Vincibilis

LUTTER CONTRE L'ESPIONNAGE INDUSTRIEL

Votre réseau interne piraté !

INTRODUCTION

Trop d'entreprises focalisent leurs actions « sécurité » sur la protection de leur périmètre extérieur. Sensibilisés face aux menaces externes comme le piratage informatique, les décideurs oublient trop souvent que le danger peut venir de l'intérieur.

En effet, si les menaces extérieures existent bel et bien, les vulnérabilités exploitées par les pirates informatiques sont de la responsabilité de l'organisation qui subit l'attaque. Et dans la majeure partie des cas, les cibles réelles des attaquants se trouvent dans le périmètre de l'entreprise. Qui héberge encore des données sensibles hors de son organisation ?

Selon une étude réalisée par un grand cabinet conseil, ce sont près de 50 % des vols de données stratégiques qui sont réalisées depuis l'interne. Seulement ces chiffres ne sont pas tout à fait exacts. En effet, les entreprises souffrant d'un manque de sécurité interne souffrent aussi de ne pas avoir les moyens de tracer l'information permettant de savoir « qui a fait quoi » ! Et c'est bien là que le bas blesse.

Comment délors se protéger et comprendre ce que vos assaillants potentiels cherchent à savoir sur votre organisation ? Quels sont les failles les plus connues et les équipements les plus vulnérables ? C'est que nous vous proposons de découvrir dans ce document.

Vincibilis

Alexandre LIENARD
Security & Safety Advisor

TABLES DES MATIÈRES

- Qui sont vos assaillants potentiels ?
- Que cherchent-ils ?
- Les équipements « réseau » vulnérables
- Quelques exemples
- Comment se protéger efficacement ?
- Littérature et liens intéressants

Vincibilis

LES ASSAILLANTS POTENTIELS

UNE RUDE CONCURRENCE !

Avec la crise économique et la mondialisation, la concurrence est souvent devenue très agressive et géographiquement très étendue. Cela pose deux problèmes de taille.

D'abord car ces concurrents n'hésitent plus à recourrir à des moyens illégaux pour obtenir de l'information confidentielle. Ensuite parce que les législations dans certains pays sont différentes en termes de cybercriminalité et d'espionnage, dans d'autres pays, l'espionnage y est culturel.

Du chef d'entreprise qui demande à son petit neveu « pro de l'informatique » de craquer la boîte email de son principal concurrent, à la société « made in U.S.A. » accompagnée par les services de renseignement économique américains en passant par le concurrent chinois qui fait appel à un pirate informatique ou qui tente de manipuler les cadres en internes, les exemples sont légions.

Il ne faut jamais sous-estimer le départ d'un employé vers une autre entreprise. Si les cas d'espionnage commercial ne font pas la une de la presse chaque semaine, ce n'est pas parce qu'ils n'existent pas, c'est simplement parce que les sociétés ne portent pas plainte ! Histoire de préserver leur notoriété sans doute.

CE QU'ILS CHERCHENT

D'une manière générale, la concurrence est toujours intéressée par des données qui lui permettront de consolider une position concurrentielle ou d'acquérir un avantage concurrentiel. Autrement dit, toutes les données commerciales, les données de production, les données financières et les données « recherche et développement » intéressent ces assaillants d'un nouveau genre.

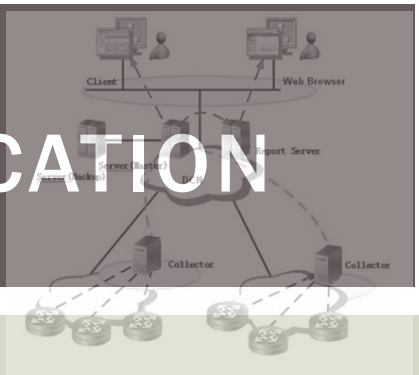
Seulement, pour parvenir à capturer cette information électroniquement (voir notre documentation sur le renseignement humain pour les aspects d'espionnage classique) les pirates cherchent avant tout de l'information dite « relais ». Les listes de mots de passe sont bien souvent leur objectif primaire car l'acquisition de tels documents évitent de devoir réaliser des opérations informatiques plus complexes pour s'infiltrer dans les réseaux. Et où se trouvent ces listes généralement ? Bien entendu sur le réseau interne.

Partout où l'information stratégique est stockée, il y a un danger potentiel. C'est pourquoi certains équipements sont à surveiller plus que d'autres; et ce ne sont pas toujours ceux que l'on croit qui sont les plus vulnérables.

Vincibilis

EQUIPEMENTS & VULNÉRABILITÉS

LES ÉQUIPEMENTS DE COMMUNICATION



Un réseau d'entreprise se compose proportionnellement à sa taille de divers équipements. L'on peut citer notamment les routeurs (filaires ou aériens), les pare feux, les serveurs de données, les ordinateurs fixes, les imprimantes…

Bien évidemment les pirates professionnels peuvent tenter de pénétrer sur le réseau depuis l'extérieur en prenant la main sur les routeurs (surtout aériens) ou sur les pare feux.

Si la menace vient de l'interne, par le biais d'un personnel externe connecté au réseau ou par le biais d'un employé malveillant ce sont les équipements plus classiques qui seront ciblés comme les ordinateurs, les serveurs ou encore les imprimantes (voir page suivante).

Même en limitant les droits d'administration et privilèges des « internes », certains outils de piratage et de captation de fichiers peuvent être utilisé à l'insu de l'organisation sans alerter l'attention (voir le cas précis Liberkey dans la suite du document).

Piratage d'imprimantes

Savez-vous que vos imprimantes sont vulnérables ?

La technologie ayant fortement évoluée durant ces derniers années, la plupart des imprimantes multifonctions sont intégrées au réseau informatique. Elles disposent d'un disque dur pour y stocker des données et sont souvent administrées depuis l'extérieur via l'Internet par les revendeurs.

Le même mot de passe pour tout le monde !

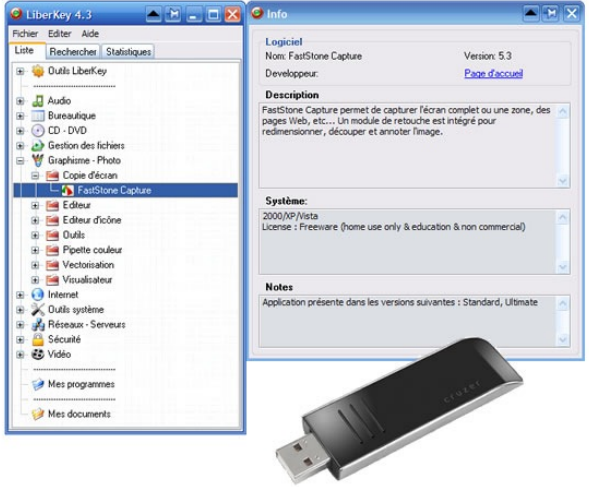
Lors d'une étude effectuée chez l'un de nos clients, nous avons contacté trois grands constructeurs par le biais de leurs installateurs. Nous avons pu constater que par défaut, les outils d'administration à distance sont configurés avec des mots de passe génériques. Ces mots de passe sont disponibles dans les manuels d'installation et sur l'Internet .

Le problème !

Les imprimantes sont parfois visibles depuis l'Internet mais surtout depuis le réseau interne. Avec quelques manipulations très faciles, n'importe qui peut accéder à la configuration de l'imprimante ciblée. Les conséquences peuvent avoir un impact considérable : possibilité de changer la configuration et ainsi rendre le réseau indisponible, captation de fichiers mais surtout possibilité de faire l'acquisition de fichiers scannés, imprimés et même photocopiés.

CAS PRÉCIS

Vincibilis



Clef USB intelligente !

Vincibilis

CAS PRÉCIS

Capturer l'information sans droit sur le réseau !

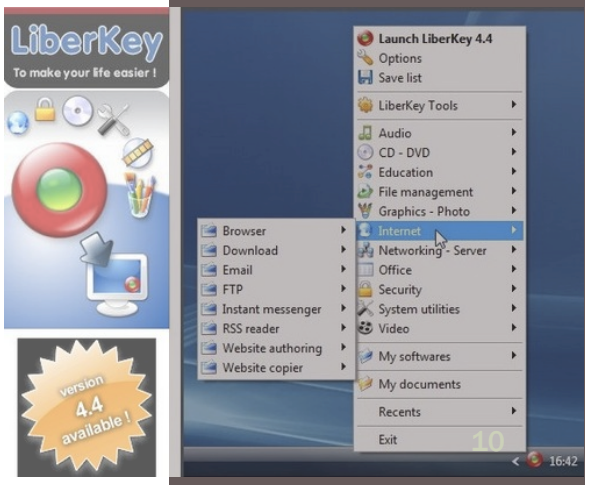
Certains logiciels permettent aujourd'hui en utilisant un clef USB de travailler en « stand alone » c'est-à-dire sans avoir besoin d'installer le logiciel sur l'ordinateur de travail. Ces logiciels « USB » sont de véritables outils de piratage car ils permettent par le biais de petits logiciels de « hacking » d'identifier les vulnérabilités du réseau.

Capture de mot de passe – vol de données stratégiques !

Ces logiciels sont très intrusifs et permettent ainsi de capturer des mots de passe sur le réseau. Utilisés par un expert, ce dernier pourra même aller chercher l'information stratégique en usurpant certains droits et en se faisant passer pour un autre utilisateur.

La seule et unique contre mesure.

Le seul moyen connu à ce jour pour éviter que ces outils soient utilisés est de bannir l'utilisation des clefs USB sur le réseau interne et sur tous les équipements qui le composent.



LES ÉQUIPEMENTS ITINÉRANTS

L'utilisation d'appareils itinérants se généralise. Ces équipements sont régulièrement connectés physiquement ou à distance au réseau interne des organisations, des entreprises.

S'ils représentent un gain en productivité, ils peuvent aussi parfois devenir de véritable failles, des passerelles de non sécurité et servir de relais à la pénétration extérieure ou encore contenir des informations stratégiques de l'organisation.

L'on parle souvent de vol d'ordinateurs portables, de Smartphones et de GPS. Ces vols ne sont pas tous de simples vols crapuleux dont le but est de revendre le matériel ! Parfois le vol est ciblé et le contenu des disques durs valent alors bien plus que la valeur du matériel dérobé.

Même encrypter les données n'est pas suffisant pour éviter les fuites d'informations stratégiques. En effet, certains logiciels offrent la possibilité de craquer certaines clefs d'encryptage. Tous les services officiels sont capables de décoder n'importe quel fichier protégé : c'est simplement une question de temps.

Un GPS peut « parler » !

Des outils de récupération de données pour les GPS existent sur le marché et sont disponibles à tous. Pour quelques 100 $ l'on peut se les procurer.
Certains assaillants commanditent le vol de GPS de cadres d'entreprises afin d'obtenir leurs itinéraires passés. Il est plus aisé et moins onéreux de dérober un GPS que de faire réaliser une filature d'un cadre durant un mois !

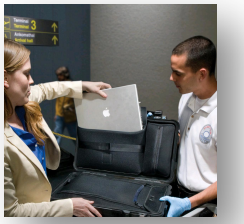
Les Smartphones

IPHONE, BLACKBERRY, HTC, LG… on ne compte plus les marques et le Smartphone est devenu un outil d'entreprise. Problème : ce dernier contient souvent des emails stratégiques, des codes d'accès et il est très facile d'en copier le contenu en moins ce cinq minutes !

Bornes WIFI chez les employés !

Le télétravail commence à se généraliser en Europe. Certains employés travaillent de chez eux et se connectent au réseau local grâce à leur connexion personnelle. Souvent mal protégées ces connexions s'avèrent être de véritables failles. Il est plus facile pour un assaillant de prendre la main sur un réseau privé que directement sur un réseau d'entreprise.

Des déplacements à l'étranger sous le signe de l'espionnage !



Certains pays, notamment en Asie, profite des contrôles aéroportuaires pour effectuer des copies intégrales de disques durs d'ordinateurs portables. Les hommes d'affaires étrangers sont particulièrement ciblés lors de ces opérations d'espionnage industriel commandités par les états.

CAS PRÉCIS

Vincibilis

QUELQUES EXEMPLES

Vincibilis

PERTE DE PARTS DE MARCHÉS

Situation :

Une entreprise suisse active dans le domaine de l'éclairage industriel nous contacte car elle soupçonne que la perte de parts de marchés et de clients depuis quatre mois est en relation avec le départ d'un cadre six mois auparavant.

Les faits :

Le cadre avait conservé des accès « webmail » à l'entreprise et continuait à accéder à des informations stratégiques. Il était parti avec la base de données et était parvenu à en faire des mises à jour régulières grâce à une complicité interne.

Intervention de notre expert:

Nous avons d'abord réaliser un audit de vulnérabilités et avons mis sous surveillance (traçabilité) les équipements de l'infrastructure réseau les plus sensibles. Après une opération « forensic » sur l'ordinateur portable de l'ancien cadre, nous avons retrouvé suffisamment de preuves informatiques pour que l'entreprise puisse porter plainte auprès des autorités compétentes; le vol d'informations avait commencé avant l'annonce de sa démission.

Mesures préventives qui auraient été nécessaires :

S'il est opportun de mener des interviews « sécurité » d'entrée lors d'un engagement de personnel, il est encore plus opportun de le faire lors d'un départ. La création d'une procédure d' « exit interview » aurait permis à l'entreprise de mesurer les risques du départ. Couper les accès dès le départ du cadre aurait été tout aussi nécessaire.

DES IMPRIMANTES TROP « PARLANTES »

Situation :

Une grande entreprise française active dans le domaine du service cherche à savoir comment certains documents stratégiques se retrouvent aux mains de la concurrence et comment les syndicats ont toujours une longueur d'avance lors de négociations sociales.

Les faits :

Un syndicaliste travaillant au département informatique vidangeait régulièrement les disques durs des copieurs. S'y trouvaient des notes stratégiques ainsi que des PV d'assemblées générales.

D'autre part, un concurrent avait mandaté un cabinet d'intelligence économique afin de collecter de l'information sensible. Ce cabinet avait fait appel à un expert informatique qui avait pris la main sur les copieurs multifonctions. Ce dernier envoyait chaque semaine un compte rendu exhaustif reprenant les numéros de fax de destination, les documents faxés ainsi que les fichiers imprimés.

Intervention de nos experts:

Après un audit du réseau, il s'est avéré que les imprimantes représentaient une faille importante. Connectées vers l'extérieur (Internet), le nom d'utilisateur était « Admin » et le mot de passe … « admin » !

Mesures préventives qui auraient été nécessaires :

Le simple fait de modifier les paramètres « usines » des copieurs aurait éviter les connexions à distance facilitées par l'absence de mot de passe spécifique.

DES BOÎTES EMAILS PILLÉES

Situation :

Une entreprise française active dans le secteur du voyages et du tourisme se plaint de pertes d'emails contenant notamment des confirmations de commandes. Cette entreprise possède cinquante agences dans toute la France.

Les faits :

Un concurrent malveillant a utilisé les services d'un étudiant en informatique pour découvrir les mots de passe des boîtes emails des cinquante agences de voyages. L'étudiant « chanceux » a découvert la liste complète au format « word » des identifiants de connexions de toutes les agences !

Intervention de nos experts:

Notre équipe était soit face à vol de documents papiers soit face à un piratage informatique. Après avoir réalisé des investigations informatiques profondes, il est apparu qu'un des employés administratifs du siège téléchargeait sur des réseaux « peer to peer » de la musique en masse. Ce dernier avait fait une erreur de configuration et avait partagé la totalité de son disque dur avait tous les utilisateurs du logiciel « peer to peer » Emule ! L'étudiant-assaillant n'avait eu qu'à taper dans le moteur de recherche du logiciel le nom de l'entreprise.

Mesures préventives qui auraient été nécessaires :

L'entreprise aurait dû dès l'annonce du départ être plus vigilante et restreindre les accès du cadre; ces derniers auraient dû être coupés dès le départ effectif.

VERS UNE PROTECTION EFFICACE

Vincibilis

L'HUMAIN : LE MAILLON FAIBLE

Pour bénéficier d'une sécurité optimale, il faut avant tout de sécuriser le maillon le plus faible. Dans la chaîne de l'information, le maillon faible est souvent le facteur humain. D'abord parce que l'humain peut commettre des erreurs mais surtout parce qu'il peut effectuer des actes malveillants.

Or la meilleure manière d'encadrer l'humain et de diminuer les risques de pertes de données confidentielles réside souvent dans la rédaction de procédures de sécurité adaptées au contexte de l'organisation, de l'entreprise.

Bien sûr la rédaction de procédures ne suffit pas, il faut aussi en faire la promotion et décliner les procédures en tâches et en recommandations d'action. La réussite d'un projet de sécurisation de l'entreprise passe par la sensibilisation de la totalité des acteurs et par la création d'un organe de gestion des incidents liés à la sécurité de l'information.

Un système d'information sécurisé à 100 % est une utopie. Croire que l'organisation n'est pas une cible potentielle c'est se comporter de manière désinvolte et totalement irréfléchie.

Politique Générale Sécurité

Directives de sécurité

Procédures

Tactiques

Exemples :

- ✓ Gestion des mots de passe
- ✓ Utilisation des emails
- ✓ Déplacement à l'étranger
- ✓ Gestion des accès
- ✓ Sécurité physique
- ✓ Classification
- ✓ Evaluation des risques
- ✓ Evaluation des partenaires IT
- ✓ ...

Analyse des risques & Vulnérabilités

1	Panorama des gravités de scénarios		Disponibilité					Intégrité					Confidentialité				
2	**Actifs de type Données et informations**		Gr. 1	Gr. 2	Gr. 3	Gr. 4		Gr. 1	Gr. 2	Gr. 3	Gr. 4		Gr. 1	Gr. 2	Gr. 3	Gr. 4	
3	***Données et informations***																
4	D01	Fichiers de données ou bases de données applicatives	0	0	22	18	>	0	0	3	13	>	0	0	7	13	>
5	D02	Fichiers bureautiques partagés	0	0	23	0	>	0	0	2	7	>	0	0	8	10	>
6	D03	Fichiers bureautiques personnels (gérés dans environnement personnel)	0	0	26	0	>	0	0	7	0	>	0	0	17	0	>
7	D04	Informations écrites ou imprimées détenues par les utilisateurs, archives personnelles	10	0	0	0	>						12	0	0	0	>
8	D05	Listings ou états imprimés des applications informatiques											0	0	6	1	>
9	D06	Données échangées, écrans applicatifs, données individuellement sensibles	0	0	6	0	>	0	0	1	13	>	0	0	1	13	>
10	D07	Courrier électronique	0	0	4	5	>	0	0	0	3	>	0	0	0	4	>
11	D08	Courrier postal et télécopies	0	0	10	4	>	0	0	0	1	>	0	0	7	0	>
12	D09	Archives patrimoniales ou documentaires	0	10	0	0	>						0	4	0	0	>
13	D10	Archives informatiques	0	18	0	0	>	0	0	3	2	>	0	0	3	0	>
14	D11	Données et informations publiées sur des sites publics ou internes	0	0	12	11	>	0	0	0	9	>					
15																	
16	**Actifs de type Services**																
17	***Services généraux communs***																
18	G01	Environnement de travail des utilisateurs	0	4	0	0	>										
19	G02	Services de télécommunication (voix, télécopies, visioconférence, etc.)	0	0	14	4	>	0	0	0	6	>					
20																	
21	***Services informatiques et télécom***																
22	R01	Service du réseau étendu	0	0	18	9	>	0	0	0	5	>					
23	R02	Service du réseau local	0	0	18	9	>	0	0	0	5	>					
24	S01	Services applicatifs	0	0	64	0	>	0	0	18	0	>	0	0	16	0	>
25	S02	Services bureautiques communs (serveurs de données, gestionnaires de documents, imprimantes partagées, etc.)	0	0	61	0	>	0	0	9	0	>					
26	S03	Equipements mis à la disposition des utilisateurs (PC, imprimantes locales, périphériques, interfaces spécifiques, etc.)	0	0	12	0	>										
27	S04	Services systèmes communs : messagerie, archivage, impression, édition, etc.	0	62	0	0	>	0	9	0	0	>					
28	S05	Services de publication d'informations sur un site web interne ou public	0	0	62	0	>	0	0	18	0	>					
29																	
30	**Actifs de type Processus de management**		Efficience														
31	***Non conformité à la loi ou à la réglementation***																
32	C01	Conformité à la loi ou aux réglementations relatives à la protection des renseignements personnels	0	0	4	0	>										
33	C02	Conformité à la loi ou aux réglementations relatives à la communication financière	0	0	3	1	>										
34	C03	Conformité à la loi ou aux réglementations relatives à la vérification de la comptabilité informatisée	0	0	4	0	>										
35	C04	Conformité à la loi ou aux réglementations relatives à la propriété intellectuelle	0	4	0	0	>										
36	C05	Conformité à la loi relative à la protection des systèmes informatisés	0	0	3	1	>										
37	C06	Conformité aux réglementations relatives à la sécurité des personnes et à la protection de l'environnement	0	0	3	1	>										

PLAN D'ACTIONS SECURISATION

ORGANISATION

Vincibilis

Vincibilis

info@vincibilis.org

+32 491 322 870

http://www.vincibilis.org
Adresse postale sur demande

Le réseau Vincibilis

Notre réseau est composé de professionnels de la sécurité des systèmes d'information ainsi que d'experts en gestion des risques.

Nos experts sont issus des milieux publics (administrations, ministères, forces de l'ordre) et privés et sont localisés en Europe et en Amérique du Nord.

Bien que les métiers de la sécurité de l'information et de la gestion des risques soient souvent considérés comme des domaines "techniques", notre approche est orientée sur les risques que courent les entreprises et organisations (espionnage industriel, contrefaçon, vol d'informations sensibles, perte de notoriété...)

Nous traitons de cette manière tout le "scope » de la cybercriminalité en mettant notre expertise au service de nos clients.

CONTACT