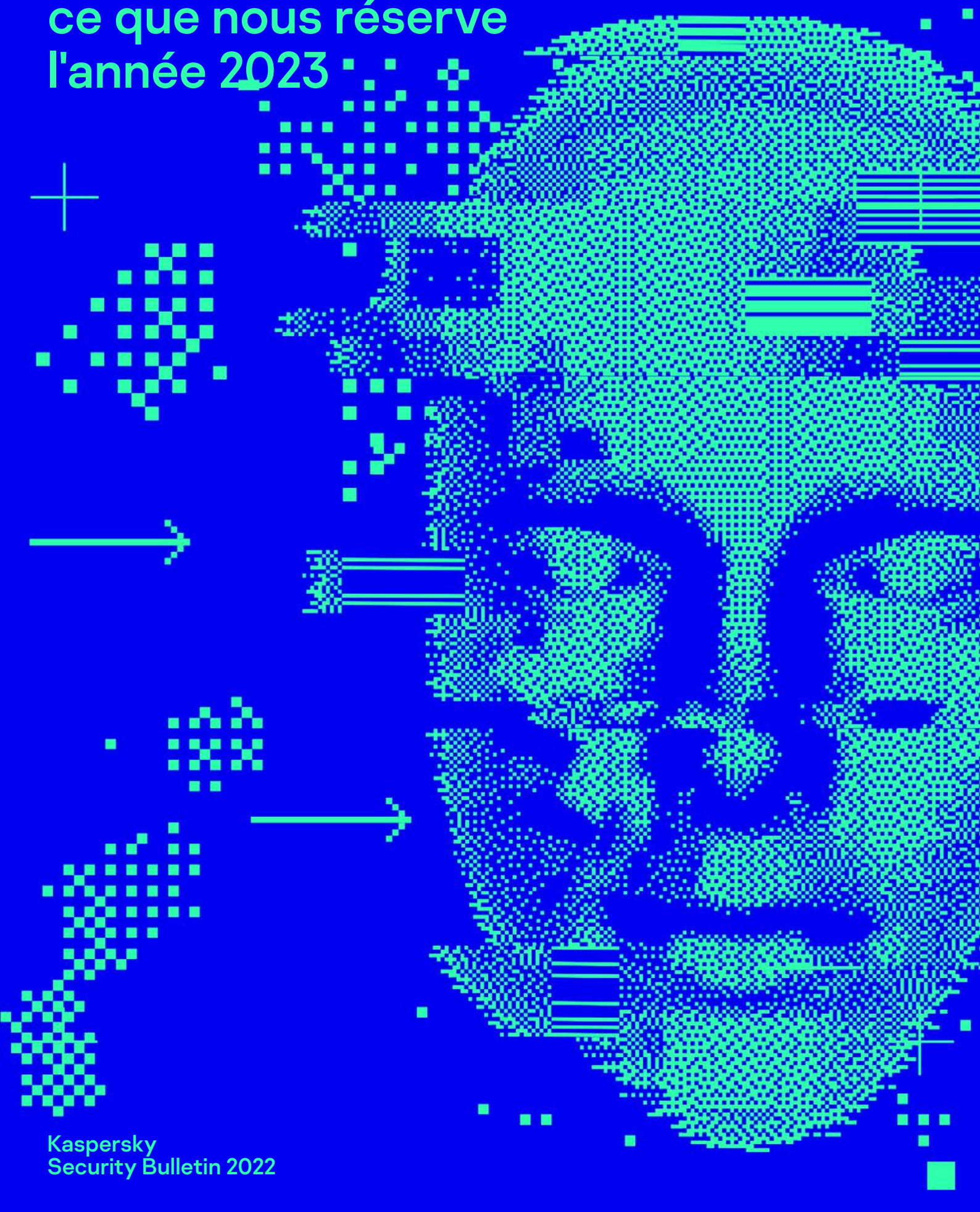
Menaces de cybersécurité : ce que nous réserve l'année 2023

kaspersky BRING ON THE FUTURE



Kaspersky
Security Bulletin 2022

Menaces de cybersécurité : ce que nous réserve l'année 2023

Savoir ce que l'avenir nous réserve peut nous aider à mieux nous préparer aux menaces émergentes. Chaque année, les experts de Kaspersky préparent des prévisions pour différents secteurs d'activité, afin de les aider à mettre en place une défense solide contre les menaces de cybersécurité auxquelles ils pourraient être confrontés dans un avenir proche. Ces prédictions constituent le Kaspersky Security Bulletin (KSB), un projet annuel mené par les experts de Kaspersky.

Pour la conférence KSB 2022, nous avons invité des experts de renom à partager leurs idées et leurs opinions impartiales sur les perspectives de la cybersécurité pour l'année à venir. Les contributeurs comprennent des représentants d'institutions gouvernementales : **H.E. Dr. Mohamed Al Kuwaiti** (Conseil de la cybersécurité des EAU), et des organisations publiques : **Kubo Mačák, Tilman Rodenhäuser, Mauro Vignati** (CICR), **Serge Droz** (FIRST), **Sven Herpig** (groupe de réflexion Stiftung Neue Verantwortung). Nous tenons également à remercier **Prof. Dr. Dennis-Kenji Kipker** (Université de Brême ; Académie européenne pour la liberté d'information et la protection des données (EAID)), **Arthur Laudrain** (Centre d'études stratégiques de La Haye), **Stefan Soesanto** (Centre d'études de sécurité (CSS) d'ETH Zurich) pour leur contribution scientifique et approfondie. De plus, nous avons inclus les prédictions faites par nos collègues des organisations commerciales – **James Range** (White Rock Security Group) et **Irena Yordanova** (Polycomp Ltd.).

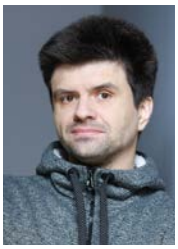
Les opinions partagées par les experts témoignent de la complexité du secteur moderne de la cybersécurité et de la nécessité d'une collaboration entre les différentes organisations pour lutter contre les cybermenaces auxquelles sont exposés les entreprises, les particuliers, voire des pays entiers.

Quelles seront les cybermenaces les plus pesantes pour les entreprises en 2023 ?

Vladimir Dashchenko, Évangéliste de la sécurité, Kaspersky

La tempête géopolitique actuelle fait peser sur les entreprises non seulement les cybermenaces classiques, mais aussi des risques imprévisibles et des « cygnes noirs ». Le principal problème pour 2023 sera la stabilité de la chaîne d'approvisionnement et la cybersécurité. Si la chaîne d'approvisionnement est un défi majeur pour les entreprises à l'heure actuelle, sa cybersécurité n'est pas seulement un problème, c'est un problème majeur. **La chaîne d'approvisionnement deviendra de plus en plus le point de mire des ransomwares ciblés et les campagnes d'espionnage commanditées par des États.**

Un autre problème important est la **pénurie mondiale de semi-conducteurs**. Cette situation jouera certainement un rôle dans la cybersécurité des entreprises. Alors que de nombreuses entreprises ont besoin de toujours plus de puissance de calcul (serveurs, stations de travail, matériel de réseau, etc.), le prix de ces équipements ne cesse d'augmenter. Il est possible que, pour couvrir les besoins en matériel, certaines entreprises doivent réduire les dépenses prévues en matière de cybersécurité.



Yury Slobodyanuk, Responsable de la recherche sur le filtrage de contenu, Kaspersky

Je pense que nous continuerons à voir des attaques visant l'infrastructure de différents pays et différentes organisations. **Les attaques de phishing vont devenir encore plus sophistiquées**, car de nombreuses tactiques de base ont déjà été essayées cette année, et les entreprises ont appris à les repousser.

Ivan Kwiatkowski, Chercheur principal en sécurité, Global Research and Analysis Team, Kaspersky

Les entreprises resteront concernées par les **ransomwares**. Le conflit entre la Russie et l'Ukraine a mis un terme à toute coopération judiciaire possible dans un avenir proche. On peut donc s'attendre à ce que les groupes de cybercriminels des deux blocs ne craignent rien en attaquant les entreprises du camp adverse. Il se peut même que certains considèrent leurs actions comme leur devoir patriotique. Le ralentissement économique (causé par les prix de l'énergie, l'inflation, les sanctions, etc.) conduira davantage de personnes à la pauvreté, ce qui se traduit toujours par une augmentation de la criminalité (qu'elle soit informatique ou non), et nous savons que les ransomwares sont extrêmement rentables.

James Range, Président de White Rock Security Group

La confiance zéro sera de plus en plus présente avec le rôle continu du travail à distance et hybride. Dans la mesure où le travail hybride est désormais la nouvelle norme, le travail à distance continuera de justifier le besoin de confiance zéro. Étant donné que le gouvernement fédéral a demandé aux agences d'adopter des stratégies et des conceptions de réseau à confiance zéro, nous nous attendons à ce que cette pratique devienne plus courante et que le secteur privé suive le mouvement, à mesure que 2023 deviendra l'année où il faudra tout vérifier.

Arthur Laudrain, Analyste stratégique (Cyber Program), Centre d'études stratégiques de La Haye

En 2023, nous pourrions assister à une légère baisse du nombre brut d'attaques par ransomwares, reflétant le ralentissement du marché des cryptomonnaies. Toutefois, **les exploitants de ransomwares continueront de perfectionner leurs opérations et cibleront des organisations de plus grande envergure**. Dans le même temps, les attaques commanditées par des États resteront au premier plan du paysage des menaces, sans qu'un apaisement des tensions géopolitiques avec la Russie, la Chine, la Corée du Nord et l'Iran soit en vue. **Les entreprises les plus exposées sont les entrepreneurs de l'aérospatiale et de la défense, ainsi que les exploitants d'infrastructures critiques** (services publics tels que l'eau, l'électricité et l'Internet, mais aussi les hôpitaux et les exploitants de grands systèmes cyber-physiques tels que les barrages).

Stefan Soesanto,
Chercheur senior en cyberdéfense, Centre d'études de sécurité (CSS) d'ETH Zurich

Si j'avais une boule de cristal, je prédirais que les plus grandes cybermenaces pour les entreprises en 2023 seront **une augmentation considérable des services de renseignement étrangers menant des opérations sous le couvert de groupes hacktivistes**, la lutte contre les grands pétroliers, le changement climatique, les politiques fiscales, etc. Par ailleurs, nous pourrions assister à une forte augmentation des campagnes d'extorsion de données par déni de service, dans la mesure où la cyberguerre en Ukraine entraîne des niveaux record d'attaques par déni de service.

Irena Yordanova,
Chef de produits logiciels,
Polycomp Ltd.

Nous prévoyons une hausse des cybermenaces en 2023, car les troubles dans le monde contribuent à une augmentation des cybercrimes. Les entreprises subiront plus fréquemment des attaques de programmes malveillants, comme les ransomwares. Enfin, **les équipes informatiques doivent être préparées à faire face à l'évolution des menaces posées par les technologies émergentes qui se généralisent, comme le phishing géociblé ou les attaques liées à la sécurité du cloud, à l'IdO et à l'IA**. Il est fort probable que les secteurs de l'éducation et des soins de santé feront l'objet d'autres attaques, ainsi que de campagnes ciblées contre les leaders de l'industrie, en particulier ceux qui détiennent des informations critiques : données confidentielles, expertise de pointe et dernières technologies. Les employés doivent donc être formés et équipés pour lutter contre ces attaques complexes, et leurs entreprises peuvent y contribuer en faisant appel à des partenaires externes spécialisés dans la sécurité pour les aider dans ce domaine. Les utilisateurs finaux peuvent se préparer aux défis à venir grâce à une solution de sécurité facile à utiliser, et ce, aussi bien pour les attaques de phishing que pour les menaces liées aux multiples couches de sécurité.

Quels défis en matière de cybersécurité les industries devront-elles relever l'année prochaine ?

Vladimir Dashchenko, Évangéliste de la sécurité, Kaspersky

Les approches de modélisation des menaces seront modifiées en 2023. La « balkanisation » de l'Internet, les conflits militaires en cours, les changements et les tensions dans les groupes politiques existants des pays influencent le cyberespace et la cybercriminalité. Nous verrons **un nombre croissant de cybercriminels prendre parti politiquement et enfreindre la loi par des déclarations politiques**. De même, les script-kiddies (pirates informatiques peu qualifiés) rejoindront plus souvent des groupes de cybercriminels dirigés par des auteurs plus qualifiés ou des pirates informatiques commandités par des États.

Le principal défi pour la cybersécurité elle-même sera **le manque de transparence et de partage des informations entre les entreprises**. Il sera extrêmement difficile de suivre le concept d'« affaires comme d'habitude » et de rester neutre. Les conglomérats politiques mondiaux influenceront malheureusement le cyberespace et la cybersécurité.

Arthur Laudrain, Analyste stratégique (Cyber Program), Centre d'études stratégiques de La Haye

Les tendances actuelles devraient se poursuivre l'année prochaine. En particulier, les gouvernements, les exploitants d'infrastructures critiques et les entreprises ayant une forte présence internationale devront relever le défi permanent de garantir la sécurité et l'intégrité de leurs chaînes d'approvisionnement, tant dans le domaine des logiciels que du matériel. Pour ce faire, ils devront souvent **collaborer plus étroitement avec leurs sous-traitants et fournisseurs**, notamment pour se conformer aux nouvelles obligations réglementaires aux États-Unis et dans l'Union européenne.

James Range, Président de White Rock Security Group

Compte tenu de l'augmentation continue des attaques par ransomwares, qui ont grimpé de 288 % au cours du seul premier semestre 2022, **le besoin d'une cyberassurance deviendra une priorité plus importante, en particulier sur le marché des PME**. Bien que de nombreux experts de l'industrie s'opposent aux indemnisations, ce qui confère aux cyberassurances un caractère controversé, l'évolution des menaces fait que la cyberassurance doit être considérée comme un aspect essentiel de la stratégie informatique des entreprises. C'est pourquoi nous nous attendons à un essor de l'industrie de la cyberassurance, à mesure que de nombreuses organisations tiennent compte de ces avertissements et cherchent à se prémunir contre les attaques par ransomwares. Pourtant, en plus de la cyberassurance, les entreprises auront besoin d'un plan de reprise après sinistre ou de rétablissement progressif.

Kubo Mačák, Conseiller juridique

Tilman Rodenhäuser, Conseiller juridique

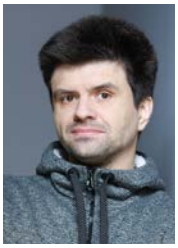
L'une des principales préoccupations pour 2023 est que **les civils seront davantage touchés par les cyberopérations pendant les conflits armés**. Les données, appareils et réseaux civils (comme les services gouvernementaux, les infrastructures critiques ou les entreprises) risquent d'être délibérément perturbés ou endommagés, souvent en violation des lois de la guerre. Les civils (particuliers et entreprises) peuvent être entraînés dans des activités de guerre numérique, encouragés à participer à des cyberopérations ou à soutenir des opérations militaires cinétiques par des moyens numériques. De tels développements mettent en danger les citoyens et les sociétés et remettent en cause la règle cardinale selon laquelle les belligérants doivent à tout moment faire la distinction entre ce qui est militaire et ce qui est civil.

Mauro Vignati, Conseiller sur les technologies numériques de la guerre, CICR

Stefan Soesanto,
Chercheur principal en cyberdéfense, Centre d'études de sécurité (CSS)

Je m'attends à ce que **le vol de données médicales** (par exemple, Vastamoo en Finlande en 2020 et Medibank en Australie en 2022) **ainsi que de données personnelles hautement privées** (par exemple, Ashley Madison en 2015) devienne le principal objectif des groupes de ransomwares et autres acteurs cybercriminels. Cette tendance s'explique par le fait qu'en imposant une pression psychologique massive directement à des milliers de victimes distinctes, on accroît la probabilité que les extorsions individuelles portent leurs fruits.

Quelles sont les cybermenaces qui représentent le plus grand danger pour les utilisateurs finaux ?



Yury Slobodyanuk,
Responsable de la recherche sur le filtrage de contenu, Kaspersky

Comme la situation géopolitique est assez tendue, **divers types de fraudes profiteront des nouveaux événements** à venir. En outre, il est possible que certaines techniques de génération de fausses informations à l'aide de l'IA soient utilisées.

Sven Herpig,
Directeur de la cybersécurité du groupe de réflexion Stiftung Neue Verantwortung

Je pense que la cybercriminalité est la plus grande menace pour les utilisateurs finaux, mais essentiellement de manière indirecte. **La cybercriminalité fait planer une menace sur les fournisseurs de services et de biens essentiels,** comme les municipalités, les hôpitaux et même les producteurs d'aliments pour bébés, qui peuvent se retrouver en partie ou entièrement hors service pendant plusieurs jours ou semaines. Cette situation a une incidence directe sur la vie des citoyens dans le monde réel et constitue donc, selon moi, l'une des menaces les plus importantes pour les particuliers.

Prof. Dr. Dennis-Kenji Kipker,
Professeur de droit de la sécurité informatique à l'université de Brême ; professeur invité à l'école supérieure de droit de Riga ; membre du conseil d'administration de l'Académie européenne pour la liberté d'information et la protection des données (EAID)

Les employés à distance qui travaillent à domicile continuent de jouer un rôle prépondérant dans la vie professionnelle de tous les jours, de même que l'utilisation croissante du modèle PAP (Prenez vos appareils personnels), qui retire aux administrateurs le contrôle des appareils. Depuis 2020, les formes de phishing ciblé, d'ingénierie sociale et de fraude au PDG, ainsi que les ransomwares, sont donc de plus en plus répandues et continueront de jouer un rôle important en 2023. **La professionnalisation de la cybercriminalité, devenue une « industrie » à part entière, contribue à un renforcement de la sécurité des utilisateurs finaux,** étant donné que les attaques de masse à faible coût deviennent ainsi accessibles.

H.E. Dr. Mohamed Al Kuwaiti,
Conseil de cybersécurité des EAU

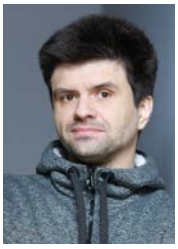
Les vulnérabilités de l'IdO. Les appareils de l'IdO qui règnent aujourd'hui sur le marché posent régulièrement des problèmes de sécurité. Alors que l'IdO combine le monde physique et l'espace virtuel, les intrusions domestiques s'ajoutent à la liste des menaces les plus effrayantes liées à l'IdO.

Les vulnérabilités dans les véhicules autonomes. En raison des risques inhérents aux véhicules autonomes, ceux-ci sont de plus en plus vulnérables aux attaques entraînant des violations de données, des perturbations de la chaîne d'approvisionnement, des dommages matériels, des pertes financières ainsi que des blessures ou des décès.

Quels sont les principaux défis auxquels la cybersécurité sera confrontée en 2023 ?

Ivan Kwiatkowski,
Chercheur principal en sécurité, GReAT Kaspersky

L'industrie de la sécurité sera confrontée à une pression directe résultant de la situation politique. La situation, déjà complexe, ne fera qu'empirer. Le plus grand défi que les fournisseurs devront relever en 2023 sera de rester neutres, s'ils n'ont pas déjà décidé de s'aligner sur un bloc ou l'autre. (Mon opinion sur ce sujet plus vaste est expliquée dans l'exposé « L'éthique à l'époque de la cyberguerre ».) D'une manière générale, la politique et la Threat Intelligence vont devenir de plus en plus imbriquées, et notre communauté n'y est pas du tout préparée.



Yury Slobodyanuk,
Responsable de la recherche sur le filtrage de contenu, Kaspersky

Je pense que les attaques évolueront beaucoup plus rapidement l'année prochaine, et **le principal défi sera de garder quelques longueurs d'avance**.

Sven Herpig,
Directeur de la cybersécurité du groupe de réflexion Stiftung Neue Verantwortung

Je ne pense pas que la situation évoluera considérablement en 2023. L'un des principaux défis à relever restera **le manque d'adoption des mesures de sécurité et de résilience de base**, que les cybercriminels sauront exploiter au mieux.

Prof. Dr. Dennis-Kenji Kipker,
Professeur de droit de la sécurité informatique à l'université de Brême ; professeur invité à l'école supérieure de droit de Riga ; membre du conseil d'administration de l'Académie européenne pour la liberté d'information et la protection des données (EAID)

La cybersécurité requiert non seulement des logiciels sécurisés, mais aussi un matériel suffisamment fiable. Pendant trop longtemps, nous avons misé sur la mondialisation de la sécurité informatique et accordé trop peu d'importance à la protection de la chaîne d'approvisionnement numérique. En Allemagne, le débat sur la protection des réseaux 5G sensibles l'a clairement démontré. Dans le conflit géostratégique entre la République populaire de Chine et Taïwan, nous constatons aujourd'hui que nous sommes déjà au cœur d'une crise des semi-conducteurs qui menace l'approvisionnement en produits informatiques de confiance. Ici, on peut présumer que les défis importants en matière de cybersécurité continueront de s'accroître en 2023 en raison des tensions politiques grandissantes.

Serge Droz,
Conseiller technique, membre du conseil d'administration, FIRST

La cybercriminalité continuera à se concentrer sur l'optimisation des gains par investissement, ce qui signifie que **les organisations plus petites et/ou moins matures seront encore plus ciblées.** Il peut s'agir de PME ou d'entreprises dans des secteurs qui n'incluent pas l'informatique dans leur activité principale, notamment les services de santé. Le problème avec ce groupe cible est qu'il a soit des priorités très différentes (un hôpital faisant l'objet d'une demande de rançon ne peut tout simplement pas se permettre de retarder son rétablissement, et paie donc le prix) et n'a pas les ressources nécessaires pour se défendre, soit il n'a tout simplement pas l'expertise nécessaire. C'est ce que Wendy Nater appelle « vivre sous le seuil de pauvreté en matière de sécurité ». Et c'est là le défi que devra relever notre industrie : **comment fournir une protection efficace qui fonctionne et qui soit abordable pour ce type d'organisations**. Ou autrement dit, peut-on fournir des services de sécurité à d'autres personnes que les spécialistes de la sécurité ? À mon avis, pour atteindre cet objectif, il faut que différentes industries travaillent ensemble. Je pense en particulier que le rôle des assurances doit être clarifié et harmonisé.

James Range,
Président de White Rock Security Group

Les cyberéquipes vont plus que jamais être au-devant de la scène. Il est essentiel de comprendre votre situation en matière de sécurité. Connaître les outils disponibles et les lacunes de votre infrastructure vous aidera à protéger votre entreprise. **Il est essentiel d'augmenter les budgets consacrés à la cybersécurité et de mettre les bonnes personnes en place.** Compte tenu de la pénurie constante de talents, envisagez de vous associer à une société tierce pour vous assurer que vous disposez de processus et de matériels à toute épreuve, ainsi que d'évaluations régulières par des tiers.

H.E. Dr. Mohamed Al Kuwaiti,
Conseil de cybersécurité des EAU

Les botnets DDOS. L'une des attaques sévères les plus récentes, vers la fin du mois de juin 2021, a été réalisée à l'aide d'un programme malveillant appelé le botnet Mēris qui a atteint des records. En raison de la nouvelle nature du programme malveillant, qui a été décrit comme une « nouvelle force d'assaut sur Internet – un botnet d'un nouveau genre », il est plus probable que des attaques DDoS similaires en temps réel liées à des programmes informatiques malveillants comme celle-ci soient utilisées en 2023.

Les ransomwares en tant que service (RaaS). Contrairement à d'autres formes de programmes malveillants, ce nouveau service fournit « une sorte de réseau de distribution de contenu (CDN) criminel semblable, en principe, à ceux utilisés par les grands portails Internet, mais utilisé exclusivement pour les programmes malveillants ». Près de la moitié des violations survenues au cours des six premiers mois de l'année 2022 concernaient des identifiants volés, a indiqué l'entreprise de cybersécurité Acronis, basée en Suisse, dans son rapport semestriel sur les cybermenaces, publié le 24 août 2022. Cette attaque a probablement été la plus discutée en 2022, car c'est la première fois qu'un pays a déclaré une urgence nationale en réponse à une cyberattaque. Les programmes malveillants basés sur les ransomwares ont été très actifs en 2022.

Le deepfake a permis la compromission des entreprises. La compromission par deepfake est un type d'attaque où les pirates informatiques ont recours à du contenu synthétique. Il s'agit notamment de vidéos ou d'enregistrements audio modifiés ou créés à l'aide d'intelligence artificielle et de machine learning pour se faire passer pour des cadres supérieurs et inciter les employés à transférer de grosses sommes d'argent

Actualités sur les cybermenaces : www.securelist.com
Actualités dédiées à la sécurité informatique : https://www.kaspersky.fr/blog/
Technologies Kaspersky : kaspersky.com/technowiki
Sécurité informatique pour les PME : kaspersky.fr/small-to-medium-business-security
Sécurité informatique pour les grandes entreprises : kaspersky.fr/enterprise-security

www.kaspersky.fr