

Bulletin n° 3 / 2010

Sommaire

- Nouvelle nomination au Comité scientifique de l'ANSSAIF
- Table ronde sur les réseaux sociaux au Security Summit de Milan
- « Internet Crime Report 2009 » : synthèse
- Les chevaux de Troie représentent 61 % des logiciels malveillants
- La sécurité aujourd'hui : ce qui change en période de crise
- À noter sur votre agenda

Nouvelle nomination au Comité scientifique de l'ANSSAIF

À notre plus grande satisfaction, le **Dr Domenico Vulpiani** a accepté sa nomination au Comité scientifique de l'ANSSAIF.

Comme chacun sait, M. Vulpiani est Dirigente generale de la police nationale italienne et Conseiller ministériel à la Direction centrale de la police de la route, des chemins de fer, des communications et des départements spéciaux.

Notre association va ainsi pouvoir bénéficier de ses conseils et de sa longue et vaste expérience dans le domaine de la sécurité.

Table ronde sur les réseaux sociaux au Security Summit de Milan

L'édition milanaise du Security Summit – qui est sans doute l'événement majeur de la Péninsule en matière de sécurité informatique – s'est déroulée du 16 au 18 mars.

À l'occasion de cette manifestation, l'ANSSAIF a organisé avec la section Latium de l'AIDP (Associazione Italiana per la Direzione del Personale – Association italienne de gestion des ressources humaines) une table ronde intitulée « Uso degli strumenti di Social Networking in banca: opportunità e rischi », soit « Les outils de réseaux sociaux dans la pratique bancaire : potentiel et risques » (www.securitysummit.it/eventi/view/55).

Les réseaux sociaux étant indéniablement un sujet d'actualité, cette table ronde avait pour objectif d'explorer à la fois les possibilités ouvertes par ces nouvelles technologies et les risques associés.

Conformément aux recommandations émises à Sienne par son Comité scientifique lors du dernier congrès annuel, l'ANSSAIF a privilégié pour l'examen de ce sujet une étude basée sur des interviews de citoyens.

Le président de l'ANSSAIF, Anthony Cecil Wright, a présenté les premiers résultats de l'enquête – qui s'est révélée plus délicate que prévu du fait de la méconnaissance du phénomène dans la population.

Plus de 500 personnes résidant dans huit villes d'Italie ont répondu à l'ensemble du questionnaire. Les interviews ont été menées par téléphone sous forme non structurée, et il a fallu plus de 3 mois pour les saisir et les mettre en base de données.

Les premières conclusions dévoilées à Milan résultaient du traitement manuel de données issues des 450 premiers questionnaires saisis (cet exposé ainsi que le questionnaire sont disponibles sur le site Internet du CLUSIT).

Nous pouvons citer ici quelques-unes des constatations semblant se dégager des réponses des participants :

- En Italie, des outils comme Facebook ne sont pas utilisés comme dans d'autres pays tels que les États-Unis et le Canada (ils servent par exemple à l'échange d'informations et de photographies entre proches – avec les amis, les petits-enfants, les grands-parents, etc.).
- Seul un pourcentage négligeable d'utilisateurs ont quitté un réseau social suite à de mauvaises expériences.
- Une bonne partie des personnes n'avaient pas conscience des possibilités de fraude ni des fréquents détournements effectivement commis (comme les vols d'identité) ; même une fois informées, la majorité ont déclaré que cela ne les ferait pas changer de comportement.
- Un pourcentage important se connecte à un réseau social plus de quatre heures par jour.
- Ceux qui utilisent des réseaux sociaux de façon intensive et depuis longtemps sont désormais à la recherche de sites spécialisés adaptés à l'usage qu'ils en ont.

La présentation des premiers enseignements de l'enquête, dont les résultats définitifs seront présentés le 9 juin lors du Security Summit de Rome, ont servi de base de discussion aux intervenants invités, qui, compte tenu de l'ampleur du sujet, étaient issus de différents horizons : l'ensemble du système bancaire (Banque d'Italie, ABILAB, SIA-SSB et MPS), les entreprises (AIDP, Federmanager et Telespazio), l'enseignement (Università Roma Tre) et la criminologie.

Le président de l'ANSSAIF et Mario Salvatori, directeur du mensuel *Azienda Banca*, se sont relayés en tant qu'animateurs.

Tous les intervenants ont présenté des données instructives sur l'utilisation des réseaux sociaux dans leurs domaines respectifs, ce qui montre bien toute l'attention dont fait l'objet le phénomène.

Par ailleurs, même s'il a été fait état d'expériences intéressantes dans le domaine du marketing ou des relations internes, la prudence semble prévaloir de façon généralisée.

En premier lieu, si les avantages que peut apporter ce type de technologies – notamment en termes de diffusion et de partage des connaissances – sont bien identifiés, la difficulté de les quantifier pour justifier des investissements est également patente.

En second lieu, les acteurs sont bien conscients de la spécificité de ces outils capables de s'ajuster aux besoins des utilisateurs par rapport à l'informatique traditionnelle, mais ils savent aussi que leur extraordinaire malléabilité ne va pas sans poser des problèmes en ce qui concerne notre capacité de les contrôler et surtout de maîtriser les risques associés.

Marco Recchia

Un compte rendu de la Table ronde sera publié prochainement, et certaines interventions sont d'ores et déjà disponibles sur le site du CLUSIT.

Les résultats de l'enquête sur les entreprises réalisée par l'AIDP seront également présentés le 9 juin et commentés par une psychologue ainsi que par le Comité scientifique.

« Internet Crime Report 2009 » : synthèse

L'Internet Crime Complaint Center (IC3) est issu d'un partenariat entre le National White Collar Crime Center (un observatoire de la criminalité « en col blanc ») et le FBI.

Depuis l'an 2000, l'IC3 établit les statistiques des signalements effectués sur son site www.ic3.gov. Une grande partie (environ la moitié) n'ont pas de suites, mais tous les autres sont pris en charge par les autorités locales ou fédérales.

En **2009, l'IC3 a reçu 336 655 signalements** de fraudes et d'escroqueries portant sur des achats en ligne, des règlements, des vols d'identité, etc., pour **un montant total de 559,7 millions de dollars**.

Voici le résumé des données recueillies :

- Classification des fraudes en fonction du **nombre de signalements** :

- articles non livrés ou paiements non reçus : 19,9 % ;
 - vol d'identité : 14,1 % ;
 - fraudes à la carte de crédit : 10,4 % ;
 - fraudes sur achats aux enchères : 10,3 % ;
 - informatiques (destruction, dommages divers, vandalisme) : 7,9 %.
- **Montant moyen du préjudice subi** selon le type de fraude :
 - placements : 3200 \$;
 - paiements indus : 2500 \$;
 - paiements à l'avance : 1500 \$.
 - Les victimes sont majoritairement des hommes et se situent principalement dans la tranche d'âge 30-50 ans ; les pertes enregistrées par les hommes sont plus importantes que celles des femmes (ratio de 1,5 pour 1).

Les chevaux de Troie représentent 61 % des logiciels malveillants

C'est le pourcentage indiqué dans le rapport que vient de publier Panda Labs pour le 1^{er} trimestre 2010, tandis que la part des virus est évaluée à 17 %. Les fameux « chevaux de Troie bancaires » demeurent majoritaires – ce qui indique qu'il y a toujours pléthore de proies potentielles prêtes à tomber dans le piège !

Selon ce rapport, le pays le plus touché est l'Espagne, avec 35 % de PC infectés.

Pour plus de détails, nous vous invitons à consulter la page suivante :

<http://www.networkworld.com/news/2010/033110-concern-over-surge-in-banking.html?hpg1=bn>

La sécurité aujourd'hui : ce qui change en période de crise

Qui sait combien nous sommes, en cette période de vaches maigres, à nous demander comment protéger notre entreprise avec des budgets limités par rapport aux projets envisagés ?

Et combien d'entreprises ont réactualisé leurs scénarios de risques en examinant toutes les possibilités ? Et notamment, outre le vol d'informations confidentielles ou stratégiques, les actes de sabotage. Tout cela, aussi et surtout à travers l'informatique.

Il convient peut-être de prendre le temps de préciser les nouveaux scénarios.

La baisse généralisée de la demande, combinée au recul des investissements, crée des conditions difficiles pour les entreprises (toute la filière est affectée), et l'on peut donc s'attendre à une accélération et à une exacerbation de la concurrence. Je ne crois pas qu'on ait jamais eu à déplorer en Italie le développement d'une concurrence malhonnête où tous les coups sont permis. Rien de plus en tout cas que la sollicitation d'appuis politiques ou, autrefois, le paiement de pots-de-vin (si l'on exclut les menaces à caractère mafieux, qui appellent des considérations spécifiques qui n'ont pas leur place ici).

Dans d'autres pays, on a déjà enregistré par le passé des cas de vol d'informations, de diffusion de fausses informations ou de sabotages visant, pour ne citer que quelques exemples, à corrompre des personnes clés ou à les forcer à la démission, ou à obtenir la connivence de fournisseurs pour retarder la livraison d'un produit vital.

On observe en Italie ce qui pourrait bien être les premiers signes d'un phénomène d'imitation de ces comportements contraires à toute éthique, à l'instar de ce qui a pu se passer à l'étranger, sous le prétexte qu'après tout, en temps de crise, il faut employer les grands moyens (« À la guerre, comme la guerre », comme disait mon grand-père !). Dans certains secteurs, ce type de concurrence déloyale n'est d'ailleurs pas nouveau (je pense notamment aux deux offensives dont Ferrari a été victime).

Y a-t-il des signes annonciateurs ? Avec les informations disponibles et... un peu d'imagination, on peut émettre des hypothèses sur la nature et l'enchaînement des attaques contre des concurrents :

- propagation de rumeurs de difficultés économiques de l'entreprise cible et de la proche possibilité d'une vague de licenciements, de façon à indisposer le personnel et à ralentir l'activité ; les rumeurs seront également diffusées auprès des clients de l'entreprise, de manière à ébranler la relation de confiance et à compromettre de futures commandes ;
- en plus de ces manœuvres, on pourra prendre contact avec un employé facile à « persuader » (d'autant qu'il craint désormais pour son emploi) pour obtenir des informations stratégiques – et, tant qu'on y est, des documents confidentiels (projet de cahier des charges, réponse à un appel d'offres, etc.) ;
- l'argent achète tout – et permet de sponsoriser des pirates pour qu'ils sabotent le site de l'entreprise à un moment bien choisi (par exemple, lors d'une démonstration sur un salon ou chez un prospect), ou lancent une « bombe logique à retardement » ; comme on l'a vu récemment en Espagne, une autre pratique consiste à acheter des chevaux de Troie sur

Internet et à les propager pour ouvrir une brèche dans les systèmes de l'entreprise ;

- autre possibilité : corrompre un membre de l'entreprise qui opérera de l'intérieur (grassement rétribué, l'informaticien félon aura démissionné à temps de sorte qu'on ne puisse remonter jusqu'à lui lors du sinistre).

La question se pose donc en ces termes : Que pouvons nous faire ? Que peut un budget sécurité limité face à de telles menaces ?

La thèse que je voudrais présenter ici dans ses grandes lignes, c'est que, d'abord et avant tout, **une bonne analyse des risques peut permettre à la direction de l'entreprise de concentrer ses ressources sur les quelques menaces les plus sérieuses.** Et pour cela, une étroite collaboration entre la Sécurité et la Gestion des risques est indispensable.

Secundo : **il est possible de mettre en œuvre des solutions de réduction des risques très efficaces pour un coût restreint.**

En fait, dans bien des cas, les contre-mesures ne nécessitent pas d'investissements conséquents, mais représentent seulement un coût interne (plus, le cas échéant, l'aide d'un consultant extérieur).

Et pour ne pas me contenter de jouer les Cassandre, je me permettrai quelques recommandations concrètes.

L'entreprise doit agir en parallèle sur plusieurs fronts – par exemple :

- veiller à préserver un bon niveau de « confiance » dans l'entreprise chez les employés ;
- identifier et développer les contre-mesures les plus stratégiques ;
- former le personnel à la sécurité, en proposant des motivations pour la certification aux normes, notamment dans le domaine de la continuité opérationnelle, car il est vital que chacun ait tous les éléments en main pour fournir à la direction l'éventail approprié d'options de réduction des risques (et pour cela, il ne suffit pas de maîtriser le cycle d'élaboration des plans de continuité et la conduite des analyses d'impact ; il faut aussi une collaboration efficace avec les unités opérationnelles, et il faut savoir exploiter l'expérience et les méthodologies de gestion des risques) ;
- diffuser et actualiser régulièrement les politiques de sécurité ;

- s'assurer régulièrement que les employés ont compris le fondement des règles de sécurité, leurs responsabilités et leur rôle personnel ;
- prendre des mesures drastiques en cas d'infraction aux règles.

Voyons à présent quelques-unes des actions propres à contribuer au **maintien d'un climat sain et constructif au sein de l'entreprise** :

- être très attentif aux « bruits de couloir » ; encourager certains collaborateurs à s'exprimer librement, et évaluer l'opportunité d'inciter les unités à ouvrir un site de réseau social pour partager les expériences, présenter des suggestions pour l'amélioration de la qualité des produits ou la rationalisation des processus opérationnels, et aussi recueillir des conseils pour améliorer les conditions de travail de certains collaborateurs. N'oublions pas que les jeunes ressentent fortement le besoin de disposer de temps libre pour leurs passions personnelles, leurs hobbies, etc. ;
- trouver des occasions de réunir tous les employés avec leurs compagnons ; certaines entreprises organisent des soirées au théâtre, ou même à l'Opéra (un lieu généralement peu fréquenté par les jeunes générations) ; ces rencontres sont source de cohésion et contribuent à entretenir l'« esprit maison » ;
- la convention annuelle – à condition d'être bien préparée (attention aux multiples maladresses à éviter et à leurs conséquences si difficiles à rattraper !) – est aussi un moment important pour ranimer l'enthousiasme et souder les troupes ; cet événement ne saurait toutefois suffire, d'autant qu'il est généralement mal perçu chez les jeunes générations.

Rappelons maintenant quelques **contre-mesures** permettant de limiter les risques de dégâts :

- veiller au maintien des données de l'entreprise sur des serveurs, dans des dossiers et dans des bases de données dûment protégés, en empêchant leur stockage sur les PC des utilisateurs (cette précaution est d'ailleurs également bénéfique en termes de productivité et de réduction des coûts de maintenance) ;
- interdire l'utilisation par les individus de clés USB, de disques durs externes, de DVD, etc. ; la gestion des besoins éventuels peut être confiée à un service chargé de contrôler l'autorisation de faire une copie sur support amovible ; il sera interdit de copier des données personnelles et, à fortiori, des

informations sensibles sur ce type de support à moins d'une autorisation officielle complétée par l'adoption préventive de mesures de protection adaptées et testées ;

- veiller à ce que les activités des administrateurs système et des utilisateurs qui manipulent des informations personnelles ou sensibles bénéficient d'une protection adéquate contre d'éventuels délinquants : par exemple, en mettant en place un système d'authentification « fort » et une surveillance des opérations par des logiciels adaptés permettant de déceler les anomalies éventuelles (ainsi, une mesure désormais classique consiste à signaler toute tentative d'accès de la part d'un employé en congés ou en arrêt de maladie) ;
- exercer un contrôle rigoureux sur les modifications des programmes système et des applications ;
- contrôler les modifications des logiciels effectuées en situation d'urgence (c'est-à-dire quand des conditions pressantes ont imposé le court-circuitage des étapes de contrôle et des demandes d'autorisation prévues dans la procédure de gestion des modifications) ;
- pour les systèmes distribués, éliminer les tâches répétitives effectuées manuellement par un opérateur en mettant en œuvre des systèmes d'exécution automatique (comme en environnement grand système) dûment protégés contre les accès non autorisés ;
- être vigilant par rapport aux opérations d'impressions (par exemple, réagir au changement d'adresse IP provisoire d'une imprimante) ainsi qu'à la circulation et à la copie de documents confidentiels.

Avant de conclure, et pour susciter le débat, je poserai **une question** :

Si une entreprise financée par un établissement financier n'adoptait pas les mesures de sécurité appropriées, elle risquerait la faillite ou, dans le meilleur des cas, de graves difficultés financières – et l'établissement financier en pâtirait également. Dans ces conditions, n'y a-t-il pas lieu, lors de **l'étude d'un dossier de prêt**, de demander des justificatifs établissant la **certification du demandeur par rapport aux standards de sécurité internationaux** et d'intégrer cet aspect dans les critères de décision ?

(acw)

anthony.wright@anssaif.it

À noter sur votre agenda

L'AIPSA, BCManager et l'ANSSAIF sont en train d'organiser un grand congrès sur l'état de l'art en matière de **protection des infrastructures critiques** qui aura lieu à **Rome le 8 juin dans les locaux de Monte dei Paschi di Siena**.

Et comme vous le savez déjà, c'est le **9 juin, à Rome**, dans le cadre du Security Summit, que seront présentés les résultats des enquêtes de l'AIDP (section Latium) et de l'ANSSAIF sur l'utilisation des outils de réseaux sociaux.