HISCOX
CYBERCLEAR®

Principales tendances de la cybersécurité pour 2023

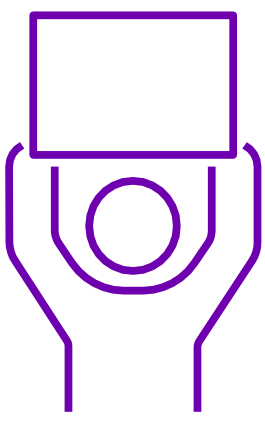
1 Menaces internes

En 2022, les ménages et les entreprises du monde entier ont subi une inflation élevée, les hausses de taux d'intérêts en découlant, la paralysie des chaines logistiques, une activité économique réduite et d'innombrables autres problèmes. Cela ne devrait pas s'arranger en 2023, mettant encore plus à l'épreuve les citoyens et les entreprises. Ces conséquences nous font craindre une hausse des attaques internes [*insider attacks*], car elles nourrissent les motivations suivantes :

Motivation financière :
Lorsque les salariés peinent à payer leurs factures, ils sont davantage enclins à prendre des risques pour obtenir une compensation financière. Cela peut prendre la forme d'une corruption de salariés par des organisations criminelles, au moyen de pots-de-vin en échange de biens de propriété intellectuelle, d'un accès à distance, d'identifiants etc. Nous nous attendons également à ce que la fraude financière augmente, car les salariés voient de plus en plus de raisons de commettre des infractions à motivation financière.

Salariés mécontents :
Face à la hausse des licenciements et au fait que les augmentations de salaires ne couvrent pas l'inflation, certains salariés peuvent décider d'exfiltrer les données d'une entreprise ou, dans des cas plus extrêmes, de les supprimer. La baisse de moral entrainera probablement davantage d'incidents dus à la négligence.

2 Des attaques sur fond d'activisme



La guerre Ukraine-Russie se déroule sur plusieurs fronts. L'un d'entre eux est la cyber-guerre. Avant la guerre, la Russie était considérée comme une cyber-puissance qu'il ne fallait pas sous-estimer, mais elle n'a pas totalement atteint ses ambitions en la matière. De l'autre côté, l'Ukraine a rassemblé une armée d'activistes forte de 210 000 membres, qui se sont baptisés « l'armée informatique d'Ukraine ». Même si la cause de l'armée informatique est noble, elle constitue un mauvais précédent pour les futurs activistes. La question qui se pose en effet est la suivante : sur quoi cette armée jettera-t-elle son dévolu après la guerre ?

Si le combat de cette armée semble légitime, où placer les limites morales lorsqu'il s'agit d'autres formes d'activisme ? En 2022, par exemple, les manifestations pour le climat sont devenues plus fréquentes et plus spectaculaires. En 2023, les tensions devraient s'accentuer, avec une possibilité accrue de recours aux cyber-attaques par les activistes.

3 Fracture parmi les gangs de ransomware

En 2021, les attaques par ransomware ont augmenté par rapport aux années précédentes, poussant les autorités internationales et locales à intensifier la pression sur les principaux groupes de ransomware. Cette pression sur les grands groupes de ransomware pourrait s'être avérée payante, car les attaques ont effectivement baissé dans certaines parties du monde en 2022. Et lorsque des attaques par ransomware se sont produites, les entreprises ont refusé de payer, ou ont été empêchées de verser des rançons à bon nombre de ces grandes organisations ayant fait l'objet de sanctions. Parallèlement, les personnes affiliées à des groupes de ransomware ne voulaient plus travailler avec des organisations ciblées par des services de renseignement occidentaux : la triste notoriété n'est pas nécessairement un gage de cyber-attaques plus réussies.

Pour continuer à perpétrer leurs actions, l'anonymat est le meilleur moyen d'échapper aux autorités. Lorsque les autorités sont sur le point de neutraliser un groupe de ransomware notoire, celui-ci se fracture souvent en groupes restreints et spécialisés, sous différents pseudonymes, et ses cibles changent. Nous pensons que cette tendance se poursuivra car les groupes considèrent qu'une mauvaise réputation est moins bénéfique et qu'ils gagnent en stabilité à réaliser de petites actions clandestines ciblant des secteurs ou zones géographiques spécifiques. Les demandes de rançon élevées qui font la une des journaux et attirent l'attention des autorités ont également diminué l'année dernière, ce qui semble corroborer cette évolution. En 2023, nous tablons sur une poursuite de la baisse des demandes de rançon et des attaques moins fréquentes, dans la mesure où les groupes fracturés disposent de moins de ressources et cherchent à naviguer sous les radars.

4 Authentification sans mot de passe

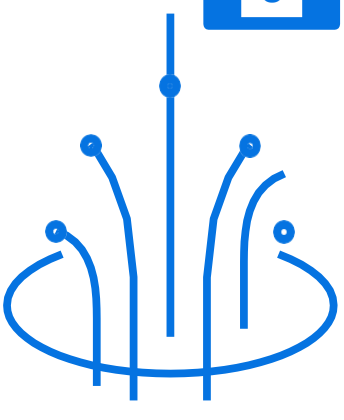
À mesure que les entreprises s'aguerrissent, il devient évident que l'authentification par mot de passe ne suffit plus. L'adoption de l'authentification à plusieurs facteurs (MFA) a beaucoup progressé, celle-ci devenant une exigence fondamentale pour la protection des services à distance et des comptes en ligne. Au milieu de l'année 2022, Apple, Microsoft et Google se sont engagées à soutenir davantage les normes promues par l'alliance FIDO (Fast ID Online), afin d'accélérer la mise en place des connexions sans mot de passe.

Nous estimons que la connexion sans mot de passe représente le futur de l'authentification. Son adoption par les trois géants de la tech favorisera son déploiement dans la mesure où beaucoup d'entreprise ont recours à leur technologie. Avec l'intégration de la biométrie dans tous les appareils modernes conçus par ces sociétés, les utilisateurs peuvent s'authentifier par la reconnaissance faciale, leurs empreintes digitales etc. Les dispositifs reposant sur la biométrie sont beaucoup plus difficiles à pirater et nécessitent un accès physique à l'appareil. Nous anticipons une adoption accélérée de l'authentification sans mot de passe en 2023 en raison de sa simplicité d'utilisation et des garanties de sécurité qu'elle offre.

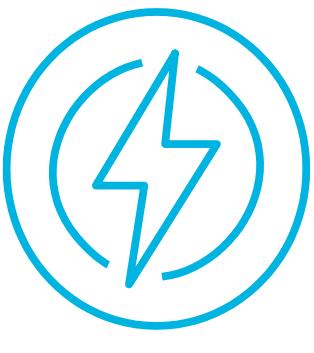
5 Câbles sectionnés

La cybersécurité est souvent cantonnée au numérique, pourtant les infrastructures physiques pour faire fonctionner l'Internet mondial sont et seront toujours nécessaires.
Récemment, le câblage de fibre optique entre les pays a montré des signes de fragilité alarmants. Ces câbles sous-marins constituent la faiblesse des communications Internet dans le monde et toute rupture pourrait être extrêmement préjudiciable à notre vie quotidienne et au fonctionnement des entreprises.

En 2022, ces câbles ont subi de nombreuses attaques. Tous les incidents se sont produits dans des circonstances suspectes et leurs responsables n'ont pas été identifiés. Des attaques de ce type vont vraisemblablement se reproduire, car les câbles constituent des cibles faciles et de grande valeur. On ignore à ce jour si ces actes sont le fait d'États hostiles visant la connectivité Internet des pays ou d'activistes ciblant les infrastructures Internet.



6 Coupures d'électricité



En raison de l'effet de la guerre entre la Russie et l'Ukraine sur les chaines d'approvisionnement en énergie dans le monde, les États ont prévenu que des coupures d'électricité seraient possibles. En 2023, le risque de coupures d'électricité reste bien réel si les fournisseurs d'énergie ne parviennent pas à satisfaire la demande. Quelles seraient les conséquences dans le monde de la cybersécurité ? Les centres de données pourraient être privés d'électricité (même si les États devraient donner la priorité à ces infrastructures) ; le travail à distance sera probablement le plus touché ; les entreprises peuvent également avoir du mal à maintenir une alimentation constante dans leurs locaux.

22334 02/23