2017 Data Breach Investigations Report

Synthèse

verizon

Aperçu

Pour la dixième année consécutive le Data Breach Investigations Report (DBIR) explore le monde opaque de la cybersécurité. Il rassemble l'expérience collective de 65 contributeurs pour vous dresser une image complète de la cybercriminalité.

Qui se cache derrière les compromissions ?

75% perpétrées par des personnes extérieures.

25% impliquaient des acteurs internes.

18% étaient réalisées par des acteurs gouvernementaux.

3% mettaient en scène des parties multiples.

2% impliquaient des partenaires.

51% impliquaient le crime organisé.

Quelles tactiques utilisent-ils ?

62% des compromissions comportaient du piratage.

51% plus de la moitié des compromissions incluaient des logiciels malveillants.

81% des compromissions de piratage exploitaient des mots de passe volés et/ou faibles.

43% étaient des attaques de type ingénierie sociale.

14% Les erreurs représentaient des évènements déterminants dans 14 % des compromissions. De même pour le détournement de privilèges.

8% Les actions physiques étaient présentes dans 8 % des compromissions.

Qui sont les victimes ?

24% des compromissions touchaient des organismes financiers.

15% des compromissions impliquaient des organismes liés à la santé.

12% Les entités du secteur public représentaient la troisième victime de compromission la plus fréquente à 12 %.

15% Le secteur de la vente au détail et de l'hôtellerie formaient ensemble 15 % des compromissions.

Quelles autres caractéristiques ?

66% des logiciels malveillants étaient installés par le biais de pièces jointes dans les emails.

73% des compromissions avaient des motivation financières.

21% des compromissions étaient liées à l'espionnage.

27% des compromissions étaient découvertes par des tiers.

Etes-vous prêt à jouer avec votre avenir ?

Si vous n'avez pas été victime d'une compromission de données, c'est que soit vous avez été particulièrement bien préparé, soit vous avez eu beaucoup de chance. Êtes-vous particulièrement bien préparé ?

Personne ne pense qu'il sera la prochaine victime. Jusqu'à ce que cela arrive.

C'est probablement la faute d'Hollywood. Si l'on en croit les films, les cybercriminels opèrent depuis des entrepôts abandonnés mal éclairés, ciblent des conglomérats soigneusement sélectionnés et utilisent des choses comme des « vers » et des « clés » pour y accéder. Cette caricature a trompé nombre de personnes se croyant à tort en sécurité et pensant que les compromissions de données étaient des choses qui n'arrivent qu'aux autres.

La réalité est que les cybercriminels correspondent rarement à ce profil. Ils sont opportunistes ; ils se servent de techniques diverses comme le phishing pour exploiter des points faibles qu'ils pourront utiliser comme base pour lancer leur attaque. Leur intention est rarement de dominer le monde, mais plutôt d'extorquer de l'argent.

Qu'il s'agisse de plans de conception, de dossiers médicaux ou de détails de carte de paiement traditionnelle, quelqu'un, quelque part, sera prêt à s'en emparer. La plupart des cybercriminels n'attache aucune importance à la personne à laquelle ils volent les données.

Les entreprises pensent être préservées et connaître les bases de la sécurité.

Les gens continuent de tomber dans le piège du phishing, oui encore aujourd'hui. Cette année, le DBIR a déterminé qu'environ 1 utilisateur sur 14 se faisait piéger en suivant un lien ou en ouvrant une pièce jointe et un quart de ceux-ci se faisaient piéger plus d'une fois. Là où le phishing permettait de mettre un pied dans le système, le logiciel malicieux entrait alors en scène pour capturer et exfiltrer des données voire prendre le contrôle de systèmes.

Les gens n'utilisent toujours pas de mots de passe suffisamment complexes.

80 % des compromissions liées au piratage exploitaient des mots de passe volés et/ou faciles à trouver.

Voir pages 6-7 pour en savoir plus sur les neuf schémas d'attaque qui couvrent 88 % des compromissions étudiées dans notre rapport de 2017.

Les gens ont tendance à faire ce qu'ils ont toujours fait.

La plupart des entreprises continuent de s'appuyer sur des défenses dépassées. Il est tentant, en particulier si vous n'avez pas été la cible d'un incident majeur, de garder les mêmes défenses année après année. Mais ces défenses sont-elles en ligne avec les menaces auxquelles une entreprise comme la vôtre est réellement confrontée ?

Voir page 4-5 pour en savoir plus sur les menaces qui selon nous sont les plus utilisées dans votre secteur.

61%

des victimes de compromission de données dans le rapport de cette année sont des sociétés de moins de 1 000 employés.

95%

des attaques de phishing menant à une compromission étaient suivies par une installation de logiciel.

Construisez vos défenses judicieusement

Tandis que les pirates utilisent de nouvelles ruses et tactiques, leurs stratégies globales n'ont pratiquement pas changé. Comprendre ces ruses et tactiques est vital pour savoir comment défendre votre entreprise contre les cyberattaques.

88%

des compromissions s'inscrivent dans les neuf schémas que nous avions identifiés en 2014.

Comprendre ces schémas d'attaque permet aux professionnels de la sécurité d'obtenir des informations sur où et comment investir leurs ressources parfois limitées. Pour d'autres, ces schémas fournissent une façon rapide et facile d'évaluer où le danger est le plus susceptible d'apparaître. Ainsi, si vous lancez une nouvelle application ou si vous créez un nouveau process, vous pouvez mieux intégrer la sécurité dès le départ.

Lisez le Data Breach Digest 2017 pour comprendre comment ces schémas d'attaque se traduisent dans la vie réelle. Chacun des 16 scénarii du DBD correspond à l'un de ces schémas d'attaque.

Cyberespionnage

Attaques liées à des acteurs gouvernementaux et/ou motivées par l'espionnage.

Bienvenue dans ce jeu de patience

L'email malveillant est la méthode d'accès préférée du cyberespion. Mais ce n'est pas une méthode éclair. L'email initial est généralement suivi d'une tactique visant à ne pas se faire remarquer, ce qui donne au pirate le temps de collecter les données dont il a besoin.

Ce que vous pouvez faire

Misez tout sur sensibilisation à la sécurité et encouragez vos équipes à signaler les emails de phishing. Compliquez pour l'attaquant l'accès à d'autres dispositifs de réseau depuis un poste de travail compromis.

Dénis de service

Toute attaque visant à compromettre la disponibilité des réseaux et systèmes.

Être frappé là où ça fait mal

Les attaques par déni de service (DDoS) visent presque toujours (98 %) les grandes entreprises. Et tandis que certains malchanceux sont constamment attaqués, la plupart des attaques se terminent en quelques jours.

Ce que vous pouvez faire

Vérifiez que vous avez mis en place des services de mitigation DDoS pour déjouer toute attaque, que ces services sont régulièrement testés et qu'ils fonctionnent réellement.

Logiciel criminel

Tous les cas impliquant des logiciels malveillants et qui ne correspondent pas à un schéma plus spécifique.

Le rançongiciel est lucratif

Le DBIR de 2014 classait le rançongiciel comme la 22e forme la plus commune des logiciels malveillants. Cette année, il est monté en 5e position et forme le schéma le plus répandu de logiciel criminel. Pour le pirate, libérer des fichiers contre une rançon est un moyen rapide, peu risqué et qui se monnaye facilement, en particulier avec l'anonymat assuré par le Bitcoin.

Ce que vous pouvez faire

Faites attention aux documents MS Office avec macro-activés et soulignez l'importance des mises à jour logicielles à quiconque est prêt à vous écouter.

Mauvais usage par le personnel internes et des privilèges

Toute utilisation non autorisée ou malveillante de ressources organisationnelles.

L'ennemi est parmi nous

Dans 60 % des cas, le criminel qui se trouve dans l'entreprise s'échappe avec les données dans l'espoir de les convertir plus tard en argent. Mais parfois, il s'agit d'intrusion non sanctionnée (17 %), de transfert de données à un nouvel employeur ou pour lancer une société concurrente (15 %).

Ce que vous pouvez faire

Implémentez des limitations, le suivi des connexions et des usages et soyez vigilant quant aux transferts importants de données et à l'utilisation de périphériques USB.

Erreurs diverses

Les actions non intentionnelles qui ont compromis directement la sécurité des données d'entreprise.

Des erreurs commises

Elles peuvent paraître inoffensives, mais les données perdues par erreur peuvent aussi être préjudiciables. En particulier si, comme dans 76 % des cas, ce sont vos clients qui vous l'annoncent.

Ce que vous pouvez faire

Ayez et mettez en œuvre une procédure formelle de destruction de tout ce qui pourrait comporter des données sensibles. Et établissez une politique à quatre-yeux pour la publication d'informations.

Dispositif de lecture pirate de cartes de paiement

Tout incident impliquant le placement d'un dispositif de lecture pirate sur un lecteur de cartes de paiement.

Stations-service

Alors que les DAB continuent de représenter la cible principale des pirates, le nombre de terminaux aux stations-service utilisés pour récolter les informations de cartes de paiement a plus que triplé comparé au DBIR de l'an dernier. Ces attaques sont presque toujours découvertes par des tiers.

Ce que vous pouvez faire

Formez les employés à détecter les signes d'altération, surveillez les terminaux de paiement par vidéo surveillance et assurez-vous que les bandes d'enregistrement soient examinées régulièrement.

Intrusions sur point de vente

Attaques à distance des terminaux et contrôleurs de PDV.

Les fruits du PDV

Les environnements de point de vente (PDV) continuent de remplir les poches des pirates, avec près de 98 % de toutes les attaques enregistrées de PDV aboutissant à une compromission confirmée. La cible des attaques est passée des chaînes d'hôtel aux restaurants et petites entreprises.

Ce que vous pouvez faire

Demandez un audit des fournisseurs de PDV tiers et de leurs pratiques de sécurité, en mettant l'accent sur les accès à distance.

Vol et perte physiques

Tout incident où le patrimoine physique disparaît – délibérément ou accidentellement.

Les employés égarent leurs affaires

Des mesures telles que le chiffrement peuvent enrayer le vol et la perte de données, pour qu'il n'y ait pas compromission. Mais le chiffrement n'est pas toujours efficace ; la majorité des compromissions confirmées impliquaient la perte de documents imprimés.

Ce que vous pouvez faire

Chiffrez les données chaque fois que cela est possible et établissez une culture d'entreprise qui décourage l'impression des données sensibles.

Attaques d'application web

Tout incident pour lequel une application web a été utilisée comme mode d'attaque.

Ne devenez pas un intermédiaire

Tous les sites web ne détiennent pas les données des cartes de paiement, mais ils demandent encore souvent aux utilisateurs de se connecter en demandant leurs noms, adresses, etc. Le niveau de sécurité est souvent plus faible que sur les sites de commerce de détail, et ainsi les pirates utilisent ces données de connexion pour accéder facilement aux données personnelles et informations d'identification afin de les utiliser ailleurs.

Ce que vous pouvez faire

Encouragez les clients à utiliser des mots de passe différents et à utiliser une authentification à deux facteurs. Limitez la quantité d'informations sensibles conservées dans les applications web.

Tout le reste

Tout incident qui ne fait pas partie des neuf schémas.

Prenez garde aux imposteurs

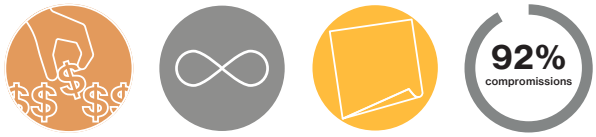
Ce peut être une catégorie « fourre-tout », mais cela ne signifie pas qu'ils ne sont pas intéressants ou que cela ne représente pas une tendance notable. Une tactique clé émergente est la compromission par email : lorsque « le PDG » ordonne un virement bancaire urgent associé à un scénario crédible.

Ce que vous pouvez faire

Répétez à vos équipes, spécialement dans la finance, que personne ne demande de paiement selon des procédés non autorisés. Demandez également au service informatique de marquer les emails externes d'un sceau reconnaissable.

Connaissez les menaces auxquelles vous êtes confronté

Hôtellerie

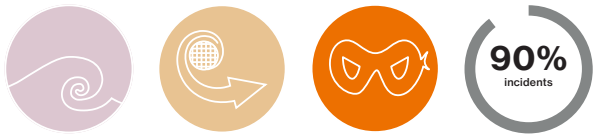


Education

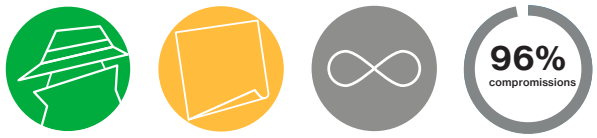
Services financiers

Secteur de la santé

Informations

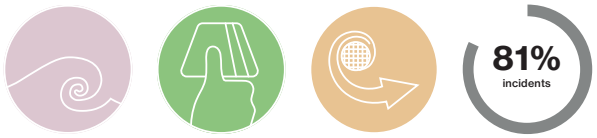


Manufacture



Secteur public

Vente de détail



Adaptez votre défense

Si vous vous destiniez pour une expédition en Arctique, vous abandonneriez probablement les shorts au profit de sous-vêtements thermoactifs. Il en va de même quand il s'agit de planifier ou de dépenser votre précieux budget. Les fiches ci-dessus vous aident à comprendre les tactiques utilisées contre d'autres sociétés de votre secteur. Savoir où se situent les plus grandes menaces, vous permet d'adapter vos défenses aux menaces.

Nul besoin d'être grand ou célèbre

La menace interne n'est pas nouvelle dans le secteur de la santé. Mais la menace ne vient pas seulement d'un accès rapide aux données de santé pour révéler le nom ou le sexe du nouveau-né d'une célébrité avant qu'il n'apparaisse dans la presse. Il s'agit souvent du vol et du clonage de l'identité de personnes ordinaires.

De même, les marques populaires ne sont pas les seules victimes des cyberattaques. Les start-ups sont ciblées pour leur technologie novatrice. Les entreprises mieux établies se font dérober leurs fichiers clients. D'autres sont identifiées comme cible facile, très utile comme point d'accès aux systèmes de leurs partenaires.

Soyez aussi informés que les escrocs !

Les cybercriminels ne se satisfont pas du statu quo. Si la valeur des données décline, ils élargissent la zone d'attaque et améliorent leurs tactiques. Aucun système n'est sûr à 100 % mais trop d'entreprises leur facilitent la tâche.

L'ingénierie sociale est un moyen courant d'établir un point d'entrée aux cybercriminels. Et les employés leur facilitent la tâche en utilisant des mots de passe faciles à trouver. Les utilisateurs, et même les départements SI, sont souvent coupables de laisser les mots de passe des systèmes par défaut, mots de passe facilement récupérable en ligne.

Autrement dit, beaucoup des compromissions que nous avons constatées auraient pu être évitées si les entreprises avaient mis en place des mesures de sécurité de base. Nos sept conseils ci-dessous couvrent les erreurs simples que nous constatons encore et encore.

Mais votre équipe SI devrait posséder une compréhension précise des menaces qui pèsent sur votre entreprise. Les cybercriminels utilisent toutes les informations possibles à leur propre profit. Faites-en autant. Le Data Breach Investigations Report (DBIR) 2017 est incontournable pour toute entreprise qui prend la cybersécurité au sérieux.

Récapitulatif

Soyez vigilant
Les fichiers de logs et les systèmes de gestion des changements permettent de vous avertir précocement d'une compromission.

Faites de vos employés la première ligne de défense
Formez les employés à reconnaitre les signaux alarmants.

Conservez les données avec le principe du « need to know ».
Seuls les employés qui ont besoin d'accéder aux systèmes dans le cadre de leur travail doivent y avoir accès.

Appliquez rapidement un correctif
Préventif à beaucoup d'attaques.

Chiffrez les données sensibles
Rendez vos données inutilisables si elles sont volées.

Utilisez l'authentification à deux facteurs
Ceci limitera les dommages pouvant être causés par des identifiants perdus ou volés.

N'oubliez pas la sécurité physique
Tous les vols de données ne se produisent pas en ligne.

En savoir plus

2017 DBIR

Téléchargez le rapport Data Breach Investigations Report (DBIR) 2017. Il s'agit de notre publication sur la sécurité la plus importante et l'une des sources d'information les plus respectées de l'industrie.

2017 DBD

Lire le Data Breach Digest relatant les enquêtes sur les cybercrimes les plus étonnants de Verizon. Apprenez les tactiques des pirates, les erreurs des victimes ainsi que la course pour limiter les dommages.

VerizonEnterprise.com/fr