E-BOOK

everbridge®

Gestion des incidents majeurs :

Des délais moyens de reprise (MTTR) raccourcis, une réponse plus rapide et une résilience opérationnelle accrue

Les organisations dépendent un peu plus chaque jour des environnements numériques, et la pandémie n'a fait que renforcer cette tendance. Les dirigeants et les professionnels de l'informatique doivent donc donner la priorité à l'élaboration de stratégies de gestion des incidents majeurs afin de répondre aux événements critiques susceptibles d'entraver la prestation des services. Un événement critique (panne de courant, cyberattaque, plantage de serveurs, etc.) peut avoir des impacts considérables sur une entreprise non préparée à y faire face : coûts élevés, perte de revenus, importants retards dans les opérations, baisse globale de la satisfaction client.

Malheureusement, avec la montée des menaces numériques, la question n'est pas de savoir « si », mais « quand » une entreprise sera confrontée à un événement de ce type. Selon CrowdStrike, les intrusions menaçant la cybersécurité des organisations à travers le monde ont augmenté de 400 % en 2019 et 2020 réunies. Rien qu'en 2020, 524 organisations ont été victimes de violations dans 17 pays et régions et 17 secteurs d'activité.

Plus récemment, le Rapport 2021 sur le coût d'une violation de données* publié par IBM Security indique que le coût total d'une violation de données en 2020-2021 a progressé de 10 % en moyenne. Il est ainsi passé de 3,86 millions à 4,24 millions de dollars, soit un record en 17 ans, depuis qu'IBM publie ce rapport. Toutefois, « les coûts étaient nettement inférieurs pour les entreprises plus matures en matière de gestion de la sécurité, et plus élevés pour les organisations moins avancées dans des domaines tels que l'IA et l'automatisation de la sécurité, la confiance zéro et la sécurité du cloud. »

** Toutes les références à IBM dans cet e-book sont tirées du Rapport 2021 sur le coût d'une violation de données publié par IBM.*

L'augmentation des coûts et des risques pour cause de perturbations dans l'activité renforce l'intérêt pour les stratégies visant à en limiter l'impact, notamment en réduisant les délais moyens de reprise. Par ailleurs, toute mesure préventive permettant de limiter le risque de temps d'arrêt accroît la résilience opérationnelle globale d'une organisation. Mais alors comment faire ? C'est par une planification bien menée, l'adoption de technologies pertinentes et l'automatisation qu'une organisation reviendra plus rapidement à une activité normale et renforcera sa résilience face aux menaces numériques.

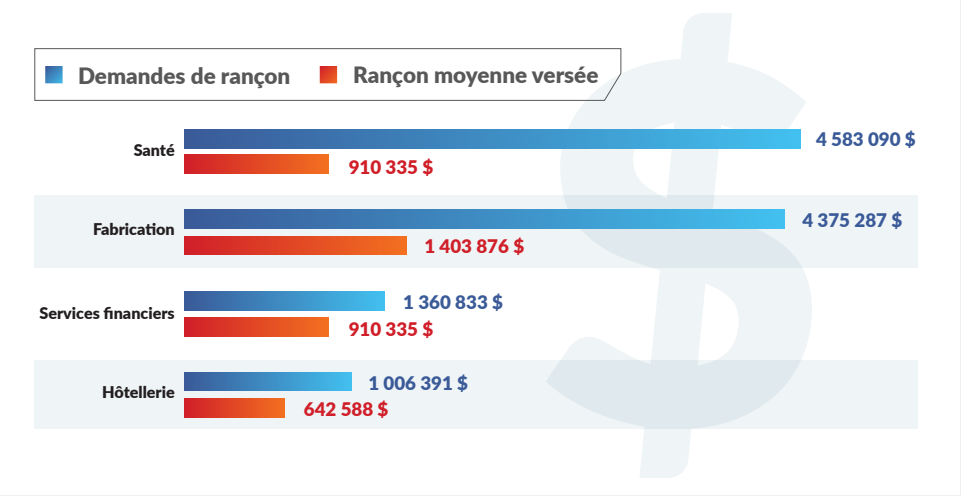
Quels sont les secteurs les plus touchés par les temps d'arrêt ?

S'il est aujourd'hui vital pour toutes les organisations d'être prêtes à faire face à des pannes de toutes sortes, les effets d'un incident informatique peuvent être nettement plus dévastateurs dans certains secteurs que dans d'autres.

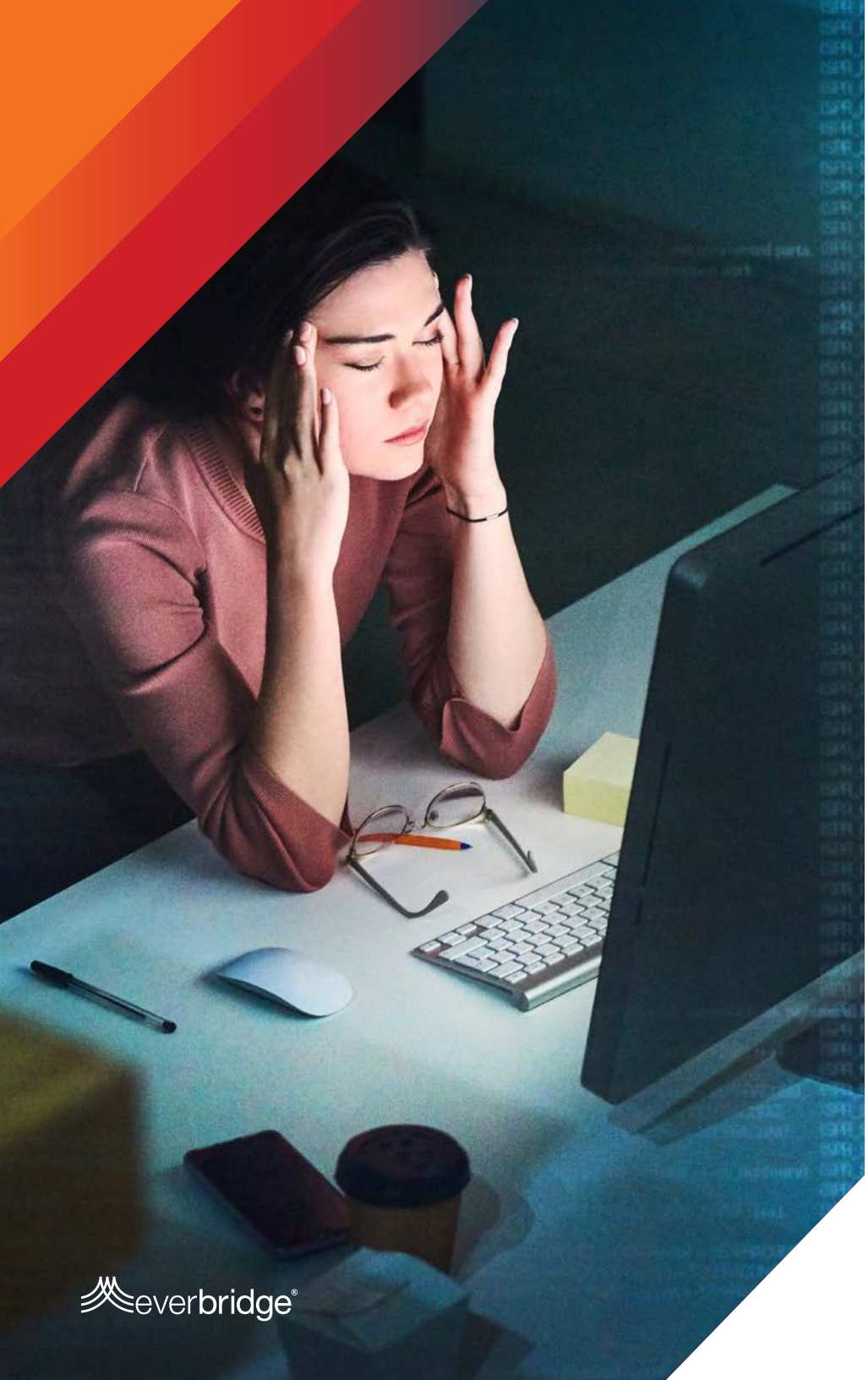
Selon le Rapport 2021 sur les réponses aux incidents publié par BakerHostetler, les cinq secteurs les plus touchés par les incidents sont les suivants :

1. Établissements d'enseignement
2. Santé
3. Fabrication
4. Finance et assurances
5. Services aux entreprises

Secteurs touchés par les demandes initiales de rançon les plus élevées



Quel que soit son secteur d'activité, une entreprise a clairement intérêt à donner la priorité aux questions de sécurité et à la gestion des incidents majeurs afin de traiter efficacement ces événements critiques extrêmement coûteux, voire de les éviter. La rapidité de l'intervention est également un aspect essentiel de cette approche.



Une demande croissante pour une réponse plus rapide aux incidents

Selon le Ponemon Institute, une minute de temps d'arrêt coûte en moyenne 9 000 $, et les coûts induits peuvent vite atteindre des sommets, compte tenu du délai moyen avant la reprise normale des activités. IBM a examiné en détail le délai moyen d'identification et de traitement d'une violation de données, et estimé qu'en moyenne, en 2021, il a fallu :

+ 212 jours pour identifier une violation
+ 75 jours pour contenir une violation
+ Soit un cycle de vie total de 287 jours pour une violation

Toujours selon ce rapport, le cycle de vie moyen d'une violation s'est allongé d'une semaine entre 2020 et 2021, ce qui s'est traduit par un coût total plus élevé pour les organisations concernées en raison de délais de reprise plus longs. Les entreprises ayant réussi à réduire ces délais ont réalisé d'importantes économies.

> Selon IBM, « en matière de violation de données, un cycle de vie inférieur à 200 jours permet de réduire de presque un tiers les coûts induits par l'incident, par rapport à un cycle de vie supérieur à 200 jours. Une violation dont le cycle de vie dépasse 200 jours a coûté en moyenne 4,87 millions de dollars en 2021, contre 3,61 millions pour une violation avec un cycle de vie inférieur à 200 jours. »

everbridge®

Par ailleurs, plus une entreprise met de temps à remédier aux perturbations, plus elle doit en subir les répercussions. La réputation de la marque peut en souffrir, avec pour effet une baisse des ventes et une fuite de la clientèle. Les interruptions de service minent la confiance que vous accordent vos parties prenantes, en particulier celles qui s'attendent à un temps de fonctionnement de 100 %. Enfin, avec la multiplication des réglementations sectorielles et gouvernementales concernant les interruptions de service, les organisations peuvent avoir à verser d'importantes amendes, dont le montant augmente avec la durée des perturbations.

Ces données prouvent l'importance de reprendre rapidement le cours normal des activités, la résolution d'un incident passant d'abord par la détection du problème.

Dans leurs stratégies visant à accélérer la reprise après un incident, les entreprises doivent s'attacher à réduire le temps passé à détecter les problèmes. Pourquoi est-ce important ? Plus il s'écoule de temps avant la détection d'une cyberattaque ou d'une faille de sécurité, plus le risque de dommages irréparables s'accroît. Aujourd'hui, de plus en plus d'organisations mettent du temps à réaliser qu'elles ont été victimes d'une cyberattaque.

Selon les chiffres d'IBM cités plus haut pour 2021, les entreprises ont mis en moyenne 212 jours à détecter une faille de sécurité. Un délai important qui amplifie les dommages causés, comme en témoignent les coûts exceptionnellement élevés associés à une détection plus tardive des incidents.

Accorder la priorité à une détection plus précoce permet de réduire le délai global de reprise. Alors, comment concentrer ses efforts sur le raccourcissement du délai de détection, et non plus seulement du délai de reprise, et économiser ainsi des millions de dollars ?

Délai de détection et délai de reprise : L'importance d'une détection rapide

Définitions

Le délai moyen de détection fait référence au temps écoulé, en moyenne, avant qu'une organisation ne se rende compte de l'existence d'un incident.

Le délai moyen de reprise fait référence au temps écoulé, en moyenne, avant le retour à une activité normale (on parle également de délai de résolution, de réparation ou de réponse). Chaque variante est porteuse de nuances, mais nous utiliserons ici le terme « reprise », qui fait référence à la durée de vie complète d'un incident, depuis le moment où le système est compromis jusqu'au moment où il redevient opérationnel.

Délai de détection et relations avec les fournisseurs

Les entreprises travaillant avec des fournisseurs doivent être particulièrement attentives à ces questions. En effet, une entreprise aura souvent connaissance d'un incident bien plus tardivement si celui-ci se produit côté fournisseur. Lors de l'établissement de relations avec un fournisseur, veillez à ce que ses normes en matière de délai de détection des incidents correspondent aux vôtres.

Les solutions de gestion des services informatiques aident les entreprises à détecter immédiatement les attaques, à prévenir les dommages, à éviter de coûteuses réparations et à préserver la confiance des clients. Les entreprises adoptent ainsi une approche plus proactive que réactive. Avec l'appui de la technologie et de l'automatisation, les organisations détectent les problèmes avant qu'ils ne se manifestent. Capables de détecter des incidents et d'y répondre rapidement, elles gardent le contrôle des dysfonctionnements dès le début, ce qui réduit à la fois leur impact et les délais de détection et de reprise.

Par ailleurs, la différence de coût en cas d'incident, entre une entreprise ayant déployé l'IA et l'automatisation pour assurer sa sécurité et une entreprise ne l'ayant pas fait, se monte à 80 % selon IBM. En effet, ce coût atteint 2,90 millions de dollars pour les organisations ayant fait le choix de l'IA et de l'automatisation pour leur sécurité, contre 6,71 millions en moyenne pour les entreprises n'ayant pas adopté cette approche. La mise en œuvre d'une technologie qui automatise les processus est positivement corrélée à une réduction du délai de détection et à une limitation des failles de sécurité.

Tendances du secteur : Gestion des incidents majeurs et évolution des technologies

Plus que jamais sous la menace de cyberattaques, les organisations ont pourtant du mal à rattraper leur retard dans ce domaine. Selon le rapport annuel 2020-21 sur la gestion des incidents majeurs, 73 % des personnes interrogées estiment que leur entreprise n'investit pas ou pas assez dans la gestion des incidents majeurs. Plus inquiétant encore, 57 % d'entre elles ignorent ce que coûte à leur entreprise un temps d'arrêt dû à un incident majeur, alors que 45 % ont subi plus de 50 heures d'arrêt.

Ces mauvais chiffres sont en grande partie dus à une organisation des activités en silos. Lorsqu'un incident se produit, les équipes doivent pouvoir collaborer entre les différents services pour gérer au mieux les perturbations. Par ailleurs, les dirigeants doivent placer la gestion des incidents majeurs en tête des priorités et s'intéresser aux ramifications exactes des menaces numériques sur leurs organisations.

Ils doivent prendre conscience que la gestion des incidents majeurs est une composante essentielle de la résilience d'une organisation, sujet qui fait l'objet d'une attention croissante. Le marché offrant désormais une gamme plus large de solutions de ce type, ces dirigeants doivent mener des recherches approfondies sur les outils qui permettront à leurs équipes de gérer au mieux toute cybermenace potentielle.

L'automatisation constitue peut-être la meilleure alliée des équipes informatiques dans ce domaine. La résilience d'une entreprise se mesure à sa capacité à fournir des services de meilleure qualité, plus rapidement, y compris après un événement critique. Comment l'automatisation peut-elle contribuer à atteindre cet objectif ? L'automatisation aide vos équipes informatiques à détecter immédiatement les incidents et à remédier efficacement et rapidement aux problèmes.

everbridge®

Reprise plus rapide grâce à l'automatisation

Avec les bons outils en place, voici comment l'automatisation contribue à accélérer la réponse et la reprise après un incident.

Un événement est signalé au moyen d'outils automatisés, par un utilisateur final ou par le personnel du centre d'exploitation du réseau (NOC).

Un opérateur identifie le problème et déclenche le processus afin de contacter les membres de l'équipe d'intervention disponibles.

Les membres Dev et Ops appropriés de l'équipe d'astreinte CIRT (équipe de réponse aux incidents critiques) sont contactés par le biais du mode de communication le plus susceptible de susciter une réponse immédiate de leur part, en fonction de l'heure de la journée.

L'outil IT Alerting indique automatiquement les personnes indisponibles pour cause de vacances, de déplacement ou de maladie et envoie une notification au personnel qui les remplacent.

L'outil IT Alerting contient déjà les coordonnées, le planning et la répartition géographique des personnes concernées.

Le système organise automatiquement un appel de groupe et vous épargne le casse-tête consistant à passer vous-même de longs appels internationaux avec des numéros de téléphone compliqués. Vous gagnez ainsi de précieuses minutes supplémentaires.

Plus important encore, le système s'intègre de manière transparente avec des outils permettant de visualiser les données de suivi et les informations de diagnostic dans des tableaux de bord pertinents, afin de comprendre ce qui ne tourne pas rond.

Pendant l'appel de groupe, les participants peuvent consulter ces données en temps réel et discuter immédiatement des étapes de résolution.

Une fois qu'une méthode de résolution a été choisie, le système peut également envoyer automatiquement des alertes et des demandes d'approbation au CAB (Change Advisory Board).

everbridge®

Atouts de la solution CEM for Digital d'Everbridge pour votre entreprise

La solution de gestion d'événements critiques pour le numérique (CEM for Digital) aide votre organisation à établir et à maintenir un « retour sur investissement de la résilience opérationnelle » en réduisant les temps d'arrêt et en accélérant la résolution des incidents, grâce à l'automatisation des communications, de la collaboration et de la coordination. Avec CEM for Digital, les organisations apportent une réponse plus fluide aux incidents et accélèrent leur résolution en prenant en compte tous les aspects opérationnels : IT Ops, Service Ops, Sec Ops, DevOps et continuité des activités informatiques/reprise après sinistre.

Elles peuvent gérer l'ensemble du cycle de vie des incidents, avec une approche combinant évaluation, localisation, action et analyse :

+ Évaluation : Évaluation automatique de la gravité et du contexte des incidents informatiques dès qu'ils se produisent
+ Localisation : Identification des équipes et du personnel adéquats en tenant compte de leur disponibilité, de leur emplacement et de leurs compétences
+ Action : Promotion de la communication, la collaboration et la coordination pour traiter rapidement les problèmes
+ Analyse : Visibilité sur la qualité et la rapidité de la réponse aux incidents dans tous les domaines de l'informatique (services, sécurité, DevOps, continuité des activités et reprise après sinistre)

Pour découvrir comment CEM for Digital peut vous aider à renforcer la résilience de votre organisation, contactez Everbridge.

À propos d'Everbridge

Everbridge, Inc. (NASDAQ : EVBG) est un leader mondial dans le domaine des solutions logicielles automatisant et accélérant la réponse opérationnelle des organisations lors d'événements critiques et permettant de maintenir la sécurité des personnes et la continuité des activités (Keep People Safe and Organizations Running™). En cas de menace à la sécurité publique (fusillade, attentat, graves intempéries) ou d'événements critiques pour l'entreprise comme les pannes informatiques, les cyberattaques ou autres incidents tels que les rappels de produits ou les interruptions de la chaîne d'approvisionnement, plus de 5 800 clients dans le monde s'appuient sur la plateforme Everbridge CEM (Critical Event Management, plateforme intégrée pour la gestion des événements critiques) pour recueillir et évaluer rapidement les données relatives aux menaces, localiser les personnes en danger et les intervenants en mesure de leur porter assistance, automatiser l'exécution de processus de communication prédéfinis grâce à la diffusion sécurisée de messages sur plus de 100 appareils de communication différents, et suivre l'avancement des plans d'intervention. Everbridge répond aux besoins de 9 des 10 plus grandes sociétés de conseil au monde, 8 des 10 plus grands constructeurs automobiles internationaux, 7 des 10 plus grandes sociétés technologiques au monde et 8 des 10 plus grandes villes américaines. Everbridge possède son siège social à Boston (Massachusetts, États-Unis) ainsi que des bureaux dans 25 villes réparties dans le monde entier, dont Abu Dhabi, Auckland, Bangalore, Beijing, Budapest, Chicago, Londres, Munich, Oslo, Pasadena, Singapour, Sydney, Tilburg et Vancouver.

Pour en savoir plus, rendez-vous sur **everbridge.com/fr**, le **blog** de l'entreprise, **LinkedIn** ou **Twitter**.

Contactez-nous

Vous voulez en savoir plus à propos de la solution CEM d'Everbridge ? Contactez-nous pour en savoir plus.