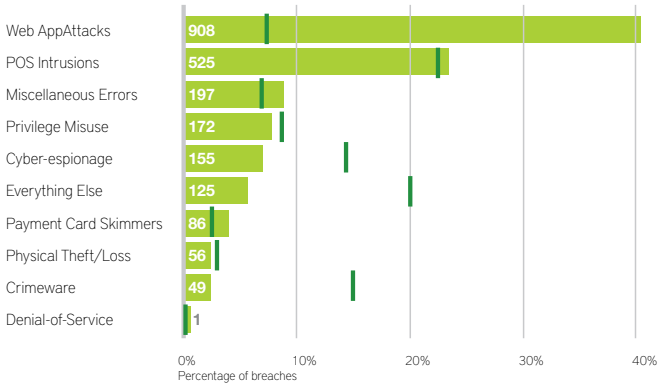
REALDOLMEN
a Gfi Group company

HYBRID CLOUD
IDENTITÉ SÉCURISÉE

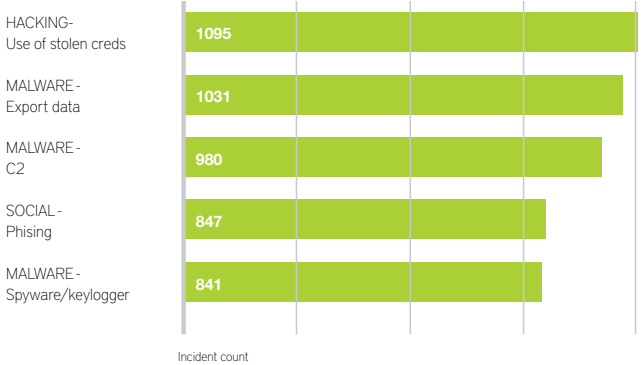
Hybrid Cloud Identité sécurisée

Verizon publie chaque année son rapport d'enquête sur les violations de données ou « Data Breach Investigations Report » (DBIR). Chaque année, les organisations envoient leurs données relatives à des milliers d'incidents de sécurité et de violations de données à Verizon, dont les chercheurs analysent ces informations en vue de déceler de nouveaux modèles, des tendances stables et des informations relatifs à l'évolution du paysage des menaces numériques.

PERCENTAGE, AND COUNT OF BREACHES PER PATTERN.



TOP THREAT ACTION VARIETIES WITHIN INCIDENTS INVOLVING CREDENTIALS



source: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

LES CITATIONS DU DBIR 2016 :

- Incidents dans plus de 82 pays
- Dans les secteurs public, du divertissement, de la finance et de l'information
- Plus d'incidents de sécurité que de violations de données
- Divulgation confirmée (pas uniquement exposition potentielle) de données à une partie non autorisée
- 1 429 incidents ou vols de références

Malheureusement, souvent les efforts consentis pour réduire les menaces de sécurité potentielles ne sont pas suffisants. La sécurité devrait néanmoins être l'affaire de chacun dans toutes les entreprises, du niveau C à l'ingénieur système. Toutefois, les précautions de sécurité « à la mode » il y a quelques années ne s'appliquent plus. Il convient d'adopter un nouveau raisonnement, afin de s'assurer que les données de l'entreprise restent sa propriété et celle de personne d'autre.

POSEZ-VOUS LES QUESTIONS SUIVANTES

Voici quelques questions parmi d'autres que vous devriez vous poser par rapport à votre environnement :

DISPOSEZ-VOUS DE NOMBREUX COMPTES AUX AUTORISATIONS LARGES, TELS QUE DES ADMINISTRATEURS DE DOMAINE ?

Octroyer des autorisations superflues peut créer des possibilités sortant des attributions de travail autorisées. Nous souhaitons uniquement fournir des autorisations d'accès aux utilisateurs qui en ont réellement besoin pour réaliser leurs tâches quotidiennes.

POUVEZ-VOUS RETRACER LES ACTIONS SELON LA PERSONNE QUI LES A RÉALISÉES, LE MOMENT D'EXÉCUTION ET LE SYSTÈME SOURCE ?

Les audits devraient faire partie intégrante de toute organisation IT, afin de permettre de visualiser ce qui a posé problème, qui a réalisé l'action concernée, quand et où.

VOS APPLICATIONS WEB SONT-ELLES PUBLIÉES EN TOUTE SÉCURITÉ EN EXTERNE ?

Rendre des applications accessibles aux utilisateurs hors du réseau est une chose, mais le faire en toute sécurité est un aspect tout à fait différent.

AVEZ-VOUS MIS EN PLACE UNE GESTION DU CYCLE DE VIE DES UTILISATEURS POUR LES UTILISATEURS QUI QUITTENT L'ORGANISATION OU PRENNENT UN AUTRE RÔLE AU SEIN DE L'ENTREPRISE ?

Un compte utilisateur inactif, par exemple, peut être utilisé pour accéder aux ressources sans avertissement puisqu'il s'agit d'un compte valide.

LES MOTS DE PASSE CONSTITUENT-ILS LE SEUL MOYEN DE SÉCURISER LES APPLICATIONS ?

Une authentification multifacteurs contribue à sécuriser l'accès aux données et applications. Il s'agit néanmoins d'une étape supplémentaire devant être réalisée par les utilisateurs finaux. Elle peut être réalisée de manière transparente en ajoutant une couche de sécurité additionnelle.

ÊTES-VOUS PROTÉGÉ CONTRE LES ATTAQUES « PASS-THE-HASH » ? DISPOSEZ-VOUS D'UNE POLITIQUE RELATIVE AUX MOTS DE PASSE CORRECTE ?

Sans solution de politique relative aux mots de passe correcte, l'entreprise n'est pas protégée contre toute une série d'attaques. L'accès à 1 machine peut impliquer l'accès à plusieurs machines.

CONTRÔLEZ-VOUS LE COMPORTEMENT DE CONNEXION AU SEIN DE VOTRE ORGANISATION ? DEPUIS QUELS APPAREILS LES COLLABORATEURS SE CONNECTENT-ILS ? COMBIEN DE TENTATIVES FONT-ILS ?

La grande majorité des violations de sécurité surviennent lorsque les attaquants accèdent à un environnement en usurpant l'identité d'un utilisateur. Un ensemble d'outils spécifiques vous permet de suivre et d'analyser le comportement de connexion avec l'aide de l'apprentissage machine.

QU'OFFRONS-NOUS ?

Realdolmen vous guide dans votre quête d'une identité hybride plus sécurisée. Nous définirons ensemble la manière dont vous pouvez donner à votre environnement actuel un niveau de sécurité d'identité contemporain.

Au cours d'une évaluation de 4 à 8 jours, nous répertorions les risques et vulnérabilités. Nous identifions des recommandations et définissons l'approche permettant de réaliser votre identité hybride sécurisée.

Les conclusions de cette évaluation sont fournies lors d'une présentation d'une demi-journée et dans un rapport, comprenant des recommandations, des meilleures pratiques de l'industrie et des définitions de projet.
Outre cette évaluation initiale, Realdolmen peut fournir un suivi annuel en vue d'identifier les progrès accomplis, car la sécurité n'est pas un domaine statique, mais un trajet en pleine évolution.

AVANTAGES D'UNE IDENTITÉ HYBRIDE SÉCURISÉE

- Publiez des applications en externe sans souci
- Accroissez la confiance des utilisateurs finaux dans les systèmes IT et administrations
- Ne paniquez plus à l'idée d'un audit externe
- Ne passez plus un temps fou à retracer des attaques malveillantes au sein de votre organisation
- Redonnez le sourire à votre responsable de la sécurité

INTÉRESSÉ(E) ?

Vous souhaitez réduire la surface d'attaque de votre entreprise ? Vous ne voulez pas finir dans le rapport sur les violations de données de Verizon ? Vous désirez que nous vous guidions dans votre évolution vers une infrastructure d'identité plus sécurisée ?

Pour plus d'informations, veuillez contacter: info@realdolmen.com.

E.R.: NV RealDolmen SA, A. Vaucampslaan 42, B-1654 Huizingen.

REALDOLMEN

info@realdolmen.com
WWW.REALDOLMEN.COM

A. Vaucampslaan 42
B-1654 Huizingen
TEL +32 2 801 55 55