Guide du responsable

PROGRESSER AVEC UNE SÉCURITÉ MODERNE :

comment les DSI peuvent améliorer la cyber-résilience

Actuellement, la cybersécurité est l'une des priorités des DSI.

La récente et rapide accélération de la transformation numérique et du travail distribué a changé la donne en matière de cybersécurité.

Lorsque la plupart des collaborateurs travaillaient exclusivement depuis un bureau, les limites de la cybersécurité étaient plus claires. Avec le télétravail, la surface des menaces s'étend à tous les endroits où vos collaborateurs se déplacent.

Selon l'étude Breakthrough de Dell Technologies (basée sur des recherches effectuées auprès de 10 500 personnes sur plus de 40 sites),

72 % des personnes interrogées ont déclaré que l'évolution du monde du travail avait exposé leur organisation à des risques de cybersécurité plus importants.

Instaurer des mesures de cybersécurité efficaces face aux réalités de la vie, tel est le défi auquel les DSI sont confrontés. Près des deux tiers des personnes interrogées (62 %) ont déclaré que leurs collaborateurs représentent le maillon le plus faible de leur environnement de sécurité. Les collaborateurs valident eux aussi cette préoccupation : plus de la moitié (56 %) indiquent qu'ils n'ont modifié ni leurs connaissances, ni leur comportement en matière de sécurité de manière substantielle malgré une prise de conscience accrue des risques.

Il s'agit d'un problème universel et humain : même la personne la plus soucieuse de la sécurité peut faire des erreurs. La stratégie la plus efficace ne consiste pas à forcer les collaborateurs à adhérer aux protocoles existants potentiellement obsolètes, mais plutôt à s'assurer que votre posture de sécurité tient compte du facteur humain.

En tant que DSI, vous êtes responsable de la sécurisation de lieux apparemment infiniment peu sûrs. Bien que vos collaborateurs puissent vous aider, vous ne pouvez pas vous appuyer uniquement sur leur participation. Cette responsabilité peut sembler impressionnante, mais elle est à votre portée.

Voici ce que vous devez savoir pour assurer la sécurité de vos collaborateurs et de votre infrastructure IT.

Cinq principales raisons pour lesquelles les personnes interrogées pensent que leur personnel est victime de cyberattaques :

1. Confiance excessive dans les pare-feu de l'organisation pour bloquer les menaces
2. Ne saisissent pas l'ampleur de la menace
3. Espèrent qu'elles ne seront pas ciblées
4. Supposent que les conséquences peuvent être facilement résolues
5. Ignorent la menace parce qu'elles ne savent pas comment la résoudre

« La sécurité est la responsabilité de tous. Face à cette menace croissante, les entreprises doivent fournir à leurs collaborateurs les connaissances adéquates et leur faire comprendre qu'ils peuvent aider à contrer les cybercriminels en respectant les exigences de sécurité mises en place par leur organisation. Les entreprises doivent également faire de ce comportement la valeur par défaut en déployant des technologies et des processus technologiques intrinsèquement sécurisés. Il est primordial d'imprégner dans la culture le message de la responsabilité partagée en matière de sécurité. En règle générale, les individus ont besoin d'entendre un message plusieurs fois, de différentes manières, pour le transformer en comportement automatique. »

John Scimone, Senior Vice President et Chief Security Officer chez Dell Technologies

Compenser les comportements non sécurisés

Les DSI et RSSI sont chargés de déployer la technologie pour sécuriser les ressources numériques de la société. Mais que se passe-t-il lorsque les éléments les moins sécurisés (et les plus volatiles) du système sont les personnes qui l'utilisent ?

Même avec les meilleures intentions, l'erreur humaine est inévitable. D'où l'importance d'avoir un plan quand (et non si) vos mesures de cybersécurité seront soumises au test ultime d'une attaque de cybersécurité réelle. Ce plan nécessite une solution réactive et évolutive pour :

1. **Protéger les données et les systèmes :** votre solution doit protéger les collaborateurs où qu'ils travaillent et sur l'appareil de leur choix.
2. **Améliorer votre cyber-résilience :** les couches de sécurité et les fonctionnalités de reprise après sinistre sont des composantes essentielles.
3. **Surmonter la complexité de la sécurité :** Une solution rationalisée et facile à utiliser permettra d'améliorer la conformité.

En tant que DSI, il vous appartient de renforcer vos technologies métier et d'instaurer la confiance chez ceux qui en dépendent. Pour y parvenir, vous devrez répondre à certaines questions importantes :

- La cybersécurité de votre organisation couvre-t-elle l'écosystème IT de bout en bout, y compris les appareils, les applications et les systèmes ?
- Comment compensez-vous les comportements non sécurisés des utilisateurs finaux ? Par exemple, utilisez-vous un logiciel d'optimisation basé sur l'IA pour automatiser les contrôles de confidentialité lorsque l'utilisateur s'éloigne de son appareil ?
- Votre organisation a-t-elle évalué les risques nouveaux et potentiellement plus importants posés par l'augmentation du télétravail ?

Protéger les données et les systèmes

La complexité et les silos inhérents aux collaborateurs décentralisés multiplient la vulnérabilité aux cyberattaques. Chaque fois que des données propriétaires sont envoyées vers des Clouds et des environnements de travail distants, elles sont menacées.

Ces failles de sécurité peuvent être contrebalancées par un modèle de sécurité de bout en bout qui surmonte les silos et la complexité, comme le Zero-Trust.

Le Zero-Trust est un modèle de sécurité IT fondé sur l'idée qu'aucune interaction n'est fiable et que chacune doit donc être vérifiée. Ce modèle d'authentification à chaque étape peut être appliqué à l'ensemble du réseau, de l'infrastructure IT, des logiciels et des microservices de votre organisation.

Une approche Zero-Trust multicouche crée un périmètre autour de chaque interaction. Même si un cybercriminel franchit un périmètre, il ne sera pas en mesure d'exploiter une présomption de confiance basée sur son accès actuel au système. Chaque passerelle qu'il tentera de franchir nécessite une authentification. Ces protocoles de sécurité de refus par défaut (« deny-by-default ») peuvent vous aider à protéger vos données, la confiance de vos collaborateurs et les relations de confiance avec vos clients.

Lorsque vous commencez à renforcer les systèmes de votre organisation pour protéger les applications et les données, posez-vous ces questions :

- Votre posture de sécurité globale évolue-t-elle vers un modèle Zero-Trust ?
- Vos fournisseurs et votre équipe DevOps interne disposent-ils des mesures de cybersécurité appropriées pour garantir un cycle de développement sécurisé qui protège les processus avec lesquels les nouveaux produits, fonctionnalités et services sont développés/implémentés ?
- Vos fonctionnalités de sécurité actuelles sont-elles ajoutées ou intégrées ? Cloisonnées ou unifiées ? Axées sur les menaces ou sur le contexte ?

La préservation de vos données dépend de l'emplacement et du mode de stockage de vos sauvegardes. Ce sont généralement celles-ci que les cybercriminels tentent de compromettre avant vos données principales.

Améliorer la cyber-résilience

Tout le monde le dit, **« la seule chose plus difficile que de planifier un sinistre est d'expliquer pourquoi vous ne l'avez pas fait ».**

Pour atteindre la cyber-résilience, il faut supposer qu'une attaque se produira et prendre des mesures à l'avance pour assurer une restauration aussi rapide que possible, avec un impact financier et opérationnel minimal.

Ces étapes incluent des simulations qui testent la résistance de vos systèmes de continuité et de reprise des activités, ainsi que vos réponses concernant la cybersécurité et l'entreprise à travers les fonctions clés comme le juridique, la gestion de crise et les communications.

Toutefois, ce type de tests rigoureux peut prendre du temps. Une solution gérée peut libérer votre équipe de ces tâches, et vous informer sur les menaces émergentes et les tendances en matière de cyberattaques. Par exemple, un service de détection et de réponse managées analysera les menaces et étudiera les réponses de votre société.

Il est également important de préserver vos données, ce qui implique de savoir où et comment vos sauvegardes sont stockées. Ce sont généralement celles-ci que les cybercriminels tentent de compromettre avant vos données principales.

La meilleure défense contre ce problème consiste à posséder une copie isolée et hors ligne de vos systèmes stratégiques. L'histoire de Founders Federal Credit Union (FFCU) illustre la façon dont cela peut être fait, et pourquoi.

FFCU a calculé qu'en cas de cyberattaque, par exemple par un rançongiciel, l'entreprise disposait d'une heure pour récupérer ses données et reprendre ses opérations. Cela a entraîné un remaniement majeur de la cybersécurité de son datacenter, axé sur une reprise rapide. L'organisme a implémenté une chambre forte de cyber-récupération, protégée par un isolement (« air gap ») opérationnel qui la sépare de son système tout en permettant une synchronisation régulière des données de production. Ainsi, FFCU a l'assurance que ses données seront toujours disponibles, protégées et non corrompues.

Lorsque vous cherchez à renforcer votre cyber-résilience dans un environnement de sécurité en évolution, posez-vous ces questions :

- Votre organisation a-t-elle déterminé la durée pendant laquelle ses opérations seraient perturbées en cas de cyberattaque ?
  - Si oui, s'agit-il de minutes, de jours ou de semaines ?
- Quand avez-vous identifié pour la dernière fois des charges applicatives et des données stratégiques à isoler pour leur protection ?
- Quels types de fonctionnalités de détection des menaces avez-vous mis en place ?
  - Sont-elles gérées en interne ou par un tiers ?
  - Votre organisation utilise-t-elle la détection des anomalies basée sur l'IA ?

La complexité est l'ennemie de la sécurité

Lorsque votre équipe chargée des opérations de sécurité gère des solutions pour votre large éventail de composants d'infrastructure IT, la complexité, et donc les risques, peuvent augmenter rapidement. Cette complexité se traduit également par une augmentation des coûts et de l'inefficacité dans vos opérations régulières. Pour trouver un équilibre entre ces deux éléments, il faut généralement faire des compromis non viables sur les deux fronts.

Il existe un meilleur moyen de faire évoluer vos opérations de cybersécurité. Vous pouvez libérer du temps et des ressources grâce à des outils de sécurité avancés qui utilisent l'intelligence artificielle (IA) et l'apprentissage automatique (ML) pour permettre une gouvernance et un fonctionnement plus cohérents.

Les outils d'IA permettent à vos solutions de détection des menaces d'identifier et de signaler les anomalies sur le réseau, ainsi que les violations de règles, en déclenchant une cascade d'actions de sécurité. La sécurité automatisée peut également améliorer le code de développement logiciel. La réduction du nombre d'erreurs, humaines ou non, diminue également le nombre de failles de sécurité.

Toutefois, pour tirer le meilleur parti de vos outils de sécurité, vous devez pouvoir les utiliser et les gérer facilement. En consolidant les applications et les partenaires de sécurité de votre organisation, vous bénéficierez d'un meilleur contrôle et simplifierez la gestion informatique, afin que vos équipes IT puissent se concentrer sur l'innovation. Les services managés peuvent être un excellent moyen d'exploiter les technologies de sécurité les plus récentes et les plus avancées, tout en réduisant les charges applicatives pour les équipes internes. Toutefois, il est important de sélectionner et de rationaliser soigneusement les fournisseurs lorsque cela est possible. N'oubliez pas de choisir un partenaire de confiance capable non seulement de comprendre vos défis uniques, mais aussi d'amplifier les capacités de vos équipes IT avec des services de cybersécurité. Vous pourrez ainsi maintenir l'efficacité au fur et à mesure de votre évolution.

Q Lorsque vous souhaitez rationaliser vos opérations sans rétrograder vos défenses, posez-vous ces questions :

- Votre organisation a-t-elle garanti le niveau de redondance approprié dans ses fonctionnalités de sécurité ?
- Votre organisation utilise-t-elle des outils d'IA pour soutenir la détection, la réponse et la récupération ?
- Votre organisation examine-t-elle régulièrement ses fournisseurs de sécurité internes et tiers pour s'assurer de leur efficacité et de leur valeur ?

Le monde du télétravail nécessite une sécurité plus intelligente

Les données distribuées, les modèles de télétravail, les environnements multicloud et l'approvisionnement as-a-service présentent une incertitude importante dans le paysage de la cybersécurité moderne. L'erreur humaine peut aggraver cette incertitude. En tant que DSI, vous devez vous assurer que la cybersécurité tient compte de chacune de ces incertitudes.

Une approche moderne de la cybersécurité est essentielle. En la matière, vos dispositifs doivent être prêts à protéger vos données et vos systèmes, à réduire l'impact des cyberattaques et à faire évoluer efficacement les mesures de cybersécurité, tout en limitant l'ajout de complexité.

Dell Technologies s'engage à vous aider à planifier, protéger, détecter et traiter les cyberattaques, puis à récupérer de celles-ci, afin que vous puissiez entièrement consacrer vos équipes et vos ressources à ce qui compte : faire progresser votre entreprise.

Pour en savoir plus, consultez la page dell.com/cio

Pour en savoir plus sur l'étude Breakthrough, consultez dell.com/breakthrough

Pour en savoir plus sur nos solutions de sécurité, consultez dell.com/en-us/dt/solutions/security/index.htm

Source : D'après l'étude « The Breakthrough Study », Dell Technologies, avril 2022. Travail de terrain effectué d'août à octobre 2021. Recherche et analyse réalisées par Vanson Bourne à la demande de Dell Technologies.

DELL Technologies