virtru

L'employé responsable

Comment gouverner et influencer positivement le comportement de sécurité dans un monde de confiance zéro

Table des matières

Nous sommes tous humains 1

Partie 1 : Susciter l'engagement 2

Je vous fais (zéro) confiance 6

Mettre le « fun » dans les « fondamentaux de la sécurité » 8

Maintenant, c'est personnel 9

Faciliter les efforts de sécurité 10

Partie 2 : Créer un cadre de sécurité en couches 11

Adopter une sécurité qui voyage avec les données 13

Éliminer les frictions inutiles 15

Construire un filet de sécurité pour l'erreur humaine 16

Donner aux employés l'autonomie 17

Partie 3 : Inspirer l'action 18

Changer le comportement des employés 19

Combler le fossé entre le travail et la maison 20

Créer un plaidoyer en interne 21

Conclusion 21

À propos de Virtru 21

Nous sommes tous humains

Nous avons tous fait des erreurs en matière de sécurité, que ce soit en cliquant accidentellement sur « Répondre à tous », en envoyant par erreur un rapport à Sarah des ventes au lieu de Sarah des ressources humaines, en cliquant distraitement sur un lien douteux ou en transférant rapidement un e-mail qui a tourné pour contenir des informations sensibles plus loin dans le fil.

Un lieu de travail productif, efficace et collaboratif exige que les employés partagent des informations rapidement et efficacement, mais ces informations sont souvent de nature sensible. Les employés doivent être équipés pour protéger ces données.

Qu'il s'agisse d'une équipe RH négociant les conditions d'un nouveau régime d'avantages sociaux,

Une équipe marketing préparant des documents pour une prochaine présentation au conseil,

Un consultant informatique préparant une approche à un problème unique,

Un prestataire de soins de santé partageant les résultats d'un test avec un patient,

Un prêteur recevant une hypothèque documents de candidature d'un acheteur potentiel,

Un enseignant d'éducation spécialisée partageant le plan d'éducation individualisé d'un élève avec un parent,

Ou partageant tout autre type d'informations potentiellement sensibles,

Il est important que vos équipes soient habilitées à partager des données en toute sécurité et en toute confiance.

Vous avez entendu les statistiques concernant la cybersécurité et les violations de données, incluant à quel point une violation peut être coûteuse et dommageable (la violation coûte en moyenne 3,86 millions de dollars1) et vous comprenez pourquoi il est si urgent que les entreprises adoptent et priorisent la protection des données.

Ce guide vous montrera ce qu'il faut faire à ce sujet, en partageant des conseils pratiques sur la façon de donner à vos équipes les moyens de protéger leurs données de manière positive et réussie tout en ayant confiance en leur capacité à les partager.

1 Cost of a Data Breach, IBM

Partie 1 : Susciter l'engagement

« Comment amener les employés à se soucier de la cybersécurité ? »

Ce défi est une priorité pour les leaders technologiques de tous les secteurs, en particulier ceux qui disposent d'un effectif important avec une grande surface de risque. Plus la main-d'œuvre est nombreuse et plus elle est répartie à l'échelle mondiale, plus il peut être difficile de surveiller et de guider les comportements des employés en matière de sécurité. Avec 88 % des violations causées par une erreur humaine[2], il s'agit d'un domaine critique à traiter.

Un changement radical dans le comportement organisationnel commence par l'évaluation de votre approche actuelle et de ce qui fonctionne ou ne fonctionne pas. Voici quelques questions à considérer :

Positionnement

- Suis-je en train d'éduquer les employés sur l'impact de la protection des données sur leur vie, à la fois au travail et à la maison ?
- Suis-je en train de diriger avec un message de peur et de négativité, ou un message qui leur permet d'agir avec confiance ?
- Suis-je en train de démontrer les avantages d'une bonne sécurité ou simplement de souligner les conséquences effrayantes d'une violation ?
- Est-ce que je montre à mes employés que je leur fais confiance ?
- Suis-je en train d'initier un dialogue constructif ou simplement d'orienter les employés vers une ressource de formation ?

Expérience

- Les employés comprennent-ils leur responsabilité en matière de protection des données ?
- Les employés sont-ils encouragés à se déclarer s'ils font une erreur ?
- Est-ce que j'intègre souvent des moments d'enseignement pour garder la sécurité à l'esprit, ou est-ce que j'ai juste besoin d'une formation à certains intervalles de l'année ?

Leadership

- Les responsables de mon entreprise adoptent-ils eux-mêmes de bonnes habitudes de sécurité ?
- Les employés de l'entreprise ont-ils la possibilité de contribuer à notre stratégie de sécurité ?
- Est-ce que je donne la parole aux autres membres de mon équipe qui peuvent partager leurs expériences ?
- En fin de compte, est-ce que je donne aux employés tous les outils dont ils ont besoin pour collaborer en toute sécurité et protéger les données, au quotidien ?

2 The Psychology of Human Error, Tessian

Pour amener vos employés à se soucier de la sécurité, il est important de diriger avec positivité et enthousiasme pour le travail important que vous faites. *Montrez-leur pourquoi ils devraient s'en soucier, et quel est leur intérêt.*

Avez-vous déjà vu quelqu'un dans un domaine de niche parler avec passion de son sujet ? Peu importe le sujet : biologie marine, Kubernetes, jardinage de tomates ou leur groupe préféré. Lorsque l'orateur est visiblement engagé et enthousiasmé par le sujet, c'est convaincant pour les auditeurs, quelles que soient leurs connaissances sur le sujet.

Si raconter des histoires n'est pas votre fort, commencez simplement par partager ce que vous savez de manière positive. Expliquez aux employés à quelle vitesse le paysage de la sécurité évolue, à la fois sur le lieu de travail et dans des contextes personnels. Parlez de la confidentialité des données et des technologies émergentes. Montrez-leur quels types de menaces vous et votre équipe avez atténué. Démontrez l'impact de leurs actions axées sur la sécurité.

En fin de compte, une sécurité renforcée conduit à plus de confiance et à plus de liberté. Quel que soit votre rôle dans une entreprise, c'est quelque chose qui vous passionne.

étude de cas

Équiper les employés pour qu'ils prennent les bonnes décisions

Cette philosophie d'apprentissage continu et d'éducation permanente se reflète à la fois en externe et en interne chez CMI. L'équipe de Cunningham utilise les règles configurables de prévention des pertes de données (DLP) de Virtru pour chiffrer certains types de données par défaut, telles que les informations de carte de crédit, mais pour certaines catégories, Cunningham préfère générer un avertissement, en l'utilisant comme un moment d'enseignement.

« Si Virtru nous offre un filet de sécurité, nous aimons aussi l'idée de pouvoir éduquer nos utilisateurs en même temps. Ainsi, au lieu de chiffrer automatiquement quelque chose de sensible, nous pouvons informer les utilisateurs et leur conseiller de le chiffrer. De cette façon, il y a toujours un processus d'apprentissage en place. Je pense que c'est la clé : garder la sécurité en tête et ne pas créer de la complaisance. Cela ne fait que réaffirmer ce processus de pensée et, avec le temps, cela devient une seconde nature pour eux… Ce ne sont pas des choses que je peux simplement leur enseigner, cela doit être quelque chose qu'ils peuvent voir et toucher par eux-mêmes.

Le changement de culture est difficile, a poursuivi Cunningham, et les gens sont habitués à faire les choses comme ils l'ont toujours fait. Nous essayons de créer un virage éducatif, donc s'il y a quelque chose qui me permet de responsabiliser les employés, et en même temps de les éduquer, c'est gagnant-gagnant>>.

Lire l'étude de cas CMI de Virtru

virtru

CMI Chartered Management Institute

« Si Virtru nous offre un filet de sécurité, nous aimons aussi l'idée de pouvoir éduquer nos utilisateurs en même temps. Ainsi, au lieu de chiffrer automatiquement quelque chose de sensible, nous pouvons informer les utilisateurs et leur conseiller de le chiffrer. De cette façon, il y a toujours un processus d'apprentissage en place. Je pense que c'est la clé : garder la sécurité en tête et ne pas créer de la complaisance. »

Je vous fais (zéro) confiance

Vos employés et collègues veulent être traités comme des décideurs intelligents, compétents et avisés. Lorsque vous abordez la sécurité, il est important de montrer aux employés que vous leur faites confiance et que vous voulez leur donner les outils dont ils ont besoin pour réussir.

Alors, comment les leaders technologiques peuvent-ils traiter leurs employés avec confiance tout en maintenant le scepticisme requis d'un cadre Zero Trust ?

L'idée derrière Zero Trust est de "ne jamais faire confiance, toujours vérifier". Cela s'applique à tout le trafic (utilisateurs et systèmes) à tout moment. Chez Virtru, nous croyons en un cadre Zero Trust car c'est une approche forte de la cybersécurité, et cela nécessite d'associer la protection des données à une gestion forte et fédérée des identités.

Zero Trust traite chaque utilisateur et chaque système avec la même prudence. Tout le monde est sur le même terrain de jeu. Et ce n'est pas parce que votre cadre de sécurité nécessite une authentification que vous, en tant qu'individu, ne faites pas confiance à vos collègues.

Vous pouvez faire confiance à vos collègues pour faire ce qu'il faut tout en mettant en place un filet de sécurité. Lorsque vous roulez en tant que passager dans une voiture, vous portez votre ceinture de sécurité, non pas parce que vous ne faites pas confiance au conducteur, mais parce qu'il y a tellement de variables qui pourraient causer un accident. Et vous voulez être en sécurité en cas d'accident.

Avec une fondation Zero Trust, vous rendez service à vos employés. Vous faites tous partie de la même équipe, vous veillez à ce que les actifs les plus vitaux de votre entreprise restent sécurisés, et un cadre Zero Trust permet exactement cela.

Comment renforcer la confiance des employés dans un environnement de sécurité Zero Trust :

Faites de la sécurité un processus collaboratif et interfonctionnel. Non seulement cela suscitera l'engagement des employés enclins à la technologie et à la sécurité des données, mais cela vous donnera également des défenseurs dans toute l'organisation. Avec l'engagement et l'adhésion des RH, des ventes, du marketing, des finances, du développement de produits, de la réussite des clients et d'autres fonctions, vous construisez un réseau qui peut éduquer, renforcer la confiance, répondre aux questions et influencer le comportement des employés.

Créez une cadence régulière de communication et de rétroaction. Vous voulez garder la sécurité en tête tout au long de l'année, pas seulement lorsque vous organisez votre formation annuelle de sensibilisation à la sécurité. De plus, si vos employés sont frustrés ou confus au sujet de la sécurité, vous voulez le savoir (afin qu'ils ne se rebellent pas et ne contournent pas les processus que vous avez mis en place). Planifiez des vérifications technologiques avec diverses équipes et/ou contactez 2 à 3 fois par an pour solliciter des commentaires, des commentaires ou des données d'enquête sur la protection des données de l'ensemble de votre organisation.

Partager les connaissances. Informez-vous sur les meilleures pratiques sans parler de haut en bas à vos employés. Supposons qu'ils travaillent avec une connaissance limitée de la sécurité des données, mais parlez-leur comme les adultes instruits qu'ils sont. Ils peuvent absorber des informations complexes et s'adapter rapidement, alors n'ayez pas peur de leur donner de nouvelles informations qui pourraient les surprendre.

Reconnaître un bon comportement. Montrez aux employés à quel point leurs actions sont importantes et à quel point vous appréciez qu'ils prennent de bonnes décisions en matière de sécurité. Si vous utilisez Virtru, vous pouvez facilement rechercher des « utilisateurs expérimentés » sécurisant les données les plus sensibles. Remerciez-les de faire leur part pour protéger votre organisation.

Rendre facile. PMettez en place des cadres qui préparent les employés à réussir, comme le chiffrement des emails et le chiffrement des fichiers, simples à utiliser et intégrés à vos applications et flux de travail existants. « C'est formidable d'avoir toutes les fonctionnalités, mais si vos utilisateurs finaux ne savent pas comment l'utiliser, ils ne l'utilisent pas, et c'est aussi simple que cela. J'aime à quel point le produit Virtru est propre et simple, c'est un simple interrupteur à bascule pour l'allumer ou l'éteindre, et cela nous donne plus d'autonomie.

Mettre le « fun » dans les « fondamentaux de la sécurité »

Vous serez peut-être surpris d'apprendre que la formation à la sensibilisation à la sécurité peut non seulement être informative, mais aussi agréable.

KnowBe4 encore plus loin : leur formation en sécurité n'est pas seulement bien produite, elle est digne d'une frénésie. (En fait, les employés de Virtru vouent un culte à leur formation, où les nouvelles saisons de KnowBe4 *The Inside Man* rencontrent un niveau d'anticipation qui rivalise avec Game of Thrones à son apogée.)

Nous nous sommes assis avec Roger Grimes, Data Driven Défense Evangelist à KnowBe4 et auteur de *A Data-Driven Computer Defense*, pour comprendre comment KnowBe4 aborde l'éducation à la sécurité et le changement de comportement.

"C'est une question de culture, ce qui en fait une mémoire musculaire", a déclaré Grimes. « Pendant longtemps, les voitures américaines avaient des ceintures de sécurité, mais personne ne les utilisait. Finalement, il y a eu un changement de culture, et maintenant, la plupart des gens mettent leur ceinture de sécurité dès qu'ils montent dans leur voiture. Et s'ils ne le font pas, la voiture le leur rappellera ! »

« Si vous êtes capable de changer la culture, vous êtes plus susceptible de faire en sorte que les gens se soucient de vous et de prendre des décisions pour changer leur comportement en matière de sécurité pour eux -mêmes -et pour la sécurité de l'entreprise. »

Maintenant, c'est personnel

« Les gens peuvent être conscients mais ne s'en soucient pas », a déclaré Grimes. "Jusqu'à ce que vous le leur rendiez personnel, ils peuvent ne pas suivre les actions qui leur ont été enseignées."

En mettant en évidence les risques des ransomwares pour la vie personnelle et professionnelle des employés, les équipes de sécurité peuvent transmettre les conséquences des cyberattaques de manière plus tangible. « Souvent, les attaques de ransomware n'attaquent pas seulement l'entreprise : elles attaquent également l'employé », a déclaré Grimes. «Le produit ransomware moyen est dans une entreprise pendant 200 jours, et pendant ce temps, il collecte tous les mots de passe des employés. Donc, si vous allez sur Amazon pour commander quelque chose, connectez-vous à votre compte bancaire pour vérifier votre 401(k), accédez à vos comptes de soins de santé, ils obtiennent tous ces mots de passe. Donc, non seulement cela peut nuire à l'entreprise, mais cela peut également infecter votre ordinateur à la maison et vous causer des problèmes financiers.

Les impacts en aval de ces attaques peuvent également nuire à une entreprise du point de vue de la productivité. « Si vous et moi sommes financièrement compromis pendant que nous traitons ce gâchis, nous ne serons pas aussi productifs que nous pourrions l'être. De plus, si votre entreprise a été financièrement touchée par une attaque de ransomware, les employés ne recevront probablement pas leurs bonus cette année-là.

« Ils vont se soucier de leurs finances personnelles encore plus que de celles de votre entreprise", a déclaré Grimes. « Vous devez faire en sorte que les gens se soucient des deux côtés. »

Faciliter les efforts de sécurité

Il est vrai que le paysage de la cybersécurité évolue rapidement et que les cyberattaques se multiplient. Le Forum économique mondial estime que les cyberattaques ont augmenté de 238 % dans le monde entre février et avril 2020 seulement[3]. Mais Grimes a de bonnes nouvelles pour les responsables de la sécurité qui peuvent se sentir dépassés par cet environnement en constante évolution.

« Les principales façons dont les gens sont compromis aujourd'hui sont les mêmes depuis 30 ans : l'ingénierie sociale et les logiciels non corrigés. Si vous voulez compléter cela, utilisez des mots de passe forts et ne réutilisez pas vos mots de passe. Ces deux choses englobent presque tout >>.

Ce sujet est au cœur du livre de Grimes, *A Data-Driven Computer Defense*. "Vous devrez combattre les choses qui sont les plus susceptibles de vous affecter", a déclaré Grimes. « Presque aucune entreprise ne fait cela parce qu'elle est inondée de directives de conformité qui font 100 pages et répertorient 300 contrôles. Tout le monde voit des menaces comme des bulles dans une coupe de champagne, et on ne leur dit pas : "Deux de ces bulles comptent plus que toutes les autres bulles", et à cause de cela, ils ne se concentrent pas correctement.

Simplifier votre récit face aux employés peut également aider à consolider les comportements les plus percutants que vous souhaitez que les gens adoptent. Pour la plupart des entreprises, cela se résume à :

- **Ralentir.** Les e-mails de phishing sont de plus en plus ciblés, tirant parti de la terminologie et du jargon des industries les plus spécialisées pour paraître plus légitimes. En conséquence, les attaques de phishing deviennent de plus en plus difficiles à détecter, il est donc essentiel de ralentir.
- **Pensez.** ""Il y a des années, lorsque vous receviez un e-mail de phishing, il arrivait et contenait toutes sortes de fautes de frappe, et il provenait d'une adresse e-mail d'apparence étrange", a déclaré Grimes. De nos jours, ils sont beaucoup plus sophistiqués. Si vous recevez une demande inattendue, même si elle vient de quelqu'un que vous connaissez, et que la demande vous demande quelque chose qu'elle ne vous a jamais demandé de faire auparavant, réfléchissez-y à deux fois. Surtout si cette action pourrait vous nuire ou nuire à votre entreprise.
- **Différenciez-vous.** Les violations de données divulguent souvent les informations d'identification des utilisateurs, incluant les mots de passe. Cela peut être extrêmement dommageable pour les personnes qui réutilisent les mêmes mots de passe sur plusieurs comptes. Il est absolument utile d'utiliser des mots de passe longs, complexes et uniques pour chacun de vos comptes. Grimes recommande d'utiliser un gestionnaire de mots de passe pour aider à générer et à garder une trace de ces mots de passe, afin que les utilisateurs n'aient pas à s'en souvenir. «Peu importe comment vous le faites, vous devez encourager les gens à ne pas réutiliser le même mot de passe », a souligné Grimes. "Parce que chaque deuxième site Web supplémentaire sur lequel vous l'utilisez, augmente de manière exponentielle votre risque."

En fin de compte, l'ingénierie sociale tire parti de la psychologie humaine pour créer un comportement humain qui exposerait des informations sensibles, de sorte à ce que le renforcement des comportements prudents, attentifs et consciencieux deviennent essentiels pour surmonter ces risques. C'est ce que Grimes et l'équipe de KnowBe4 s'efforcent de faire chaque jour : l'équipe a même un conseiller en phishing dans son équipe pour examiner pourquoi les gens prennent les décisions qu'ils prennent.

3 *Why the Hybrid Workplace is a Cybersecurity Nightmare* | The Wall Street Journal

Partie 2 : Créer un cadre de sécurité en couches

Malgré tous nos efforts, aucun de nous n'est parfait.

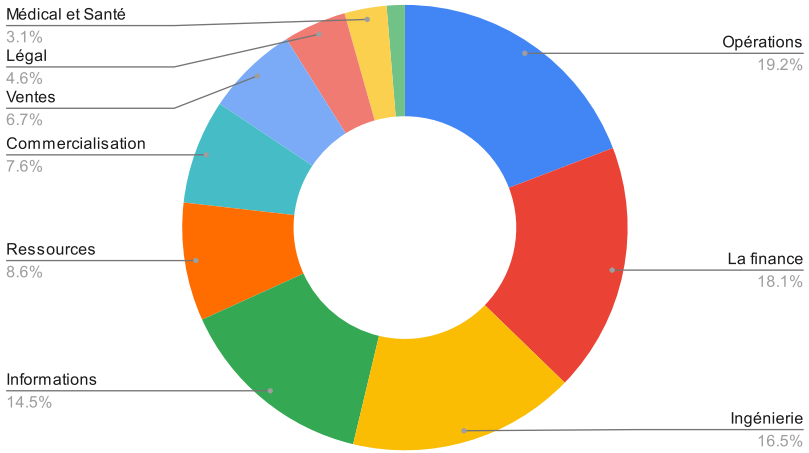
Les gens ouvrent les e-mails à la hâte. Ils peuvent être distraits lorsqu'ils cliquent sur un lien. Ils peuvent hésiter à signaler une erreur à l'équipe informatique de peur d'avoir des ennuis.

Une partie de l'autonomisation de vos employés consiste à leur permettre de faire le plus facilement possible avec leurs données. Pour les leaders technologiques, cela signifie mettre en œuvre une approche multicouche de la sécurité, notamment :

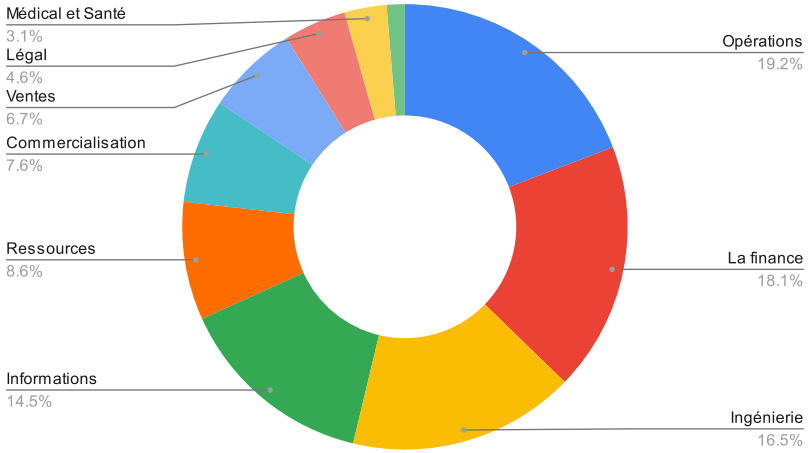
- Des outils faciles à utiliser qui permettent aux employés de protéger les informations qu'ils partagent
- Une authentification multifacteur et une identité fédérée pour régir l'accès aux données
- Une formation et une éducation complètes des employés
- Protéger les données au niveau de l'objet afin qu'elles soient en sécurité partout où elles voyagent
- Un « filet de sécurité » qui atténue les erreurs humaines
- Surveillance étroite du trafic réseau pour anomalies

Les erreurs vont se produire, mais vous pouvez prendre des mesures pour les atténuer.

Utilisateurs actifs par département



Politiques actives par département



Adopter une sécurité qui voyage avec les données

L'employé moyen envoie plus de 10 000 emails chaque année.

Faites quelques calculs rapides et multipliez cela par le nombre d'employés de votre entreprise. Cela fait beaucoup de données partagées.

Si vous n'avez aucune visibilité sur la destination de ces e-mails (à quelle fréquence ils sont transférés, où les pièces jointes sont finalement partagées), cette surface de risque n'est pas seulement importante : elle est en grande partie **inconnue**.

Selon une étude récente de Virtru, les départements des finances, des ressources humaines et des opérations (qui comprend le support client) représentaient près des deux tiers des données sensibles partagées. Ces services peuvent être considérés comme des « super-utilisateurs » de la protection des données. D'autres équipes, incluant la suite C, les équipes commerciales, juridiques et d'ingénierie, ont également partagé une quantité considérable d'informations sensibles.

Les organisations d'aujourd'hui ont besoin de partager des données afin de collaborer et d'innover, dans tous les départements et à tous les niveaux d'une organisation. Alors, comment les leaders technologiques peuvent-ils gagner en confiance et en visibilité sur la façon dont ces données sont créées, partagées et stockées ?

Si vous mettez en œuvre une stratégie de sécurité centrée sur les données qui protège les données avec un chiffrement au niveau de l'objet, elle enveloppera essentiellement chaque fichier ou message avec sa propre couche de protection distincte, ce qui rendra le partage des données beaucoup plus gérable.

Un autre avantage de la sécurité centrée sur les données est qu'elle protège les données elles-mêmes, partout où elles voyagent, vous laissant une plus grande flexibilité pour l'avenir. Ceci est essentiel pour vous préparer au succès dans un paysage de sécurité qui évolue si rapidement. En protégeant les données elles-mêmes, où qu'elles soient, vous avez la possibilité d'adopter de nouveaux outils et fournisseurs, en dotant vos employés des outils de collaboration et de partage de données qu'ils *souhaitent* utiliser.

Avec des méthodologies centrées sur les données, vous pouvez être sûr que votre stratégie est durable pour l'avenir. Dans cet état d'esprit, vous choisirez des fournisseurs et des partenaires qui s'alignent sur votre approche et peuvent vous offrir un contrôle total sur vos propres données, où qu'elles aillent.

« La confidentialité est un droit humain, et les gens ne devraient pas avoir à sacrifier la sécurité ou la propriété lorsqu'ils partagent leurs données. »

«Mon frère et moi avons lancé Virtru il y a près de dix ans, avec l'objectif de rendre la protection des données accessible à tous », a déclaré Will Ackerly, cofondateur, CTO et inventeur du Trusted Data Format (TDF). « La confidentialité est un droit humain, et les gens ne devraient pas avoir à sacrifier la sécurité ou la propriété lorsqu'ils partagent leurs données. Neuf ans plus tard, les offres de Virtru sont déployées auprès de 6 000 clients, des petites entreprises aux grandes entreprises mondiales, tout en restant gratuites pour un usage individuel et personnel. Cette mission de confidentialité continue de guider notre innovation, et nous utilisons le TDF pour protéger toutes sortes de données : pas seulement les e-mails et les fichiers, mais les données qui sont relayées à partir d'appareils IoT de périphérie à faible bande passante dans des environnements difficiles.

Avec les solutions de chiffrement des e-mails de Virtru pour Gmail et Outlook, les employés peuvent facilement partager des données sensibles et déterminer comment ils souhaitent sécuriser ces données, s'ils souhaitent autoriser le transfert, faire expirer les messages après une certaine date ou même révoquer un e-mail en cas de besoin.

Éliminer les frictions inutiles

En règle générale, les employés doivent faire un compromis entre la commodité et la sécurité. L'authentification de leur identité pour l'authentification multifacteur ajoute une étape au processus de connexion. Le chiffrement d'un e-mail ajoute une étape supplémentaire à l'envoi. Ralentir et prendre un moment pour examiner un e-mail suspect demande un effort conscient.

La clé pour amener les employés à adopter vos recommandations et outils de sécurité est de les rendre vraiment simples, transparents et faciles à utiliser. Dans la mesure du possible, supprimez les frictions de l'expérience de sécurité de vos employés et réduisez le «compromis d'inconvénients» qu'ils font pour divers aspects de votre pile technologique de sécurité.

Posez-vous la question :

- Comment puis-je libérer mes employés pour qu'ils fassent leur travail au mieux de leurs capacités ?
- Où puis-je éliminer les frictions pour leur permettre de communiquer et d'innover de manière plus fluide ?
- Quels outils et produits hérités ne répondent plus à nos besoins ? (Ou n'évoluent pas assez rapidement pour suivre le rythme de mon organisation ?)
- Comment puis-je surprendre mon équipe avec des solutions faciles à utiliser ?

Pour que vos employés utilisent réellement les outils de sécurité que vous fournissez, ils doivent être faciles pour vos utilisateurs internes *et* externes à adopter. Recherchez des solutions intégrées nativement dans Gmail et Microsoft Outlook, afin que les utilisateurs puissent facilement chiffrer les e-mails et définir des contrôles d'accès en appuyant simplement sur un commutateur. En outre, recherchez des solutions qui permettent aux destinataires de vérifier facilement leur identité afin qu'ils puissent accéder aux e-mails sans avoir besoin de créer des informations d'identification distinctes.

> « Avec les produits de sécurité, vous devez toujours vous soucier de l'adoption par les utilisateurs, mais Virtru est si facile à utiliser que cela n'a pas été un problème. Après tout, la sécurité et la conformité ne concernent pas les technologies que vous achetez, elles concernent les produits qui sont réellement utilisés. »
>
> -Mark Dieterich, RSSI, Brown University

Il est essentiel de prendre en compte l'expérience de l'utilisateur final. Votre équipe de direction, vos équipes de réussite client et vos équipes commerciales attachent une grande importance à faire bonne impression, et elles veulent faire de leur mieux. S'ils savent que vos outils de chiffrement vont être maladroits ou créer des freins pour leurs clients, ils ne les utilisent probablement pas.

Mais si vous adoptez une solution qui offre à vos employés facilité d'utilisation et sécurité, c'est gagnant-gagnant.

Construire un filet de sécurité pour l'erreur humaine

Dans un monde parfait, vos employés travaillent en permanence avec la sécurité à l'esprit, prenant les meilleures décisions pour protéger leurs données, à chaque fois.

Mais nous ne vivons pas dans un monde parfait, et ce n'est pas grave. Nous pouvons toujours créer un filet de sécurité lorsque les employés ne prennent pas les bonnes décisions. .

Des règles de prévention des pertes de données (DLP) peuvent être mises en place comme filet de sécurité pour intercepter les e-mails et les fichiers que les employés, intentionnellement ou non, ne parviennent pas à chiffrer. Les administrateurs peuvent définir et personnaliser des règles DLP pour chiffrer automatiquement les messages contenant certains types d'informations sensibles.

Pour les soins de santé prestataires, cela pourrait inclure des informations de santé protégées (PHI) - incluant les dossiers médicaux et les résultats des tests - ou des éléments tels que les informations de facturation et d'autres PII (informations personnellement identifiables). Pour les services financiers, il peut s'agir de formulaires fiscaux et de données de paie. Pour les établissements d'enseignement, cela pourrait inclure des plans d'enseignement individualisés (PEI) ou des données sur la santé des étudiants soumises à la loi HIPAA.

Recherchez des solutions qui vous permettent de choisir comment mettre en œuvre certaines règles DLP : équipez votre organisation pour chiffrer automatiquement certains types de données ou avertissez les utilisateurs lorsque des informations potentiellement sensibles sont détectées dans un e-mail. Par exemple, une organisation pourrait choisir de toujours chiffrer les e-mails contenant un numéro de sécurité sociale, mais en cas de partage d'une adresse ou d'un numéro de téléphone, elle pourrait envoyer un avertissement à l'expéditeur et lui permettre de prendre la décision finale. Sur la base des données de Virtru, lorsque les utilisateurs reçoivent un avertissement, 22% d'entre eux décident de chiffrer le message qu'ils envoient.

Ce rappel peut être un coup de pouce utile pour amener les employés à réfléchir à la sécurisation de leurs données, c'est pourquoi de nombreux administrateurs l'utilisent comme une opportunité. « Si Virtru nous offre un filet de sécurité, nous aimons aussi l'idée de pouvoir éduquer nos utilisateurs en même temps. Ainsi, au lieu de chiffrer automatiquement quelque chose de sensible, nous pouvons informer les utilisateurs et leur conseiller de le chiffrer. De cette façon, il y a toujours un processus d'apprentissage en place. Je pense que c'est la clé : garder la sécurité en tête et ne pas créer de la complaisance. Cela ne fait que réaffirmer ce processus de pensée et, avec le temps, cela devient une seconde nature pour eux... Ce ne sont pas des choses que je peux simplement leur enseigner, cela doit être quelque chose qu'ils peuvent voir et toucher par eux-mêmes.

Certains types de données doivent toujours être chiffrés, quelles que soient les circonstances. En mettant en place des règles DLP, vous pouvez permettre à vos employés de collaborer selon leurs besoins avec la certitude que vos données les plus vitales seront toujours protégées.

Donner aux employés l'autonomie

Parfois, le partage de données n'est pas noir et blanc. La sensibilité des données est nuancée et chaque situation peut nécessiter ses propres paramètres de partage des données.

Virtru met des contrôles sophistiqués entre les mains de l'utilisateur final, lui donnant des options pour définir des paramètres sur la façon dont ses données peuvent être utilisées. Ils peuvent désactiver le transfert, ajouter des filigranes aux pièces jointes ou définir une date d'expiration pour les informations qu'ils partagent.

L'outil le plus puissant fourni par Virtru est peut-être la possibilité de révoquer l'accès aux fichiers ou aux messages à tout moment. Si un fournisseur tiers subit une violation, ou qu'un certain fichier a été partagé par inadvertance, ou que l'utilisateur clique par erreur sur « Répondre à tous », il peut immédiatement révoquer l'accès, même si ce fichier a déjà été consulté par le destinataire.

Cela donne également à l'employé l'occasion de corriger ses propres erreurs. Plutôt que d'espérer que leurs données ne finissent pas entre de mauvaises mains, ils peuvent en prendre le contrôle immédiatement, à tout moment.

Maintenant, c'est l'autonomisation.

virtru

Partie 3 : Inspirer l'action

Maintenant que vous avez suscité l'intérêt des employés et mis en place un cadre de sécurité solide pour les soutenir, comment mettre tout cela en mouvement et commencer à influencer les comportements dans l'ensemble de votre organisation ?

La clé est de faire de la sécurité une habitude, une partie quotidienne de la vie de votre organisation. Comme toute autre habitude, il s'agit de petits changements continus qui s'ajoutent à un grand impact.

En tant que leader de la sécurité, les outils et les communications que vous introduisez peuvent aider à faciliter un changement de comportement et rappeler doucement aux employés d'être attentifs à la sécurité dans un lieu de travail en évolution rapide.

Changer le comportement des employés

Rien qu'en 2020, les utilisateurs de Virtru ont créé plus de 68 millions de politiques de partage de données sécurisées (emails et fichiers) : c'est beaucoup de données qui auraient pu autrement être envoyées sans protection. Sur ces 68 millions d'actifs de données, 13,7 millions ont été chiffrés automatiquement via la passerelle de messagerie de Virtru, qui protège les données circulant via les applications SaaS d'entreprise telles que Salesforce, Zendesk et SAP. Les 54,3 millions restants ont été chiffrés soit individuellement par les utilisateurs dans Gmail ou Outlook, soit automatiquement chiffrés avec règles DLP définies par les administrateurs.

Cela crée un mélange de protection automatisée des données du filet de sécurité et de protection des données volontaire et facultative que les employés décident d'appliquer.

Utilisez les outils à votre disposition pour faire passer des messages positifs et sécuritaires à vos équipes. Voici quelques idées :

- Prenez parti de la fonction d'avertissement de Virtru, mentionnée ci-dessus, pour alerter les employés sur certains types de données sensibles qu'ils partagent.
- Mettez en avant les « héros de la sécurité » de votre organisation sur une base mensuelle ou trimestrielle, qu'il s'agisse d'un membre de votre équipe technologique d'entreprise ou d'un utilisateur final qui fait un excellent travail en protégeant les données sensibles de l'organisation. Cela peut être l'occasion de mettre en évidence et de reconnaître des comportements positifs, comme signaler des spams suspects ou s'aligner avec votre équipe sur un certain type de données qui doivent être mieux protégées.
- Partagez les gains de votre équipe, qu'il s'agisse d'appliquer un correctif critique, de développer de nouveaux flux de travail ou de moderniser une partie de votre pile technologique. Profitez-en pour informer l'entreprise du travail important effectué dans votre service, afin qu'elle ne le prenne pas pour acquis.

Combler le fossé entre le travail et la maison

Les violations de données à grande échelle font l'actualité avec une fréquence et une ampleur croissantes. Des incidents tels que la violation de données de SolarWinds font la une des journaux, avec divers incidents de ransomware et de violation de données se révélant à un rythme soutenu.

Utilisez ces incidents comme une occasion d'éduquer et de vous engager. Aidez vos employés à comprendre ce que signifient ces violations, ce qui s'est passé et ce qu'ils peuvent faire pour aider votre organisation à rester sécurisée dans un paysage de menaces de plus en plus sophistiqué et difficile. Montrez-leur les types de menaces à surveiller et rappelez-leur l'importance des actions de chacun.

De plus, montrez comment les meilleures pratiques au travail peuvent se transformer en meilleures pratiques à la maison. Personne ne veut se faire voler son identité. Personne ne veut voir son compte bancaire soudainement vidé. Montrez aux employés que les conséquences des ransomwares, des mots de passe faibles et du partage de données non sécurisé peuvent avoir un impact important sur leur vie personnelle, ainsi que sur l'avenir de l'entreprise.

Cela devrait aider à mettre la sécurité en perspective et à démontrer que ce n'est pas seulement le travail de l'équipe informatique, et ce n'est pas seulement quelque chose à prendre en compte au travail. Cela devrait faire partie de chaque interaction avec la technologie, des ordinateurs aux téléphones et aux appareils IoT, à la fois au travail et à la maison.

Idées pour susciter une conversation autour de la sécurité

- Expliquer les violations de données dans l'actualité
- Fournir des conseils pour gérer la technologie à la maison et au travail
- Répondre aux questions des employés sur les concepts liés à la sécurité
- Démontrer la puissance des actions de chaque individu
- Relier les points entre les cyberattaques sur le lieu de travail et les comptes et données personnels des individus

Créer un plaidoyer en interne

Une fois que vous avez cultivé l'engagement des employés autour du sujet de la sécurité, exploitez cette puissance et maintenez-la. Un employé qui peut plaider en faveur de pratiques de sécurité solides peut non seulement avoir un impact positif, mais il peut également vous fournir des recommandations basées sur ses observations quotidiennes. Si certaines plates-formes sont trop lourdes à utiliser ou si les gens se lassent de certains messages de sécurité, ils peuvent vous le faire savoir.

Notez les personnes qui posent le plus de questions sur les meilleures pratiques de sécurité. Gardez un œil sur votre Virtru Control Center pour voir qui sont vos « super utilisateurs » et comprendre ce qui rend le chiffrement si précieux pour eux. Vous commencerez à trouver des défenseurs dans toute votre entreprise, qui peuvent influencer positivement le comportement tout en vous donnant des commentaires honnêtes de leurs propres équipes.

Conclusion

En fin de compte, l'un des piliers de la gestion de la sécurité est la gestion des personnes et, comme tout exercice de leadership, la gouvernance du comportement des employés nécessite une communication claire, la promotion de l'engagement et la création de liens.

En dotant vos employés d'outils faciles à utiliser, d'une formation convaincante et d'une culture d'entreprise soucieuse de la sécurité, vous pouvez préparer votre organisation à la réussite. Même si le paysage des menaces évolue, vous disposerez d'une défense de sécurité engagée qui couvre l'ensemble de votre organisation.

À votre équipe engagée, responsabilisée et dynamisée !

À propos de Virtru

Chez Virtru, nous permettons aux organisations de libérer la puissance des données tout en gardant le contrôle, partout où elles sont stockées et partagées. Notre portefeuille de solutions et d'outils de chiffrement, construit sur notre plateforme ouverte de protection des données, régit les données tout au long de leur cycle de vie. Plus de 6 000 clients font confiance à Virtru pour la sécurité des données et la protection de la vie privée.

Pour en savoir plus sur la façon dont nous pouvons vous aider à doter votre équipe d'une sécurité conviviale et centrée sur les données, contactez Virtru pour démarrer la conversation.