mimecast

Risque Humain et AI

ENCADRER L'AVENIR

L'état de la sécurité de la messagerie et des outils collaboratifs en 2024

Partie I:

Préparation croissante à la cybersécurité

En 2023, le monde était tendu et rempli de risques, et les menaces en matière de cybersécurité continuaient de s'intensifier. Comment pourraient-ils ne pas le faire ? Les acteurs étatiques menaçant un grand nombre de pays et les bouleversements économiques et politiques généralisés déclenchant des torrents d'activités criminelles, il était inévitable que la cybercriminalité augmente elle aussi.

Cest la mauvaise nouvelle. La bonne nouvelle peut être trouvée ici dans le rapport State of Email and Collaboration Security 2024 (SOECS) de Mimecast. Cette huitième étude annuelle – élargie pour 2024 pour inclure les risques associés aux outils de collaboration – est encourageante, car elle démontre une augmentation spectaculaire de la préparation aux cyberattaques des entreprises du monde entier.

3 % mettent actuellement en œuvre une stratégie officielle et 6 % ont adopté des directives et des meilleures pratiques en matière de cybersécurité, mais aucune stratégie officielle.

100 %

des entreprises sont fortement engagées dans la course à la cybersécurité

Un tel degré de préparation se retrouve dans toutes les entreprises de toutes tailles, tous secteurs confondus

Ce degré de préparation s'étend à tous les secteurs industriels et aux entreprises de toutes tailles. Le secteur des services financiers, par exemple, compte le pourcentage le plus élevé de participants à la SOECS dotés d'une stratégie de cybersécurité officielle couvrant l'ensemble de l'entreprise (60 %). Cela se compare à seulement 33 % pour le secteur des médias et du divertissement, soit le taux le plus faible parmi les secteurs inclus dans l'enquête. Malgrétout, toutes les entreprises interrogées dans les deux secteurs ont intégré soit une stratégie de cybersécurité officielle, soit un ensemble de bonnes pratiques.

Une préparation cohérente dans l'ensemble de l'entreprise

De même, parmi les entreprises de différentes tailles, la différence en matière de préparation est faible. Les plus grandes entreprises, comptant plus de 10 000 employés, ont ouvert la voie, 60 % d'entre elles ayant adopté une stratégie formelle à l'échelle de l'entreprise. Par rapport à seulement 43 % des entreprises de la gamme des employés de 500 à 1,000. Mais les petites entreprises ont compensé ce manque par un pourcentage plus élevé de participants qui ont adopté une stratégie ou des meilleures pratiques basées sur les technologies de l'information.

Bien entendu, cela ne signifie pas que la préparation des entreprises à la cybersécurité est parfaitement au point ou aussi solide qu'elle devrait l'être. Comme l' explique lereste de ce rapport SOECS 2024, les mesures défensives de nombreuses entreprises présentent encore des lacunes importantes et dangereuses, et de nombreux professionnels de la cybersécurité restent frustrés par l'insuffisance des financements, le manque de soutien organisationnel et les pressions exercées par la haute direction pour limiter les dépenses en outils de sécurité à ceux fournis par Microsoft 365. De nombreux facteurs de risque humains en particulier - qui représentent la plus grande lacune actuelle en matière de cybersécurité - ne sont pas pris en compte et échappent au contrôle des professionnels de la cybersécurité.

Malgré ces limites, il y a lieu d'être très optimiste, car les entreprises prennent les unes après les autres des mesures pour intégrer la cybersécurité dans leurs activités quotidiennes. Nous nous pencherons plus en détail sur ces étapes après avoir examiné de plus près le paysage actuel des cybermenaces.

LE RISQUE HUMAIN

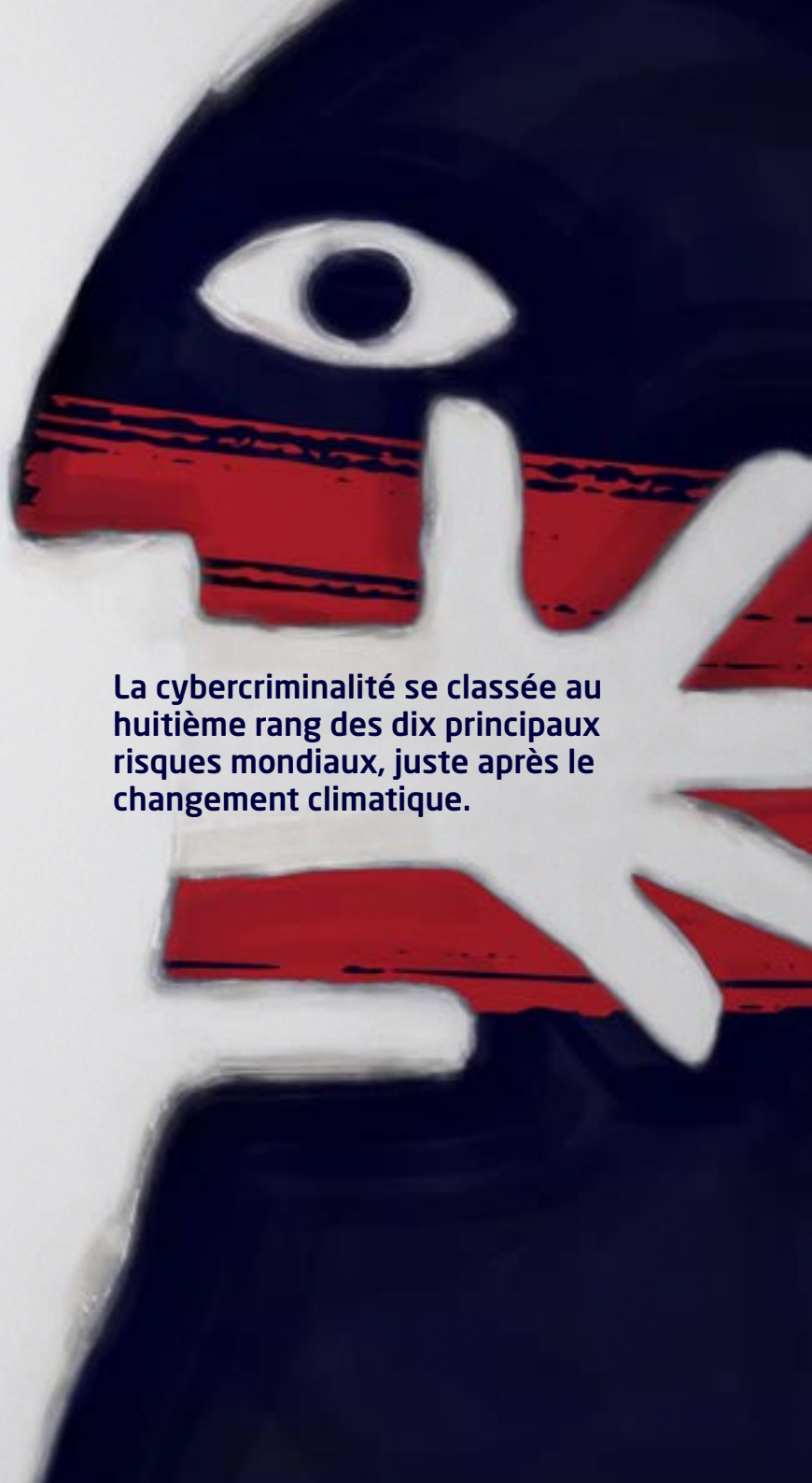
constitue la plus grande faille de cybersécurité, tout en étant largement sous-estimé

Partie II:

Les cyber-risques à l'intersection des personnes, des communications et des données

Le Forum économique mondial (WEF) classe désormais la cybercriminalité au 8ème rang parmi les 10 principaux risques mondiaux, juste après le changement climatique et devant les migrations humaines à grande échelle. Selon la définition du WEF, « le risque mondial est... la possibilité que se produise un événement ou une situation qui, s'il se produisait, aurait un impact négatif sur une part significative du PIB, de la population ou des ressources naturelles mondiaux. »[1]

Le coût moyen d'une violation de données est maintenant de 4,45 millions de dollars, en hausse de 15 % sur trois ans.
Dans l'économie numérique et hautement réseautée d'aujourd'hui, chaque entreprise doit faire face au cyber-risque. Les opérations, la réputation et les revenus de chaque entreprise, grande ou petite, sont exposés à un risque de violation de données ou d'incursion du système – et cela est désormais largement reconnu. Selon un sondage du Deloitte Center for Controllaudience, « près de la moitié (48.8 %) des cadres dirigeants et autres dirigeants s'attendent à ce que le nombre et la taille des cyberévénements ciblant les données comptables et financières de leur entreprise augmentent dans l'année à venir. »[2]



La cybercriminalité se classée au huitième rang des dix principaux risques mondiaux, juste après le changement climatique.

La messagerie électronique [redacted]

[redacted] demeure [redacted]

and the exploitation of network vulnerabilities, remain the

premier [redacted]

[redacted]

This affects some types of [redacted] Email remains

attack ve[redacted]he vecteur d'attaque [redacted]

[redacted]

des cybercriminels [redacted]

for fo[redacted]

[redacted]

publi[redacted] includes law and [redacted]

L’ampleur de la cybermenace est effroyable :

+15 %

La cybercriminalité devrait augmenter de 15% par an au cours des deux prochaines années, passant de 8 billions de dollars dans le monde en 2023 à 10,5 billions de dollars d’ici 2025.[3] Cela représente une hausse par rapport aux 3 billions de dollars enregistrés en 2015 et cela représente le plus important transfert de richesse de l’histoire de l’humanité.[4]

1 BILLION

Près d’un milliard de courriels frauduleux ont affecté un internaute sur cinq en 2023.

4,45 MILLIONS DE $

À l’échelle mondiale, le coût moyen d’une violation de données s’élève désormais à 4,45 millions de dollars, soit une hausse de 15 % sur trois ans. Pour les entreprises américaines, la moyenne est plus du double, soit 9,48 millions de dollars par violation.[6]

À l’échelle mondiale, en 2023, le nombre de dossiers électroniques volés s’élevait à un peu moins de six milliards.[7]

Le courrier électronique reste le premier vecteur d’attaque pour les cybercriminels, et les attaques par hameçonnage demeurent la principale menace pour les utilisateurs de courrier électronique.

C’est ce que confirme l’enquête SOECS 2024, qui révèle que le volume des attaques de phishing, de spoofing et de ransomware par courrier électronique ne cesse d’augmenter.

Le courrier électronique reste le

PRINCIPAL VECTEUR

Le phishing

En 2023, la compromission des courriers électroniques professionnels (BEC), une forme particulièrement dangereuse d'hameçonnage, a presque doublé, et l'hameçonnage, ainsi que le vol d'informations d'identification et l'exploitation des vulnérabilités du réseau, restent les trois principaux moyens utilisés par les entreprises pour se faire pirate.[10]

Cela touche certains types d'entreprises bien plus que d'autres. Alors que 39 % des personnes interrogées par la SOECS 2024 ont fait état d'une augmentation des activités de phishing, ce pourcentage était nettement plus élevé pour six des 12 secteurs représentés dans l'enquête. Cela incluait plus de la moitié (54 %) des organisations du secteur public et près de la moitié (49 %) du secteur des services commerciaux et professionnels, qui comprend des cabinets d'avocats et d'expertise comptable, entre autres.

Dans l'ensemble, 41 % des participants à la SOECS 2024 ont été confrontés à de nouvelles menaces par e-mail au cours des 12 derniers mois, et 38 % considèrent la sophistication croissante de ces attaques comme leur principal défi en matière de sécurité des e-mails en 2024.

Le spoofing

L'usurpation d'e-mails, qui consiste à faire croire qu'un e-mail provient d'une source fiable, continue également de se propager. Plus d'un tiers (35 %) des personnes interrogées par la SOECS 2024 ont indiqué que le nombre de ces attaques avait encore augmenté l'année dernière. Mais comme pour le phishing, certains secteurs ont été bien plus durement touchés que d'autres : le secteur des services aux entreprises et professionnels a obtenu la distinction douteuse d'avoir enregistré le plus grand nombre de personnes interrogées (52 %) signalant une augmentation de ce type d' attaques.

De même, l'usurpation d'identité sur le Web, par laquelle l'auteur tente de frauder des entreprises et leurs clients en créant un site Web usurpant l'identité du site de l'entreprise, continue de sévir. La quasi-totalité (98 %) des participants à la SOECS 2024 ont découvert un domaine Web contrefait l'année dernière, et plus de 60 % ont découvert ce type de fraude à de nombreuses reprises.

Les ransomwares

Cependant, le type de menace transmise par courrier électronique qui se propage le plus rapidement – et qui coûte le plus cher à ses victimes – est de loin les ransomwares.

En 2023, les attaques de ransomwares ont augmenté de 95 % d'une année sur l'autre.[11] Dans le même temps, le montant moyen des rançons est passé de 212 000 dollars en 2022 à 740 000 dollars en 2023, soit une augmentation de 250 %.[12]

Huit personnes interrogées sur dix lors de lenquêteSOECS 2024 ont été victimes dun ransomware au cours de lannée écoulée, et trois victimes sur quatre se sont senties obligées de payer la rançon. Et si les deux tiers de ces payeurs de rançon ont réussi à récupérer leurs données, le tiers restant n'y est pas parvenu.

Fait significatif, parmi les victimes du rançongiciel, 23 % n'ont pas payé la rançon et ont tout de même réussi à récupérer leurs données.

Conclusions principales de l'enquête SOES sur les 12 derniers mois

strategy

9 PERSONNES INTERROGÉES SUR 10
ont désormais une stratégie de cybersécurité officielle

96 %
d'entre elles attribuent à cette stratégie la réduction des risques de cybersécurité de leur entreprise

37 %
des personnes interrogées affirment que M365 ne parvient pas à

3 ENTREPRISES SUR 4
utilisent ou sont en train de déployer la DMARC pour lutter contre les attaques par usurpation d'identité

AI

80 %
des personnes interrogées sont s'inquiètent des nouvelles menaces posées par l'IA

employees

3 SUR 4
personnes interrogées déclarent que leur entreprise est exposée à des fuites de données accidentelles par des employés négligents

Pourtant,

15 %
seulement des entreprises proposent des formations de sensibilisation à la cybersécurité à leurs collaborateurs de manière continue

collaboration

70 %
les personnes interrogées déclarent que les outils collaboratifs posent de nouvelles menaces urgentes

7 PERSONNES INTERROGÉES SUR 10
anticipent les conséquences d'une attaque basée sur des outils de collaboration

email

4 ENTREPRISES SUR 10
continuent de constater une augmentation des menaces liées aux e-mails

ransom

8 ENTREPRISES SUR 10
ont été victimes d'un rançongiciel et 3 entreprises sur 4 ont payé la rançon

3 OF 4
ont payé une rançon

67 %
des personnes interrogées ne considèrent plus ne considèrent plus l'assurance cyber comme un filet de sécurité

support

97 %
des personnes interrogées affirment que leur conseil d'administration et leurs cadres supérieurs soutiennent leurs efforts en matière de cybersécurité

67 %

des entreprises pensent que les attaques provoquées par l'IA deviendront inévitables au cours des prochains mois

86 %

pensent qu'elles seront capables de répondre à une attaque engendrée par l'IA

Menaces basées sur l'IA

L'une des principales raisons de la propagation accélérée du phishing et des ransomwares est l'émergence de l'IA générative, qui permet aux malfaiteurs de perpétrer plus facilement des attaques réussies. Un outil comme ChatGPT, par exemple, peut être utilisé pour générer des e-mails à l'attention des employés, qui semblent provenir de leur patron et qui font référence à des événements de l'entreprise ou à des informations personnelles.

8 personnes interrogées sur 10 au SOECS 2024 sont préoccupées par l'utilisation de l'IA pour mener des attaques contre leur organisation, et près de 7 personnes sur 10 (67 %) admettent que les attaques générées par l'IA deviendront inévitables au cours des prochains mois. Contrairement à l'intuition, la grande majorité (86 %) pense être capable de répondre à une attaque générée par l'IA aussi facilement qu'à n'importe quelle autre incursion.

Risques et facteurs humains en dehors du contrôle de la cybersécurité

Il existe cependant dautres problèmes qui menacent la cyberpréparation de leurs entreprises et que les répondants à létude SOECS 2024 sont moins sûrs de pouvoir gérer

Le risque humain

Il sagit de facteurs indépendants de leur volonté et souvent liés au risque humain, comme la capacité des employés à reconnaître et à répondre aux cybermenaces (cités par 36 % des personnes interrogées), et si les protocoles de sécurité pour les travailleurs à distance sont strictement appliqués (également cités). par 36 % des répondants).

Outils collaboratifs

Une préoccupation essentielle, mise en évidence par 69 % des personnes interrogées, est le large éventail d’outils de collaboration utilisés par leur entreprise. Ces outils et leur utilisation généralisée sont devenus un élément majeur de conflit pour ceux responsables de la cybersécurité de leur organisation.

Partie III:

La collaboration et l'expansion de la surface d'attaque

Si le courrier électronique reste leur principale voie d'attaque, les malfaiteurs profitent également de la façon dont l'utilisation des outils de collaboration élargit la surface d'attaque d'une organisation.

Peu d'entreprises contemporaines peuvent fonctionner sans outils de collaboration, qui intègrent les communications et la messagerie aux fonctions de gestion de projet. Conçue pour fournir une plateforme centrale de partage des données et des documents, les logiciels collaboratifs sont devenus les sine qua non des environnements de travail à distance et hybrides.

Ces outils, qui incluent des plateformes de communication virtuelles telles que Zoom et des applications permettant le travail d'équipe telles que Google Workspace, Slack et Microsoft Teams, continuent de gagner en popularité. Parmi les personnes interrogées par la SOECS 2024, 84 % ont constaté que ces outils continuaient de se multiplier au cours des 12 derniers mois, et un pourcentage encore plus élevé (90 %) convient qu'ils sont devenus essentiels à leur organisation et à ses opérations quotidiennes.

Des mesures de protection inadéquates

Mais ces professionnels de l'informatique et de la cybersécurité sont également extrêmement préoccupés par le fait que la diffusion rapide et la dépendance croissante à l'égard des logiciels collaboratifs en font une cible de plus en plus attrayante pour les criminels. Sept personnes sur 10 (70 %) déclarent représenter de nouvelles menaces urgentes, tandis qu'un nombre presque identique (69 %) pensent qu'il est probable, extrêmement probable ou même inévitable que leur entreprise soit touchée par une attaque basée sur des outils de collaboration.

Les personnes interrogées par la SOECS en 2024 soulignent un certain nombre de facteurs qui aggravent la situation :

59 %

Le gros problème, c'est que les employés téléchargent et utilisent régulièrement de nouveaux outils de collaboration qui n'ont pas été approuvés par le service informatique (cité par 59 % des personnes interrogées)

69 %

des personnes interrogées se disent débordées d'essayer de suivre le nombre d'outils de collaboration utilisés par leur entreprise

61 %

déclarent que la majeure partie de la sécurité native fournie par ces outils est inadéquate

56 %

craignent que les cyberdéfenses de leur organisation ne puissent pas suivre le rythme de ces nouvelles menaces

En réponse, ces professionnels de la cybersécurité incitent leurs organisations à prendre des mesures défensives plus robustes.

48 %

déclarent que leur entreprise a déjà déployé des couches supplémentaires de logiciels de protection pour se prémunir contre les attaques basées sur des outils de collaboration.

47 %

prennent des mesures pour mieux connaître et contrôler les outils utilisés par les employés et la manière dont ils sont utilisés.

47 %

dispense une formation de sensibilisation à la sécurité spécifique aux outils de collaboration pour aider les employés à reconnaître les menaces potentielles et à y réagir de manière appropriée.

37 %

des personnes interrogées déclarent que leurs entreprises ne s'appuient que sur les protections de sécurité natives incluses dans leur logiciel collaboratif

1 %

admettent ne rien faire pour empêcher une attaque basée sur des outils de collaboration

L'anxiété suscitée par les outils de collaboration reflète le yin et le yang actuels de la cybersécurité des entreprises. En effet, bien que les postures défensives des entreprises se soient considérablement améliorées au cours des dernières années, de nouveaux cyber-risques continuent de proliférer et des lacunes importantes persistent en matière de cyber-préparation.

Partie IV:

Protéger le travail et gérer les cyberrisques

La plupart des entreprises ont désormais mis en place une stratégie formelle de cybersécurité, et presque toutes (96 %) estiment que celle-ci a réduit leur cyber-risque. Considérée sous l'angle des personnes, des processus et de la technologie, l'adoption d'une approche plus stratégique a été un franc succès.

Personnes:

99 %

Pratiquement toutes les personnes interrogées SOECS 2024 (99 %) déclarent que les pratiques de cybersécurité de leur entreprise protègent efficacement les clients, les employés et les partenaires commerciaux de l'entreprise.

Processus:

99 %

Les personnes interrogées sont également presque unanimes (99 %) pour dire que leurs mesures de cybersécurité protègent les processus commerciaux et opérationnels de leur organisation.

Technologie:

100 %

Et ils sontunanimes à 100 % pour dire que ces mêmes politiques visent à sécuriser leurs e-mails, leurs outils de collaboration et d'autres actifs technologiques.

Mais ces résultats, bien que bienvenus, soulèvent également la question suivante: si les stratégies de cybersécurité de toutes ces organisations s'avèrent si efficaces, pourquoi plus de 500 millions d'attaques de phishing ont-elles été signalées rien qu'aux États-Unis en 2022 ?[13] Et pourquoi les entreprises du monde entier ont-elles déboursé 449 millions de dollars pour rançonner leurs données au premier semestre 2023 ?[14]

La réponse, bien sûr, est que si l'adoption d'un ensemble complet de mesures de sécurité a permis d'atténuer le risque cybernétique dans de nombreuses entreprises, elle est loin de l'avoir éliminé. Lorsqu'on leur a demandé de qualifier le degré de protection offert par les pratiques de cybersécurité de leur organisation, seules 7 % des personnes interrogées ont affirmé avoir fourni une protection complète, tandis que 92 % ont admis que la protection était incomplète.

500 MILLIONS

d'attaques par phishing déclarées aux Etats-Unis en 2023

Plus de ressources nécessaires

Un manque de ressources fait partie du problème. Dans un développement positif, la plupart des personnes interrogées (97 %) déclarent que leurs conseils d'administration et leurs cadres supérieurs soutiennent leurs efforts en matière de cybersécurité, et la majorité (57 %) caractérise ce niveau de support aussi élevé. Dans le même temps, de nombreuses personnes interrogées estiment que leurs efforts sont entravés par des budgets inadéquats et des limites quant à la manière dont ces fonds peuvent être dépensés.

Les personnes interrogées indiquent quen moyenne 9 % du budget informatique de leur organisation est alloué à la cybersécurité – et ce chiffre est bien inférieur pour certains secteurs, comme le secteur de lénergie, qui ne consacre que 3 % des dépenses informatiques à la sécurité. Les personnes interrogées, quant à elles, pensent que la moyenne de 9 % est inférieure d'un tiers à ce qu'elle devrait être. Ils aimeraient voir en moyenne 12 % de leurs budgets informatiques d'entreprise consacrés à la cyberpréparation.

Parmi les conséquences de cette sous-utilisation :

40 %

déclarent avoir dû faire des compromis quant aux outils de cybersécurité qu'ils utilisent pour surveiller les menaces liées aux e-mails et aux outils de collaboration

37 %

déclarent qu'ils ne sont pas en mesure de détecter les menaces et d'y répondre aussi rapidement et efficacement que nécessaire

36 %

affirment que la sous-utilisation des dépenses a conduit à des failles importantes dans les défenses de leur organisation

Obligé de sappuyer sur Microsoft 365

Ces contraintes de dépenses ont un autre impact sérieux. Pour limiter les dépenses, plus d'un tiers des personnes interrogées (35 %) affirment avoir été empêchées d'investir dans des solutions de cybersécurité autres que celles proposées par Microsoft 365. Les protections fournies par la suite logicielle de Microsoft présentent toutefois des limites importantes, ce qui a nui à leur cyberpréparation.

Les personnes interrogées soulignent diverses lacunes dans les mesures de sécurité de M365. Au premier rang dentre eux :

32 %

Capacité limitée de voir au-delà d'incidents précis (les arbres) et d'avoir une vue d'ensemble de la menace (la forêt)

30 %

Ne pas réussir à empêcher « trop dattaques pour atteindre la boîte de réception de lutilisateur

30 %

Rendre trop difficile la mise en œuvre d'une politique de confiance zéro

Plus important encore, sans l'utilisation d'outils de sécurité supplémentaires non natifs, un tiers des personnes interrogées ont déclaré que les protections de sécurité natives de M365 étaient incapables de prévenir les malware (37 %), le spam (33 %) ou le Phishing (33 %) attaques. Presque autant (32 %) ont déclaré que les applications de sécurité M365 ne pouvaient pas à elles seules bloquer les attaques de type BEC et spoofing contre leur entreprise.

Ligne de DMARCation

Pour empêcher les hameçonneurs et autres fraudeurs d'usurper leurs domaines de messagerie, les entreprises intègrent la DMARC à leur stratégie de cybersécurité.

Domain Message Authentication Reporting and Conformance (DMARC) est un protocole qui permet de déterminer si un e-mail a été envoyé à partir du domaine auquel il est associé. Il est ainsi beaucoup plus facile d'identifier et de bloquer les e-mails qui prétendent provenir d'une partie mais qui ont été envoyés par une autre. La mise en œuvre de la DMARC peut toutefois être fastidieuse et prendre du temps. C'est pourquoi certaines entreprises ont mis du temps à l'adopter.

Mais c'était alors. Aujourd'hui, les entreprises dans tous les domaines semblent avoir décidé que la protection accrue qu'elle offre en vaut la peine. À savoir que 94 % des participants à l'étude de cette année utilisent déjà le DMARC, sont en train de le déployer ou prévoient de le faire au cours des 12 prochains mois, soit le pourcentage le plus élevé depuis que Mimecast a lancé l'enquête pour la première fois en 2016.

Les principales raisons invoquées pour mettre en œuvre DMARC sont de:

56 %

rendre le courrier électronique plus fiable

54 %

de garantir la conformité aux réglementations du secteur

48 %

et de protéger la marque de lentreprise

94 %

des personnes interrogées utilisent déjà le protocole DMARC, sont en train de le déployer ou prévoient de le faire au cours des 12 prochains mois

Les obstacles majeurs évoqués sont :

46 %

le temps nécessaire à la gestion et à la maintenance du protocole

45 %

la mesure dans laquelle il peut interférer avec les activités commerciales

39 %

et la réticence des parties prenantes de l'organisation à l'utiliser

Le risque humain constitue la principale lacune en matière de cybersécurité actuelle, comme en témoigne clairement le rapport 2024 de la SOECS : plus des deux tiers des personnes interrogées pensent que les employés mettent l'organisation en danger en utilisant à mauvais escient les e-mails, en partageant trop d'informations sur l'entreprise sur les réseaux sociaux et en naviguant imprudemment sur le Web.

L'inquiétude est encore plus grande dans certains secteurs, comme le secteur public, où près de 9 personnes interrogées sur 10 (87 %) craignent que les défaillances des e-mails des employés et des réseaux sociaux ne nuisent à leur institution .

74 %

des failles de cybersécurité sont causées par des erreurs humaines[15]

Pourtant, malgré ces craintes, seulement un peu plus de la moitié des personnes interrogées déclarent que leur organisation propose des formations mensuelles ou continues de sensibilisation à la cybersécurité, et ce chiffre est en légère baisse par rapport à 2023 (52 % contre 54 %).

Les éducateurs professionnels soutiennent depuis longtemps que pour être efficace, la formation de sensibilisation à la sécurité doit être cohérente, dispensée régulièrement à petites doses et adaptée à chaque employé. Mais au-delà, pour combler le fossé et réduire de manière significative les facteurs de risque représentés par leur personnel, il est de plus en plus admis que les entreprises doivent aller au-delà d'une formation unique qui vérifie la conformité mais ne réduit guère les risques encourus par les employés.

54 %

déclarent que leur entreprise propose des formations mensuelles ou continues de sensibilisation à la cybersécurit

Des formations adaptatives plus efficaces émergent, selon la reconnaissance que 8 % des utilisateurs d'une entreprise sont responsables de 80 % de ses incidents de sécurité.[16] Ces programmes de formation commencent par déterminer le niveau de risque représenté par les différents employés, puis se concentrent sur ces comportements.

Les répondantsdu SOECS 2024 ne sont pas encore là. Mais leur conscience aiguë du risque humain et de la façon dont il se traduit en cyber-risque suggère qu'à l'avenir, ils feront de plus en plus pression pour que leurs organisations adoptent des méthodes de formation adaptatives.

Partie V:

Cyberassurance contre préparation à la cybercriminalité

En intensifiant leurs efforts de préparation à la cybercriminalité, les entreprises sont devenues moins dépendantes de leurs polices d'assurance cybernétique.

En aucun cas les entreprises abandonnent leur assurance : 95 % des participants SOECS 2024 ont au moins une police et 45 % en ont plus. Cependant, ils deviennent beaucoup moins susceptibles de considérer ces politiques comme un substitut à une culture de résilience.

2/3

des personnes interrogées pensent que l'assurance cyber n'est plus considérée comme un filet de sécurité

Par exemple, lorsqu'on leur demande si leur organisation considère l'assurance cybernétique comme un filet de sécurité complet pour faire face aux cybermenaces, un peu moins de deux tiers des répondants ont répondu par l'affirmative. Les personnes interrogées (65 %) ont catégoriquement répondu par la négative. Cela se compare à seulement 50 % qui partageaient ce point de vue l'année dernière.

De même, lorsqu'on leur demande si leur organisation est moins susceptible de recourir à la cyber-assurance en raison des restrictions imposées par les assureurs sur ces polices, les deux tiers (66 %) sont d'accord, contre 52 % en 2023.

De plus, en raison de cette dépendance réduite, près de 9 personnes interrogées sur 10 (86 %) ont déclaré quelles pensaient que leur organisation devait compenser en investissant davantage dans ses propres cyberdéfenses. Lorsqu'on leur a demandé où ces investissements étaient le plus susceptibles de se produire, les trois catégories les plus fréquemment citées par les répondants étaient une plus grande sécurité du courrier électronique (45 %), une plus grande sécurité des outils de collaboration (44 %) et une plus grande utilisation de l'IA pour les applications de cybersécurité (41 %).

Ainsi, si la couverture d'assurance cybernétique reste importante, les entreprises de toutes tailles et de tous secteurs reconnaissent que leur propre résilience cybernétique est encore plus importante.

Partie VI:

Les 10 meilleurs plats à emporter

.01

La plupart des cyber-risques sont dus au risque humain.

Quels que soient les processus et les technologies utilisés, une solide cybersécurité dépend principalement du comportement des personnes. Mais le risque humain représente une énorme faille de sécurité dans la plupart des organisations. Pour y remédier, les entreprises doivent adopter des formes plus adaptatives de formation à la cyberconscience qui leur permettent d'identifier les employés qui ont les comportements les plus risqués, puis de leur proposer une formation individualisée pour remédier à ces comportements.

.02

La menace se trouve dans l'e-mail.

Le courrier électronique reste le principal vecteur d'attaque des plus grandes cybermenaces auxquelles la plupart des entreprises sont confrontées : hameçonnage, usurpation d'identité et rançongiciel. En d'autres termes, il n'y a pas de cybersécurité sans une sécurité solide des e-mails. Et une sécurité robuste des e-mails dépend de protections multicouches capables de faire face à des attaques de plus en plus sophistiquées.

.03

Phishing attrape les gens.

Les Phishing sont omniprésentes et se multiplient rapidement. Mais le problème avec le phishing, c'est qu'il ne fonctionne que si les gens se laissent prendre au piège. Les protections adéquates du courrier électronique contribuent grandement à atténuer la menace, mais il faut avant tout que les employés soient conscients du danger et formés pour l'éviter.

.04

La collaboration est une arme à double tranchant.

Le courrier électronique est peut-être leur principale voie d'attaque, mais le nombre croissant d'outils de collaboration ouvre de nouvelles perspectives dangereuses aux cybercriminels. Si peu d'entreprises peuvent fonctionner dans l'environnement de travail mondial d'aujourd'hui sans s'appuyer sur ces outils, elles doivent de toute urgence prendre en compte les nouvelles menaces qu'ils représentent.

.05

DMARC fait échec à l'usurpation d'identité.

DMARC n'est pas le protocole le plus facile à administrer, mais il est très efficace contre l'usurpation d'adresse électronique, qui continue de proliférer. Ainsi, la minorité d'entreprises qui ne l'ont pas encore adopté doivent serrer les dents et adhérer au programme. La mise en œuvre de DMARC peut sembler être plus qu'une once de prévention, mais se faire usurper le nom d'une personne à plusieurs reprises parce qu'une organisation ne l'a pas fait nécessitera certainement de nombreux livres de remède.

.06

La consolidation de Microsoft 365 est aussi penny que pound-foolish.

Essayer d'économiser quelques dollars en limitant les dépenses de cybersécurité aux outils inclus dans M365 est une proposition vouée à l'échec. Les mesures de protection de Microsoft ne sont tout simplement pas assez efficaces à elles seules ; ils doivent être complétés par d'autres outils de sécurité pour atteindre un degré raisonnable de cyberpréparation.

.07

La menace de l'IA est imminente ! La menace de l'IA est imminente !

Les personnes interrogées dans le cadre deSOCES 2024 considèrent déjà que la sophistication croissante des attaques par courrier électronique constitue leur principal défi en matière de cybersécurité. Mais bientôt, la prolifération largement attendue des menaces générées par l'IA amplifiera le danger. Les entreprises, toutes catégories confondues, doivent combattre le feu par le feu en augmentant leurs investissements dans les outils de détection et de prévention des menaces basés sur l'IA.

.08

La cyberpréparation réduit les cyberrisques.

La preuve est dans le pudding. Neuf entreprises sur dix ont désormais mis en place une stratégie de cybersécurité officielle, et 96 % d'entre elles estiment que cela a considérablement renforcé leur capacité à protéger leur personnel, leurs processus et leurs technologies. La plupart des cadres supérieurs et des membres des conseils d'administration l'ont largement reconnu et plaident désormais activement en faveur d'une meilleure préparation à la cybercriminalité.

.09

La cyberassurance n'est pas synonyme de cyberpréparation.

La plupart des entreprises reconnaissent aujourd'hui cette vérité fondamentale : une police d'assurance cybernétique ne remplace pas le plan de cyberpréparation de l'entreprise. Bien qu'il puisse être financièrement judicieux de s'assurer contre les cyberrisques, même la meilleure cyberassurance ne peut compenser que les dommages déjà causés. Cela ne peut pas empêcher les dommages de se produire en premier lieu. Seule la cybersécurité d'une organisation peut y parvenir.

.10

Il n'y a pas de dépenses comme celles liées à la cybersécurité.

Là où les stratégies actuelles de cyberpréparation échouent, cest dans la manière dont elles sont mises en œuvre. Trop de conseils d'administration et de cadres supérieurs soutiennent activement ces efforts, mais ne les soutiennent pas avec des ressources suffisantes. Mais la cyberpréparation est comme un être vivant : pour survivre et s'épanouir dans un environnement de plus en plus dangereux, elle a besoin d'être constamment soignée et nourrie.

les résultats

La tempête mondiale de cybermenaces continue de s'intensifier. Les entreprises de toutes tailles et de tous secteurs sont plus que jamais conscientes du danger que représente ce siège cybernétique de leurs employés et prennent des mesures importantes pour y faire face. Ils devront néanmoins améliorer leur jeu à l'avenir. Les nouvelles sources de menaces et les attaques basées sur l'IA ne manqueront pas de bouleverser encore davantage des eaux déjà troubles. Heureusement, de nouveaux outils de sécurité et méthodes de formation, tels que la formation adaptative, sont également arrivés pour contribuer à protéger les personnes et leur travail.

À propos des résultats de l'enquête inclus dans ce rapport

Le rapport State of Email and Collaboration Security 2024 est basé sur une enquête mondiale approfondie menée auprès de 1 100 professionnels des technologies de l'information et de la cybersécurité. Mimecast a chargé le cabinet d'études britannique Vanson Bourne de réaliser l'enquête, qui a eu lieu entre octobre et novembre 2023. Les participants à l'enquête venaient de six pays, dont les États-Unis (27 % du total), le Royaume-Uni (18 %), la France (18 %), l'Allemagne (9 %), l'Afrique du Sud (9 %) et l'Australie (18 %).

Les participants au sondage travaillaient dans des organisations comptant de 250 à 500 employés (9 % du total) à plus de 10 000 employés (8 % du total). Ces entreprises étaient réparties dans 12 secteurs industriels, dont les technologies de l'information et les télécommunications (15 %), le commerce de détail (14 %), l'industrie manufacturière (12 %), les services aux entreprises et les services professionnels (12 %), les services financiers (11 %), la santé (10 %), l'énergie (6 %), les médias et le divertissement (5 %), le secteur public (5 %), la construction et l'immobilier (3 %), les services aux consommateurs (2 %) et d'autres entreprises commerciales (4 %).

Parmi les participants, les DSI, les directeurs techniques, les RSSI, les directeurs informatiques et les directeurs de la sécurité informatique représentaient 78 % du total. Le reste comprenait des responsables informatiques et SOC, ainsi que des architectes et analystes de sécurité.

WORK PROTECTED.™

mimecast®

1. «Le Rapport sur les risques mondiaux 2023», Forum économique mondial
2. « Près de la moitié des dirigeants s'attendent à une hausse du ciblage des cyberévénements en matière de comptabilité et de données financières dans l'année, « Deloitte
3. «Almanach de la cybersécurité 2023», Cybercrime Magazine
4. «La cybercriminalité coûtera au monde 10,5 billions de dollars par an dici 2025», Cybercrime Magazine
5. «Rapport sur le coût d'une violation de données 2023», IBM
6. « Liste des violations de données et cyberattaques en 2023, » gouvernance informatique
7. «Rapport mondial sur les menaces», Mimecast
8. «Rapport denquête sur les violations de données 2023», Verizon
9. «Le courrier électronique reste le principal vecteur d'attaque des cybercriminels », Cybernews
10. «Rapport denquête sur les violations de données 2023», Verizon
11. «Rapport sur les Ransomware au troisième trimestre», Corvus Insurance
12. «Montant moyen des paiements de cyber-rançons», Statista
13. «Phishing Statistics by State in 2024», Forbes
14. «Mise à jour semestrielle sur la criminalité liée à la cryptographie», Chainalysis
15. «Rapport denquête sur les violations de données 2023», Verizon
16. «8 % de vos utilisateurs sont à l'origine de 80 % de vos incidents de sécurité», ElevateSecurity

Mimecast: Work Protected™

Depuis 2003, Mimecast assure une protection efficace des entreprises en leur permettant de travailler et collaborer en toute sécurité. Nous offrons à plus de 40 000 clients les moyens d'atténuer les risques et de gérer les complexités d'un paysage de menaces dominé par les cyberattaques malveillantes, l'erreur humaine et les limites de la technologie. Adaptées à la complexité des environnements informatiques modernes, nos solutions avancées permettent de détecter proactivement les menaces, de protéger l'image de la marque de l'entreprise, de sensibiliser les collaborateurs et de conserver les données critiques. Déployées dans le monde entier, les solutions Mimecast assurent la sécurité de la messagerie électronique et des outils collaboratifs des entreprises modernes.

www.mimecast.com I ©2024 mimecast I All Rights Reserved I GL-05959