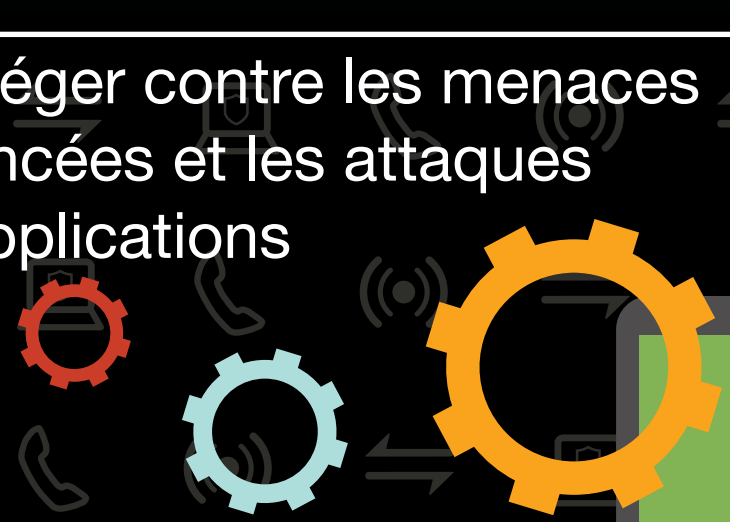
Mighty Guides

Sécuriser votre infrastructure réseau et applications

Partie 4 : Se protéger contre les menaces persistantes avancées et les attaques basées sur les applications

2 Des experts partagent leurs secrets



SPONSORED BY:

FORTINET®

AVANT-PROPOS

Les défis liés à la sécurité du réseau évoluent plus rapidement que jamais en raison de la complexité des nouvelles technologies et applications. En outre, les entreprises continuent de subir de nombreux problèmes historiques, allant de la simple sécurité des mots de passe à la mise à jour des logiciels.

Ce recueil de 24 études couvre une grande variété de sujets regroupés dans cinq grandes catégories, allant de la nécessité de planifier à l'avance la sécurité de votre réseau aux nouveaux défis posés par l'ingénierie sociale et d'autres menaces persistantes avancées. Un thème majeur de plusieurs de ces études est la perte du périmètre et de l'efficacité des défenses traditionnelles. Les politiques BYOD (Bring Your Own Device, apportez votre appareil personnel) et les services basés sur le Cloud créent de nombreuses brèches dans un réseau d'entreprise qui nécessitent de repenser la sécurité pour protéger les données, et pas seulement les méthodes d'accès.

La plateforme de sécurité de Fortinet peut résoudre la plupart des problèmes décrits dans les études réunies dans ce livre électronique. Nos firewalls FortiGate optimisés par la technologie ASIC offrent les performances NGFW (Next Generation Firewall, firewall nouvelle génération) les plus rapides du secteur et sont la fondation d'une solution de sécurité de bout en bout couvrant vos utilisateurs, votre réseau, vos datacenters et le Cloud. Concernant les problèmes que nous ne pouvons pas résoudre directement, nous proposons des outils tels que l'application de politiques d'entreprise pour les changements de mot de passe et des scanners de vulnérabilités pour vos applications, pour vous aider à identifier les failles.

Nous espérons que vous trouverez ces études aussi intéressantes et aptes à susciter la réflexion que nous, et qu'elles vous aideront à renforcer les défenses de sécurité de votre réseau et de vos applications.

INTRODUCTION

Avec toute l'attention dont la sécurité des données a fait l'objet au cours de ces dernières années et maintenant que toutes les avancées techniques réalisées dans la détection des risques sont disponibles pour protéger les infrastructures de réseau, vous pourriez croire que les données sont aujourd'hui plus sécurisées que jamais. Malheureusement, le nombre de récentes fuites de données d'une ampleur terrifiante vient contredire cette impression. Rien qu'au cours de ces 18 derniers mois, Adobe, eBay, JPMorgan Chase, Target, Home Depot, Community Health Services et le Gouvernement des États-Unis ont subi des brèches qui, cumulées, représentent plus de 500 millions d'enregistrements. Le monde sera-t-il un jour un endroit sûr pour des données revêtant un caractère aussi vital pour les entreprises et les individus ?

Avec le généreux soutien de Fortinet, nous avons créé ce livre électronique pour vous aider à mieux comprendre les défis que les entreprises, et plus particulièrement les entreprises de taille moyenne, doivent aujourd'hui relever en matière de sécurité. Ce livre électronique compile les réponses à la question suivante :

Quels sont les plus grands défis que vous devez relever pour sécuriser votre infrastructure de réseau et d'applications ?

Des analystes du secteur, des consultants et des experts en sécurité ont répondu à cette question. Ils ont fourni un éclairage fascinant sur les défis que nous devons aujourd'hui relever en matière de sécurité. Les problèmes de sécurité sont aggravés par le caractère changeant de l'infrastructure et la perte du périmètre réseau, l'évolution rapide de l'environnement applicatif, le manque de sensibilisation à la sécurité parmi les utilisateurs et la complexité croissante des solutions de sécurité. Les attaques et les vols de données sont également devenus une industrie florissante gérée par des entités sophistiquées et bien financées.

Bien que la sécurité et la vigilance soient une lutte sans fin, je ne doute pas que vous trouverez utiles les nombreux points de vue de ceux qui se trouvent en première ligne dans le cadre de vos efforts de sécurisation de l'infrastructure d'entreprise.

Cordialement,
David Rogelberg
Éditeur

Mighty Guides

Les Mighty Guides vous rendent plus fort.

Ces divers guides de référence fournissent une vue complète sur un sujet. Ils vous aident à explorer, comparer et confronter différents points de vue pour identifier la meilleure solution. Lire un Mighty Guide, c'est un peu comme disposer de votre propre équipe d'experts. Chaque conseil bienveillant et sincère fourni par ce guide se trouve juste à côté du nom, de la biographie et des liens de son contributeur, ce qui vous permet d'en savoir plus sur lui. Ces informations vous permettent de connaître le contexte dans lequel chaque expert exprime son point de vue indépendant.

Les conseils éclairés des meilleurs experts vous aident à prendre les décisions importantes qui vous rendent plus fort.

Se protéger contre les menaces persistantes avancées et les attaques basées sur les applications

Dans le monde de la cybersécurité,

il y a

BEAUCOUP DE BRUIT...

...et il y a les faits.

Le marketing tapageur a une façon de brouiller la vérité : la lenteur c'est dépassé. Vous n'avez pas besoin de choisir entre une stratégie de sécurité forte et des performances réseau optimales pour gérer efficacement votre entreprise.

97,3 % de détection efficace des brèches
5 x les performances des **firewalls nouvelle génération**
N°1 en parts de marché dans le monde pour la sécurité réseau
Plus de 200 attaques zero-day découvertes

Vous pouvez avoir les deux, mais uniquement auprès de nous.

Procédez dès aujourd'hui à une évaluation des cybermenaces et faites le point sur votre stratégie de sécurité.
www.fortinet.com/ctap

FORTINET

Une sécurité sans compromis

LES APPLICATIONS REPRÉSENTENT AUJOURD'HUI LES PLUS GRANDS RISQUES EN MATIÈRE DE SÉCURITÉ

MIKHAEL FELKER

Directeur de la sécurité de l'information,
VC backed eCommerce

Mikhael Felker est le directeur de la sécurité de l'information d'une entreprise en pleine croissance à Santa Monica, en Californie. Son expérience professionnelle combine la sécurité de l'information, la confidentialité, l'enseignement, le journalisme technique et la direction d'ONG dans des secteurs tels que la défense, la santé, les ONG, l'éducation et les technologies. Mikhael a obtenu une maîtrise en politique et gestion de la sécurité de l'information à l'université Carnegie-Mellon et une licence d'informatique à l'université de Californie à Los Angeles.

Twitter I Blog

Téléchargez le livre électronique complet :
Sécuriser votre infrastructure réseau et applications

Dans une infrastructure de réseau et d'applications moderne, les applications sont devenues le risque principal pour plusieurs raisons. La première est la prolifération des applications rendue possible par le fait qu'elles n'ont jamais été aussi faciles à développer. Le nombre d'applications qui apparaissent dans un environnement d'entreprise ordinaire augmente sans cesse et ces applications évoluent rapidement. Malheureusement, les ressources disponibles pour résoudre les problèmes de sécurité que ces applications peuvent engendrer sont comparativement fixes. En outre, plusieurs dynamiques d'entreprise aggravent le problème de la sécurité des applications.

PRINCIPAUX ENSEIGNEMENTS

1. LE NOMBRE D'APPLICATIONS QUI APPARAISSENT DANS UN ENVIRONNEMENT D'ENTREPRISE ORDINAIRE AUGMENTE SANS CESSE, TANDIS QUE LES RESSOURCES DISPONIBLES POUR RÉSOUDRE LES PROBLÈMES DE SÉCURITÉ QUE CES APPLICATIONS PEUVENT ENGENDRER SONT COMPARATIVEMENT FIXES.
2. MÊME SI VOUS POUVIEZ RÉDUIRE LA LISTE DES FAILLES CONNUES À UN SEUL RISQUE ÉLEVÉ, VOUS DEVRIEZ TOUT DE MÊME DONNER LA PRIORITÉ À CE CORRECTIF PLUTÔT QU'AU REVENU POTENTIEL DU DÉVELOPPEMENT DE NOUVELLES FONCTIONNALITÉS.

Il fut un temps où l'infrastructure se trouvait sur site et où les cycles de développement n'étaient pas aussi rapides. Dans ce type d'environnement, la sécurisation de l'infrastructure était plus simple. Aujourd'hui, avec des environnements hybrides complexes et l'impératif d'accélérer les cycles de développement des applications, il est beaucoup plus difficile de développer des applications sécurisées dans les délais impartis. Chaque division peut avoir son propre environnement et travailler avec ses propres fournisseurs. De plus, ces environnements changent constamment. Le personnel informatique ne cesse de créer et de démanteler des réseaux privés virtuels.

> *« Corriger les failles connues . . . revient à faire passer la maintenance avant les efforts de développement de fonctionnalités applicatives génératrices de revenus. »*

LES APPLICATIONS REPRÉSENTENT AUJOURD'HUI LES PLUS GRANDS RISQUES EN MATIÈRE DE SÉCURITÉ

Les entreprises qui ont une vue d'ensemble en temps réel de l'environnement peuvent se concentrer sur les priorités absolues en matière de sécurité. Toutefois, cette vision globale est difficile à obtenir. Des produits sont disponibles pour faciliter l'agrégation d'une vue de l'environnement d'entreprise. Des outils d'analyse et de visualisation peuvent fournir au personnel informatique un instantané de l'environnement, qu'ils peuvent ensuite utiliser pour hiérarchiser leurs efforts en matière de sécurité.

Toutefois, même en disposant d'instantanés d'un environnement complexe changeant constamment, d'autres défis liés au développement d'applications sécurisées existent, tels que la hiérarchisation des efforts de développement et l'allocation des ressources de développement. Concernant la hiérarchisation, supposons que le service informatique connaisse toutes les vulnérabilités d'une application et comprenne parfaitement les cas d'utilisation de l'entreprise pouvant faire l'objet d'abus. Le service informatique doit corriger ces failles avant de développer de nouvelles fonctions, c'est-à-dire faire passer la maintenance avant les efforts de développement de fonctionnalités applicatives génératrices de revenus. Même si le service informatique pouvait réduire la liste des failles connues à un seul risque élevé à corriger, il devrait tout de même donner la priorité à ce correctif plutôt qu'au revenu potentiel du développement de nouvelles fonctionnalités.

Au problème de la hiérarchisation vient s'ajouter celui de l'allocation des ressources. Lorsqu'elles évaluent la sécurité globale des applications, les entreprises doivent prendre en compte les services applicatifs, les applications mobiles et les interfaces de programmation d'applications. Elles doivent également tenir compte de l'environnement applicatif : sur site, plateforme en tant que service ou infrastructure en tant que service. La pression pour développer et lancer des applications rapidement est telle que les entreprises manquent souvent de ressources pour tester ces applications dans tous les environnements dans lesquels le personnel pourrait les utiliser.

> *« Il est plus important que jamais d'impliquer les professionnels de la sécurité de l'information dès les premières étapes des projets d'entreprise. »*

La combinaison de ces trois facteurs (le nombre croissant d'applications ; l'allocation des ressources de développement et de test pour des environnements hybrides de plus en plus complexes ; et la priorité donnée aux correctifs de sécurité plutôt qu'au développement de nouvelles fonctionnalités génératrices de revenus) fait des applications l'un des plus grands risques en matière de sécurité pour les entreprises actuelles. Pour relever ce défi, il est plus important que jamais d'impliquer les professionnels de la sécurité de l'information dès les premières étapes des projets d'entreprise, notamment la définition des exigences en matière de sécurité et de conformité, ainsi que de minimiser les risques et la refonte des projets. Il est également important de tirer parti des normes, des cadres et des méthodologies existants, tels que le National Institute of Standards and Technology et l'International Organization for Standardization, pour que les projets aient une référence en matière de sécurité.

LA DÉTECTION TARDIVE DES MENACES ET LA RÉPONSE LENTE CONSTITUENT LES PLUS GRANDES MENACES

ERLEND OFTEDAL

Consultant senior en sécurité,
F-Secure

Erlend Oftedal a travaillé pendant plus de 10 ans en tant développeur de logiciels et testeur de sécurité. Il est intervenu dans plusieurs conférences sur la sécurité et le développement, et développe des outils de sécurité Open Source. Erlend est le responsable du "chapitre" norvégien d'OWASP (Open Web Application Security Project).

Twitter I Blog

Téléchargez le livre électronique complet :

Sécuriser votre infrastructure réseau et applications

Il est important de reconnaître que quel que soit le nombre de protections que nous intégrons à notre infrastructure, nos systèmes seront toujours vulnérables. La vraie menace pour la sécurité vient du fait de ne pas détecter les attaques suffisamment tôt et de ne pas y répondre suffisamment rapidement. Plusieurs violations majeures de la sécurité perpétrées au cours de ces dernières années se sont poursuivies pendant des mois avant d'être détectées.

PRINCIPAUX ENSEIGNEMENTS

1. TANT QUE LES ANCIENNES APPLICATIONS VULNÉRABLES EXISTERONT, LES DÉVELOPPEURS COMMETTRONT DES ERREURS, LES UTILISATEURS FERONT DES CHOSES QU'ILS NE SONT PAS CENSÉS FAIRE ET LES PIRATES ACCÉDERONT AU SYSTÈME.
2. DE NOUVEAUX OUTILS PERMETTANT AUX DÉVELOPPEURS D'INTÉGRER UNE SURVEILLANCE ACTIVE DE LA SÉCURITÉ DANS LES APPLICATIONS.

Quels facteurs contribuent à l'insécurité des réseaux et de l'infrastructure ? Un facteur important est la complexité croissante des réseaux et des environnements logiciels. Les entreprises possèdent souvent une grande variété de systèmes acquis au fil des années, y compris des applications basées sur des infrastructures vétustes et des bibliothèques au sujet desquelles plus personne ne sait rien au sein de l'entreprise. Parfois, le fabricant d'origine d'une application a disparu et l'entreprise ferait mieux de développer un nouveau code plutôt que de corriger d'anciennes vulnérabilités.

Les logiciels eux-mêmes deviennent de plus en plus complexes et tributaires de code tiers. Il y a dix ans, d'après certaines études, 80 % du code d'une nouvelle application était personnalisé et 20 % provenait de bibliothèques. Aujourd'hui, 20 % des nouvelles applications sont constituées de code personnalisé et 80 % du code provient de bibliothèques.

> *« Quel que soit le nombre de protections que nous intégrons à notre infrastructure, nos systèmes seront toujours vulnérables. »*

LA DÉTECTION TARDIVE DES MENACES ET LA RÉPONSE LENTE CONSTITUENT LES PLUS GRANDES MENACES

Le développement des applications a changé. Il inclut davantage de tests de sécurité durant le processus de développement, avec des outils qui détectent le code de bibliothèque vulnérable et des routines de sécurité intégrées au stade des tests d'unité. Malgré cela, les développeurs font des erreurs. Et les utilisateurs aussi.

Tant que les anciennes applications vulnérables existeront, les développeurs commettront des erreurs, les utilisateurs feront des choses qu'ils ne sont pas censés faire et les pirates accéderont au système. La meilleure protection contre ces menaces est une détection précoce et une réponse rapide. Les entreprises se fient à des solutions telles que les firewalls nouvelle génération et les pots de miel pour se protéger contre les menaces connues et rechercher toute activité suspecte pouvant indiquer une menace jusqu'alors inconnue. Une nouvelle approche du développement logiciel potentiellement plus efficace pour certains types d'application consiste à utiliser de nouveaux outils permettant aux développeurs d'intégrer une surveillance active de la sécurité et des capteurs dans les applications. Si l'application détecte une violation de son comportement opérationnel connu, elle peut envoyer des alertes, bloquer une activité, voire fermer l'application. Chaque application intégrerait des contrôles de sécurité spécialement conçus pour la protéger contre les comportements illégaux. L'avantage par rapport aux solutions de sécurité génériques est que celles-ci ne savent jamais précisément comment une application autorisée est censée se comporter.

À l'heure où notre dépendance envers les logiciels dans notre vie quotidienne croît au travail, à la maison et même en voiture, il est crucial d'avoir une visibilité permettant d'accélérer la détection, la réponse (pour contenir toutes sortes d'attaques) et le déploiement des correctifs lorsque des vulnérabilités sont découvertes.

> *« La meilleure protection contre ces menaces est une détection précoce et une réponse rapide. »*

Dans le monde de la cybersécurité, il y a l'

ARGUMENTAIRE COMMERCIAL...

...et il y a les faits.

Notre concentration sur l'innovation au cours de ces 15 dernières années vous permet de simplifier votre stratégie de sécurité et de conserver une longueur d'avance sur les menaces actuelles, pas dans une prochaine version qui n'existe que dans un argumentaire.
Nous proposons une approche consolidée du datacenter au terminal, ainsi qu'une visibilité et un contrôle globaux sur un seul système d'exploitation avec une seule console de gestion.

Nous sommes fiers du travail de nos laboratoires.

97,3 % de détection efficace des brèches
5 x les performances des **firewalls nouvelle génération**
N°1 en parts de marché dans le monde pour la sécurité réseau
Plus de 200 attaques zero-day découvertes

Procédez dès aujourd'hui à une évaluation des cybermenaces et faites le point sur votre stratégie de sécurité.
www.fortinet.com/ctap

FORTINET

Une sécurité sans compromis