STORMSHIELD

STORMSHIELD NETWORK VULNERABILITY MANAGER

DEVANCER LES NOUVELLES MENACES

OPTION

Bénéfices client

- Inventaire applicatif
- Détection des vulnérabilités en temps réel
- Préconisations de remédiation
- Adaptation aux contraintes opérationnelles
- Disponibilité du SI et des actifs sensibles

Face aux attaques modernes qui concernent les entreprises de toutes tailles, les systèmes de protection traditionnels ne sont plus suffisants. Une gestion efficace et continue des vulnérabilités est nécessaire.

Dotez-vous d'un outil de détection de vulnérabilités simple et performant sans impact sur votre système d'information.

ÉVOLUTION DES MENACES

L'explosion des réseaux sociaux, la mise en ligne de contenu web 2.0 par les internautes et l'usage des terminaux mobiles ont offert de nouveaux moyens à la cybercriminalité pour se développer. Cette dernière redouble d'inventivité pour concevoir des contenus malveillants toujours plus sophistiqués et ainsi attendre ses objectifs.

Les codes malicieux sont conçus pour être de moins en moins détectables par les systèmes de protection traditionnels. Ils s'appuient sur les vulnérabilités des applications utilisées par les utilisateurs finaux pour compromettre de plus en plus de machines.

TOUS CONCERNÉS

Les objectifs de la cybercriminalité sont principalement financiers (rançon, vol et revente de données, attaques à la demande) ou activiste (politique, idéologique). La création de botnets, le rebond vers une autre société d'un même écosystème informatique, les attaques à moindre coût rendues possibles grâce à la banalisation de services de piratage en ligne, sont autant de menaces qui ciblent toutes les entreprises, quelque soit leur taille ou leur notoriété.

Chaque jour de nouveaux sites web, y compris ceux de grandes organisations ou des sites à-priori de confiance, sont pris pour cible dans le but d'injecter et d'héberger des codes malveillants. Ces codes exploitent les nombreuses vulnérabilités des navigateurs web et des composants associés, comme Flash ou Java, pour compromettre les postes des visiteurs. Plus de 30% des attaques basées sur le web exploiteraient les vulnérabilités des plugins Java.

À PROPOS

Arkoon et Netasq, filiales à 100% d'Airbus Defence and Space CyberSecurity, opèrent sous la marque Stormshield et proposent tant en France qu'à l'international des solutions de sécurité de bout-en-bout innovantes pour protéger les réseaux (Stormshield Network Security), les postes de travail (Stormshield Endpoint Security) et les données (Stormshield Data Security).

WWW.STORMSHIELD.EU

Téléphone

N°Cristal 09 69 32 96 29
APPEL NON SURTAXE

Page de contact email

DÉTECTION TEMPS RÉEL

Pour contrer ces attaques modernes, la détection et le traitement des failles sur lesquelles elles s'appuient constitue un premier rempart de protection.

Le temps moyen nécessaire pour qu'un attaquant exploite une vulnérabilité a considérablement diminué ces dernières années. Dans la course contre les menaces, une approche par détection planifiée, proposée par les scanners de vulnérabilités dits « actifs », n'apporte pas la réactivité nécessaire. Il est préférable d'opter pour une solution détecte les vulnérabilités en continu et en temps réel.

UN OUTIL DÉDIÉ AUX ÉQUIPES OPÉRATIONNELLES

Stormshield Network Vulnerability Manager est embarqué nativement dans le moteur de prévention des attaques de tous les appliances Stormshield Network Security. Sa technologie unique et brevetée vous donne, en temps réel, l'assurance que vos actifs ne présentent pas de failles connues.

A partir des données transitant par l'appliance, Stormshield Network Vulnerability Manager inventorie les systèmes d'exploitation, les applications utilisées et leurs vulnérabilités. Cette cartographie vous offre une visibilité continue de votre parc informatique. Aussitôt qu'une vulnérabilité est détectée sur votre réseau, vous en êtes averti.

CONTINUITÉ D'ACTIVITÉ

Les réseaux des entreprises doivent rester opérationnels en permanence pour répondre aux besoins des métiers et des utilisateurs. La détection de vulnérabilités est fréquemment réalisée au moyen de scans dits « actifs » qui génèrent plusieurs centaines de connexions par machine auditée. Ces scans provoquent fréquemment des dysfonctionnements matériels et/ou des perturbations réseau.

Grâce à son système de détection des vulnérabilités directement dans le flux, Stormshield Network Vulnerability Manager est non intrusif. La recherche des vulnérabilités s'effectuant par analyse des connexions, elle n'a aucune incidence sur la disponibilité des serveurs ou des équipements sensibles.

REMEDIATION (PASSEZ À L'ACTION)

Stormshield Network Vulnerability Manager propose un ensemble de rapports dédiés ainsi qu'un tableau de bord temps réel qui vous permettent de garder la maîtrise de votre parc informatique.

Vous pouvez ainsi identifier facilement les applications, les systèmes d'exploitation et les machines vulnérables. Les failles remontées sont classifiées par criticité et par type d'exploitation (distante ou locale).

Les rapports proposés présentent, de manière intuitive, les actions correctives qu'il convient de réaliser. Si aucun correctif ne peut être appliqué pour une vulnérabilité, la création d'une règle de filtrage pour mitiger le risque sera aisée car réalisée depuis la même interface graphique. Cet accompagnement à la remédiation permet un gain de temps non négligeable dans l'administration du système d'information.

Grâce à Stormshield Network Vulnerability Manager, vous pouvez être plus réactifs vis-à-vis des demandes internes liées à la conformité du système d'information. Vous pouvez anticiper les audits et démontrer ainsi la valeur ajoutée de vos actions.

Netasq
Parc Scientifique Haute Borne - Parc Horizon, Bat 6, Avenue de l'Horizon 59650 Villeneuve d'Ascq