NetObservatory : un observatoire national de la sécurité Internet

Autor(en): **Joye, Philippe**

Objekttyp: **Article**

Zeitschrift: **Bulletin.ch : Fachzeitschrift und Verbandsinformationen von Electrosuisse, VSE = revue spécialisée et informations des associations Electrosuisse, AES**

Band (Jahr): **102 (2011)**

Heft (10)

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-856862

NetObservatory : un observatoire national de la sécurité Internet

Deux mots d'ordre : observation et prévention

Sites web et messageries électroniques font partie des éléments incontournables de la productivité des entreprises. Cependant, chaque connexion vers l'Internet représente une porte d'accès, dont la somme correspond, en termes de sécurité, à la surface d'attaque qu'offre une infrastructure à ses agresseurs potentiels. Or, avec la variété du matériel et des logiciels utilisés, il est devenu difficile pour les hébergeurs et les fournisseurs d'accès d'offrir des mesures de sécurité ciblées.

Philippe Joye

Les activités des entreprises et autres organisations installées en Suisse dépendent de plus en plus fortement de la qualité et de la fiabilité des connexions Internet mises à disposition dans notre pays. En effet, nombre d'activités et de services utilisent intensivement et systématiquement le « réseau des réseaux » pour communiquer, informer, acheter ou vendre.

Mais qu'en est-il de la sécurité Internet en Suisse ? Cet article met en évidence les vulnérabilités constatées par NetObservatory, un projet dédié à l'évaluation de la sécurité des infrastructures et à la prévention des risques.

Contexte

L'actualité des derniers mois met en évidence la dépendance des sociétés dites modernes aux technologies de l'information. Les nouvelles concernant les attaques, infections virales ou autres «défacements» se multiplient à un rythme soutenu et font régulièrement la première page des médias. Si les risques que courent les entreprises et organismes présents sur le Web dépendent du nombre et de la taille des services et produits mis à disposition du public sur l'Internet, ils peuvent être limités en renforçant certaines mesures simples de précaution et de surveillance. Dans ce contexte, une mise à jour régulière des serveurs et logiciels suivie d'une action de révision des configurations rendent la majorité des tentatives d'agression inopérantes.

Conséquences et responsabilités lors d'une attaque

Certes, les grandes entreprises disposent de moyens adéquats pour minimiser les risques inhérents à leur présence sur le réseau universel Internet, ce n'est toutefois pas le cas de la grande majorité des PME qui constituent la plus grande partie du tissu économique suisse. Chaque présence et service visible sur l'Internet engendre un risque pour la structure et la stabilité des activités de la place économique nationale dans son ensemble.

Les conséquences résultant d'une attaque sont toujours difficiles à évaluer. Ce n'est qu'une fois l'attaque survenue que l'entreprise est en mesure de rassembler toutes les pièces. Elle tente alors de mesurer puis de réparer les dégâts.

Les intentions des agresseurs peuvent considérablement varier, allant du simple exploit gratuit (vandalisme) au vol pur et simple d'informations vitales pouvant conduire une entreprise jusqu'à la faillite en l'exposant à des poursuites. En effet, les responsabilités sont toujours très difficiles à établir. Si, par exemple, un code vicieux est injecté sur un site mal protégé et très fréquenté, un maximum d'utilisateurs sera contaminé et l'image de l'entreprise en question en sortira ternie, notamment parce qu'elle n'aura pas su assurer un niveau de sécurité suffisant.

Réduire les risques

Deux approches permettent de diminuer l'impact d'une sécurité informatique déficiente. La première concerne l'information à propos des risques et des tendances relevées sur les agressions en cours. Cette information doit être distribuée et traitée au plus vite. Si de nouvelles failles ou de nouvelles attaques apparaissent, les responsables des infrastructures doivent pouvoir mettre ces dernières à jour dans les délais les plus courts possible.

La deuxième approche concerne la formation qui doit être dispensée de manière à connaître et reconnaître les outils et les méthodes utilisées par les agresseurs. Une analyse périodique, systématique et approfondie des infrastructures permet à une personne initiée aux principes de prévention et d'observation de quantifier le niveau de sécurité d'une installation. C'est avec l'objectif de fournir des services de ce type que l'observatoire national de la sécurité NetObservatory a été conçu.

L'information : une arme à double tranchant

L'amélioration de la sécurité passe par l'échange d'informations. Savoir reconnaître les failles et les vulnérabilités d'un système avant qu'il ne soit la cible d'une agression, procure non seulement un

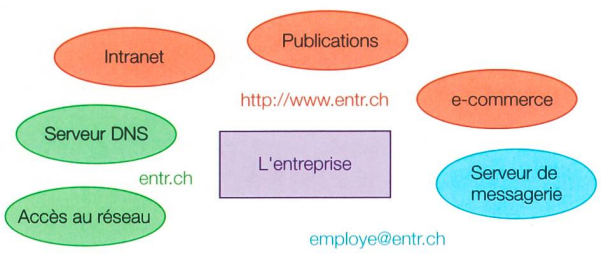


Figure 1 Les diverses utilisations d'un nom de domaine.

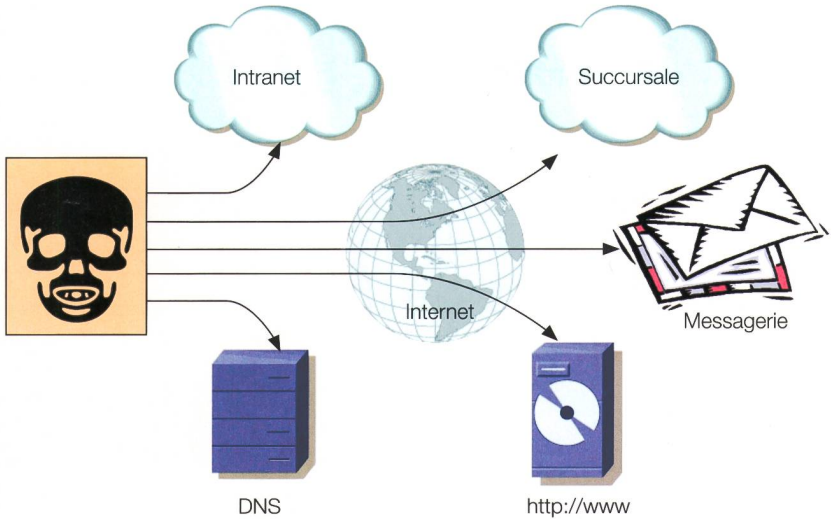


Figure 2 Surface d'attaque liée à un nom de domaine.

avantage sur les criminels, mais permet surtout de faire pression sur les fournisseurs de logiciels afin qu'ils produisent les mises à jour indispensables.

De nombreux sites présentent des listes complètes de vulnérabilités et de failles exploitables [1-2]. La plus courante est connue sous le nom de CVE (Common Vulnerabilities and Exposures). Cependant, la publication de telles listes est une arme à double tranchant, car avec relativement peu de connaissances, une personne ou une organisation mal intentionnée sera capable d'exploiter ces vulnérabilités. Néanmoins, ce genre de site représente une source d'information très importante et permet de vérifier, après corrélation, les risques inhérents à chaque logiciel.

Les hackers utilisent eux aussi une large palette de sites appartenant à la zone louche de l'Internet. Ils y laissent des traces et l'analyse systématique de leurs exploits permet d'en déduire les méthodes utilisées lors de leurs raids dévastateurs. Le site «zone-h» [3] en est l'un des plus propres, mais il fournit néanmoins des informations pertinentes pour NetObservatory.

Chaque éditeur de logiciels (systèmes d'exploitation ou autres logiciels applicatifs) se fait un devoir de tenir à jour une liste des failles et vulnérabilités constatées. Cette liste représente la référence principale utilisée lors de l'élaboration des mises à jour. Il se peut que l'un des composants d'un système contienne une faille hautement critique. Son éditeur générera alors un message urgent de mise à jour en espérant que les utilisateurs le suivent au plus vite, car la communauté des hackers l'aura également intercepté.

Evaluation et formation: le projet NetObservatory

Le projet NetObservatory a été conçu, d'une part afin d'évaluer de manière systématique le niveau de sécurité offert par les infrastructures suisses et, d'autre part dans le but de rendre leurs administrateurs plus attentifs aux risques actuels à l'aide d'une formation plus ciblée, notamment sur les méthodes utilisées par les agresseurs.

Présence publique et surface d'attaque

Lors de la réservation d'un nom de domaine auprès du «Top Level Domain» (TLD) – la fondation SWITCH pour la Suisse et le Liechtenstein [4] –, une entreprise acquiert en exclusivité une «identité Internet» qu'elle peut utiliser pour ses communications sur l'espace public (Internet) et privé (Intranet). Les services usuels, tels que Web et messagerie dépendent alors de ce nom comme le montre la figure 1. Une entreprise dispose, avec la possession d'un nom de domaine Internet, d'une foule de services qui lui permettent d'utiliser l'Internet en tant qu'outil de communication et de production de valeur ajoutée.

La mise en place d'un serveur Web (dans notre exemple http://www.entr.ch) et d'un serveur de messagerie basés sur le nouveau domaine, nécessite l'activation de ce dernier dans le système de noms de domaine appelé DNS (Domain Name System). Le serveur DNS se chargera alors de traduire le nom de domaine tapé par les internautes en une série de numéros Internet (IP) utilisés par ces machines.

Suivant les contrats passés entre l'entreprise et ses différents fournisseurs (hébergeur, éditeur, ou fournisseur d'accès ou de matériel), les numéros IP sont répartis dans plusieurs zones de l'Internet. Pour un attaquant, cette visibilité (nom de domaine, numéros IP) représente ce qu'il est courant d'appeler la «surface d'attaque» [5]. Chaque serveur, machine ou accès représente une opportunité, comme l'illustre la figure 2.

Identification des failles et vulnérabilités

Le service «Whois» [6] donne la possibilité de relier, en consultant le registre d'enregistrement, un nom de domaine public avec son propriétaire (entreprise) et les serveurs DNS. Puis, grâce à l'outil «DIG», les serveurs DNS permettent de retrouver l'identité (nom de domaine et

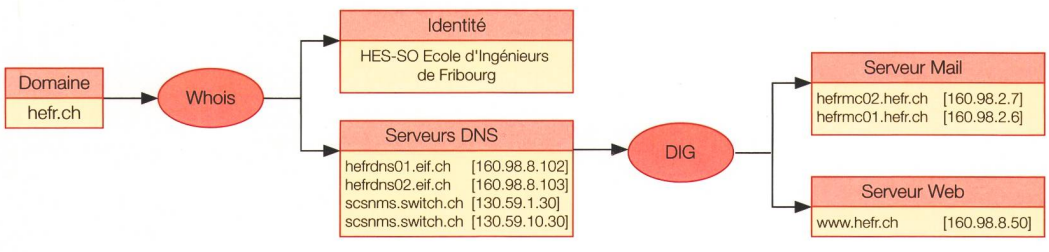


Figure 3 Acquisition d'informations publiques: identification des ordinateurs liés à un nom de domaine.

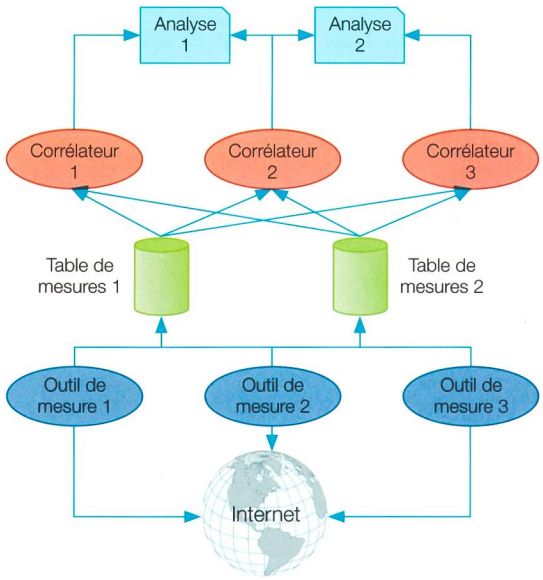


Figure 4 Infrastructure d'investigation automatique.

numéros IP) des différents serveurs opérationnels liés à cette entreprise. La figure 3 illustre cette démarche qui conduit à l'identification des machines (ordinateurs) visibles sur l'espace public de l'Internet.

Chaque serveur a ses propres caractéristiques et configurations. Une partie de celles-ci peuvent être vérifiées par de simples sollicitations. L'identification des failles et vulnérabilités se base sur une série d'éléments plus ou moins subjectifs révélés et divulgués sur l'interface publique.

Dans un premier temps, il s'agit d'identifier les natures et versions des systèmes d'exploitation et des logiciels applicatifs utilisés. Puis, l'attention est focalisée sur les erreurs de configuration typiques et dangereuses. Finalement, l'analyse des réponses à ces sollicitations permet de connaître le taux de « propreté » d'un domaine. L'analyse systématique d'un très grand nombre de domaines donne des informations pertinentes sur l'état de mise à jour et de sécurité de l'Internet en Suisse.

Infrastructure utilisée

L'infrastructure mise en place permet de conduire les campagnes de mesure et d'en analyser les résultats. Elle doit répondre à des exigences de performance, de fiabilité et surtout de sécurité très pointues puisque que plus de 1,3 millions de domaines et 600 000 serveurs ont été analysés. Les sollicitations transmises sont des sollicitations d'ordre « public » dans le sens où elles respectent scrupuleusement les formats des différentes normes et restent « furtives » afin de ne pas éveiller de faux soupçons quant à leurs objectifs.

La figure 4 schématise la structure d'outils de recherche et d'analyse mis au point. Une série d'outils de mesure récoltent des informations sur les systèmes, informations qu'ils sauvegardent sous une forme brute dans des tables intermédiaires. Les corrélateurs analysent ces tables en fonction des menaces et des attaques actuelles, et publient automatiquement leurs résultats de manière périodique [7].

Analyses

Les premières mesures ont montré que la grande majorité des serveurs Web des domaines « .ch » se répartissent entre deux produits, soit « Apache » et « IIS de Microsoft ». Comme l'illustre la figure 5, le premier, certes gratuit et « open source », représente 76 % du marché, contre 15 % pour le second. Au-delà de cette situation dominante – plus forte en Suisse que dans le reste du monde (Apache 60 % contre Microsoft 20 % [8]) – cette dépendance très forte des infrastructures Web en Suisse pour un produit stratégique pourrait, sous certains aspects, se révéler regrettable. Si une faille vitale devait être détectée dans ce logiciel, 80 % des serveurs Web hébergeant des domaines « .ch » deviendraient subitement vulnérables !

Un autre exemple d'analyse concerne l'utilisation des certificats SSL (Secure Socket Layer) permettant de garantir l'authentification et la confidentialité lors de transactions d'affaire (banque, e-commerce). Ce mécanisme permet à l'utilisateur de s'assurer qu'il est bien en présence du site désiré. Le cadenas du browser est alors fermé et la barre supérieure est de couleur verte ou bleue si la qualité du certificat présenté est suffisante.

Bon nombre d'algorithmes employés en sécurité ne sont, en raison de la puissance de calcul disponible actuellement sur de simples ordinateurs, plus considérés comme suffisamment forts. C'est le cas, par exemple, pour MD5 dont la vul-

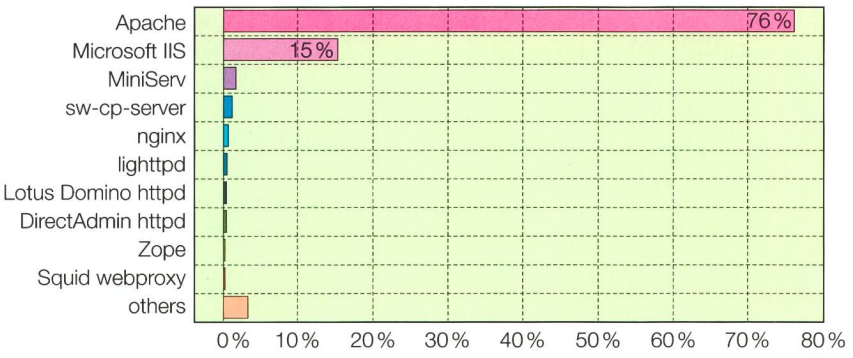
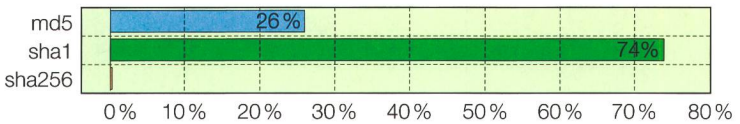


Figure 5 Parts de marché des serveurs Web sur les domaines « .ch ».



Figures: EIA-FR

Figure 6 Utilisation des algorithmes de hachage dans les certificats SSL.

Zusammenfassung

NetObservatory: Eine nationale Überwachungsstelle für die IT-Sicherheit im Internet

Zwei Schwerpunkte: Überwachung und Prävention

Websites und E-Mail sind heute unumgängliche Voraussetzungen für die Unternehmensproduktivität. Jede Internetverbindung ist jedoch ein potenzielles Einfallstor. In der Summe stellen diese Zugänge eine sicherheitstechnische Angriffsfläche dar, die potenziellen Angreifern die für ihre Zwecke erforderliche Infrastruktur bietet. Aufgrund der Vielfalt der eingesetzten Hardware und Software ist es jedoch für Webhosting- und Internetzugangsanbieter schwierig geworden, gezielte Sicherheitsmassnahmen anzubieten.
Dieser Artikel hebt deutlich die Schwächen der Internetsicherheit in der Schweiz hervor, wie sie von NetObservatory ermittelt wurden. NetObservatory ist ein Projekt, das sich der Evaluierung der Sicherheit von Infrastrukturen und der Risiko-Prävention widmet. CHe

nérabilité a été prouvée. La figure 6 représente la distribution des algorithmes de hachage (Hash) sur les certificats SSL utilisés par les domaines «.ch». Le constat est saisissant: 26% d'entre eux emploient encore MD5. A noter que SHA1 est actuellement considéré comme le standard et sha256 comme la solution la plus sûre.

Ces deux exemples mettent en évidence l'importance des démarches de prévention et d'information dans un processus d'amélioration (ou simplement de maintien) de la sécurité de l'Internet suisse.

Objectifs et perspectives

Le projet NetObservatory fournira à terme les éléments suivants:

- Des informations neutres et anonymes concernant l'état de sécurité de l'Internet suisse. Un rapport régulièrement mis à jour résume déjà les tendances et les risques majeurs encourus par les sites et autres infrastructures de type Internet présents en Suisse [7], ceci grâce à l'analyse de près de 1,3 million de domaines Internet de type «.ch» représentant majoritairement des entreprises et organisations actives en Suisse.
- Des informations ciblées et destinées aux entreprises (PME) qui le désirent. Chaque PME ou organisation aura la possibilité de consulter les informations concernant sa propre vulnérabilité et l'état de sa sécurité.
- Des cours de formation destinés aux développeurs et aux responsables de la gestion des infrastructures afin d'augmenter de manière concrète et durable la sensibilité aux problèmes de sécurité dans les infrastructures IT.

Aucune mesure en matière de sécurité ne saurait être efficace sans un intense échange d'informations entre toutes les parties prenantes (hébergeurs, éditeurs, ISP, chercheurs ou vendeurs). NetObservatory se veut également être un lieu de rassemblement et de dialogue entre tous ces partenaires.

A propos de NetObservatory

Démarré en septembre 2009, le projet NetObservatory est né de la collaboration entre l'École d'ingénieurs et d'architectes de Fribourg et deux leaders internationaux de la sécurité informatique: Dreamlab Technologies AG, dont le siège principal est à Berne, et OS Objectif Sécurité SA, sis à Gland. Il est soutenu par le réseau IT Valley du Pôle scientifique et technologique du canton de Fribourg. Ce dernier a pour objectif de favoriser la croissance et la création de postes de travail à haute valeur ajoutée en activant les collaborations entre les secteurs public et privé. NetObservatory bénéficie également des apports financiers de quatre entreprises partenaires: CDI SA, Tebicom SA, Accessible sàrl et Eb-Qual SA.

Références

[1] Common Vulnerabilities and Exposures (CVE): http://cve.mitre.org.
[2] The Open Source Vulnerability Database (OSVDB): http://www.osvdb.org.
[3] Zone-h, unrestricted information: http://www.zone-h.org.
[4] Fondation SWITCH, enregistrement de domaines: https://www.nic.ch/reg/index/view.html?.
[5] The Open Source Security Testing Methodology Manual 3, Institute for Security and Open Methodologies (isecom): http://www.isecom.org/mirror/OSSTMM.3.pdf .
[6] Domain-Based Research Services: http://www.whois.net/.
[7] NetObservatory: Aggregate Repport, December 2010: http://www.netobservatory.ch/report/pdf/NetObs_Report_01.12.2010.pdf.
[8] Netcraft Web Server Survey: http://news.netcraft.com/.

Informations sur l'auteur

Philippe Joye a été professeur de systèmes d'information et de sécurité IT à l'École d'ingénieurs et d'architectes de Fribourg (EIA-FR) de 1999 à mars 2011. Ingénieur électricien ETS de l'EIA-FR avec spécialisation en énergie électrique, il a obtenu son diplôme d'ingénieur EPFL en électricité en 1989. Philippe Joye a ensuite développé les parties commande et régulation des installations de puissance pour Reliance AG, avant de bifurquer dans le monde des télécommunications et de leur sécurité pour l'entreprise Ascom Autelca. Le 1er avril 2011, il a rejoint le groupe de recherche et développement de l'entreprise SICPA à Prilly (VD).

EIA-FR, 1705 Fribourg, info@netobservatory.ch