



## S'informer pour se protéger

Pour plus de sécurité, adoptez les réflexes CASES !

### Ce à quoi les entreprises doivent veiller

Les attaques d'entreprises sont aujourd'hui le revers des activités numériques quotidiennes. Les analyses de ces attaques se lisent souvent comme un polar. À la différence que l'objectif premier des cybercriminels est généralement le vol de données. Bon nombre de ces délits peuvent toutefois être évités par des mesures simples et abordables.

Juin 2009 dans un hôtel luxembourgeois. Une conférence sur la sécurité est à l'ordre du jour. Des représentants de différents domaines de la sécurité de l'information sont présents, comme l'entreprise technologique VerizonBusiness, notamment active dans l'analyse de cyberattaques.

Cet après-midi-là, VerizonBusiness résume les résultats d'analyse de quatre-vingt-dix délits réussis dans des entreprises via Internet. La société passe en revue les causes des intrusions, les modus operandi des criminels, les moyens utilisés, les objectifs des malfaiteurs, le délai écoulé jusqu'à l'identification de l'intrusion ainsi que les mesures qui auraient pu éviter un accès non autorisé.

L'universalité des résultats de l'entreprise de sécurité est certainement discutable mais les entreprises peuvent toutefois en tirer quelques idées pour améliorer la protection de leur propre organisation.

### Que cachent les intrusions dans les entreprises ?

Selon VerizonBusiness, une large majorité des attaques des entreprises concernées a eu lieu de l'extérieur. Cela ne correspond certes pas aux résultats de ces dernières années où



de nombreuses attaques avaient lieu au sein de l'entreprise, mais cela pourrait dessiner une tendance et mérite d'être signalé.

Dans 67 % des cas, les agresseurs n'ont pas eu beaucoup de difficultés grâce à des failles internes. Le recours au piratage a également été constaté dans un grand nombre de délits. 38 % des criminels ont en outre utilisé des logiciels malveillants et, dans près d'un quart des cas, les pirates ont exploité les accès d'utilisateurs protégés par des droits particuliers.

Il est intéressant de constater que bon nombre d'entreprises ne correspondaient pas aux normes de sécurité des systèmes de paiement par carte. Par conséquent, dans 83 % des cas, aucune connaissance spécialisée n'était nécessaire pour réussir des attaques grâce aux points faibles des sociétés. Les pirates ont réussi à accéder aux données recherchées via des applications web.

Les criminels se sont aussi souvent aidés de mauvaises configurations et de négligences ou d'erreurs de programmation. L'escroquerie ou le Social Engineering (ingénierie sociale), c'est-à-dire l'abus de confiance de personnes, est une autre méthode qui a été utilisée, dans 5 cas par e-mail et dans 4 autres cas directement via une personne.

Certes, les attaques suite à l'absence de mise à jour de programmes ont été rares mais cinq cas ont néanmoins été recensés. Dans ces cas, des rustines logicielles étaient déjà disponibles depuis plus d'un an.

L'accès non autorisé à pratiquement toutes les données se fait via les serveurs ou les applications. Trois quarts des données consultées sans autorisation se trouvaient sur des serveurs de bases de données. Dans 67 % des cas, les entreprises ne savaient pas, par exemple, que les données étaient stockées sur la machine attaquée. Dans plus de la

moitié des cas, les entreprises n'avaient même pas connaissance de l'existence des accès correspondants avec « droits particuliers » que les pirates ont utilisés pour consulter les données.

Dans 98 % des cas, les accès non autorisés aux données ont ciblé des informations concernant les données des cartes de paiement de clients, notamment les codes PIN et les comptes correspondants. Les criminels se sont aussi particulièrement intéressés aux données permettant un vol d'identité, comme les noms, les numéros d'identification, etc.

Pour les piratages analysés, il faut signaler la généralisation de l'utilisation de logiciels malveillants spécialement créés ou adaptés pour l'entreprise visée. Cette forme d'attaque est responsable de la majorité des vols de données, ce qui ne signifie pas pour autant que ces intrusions n'auraient pas pu être évitées par des moyens et mesures simples. Au contraire, 87 % des attaques auraient échoué avec des contrôles simples à moyens.

## Du piratage à l'identification

Si certaines attaques n'ont demandé qu'une préparation de quelques minutes aux criminels, d'autres (26 %) ont nécessité plusieurs mois de préparation.

La constatation des intrusions prend toujours quelques semaines à plusieurs mois. Seuls 16 % des méfaits ont été découverts en quelques jours. Une fois une intrusion constatée, il fallait encore plusieurs jours et semaines pour l'endiguer. Dans 6 % des cas seulement, cette opération n'a pris que quelques heures. On n'entend pas par endiguement la suppression des points faibles, mais simplement la fermeture de l'accès.

La plupart des attaques n'ont pas été découvertes par l'entreprise concernée mais par des tiers, comme des partenaires commerciaux ou des prestataires financiers. Dans 53 % des cas, des tiers ont identifié le vol suite à des escroqueries auxquelles ils ont été attentifs. 24 % des piratages ont été remarqués par les entreprises ciblées parce que des employés les ont constatées par hasard ou que des réactions

inhabituelles du système ont attiré leur attention. Dans 6 % des cas seulement, l'entreprise concernée a découvert une attaque grâce à une surveillance active ou par l'analyse de fichiers journaux.

En plus de leurs défaillances à découvrir des attaques, beaucoup d'entreprises étaient mal équipées pour pouvoir y réagir. Seulement 28 % des sociétés concernées disposaient de plans, procédures et mesures correspondants pour contrer efficacement les délits.

## Pour éviter les attaques

Quelques règles de base permettent déjà de réduire le risque d'attaque, notamment la mise en place d'une politique de sécurité. Il faut veiller particulièrement ici à l'application intelligente et à la vérification de la politique et des procédures correspondantes. Il s'agit aussi d'analyser les accès des partenaires commerciaux. Il est recommandé de commencer par supprimer les failles de sécurité essentielles dans l'entreprise car les criminels recherchent toujours le chemin le plus court. Une fois la politique mise en

place, l'entreprise peut s'attaquer à d'autres points faibles.

En général, l'entreprise doit connaître le cycle des données. Celui-ci doit être consigné et être analysé à la lumière des aspects de sécurité. Cette mesure concerne aussi bien les données numériques et leurs supports que les données sur papier. Un « Traffic Light Protocol » aide à identifier, à classer et à protéger les données confidentielles. Cette méthode permet de répartir différentes zones de risque en zones de transactions, ce qui rendra la mise en place de mécanismes de contrôle appropriés plus compréhensible et facilitera les contrôles.

Une bonne part des attaques analysées auraient pu être identifiées si des procédures efficaces de surveillance des fichiers journaux avaient existé. Les entreprises devraient disposer de ce genre de procédures et contrôler régulièrement leur exécution. De plus, il faut éviter à tout prix les configurations standard et les preuves d'autorisation en commun. Les comptes d'utilisateur et les autorisations correspondantes doivent aussi être vérifiés régulièrement. Les

### Conseil de sécurité : guide pour améliorer la sécurité des entreprises

L'analyse de quatre-vingt-dix attaques d'entreprises réussies par des cybercriminels montre que 86 % des sociétés concernées ne satisfaisaient pas aux normes recommandées en matière de politique de sécurité. 70 % des entreprises négligeaient les mesures de sécurité nécessaires pour l'installation et la mise en service d'un pare-feu. Seules 11 % des entreprises attaquées répondaient aux normes recommandées pour les données enregistrées.

CASES, le portail luxembourgeois de la sécurité de l'information du Ministère de l'Économie et du Commerce extérieur, [www.cases.lu](http://www.cases.lu), met à la disposition des entreprises des informations détaillées sur l'application et le respect d'une politique de sécurité sous la rubrique Publications / Politique de Sécurité. Pour améliorer la protection des données, la rubrique Publications / Dossiers / Classification – Confidentialité – Intégrité – Disponibilité propose aussi un guide pour classer les données. En outre, les entreprises trouvent sous Publications / Dossiers / Référentiel de sécurité des applications web un guide comprenant une check-list pour éviter les failles de sécurité dans les applications web. Ce guide peut être intégré dans un cahier des charges. L'Open Web Application Security Project Community, [www.owasp.org](http://www.owasp.org), dispense aussi des informations précieuses sur la sécurité des applications web des entreprises.

### Définition : Traffic Light Protocol

Avant de partager des informations, il est important de savoir qui peut consulter les données au-delà du destinataire, et si lui-même peut les consulter. Le Traffic Light Protocol, en abrégé TLP, est une méthode destinée à identifier facilement les informations.

criminels aiment beaucoup exploiter ces faiblesses.

Les applications et codes écrits nécessitent des tests de sécurité approfondis. Une vérification standard de sécurité des applications web des entreprises concernées aurait déjà pu supprimer ces failles exploitées par les pirates. La même vigilance doit être appliquée aux procédures et à

leur respect dans le domaine de la mise à jour des systèmes et d'une politique claire en matière de droits d'accès et de licenciement de personnel.

Il arrive que des plans d'urgence et procédures soient nécessaires pour endiguer une attaque. Les entreprises devraient examiner préalablement les risques, points d'attaque potentiels et

mécanismes de réaction. Des plans de réaction devraient être disponibles. Les comportements suspects et anomalies possibles doivent être définis à l'avance pour que les collaborateurs puissent réagir plus rapidement. En général, chaque entreprise devrait miser sur les formations du personnel et les tests de sécurité.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

[www.cases.lu](http://www.cases.lu)