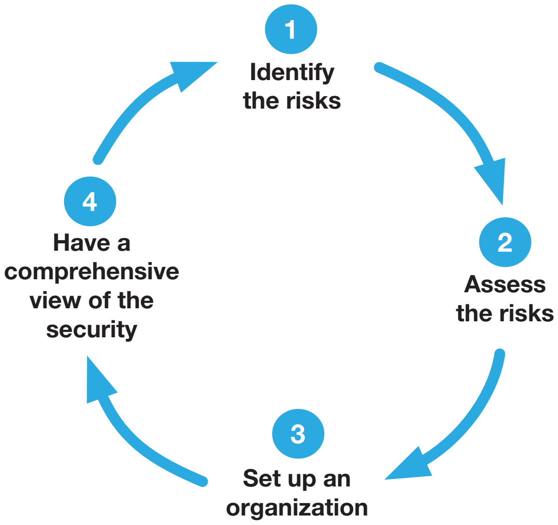
Issue paper n°9

Securing
the management of domain names

This issue paper is primarily intended for companies, whose presence on the Internet (commercial sites, communication campaigns, e-mail addresses, etc.) partially depends on their domain names and on how they manage them. That being said, the risks associated with domain names are sometimes little known. «Secure» management of domain names largely means having a view of the risks involved and of the «best practices» that can be used to limit them.

Applying the «best practices» outlined below helps protect the company against possible malfunctions or attacks from the outside. There are numerous cases of domain names that have been «stolen» (sex.com), improperly transferred (ebay.de) or suspended for lack of renewal (washpost.com).

These problems can be largely avoided, however.



The initiative presented in this issue paper can be summarized in a few key steps:

- identify the «endogenous» and «exogenous» risks to which the company's domain names are subject, and adopt counter-measures to limit those risks, if not delete them altogether;
- assess the risks associated with each domain name (probability of occurrence / impact in case of occurrence) and pay particular attention to protecting the most strategic domain names;
- set up an organization inside the company but involving the various outside stakeholders concerned, so that the security system can be consolidated in a sustainable manner;
- have a comprehensive view of the security issues involve and include domain names in the same way as the other items.

The complexity of the initiative is proportional to the size of the company. The rules presented are very simple to apply to the domain names held by any SOHO-SME.

Companies with a large number of domain names, and whose presence on the Internet is managed in a fragmented manner by a large number of partners and providers, will naturally gain from calling on specialists: in so doing, the companies will save time as well as benefit from the specialists' know-how of the issues involved.

1 Identifying and assessing risks

The risks associated with managing domain names are of two kinds:

- «Endogenous» risks, the symptoms of which are malfunctions and / or the loss of domain names, in general resulting from breakdowns of the management system in place;
- «Exogenous» risks, in the form of the theft or diversion of domain names by third parties exploiting one or more flaws in the management system in place.

Endogenous risks

This category of risks covers all the risks created by holders. Examples include the following:

- Failure to renew a name in time, leading to its suspension and then loss. The domain names of hotmail.com and washpost.com are well-known examples. In general, the suspension period is sufficient to identify the problem but results in a loss which although only lasting a few hours, can sometimes be extremely expensive. In the case of names used less, however, that negligence can even result in the return of the name to the public domain;
- The failure to update the identity of the holder of a name, sometimes resulting in situations of considerable legal complexity in which it is impossible to clearly establish who owns a name, since the holder has ceased to exist. Comparable situations may arise when the domain name of a company is filed by one of the partners in his or her own name, resulting in a dispute between all of the partners. The rules implemented by ICANN also clearly show that names may be deleted if the WHOIS data are not correct;
- The deliberate or unconscious «delegation» of ownership and / or administrative contact of a domain name to a service provider or a partner, whose interests may one day diverge from those of their client, and who may be tempted to use the control they have over the client's domain names against their client's best interests. This case is extremely common;
- The obsolescence of contacts including email addresses, such that the holder no longer receives any messages associated with the management of the domain name. The immediate consequence of this is that change requests can neither be approved nor rejected, and reminders when renewal deadlines have passed are never received;
- The careless abandonment by the holder of domain names used as e-mail support for administrative contacts of other names in the portfolio, without suspecting that this opens a security hole in the system, by allowing third parties that have re-registered the domain name to take control of all the domain names, since the contacts in question continue to depend on the abandoned name;
- An insufficient policy (or even a total lack of policy) in terms of securing access to the domain name management interfaces. In general, domain names are managed and configured via web interfaces provided by the registrars. A person who has the password to access these interfaces can repoint names, cut the service or change the DNS servers and contacts. This happened to twitter.com in 2009;
- A faulty internal organization does not enable the management of domain names with proper security. Typically, name management is conducted empirically without any in-depth reflection about the best practices to be followed in terms of organization, which creates vulnerabilities in case of malfunctions (such as the lead-time to solve the problem) or attacks (such as a limited ability to identify the nature of the attack and appropriately respond);

Exogenous risks

Exogenous risks are better known than endogenous risks because their relatively high media coverage. They are closely related, however, since numerous attacks by third parties are made possible or facilitated by the existence of flaws in the various points outlined above.

- The theft of domain names is the most salient risk, a number of cases having made the public aware of this possibility. «sex.com» was one of the best-known domain names stolen. There are various motivations for these thefts, from the prospect of reselling the name to others, to industrial espionage (by collecting sensitive information via e-mail) to extortion, damaging the holder's brand image or interruption of service altogether;
- The immediate registration by a third party of a domain sensitive deleted or abandoned by mistake. This is a common occurrence, and facilitated even further by the existence of automated tools and systems to assess the traffic generated by a domain name about to fall into the public domain. The harm can be considerable, from the interruption of email and web services to the hasty buyback of the name in question at prices well above market rates;
- Abusive transfers, used to install a domain name on servers that are not «legitimate» after the name has been transferred to a new registrar, and then point the name to the website selected by the abuser. Names as well-known as nike.com, ebay.de or panix.com have been subject to attacks of this kind;
- The diversion of domain names when the attacker has access to the management interface of the domain names in question. Cases of such attacks are less well known, but the press has reported disputes between companies and unscrupulous former employees who used their access to cause detriment to their former employer;
- Security flaws in the procedures for exchange between holders and their service providers, or at the service providers. These risks can occur if the access is not secure (https), which potentially allows the «hacker» to capture information. Another example is when there is no mutual authentication / identification system of contacts, which can promote the theft of the holder's identity or that of a service provider by a third party, the latter thereafter being in a position to «request» information or «recommend» actions detrimental to the holder. This kind of mishap has already affected holders whose service providers accept documents sent by fax as proof. The attackers obtained an update of the administrative contact on the basis of the fax alone, and were then able to transfer the domain names concerned;

We prefer to refer to «service providers» in the broad sense, because a wide variety of stakeholders can be involved in the management of domain names for an end-customer, from the registrar to the employees of the client as well as intermediaries such as web agencies, legal consultants and others.

In certain cases, a business partner holds the domain name or is responsible for its management. The company must be capable of assessing the reliability of the partner in question, and legally protecting itself against any unexpected contingencies, for example due to formal contracts granting the use of the domain names involved, and providing for their «restitution» should the ties with the partner be broken.

Since the golden rule of security is that «the strength of a chain is equal to that of its weakest link», a holder who is aware of the issues involved will tend either to ensure that each link is «secured» or shorten the chain of stakeholders as much as possible, or both. The ideal situation is reached when all the domain names of a holder are under the latter's exclusive, direct, legal and administrative control, the remaining technical issues generally being entrusted to a service provider.

Risk assessment

One approach to risk assessment could be as follows:

- Identify the criticality level of each domain name in the portfolio (related services, impact in case of malfunction, suspension, loss, misuse or theft, etc.);
- Analyze the WHOIS data, taking care to ensure that the name is managed in accordance with the best practices described below;
- For names that are not managed according to best practices, assess the likelihood of the risk induced by non-compliance (e.g., a name used as a communication support for a flagship brand is more likely to be attacked than a defensive name using an unknown TLD);
- Set up an action plan to correct any potential faults on strategic names with a high probability of attacks or in which failures would result in serious harm to the holder;
- Place ad hoc monitoring tools on the most strategic names, including in particular the WHOIS and DNS data for these names;

2 Limiting endogenous risks

In this second section we address the best practices that can be used to limit endogenous risks.

Controlling renewals

The renewal deadlines for domain names must be known and monitored. The only valid dates are those listed in the official WHOIS for the registries in charge of the TLD in question. Discrepancies sometimes occur between the anniversary dates for domain name renewal by a service provider and the renewal dates provided by the registry, leading to errors.

When the service provider offers this service, the safest option to avoid problems related to renewals is to switch to «automatic renewal» mode, the client naturally retaining the ability to formally request the non-renewal of a specific name. This practice requires greater supervision by the customer in terms of the choice of names to be renewed or not (since the provider will automatically bill for names on each renewal). It is a much safer method, however.

Renewal for X years reduces the number of payments (once every 5 years instead of five times) but does not solve anything in substantive terms, and limits management flexibility since it forces holders to make X down payments in advance for names that they may wish to abandon in the meantime.

When a domain name suddenly stops operation, the status in terms of its renewal is the first thing to consider.

Being the real holder of domain names

Just as a company owns its brands, it must ensure that it is the effective holder (or «registrant») of the domain names it has registered or that have been registered in its name.

It should be clearly and formally stated the company owns all the domain names registered through its association with a given service provider or partner. Any domain name registered by a third party in connection with the company must be returned without any consideration over and above the costs incurred by the transaction, if it has been registered in good faith.

This rule also applies in the case of domain names registered in their own name by the partners in a business. This is often justified by the need to register domain names before the corporation owning them has been created. But once the latter has been duly registered, it is important that the ownership of the domain names be transferred to it in order to prevent «physical» i.e. individual holders one day from using this to the detriment of the other partners.

Negligence in this respect exposes the company to conflicts over ownership and operation of the domain name, if a dispute arises between it and the service provider or holder.

The company should apply this requirement to itself, by ensuring that the domain names it owns always have ‘active’ legal entities as holders (parent company, subsidiary, etc.). Updates are therefore required if and when the company’s situation changes, such as further to mergers, acquisitions or disposals, changes in trade name, etc. Ideally, the holders of domain names should be aligned with the holders of the brands to which the domain names correspond.

Contacts: relevant and sustainable

Contacts, including the email address of the administrative contact, must be relevant and sustainable. It is useless to indicate the company manager as the administrative contact if the person has no dealings at all with domain names, even if the manager is the company’s only legal representative.

By default, a «generic» email address (dns.admin@example.fr) must be used to avoid having to update it with each change in the person in charge of domain names. Conversely, if the person leaves the company, his/her email address must not be deleted. Ideally, the address should be maintained for as long as it takes the new manager to ensure that it is not registered for use as the contact address for any of the domain names in the company’s portfolio.

From the security optimization point of view, it is better to avoid having a contact email address for a domain name which is the same as for support. This is to avoid deadlock situations in which a malfunction affecting the domain name also prevents the email system from functioning. As a corollary, it is imperative not to abandon a domain name used to support emails before making sure that it is no longer used for contacts.

Finally, it should also be noted that contact addresses using «free» email accounts may present risks in terms of security, if reference is made to some recent cases. Whatever the choices made, the company must ensure that it keeps control of the contact addresses with respect both to the domain names and to the codes used to access or send messages.

Login information: keep your secret secret

The IDs and passwords used to access the management interfaces of domain names are particularly sensitive data. Any person holding them can connect to the account anywhere in the world and make any changes to the domain names involved, including repointing, updates to servers and contacts or transfers to another registrar.

IDs and passwords must not be communicated by email or recorded on media accessible to one and all. They should be entrusted to a deliberately limited number of fully identified persons, formally empowered to intervene in the interface, where applicable, specifying the rights of each of the persons in questions. Access codes must be sufficiently «robust» and changed at regular intervals. Any departure of one of the people on the team should automatically result in the updating of passwords, this rule also being applied when the company's portfolio is specifically monitored by one or more contacts within the service provider company, and whenever one of those contacts leaves the company.

Based on the same logic of controlling the ownership of domain names and administrative contacts, it is important that the company has the «keys» to the management interface of its domain names, and is the only one to have them. This can be difficult to do when an intermediary manages all the names of its customers on a single account with a given registrar. Although common, this situation is not to be recommended from the point of view of making domain name management secure, because it leads to over-dependence on third parties. A service provider with «co-access» to the interface can do whatever it wants with the company's domain names, including changing the password to access the interface without the client's knowledge in the event of a conflict. If nothing more, the contract governing the partnership should at least prohibit any such practice.

For security reasons, access codes to interfaces should also be stored in a safe place, accessible in the event of an emergency and if the qualified persons are not available. The persons authorized to obtain the codes under these exceptional circumstances must be identified and known to the accredited registrars in order to take the necessary measures.

An internal organization tailored to requirements

The three principles of internal organization are as follows:

- Have a referral identified in the file, to act as an in-house «expert» and coordinator. The rights of the referral can be extremely extensive in the case of concentrated management methods, or very limited in the case of decentralized management. But there must be one in every case, in order to manage the second principle;
- Adopt a cross-company approach combining the different skills needed in order to take decisions with a global vision of requirements and risks. The theft of a domain name for example may have implications in terms of sales, image, security and litigation. All the necessary disciplines must be involved in the control of the file;
- Have clear procedures for any transaction request concerning one of the company's domain names. The procedures may vary quite widely depending on the mode of management adopted, but they must make it possible to know who has done what, and ideally, why. This makes it possible to quickly find the author or originator of a transaction causing a problem and understand what has happened. Conversely, any request to perform a transaction not complying with the procedure can be identified as suspicious, which reduces the risk of so-called «social» attacks;

The objective of the internal organization is to be capable of limiting the risks while responding quickly and appropriately to failures and to attacks. This requires both skill(s) and coordination. The AFNIC issue paper devoted to Slamming, for example, stresses the value of an internal referral who is aware of these fraudulent practices and that can warn his/her correspondents in an emergency.

3 Limiting exogenous risks

In this third section we address the best practices that can be used to limit exogenous risks.

Secure exchanges between holder and service provider

Most registrars offer their customers management interfaces with which to manage domain names without using the service provider's team. Over and above the password issues mentioned above, access to them should be in https mode.

This solution, however, is rarely possible when the holder uses the services of a reseller (web agency, consultant, etc.) managing the domain names of its customers via its own account with a registrar. In this context, end users should set up with their service providers a communications system limiting the risk of 'social' attacks:

- Clear identification of the e-mail addresses used by the end customer and by the service provider. Any email received from another address concerning the management of domain names should be regarded with suspicion (but not necessarily ignored). This rule – which does not exclude a critical look at emails which are apparently «legitimate» – also applies to «paper» mail from a service provider other than the one with which the end customer is in contact;
- In the case of service providers offering their customers support services, clear identification of the account managers and contacts authorized to act on the client's domain names, and conversely, staff at the customer site who are entitled to give instructions to the service provider;
- Confirmation procedure by another channel in case of transactions that may affect the management of the domain name (pointing, changes of contacts, etc.). This issue is sometimes «transparent» for the end-customer when the service provider takes care of everything, but in that case the customer has control over nothing, which is not a desirable situation;
- Confirmation of receipt by the service provider of any transaction request carried out on domain names. In this way, clients know that their instructions have been taken into account and carried out, and can react if they made no such request;
- Existence of an «emergency» procedure and contacts allowing the end-user to obtain immediate assistance from the service provider in case of a serious problem (theft, unexpected deletion of a name, etc.);

Although this is not the only criterion for choosing a registrar, using a service provider with the same working hours that is capable of communicating in the appropriate language may be considerable advantages in a crisis situation.

Security levels appropriate to the criticality of the domain names

The domain names in a portfolio do not all need to be overprotected. But a registrar which does not make it possible to properly secure the domain names entrusted to it could become a source of vulnerabilities in the global corporate security system.

- The existence of «recovery» systems enabling an immediate return to the configuration prior to a change considered to be detrimental;
- The ability to "lock" names at the registrar level. Domain names must be protected against any transaction not initiated by the holder. The usual status in the gTLDs is «RegistarLock» or clientTransfert-Prohibited, clientUpdateProhibited, clientDelete-Prohibited which prohibit transfers, data changes or deletions by other parties;
- This vital security measure must be complemented by the possibility for the customer via the interface to access authInfo and other codes to unlock the domain names, without the intervention of the registrar. Otherwise, the client depends on the efficiency and / or the goodwill of its service provider, including what happens in situations where intermediaries are the only people with access to the management interface;
- Installation of an automatic recovery system of strategic names falling into the public domain. A number of tools are available free of charge on the market, as long as the monitored domain name has not been recovered. This level of security is rarely implemented today, but it can be an effective answer to an unexpected deletion of a domain name because of an attack by a third party, for example who has managed to «fool» the claimant or to gain access to the management interface;
- For the most strategic names, recourse to «Registry Lock» services, i.e. to lock the domain name at the level of the Registry for the TLD, if it provides this service;

Internal precautions taken by the company

These «precautions» are of various kinds and this is why they are grouped together in a special section. Examples include:

- Taking into account domain name issues in the company's overall risk management policy. This precaution may be useful in that it complements this policy by helping staff to understand why the issues related to the management of domain names should not be neglected;
- Developing a business continuity plan in the case of an incident involving a strategic domain name, detailing in particular the interactions with one or more service providers. The staff involved in the plan must be trained and regularly exercise the use of the plan;
- Coverage by insurance policies of the potential damage related to incidents involving domain names. This issue is still underdeveloped in France, but seems to have become an obvious factor in the U.S.;
- Setting up surveillance systems on WHOIS servers in order to check that the domain names are securely locked and that the information recorded have not been modified without the company's knowledge;

4 Find out more

The links provided below refer to actual cases of theft and incidents involving domain names stemming from the non-compliance with the rules set out in this issue paper. We also mentioned articles and documents on the same subject.

Real cases

Internal Twitter Credentials Used in DNS Hack, Redirect
http://www.wired.com/threatlevel/2009/12/twitter-hacked-redirected/

Firm to sue employee for domain name theft
http://www.out-law.com/page-4964

Washington Post Misses Domain Deadline
http://www.internetnews.com/xSP/article.php/3309801/Washington+Post+Misses+Domain+Deadline.htm

Grand Jury Indicts Daniel Goncalves On Domain Theft Charges
http://www.domainnamenews.com/legal-issues/grand-jury-indicts-daniel-goncalves-domain-theft-charges/6613

Major Domain Hijacking Alert: Industry Pioneer Warren Weitzman Has Over a Dozen Domains Stolen From his Enom Account
http://www.dnjournal.com/archive/lowdown/2009/dailyposts/20090721.htm

Hushmail DNS Attack Blamed on Network Solutions
http://www.eweek.com/c/a/Security/Hushmail-DNS-Attack-Blamed-on-Network-Solutions/

ISP Panix Domain Name Hijacked
http://www.thewhir.com/web-hosting-news/isp-panix-domain-name-hijacked

Articles and reports

How To Protect Yourself Against Domain Name Hijackers
http://securityskeptic.typepad.com/the-security-skeptic/how-to-protect-yourself-against-domain-name-hijackers-.html

Vol de nom de domaine : comment l'éviter et que faire si ça vous arrive (Domain name theft: how to avoid it and what to do if it happens to you)
http://www.olivier-duffez.fr/conseils-contre-vol-de-nom-de-domaine

How Secure Is Your Domain Name?
http://www.inc.com/articles/2001/06/23147.html

SPECIAL REPORT: How to protect your domain name from hijackers, porn pirates, and your registrar.
http://www.betterwhois.com/domainhijacking.htm

Protecting Your Domain Name: Control is the Key.
http://tcattorney.typepad.com/anticybersquatting_consum/2007/08/protecting-your.html

SSAC Report – Hijacking – 12 07 05
http://www.icann.org/announcements/hijacking-report-12jul05.pdf

SSAC Report – SAC 044 - A Registrant's Guide to Protecting Domain Name Registration Accounts
http://www.icann.org/en/groups/ssac/documents/sac-044-en.pdf

Afnic is the French Registry for the .fr (France), .re (Reunion Island), .yt (Mayotte), .wf (Wallis and Futuna), .tf (French Southern Territories), .pm (Saint-Pierre and Miquelon).

Afnic is also positioned as a provider of technical solutions and services for registries and registrars. Afnic (the French Network Information Centre) comprises public and private stakeholders, including government authorities, users, and Internet service providers (Registrars). It is a non-profit organisation.

www.afnic.fr

Read all of our issues papers:
http://www.afnic.fr/en/ressources/publications/issue-papers-3.html