DELL Technologies

Le guide de survie en matière de cybersécurité :

Comment réagir face aux cybermenaces modernes

Le monde numérique est devenu une nature sauvage perfide où chaque clic, chaque téléchargement ou chaque connexion peut dissimuler un piège sur le plan de la cybersécurité.

L'environnement actuel est plus dangereux que jamais, avec des menaces aussi variées que les ransomwares, les attaques DDoS, les escroqueries par phishing et les infiltrations de sauvegarde de plus en plus sophistiquées. Les pirates utilisent désormais l'IA pour déjouer les défenses traditionnelles, transformant ce qui était autrefois des attaques opportunistes en menaces calculées et persistantes capables de causer d'immenses dommages.

Des clients Dell ont signalé des attaques alarmantes basées sur l'IA, au cours desquelles des hackers se faufilaient dans les réseaux sociaux pour créer des messages convaincants au point de tromper même les employés les plus avertis dans le domaine de la cybersécurité.

Ces anecdotes rappellent clairement comment les pirates exploitent des technologies avancées pour manipuler, tromper et infiltrer les organisations avec une précision sans précédent.

Pour surmonter les obstacles dans cet environnement hostile, les organisations ont besoin d'une stratégie de cybersécurité complète : un kit de survie qui associe des outils de pointe, des stratégies proactives et une culture de vigilance. Ce guide explore les composantes de ce type de stratégie, afin d'aider les organisations à renforcer leur résilience face aux cybermenaces les plus impérieuses d'aujourd'hui.

Le secret pour bien protéger votre organisation : un cadre Zero-Trust

Dans le paysage actuel des menaces basées sur l'IA, l'adoption d'un cadre Zero-Trust n'est plus une option. Les pirates exploitent l'IA pour automatiser la reconnaissance, dérober des informations d'identification et adapter rapidement leurs techniques, au point de rendre les défenses traditionnelles moins efficaces. L'approche Zero-Trust consiste à partir du principe qu'il y a eu violation, à vérifier en permanence chaque demande d'accès et à mettre en œuvre des processus d'authentification stricts afin de minimiser les risques.

En surveillant les utilisateurs, les appareils et les applications de manière proactive, le cadre Zero-Trust réduit les risques d'accès non autorisés et de violations de données. Il s'agit d'une approche moderne et unifiée de la gestion des identités.

Sécuriser le campement en réduisant la surface d'attaque

À l'heure où les hackers exploitent souvent les points de terminaison, les API et les failles de sécurité de la chaîne logistique, il devient essentiel de réduire la surface d'attaque pour se prémunir des menaces basées sur l'IA. Les points de terminaison et les API servent de points d'accès aux réseaux et sont fréquemment ciblés pour déployer des logiciels malveillants ou mettre la main sur des données sensibles.

La sécurisation de ces zones impose d'adopter une stratégie de défense en couches, avec une authentification forte, un chiffrement des données en transit, des tests réguliers de vulnérabilité, des outils de détection et de réponse au niveau des points de terminaison (EDR), une gestion des correctifs et un renforcement des appareils. Les solutions de surveillance des points de terminaison et la détection continue des menaces permettent d'identifier et de bloquer les activités malveillantes en temps réel.

Les organisations doivent impérativement adopter des stratégies proactives pour sécuriser leurs chaînes logistiques et leur cycle de vie de développement de logiciels. L'application des principes du moindre privilège permet de veiller à ce que seuls les utilisateurs et les applications autorisés soient en mesure d'interagir avec les systèmes stratégiques. Quant aux mécanismes de détection et de neutralisation automatisées des menaces, ils contribuent à résoudre rapidement les vulnérabilités émergentes.

Suivre un guide spécialiste des milieux sauvages : détection et neutralisation proactives des menaces

Les attaques pilotées par l'IA exploitent les faiblesses, imitent les comportements légitimes et s'adaptent en permanence pour contourner les mesures de sécurité, ce qui les rend difficiles à détecter. Pour lutter contre ces menaces sophistiquées, les organisations ne peuvent plus se contenter de simples mesures réactives : elles ont besoin de systèmes avancés de détection des menaces associés à des capacités de réponse rapide. En utilisant l'IA et l'apprentissage automatique, les équipes de sécurité peuvent analyser les schémas comportementaux, détecter les anomalies et répondre aux menaces en temps réel, en traitant les problèmes avant qu'ils ne prennent trop d'ampleur.

Pour être efficaces, les systèmes de détection et de réponse doivent analyser d'énormes quantités de données opérationnelles afin de détecter les risques et de déclencher des réponses automatisées. Cette intelligence sur les menaces s'améliore également au fil du temps : le système, qui devient alors plus intelligent, est capable de détecter et de contrer de manière proactive les tactiques adverses émergentes.

DELL Technologies

Apprendre à construire un abri avant la tempête : réponse aux incidents et récupération

La prévention des attaques constitue la première étape, mais les entreprises doivent agir comme si une attaque était inévitable. L'objectif est de survivre à l'attaque avec un minimum de dégâts, et une stratégie efficace s'articule autour de deux éléments :

- un plan robuste de réponse aux incidents et de récupération (IRR) ;
- des mesures technologiques centrées sur la sauvegarde des données et applications critiques.

Un plan de reprise après incident doit être exhaustif. Une attaque puissante risque de bloquer la plupart des opérations de l'entreprise, sinon la totalité, c'est pourquoi le plan doit couvrir toutes les mesures que prendrait chaque département de l'entreprise en cas de cyberincident. Le plan doit également aborder la façon dont l'organisation entend communiquer en interne et en externe, avec des modèles de communication prérédigés et prêts à l'emploi. Le plan doit être régulièrement contrôlé et mis à jour. En définitive, l'efficacité du plan dépend de la fréquence à laquelle il est mis en pratique. Au moment de l'attaque, tout le monde doit être instinctivement prêt à agir.

D'un point de vue technologique, les organisations doivent commencer par déterminer le **minimum viable pour l'entreprise (MVC)** : quels sont les systèmes qui doivent IMPÉRATIVEMENT rester opérationnels, même si cela suppose de revenir au papier et au crayon ? Est-il important que le service commercial soit constamment opérationnel ? Et qu'en est-il du service client ?

Une fois ces questions évaluées, les mécanismes de sauvegarde et de restauration doivent être conçus en fonction des résultats. Une organisation qui a la possibilité de revenir à des données fiables est en mesure non seulement de reprendre rapidement ses activités, mais également d'empêcher des acteurs malveillants de tenter de prendre leurs données en otage. Les stratégies modernes de réponse aux incidents doivent également aller au-delà des approches traditionnelles, en traitant les systèmes d'IA/LLM tels que les chatbots et les agents virtuels comme des actifs de niveau 1, c'est-à-dire en leur accordant, en matière de récupération, le même niveau de priorité que les systèmes de paiement ou les données clients.

Pour lutter contre les menaces avancées, les plans de réponse aux incidents doivent parvenir à un juste équilibre entre automatisation et contrôles manuels. Il est essentiel de savoir comment votre organisation fonctionnera en cas de panne totale du système. Et si vous deviez revenir au papier et au crayon ?

Tout le monde doit participer : sensibilisation des employés

Vos employés constituent votre première ligne de défense contre les cybermenaces, telle une équipe de survie qui parcourt les dangers dans la nature sauvage. Chaque membre joue un rôle essentiel dans l'identification des risques et la protection des ressources. Pour renforcer cette défense, les organisations ont besoin de programmes de sensibilisation robustes, comprenant par exemple des simulations d'attaque qui incluent des menaces spécifiques à l'IA, telles que le phishing avancé et les deepfakes.

Les meilleurs programmes associent formation continue, communication ouverte, simulations en situation réelle et culture de la responsabilité partagée. C'est en sensibilisant l'ensemble du personnel, des employés de première ligne jusqu'aux dirigeants, aux menaces traditionnelles et aux menaces liées à l'IA que l'entreprise pourra s'établir en organisation véritablement vigilante et informée. En favorisant le travail d'équipe et la préparation, votre entreprise pourra garder une longueur d'avance sur l'évolution des cyberrisques et mettre en place une défense résiliente contre les attaques potentielles.

Pratiques d'excellence pour préserver votre résilience face aux attaques basées sur l'IA

Pour rester résilientes face aux attaques basées sur l'IA, les organisations doivent adopter une approche proactive et stratégique. Voici 10 pratiques d'excellence à adopter :

Architecture Zero-Trust

Imposer une vérification continue, des contrôles d'accès stricts et une segmentation du réseau pour s'assurer que chaque utilisateur et chaque appareil sont authentifiés avant de leur accorder un accès, de manière à bloquer et contenir les attaques rapides basées sur l'IA.

Renforcement de la gestion des accès et des identités :

Déployer des moyens d'authentification robustes (MFA, RBAC) et appliquer des stratégies d'identification strictes pour limiter les chances de réussite des attaques par phishing et par credential stuffing.

Inventaire et découverte automatisés des actifs :

Détecter et surveiller en permanence l'ensemble des actifs, y compris Cloud, IoT et IT fantôme, afin d'éviter les expositions cachées.

Micro-segmentation et contrôles d'accès réseau :

Segmenter et isoler les réseaux et les charges applicatives afin de prévenir les attaques latérales et de contenir les menaces.

Renforcement des points de terminaison et des API :

Utiliser une protection avancée des points de terminaison (EDR/XDR) et des passerelles API sécurisées ; authentification forte, limitation du débit, validation des entrées et chiffrement.

Gestion rigoureuse des failles de sécurité et des correctifs :

Automatiser l'analyse et l'application rapide de correctifs pour les systèmes d'exploitation, le firmware, les applications, les API et les logiciels tiers.

Détection et surveillance des menaces basées sur l'IA :

Exploiter la détection des comportements et anomalies optimisée par l'IA/ML pour repérer les menaces subtiles ou automatisées en temps réel.

Réponse aux incidents automatisée :

Utiliser des playbooks automatisés pour isoler, contenir et corriger rapidement les menaces, de manière à réduire le temps d'intervention des hackers.

Des simulations réalistes régulières et une amélioration continue :

Entreprendre des exercices de simulation en salle, des attaques fictives (red teaming) et des simulations de phishing ; mettre à jour les plans de réponse aux incidents et les modèles de détection en fonction des résultats.

Sauvegardes et restaurations immuables et isolées :

Conserver des sauvegardes inviolables et, dans l'idéal, isolées et régulièrement testées pour garantir une restauration rapide et propre.

DELL Technologies

Dell Technologies : votre guide pour naviguer dans l’inconnu

Pour protéger votre organisation contre les cybermenaces avancées, vous avez besoin des bons outils et d’une expertise adéquate pour garder une longueur d’avance sur des risques qui évoluent constamment. Dans le paysage complexe de la cybersécurité actuelle, une stratégie robuste est essentielle pour protéger vos données, vos systèmes et votre réputation. C’est là que Dell Technologies intervient, en proposant une gamme complète de solutions adaptées aux besoins des organisations de toutes tailles.

De la protection de la chaîne logistique à la détection avancée des menaces, en passant par la protection des points de terminaison et la gestion sécurisée des données, Dell donne à votre entreprise la technologie nécessaire pour se défendre contre les cyberattaques modernes. Forte de son expertise de pointe, l’équipe Dell intervient en étroite collaboration à vos côtés pour élaborer une stratégie de sécurité personnalisée. Avec des fonctionnalités telles que la surveillance en temps réel, la réponse aux menaces automatisée et l’architecture Zero-Trust, Dell met tout en œuvre pour aider votre organisation à rester proactive et résiliente.

Que vous cherchiez à lutter contre le ransomware, à vous prémunir des attaques par phishing ou à vous conformer aux réglementations, Dell Technologies vous aide à surmonter en toute confiance les difficultés du paysage actuel des menaces. Faites équipe avec Dell pour protéger votre entreprise et prospérer à l’ère du numérique, en veillant à ce que vos opérations restent sécurisées, efficaces et parées à toute éventualité.

> Votre plan de réponse aux incidents doit être imprimé sur papier car vos systèmes peuvent devenir inaccessibles lors d’une attaque. »
>
> ***Rachel Tyler***
> *Cybersecurity Advisory Consultant, Dell Services*

Produits et solutions Dell qui peuvent vous aider

Solution Dell proposée	Description
Infrastructure Dell de confiance	associer des serveurs à des solutions réseau, de stockage et de cyberrésilience Dell pour établir les bases modernes, sécurisées et résilientes indispensables à l’innovation.
Cyber-résilience	Une gamme complète de solutions conçues pour protéger vos données et garantir une restauration en toute sécurité. Comprend des appliances, des logiciels et des offres as-a-service.
Services de cybersécurité	Une suite de services conçue pour vous aider à développer et mettre en œuvre une stratégie de sécurité complète pour toutes les charges applicatives. La suite comprend, entre autres offres, des services de conseil, un vCISO, la solution Managed Detection and Response, des tests de pénétration et de vulnérabilité, ainsi que des services de réponse aux incidents et de récupération.
Dell Trusted Workspace (sécurité des points de terminaison)	Une combinaison de fonctionnalités intégrées et complémentaires en option conçues pour sécuriser les PC professionnels. Inspirées des pratiques de chaîne logistique sécurisées, les fonctionnalités intégrées incluent SafeBIOS et SafeID avec TPM. Les modules complémentaires Secured Component Verification et SafeID with ControlVault sont proposés en option, de même que les logiciels partenaires CrowdStrike et Absolute conçus pour optimiser la sécurité de l’espace de travail.

Découvrez comment relever certains des défis actuels majeurs en matière de cybersécurité sur **dell.com/cybersecuritymonth**