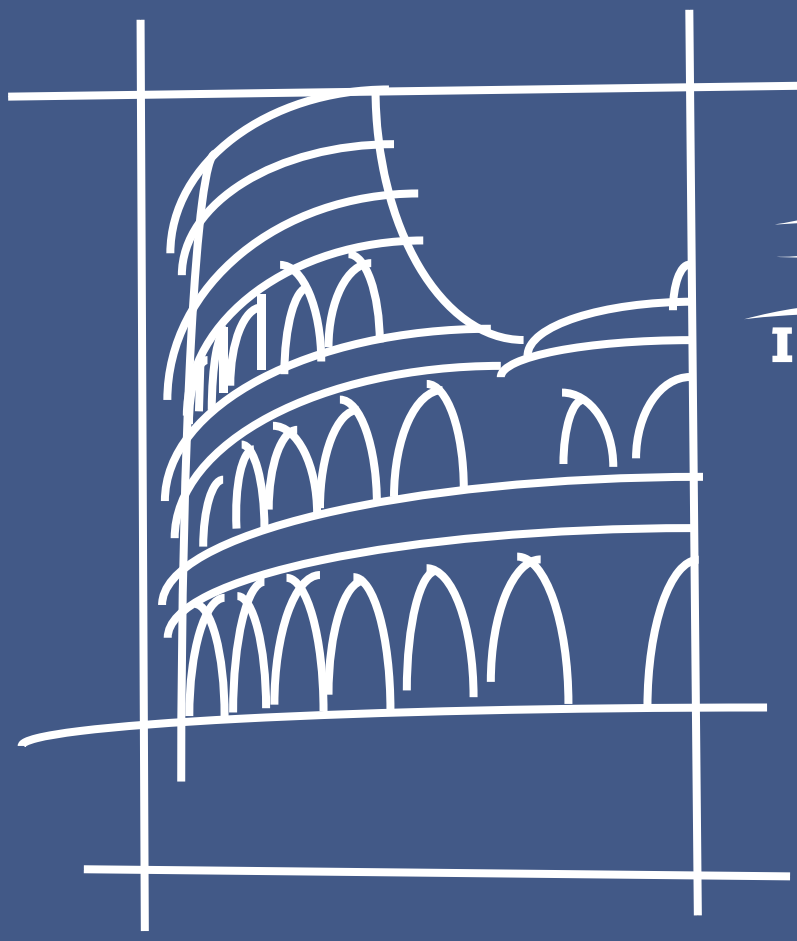
R.A. News
marzo 2004

Istituto di Informatica e Telematica del CNR



ICANN

ROME 2004

FOCUS ON

ICANN ROME MEETING

CUSTOMER CARE MANAGEMENT

SURFING THE DEVELOPMENTS OF THE NET

NET-SECURITY ISSUES

Editoriale

Internet non è nato sotto un cavolo…

Da pochi giorni si è concluso a Roma il primo meeting 2004 dell'Internet Corporation for Assigned Names and Numbers (***www.icannrome.it***), organismo internazionale che gestisce buona parte del governo della rete su incarico del Dipartimento del Commercio americano.
Il meeting ha riunito oltre 700 delegati provenienti da oltre 80 paesi, conquistando il primato della riunione ICANN con il più alto tasso di affluenza.
Organizzare questo evento non è stato facile: negli ultimi otto mesi il lavoro è stato frenetico e, di fronte a molte pretese in stile "Las Vegas diva", snervante.
Basti pensare ad alcuni numeri: 191 lettere di invito per delegati che necessitavano di visto consolare per venire in Italia; 16 sale riunioni; 4000 coffee break; oltre 200 richieste da parte di giornalisti della stampa nazionale ed internazionale; 24 sponsor ufficiali.
Al meeting ha partecipato Vinton G. Cerf, Presidente del Board of Directors di ICANN, un signore americano magro e slanciato, con l'occhio attento a quello che gli ruota attorno, un gentleman di altri tempi, che, negli anni sessanta, poco dopo la laurea, partecipò al progetto che fece nascere la rete. Non a caso, ancora oggi, viene considerato il "padre di Internet".
Un uomo dai modi raffinati che si è appassionato alle bellezze della città eterna, all'indimenticabile tiburio e alla navata color oro sotto cui si è svolta la cena di gala di ICANN ROME 2004, agli scavi archeologici sotto la basilica di San Pietro, ai sapori ed ai profumi di una delle cucine più rinomate al mondo.
Un uomo che è la prova che la rete è nata da studi ed esperimenti, che non è emersa dalle acque o ha preso vita da un fulmine, che non è stata trovata sotto un cavolo o lasciata da una cicogna su un comignolo della California.
La rete esiste perché Cerf ed altri, tra cui Robert E. Kahn, ne hanno "disegnato" l'architettura.
Il 2004 segna, tra l'altro, il trentesimo anniversario della prima pubblicazione su Internet: ricordando questa tappa nella storia della rete, Cerf, all'interno del sito MCI (***http://www.mci.com***), ha dichiarato che non avrebbe mai immaginato un impatto così forte e rivoluzionario dei risultati del suo progetto di ricerca.
Tuttavia così è: Internet è divenuto nel giro di pochi decenni il più potente ed universale mezzo di comunicazione.
Questo numero di RA News è ampiamente incentrato su ICANN ROME 2004, con tre approfondimenti sugli aspetti relativi al Customer Care Management, al futuro della rete ed alle tematiche di sicurezza.
Al contempo, concedetemi di dedicarlo a chi, e sono in molti, ha confessato la sua ignoranza, credendo che Internet fosse più o meno nato sotto un cavolo (*g.s.*).

Editorial

The Internet was not delivered by the stork…

The first 2004 meeting of the Internet Corporation for Assigned Names and Numbers (***www.icannrome.it***), the international body appointed by the US Trade Department to handle a large part of the Internet governance, closed in Rome a few days ago.
The meeting was attended by over 700 delegates from over 80 countries, turning out to be the most widely attended ICANN meeting.
It was not easy to organise the event: over the last eight months, work was frantic and nerve-racking when primadonna demands began to flock in.
Just think of the figures: 191 invitation letters to delegates who needed a consular visa to come to Italy; 16 conference rooms; 4000 coffee breaks; over 200 requests from national and international press; 24 official sponsors.
The "father of the Internet" was there: Mr. Vinton G. Cerf, Chairman of ICANN's Board of Directors, a tall and thin American gentleman, who always keeps an eye on what goes on around him, an old-style gentleman who in the Sixties, just after graduating, took part in the project that gave rise to the Internet.
An elegant, well-mannered sir who was fascinated by the beautiful sights of the Eternal City, the unforgettable tiburium and the golden-coloured aisle under which the gala dinner for ICANN ROME 2004 was held, the archaeological sites underneath Saint Peter's, the flavours and tastes of the most famous food in the world.
A man who is living proof of the fact that the Internet was the fruit of research and tests, which did not come out of the blue or grow where the earth was struck by lightning, who was not delivered by the stork or picked up somewhere in California.
The Internet is there because Cerf and others, including Robert E. Kahn, "designed" its architecture.
In addition, the year 2004 marks the thirtieth anniversary of the very first publication regarding the net: on recalling that day, Cerf, on the MCI web site (http://www.mci.com), said he would never have expected that his research project would have had an impact so powerful and revolutionary.
And yet it did: the Internet has become the most powerful and universal communication media in just a few decades.
This issue of RA News is widely focussed on ICANN ROME 2004, with some articles on Customer Care Management, the future of the Net and security issues.
At the same time, allow me to dedicate it to those, and they are many, who confessed their ignorance, thinking the Internet had been more or less delivered by the stork (*g.s.*).

ICANN e la gestione della rete: intervista a Paul Twomey, Presidente di ICANN

Cosa è ICANN e qual'è la sua missione?

ICANN è un ente no profit organizzato a livello internazionale che coordina la gestione del sistema Internet di identificativi univoci, in particolare il sistema dei nomi a dominio, indirizzi IP e parametri legali (importanti per la comunità tecnica che sta sviluppando l'MRC). ICANN è anche responsabile della gestione della concorrenza e della scelta nei mercati dei domini di primo livello generici, .com, .biz, .info.

Quali rapporti intercorrono tra ICANN e i suoi Comitati e Organizzazioni quali l'ALAC, l'ASO, il ccNSO, il GAC e il GNSO?

ICANN è un organismo politico/decisionale che applica un approccio "dal basso verso l'alto" e dispone di organi per le varie constituency della comunità.
Una delle tre organizzazioni di supporto è il GNSO (Generic Name Supporting Organization), che rappresenta svariate constituency di gruppi d'interesse che si occupano dei nomi generici, come ad esempio gli ISP, i registri, i registrar, il settore della proprietà intellettuale, gli assegnatari di nomi a dominio non commerciali.
La Address Supporting Organization rappresenta gli interessi di coloro che partecipano al processo di attribuzione degli indirizzi IP, in particolare i registri regionali, come ad esempio il RIPE, l'ARIN, l'APNIC e il LACNIC.
Tra gli organi consultivi il più importante è il Governmental Advisory Committee, che svolge un ruolo di particolare rilievo insieme ad ICANN.
Il governo fornisce al consiglio di ICANN pareri inerenti a tematiche legate alle politiche pubbliche e di governo.
Il Governmental Advisory Committee conta più di cento membri provenienti da cento paesi e la presidenza è attualmente detenuta dalla Malesia.
Ci sono poi altri comitati consultivi di tipo specialistico: uno di questi è il Root-Server System Advisory Committee a cui prendono parte coloro che operano nel settore dei root server; un altro importante comitato è il Security and Stability Advisory Committee, i cui membri sono stati nominati dopo l'11 settembre del 2001 e che ha il compito di fornire al consiglio di ICANN dei pareri in materia di sicurezza su internet.
Un altro comitato consultivo di grande rilievo, che sta diventando sempre più importante, è l'At-large Advisory Committee, che svolge un ruolo chiave all'interno dell'ICANN.

The ICANN vision of the net: interview with Paul Twomey, ICANN CEO

What is ICANN and which is its mission?

ICANN is an international organized, non-profit organization which coordinates the management of the internet system of unique identifiers, in particular domain name system, internet protocol addresses and court parameters (important for the technical community developing (MRC). ICANN also is responsible for running competition and choice in the generic top level domain markets, .com, .biz, .info.

What are the relationships between ICANN and the other Committees and Organizations as ALAC, ASO, ccNSO, GAC, GNSO?

ICANN is a bottom-up decision/policy making body, which has organs for the various constituencies of the community.

Paul Twomey

One of the three supporting organization is the generic name supporting organization, is GNSO, which represents various interest groups constituencies involved with generic names, for instance the ISPs, the registries, the registrars, intellectual property community, non-commercial domain name holders.
The address supporting organization represents the interests of the people involved with the allocation of IP addresses and in particular the regional internet registries like RIPE, ARIN, APNIC, LACNIC. Within the series of advisory communities, the most important is the Governmental Advisory Committee that has a special role with ICANN.
The government gives advise to the ICANN board on issues that are related to the government policy, the public policy and the Governmental Advisory Committee has over one hundred members of one hundred countries and members and the chair is from Malaysia.
Other advisory Committees that we have, specialist advisory Committees, one is the Root-Server System Advisory Committee which consists of the various people who operates root servers, one is the Security and Stability Advisory Committee, they are group of people appointed after the 11th of September of 2001, who gives the ICANN board advise on issues related to the internet security.
We have one of the other key advisory committees and its growing all the time on importance is the At-large Advisory Committee that is a very important part of ICANN.

Si tratta di persone che rappresentano gli interessi degli utenti di Internet, e attualmente stiamo cercando di puntare in maniera del tutto particolare sullo sviluppo di una base più ampia di organizzazioni di consumatori e organizzazioni di utenti Internet, per consentire loro di partecipare all'Advisory Project Committee, potendo così fornire al consiglio dei pareri su tematiche legate ad Internet. Un'altra componente di ICANN che verrà presto annunciata, o meglio definita, è la Country Codes Name Supporting Organization, che rappresenterà gli interessi dei gestori dei country code.

Perché è stato necessario fondare il GNSO, una task force sulla privacy dei dati del WHOIS?

Innanzitutto la questione del WHOIS non riguarda solo la privacy dei dati. Ci sono in realtà tre task force nel GNSO, se facciamo riferimento ai workshop sul WHOIS che abbiamo tenuto durante gli ultimi due incontri, e queste task force hanno un unico obiettivo, determinare in che modo rispondere alle molteplici richieste sulla gestione del database del WHOIS. I database del WHOIS sono stati a lungo utilizzati come strumenti standard su Internet per permettere alla comunità tecnica di identificare la persona responsabile di un dato nome a dominio, e per poterla contattare nel caso in cui si fossero verificati dei problemi.Esistono altri gruppi d'interesse che vogliono utilizzare questi database per scopi diversi, gruppi o agenzie per l'applicazione delle leggi, gruppi d'interesse legati alla proprietà intellettuale che proteggono i diritti di proprietà intellettuale dal "cyber squatting", organizzazioni di consumatori; tutti questi soggetti sono interessati ai database WHOIS, che sono sia delle liste di dati molto accurate che strumenti che le persone possono utilizzare. O almeno questa è la percezione che ne hanno i consumatori.
D'altro canto, c'è anche chi ritiene che i database del WHOIS dovrebbero essere protetti, dovrebbero essere più privati. I registrar spesso pensano che i dati dovrebbero essere riservati perché, credo, hanno la sensazione di poter essere sempre soggetti ad attacchi esterni, ed in effetti anch'io sono d'accordo. La chiave di volta delle richieste di maggiore privacy non è molto diversa dai data protection commissionaire.Quindi la difficoltà che incontriamo consiste nel fatto che esistono due diversi gruppi d'interesse, entrambi con motivazioni valide: uno chiede che tutto divenga sempre più accurato e aperto, mentre l'altro chiede che prevalgano la riservatezza e la chiusura. Dobbiamo cercare di trovare una soluzione pragmatica che possa essere accettabile per tutti, che metta d'accordo le due parti.
Dobbiamo cercare una via pragmatica per aiutarli a raggiungere una conclusione che sia soddisfacente per entrambi. È proprio su questa tematica che si stanno concentrando i gruppi di lavoro. La politica di sviluppo di ICANN non viene dall'alto, non viene formulata dallo staff ma è sviluppata in collaborazione con queste organizzazioni che svolgono una reale funzione di supporto. Si tratta di un processo che parte dal basso e che si sviluppa grazie a loro; è per questo motivo che esistono questi gruppi all'interno del GNSO.

These are people who represent the interests and the users of consumers of internet, and we are putting a lot of emphasis into trying to develop a broader base of individual consumers' organization, internet users' organization, to be part of the Advisory Project committee and to advise the board on issues related internet.
One of the parts of the ICANN structures is also close to be announced, best to be formulated, is country codes name supporting organization which will represent the interests of the country code managers.

Why was there the necessity to found GNSO, task force on WHOIS data privacy?

The issue of WHOIS is not just on data privacy, by the way.
There are three task forces on the GNSO looking at the WHOIS workshops that we've had on the last two meetings and the task forces under the GNSO are all focused on the same target, which is how do we address the different demands that exists in terms of the operation of WHOIS database.
WHOIS databases have existed for a long of time as standard of the internet, so the technical community could identify who is the person responsible for a particular domain name, to actually get in contact with if something went wrong.
There are other interest groups who want us to use this databases for other purposes, law enforcement groups, law enforcement agencies, intellectual property interests who protect intellectual property rights against cyber squatting, consumer protection organizations, they all have an interest in WHOIS databases, being both accurate data and being a tool to people to use.
As due to that matter in uses, because the consumers have that perception.
Then on another side, there are people who think that WHOIS database should be protected and be more private, the registrars often think that data should be private because I think they feel that their costumers bases are always under attack from other people and I think also, the key to their privacy concerns from privacy applicants its not so different from data protection commissionaires.
So the difficulty we have is that we have two different groups of interests, both have a valid argument which says either make it a very accurate and very open our make it very private and not open.
We need to try to find a pragmatic solution that all the people can live with it.
That will be perfect for each part. We've got to find the pragmatic solution to help them arrive at a mutually successful conclusion.
That's what working groups are working on.
The development policy in ICANN doesn't came from the board down, it doesn't come from the staff, it develops up this really supporting organizations, it's a bottom up process of policy coming up through them, that's why we've got this groups happening in the GNSO.

Il nuovo dominio "eu" è ormai alle porte: ICANN ha una posizione precisa in merito ai TLD "regionali" da adottare in futuro?

Innanzitutto vogliamo concludere presto gli accordi necessari al lancio del dominio "eu". Ritengo che ci siano ancora elementi che sono oggetto di discussione tra la Commissione europea e l'unione dei registri, di cui fa parte il suffisso "it". Ma una volta conclusa questa fase intendiamo perfezionare gli accordi che sono di nostra competenza.
Per quanto riguarda nuovi TLD a livello regionale, una cosa secondo noi estremamente importante, non ci sono pervenute richieste e ci siamo orientati verso il dominio "eu", dato che riconosciamo quei TLD, TLD nazionali e regionali, che sono inseriti in una lista denominata ISO 3166. I nostri governi utilizzano quella lista e il dominio "eu" è stato attivato proprio dalla lista, ma non abbiamo ricevuto altre richieste di ccTLD regionali o TLD regionali, perciò non prevediamo di attivarne altri.

Quali sono stati i principali successi di ICANN negli ultimi anni?

Ottima domanda. A mio parere il primo riguarda la creazione di una "casa comune" a livello mondiale in cui tutti coloro che hanno a che fare con il sistema dei nomi a dominio e l'indirizzamento IP possano incontrarsi per discutere e risolvere le diverse problematiche che possono incontrare. Adesso questa "casa comune" esiste. La seconda parte della mia affermazione riguarda proprio quello su cui stiamo lavorando adesso, stiamo continuando a globalizzare il nostro linguaggio: ad esempio a gennaio ci siamo recati nell'ufficio europeo e abbiamo realizzato che il vicepresidente sig. Paul Verhoef vive in Europa. Precedentemente aveva lavorato nella Direzione Società dell'Informazione alla Commissione europea. L'altro grande successo, a mio parere, è la creazione della concorrenza nel mercato dei registrar per i principali nomi a dominio generici di primo livello, "com", "net" e "org". Questo ha portato ad una diminuzione dei prezzi per i consumatori pari all'80%, che equivale ad un risparmio annuale per i consumatori di circa 1,5 miliardi di dollari. Abbiamo introdotto i sette nuovi nomi a dominio generici di primo livello, compresi quelli "sponsored" come "coop", "museum", "aero" e attualmente stiamo prendendo in considerazione le molte richieste che ci arrivano riguardo ad un nuovo round di nomi a dominio di primo livello "sponsored". Ritengo che abbiamo fatto un buon lavoro per quanto riguarda la protezione della stabilità di Internet e la sua sicurezza. Un altro punto chiave del nostro lavoro è stata l'introduzione di maggiori sistemi per la salvaguardia degli interessi dei consumatori: per citare solo due esempi, abbiamo introdotto quello che chiamiamo il periodo "di riscatto e di grazia" per quei consumatori che per un motivo qualsiasi non abbiano rinnovato la registrazione del nome a dominio. Ciò implica che una persona non perda il proprio nome a dominio solo perché si è dimenticata di pagare. Inoltre abbiamo lavorato sulla politica di trasferimento tra registrar, in modo che se un utente non è soddisfatto dei servizi offerti da un registrar possa trasferire il proprio nome a dominio ad un altro registrar. Questi sono solo alcuni esempi.

The new "eu" is round the corner: has ICANN a specific point of view about any other "regional" TLD to be adopted in the future?

First of all we are looking forward to concluding the arrangements for the launching of "eu". My understanding is that are still discussions and issues being worked through between the European Commission and the alliance of registries, which "it" is a member. But once that has been concluded, we are look forward to concluding the arrangements from our side. As far as, and we think that it would be a very important move, new TLD's regional level, there are we had no requests for such things and we have moved on "eu", as we recognise TLD's, country and regional TLD's from a list which is called the ISO 3166, a list maintained by the ISO. Our government works on that list so "eu" was activated from that list, we have not yet received any other sort of requests for regional cc's our regional Top Level domains and we haven't got a view on any other.

What are the best results gained by ICANN in the last years?

It's a good question. I think the first one is to establish a single place in the world where people involved with the issues around the domain name system and in IP addressing can come together and have the issues that affect them discussed and resolved.
We now have a single place to do that.
The second part of that is part of what we are doing now, we are just continuing to globalizing the language we operate, so for example, we have been in the European office in January, we found out the vice president is based in Europe, Mr. Paul Verhoef.
He was formerly within the Information Society Directorate at the European Commission. The other great, I think, things we've done, is first of all to introduce competition on the registrar market for the big generic top level domains "com", "net" and "org". the result of that has been an 80% price decrease to consumers, which is something like 1,5 billion Us dollars a year back to consumers in price of savings, we introduced seven new generic Top Level domain including sponsored Top Level domains like "coop", "museum", "aero" and we have a enterprises at the moment of a considering, we're receiving applications for a new round of sponsored Top Level domains.
I think that we've done good work when it comes to protecting the stability of the internet and also improving security of the internet. Other things that are important for us were introducing more systems for looking after for the interests of consumers, so there's two examples of that one is introducing what we call "redemption and grace" period for consumers who for one reason our another have fail to renew the domain name registration.
That just because you forget to pay your bill doesn't mean that you lose your domain name, and the others are we moved in is transfer of policy of between registrars, which that ensures if you're not happy with the service with one registrar, you can transfer the domain name to another registrar.
Here's some examples.

Il meeting di ICANN a Roma: l'impero di Internet sbarca nel vecchio continente

Intervista ai responsabili dei due enti che hanno organizzato l'evento: Franco Denoth, direttore dell'Istituto di Informatica e Telematica del CNR, e Claudio Corbetta, CEO Register.it, Gruppo DADA

Qual è il significato di ICANN in Italia?

Denoth: L'avere affidato l'organizzazione del meeting all'Italia è un riconoscimento del livello raggiunto da Internet nel nostro Paese. Se da una parte è vero che la diffusione dell'Internet a livello "domestico" è ancora non allineata allo sviluppo della cultura tecnologica (per esempio alla diffusione dei telefoni cellulari), è altrettanto vero che, da quando è stata liberalizzata la registrazione dei nomi a dominio per le persone giuridiche nel dicembre 1999, si è assistito ad una impennata del numero dei nomi a dominio sotto il ccTLD "it", che ci pone, oggi, tra i grandi registri mondiali.

Corbetta: Si tratta della prima volta in assoluto che tutta la comunità Internet internazionale si raccoglie qui in Italia: è un momento storico per il nostro Paese, da sempre un po' lontano dalla "stanza dei bottoni" per quanto riguarda il governo di Internet.
Durante il meeting di ICANN, privati ed aziende, oltre ovviamente a centri di ricerca e professionisti del settore, saranno coinvolti in riunioni mirate a favorire il rapido successo tecnologico di Internet e la sua continua evoluzione.
Sarà una grande opportunità di discussione in merito alle vie percorribili per rendere l'utilizzo di Internet realmente universale e un momento di promozione affinché il ruolo e la presenza italiani nello sviluppo di Internet si facciano più significativi

Qual è il Vostro ruolo in questo importante evento mondiale?

Denoth: Lo IIT mette a disposizione una notevole esperienza di organizzazione di eventi legati all'Internet; il ruolo storico e attuale dello IIT nelle reti telematiche e nella diffusione della "cultura informatica" gli hanno consentito di acquisire una capacità e competenza difficilmente riscontrabile in altri organismi. Di questo si avvantaggerà ICANN 2004.
Se l'Istituto saprà essere, come sono convinto sarà, all'altezza del compito, lo vedremo ad evento concluso.

Corbetta: Register.it S.p.A. è il primo registrar italiano accreditato da ICANN: da sempre partecipiamo attivamente ai vari meeting che si tengono nei vari continenti, con particolare riferimento alle sessioni aperte ai registrar, e ogni anno invitiamo un membro del Board di ICANN a partecipare alle giornate che la stessa Register.it dedica all'aggiornamento sui domini Internet a beneficio della comunità Internet italiana e di tutti gli interessati in genere.

The ICANN meeting in Rome: the Internet empire lands in Europe

Interview with the directors of the two bodies that have organised this event: Mr. Franco Denoth, director of the Institute of Informatics and Telematics of the Italian National Research Council, and Mr. Claudio Corbetta, CEO of Register.it, DADA Group

What does ICANN mean for Italy?

Denoth: Having entrusted Italy with the organisation of the meeting recognises the level that the Internet has attained in our country. Whilst it is true that the use of the Internet by families is not yet in line with the development of the technological culture (for instance, the use of mobile phones), it is also true that, since the domain name registration for legal persons has been liberalised in December 1999, there has been an upsurge in the number of domain names under the ccTLD "it", which today makes us one of the world's leaders.

Corbetta: It is the very first time the whole international Internet community will gather in Italy: it is an epoch-making event for our country, which has always been a bit far from the "nerve centre" of the Internet government.
During the ICANN meeting, individuals and companies as well as of course research centres and industry professionals will attend specific meetings aimed at boosting the quick technological success and the endless development of the Internet.
It will be a great opportunity to discuss the viable courses of action to make the use of the Internet really universal and a promotional opportunity for increasing the weight of the role and the presence of Italy in the development of the Internet.

What is your role in this important international event?

Denoth: IIT offers its great experience in the organisation of Internet events; the role that ITT did and does play in telematic networks and in the spreading of the "informatic culture" have given it such skills and know-how as hardly any other body can have.
This will benefit ICANN 2004.
If the Institute will be up to its task, as I am convinced it will, we will see it after the event.

Corbetta: Register.it S.p.A. is the first Italian registrar accredited by ICANN: we have always proactively taken part in the many meetings that are held all over the world, in particular in the registrars' sessions, and every year we invite one member from the ICANN Board to attend the workshops that Register.it organises to provide updated information on the Internet domains to the Italian Internet community as well as anyone that may be interested.

Due anni fa abbiamo presentato insieme al Registro Italiano la nostra candidatura ad ospitare qui in Italia il meeting di ICANN: abbiamo preparato un documento complesso che sintetizzava il progetto, le aspettative di spesa, le nostre idee in merito all'organizzazione generale dell'evento.
L'annuncio ufficiale della selezione della nostra candidatura è stato dato lo scorso marzo durante il meeting del Board di ICANN di Rio de Janeiro.

Si è parlato di "crisi di ICANN": cosa pensa se ICANN scomparisse?

Denoth: Ritengo indispensabile che esista un organismo operante a livello internazionale che sovrintenda alla conduzione di Internet, stabilendo e aggiornando le linee generali di sviluppo.
ICANN soffre dei mali che sono caratteristici di tutti i grandi organismi quando si trovano di fronte ad interessi e aspettative di più paesi, interessi, a volte, fra loro conflittuali.

Corbetta: Personalmente ritengo che la Rete che conosciamo oggi, governata com'è da ICANN, sia solo una delle Reti "possibili".
Premesso poi che Internet debba funzionare solo in presenza di standard unici, condivisi da tutti i Paesi, se ICANN scomparisse credo ci vorrebbe immediatamente un nuovo organismo internazionale con gli stessi compiti di coordinamento tecnico della Rete a livello globale e con lo stesso focus sulla risolvibilità universale degli indirizzi e sulla partecipazione di tutti i gruppi di interesse, commerciali e non.
In realtà la tecnologia per costruire nuovi network esiste già e se alcune nazioni non tollerassero più il coordinamento di Internet da parte di un organismo californiano quale è ICANN, avrebbero i mezzi per costruire ciascuno la propria Rete. Fortunatamente però questo rimane uno scenario altamente improbabile, soprattutto in considerazione degli interessi che oggi ruotano attorno ad una Rete globale, unica e universale. Ritengo che una Internet nazionale non avrebbe alcuna ragion d'essere per nessuno!

Come vede ICANN in Europa?

Denoth: ICANN ha recentemente aperto una sorta di "ufficio di rappresentanza" a Bruxelles. Il progredire dell'integrazione europea, l'avvento del TLD "eu" ne è un ulteriore –anche se modesto- segno, rende necessario un rafforzamento del peso dell'Europa in ICANN.

Corbetta: Credo che sia ormai giunto il momento per una più decisa assunzione di responsabilità da parte dell'Europa in tema di Internet Governance e in generale per un coinvolgimento più fattivo in materia di evoluzione delle nuove tecnologie.
Il mio auspicio è che l'Europa dimostri lo stesso impegno a favorire il rapido successo tecnologico di Internet e la sua continua evoluzione dimostrato sin qui dagli Stati Uniti.

Two years ago, we and the Italian Registrar stood as candidates to host the ICANN meeting here, in Italy: we drew up a far-ranging document that summarised the plan, the expected costs, our ideas on the general organisation of the event.
The official announcement that we had been selected was given last March at the meeting of ICANN in Rio de Janeiro.

Someone talked of a "crisis of ICANN": what do you think about the potential disappearance of ICANN?

Denoth: I think it is absolutely necessary to have a body that works on an international scale and supervises the running of the Internet by determining and updating its general lines of development.
ICANN is affected by the troubles that are typical of all large-scale bodies when they are have to address the interests and expectations of different countries, interests which sometimes clash with each other.

Corbetta: Personally, I think the network as we know it today, run as it is by ICANN, is just one of the "possible" networks.
Considering that the Internet should work only with common standards, shared by all countries, should ICANN disappear I think we would immediately need a new international body in charge of the same kind of technical co-ordination of the network on a global level and with the same focus on the universal solvability of addresses and on the involvement of all groups concerned, whether commercial or not.
In fact, the technology to set up new networks is already there, and should some countries be tired of having the Internet co-ordinated by a Californian body as ICANN is they would have the means to set up their own network.
Luckily though, this remains a highly unlikely scenario, especially considering the interests that hinge around a global, single and universal network today.
I think a national Internet would make no sense to anyone!

What do you think of ICANN in Europe?

Denoth: ICANN has recently opened a sort of "agency" in Brussels. The progress made in European integration, of which the coming of the TLD "eu" is one further – although modest- sign, make it necessary to strengthen the role of Europe within ICANN.

Corbetta: I think the time has come for Europe to take on more responsibility for Internet Governance and generally for a more factual involvement in the development of the new technology.
I hope Europe will prove to be as committed to boost the quick technological success and endless development of the Internet as the United States have proven to be so far.

ICANN ed i ccTLD: le sfide del futuro

Tim Mertens

All'inizio di marzo 2004 a Roma si svolgerà il primo meeting ICANN. Quindi, un'organizzazione molto giovane incontrerà una città molto antica: ICANN incontrerà la città eterna.
Nella sua lunga storia Roma ha assistito alla nascita e alla morte di diversi regni, ha visto periodi di guerra e periodi di pace e libertà. Roma è stata per secoli la sede di crudeli imperatori, così come oggi è la sede di pacifici papi.
All'interno della comunità interessata è noto che i registri dei ccTLD hanno un rapporto difficile con ICANN. In particolare lo scarso rendimento della funzione IANA ha offerto (e offre!) spesso l'opportunità di lamentarsi di questa essenziale funzione tecnica condotta all'interno di ICANN. Per i registri dei ccTLD questo è un servizio di estrema importanza.
I registri devono fare affidamento su un servizio veloce e sul fatto che le modifiche al database IANA sono effettuate in un lasso di tempo ragionevole ed estremamente breve. Si tratta di una questione essenziale alla base dell'erogazione del servizio ai clienti dei registri.
Diverse volte i registri membri del CENTR hanno riferito che una semplice modifica richiedeva più di due mesi. È stato riferito che durante il weekend non c'era nessuno rintracciabile allo IANA per le emergenze. È impensabile per noi che un'istituzione così importante non sia disponibile nel weekend o di notte.
Ci domandiamo anche se debba essere proprio lo IANA a detenere l'autorità di giudicare le richieste di modifiche nel database. Solo il gestore del ccTLD dovrebbe avere la responsabilità di fare richieste sul database e solo il gestore del ccTLD dovrebbe essere ritenuto responsabile se commette un errore.
Il gestore del ccTLD è responsabile solo nei confronti della sua Comunità Internet Locale, ma non nei confronti di qualcuno allo IANA. ICANN/IANA hanno diverse volte promesso di migliorare. Comunque, ci auguriamo che lo IANA sia portato avanti con performance di alto livello e per la soddisfazione di tutti. Abbiamo più volte richiesto dei processi automatici per la gestione delle richieste e lo IANA aveva promesso di lavorarci sopra. CENTR è impaziente di vedere la realizzazione dei processi promessi e la loro pubblicazione!
Fortunatamente il tempo delle lotte tra gladiatori è passato e gli scambi di opinioni e di idee avvengono in maniera più pacifica. CENTR si incontra a quasi tutte le Assemblee Generali (che si svolgono 4 volte all'anno) con i rappresentanti responsabili dell'ICANN/IANA instaurando con loro uno scambio fruttuoso e reciprocamente vantaggioso. Inoltre, gli incontri ICANN offrono ai nostri manager ccTLD e a CENTR stesso, rappresentato da parte dello staff, l'opportunità di affrontare diversi argomenti insieme a ICANN.
La nostra industria deve affrontare la crescente richiesta da parte della scena politica di essere coinvolta nelle questioni collegate ad Internet. Ciò non deve preoccupare ed è abbastanza naturale.

ICANN and the ccTLD's: new challenges ahead

Tim Mertens

At the beginning of March 2004 the first ICANN meeting in 2004 will take place in Rome. So a very young organisation meets a very old city – ICANN meets the eternal city.
In its long history Rome saw kingdoms raising and vanishing, Rome saw times of war and periods of peace and freedom. Rome was for centuries the seat of cruel Emperors as it is until today the stool for peaceful popes.
Within the interested community it is well known, that the country code registries have a difficult relationship to the body of ICANN. Notably the low performance of the IANA function gave (and gives!) often the opportunity to complain about this technical core function carried out in the ICANN framework.
For the country code registries this service is of utmost importance. Registries must rely on a fast service and that the changes in the IANA database are being made in a reasonable and utmost short timeframe. This is a basic question of service provision to the registries' customers.
At several and various times it was reported by CENTR members registries that a simple change took longer than two or more months.
It was reported that during the weekend there was no one reachable at IANA to provide an emergency service.
It lies out of our imagination capability that such an important institute in the Internet is away over the week-end or at night. Further we question, if it lies in the authority of IANA to give any judgement about a request of a change in the database. It should be the sole responsibility of the ccTLD manager to make requests of the database and only the ccTLD manager should be accountable for the consequences if he acts in error. The ccTLD manager is only responsible and accountable to his Local Internet Community – not to any person of IANA.
ICANN/IANA made at various times promises to improve. However, we hope that IANA will be carried out with a high level performance and to the satisfaction of all.
We asked several time for automation processes of how to handle requests and IANA promised to work on that. CENTR is looking forward to see the promised processes established – and published! Thankfully the time of gladiator fights is gone and the exchange of opinions and ideas take place in a more peaceful way. CENTR meets nearly at every General Assembly (which take place 4 times a year) responsible representatives from ICANN/IANA and have a fruitful and mutually beneficial exchange with them. Further on, the ICANN meetings gives our ccTLD managers as CENTR itself, represented by attending staff, the opportunity to discuss with ICANN on various issues.
Our industry faces an increasing demand of the political scene to become involved in Internet related issues. This is in the first instance not worrying and quite natural.

I ccTLD già oggi sono soggetti a molte norme, come le leggi locali, i diritti internazionali sulla privacy e molte altre legislazioni e la maggior parte dei registri del CENTR ha ottimi rapporti con il proprio governo e coopera con esso.
Tutti noi che lavoriamo nell'industria Internet siamo riusciti a dimostrare per anni di essere in grado di mantenere e conservare un Internet funzionante e solido.
È stato il settore privato a rendere Internet quello che è oggi.
La nostra vita sarebbe impensabile senza il settore privato, milioni di persone perderebbero il loro impiego e la ricchezza e la prosperità nazionale tornerebbero indietro ai tempi dell'antica Roma.
Tutti noi dovremmo essere orgogliosi di questo sviluppo e di essere riusciti a farne parte e di esserne ancora parte.
Abbiamo menzionato questi fatti perché si stanno verificando alcuni preoccupanti sviluppi che contraddicono l'approccio di autoregolamentazione.
Alcuni governi vogliono assumere il controllo di Internet tramite il processo del WSIS (il Summit Mondiale della Società dell'Informazione) ed esprimono un evidente supporto per un'organizzazione intergovernativa, presumibilmente con il supporto e sotto la protezione dell'ITU.
L'intero processo merita più ampie ed approfondite spiegazioni e considerazioni di quanto non sia possibile fare all'interno di questa newsletter.
Ma perché l'ho menzionato?
ICANN non è privo di difetti e deve ancora essere fatto molto per renderlo un'istituzione aperta, trasparente, affidabile ed apprezzata che meriti la fiducia di tutte le parti coinvolte in Internet.
Ma se facciamo riferimento alle tempeste che si stanno verificando sulla scena politica, potrebbe essere una scelta saggia unirsi a ICANN e votare per un approccio da settore privato e di autoregolamentazione.
Ma tutti noi dovremmo sapere cos'è in effetti ICANN.
La comunità di Internet sta iniziando a discutere su come vogliamo che sia ICANN e su cos'è ICANN: dovrebbe trattarsi di un'organizzazione internazionale di scarsa importanza, che si occupa soprattutto dello scambio di informazioni e che non interferisce troppo (o niente affatto) con la politica, oppure dovrebbe diventare una vera e propria organizzazione internazionale con una forte influenza sul GAC ed una forte capacità di sviluppare delle politiche vincolanti su scala globale?
Questa discussione deve avere luogo entro la prossima volta, ricordando che un'organizzazione governativa per Internet (guidata da ITU) probabilmente avrà degli effetti negativi sullo sviluppo di Internet e la creazione di un'organizzazione di questo tipo, con procedure decisionali lunghe, non trasparenti e complicate, cambierà in maniera sostanziale l'aspetto di Internet rispetto a come lo vediamo oggi.
Roma ha sopravvissuto a tutte le tempeste della storia, quindi siamo certi che anche Internet ci riuscirà.

The ccTLD's are already today subject to many regulations, like local laws and International privacy rights and various other legislations and most of CENTR registries have excellent relations to their governments and do co-operate with them.
We all, that are involved in the Internet industry have proven for years that we are able to keep and maintain a functioning and robust Internet.
It was the private sector that made the Internet to that what it is today.
Our life would be unthinkable without the technology we all invented – and we are permanently working on. Without a strong private sector, millions of people would loose their employment and the national wealth and prosperity will fall back to antique times of the ancient Rome. We all could be proud of that development and that were being able to be part of it – and we still are.
It is to point to these facts because some worrying developments contradicting the positive self regulating approach are coming up.
There are some governments that want to grab control over the Internet through the WSIS (World Summit on Information Society) process and they expresses clear support for an intergovernmental organisation – presumably with the support and under the umbrella of the ITU.
The whole process deserves longer and deeper explanations and considerations as it is possible within this newsletter.
But why do I mention that ?
ICANN is not flawless and still many steps must be undertaken to make it an open, transparent, reliable and well regarded institution that deserves trust from all parties involved in the Internet.
But with regard to the storms coming up on the international political scene it might be a considerable option to stand together with ICANN and for a private sector, self-regulating approach. But all of us must know of what ICANN in fact is about ?
The Internet community is beginning to discuss how we want to see ICANN and what ICANN is about: should it be a lightweight international organisation, mainly for information exchange and not interfering too much (or not at all) into politics or should it become a truly international organisation with a strong influence of the GAC and a strong capability to develop binding policies on a global scale ?
This discussion has to take place within the next time, bearing in mind that a (ITU driven) governmental Internet organisation – will presumably have detrimental effects on the development of the Internet and bearing in mind that the creation of such an organisation with lengthy, intransparent and complicated decision procedures will change the face of the Internet as we see it today in a fundamental way.
Rome survived all storms of history – so the Internet will certainly too.

Verso una rete più democratica

Comunicato stampa ufficiale al termine del meeting ICANN ROME 2004

Fra le decisioni più importanti la possibilità di registrare domini con caratteri di alfabeti non latini – dal 1 marzo in Germania già 600.000 le richieste di domini con la dieresi – e la creazione di un organismo dedicato allo sviluppo dei domini nazionali, la Country Code Name Supporting Organisation (ccNSO). Soddisfatti gli organizzatori, Register.it e l'Istituto di Informatica e Telematica del CNR: con più di 700 delegati presenti da tutto il mondo è il meeting di maggior successo nella storia di ICANN

Il 6 marzo 2004, si è chiuso a Roma il meeting mondiale di ICANN (Internet Corporation for Assigned Names and Numbers), l'organismo mondiale che governa la Rete su delega del governo americano.

L'evento, che si è tenuto per la prima volta in Italia, con l'organizzazione di Register.it, Gruppo DADA, e dell'Istituto di Informatica e Telematica del CNR, ha riscontrato un numero record di partecipanti: più di 700, in 27 differenti forum, fra rappresentanti della Comunità Europea e dei governi di tutti i continenti, utenti della rete e operatori del settore delle telecomunicazioni di vari paesi tra cui Giappone, Brasile, India e Australia.

Un'importante decisione comunicata alla chiusura del meeting è stata la costituzione della Country Code Name Supporting Organisation (ccNSO), un'organismo globale che riunirà tutti i ccTLD (country code Top Level Domain), cioè le estensioni relative ai singoli paesi (as esempio .it per l'Italia o .fr per la Francia). Si tratta di un significativo passo avanti verso un maggiore consenso internazionale su questioni al centro di dibattito da più di sei anni e verso una definizione sempre più globale dell'identità di ICANN, al di là della sua origine statunitense. Grazie a questa nuova entità sarà possibile stabilire procedure comuni e omogenee per tutti i ccTLD, eliminare gli ostacoli burocratici e, più in generale, favorire lo sviluppo dei domini nazionali, accanto alle estensioni gTLD (generic Top Level Domain) più "americane" quali .com, .net. e .org.

Risponde allo stesso spirito di maggiore democratizzazione anche la decisione di rendere possibile la registrazione di domini con caratteri diversi da quelli degli alfabeti latini (il cirillico, l'arabo, ma anche il tedesco per via della "umlaut" o dieresi), mentre fino ad oggi erano validi solo i caratteri dall'A alla Z. Proprio la Germania dà il segnale del successo che sta riscuotendo questa opportunità: sono già 600.000 la richieste di domini con la dieresi.

Towards a more democratic Net

Official Press Release after the ICANN ROME 2004 meeting

One of most important decisions was to offer the opportunity to register domains with non-Latin characters– since March 1st in Germany as many as 600,000 applications for domain names with diereses – and the establishment of a special Committee for the development of national domains, the Country Code Name Supporting Organisation (ccNSO). The organisers, Register.it and the Institute of Informatics and Telematics of the Italian National Research Council were extremely satisfied: with over 700 delegates from all over the world, it was the most successful meeting in ICANN's history.

The international meeting of ICANN (Internet Corporation for Assigned Names and Numbers), the international body appointed by the US Government to run the Internet, closed in Rome on March 6th, 2004.

The event, which took place in Italy for the first time, organised by Register.it, DADA Group and the Institute of Informatics and Telematics of the Italian National Research Council, was attended by a record-breaking number of delegates: over 700, in 27 different forums, including representatives from the European Community and from the governments of every continent, Internet users and telecommunication operators from many countries, including Japan, Brazil, India and Australia.

An important decision announced just before closing the meeting was the establishment of the Country Code Name Supporting Organisation (ccNSO), an international body that is going to bring together all ccTLDs (country code Top Level Domains), i.e. country extensions (for instance, .it for Italy or .fr for France). It is a great step forward, in the attempt to build more international consensus on issues that have been debated for over six years and to give an increasingly global definition to ICANN's identity, one that may go beyond its US origin. This new body will help develop common standard procedures for all ccTLDs, remove bureaucratic hindrances and generally support the development of country domains, along with such more "American" gTLD (generic Top Level Domain) extensions as .com, .net. and .org.

In the same attempt to move towards wider democratisation, they also decided to offer the opportunity to register domains with characters other than the Latin alphabet (Cyrillic, Arab as well as German because of its "umlaut" or dieresis), while only A to Z characters had been allowed so far. And it is Germany that shows how successful this new opportunity has been so far: 600,000 applications for domains with diereses have already been submitted.

Per quanto riguarda invece la designazione di un nuovo operatore autorizzato a registrare i domini con estensione .net, succedendo a Verisign, attuale gestore del registro del .net, è stato stabilito che ICANN avvierà una formale procedura per la definizione di tale successore entro il 30 giugno del 2004 e che Verisign stessa è rieleggibile in tale ruolo.
In fase di risoluzione inoltre la diatriba fra ICANN, Verisign e gli altri operatori del mondo dei domini, riguardo la liceità del Waiting List Service (WLS), il servizio creato da Verisign per mettere in una lista d'attesa (a pagamento) gli utenti interessati a registrare domini eventualmente non rinnovati dai titolari alla scadenza.
A tale proposto il Consiglio di Amministrazione di ICANN ha approvato i risultati della negoziazione con Verisign riguardanti lo sviluppo del Waiting List Service.
Fra le presenze illustri al meeting, il Ministro per l'Innovazione e le Tecnologie, Lucio Stanca, che, rivolgendosi durante il Public Forum ai partecipanti e agli organizzatori ha riconosciuto, a nome del Governo italiano, il ruolo che ICANN svolge nello sviluppo e nella crescita di Internet, soprattutto con riferimento al compito cruciale di assicurarne la stabilità tecnica.

As to the appointment of a new .net domain registry operator to replace Verisign, the current .net registry operator, it was decided that ICANN should open a formal procedure to appoint such successor by June 30th 2004 and that Verisign itself can be re-elected.
In addition, the controversy between ICANN, Verisign and other domain operators regarding the legitimacy of the Waiting List Service (WLS), the service developed by Verisign to put on a waiting list (for a fee) those users who are interested to register any domain that should not be renewed by their holders on their expiration, is heading to a close.
In this respect, ICANN's Board of Directors approved the results of negotiations with Verisign on the development of the Waiting List Service.
The illustrious guests of the meeting included Lucio Stanca, Minister of Innovation and Technology, who, on addressing the participants and the organisers at the Public Forum, recognised, on behalf of the Italian Government, the role that ICANN plays in the development and in the growth of the Internet, with special reference to the vital task of guaranteeing its technical stability.

Al servizio dell'utente, al servizio di se stessi: le implicazioni della "cura del cliente"

Enrica Poltronieri

Se ci è capitato, come utenti/clienti di un servizio, di rivolgerci ad un operatore ponendo una richiesta e sentendoci rispondere "Non saprei…", "Non è di mia competenza…"; conosciamo l'effetto indisponente di sentirsi non aiutati, lasciati in balia del nostro problema o, peggio, percepiti come seccatori. E sappiamo anche di esserci costruiti un'immagine negativa dell'organizzazione a cui ci eravamo rivolti.
Questo può avvenire perché non in tutti gli ambiti si è sviluppata omogeneamente una forte ed attenta cultura del servizio. Attualmente "essere al servizio" (e già lessicalmente l'espressione non ci piace perché rimanda all'idea di subordinazione) dell'utente richiede alta professionalità e competenza, perché su questo aspetto e sulla capacità di farlo recepire all'utente si gioca la differenziazione tra le organizzazioni e chi è maggiormente in grado di esprimere qualità si garantisce un vantaggio competitivo.
Ma che cosa in fondo richiede l'utente?
L'utente si rivolge ad una organizzazione con un bisogno, una necessità, una preoccupazione e si aspetta in primo luogo che il suo interlocutore se ne faccia carico, comprenda e assuma su di sé la richiesta.
Si aspetta anche, e ne valuterà il risultato, che un'organizzazione gli metta a disposizione, attraverso gli operatori con cui entra in contatto, competenza, sicurezza, affidabilità e capacità di portare a risoluzione quanto richiesto.

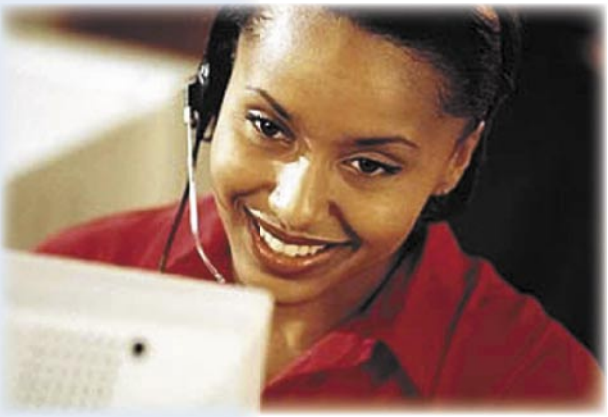
Serving a user, serving yourself: "customer care" implications

Enrica Poltronieri

In case it ever happened to you, as a user/client of a service, to ask an operator a question and have this person answer "I don't know…", "It is not my area…", you know the off-putting effect of not being helped, left at the mercy of our problem or, worst of all, being treated as a bother. We also have a negative image of the company we apply to.
This can happen because not all environments have homogeneously developed a strong and diligent culture of service.
Nowadays, "to attend to" a customer (and we don't like this expression from a lexical point of view because it refers to the idea of subordination) calls for high standards of professionalism and skill, because this aspect and the ability of making the customer understand he plays a key role in the diversification of the organizations and the capability in expressing quality, secures a competitive benefit.
But after all, what does a customer really ask for?
A customer applies to an organization with a need, a requirement, a concern and, first of all, expects the person they are talking to take on all the responsibilities, understand and personally take care of the request.
They also expect an organization to deliver through the operators they contact: skills, safety, reliability and problem solving, and, in the end, they will weigh the result.

CUSTOMER CARE MANAGEMENT

Che cosa, inoltre, osserverà l'utente? Noterà se è stato facile, rapido mettersi in contatto con l'organizzazione, se ha avuto interlocutori gentili, cortesi.
Noterà se la persona con cui ha parlato l'ha messo in grado di capire bene, è stata chiara, è stata paziente.
Rileverà molto se c'è stata rapidità nel risolvere quanto richiesto o se ha dovuto sopportare tempi lunghi, sollecitare, richiamare.
In altre parole ogni organizzazione che eroga un servizio deve mettersi in grado di non solo di gestire al meglio l'aspetto tecnico del servizio, ma di curare la relazione con i clienti. L'obiettivo è quello di fare in modo che l'utente percepisca, colga, rilevi l'attenzione complessiva con cui è considerato e trattato.
Questo vuol dire rendere visibile, esplicita la cura di cui è oggetto.
Significa anche che non ci si può accontentare di saper rispondere alla richiesta nella pratica.
Il "come" lo si fa , non solo il "che cosa" si fa, importa all'utente.
Si tratta cioè di combinare strategie di "customer service" e strategie di "customer care".
Per ottenere questo risultato è irrinunciabile la qualità "relazionale" che gli operatori a contatto con l'utente mettono nel proprio lavoro.



Le capacità di entrare in contatto positivamente con utenti diversi, di gestire situazioni o persone "difficili" mantenendo alta la disponibilità e l'attenzione richiedono competenze relazionali elevate, che si avvalgono della sensibilità della persona, ma non si limitano a questo.
È importante che chi gestisce il contatto con l'utente sappia come fare, come procedere anche nelle situazioni più delicate, come trasmettere l'immagine positiva della propria organizzazione sempre.
Siamo su un terreno dove sono in gioco da parte sia del cliente, sia dell'operatore emozioni, stati d'animo, ansie, preoccupazioni, che possono limare la lucidità con cui si affrontano le situazioni.
Ma è proprio nell'interazione utente-operatore che si crea la qualità del servizio.
Se l'operatore sa come gestire il cliente, è tranquillo sulla propria capacità professionale e relazionale, riconosce di avere un obiettivo ed un interesse comune con l'utente (chiudere positivamente il contatto), la situazione procederà verso una conclusione positiva per entrambi.L'operatore potrà sentirsi soddisfatto di aver "guidato" il dialogo, sperimenterà gratificazione e autostima, rafforzerà l'immagine personale e professionale.
Il cliente si confermerà l'immagine positiva dell'organizzazione a cui si è rivolto, si rivolgerà ancora con fiducia la prossima volta (sarà un cliente migliore, pieno di attese positive).
Quindi: "In che cosa posso esserle utile?"

What else does a user notice?
The user notices how easy and fast it was to get in touch with the organization and furthermore how kind and polite the person they speak to is.
They notice if the person they spoke to enabled them to understand in a clear and patient manner.
The speed in handling the request or the long wait, the urging and the calling back become of great prominence.
In other words, each organization which offers a service must be able to not only manage the technical aspect of the service in the best possible way, but also take care of relations with their customers.
The aim is to make the user understand, notice and be aware of the overall care used to treat them.
This means that the extent of user care must be clearly and explicitly expressed.
This also means that you can't be content with simply answering the request.
It's "how" you do it, not only "what" you do, that is important for the user.
It's all about combining "customer service" and "customer care" strategies.
In order to obtain this result, the "relational" quality, adopted by the operators who are in contact with the users, is irremissible.
The skill of establishing a positive contact with several clients and of handling "difficult" situations and people and at the same time, keeping a high-level of availability and care, call for outstanding relational ability, which makes use of the person's sensitivity, but is not restricted to this.It is important that who is in contact with the user know what to do, how to deal with delicate questions, how to always convey a positive image of their organization.
We are in a field where both the client's and the operator's emotions, moods, anxieties, concerns, which can gnaw at the clearness needed to face the situations, are at stake.
But it is exactly this user-operator interaction, which creates the quality of the service.
If the operator knows how to handle the client, and doesn't worry about his/her own professional and relational ability, understands he/she shares the user's common aim and interest (to end the contact positively), the situation will proceed towards a positive ending for both of them.
The operator will be satisfied about having "guided" the dialogue, will experience satisfaction and self-esteem, and will strengthen his/her personal and professional image.
The client will confirm the positive image of the organization he/she contacted, and will contact it again with trust (will be a better client, with positive expectations).
Therefore: "How can I help you?"

Uno sguardo ai Customer Care di alcuni provider maintainer

Aruba.it – TECHNORAIL-MNT

Aruba.it offre assistenza ai propri clienti utilizzando tutte le forme possibili di contatto. In particolare, oltre al canonico supporto via e-mail, viene usato in modo innovativo il support via Forum che, includendo anche la community dei clienti, offre sia l'assistenza diretta del nostro Staff, sia la possibilità di interagire con altri clienti per approfondire temi che esulano dal mero supporto tecnico. In questo modo il nostro forum diviene una sorta di grande knowledge base dinamica, che si aggiorna e cresce con le segnalazioni dei clienti stessi e relative risposte.
Inoltre le sezioni FAQ e Vademecum contengono domande-risposte e guide specifiche calibrate sulle richieste ricorrenti; entrambe le sezioni prevedono un comodo motore di ricerca.
È infine disponibile un tradizionale Call Center telefonico per dare rapido supporto sulle problematiche commerciali-amministrative e per lo smistamento delle richieste tecniche che trovano collocazione sul forum o risposta in FAQ e vademecum.
Lasciare consultabile pubblicamente tutto il forum di Assistenza, la community dei clienti, le guide sul vademecum e le FAQ dimostrano la politica di grande trasparenza adottata da Aruba.it e questo è nel panorama dei servizi ISP un elemento distintivo e precursore. Questo sistema è stato adottato da più di 3 anni e ha dato ottimi risultati sia in termini di soddisfazione dei clienti che di ottimizzazione delle risorse destinate al customer care.

Register.it – REGISTER-MNT

Sono 15 gli operatori che forniscono assistenza tecnica ai clienti di Register.it S.p.A.: hanno una media di 27 anni, vengono da tutta Italia (ma ci sono anche due operatori di nazionalità spagnola e polacca), appartengono in netta prevalenza al gentil sesso (10 donne contro 5 uomini), vantano un'anzianità in Register.it di oltre due anni, coprono turni su 12 ore (dalle 8 del mattino alle 20) e ricevono una media di 400 contatti al giorno per complessivi 2200 contatti settimanali. Le risorse del Customer Care di Register.it operano in piccoli team dedicati a specifici prodotti (domini, email, hosting) e distinti per tipologia di problemi (tecnici, amministrativi, commerciali): ciascun operatore è leader di un team e contemporaneamente parte integrante di un altro per una migliore responsabilizzazione del gruppo.
Grazie al potenziamento dell'assistenza tecnica via email – con priorità accordata alle email dei clienti che scrivono da pannello di controllo tramite il link "richiedi assistenza" – gli operatori del Customer Care di Register.it riescono a prendere in carico tutte le richieste dei clienti entro le 8 ore successive alla richiesta stessa. Contribuiscono ad una sempre migliore efficacia del Customer Care di Register.it anche le riunioni settimanali di condivisione delle varie criticità e i corsi di aggiornamento organizzati su base mensile sia dalla struttura Marketing che da quella IT di Register.it a beneficio di ciascun operatore del Customer Care.

A quick glance at some provider maintainer's Customer Care Services

Aruba.it – TECHNORAIL-MNT

Aruba.it offers its service to clients by means of any type of contact.
In particular, in addition to the traditional email support, an innovative Forum support is used which offers direct service by our Staff and the possibility to interact with other clients in order to analyse subjects which differ from sheer technical support. This is how our forum becomes great knowledge with a dynamical base, which updates and grows through the client's reports and feedback.
Furthermore, the FAQ and Vademecum sections contain questions-answers and detailed guides on recurring requests; both sections have a useful search engine.
There is a traditional telephone Call Center available for fast support in commercial-administrative problems and in the sorting of technical requests, which can be found in the forum or answered to in the FAQs and vademecum.
Letting the public consult all the Service forum, client's community, vademecum and FAQ guides underlines the policy of great clearness adopted by Aruba.it and this is, in the survey of ISP services, a distinguishing and unprecedented factor.
This system has been used for over three years and has produced great results both in terms of client's satisfaction and optimisation of the resources assigned to customer care.

Register.it – REGISTER-MNT

15 operators provide clients of Register.it S.p.A. with technical assistance: they are 27 years old on an average, they come from all over Italy (but there is also 1 Spanish and 1 Polish operator), they mainly belong to the fair sex (10 women against 5 men), they can boast an over two years' experience with Register.it, they cover a 12 hour shift (from 8 in the morning to 20 at night) and they receive an average of 400 contacts per day for an overall of 2,200 contacts per week.The Customer Care human resources of Register.it operate in small teams and take care of specific products (domains, e-mails, hosting) and are distinguished by type of problems (technical, administrative, commercial): each operator is a team leader and at the same time is part of another team in order to make the group more responsive.
Thanks to the development of technical assistance via e-mail – giving priority to the e-mails of clients who write from a control panel through the "ask for assistance" link – the Register.it Customer Care operators can take care of all the client's requests within 8 hours from the request.
Weekly meetings of problem sharing and refresher courses organized by both the Marketing and IT organizations of Register.it, on a monthly basis, for all Customer Care operators, help improve the efficiency of Regiter.it's Customer Care.

Oltre all'assistenza "day by day", gli operatori del Customer Care aggiornano una completa sezione del sito www.register.it dedicata alle domande più frequenti relative ai vari servizi, il forum di assistenza tecnica in cui inseriscono le risposte ai quesiti posti e già risolti da altri clienti e uno specifico forum legale sui domini internet.

Wind – IUNET-MNT

La Wind Telecomunicazione SPA nasce nel 1997 da un'iniziativa di ENEL, France Telecom e Deutsche Telecom. Nel 2001 Wind tramite Enel acquisisce INFOSTRADA con tutte le sue strutture.
La nuova WIND viene divisa in :
TELEFONIA FISSA (con circa 7 milioni di clienti)
TELEFONIA MOBILE (con circa 7,7 milioni di clienti)
INTERNET (con circa 8,4 milioni di clienti)
Bisogna tenere presente che gli strumenti utilizzati dal customer care sono:

- il telefono: che è il mezzo più utilizzato per creare un contatto diretto ed è indispensabile per risolvere problemi in breve tempo;
- l'e-mail: mezzo ancora poco usato in quanto molti cliente trovano le e-mail tendenzialmente impersonali e non danno ancora piena garanzia che il messaggio sia stato recapitato.

Un recente studio ha stabilito che la posta elettronica ha comunque sorpassato il telefono come strumento di comunicazione d'affari.
Per dare un servizio completo ai nostri clienti il customer care è diviso in due grandi rami in base al tipo di clientela ed a sua volta ogni ramo viene diviso per tipo di fonia e per problema. Complessivamente le persone che svolgono l'attività di customer care sono 2400 circa in totale sparse su tutto il territorio nazionale.

Tiscali – TISCALI-MNT

Il Servizio Clienti di Tiscali è articolato in tre unità organizzative:
Help Desk Tecnico (HDT): offre supporto tecnico per la configurazione e l'utilizzo di tutti i prodotti e servizi Tiscali, dagli abbonamenti Internet ai servizi telefonici, e aiuta i clienti nella gestione del dominio e dello spazio web ad esso collegato.
Front End (FE) : gestisce i contatti con i clienti, fornendo informazioni su prodotti e servizi Tiscali, sugli abbonamenti sottoscritti e sul loro stato di attivazione.
Back Office (BO): svolge attività specialistiche come la verifica e registrazione degli abbonamenti, le modifiche contrattuali, e fornisce informazioni relativamente alla fatturazione e ai pagamenti.
Il Servizio Clienti Tiscali è raggiungibile:

- al numero 130 (gratuito per le chiamate provenienti da rete fissa);
- compilando il modulo on line all'indirizzo ***http://assistenza.tiscali.it/supporto/***

In addition to "day by day" assistance, Customer Care operators update a complete section of the site www.register.it dedicated to all the most frequently asked questions about various services, the technical assistance forum where they enter the answers by other clients to already solved problems and a specific legal forum about internet domains.

Wind – IUNET-MNT

Wind Telecomunicazione SPA was established in 1997 on the initiative of ENEL, France Telecom and Deutsche Telecom. In 2001 Wind acquired INFOSTRADA through Enel with all its facilities.
The new WIND is divided into:
LANDLINE TELEPHONY (with approx 7 million clients)
MOBILE TELEPHONY (with approx 7.7 million clients)
INTERNET (with approx 8.4 million clients)
WE must bear in mind that the instruments used by customer care are:

- The telephone: which is the means of communication mostly used in order to create direct contacts and is essential for problem solving in a short-term;
- The e-mail: which is a means of communication still not largely used because many clients find e-mails basically impersonal and find that they do not fully guarantee message delivery.

A recent research has established that e-mails have, however, outweighed the telephone as a tool for business communication.
In order to offer our clients a full service, customer care is divided into two big areas, according to the kind of clients and in its turn each field is divided into subclasses according to phonic standards and type of problems. The people who carry out customer care are altogether approximately 2400 nationwide.

Tiscali – TISCALI-MNT

Tiscali Customer Care is divided into three organizational units:
Help Desk Tecnico (HDT) – Technical Help Desk: gives technical support for the configuration and use of all Tiscali products and services, from Internet subscriptions to telephone services, and helps clients to run their domain and related web site.
Front End (FE): takes care of client contacts, giving information about Tiscali products and services, subscriptions and their activation status
Back Office (BO): carries out specialized activities such as the check and registration of subscriptions, amendment of contracts, and provides information on invoicing and payments.
Tiscali Customer Care can be contacted:

- By dialling 130 (free for all incoming landline calls);
- By filling in the on-line form at ***http://assistenza.tiscali.it/supporto/***

Tuonome – TUONOME-MNT

Come per tutti i Registrar che fanno alti volumi con procedure di registrazione on line o via gateway, il mantenimento di un servizio call center adeguato costituisce uno dei principali sforzi dell'intera organizzazione, ma è al contempo un elevato valore aggiunto.Il servizio call center di Tuonome.it è strutturato su 3 livelli: registrante individuale, dealer (rivenditore), registrar outsourcing.
Il registrante individuale o cliente diretto ha accesso al customer service prevalentemente via e-mail, ma può anche interagire con il nostro staff tramite numeri pubblici via telefono e fax . Il personale addetto all'help-desk è in grado di fornire assistenza al cliente in 6 lingue:
Italiano, Inglese, Francese, Tedesco, Spagnolo e Olandese, esigenza ormai molto forte in Tuonome.it in considerazione del proprio parco clienti sempre più internazionale, grazie anche al progetto TuonomeGroup.com.
Il nostro Dealer autorizzato sin dall'ottobre del 2002, può utilizzare i metodi di contatto sopra citati ma può anche avere accesso ad un servizio telefonico su richiamata (denominato "help-desk on demand"), attivabile con estrema semplicità tramite un' apposita area nel sito web ad essi riservato.
Solitamente entro fine mattinata, da parte dello staff, vengono evase tutte le richieste pervenute nella notte e nel corso del mattino, mentre entro le 18:30 trovano risoluzione tutte le richieste ricevute dopo le 12:30.
Questo servizio ha, sin dall'inizio, registrato notevoli consensi; il nostro operatore, grazie alla presa visione della "motivazione di contatto" che il nostro Dealer deve includere nella form di richiesta, sarà di fatto il soggetto con le competenze specifiche necessarie. Infine, ma non in ordine di importanza né di complessità, in Tuonome.it e TuonomeGroup.com, vi sono servizi call center con numeri e operatori dedicati per singole contrattualizzazioni di Registrar Outsourcing.
Si tratta in questo caso, di un servizio Helpdesk prevalentemente tecnico su problematiche legate a nomi a dominio, ma più in generale a problematiche annesse al DNS. Tale servizio viene erogato direttamente ai registranti di nomi a dominio, ma in nome e per conto del nostro committente (intestatario del contratto Registrar Outsourcing).
Lo staff dell'help-desk opera in questi casi sulla base di procedure preventivamente concordate tra Tuonome.it e l'entità che ha scelto i nostri servizi outsourcing, il tutto in funzione di una gestione personalizzata del parco clienti di quest'ultimo.

Telecom Italia – TIN-MNT

I clienti possono rivolgersi al nostro Customer Care multimediale tramite Numero Verde 80 33 80 o i canali web (e-mail, chat o Voice Over IP) o un sito d'assistenza ***http://help.virgilio.it*** ricco di contenuti e informazioni per utilizzare al meglio il proprio abbonamento ad Internet.
In particolare, le richieste di assistenza tecnica ricevute sono evase in linea con il cliente (1° livello) o, nei casi più complessi, attraverso strutture di back office (2° livello), che nell'eventualità possono richiedere l'intervento di un tecnico del "Gestore della Rete" (TI Wireline).

Tuonome – TUONOME-MNT

Like all Registrars which work with a large volume of on-line or gateway registrations, the running of an adequate call center is one of the main efforts the entire organization makes, but, at the same time, becomes a high added value.
Tuonome.it's call center service has a 3 level structure: individual registrant, dealer, registrar outsourcing.
The individual registrant or direct client has access to customer service mainly via e-mail, but can interact with our staff by means of landline numbers and fax.
Help Desk staff are able to assist customers in 6 languages:
Italian, English, French, German, Spanish and Dutch, an important requirement for Tuonome.it in view of more and more international customers, thanks to the TuonomeGroup.com project.
Since October 2002 our authorized Dealer can use the above mentioned contact methods but can also access a call-back telephone service (called "Helpdesk on Demand"), which can be easily activated in the special web site area we use for it.
By the end of the morning, our staff usually handle all the incoming night and morning requests, while by 18:30 they take care of all the requests received after 12:30.
Since it started, this service has achieved widespread success; our operator, thanks to the "contact reason" area which our Dealer must put in the request form, becomes a person with the specific skills needed.
Finally, but of no less importance or complexity, in Tuonome.it and TuonomeGroup.com there are call center services with telephone numbers and operators just for individual contracts of Registrar Outsourcing.
This is a predominant technical Helpdesk service, which takes care of domain name problems, but generally of DNS problems.
This service is granted directly to domain name registrants, but on behalf of our customer (holder of the Registrar Outsourcing contract).
The helpdesk staff, in this case, work according to procedures agreed upon in advance between Tuonome.it and the company who has picked our outsourcing service, all this happens to serve the purpose of a custom-made administration of the company's clients.

Telecom Italia – TIN-MNT

Clients can contact our multimedia Customer Care through the free phone number 80 33 80 or the web (e-mail, chat or Voice Over IP) or the assistance web site ***http://help.virgilio.it*** full of information which can help you use your Internet subscription in the best of ways.
In particular, the technical assistance requests we receive are taken care of directly with the client (first level) or, in the most complicated cases, by means of back office structures (second level), which can ask for technical support directly by "TI Wireline".

Per l'evasione delle segnalazioni, gli operatori del customer care dispongono di strumenti dedicati di diagnosi / intervento e di procedure specifiche per tipo di guasto diagnosticato (connessione, navigazione, posta elettronica, ecc); inoltre utilizzano un sistema di trouble ticketing per tracciare i contatti dei clienti e l'esito delle verifiche effettuate.
I tempi standard (obiettivo) per l'evasione delle segnalazioni dei clienti sono di 2 giorni (solari) nel 92% dei casi .
Anche per l'assistenza dei clienti che utilizzano i nostri servizi di Hosting, esistono 2 livelli di gestione del contatto. Il primo livello gestisce tutte le chiamate provenienti al numero verde, cercando di fornire una soluzione adeguata, sia commerciale che tecnica. Nel caso in cui la complessità della soluzione lo richiedesse, il problema viene passato, tramite segnalazione interna, al secondo livello che, utilizza conoscenze specialistiche e strumentazioni più avanzate.
Il secondo livello oltre a gestire le segnalazioni interne, si occupa anche di trattare le richieste provenienti, via e-mail, dai clienti e tutte le mail provenienti dal Registro per la registrazione dei domini di secondo livello.

Asiacom – ASIACOM-MNT

Alla base di una buona gestione di un servizio come quello di un call-center ci sono due elementi qualificanti: il tempo e l'efficacia della risposta. Chi telefona è tipicamente qualcuno che non ha tempo da perdere e/o che non conosce la risposta alla sua domanda. Entrambe le cose, anche se banali, spesso non sono sufficientemente prese in considerazione.
Questa esperienza/obiettivo ci ha guidato nell' allestimento del nostro servizio.
Il tempo è legato al dimensionamento del servizio, anche se non sempre è facile trovare il giusto compromesso. Utilizzare poche linee telefoniche con un elevato numero di clienti/utenti ha come unico (spiacevole) risultato quello di una lunga attesa, al limite addolcita da qualche canzoncina. Nel nostro caso l'esperienza ci ha portato a dedicare due/tre persone a questo servizio, debitamente formate e supportate, eventualmente, da personale tecnico per le domande più specifiche.Qui si inserisce l'altro elemento fondamentale: l'efficacia della risposta.
Chi fa una domanda non conosce in anticipo la risposta. Nasce la necessità di essere chiari ed il modo migliore è quello di guidare praticamente il cliente nella soluzione del problema. Non è sufficiente descrivere le operazioni che dovrà compiere: chiamerà di nuovo il nostro centralino, il che non è un bene né per lui né per noi. Oltre a ciò, è fondamentale costruire una casistica delle domande che principalmente vengono rivolte. Questo si costruisce sul campo e nel tempo, ma permette di rispondere velocemente e bene, essendo il problema già stato risolto per situazioni analoghe.
Tale casistica si potrà anche rendere disponibile sul Web, per ridurre in futuro il numero delle "chiamate evitabili", anche se, nonostante le avvertenze in proposito, quasi nessuno legge le FAQ di un sito.
L'ultimo aspetto, non meno importante degli altri, è la pazienza. Ma questa è una virtù umana che spesso non dipende solo dall'operatore e non è facile né da insegnare né da mantenere dopo la ventesima volta consecutiva che si risponde alla stessa domanda. L'importante è, almeno, sforzarsi.

In order to take care of the requests, customer care operators use diagnosis / intervention tools and specific procedures according to the diagnosed problem (connection, surfing, e-mail, etc.); in addition to this, they use a troubleshooting system in order to trace the clients' contacts and follow up the results of the checks.
In 92% of the cases, the average time it takes to solve clients' problems (target) is 2 days (48 hours).
Customer Care, for those who use our Hosting services, is also divided into 2 different levels of contact.
The first level receives all the free phone calls, trying to give the right solutions, both commercial and technical.
In case the solution is of a certain extent of complexity, the problem, through an in-house report, is passed on to the second level which uses specialised knowledge and advanced tools.
The second level not only takes care of in-house reports but also tackles all the clients' requests via e-mail and all the e-mails from the Registry for the registration of second level domains.

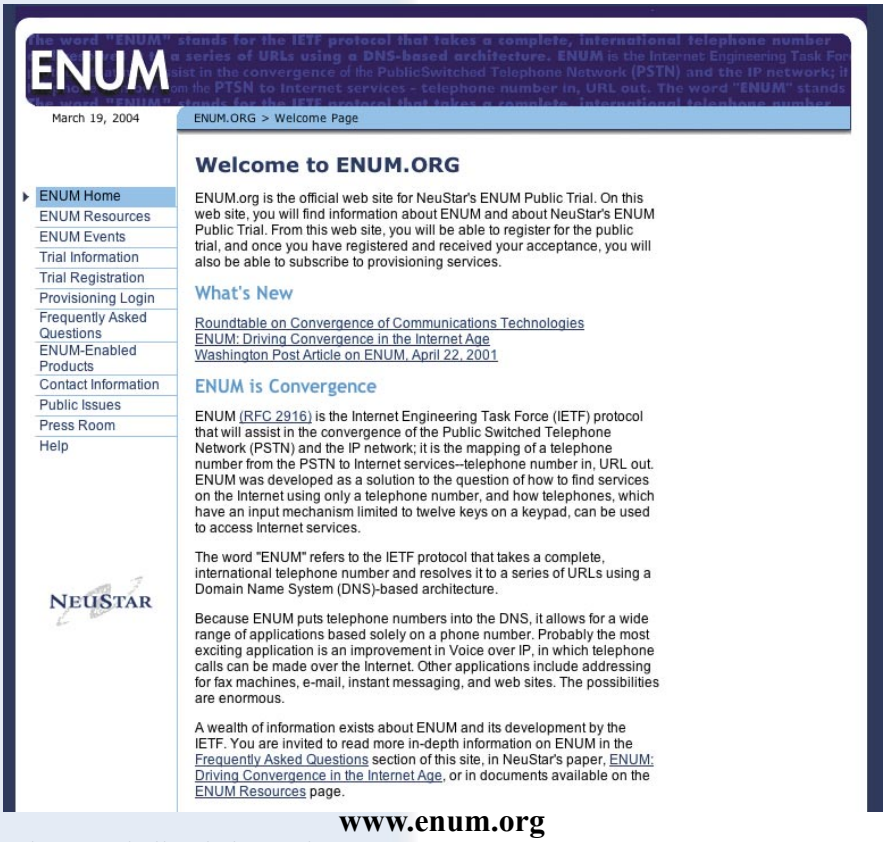
Asiacom – ASIACOM-MNT

There are two qualifying elements behind a good management of such a service as a call centre: time and the effectiveness of the answer. Those who telephone are usually people with no time to waste and/or who do not know the answers to their questions. Both things, although obvious, are often underestimated. This experience/objective is what led us to set up our service.
Time has to do with the size of the service, even if it is not always easy to find a good compromise. Using few telephone lines with a high number of customers/users delivers the only (unpleasant) result that people on the other end of the line have to wait for a long time, at most calmed down by some nice song. In our case, experience has led us to assign two/three people specifically to this service, duly trained and assisted as needed by technical staff for the most specific questions.
Here comes the other essential element: the effectiveness of the answer. Those who ask a question do not know the answer yet. Hence the need to be clear, and the best way to do this is to really guide the customer through the problem-solving process.
Describing the operations that the customer has to carry out is not enough: the customer will call the centre again, which is not good either for him or for us.
Besides this, it is essential to set up a record of the most frequently asked questions. This is built up on the field and with time, but it is a useful means to answer quickly ad effectively, since the problem has already been solved in similar circumstances.
Such case record could also be available on the web to reduce the number of "avoidable questions", even if despite the notice virtually nobody ever reads the FAQs on a web site.
The last but not least important aspect is patience. But this is a human virtue that often does not depend on the operator only and that cannot be easily taught or kept when one has to answer the same question for the twentieth time on end. The important thing is to make an effort, at least.

ENUM: la nuova frontiera della rete

a cura di Guglielmo Grisley e Giovanni Tortora, amministratori del Sistema NPTS (Number Portability Tracking System) e rispettivamente Vice Relatore Nazionale della Commissione 2 dell'ITU-T e Relatore Nazionale della stessa

La sempre maggiore convergenza tra la rete telefonica e la rete Internet, nonché la crescita esponenziale degli utenti internet, ha spinto la comunità scientifica a sviluppare un nuovo protocollo, specificatamente orientato alla convergenza tra la rete PSTN (la rete telefonica pubblica) e la rete IP (Internet).
L'Internet Engineering Task Force (IETF) e più specificatamente il gruppo di lavoro "Telephony Number Mapping" ha definito un nuovo protocollo, chiamato "ENUM", che costituisce il vero punto di congiunzione tra la rete telefonica e il web, permettendo l'associazione tra un numero telefonico E.164 (piano di numerazione internazionale) ed un indirizzo IP.
Questa soluzione consente agli utenti di utilizzare un singolo numero per accedere a molteplici servizi, quali telefonia fissa e mobile, fax, e-mail, telefonia su IP e Internet.
L'indubbio vantaggio che ne deriva è costituito dalla possibilità di far convergere molteplici informazioni personali, come quelle contenute in un classico biglietto da visita (vari numeri di telefono, fax e indirizzi email), in un unico "numero ENUM"; quest'ultimo potrà essere fornito alle persone dalle quali si desidera essere raggiunti dando così, nel caso le necessità personali lo richiedano, la massima reperibilità possibile.
Questo nuovo protocollo, degno di attenzione per gli operatori di telecomunicazioni e Internet Service Providers interessati a nuove modalità di fornitura di servizi personalizzati, ha destato interesse anche presso Istituzioni Comunitarie e Internazionali, come l'ETSI (European Telecommunication Standard Institute) e l'ITU-T (International Telecommunication Union).



www.enum.org

ENUM: the new Net frontier

by Guglielmo Grisley and Giovanni Tortora, NPTS (Number Portability Tracking System) administrators, National Assistant Supervisor and Supervisor of ITU-T's Commission 2 respectively

The growing convergence between telephone Network and Internet, as well as the exponential growth of internet users, has induced the scientific community to develop a new protocol, specifically inclined towards a convergence between PSTN (public telephone network) and IP network (Internet).
The Internet Engineering Task Force (IETF), and precisely the "Telephony Number Mapping" work group, has drawn up a new protocol, called "ENUM", which establishes the real point of junction between the telephone network and the web, in order to match a telephone number E.164 (according to an international numbering system) with an IP address.
This solution enables the users to use one number and have access to various services, such as landline and mobile telephony, fax, e-mail, IP telephony and Internet.
The unquestionable benefit is represented by the possibility to converge a great amount of personal information, like the information we find in a business card (telephone numbers, fax numbers and e-mail addresses), towards a single "ENUM number"; this exact number can be given to all those people you want to be contacted by and therefore creates, in case of personal needs, the best traceableness.
This new protocol, worthy of the attention of telecommunication operators and of Internet Service Providers interested in the new supply of customised services, has awakened the interest of International and Community Institutions, such as the ETSI (European Telecommunication Standard Institute) and the ITU-T (International Telecommunication Union).

L'ETSI, attraverso l'operato di un gruppo di lavoro ad-hoc ha prodotto la raccomandazione ETSI TS 102 051 v1.1.1 (2000-07) "ENUM Administration in Europe", nella quale si delineano aspetti gestionali delle numerazioni ENUM e il documento ETSI TS 102 172 v1.1.1 (2003-03) "Minimum Requirements for Interoperability of European ENUM trias", nel quale vengono trattate le problematiche dell'interoperabilità tra le sperimentazioni sul nuovo protocollo in ambito europeo.

Il Settore Standardizzzazione dell'International Telecommunication Union (ITU-T) ha organizzato varie attività al fine di risoluzione delle problematiche inerenti a ENUM.

In particolare, alla pagina web ENUM dell'ITU (***http://www.itu.int/osg/spu/enum/index.html***) vi sono informazioni riguardanti lo stato dei lavori, delle iniziative intraprese oltre che riferimenti per ulteriori informazioni riguardo a questa problematica, tra cui convegni sponsorizzati dall'ITU e da altre organizzazioni.

Il Gruppo di Studio 2 dello stesso ITU-T, organismo competente in materia di gestione ed organizzazione delle risorse di numerazione Internazionali, sta producendo delle Raccomandazioni che hanno lo scopo di regolamentare la mappatura delle numerazioni E.164 nel DNS.

È facile intuire che le problematiche da tenere in onsiderazione sono molteplici, dalla scelta del TLD che dovrà ospitare il data base ENUM, alla questione della sicurezza dei dati e del mantenimento dell'integrità della numerazione E.164.

Alcuni Stati Europei da poco più di un anno hanno dato inizio alla sperimentazione utilizzando l'esistente TLD .arpa, in attesa della conclusione della discussione, attualmente aperta in sede ITU-T, sull'opportunità della creazione di un TLD dedicato allo scopo (.enum).

Come detto in precedenza, in vari paesi (Austria, Francia, Olanda, Regno Unito, Svezia e Svizzera) sono stati accolti i suggerimenti di avvio di attività riguardanti ENUM, in particolare, successivamente a consultazioni pubbliche, sono state avviate sperimentazioni il cui stato, in alcuni casi è piuttosto avanzato.

Un esempio in tal senso è rappresentato dall'Austria, senz'altro il Paese più attivo a tale proposito, dove già si parla di lancio di una "fase commerciale".

Per quanto riguarda l'Italia, l'approccio è stato cauto a riguardo, attualmente, a seguito di una consultazione pubblica indetta dall'Autorità per le Garanzie nelle Comunicazioni, gli Operatori nazionali di telecomunicazione interessati stanno muovendo i primi passi per l'avvio di una fase di sperimentazione.

È quindi ragionevole pensare che per la diffusione dei risultati delle suddette prove occorrerà attendere almeno la fine dell'anno.

The ETSI has produced, through a specifically-established work group, the recommendation ETSI TS 102 051 v1.1.1 (2000-07) "ENUM Administration in Europe", which outlines the operational aspects of ENUM numbers and the document ETSI TS 102 172 v1.1.1 (2003-03) "Minimum Requirements for Interoperability of European ENUM trias", which deals with interoperability problems which happen during the experimentation of the new protocol in Europe.

The Standardization Sector of the International Telecommunication Union (ITU-T) has organized various activities in order to solve problems linked to ENUM.

In particular, at ITU's ENUM web page (***http://www.itu.int/osg/spu/enum/index.html***) you can find information about the work progress report, the launch of new initiatives as well as helpful links for further information about this issue, like meetings sponsored by ITU and by other organizations.

ITU-T's Study Group 2, the agency which takes care of the operation and organization of International numbering resources, is drawing up some Recommendations which aim to regulate the mapping of E.164 numbering in DNS.

It is easy to understand that there are many problems to hold in due consideration, starting from the selection of the TLD which will host the ENUM data base, data security issues and preservation of E.164 type numeration integrity.

Since just over a year ago, some European States have started to experiment the pre-existent TLD .arpa, looking forward to the end of the debate, currently open at ITU-T, the subject of the debate being the opportunity of creating a TLD with (.enum) purposes.

As we have already stated, indications as to the start of ENUM activities have been received from various countries (Austria, France, Holland, Great Britain, Sweden and Switzerland); in particular, after public consultation, experiments have been started, and in some cases, at an advanced level.

An example is Austria, without doubt the most active country on this subject, where they are already discussing the launch of a "commercial phase".

As far as Italy is concerned, its approach on this subject has been cautious; at present, following up a public consultation organized by the appointed Authority for the Security of Communications, all the national telecommunication operators who are interested are taking the first steps towards the start of an experimental phase.

It is therefore reasonable to think that we must wait at least until the end of the year to see the results of the tests above mentioned.

Nuovi caratteri per i nomi a dominio

Kim Davies, CENTR

In Europa è stata recentemente lanciata l'ultima innovazione tecnologica nel campo dei nomi a dominio: la possibilità di registrare domini che contengano una più ampia scelta di caratteri rispetto allo standard A-Z.

Tradizionalmente il sistema del nome a dominio permetteva di usare solo le 26 lettere dell'alfabeto latino, i numeri ed i trattini. Con il diffondersi di Internet in tutto il mondo, è sorta anche la necessità di usare nomi a dominio che riflettano la scrittura locale.

Gli "Internationalised Domain Names", espressione abbreviata in IDN, forniscono tale possibilità.

Mentre gli IDN offriranno ai francesi la possibilità di usare café.fr invece di cafe.fr, chi ne trarrà il maggiore vantaggio saranno i paesi che non usano i caratteri latini. Nei paesi asiatici, per esempio, l'uso del latino ha sempre creato difficoltà nelle comunicazioni via Internet.

Gli IDN, invece, permetteranno a questi utenti di usare Internet con maggiore immediatezza, usando caratteri che risultino loro più facilmente comprensibili. Tecnicamente, gli IDN funzionano aggiungendo al DNS un livello ulteriore.

I caratteri non latini vengono espressi con lo standard Unicode e poi codificati usando un metodo particolare.

L'applicazione di questo ulteriore livello di conversione permette di lasciare il nome a dominio nel formato ASCII e consente a tutti i server del mondo di continuare a funzionare senza modifiche.

Gli internet provider, per esempio, non dovranno apportare alcuna modifica tecnica ai propri server per supportare gli IDN. Il formato ASCII è sempre preceduto dal prefisso "xn—" e quindi facilmente identificabile.

Durante la fase di lancio, i gestori dei registri e gli internet provider probabilmente useranno proprio questo formato. Il dominio "café.fr", per esempio, sarà espresso da "xn--caf-dma.fr".

La conversione tra le due forme ha luogo al livello del software, e può essere effettuata dal vostro client e-mail o dal vostro web browser. Quando digitate café.fr il vostro software lo converte immediatamente in xn—caf-dma.fr per controllare il DNS.

Quindi Internet è quasi pronto ad usare gli IDN. Le uniche modifiche necessarie riguardano i registri dei domini, che dovranno fornire opzioni di registrazione che permettano l'uso degli IDN, e i software dei computer, che dovranno essere aggiornati affinché supportino la conversione IDN.

Internationalised Domain Names

Kim Davies, CENTR

The latest technical innovation for domain names has recently launched in a big way within Europe - the ability to register domains with a larger choice of characters than the standard A to Z.

Traditionally, the domain name system has only allowed the 26 letters of the Latin alphabet, numbers, and hyphens in a domain name.

With the growing use of the Internet worldwide, there has been a demand to use domain names that reflect local writing styles. "Internationalised Domain Names", or IDNs for short, provide this ability.

Whilst IDNs will provide the possibility for the French to use café.fr instead of cafe.fr, the greatest benefits will be in countries that do not use a Latin based character set for their writing.

Kim Davies

In Asian countries, for example, the use of Latin has always been difficult in Internet communications. Using IDNs will enable users to more seamlessly use the Internet using characters they better understand.

At a technical level, IDNs work by adding an extra layer to the DNS. Characters from non-Latin character sets are represented in the Unicode standard, and then encoded in a special way.

This extra conversion layer means that the domain name remains in an ASCII format, and means that all the DNS servers around the world can continue to operate unchanged.

Internet providers, for example, don't need to make any technical changes to their servers to support IDNs.

The ASCII encoded format is always prefixed with "xn--", and therefore are easily identifiable.

During launch, registrars and ISPs will likely deal with this form.

The domain "café.fr" would be represented as "xn--caf-dma.fr", for example.

The conversion between these two forms happens in software – for example, your email client or web browser.

When you type in café.fr into your software, it will immediately convert it to xn--caf-dma.fr for checking in the DNS.

Therefore, to implement IDNs, most of the Internet is ready to go. The only changes required is in domain registries, which must provide registration options to allow IDNs, and in computer software, which must be updated to support the IDN conversion step.

THE FUTURE OF THE NET

Verso la fine del 2003 alcuni software sono stati prontamente aggiornati per supportare gli IDN.
Le ultime versioni di Mozilla, Netscape, Opera e Safari presentano il supporto IDN.
Per i prodotti Microsoft Internet Explorer e Outlook, che non presentano ancora il supporto IDN, è invece disponibile sul web un plugin gratuito che aggiunge questa funzione.
È auspicabile che Microsoft fornisca un supporto IDN nativo nelle prossime edizioni dei software di sua produzione. Il problema dell'uso degli IDN in un registro del ccTLD è un po' più complesso.
Nonostante lo sviluppo degli IDN non sia tecnicamente difficile, sarà necessaria la revisione e l'adattamento dei processi amministrativi e delle politiche sull'idoneità dei nomi a dominio.
La questione di maggiore interesse per chi si registra sarà verificare quali caratteri sono accettati.
La maggior parte dei registri limiterà le registrazioni ai caratteri utilizzati nella lingua locale.
In tal modo si limiteranno le difficoltà di tipo amministrativo per il registro, per il gestore del registro e per i provider, che dovranno esclusivamente elaborare richieste nelle lingue che conoscono.
Senza tali limitazioni, sarebbe piuttosto difficile per un gestore di registro italiano occuparsi di una richiesta in russo con caratteri cirillici oppure in thai.
Il lancio degli IDN varia di paese in paese, ma i primi paesi europei ad utilizzare gli IDN hanno iniziato le registrazioni verso la fine del 2003.
La Polonia e la Svezia sono state tra le pioniere, insieme ad altre nazioni come la Germania, l'Austria, L'Ungheria e l'Islanda che si sono aggregate all'inizio del 2004. I paesi europei hanno adottato approcci diversi.
La Svezia per il lancio ha scelto di accettare registrazioni con l'introduzione di soli 5 caratteri aggiuntivi, utili per esprimersi nella lingua svedese: åääöéü, mentre i paesi di lingua tedesca aggiungeranno 92 caratteri, necessari a gran parte delle lingue dell'Europa occidentale e centrale.
Il registro polacco, per il momento, è stato uno dei più liberali, accettando i caratteri latini, cirillici, ebraici, arabi e greci.
Non è ancora chiaro quanto siano destinati a diventare popolari gli IDN.
In Europa molti sono abituati ad usare solo le lettere che vanno dalla A alla Z e non trovano scomodo attenersi a tale combinazione.
Inoltre, il fatto che i principali web browser e programmi e-mail non supportano adeguatamente gli IDN, non incoraggia ancora all'uso degli IDN, in quanto c'è il rischio che non siano leggibili dagli altri programmi.
Comunque, i registri dei domini sono già pronti, e nel momento in cui la domanda per gli IDN crescerà, i sistemi saranno in grado di gestirli in maniera stabile e prevedibile.

Computer software has quickly been updated to support IDNs in late 2003. The latest versions of the Mozilla, Netscape, Opera and Safari have IDN support.
Whilst Microsoft's Internet Explorer and Outlook do not have IDN support yet, a free software plugin is available which adds the functionality is available from the web.
It is hoped Microsoft will natively support IDNs in the next releases of their software.
The matter of allowing IDNs in a ccTLD registry is a little more complex.
Whilst deploying IDNs is not a difficult technical task, policies on domain name eligibility and well as administrative processes must be reviewed and adapted.
The key policy of interest to registrants is likely to be which characters are permitted.
Most registries will likely restrict registrations to only those characters needed to represent local languages.
This would limit the administrative difficulties for the registry, registrars and ISPs – who only have to process requests in languages which they are familiar with.
Without these kind of restrictions, there would likely be considerable difficulty for an Italian registrar to handle a request for a domain written in Russian Cyrillic or Thai.
The rollout of IDNs varies from country to country, but the first European countries to allow IDNs began registrations in late 2003.
Poland and Sweden were amongst the pioneers, with other countries like Germany, Austria, Hungary and Iceland coming on board in early 2004.
European countries have taken various different approaches to their policy.
Sweden, for their launch, have only allowed registrations with five additional letters needed to express their language – åääöéü, whereas the German speaking countries will add an additional 92 characters needed for most western and central European languages.
The Polish registry has been one of the most liberal to date - permitting a collection of Latin, Cyrillic, Hebrew, Arabic and Greek.
It is unclear how popular IDNs will become. In Europe, many are used to simply being restricted to the letters A-Z, and it is not too inconvenient to stick to this combination.
Without all the major web browsers and email programs supporting IDNs properly, there is little incentive to use IDNs yet – as they may not work for others.
However, domain registries are prepared so that when community demand for IDNs improves, systems are in place to deal with it in a stable and predictable way.

Migliorare il WHOIS assicurando buone pratiche nel campo della privacy

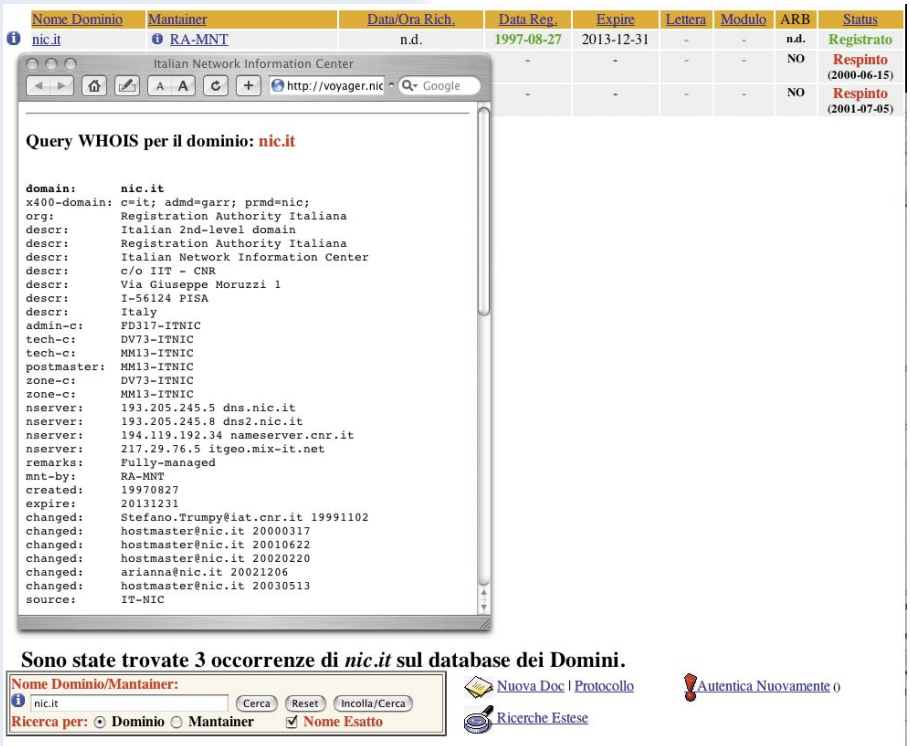
Gabriella Schittek, CENTR

CENTR ha di recente prodotto una bozza di documento che si occupa del WHOIS e delle questioni collegate all'uso di tale database.
Il WHOIS è uno strumento valido, che permette di identificare chi ha registrato un nome a dominio e che fornisce al registrato informazioni su chi contattare.
Il documento di CENTR oltre a cercare di fornire informazioni su argomenti collegati al servizio WHOIS, fornisce anche dei consigli su come utilizzarlo.
La bozza, dopo l'approvazione da parte dei membri, dovrebbe essere messa a disposizione del pubblico, ed è auspi-cabile che diventi una sorta di "ma-nuale" per i registri del ccTLD e per le altre parti interessate (come i gestori del registro).
Ogni registro è soggetto alla legge sulla privacy in vigore nella nazione di appartenenza, e quindi adotta un approccio diverso per la gestione del database WHOIS.
Tuttavia, poiché molti membri del CENTR sono, o sono in procinto di diventare, membri dell'UE, la bozza di documento si basa principalmente sul contenuto della Direttiva della Commissione europea (95/46/EC) sulla riservatezza dei dati. Sebbene la direttiva CE sia stata approvata del 1995, non è ancora stata adottata dalla legislazione di molti stati membri e la sua interpretazione varia da stato a stato.
Tuttavia, come indicato dal documento di CENTR, gli individui che subiscono dei danni ascrivibili alla mancata applicazione della direttiva da parte di uno stato membro hanno diritto a richiedere un risarcimento e ad appellarsi ad alcune norme della direttiva di fronte ai tribunali nazionali.
Questo potrebbe avere un impatto sul servizio WHOIS dei registri degli stati membri.

Improving the WHOIS ensuring good privacy practices

Gabriella Schittek, CENTR

CENTR has recently produced a draft document dealing with WHOIS and the issues associated with operating such a database.
WHOIS is a valuable tool which allows you to identify who has registered a domain name, plus provides contact information for this registrant.
The CENTR document not only tries to explain issues surrounding the WHOIS service, but also gives suggestions on how it could be implemented in practice.
The draft, when en-dorsed by its members, is meant to become publicly available and it is hoped it will serve as a kind of "handbook" for ccTLD registries and other interested parties (such as registrars)



Nic.it whois database

Every registry is subject to their country's own legislation on data privacy matters and therefore has a different approach on how to handle the WHOIS database.
However, as many CENTR members states are – or are about to become – EU members, the draft paper is very much based on the content of the European Commission Directive (95/46/EC) on data privacy.
Although the EC directive was passed in 1995, many member states still have not implemented it into local legislation, and the interpretations of it vary from state to state.
However, as the CENTR paper identifies, individuals suffering damage as a result of a Member State's failure to implement the directive are entitled to both seek compensation, as well as invoke some of the directive's provisions before national courts.
This could also have a direct impact on member state registries' WHOIS service.

THE FUTURE OF THE NET

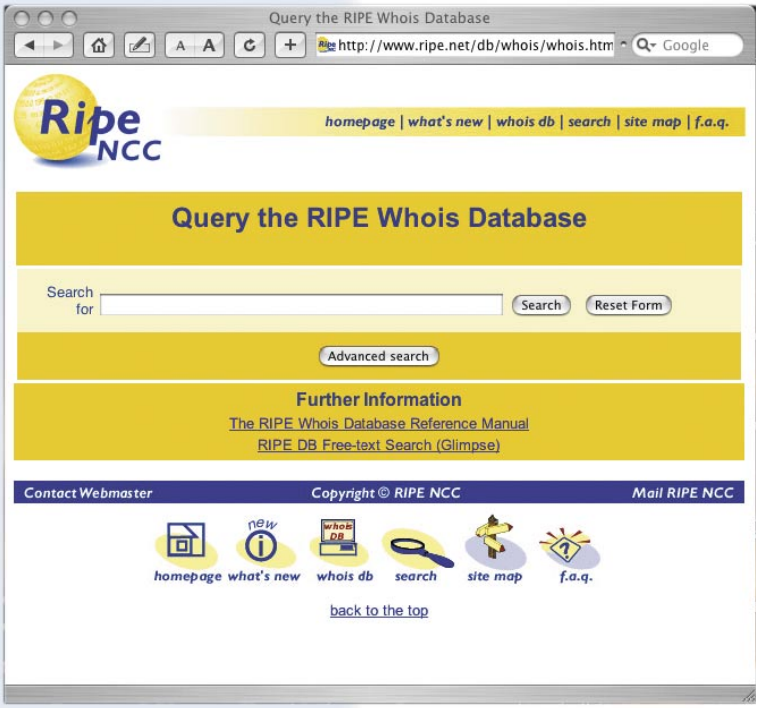
A tale riguardo la bozza di CENTR consiglia alcune misure amministrative e tecniche di base che i registri degli stati membri dell'UE dovrebbero adottare e che altri registri potrebbero adottare, per essere conformi a quanto indicato nella direttiva.
Ecco alcuni dei consigli per l'amministrazione:

- il registro deve informare il richiedente sul motivo per cui vengono raccolti i dati, su come verranno usati e sull'eventuale cessione o trasferimento a terzi;
- chi si registra deve anche essere messo a conoscenza del diritto di rifiutare che i propri dati siano visibili sul WHOIS e deve essere messo in condizione di applicare tale diritto. Per garantire che il richiedente abbia compreso tale punto, questi dovrà dichiarare esplicitamente di averlo compreso. A chi si registra viene anche offerta l'opzione di "non accettazione", nel caso in cui preferisca non mettere a disposizione i propri dati;
- il registro dovrebbe anche offrire a chi si registra la possibilità di accedere, visionare e modificare i propri dati. Ciò potrà essere reso possibile con la creazione di uno speciale sito web protetto da password;
- se la registrazione viene effettuata da un agente, il registro dovrà assicurarsi che questi fornisca ai richiedenti informazioni esaurienti sui requisiti per la privacy.

Alcune delle questioni tecniche di base sono:

- fare un back up dei dati raccolti e conservarli adeguatamente su server sicuri;
- assicurarsi che la possibilità di effettuare "ricerche incrociate" in diversi campi non sia eccessiva;
- occuparsi di questioni future, come il nuovo protocollo Internet IRIS e del suo impatto sull'uso di un servizio WHOIS.

Al momento in cui scriviamo le reazioni a questa iniziativa sono state positive, ed il manuale è considerato un utile riferimento da molti registri.
Tuttavia, ci aspettiamo nuove bozze e modifiche, con l'intervento migliorativo di molti membri, che lavoreranno insieme per ottenere un approccio unitario che sia approvato da tutti. Quando il documento CENTR WHOIS sarà stato approvato dai suoi membri, diventerà un documento ufficiale e sarà disponibile sul sito del CENTR ***www.centr.org***



www.ripe.net/db/whois/whois.html

In order to address this, the CENTR draft suggests some basic administrative and technical measurements that EU member states registries should - and other registries could – follow, to be in line with the directive.
Some of the basic administrative suggestions are:

- the registry must inform the registrant why data is collected, how it will be used, when it will be given out, or transferred to third parties;
- the registrant must also be informed and able to enforce its right to refuse its data being displayed in the WHOIS.
  To ensure that the registrant has understood this, they must actively confirm they understand this. Registrants are also given the possibility to "opt out" if they prefer their data not to be displayed;
- the registry should give the registrant the possibility to access, view and modify their own data if they so wish.
  This could be done by setting up a special, password-protected website;
- if the registration is carried out by an agent, the registry must ensure that they fully inform the registrant about these privacy requirements.

Some of the basic technical issues are:

- the collected data should be properly backed up and stored on secure servers;
- ensuring the ability to "cross search" different fields is not excessive;
- dealing with next generation issues, such as a new Internet protocol IRIS, and how it impacts providing a WHOIS service.

At the time of writing the reactions to this initiative have been positive, with the guidebook seen as a useful reference for many registries.
However, it is expected there will be new drafts and rewrites as members refine the document, working toward a unified approach that all can endorse.
Once the CENTR WHOIS document has been approved by its members, it will become an official document and will be available from CENTR's website at ***www.centr.org***.

La firma digitale a 360°: intervista a Carlo Sangalli, Presidente di Unioncamere

A partire dal 2004, l'utilizzo della firma digitale potrà definirsi "pratico" e non più "teorico"?

Il 2003 è stato un anno decisivo per la diffusione della firma digitale in Italia. Gli imprenditori e i professionisti titolari di un dispositivo di firma sono oggi circa 1 milione.
Nel 2004 prevediamo un consolidamento del suo utilizzo ed un'estensione ulteriore della sua diffusione.
Certamente, l'introduzione dell'obbligo di legge ad utilizzare la firma digitale per gli adempimenti verso il Registro delle Imprese è stato determinante per questi risultati, ma adesso è necessario che, da un lato le Pubbliche Amministrazioni, dall'altro i privati imparino a sfruttare le opportunità derivanti da questa "eccezionale" diffusione della firma digitale che fa dell'Italia il Paese-guida in Europa su questo terreno.

È utopico chiedersi se le amministrazioni pubbliche potranno utilizzare a breve la firma digitale anche per atti che riguardano i cittadini e non solo per atti interni?

Tutt'altro. L'esperienza delle Camere di commercio dimostra che la firma digitale sta contribuendo concretamente alla pro-gressiva "virtualizzazione" del rapporto tra pubblica amministrazione e cittadino-imprenditore.
Credo che la diffusione dell'uso di altri importanti strumenti, quali ad esempio il protocollo informatico nella pubblica amministrazione, potrà rivelarsi molto utile per rafforzare ed accelerare questo processo di sviluppo.

Sembra che per un utilizzo ottimale e su larga scala della firma digitale dobbiamo attendere la diffusione della carta d'identità elettronica, che ha già al suo interno la firma digitale. Quali sono i tempi previsti di diffusione della carta d'identità elettronica?

Carlo Sangalli *

The digital signature at 360°: interview with Mr. Carlo Sangalli, President of Unioncamere

From 2004, will the use of digital signatures cease being merely "theoretical" and actually become "practical"?

2003 was a decisive year for the diffusion of the digital signature in Italy.
Today around 1 million businessmen and professionals have their own digital signature.
We expect its use to become consolidated and more widespread in 2004. Obviously, the introduction of the law requiring the use of digital signatures for the Business Register played a decisive role in achieving these results.
However, the public administration on the one hand, and private individuals on the other, now need to learn how to take advantage of the opportunities deriving from this "exceptional" diffusion of the digital signature, which puts Italy ahead of other European countries in this field.

Is it hoping too much to ask the Public Administration to implement the digital signature for uses regarding the normal citizen in the short term, and not just for internal uses?

Quite the opposite. The experience gained by the Chambers of Commerce shows that the digital signature is making a substantial contribution to the progressive "virtualization" of the relationship between the public administration and the citizen/businessman. I believe that the spread of other important tools, such as computerized records in public administration, will prove itself to be very useful in reinforcing and accelerating this development process.

It seems we must await the introduction of the electronic identity card, which contains a digital signature, in order to achieve optimal, large-scale use of the digital signature. When is the electronic ID card expected to be introduced?

**Nato nel 1937 e laureato in giurisprudenza, è imprenditore commerciale nel ramo automobilistico. Dall'agosto 1997 è Presidente della Camera di Commercio Industria Artigianato e Agricoltura di Milano e dal luglio 1999 è Presidente dell'Unione Italiana delle Camere di Commercio, Industria, Artigianato e Agricoltura, carica nella quale è stato riconfermato per altri tre anni nel novembre 2003.*

**Born in 1937, with a degree in Law, he is a businessman in the car sector. Since August 1997 he is the President of the Chamber of Commerce, Industry, Craft and Agriculture of Milan. Since July 1999 he is the President of the Italian Union of Chambers of Commerce, Industry, Craft and Agriculture: his mandate has been renewed for three years in November 2003.*

Per il comune cittadino gli ambiti attuali di utilizzo della firma digitale sono pochi e la loro crescita dipende certamente dallo sviluppo di alcuni servizi pubblici e, in particolare, di servizi bancari. Nei servizi pubblici probabilmente la sanità farà la parte del leone, perché è lì che ci sono maggiori problemi di privacy, che la firma digitale può aiutare a risolvere.
Ma un ruolo molto importante l'avrà anche il progetto della carta d'identità elettronica, che prevede di ospitare un dispositivo di firma digitale. Il governo è molto determinato a condurre in porto in tempi stretti questo programma e il mio augurio è che, già nel 2004, si possano vedere frutti concreti.

Quali i vantaggi per le società tenendo in considerazione anche l'aspetto economico?

Abbiamo calcolato che, nei rapporti con le Camere di commercio, l'utilizzo della firma digitale potrà consentire risparmi alle imprese dell'ordine di 260 milioni di euro all'anno. Un risparmio cui va sommato quello che le stesse Camere di Commercio possono realizzare in termini di maggiori risorse umane disponibili per fornire altri servizi alle imprese. Un ulteriore vantaggio dall'introduzione della firma digitale riguarda poi la maggiore trasparenza e tempestività nella messa a disposizione delle informazioni sulle imprese: tutti gli atti firmati digitalmente, infatti, saranno rintracciabili il giorno successivo alla loro protocollazione elettronica nel Registro delle imprese.

www.unioncamere.it

When it comes to the normal citizen, there are currently very few areas where the digital signature can be used and their growth certainly depends on the development of public services and banking services in particular. The health service will probably play the main role from amongst the public services, because this is the area where there are most privacy problems which the digital signature can help to resolve. However, the electronic ID card project will also play a very important role, as the card will be actually contain a digital signature device. The government is determined to bring this project to a successful conclusion within a very short space of time and I hope that we will begin to see some concrete results in 2004.

What are the financial advantages for society as a whole?

We have calculated that, in dealings with the Chambers of Commerce, the use of the digital signature will make it possible for businesses to save around 260 million Euros per year. This saving should then be added to that which the Chambers of Commerce can make in terms of greater human resources available for providing other business-related services. Another advantage deriving from the introduction of the digital signature regards greater transparency and speed in providing information on businesses: in fact, all digitally signed documents will be traceable to their electronic records in the Business Register by the next day.

Quali ostacoli possono ancora limitare la distribuzione e l'utilizzo della firma digitale? Il problema della sicurezza ad esempio e' un ostacolo ancora da superare, si possono evitare tentativi di falsificazione e fino a che punto i codici di sicurezza sono affidabili?

L'introduzione di nuove tecnologie crea sempre apprensione e diffidenza in chi è abituato a strumenti di uso consolidato che però, proprio per questo motivo, alla fine si rivelano obsoleti rispetto alle esigenze di lavoro.
Le carte che abbiamo adottato rispondono ai requisiti di sicurezza più stringenti. In particolare sono conformi alle norme ISO 7816 per le carte con microprocessori e sono dotate di certificazione di sicurezza secondo la normativa europea CWA 14169. In questi ultimi decenni la nostra società è cresciuta sotto molti profili ed è diventata certamente più complessa. A mio avviso, per gestire questa complessità occorrono saperi nuovi e strumenti nuovi, accompagnati sempre dalla giusta dose di saggezza. Come diceva agli albori dell'informatica un grande scrittore come Isaac Asimov, non bisogna avere paura dei computer ma, semmai, della loro mancanza.

What obstacles may still hold back the spread and use of the digital signature? For example, does the security problem still need to be overcome, is it possible to prevent fraud and to what extend are the security codes reliable?

The introduction of new technology always creates some apprehension and mistrust in those who are used to traditional tools that, for this very reason, have been found to be obsolete with regard to work requirements.
The cards that we have adopted meet the strictest security requirements. They comply with ISO 7816 standards for cards with microprocessors and are certified in compliance with CWA 14169 European standards.
Over recent decades, our society has progressed under many aspects and has certainly become more complex. In my opinion, new knowledge and new tools, accompanied by the right dose of wisdom, are necessary for managing these complexities.
As the great writer, Isaac Asimov, said at the dawn of the I.T. era, we don't need to fear computers but, rather, fear their absence.

Internet 2004: l'ultimo campo di battaglia

Mikko Hypponen, direttore della Ricerca Anti-Virus presso F-Secure Corporation

Sommario

I problemi legati ai virus informatici sembrano arrivare ad ondate. Il 2001 fu un anno molto impegnativo sotto questo punto di vista, mentre il 2002 fu relativamente più tranquillo.

Purtroppo, il 2003 ha superato gli anni precedenti sia dal punto di vista del numero di virus, sia dal punto di vista della loro diffusione e gravità.

Le nuove tendenze riguardano il modo in cui gli spammer iniziano ad usare lo strumento dei virus ed il modo in cui molti importanti sistemi di infrastrutture hanno sofferto per le conseguenze dei virus.

I problemi dei bachi nella rete hanno dimostrato quanto sia importante dotare ogni singolo computer di un proprio firewall. Attualmente, il numero di virus conosciuti è di circa 90.000.

Il caso Slammer

Lo scoppio del baco della rete Slammer (o Sapphire) nel gennaio del 2003 fu il più grande attacco mai sferrato contro Internet.

Slammer era un baco completamente automatico, in grado di colpire i computer direttamente tramite una connessione in rete.

In altre parole, non si diffondeva tramite l'e-mail come gli altri maggiori virus.

Slammer colpì i sistemi Windows su cui era installato il software del database Microsoft SQL. Molte delle applicazioni da ufficio più diffuse installano automaticamente questo software nel sistema. Tuttavia, la maggior parte dei computer del mondo non l'avevano installato e Slammer non li ha potuti colpire. In realtà, il problema principale non era che Slammer avrebbe potuto contagiare un gran numero di computer, ma l'aggressività con cui cercava nuove vittime nella rete causando un'enorme quantità di traffico in rete.

In teoria, esistono circa 4 miliardi di indirizzi IP su Internet.

Il baco Slammer fu lanciato il 25 gennaio 2003 verso le 04:31 UTC (Tempo Universale Coordinato).

Alle 04:45 aveva già scansionato tutti gli indirizzi Internet, in meno di 15 minuti!

Questa operazione può essere paragonata ad un sistema automatico che compone tutti i numeri telefonici del mondo in 15 minuti.

Mikko Hypponen

Internet 2004: the last battle field

Mikko Hypponen, Director of Anti-Virus Research F-Secure Corporation

Overview

Computer virus problems seem to arrive in waves. Year 2001 was a very busy virus year, while 2002 was clearly quieter.

Unfortunately, 2003 exceeded previous years in terms of both the number of virus outbreaks as well as their extensiveness and severity.

New trends we've seen lately include the way spammers began to use viruses as a tool and how several critical infrastructure systems suffered from the consequences of virus outbreaks. The network worm problems we've seen have shown how important it is to equip every single computer with a personal firewall.

The number of known viruses is at the moment some 90,000.

Case Slammer

The explosive outburst of the network worm Slammer (or Sapphire) in January 2003 was the biggest attack against the Internet ever.

Slammer was a fully automatic network worm and it was able to infect computers directly over a network connection.

In other words, it did not spread through e-mail like many other major outbreaks.

Slammer infected Windows systems with Microsoft SQL database software installed on them. Many widely used office applications automatically install this software on the systems.

However, most of the computers around the world did not have it installed and Slammer could not infect them.

In fact, the main problem was not that Slammer would have infected that many systems, but the way it aggressively looked for new victims in the network and caused an enormous amount of network traffic.

In theory, there are some 4 billion public IP addresses on the Internet.

The Slammer worm was released on January 25, 2003 around 04:31 UTC. By 04:45 it had scanned through all Internet addresses – in less than 15 minutes!

This operation can be compared to an automatic system dialing all available phone numbers in the world in 15 minutes.

Trattandosi della rete, solo pochi numeri di telefono risponderebbero alla chiamata, ma senza dubbio le linee sarebbero congestionate. La congestione della rete causata da Slammer ha avuto conseguenze drammatiche, di cui parleremo più dettagliatamente in seguito, in questo stesso sommario.

Il caso Blaster

Anche Blaster (o Lovsan o MSBlast), che fu scoperto l'11 agosto, era un baco automatico simile a Slammer, ma fu in grado di colpire un numero considerevolmente maggiore di computer. la vulnerabilità sfruttata da Blaster colpì milioni di utenti di Windows 2000 e Windows XP, il cui sistema operativo di Windows non era stato aggiornato in maniera appropriata. Tuttavia, Blaster si propagava ad una velocità considerevolmente inferiore rispetto a Slammer, pur essendo molto più veloce dei virus che si diffondono tramite e-mail.

Il punto debole di RPC sfruttato da Blaster era stato identificato il 16 luglio, meno di un mese prima. Poiché luglio ed agosto sono tradizionalmente i mesi delle ferie estive, molte aziende non avevano installato il security patch prima che comparisse il baco.

Il primo sintomo del virus Blaster si manifestò per gli utenti di Windows XP con un messaggio che avvertiva della chiusura del processo RPC e del riavviamento di Windows in 60 secondi. Dopo aver riavviato il sistema, spesso a distanza di qualche minuto ricompariva lo stesso messaggio.

Ciò si ripeteva fino a quando l'utente scollegava il computer da Internet o aggiornava Windows. Erano necessari 10 minuti per scaricare gli aggiornamenti di sicurezza dal servizio windowsupdate.com. Molti utenti che si sono imbattuti in questo problema non sono riusciti ad aggiornare il sistema operativo, perché il sistema continuava a riavviarsi a causa del baco ed il processo di download si interrompeva.

L'autore del baco Blaster era probabilmente un giovane hacker che voleva esprimere la propria ostilità nei confronti di Microsoft. Un indicazione a riguardo si trova all'interno del virus: "billy gates perché permetti che ciò accada? Smettila di fare soldi e ripara il tuo software!!", oltre al fatto che il baco era programmato per dare inizio, cinque giorni dopo la sua scoperta, al suo attacco contro il sito windowsupdate.com con il Denial Of Service (rifiuto di servizio). Poiché windowsupdate non era il sito ufficiale di Microsoft per gli aggiornamenti, l'azienda rispose rimuovendo il sito da Internet poche ore prima che iniziasse l'attacco, mentre indirizzi come windowsupdate.microsoft.com rimasero operativi. Tuttavia, il virus ottenne quello che voleva: windowsupdate.com non esiste più.

Una delle conseguenze del baco Blaster fu che un altro autore di virus, un concorrente, creò un virus che combatteva Blaster.

Questo virus, conosciuto come Welchi o Nachi, colpiva i computer che erano già stati colpiti da Blaster. Non appena Welchi entrava nel sistema, distruggeva Blaster e cercava di scaricare ed installare gli aggiornamenti di Windows Security Update. In altre parole, era un virus anti-virus. Purtroppo, la cura si dimostrò peggiore della malattia: Welchi generò un maggior traffico in rete rispetto a Blaster e fu il motivo delle gravi interruzioni dei sistemi delle aziende alla metà di agosto.

As on the net, only a small number of phones would answer the call but the lines would certainly be congested.

The network jam caused by Slammer had dramatic consequences, which are discussed in more detail further on in this summary.

Case Blaster

Blaster (or Lovsan or MSBlast), which was detected on August 11, was also an automatic network worm and basically similar to Slammer, but it was able to infect a significantly larger amount of computers.

The vulnerability used by Blaster affected millions of Windows 2000 and Windows XP users, whose Windows operating system had not been appropriately updated. Blaster, however, propagated at a considerably slower speed than Slammer, yet it was significantly faster than viruses spreading through e-mail.

The RPC hole used by Blaster had been detected on July 16, less than a month earlier. As July – August is the main summer holiday season, many organizations had failed to install security patches before the worm appeared.

The first symptom of the Blaster virus was that Windows XP users started seeing a message about the shutdown of the RPC process and about Windows restarting in 60 seconds.

After the system had restarted, the same message often appeared again in a few minutes.

This was repeated until the user disconnected the computer from the Internet or updated Windows.

It took some 10 minutes to download the security updates from Microsoft's windowsupdate.com service.

Many users running into the problem were unable to update the operating system as the system restarted over and over again because of the worm and the downloading process was interrupted.

The writer of the Blaster worm was probably a young hacker who wanted to express his or her hostility towards Microsoft. An indication of this is the text found inside the virus: "billy gates why do you make this possible?

Stop making money and fix your software!!", and the fact that the worm was programmed to start its denial of service attack against the windowsupdate.com site five days after it was found.

Since windowsupdate.com was not Microsoft's official update site, the company responded by removing the site from the Internet a few hours before the attack started, while addresses like windowsupdate.microsoft.com remained in operation. However, the virus got what it wanted: windowsupdate.com does not exist any more.

One of the consequences of the Blaster worm was that some competing virus writer created a virus fighting against Blaster. This virus, known as Welchi or Nachi, infected computers already infected by Blaster.

As soon as Welchi had entered a system it destroyed Blaster and tried to download and install Windows security updates. In other words, it was an anti-virus virus.

Too bad that the cure was worse than the disease: Welchi generated considerably more network traffic than Blaster and was the reason for most of the severe system outages in companies in mid-August.

Sia Blaster sia Welchi ostacolavano l'operatività di importanti sistemi, come i bancomat ed i trasporti pubblici. Ne parleremo approfonditamente in un capitolo separato. In ogni caso, è importante ricordare che Welchi in particolare, continua a diffondersi.
A distanza di alcuni mesi dall'epidemia vera e propria, una macchina Windows non protetta può essere colpita in pochi minuti dopo essersi collegata in rete.

Il caso Swen

Il baco dell'e-mail Swen fu identificato il 18 settembre 2003, ma i problemi che ha generato continuarono a diffondersi per settimane nei sistemi e-mail di tutto il mondo. I messaggi e-mail inviati da Swen erano forgiati per sembrare degli originali safety updates di Microsoft. Ricordate che Microsoft non invia mai gli aggiornamenti per e-mail come attachments.
Per gli utenti finali, Swen non era così evidentemente dannoso come Sobig.F. Causò invece seri problemi agli operatori Internet. Il motivo era che la maggior parte delle e-mail inviate da Swen utilizzavano indirizzi e-mail inesatti che gli utenti finali non vedevano, ma che generavano messaggi di errore a loro volta rimandati indietro alle reti degli operatori. Risultato finale: diversi grandi operatori internet riportarono notevoli ritardi nell'invio delle e-mail. In alcuni casi le e-mail arrivarono con un ritardo di settimane,
I problemi causati da Swen erano un chiaro segnale dell'importanza che la posta elettrica ha assunto in pochi anni come mezzo di comunicazione.

Virus e infrastrutture critiche

Nel 2003 i virus hanno provocato nella vita reale dei problemi che non hanno precedenti per la loro gravità. I principali colpevoli furono Slammer, Blaster e Welchi. Inoltre, le interruzioni nella posta elettronica causate da Sobig.F e da Swen hanno ostacolato le operazioni dei sistemi aziendali.
La congestione della rete causata da Slammer rallentò clamorosamente il traffico su tutta la rete Internet. Una delle maggiori reti di bancomat del mondo si bloccò e rimase inattiva per l'intero weekend. Molti aeroporti internazionali riferirono che i loro sistemi di controllo aereo erano stati rallentati. Si verificarono problemi con i sistemi telefonici di emergenza in diverse parti degli USA.
Il virus riuscì addirittura ad entrare nella rete interna della centrale nucleare Davis-Besse nell'Ohio, bloccando il computer che controlla lo stato del reattore nucleare.
Il traffico RPC creato da Blaster provocò gravi problemi in tutto il mondo. Si verificarono problemi nei sistemi bancari e nelle reti o nei grandi integratori dei sistemi.
Inoltre, diverse compagnie aeree riportarono problemi nei loro sistemi, dovuti a Blaster e a Welchi, che le costrinsero a cancellare alcuni voli. Welchi colpì anche i bancomat costruiti da Diebold e basati sul sistema Windows XP, ostacolando le transazioni monetarie. Ne risentì anche il sistema per l'emissione di visti del Dipartimento di Stato Americano. L'azienda ferroviaria CSX riferì che il virus aveva interferito con i sistemi di segnalazione dei treni, interrompendo tutto il traffico passeggeri e merci. A causa di ciò, tutti i treni di pendolari intorno alla capitale degli Stati Uniti si fermarono sui binari.

Both Blaster and Welchi hampered the operation of important systems, such as automatic teller machines and public transportation. These are discussed in more detail in a separate section. However, it is important to note that especially Welchi still continues to spread. After several months since the actual epidemic, an unprotected Windows machine can get infected in just minutes when connected to network.

Case Swen

The Swen e-mail worm was detected on September 18, 2003, but the problems arising from it continued for weeks in e-mail systems around the world.
E-mail messages sent by Swen were forged to look like genuine Microsoft safety updates.
It is good to remember that Microsoft never sends updates as e-mail attachments.
For end users, Swen was not as visible a harm as Sobig.F. Instead, it caused severe problems to Internet operators.
The reason was that the majority of the e-mails sent by Swen used incorrect e-mail addresses.
Thus, the end users never saw them, but they generated error messages and the messages bounced back to the operators' networks. End result: several large internet operators reported severe delays in email delivery. In some cases emails were delayed by weeks.
The problems caused by Swen were a concrete indication of how important the e-mail has become as a communications channel in only a few years.

Viruses and critical infrastructure

Year 2003 saw virus induced problems in real-life systems which were unprecedented in their severity. The main culprits were Slammer, Blaster and Welchi. Additionally, the e-mail outages caused by Sobig.F and Swen hampered the operation of corporate systems.
The network congestion caused by Slammer dramatically slowed down the network traffic of the entire Internet. One of the world's largest automatic teller machine networks crashed and remained inoperative over the whole weekend. Many international airports reported that their air control systems slowed down.
Emergency phone systems were reported to have problems in different parts of the USA.
The virus even managed to enter the internal network of the Davis-Besse nuclear power plant in Ohio, taking down the computer monitoring the state of the nuclear reactor.
The RPC traffic created by Blaster caused big problems worldwide. Problems were reported in banking systems and in the networks or large system integrators.
Also, several airlines reported problems in their systems caused by Blaster and Welchi, and flights had to be canceled.
Welchi also infected Windows XP-based automatic teller machines made by Diebold, which hampered monetary transactions. The operation of the US State Department's visa system suffered.
The rail company CSX reported that the virus had interfered with the train signaling systems stopping all passenger and freight traffic. As a result of this, all commuter trains around the US capital stopped on their tracks.

I mass media hanno trattato con grande interesse gli effetti indiretti di Blaster sul blackout energetico nel nord-est degli Stati Uniti che si verificò nella settimana dello scoppio del virus.
Secondo il rapporto intermedio del comitato investigativo del blackout, ci furono quattro motivi principali alla base dell'interruzione della corrente, uno dei quali era dovuto a problemi informatici.
F-Secure ritiene che questi problemi furono per la maggior parte causati da Blaster.
Un altro comitato ufficiale sta ancora indagando la questione in maniera approfondita.
Occorre sottolineare che anche se i problemi causati al sistema da Slammer e Blaster furono effettivamente significativi, erano solo conseguenze del baco.
I bachi cercavano solo di propagarsi: non erano stati ideati per colpire sistemi essenziali. I virus colpirono ambienti che non avevano niente a che fare con Windows: l'enorme traffico nella rete causato dai bachi riuscì da solo ad interferire con le loro operazioni.
I bachi della rete, come Slammer, riescono a diffondersi in sistemi virtualmente isolati grazie alla loro operazione efficace e sistematica: Slammer scansiona esaurientemente ogni singolo indirizzo Internet che riesce a raggiungere.
Quindi se un computer critico è connesso anche indirettamente a qualsiasi dispositivo collegato ad una rete pubblica, prima o poi Slammer lo troverà.
In teoria, i bachi basati su SQL o RPC non dovrebbero mai riuscire ad entrare nell'intranet di un'azienda, perché i firewall dovrebbero impedire questo tipo di traffico.
A volte i virus sono riusciti ad attraversare il firewall a causa di errori nella configurazione, ma un percorso tipico era il portatile di un impiegato che veniva contagiato a casa o nella rete di un hotel.
Quando la macchina era riportata in ufficio, il baco si diffondeva in un lampo nell'intranet dell'azienda.
Ci sono stati anche casi in cui una scheda di rete WLAN inserita nel PC di un'azienda contattava una rete pubblica quando la macchina veniva connessa all'intranet con un cavo di rete.
Trasferire la gestione della sicurezza ad un fornitore di servizi o ad un operatore Internet si è dimostrato un metodo efficace per i privati o per le piccole aziende per risolvere i problemi quotidiani legati alla sicurezza dei dati.
F-Secure continua a cooperare con gli operatori del campo per fornire soluzioni applicabili.
Vorremmo anche sottolineare che l'unico modo per proteggere i sistemi informatici critici è tenerli scollegati da tutte le reti.

Il futuro

Gli attacchi contro i sistemi di dati sono destinati ad aumentare e a diventare sempre più professionali. La tecnologia utilizzata dagli spammer nei virus minaccia di trasformare Internet in un campo di battaglia. Le persone che si trovano dietro agli attacchi alla rete sono hacker, attivisti, spie industriali, gruppi di terroristi e gruppi di criminalità organizzata, ma la società moderna deve essere in grado di funzionare anche in presenza degli attacchi alla sicurezza dei dati.

The media has given a lot of attention to the indirect effects of Blaster on the power blackout in the northeastern USA which occurred during the outbreak week.
According to the intermediate report of the blackout investigative committee there were four main reasons behind the power failure, one of them being specifically computer problems.
F-Secure believes that these problems were to a great extent caused by the Blaster.
A separate official committee is still investigating this issue in detail.
It is important to note that even though the system problems caused by Slammer and Blaster were truly considerable, they were only byproducts of the worms.
The worms only tried to propagate: they were not intended to affect critical systems.
The viruses affected environments that had nothing to do with Windows: the massive network traffic caused by the worms alone disrupted their operation.
Network worms, such as Slammer, manage to spread into virtually isolated systems thanks to their effective and systematic operation: Slammer exhaustively scans every single Internet address it can reach.
Therefore, if a critical computer is connected to any device which is linked to some public network, even indirectly, Slammer will find it sooner or later.
In principle, SQL or RPC-based worms should never be able to enter company intranets through the public Internet, because firewalls should prevent this type of traffic.
Sometimes viruses were able to pass through the firewall because of errors in configuration, but a typical route to the internal networks was an employee's laptop that had been infected at home or for example in a hotel network.
When the infected machine was taken back to the office, the worm was able to spread like wildfire in the company intranet.
There have also been cases where a WLAN network card inserted in a company PC contacted a public network at the same time as the machine was connected to the intranet through a network cable.
Outsourcing security to a service provider or Internet operator has proved an efficient way for home users or small companies to solve everyday data security problems.
F-Secure continues to work together with operators in this field to provide applicable solutions.
We would also like to point out that the only way to protect critical computer systems is to keep disconnected from all networks.

Future

Attacks against data systems will increase and become more and more professional.
The virus technology used by spammers is threatening to change the entire Internet into a battle field.
The people behind the network attacks are hackers, activists, industrial spies, terrorist groups and organized crime, but the modern society must be able to function in spite of attacks against data security.

Strategie di sicurezza

Angelo Neri, responsabile Network security del CINECA

Al giorno d'oggi, garantire la sicurezza della propria infrastruttura informatica è un compito sempre più importante e al contempo gravoso. La perdita di confidenzialità delle informazioni o l'impossibilità anche temporanea di disporre delle risorse hardware o della posta elettronica, sono situazioni che comportano danni economici oltre che di immagine. Inoltre, il *Testo Unico sulla Privacy*, che dal 1 gennaio del 2004 ha sostituito la Legge 675/96 relativa al trattamento dei dati personali, dispone di *ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta mediante l'adozione di idonee e preventive misure di sicurezza* .

Ogni organizzazione deve garantire la segretezza e l'integrità delle informazioni riservate, impedendo che queste possano essere indebitamente modificate o impropriamente utilizzate, in modo costante ed omogeneo nello spazio e nel tempo. Per far ciò è necessario, oltre che sancito dalla legge, che l'infrastruttura informatica sia ben protetta da possibili intrusioni mediante l'utilizzo di idonei programmi costantemente aggiornati e verificati.

Nessuno è esentato dal predisporre adeguati sistemi di sicurezza: chiunque abbia modo di scambiare informazioni, dati o programmi con soggetti non fidati è a rischio. E non solo i pirati informatici o i sempre più diffusi virus e worm a minacciare l'integrità del sistema informativo aziendale: anche concorrenti o dipendenti insoddisfatti possono essere soggetti determinati a danneggiare un'azienda. Inoltre, la debolezza del sistema informativo di un'organizzazione, anche poco interessante dal punto di vista strategico, può essere utilizzata come mezzo per poter condurre ulteriori attacchi verso altre organizzazioni, o per confondere le tracce. Quindi non sono necessariamente l'importanza o la visibilità di un'azienda a determinarne il potenziale di richiamo in termini di intrusione.

Due sono gli elementi fondamentali di un sistema di sicurezza: la capacità di riconoscere l'identità di chi richiede accesso al sistema (autenticazione) e la capacità di applicare i limiti di accesso imposti ad un soggetto la cui identità sia nota (autorizzazione).

Security strategies

Angelo Neri, Responsible for CINECA Network Security

Nowadays, the security guarantee of your computer facilities has become a harder and more important task.

The loss of information privacy or the temporary impossibility to dispose of hardware resources or e-mail, create economical damages and affect reputation.

Besides, the *Consolidated Privacy Act*, which from 1 January 2004 has replaced the Act 675/96 relevant to personal data processing, orders to *reduce to the minimum risk, destruction or loss, even accidental, of data, unauthorized access or unauthorized processing or processing not in accordance with the purpose of logging data acquisition through the adoption of appropriate and preventive security measures* .

Every organization must guarantee secrecy and integrity of confidential information, preventing them to be, in a constant and homogeneous manner, improperly altered or used, referring to time and space.

In order to do this, it is important, apart from it being sanctioned by law, that your computer facilities are protected against intrusions, by means of appropriate programs, which are constantly updated and checked.

Nobody is free from using appropriate security systems: whoever exchanges information, data or programs with unreliable people is at risk.

Hackers or more and more common viruses are not the only threats for the integrity of the company's informative system: rivals or dissatisfied employees can damage a company.

Furthermore, a weak informative system of a company, which can be a poor strategic interest, can be used to lead an attack against another company, or to lose traces.

Therefore the importance or evidence of a company is not relevant in order to determine a potential intrusion.

Two are the important elements in a security system: the ability to recognize the identity of those who try and access the system (authentication) and the ability to enforce access restrictions to those who have a known identity (authorization).

SECURITY ASPECTS

L'autenticazione avviene solitamente in base a qualcosa che si conosce, (la classica password), o a qualcosa che si possiede (una smart-card, un generatore di one-time password, anche la propria identità fisica, come il riconoscimento delle impronte digitali, o dell'iride…). L'autorizzazione viene di conseguenza imposta dal programma applicativo o dal sistema operativo sottostante.
Ad esempio il server che ospita un sito web deve garantire che l'accesso avvenga in sola lettura e limitatamente ai contenuti del sito, senza che attraverso di esso possano essere ottenute altre informazioni presenti sul sistema. Anche le tipologie di attacco si concentrano attorno a questi due aspetti fondamentali. Le password tradizionali possono essere indovinate, se troppo semplici, o intercettate mentre transitano sulla rete.
Altre tecniche consistono nel sostituirsi al server di autenticazione in modo simile a quanto accade per gli sportelli Bancomat fasulli. Inoltre, i meccanismi di autorizzazione possono essere alterati inducendo il programma a comportarsi in modo diverso da come era stato progettato. Da non sottovalutare, poi, la possibilità di convincere qualcuno ad "abbassare la guardia" ad esempio impersonando soggetti in cui la vittima ripone fiducia. Non a tutti è noto che il mittente di un messaggio di posta elettronica può essere facilmente artefatto.
È quindi probabile avere successo inviando un messaggio a nome dell'amministratore di sistema in cui, citando un fantomatico problema di sicurezza, si chiede di eseguire un programma che in realtà consentirà al mittente l'accesso alla postazione. In fondo tutto ciò che serve è conoscere il nome dell'amministratore di sistema e la sua signature, mandare il messaggio ad un certo numero di persone e sperare che qualcuno ci caschi... Per proteggere efficacemente il proprio sistema informativo, innanzitutto è necessario procedere ad un'accurata analisi del rischio. Lo studio parte dall'analisi della struttura informatica dell'organizzazione, in particolare nell'individuazione dei dati sensibili e delle loro modalità di gestione. Deve essere eseguita da personale specializzato in tema di sicurezza informatica e non può prescindere dal contributo di chi si occupa dell'organizzazione dell'azienda e della definizione delle priorità strategiche della stessa. "You can have easy, cheap or secure: pick two", è una frase che circola tra chi si occupa di sicurezza informatica e rappresenta efficacemente il dilemma di fronte al quale l'IT manager spesso si trova. La sicurezza totale non esiste, è sempre necessario trovare un compromesso tra sicurezza, usabilità e costi. L'analisi del rischio consente di identificare le aree in cui è maggiormente produttivo investire in termini di sicurezza. Sulla base dell'analisi del rischio viene poi redatta la Politica di Sicurezza. La "security policy" consiste nell'insieme delle regole che l'organizzazione si dà per proteggere le proprie risorse.
Fondamentale è identificare la "matrice d'accesso" tra individui (esterni o interni) e risorse aziendali (informazioni, risorse hardware) e identificare le aree di responsabilità. Vanno poi definite misure minime che devono essere seguite dai responsabili, al fine di garantire un'adeguata omogeneità del sistema di difesa. Indispensabile è poi programmare piani di formazione e aggiornamento del personale in materia di sicurezza.

Authentication usually occurs on the basis of something we know (the classical password), or on the basis of something we own (a smart-card, a one-time password generator, or even physical identity, like fingerprints, or irises…).
Authorization is consequently established by the application-oriented program or by the operating system.
For example, the server which hosts a web site must guarantee that access is granted for reading only and to the limited extent of the site's content, without obtaining, through this, further information on the system.
Even the type of attacks differs in accordance to these two important aspects.
Traditional passwords can be guessed, if they are too easy, or intercepted while they travel through the net.
Other techniques can be: to take the authentication server's place in a similar way to what happens with false cash points.
In addition to this, the authorization process can be altered, making the program run differently to how it had been planned to run.
We mustn't underestimate the possibility to convince somebody to "lower their guard", for example, by personifying those people who the victim trusts.
Not everybody knows that the sender of an e-mail can be easily counterfeited.
Somebody can probably succeed in sending a message in the name of a system administrator, by mentioning an imaginary security issue, and asking to run a program, which will actually enable the sender to have total access.
After all, you just need the system administrator's name and signature, send the message to a certain number of people and hope that somebody falls for it...
In order to effectively protect one's informative program, first of all, one must carry out a careful risk analysis.
This research starts from the analysis of the organization's computer structure, and in particular, the sensitive ID data and its management procedures.
This must be carried out by specialised computer security staff and can't do without the contribution of those who take care of the business management and decide about the strategic priorities of the company. "You can have it easy, cheap or secure: pick two", is an expression you can hear from those who deal with computer security and effectively represents the dilemma an IT manager frequently comes across.
Total security does not exist; it is always necessary to find a compromise between security, usage and costs.
Risk analysis enables us to identify the areas where you can most effectively invest, in terms of security.
Then, in accordance to risk analysis, a Security Policy is drawn up. "Security Policy" is the set of rules the organization follows in order to protect its resources.
It is of essential importance to identify the "access matrix" between individuals (external or internal) and company resources (information, hardware resources) and then identify le the responsibility areas.
Minimum-security measures must be then determined and carried out by the people in charge, in order to guarantee adequate consistency within the security system.
The planning of security training and refresher courses is absolutely necessary.

Il mancato aggiornamento può vanificare rapidamente gli sforzi e gli investimenti fatti. Come regola generale, la politica di sicurezza deve essere ben definita, costantemente aggiornata e soprattutto realizzabile e verificabile in concreto.
Dal punto di vista tecnologico, per impostare correttamente un'adeguata strategia di protezione dei sistemi informativi è necessario che la rete aziendale sia progettata in modo da separare opportunamente i diversi domini di sicurezza. È opportuno predisporre strumenti che consentano di filtrare o controllare le informazioni in transito, come il firewall, che ha la valenza strategica di poter concentrare in sé una gran parte delle regole d'accesso. In aggiunta, l'introduzione di strumenti di Intrusion Detection (IDS) consente, attraverso sonde disposte in diversi punti della rete e sui principali server, di raccogliere e correlare informazioni allo scopo di individuare tentativi di intrusione e attuare conseguenti misure difensive. È poi assolutamente indispensabile l'installazione e l'aggiornamento puntuale dei sistemi antivirus, sia a livello centralizzato che nelle singole postazioni di lavoro.

The lack of updating can rapidly make the efforts and investments fruitless. As a general rule, the security policy must be well defined, constantly updated and above all feasible and verifiable in real terms.
As far as technology is concerned, in order to correctly set up an adequate computer security strategy, it is essential that the company's network be planned in such a way as to appropriately separate the separate security domains.
It is then appropriate to prearrange tools that allow for filtering and checking all the passing information, like a firewall, which has the strategic value of incorporating a great extent of the access controllers.
In addition to this, the introduction of Intrusion Detection (IDS) tools allows, by means of probes placed in several spots in the network and in the main servers, to collect and correlate information in order to detect intrusion attempts and then take security measures.
The installation and updating of anti-virus systems is absolutely essential, at both central and individual workstations.

Il Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle Pubbliche Amministrazioni

a cura della segreteria tecnica del Comitato tecnico nazionale sulla sicurezza informatica

Il Comitato è stato istituito con Decreto Interministeriale del Ministro delle Comunicazioni e del Ministro dell'Innovazione e le Tecnologie il 24 luglio 2002.
Le principali funzioni sono di indirizzo e coordinamento delle iniziative in materia di sicurezza nelle tecnologie dell'informazione e della comunicazione nelle pubbliche amministrazioni, di cui alla direttiva del Ministro per l'innovazione e le tecnologie del 16 gennaio 2002.
Il Comitato è composto da Claudio Manganelli (Presidente), Carlo Sarzana di Sant'Ippolito, Danilo Bruschi, Franco Guida, Giorgio Tonelli.
Operativamente, il Comitato formula le proposte per le strategie in materia di sicurezza informatica e delle telecomunicazioni (ICT) per la pubblica amministrazione, ai fini della redazione:

www.cnipa.gov.it

The National Technical Committee on Information and Telecommunication Security in Public Administrations

by the Technical Secretariat of the Italian National technical Committee on informatics security

The Committee was established by an Interdepartmental Decree issued by the Minister of Communication and by the Minister of Innovation and Technology on July 24 2002.
The main functions are guidance and co-ordination on initiatives regarding the security of information and communication technology in public administrations, as per the Directive issued by the Ministry of Innovation and Technology on January 16 2002.
The members of the Committee are Claudio Manganelli (Chairman), Carlo Sarzana di Sant'Ippolito, Danilo Bruschi, Franco Guida, Giorgio Tonelli.
In factual terms, the Committee develops proposals for information and telecommunication (ICT) security strategies for public administrations, in order to draw up:

- del Piano nazionale della sicurezza delle tecnologie dell'informazione e comunicazione della pubblica amministrazione;
- della predisposizione del modello organizzativo nazionale di sicurezza ICT per la pubblica amministrazione.

Dopo un'intensa attività di ricognizione dello stato della sicurezza ICT nella PA, il Comitato ha prodotto un primo documento, "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni (ICT) per la Pubblica Amministrazione".
Il documento sarà ufficialmente presentato il 18 marzo dalla Presidenza del Consiglio e rappresenta un primo livello di documentazione per le PA ed è aperto ai contributi da parte delle PA stesse e degli operatori più significativi in materia di sicurezza ICT.
Nella prima parte di questo documento, "Proposte per un sistema di governo della sicurezza ICT nella PA", vengono presentate una serie di indicazioni relative alla costituzione di una infrastruttura organizzativa, che possa farsi carico a livello nazionale di coordinare un processo di "messa in sicurezza" delle PPAA, unitamente ad una serie di indicazioni in merito alle iniziative di tipo legislativo che dovrebbero essere intraprese nel settore.
La seconda parte del documento, "Linee guida per l'attuazione della sicurezza ICT nella PA", contiene l'indicazione di una serie di attività da intraprendere con estrema urgenza per avviare il suddetto processo.
Il disegno organizzativo delineato dal Comitato prevede la istituzione, ormai prossima nel CNIPA, di una "Unità di gestione degli attacchi informatici", cioè di un Computer Emergency Response Team che opera a livello di pubblica amministrazione e la cui evoluzione può anche essere un'Agenzia nazionale.
Lo stesso disegno prevede anche un'intensa attività di formazione per personale della PA sul tema, che sarà curata dall'Istituto Superiore di Comunicazioni.
Il Comitato intende poi svolgere attività di cooperazione con l'Agenzia europea per la sicurezza informatica e promuovere alcune altre iniziative concrete, di supporto all'attuazione del Piano, così come richiesto nel Decreto; in particolare:

- la produzione di linee guida sulla sicurezza informatica, redatte con il contributo non solo dei responsabili informatici della PA, ma anche con quello delle associazioni rappresentative delle imprese e dei cittadini;
- la determinazione di alcuni obiettivi operativi relativi ad aspetti urgenti e sentiti dagli utenti ICT, come l'abuso di spamming e dei cookie;
- la promozione di incontri periodici con la PA, con provider internet, con realtà rilevanti di banche, finanza, assicurazioni, commercio e industria, al fine di armonizzare il sistema sicurezza ICT italiano, sfruttando le più riuscite esperienze e capacità di tutte le realtà nazionali.

- A National information and telecommunication security plan for public administrations;
- A national ICT security organisation model for public administrations.

After an intensive survey of the current state of ICT security in PAs, the Committee produced a first document, "Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni (ICT) per la Pubblica Amministrazione" (Proposals on Information and Telecommunication (ICT) security strategies for public administrations).
The document will be officially presented on March 18 by the Cabinet and is the first level of PA documentation, open to contributions from the PAs themselves and from the most important ICT security operators.
The first part of this document, "Proposte per un sistema di governo della sicurezza ICT nella PA" (Proposals for an ICT security government system in PAs), gives guidance on the establishment of an organisational facility that might take care of co-ordinating a nation-wide process for making PAs secure along with guidance on the legislative initiatives that should be taken in this area.
The second part of the document, "Linee guida per l'attuazione della sicurezza ICT nella PA" (Guidelines on the implementation of ICT security in PAs), lists the measures that should be urgently taken to kick-start such process.
The organisational proposal outlined by the Committee involves the establishment, not too far off in CNIPA, of a "Computer Attack Handling Unit", i.e. a Computer Emergency Response Team working with public administrations, which could one day become a national agency.
The same proposal also involves intensive training for PA staff on this issue, which will be provided by the Istituto Superiore di Comunicazioni.
Then, the Committee intends to engage in co-operation with the European Information Security Agency and promote some more concrete initiatives to support the implementation of the Plan, as set forth by the Decree, in particular:

- Production of guidelines on information security, with contributions not only from PA information operators but also from associations that represent the business sector and the citizens;
- Determination of operating goals on urgent aspects that ICT users are most concerned about, such as spamming and cookies;
- Promotion of regular meetings with PAs, with Internet providers, with important members of the bank, finance, insurance, trade and industry world, in order to harmonise the Italian ICT security system by making the most of the most successful experiences and abilities of all countries.

Gestire la sicurezza di uno dei più grandi database italiani

intervista a Simone Nasoni, Responsabile Divisione Prodotti e Servizi Applicativi di InfoCamere

Infocamere fornisce attraverso un sistema telematico l'accesso immediato ai dati contenuti negli archivi camerali. Come e perché questo sistema telematico può definirsi "sicuro"? Quali garanzie hanno le imprese iscritte alle Camere di Commercio?

I temi della sicurezza sono fondamentali nella gestione di un sistema molto complesso come quello realizzato da InfoCamere per le Camere di commercio. Per garantire l'integrità e la disponibilità dei dati camerali, InfoCamere adotta un sistema di difesa integrato. Gli elementi di questo sistema comprendono firewall strutturati su più livelli - sempre più selettivi man mano che si procede dall'esterno verso i sistemi database, ridondati in configurazione di alta affidabilità - sistemi di intrusion detection, per finire con un ambiente integrato di antivirus che va dal server di posta alle singole stazioni di lavoro delle Camere. Per le operazioni che vanno a modificare i dati contenuti nei database i sistemi di autenticazione prevedono modalità sicure la come crittografia e l'autenticazione forte basata su smart card. Poiché le minacce alla sicurezza si evolvono e cambiano continuamente, fanno parte della difesa integrata diverse procedure di controllo (vulnerability assessment, audit di sicurezza, analisi di log, ...) che guidano l'adeguamento continuo dei sistemi e delle applicazioni, necessario a fronteggiare le nuove minacce.

Simone Nasoni *

Come vengono gestiti i flussi di archiviazione dei dati?

Il flusso di archiviazione dati adottato per le informazioni camerali è un esempio operativo di Information Lifecycle Management. In pratica l'informazione, nei vari stadi di elaborazione, viene conservata e gestita con le tecnologie più adatte al livello di servizio richiesto per ogni specifica fase.
Tutto parte dalla "pratica telematica", fonte primaria di aggiornamento dei dati, che viene acquisita su veloci sistemi di front-end, connessi ad altrettanto veloci sistemi di memorizzazione Network Attached Storage, in grado di accettare senza problemi flussi d'invio tipici dell'utenza Internet.

Managing the security of one of the largest Italian databases

interview with Simone Nasoni, Product Division and Applications Service Manager for InfoCamere

InfoCamere provides immediate access to data in Chamber of Commerce archives through a telematic system. How and why can this telematic system be termed "secure"? What guarantees are there for businesses registered with the Chambers of Commerce?

The subject of security is fundamental when running a very complex system such as that developed by InfoCamere for the Chambers of Commerce.
In order to guarantee the integrity and availability of the data, InfoCamere uses an integrated defence system. This system includes structured firewalls on several levels – becoming increasingly selective while proceeding from the outside towards the database systems, looped in a highly reliable configuration – intrusion detection systems, and finally an integrated antivirus environment that encompasses everything from the mail server to the individual Chamber work stations.
For operations that modify the data contained in the databases, the authentication systems use secure modes such as cryptography and strong smart card-based authentication. Since security threats constantly evolve and change, the integrated defence system includes various monitoring procedures (vulnerability assessment, security audit, log analysis, ...) which guide the constant adaptation of the systems and applications, necessary for tackling the new threats.

How are the data archiving flows managed?

The data archiving flow adopted for Chambers of Commerce information is an operative example of Information Lifecycle Management. In practice, the information, in its various phases of processing, is stored and managed by the most suitable technology for the service level required for each specific phase.
Everything starts from the "telematic file", primary source for updating data, which is acquired on fast front-end systems, connected to equally fast Network Attached Storage memory systems, able to accept typical Internet usage delivery flows without problems.

**Nato nel 1963 e laureato in Scienze Politiche "summa cum laude" all'Università di Firenze, lavora presso Infocamere S.C.p.A., Società Consortile per azioni delle Camere di Commercio Italiane, in veste di responsabile della Divisione Prodotti e Servizi Applicativi, la struttura che gestisce i servizi di e-government e Certificazione Digitale di InfoCamere.*

**Born in 1963, with a degree with honours in Political Science at the University of Florence, he has been working for Infocamere S.C.p.A., the IT Consortium of the Italian Chambers of Commerce, as responsible of the Products and Services Unit, the division that runs the e-government and digital signature services of InfoCamere.*

Una volta acquisita, la pratica telematica viene trasferita sui sistemi interni di back-end, i quali, appoggiandosi su un'unica Storage Area Network ad alte prestazioni ed adeguata capacità, supportano le fasi di controllo ed istruttoria del documento. Solo dopo il processo di validazione delle informazioni, effettuato dal personale camerale, può avvenire l'ultimo stadio del processo che prevede l'archiviazione documentale su appositi Content Storage. Questi sono contraddistinti da affidabilità e sicurezza paragonabili alle tecnologie di archiviazione ottica ma offrono prestazioni in fase di caricamento ed erogazione sensibilmente superiori.

I dati vengono concentrati in un'unica "storage area network" (San, area di archiviazione in rete), ma come vengono affrontati imprevisti di ogni genere come potrebbe essere ad esempio un black-out?

L'efficienza degli impianti tecnologici e le condizioni ambientali della sede di Padova sono controllate da un sistema di supervisione centralizzato. In particolare, le apparecchiature del CED sono alimentate da gruppi di continuità di tipo rotante che garantiscono una protezione dalle microinterruzioni e dagli sbalzi di tensione. Relativamente al rischio di black-out elettrico, è previsto l'intervento dei gruppi elettrogeni di emergenza che garantiscono una autonomia di oltre una settimana. In occasione del disastroso black-out di settembre 2003, ad esempio, tutti gli apparati del CED hanno sempre continuato a funzionare regolarmente.Anche gli impianti di climatizzazione e di alimentazione elettrica sono realizzati con il criterio della massima affidabilità e ridondanza, proprio per garantire l'erogazione del servizio anche in caso di singolo guasto in qualunque sezione degli impianti stessi.Fisicamente, la sede operativa di InfoCamere è presidiata senza interruzione da un servizio di vigilanza ed è attivo un impianto di antintrusione e TV a circuito chiuso. L'accesso alle aree riservate, in cui sono installati gli apparati per l'erogazione del servizio, è segregato per zone e l'ingresso è consentito unicamente al personale abilitato che si identifica mediante badge. Per le aree più critiche è associato anche un riconoscimento antropometrico, attraverso l'impronta del pollice. In tutte le aree riservate sono attivi gli impianti di allarme anti-allagamento, rivelazione fumi e spegnimento automatico a gas inerte NAF SIII.

Come vengono implementati i sistemi di sicurezza?

Il modello utilizzato da InfoCamere per implementare la sicurezza dei dati tiene conto degli standard ITSEC, dei Common Criteria for Information Technology Security Evaluation e del British Standard 7799, oltre che delle norme di legge attualmente in vigore. Dei criteri ITSEC si sono accolti i concetti, la relativa terminologia e l'approccio top-down alla sicurezza. Secondo tale approccio, a seguito di un processo di analisi del rischio, sono state individuate le minacce al sistema, fissate le esigenze e identificate le funzionalità di sicurezza che le soddisfano.

Once acquired, the telematic file is transferred to internal back-end systems, which, supported by a single high-performance high-capacity Storage Area Network, support the document control and investigation phases.
The last stage of the process, which involves the document being archived in specific Content Storage, can only take place after the information has been validated by Chambers of Commerce staff. The Content Storage is marked by reliability and security levels comparable to optical archiving technology, but offers a noticeably better performance during the loading and supply phase.

The data are concentrated in a single "storage area network" (SAN), but how do you deal with unexpected situations such as a black-out?

The efficiency of the technological systems and the environmental conditions in the Padua offices are monitored by a centralized monitoring system. The CED devices in particular are powered by continuous rotating generating sets, guaranteeing protection against microinterruptions and surges.
Emergency generators, which can operate autonomously for over a week, are programmed to take over in the event of a black-out.
During the devastating black-out in September 2003, all the CED devices continued to function normally.
The air conditioning and power systems are also made following maximum reliability and looped criteria, so as to guarantee that the services continue to be provided even when there is a failure in one of the systems.
The InfoCamere headquarters are constantly monitored by a surveillance service, and an intruder detection and CCTV system are operative 24 hours a day. Access to the reserved areas, which contain the service provision systems, is segregated by zones and access is only permitted to authorized personnel identified by badges.
The most critical areas are also fitted with anthropometric recognition systems, using thumb prints.
All the reserved areas are protected by anti-flooding alarm systems, smoke detectors and NAF SIII inert gas automatic extinction systems.

How are the security systems implemented?

The data security model used by InfoCamere complies with ITSEC standards, the Common Criteria for Information Technology Security Evaluation and British Standard 7799, as well as current laws.
InfoCamere used the concepts, relative terminology and top-down security approach contained in the ITSEC criteria. By following this approach, a risk analysis procedure was used to identify threats to the system, establish requirements and identify the security functions that fulfil them.

Tali funzionalità hanno impatto non solo sugli aspetti tecnologici dei sistemi informatici, ma anche sugli aspetti organizzativi e logistici quali i ruoli, le responsabilità e la sicurezza fisica degli ambienti di elaborazione. Il livello di sicurezza viene costantemente verificato in modo sistematico, con una attività continua ed organizzata di rilevazione e rimozione delle vulnerabilità. Le procedure di sicurezza fanno parte delle procedure di Qualità per le quali Infocamere ha ottenuto la certificazione ISO/Vision 2000.

Potete spiegarci brevemente la definizione di "disaster recovery" e che relazione esiste tra questo concetto e Infocamere?

Per disaster recovery possiamo intendere l'insieme di quei processi organizzativi e tecnici, anzitempo codificati, che hanno luogo durante e subito dopo una situazione di crisi allo scopo di minimizzare l'interruzione del business e far ritornare l'erogazione dei servizi tecnologici il più rapidamente possibile allo stato precedente la crisi.Visto il rilievo delle informazioni trattate per conto del sistema camerale, InfoCamere ha messo a punto diverse strategie di disaster recovery proporzionalmente dipendenti dalla criticità dei servizi e delle informazioni stesse. Sono state, quindi, realizzate soluzioni a complessità crescente che, ad esempio sui servizi ad alta criticità, consentono di ripristinare l'infrastruttura tecnologica entro 48 ore, attraverso un hot-site remoto, anche a fronte di eventi calamitosi.

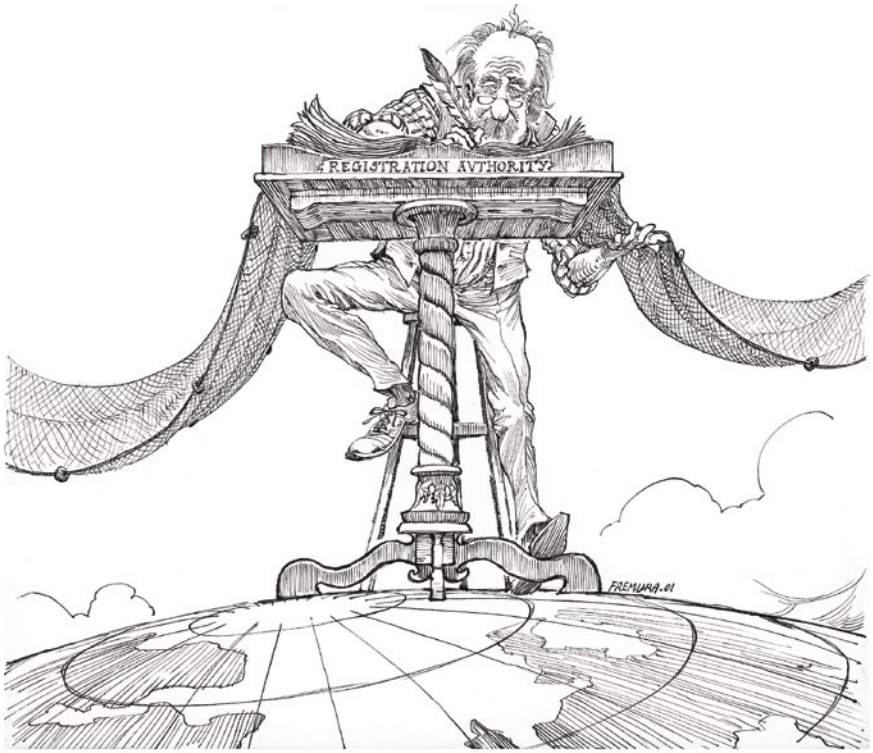
These functions do not just affect the technological aspects of the I.T. systems, but also the organizational and logistical aspects, such as roles, responsibilities and physical safety in the processing environments.
The security level is constantly monitored in a systematic fashion, with continuous organized vulnerability detection and removal operations. The security procedures are part of the Quality procedures which have enabled InfoCamere to obtain ISO/Vision 2000 certification.

Can you briefly explain the meaning of "disaster recovery" and the relationship between this concept and InfoCamere?

Disaster recovery means the ensemble of encoded organizational and technical procedures that take place during and immediately after an emergency situation in order to minimize interruption to business and restore the technological services to pre-crisis conditions as soon as possible.Given the importance of the information in the Chambers of Commerce system, InfoCamere has developed various disaster recovery strategies in proportion to the importance of the services and the information itself. We have therefore developed solutions of increasing complexity that make it possible to restore the technological infrastructure for critical services within 48 hours, using a remote hot-site, even in the case of disasters.

Lettere all'editore

Letters to the Editor



Attendiamo vostre lettere e commenti all'indirizzo: newsletter@nic.it oppure tramite posta di superficie a Istituto di Informatica e Telematica del CNR - Registration Authority Italiana, Unità Relazioni Esterne, Redazione Newsletter RA News, Via Moruzzi, 1, 56124 Pisa

We'll be waiting for your letters and comments at: newsletter@nic.it or via ordinary mail to be addressed to Istituto di Informatica e Telematica del CNR - Registration Authority Italiana, External Relations, Redazione Newsletter RA News, Via Moruzzi, 1, 56124 Pisa

Calendario eventi 2004

(aggiornato a marzo)

Data	Evento	Sede
3-7 maggio	RIPE 48	Amsterdam, Olanda
21-22 giugno	CENTR 22 Assemblea General	Stoccolma, Svezia
19-23 luglio	ICANN meeting	Kuala Lampur, Malesia
1-6 agosto	IETF 60	San Diego, USA
7-12 novembre	IETF 61	sede da confermare
1-5 dicembre	ICANN meeting	Cape Town, Sudafrica

Per informazioni e per le iscrizioni ai corsi dello IIT-A, è possibile consultare il sito Web:
http://www.nic.it/RA/index.html, nell'area riservata ai provider/maintainer
Per informazioni sui meeting ICANN: *http://www.icann.org*
Per informazioni sulle riunioni di CENTR: *http://www.centr.org*
Per informazioni sui meeting RIPE: *http://www.ripe.net*
Per informazioni sui meeting di IETF: *http://www.ietf.org*

Calendar of 2004 events

(updated to March)

Date	Event	Location
3-7 May	RIPE 48	Amsterdam, Netherlands
21-22 June	CENTR 22 General Assembly	Stockholm, Sweden
19-23 July	ICANN meetings	Kuala Lampur, Malaysia
1-6 August	IETF 60	San Diego, USA
7-12 November	ICANN meetings	venue to be decided
1-5 December	ICANN meetings	Cape Town, South Africa

For further information and to participate into the IIT-RA courses, please visit
http://www.nic.it/RA/en/index.html, provider/maintainer section
For further information on ICANN meeting: *http://www.icann.org*
For further information on CENTR General Assembly:*http://www.centr.org*
For further information on RIPE meeting: *http://www.ripe.net*
For further information on IETF meeting: *http://www.ietf.org*

Redazione/Central office:
Istituto di Informatica e Telematica - CNR
Registration Authority Italiana
Relazioni Esterne
Via G. Moruzzi, 1
I-56124 Pisa
Tel.+39-050-3139811
Fax +39-050-3152713
e-mail: newsletter@nic.it

Direttore responsabile/Director in charge:
Prof. Franco Denoth

Responsabile di redazione/Editing:
Giovanni Seppia

Collaboratori in redazione:
Ana Corujo, Ada De Giorgio, Stefania Fabbri, Francesco Gianetti, Natalia Malvaldi, Ilaria Mazzoni, Daniela Medda, Francesca Nicolini

Progetto grafico e impaginazione/Graphics and paging:
Francesco Gianetti

Stampa/Printed by:
Tipografia Graphicarts Snc

Si ringrazia per la preziosa collaborazione a questo numero/Special thanks for the publication of this issue:
Ara Congressi; ICANN, ufficio stampa; InfoCamere; CENTR Secretariat; Chiara Ronchetti, Register.it Spa; all providers/maintainers that submitted their contributions for the "Customer Care Management" report

Autorizzazione del Tribunale di Pisa n. 1369

Stampato su carta ecologica/Printed on ecologic paper

Registration Authority Italiana

IIT