Consiglio Nazionale delle Ricerche

P. le Aldo Moro, 7 00185 Roma

Tel. 06-49931 Fax 06-49933159

DIREZIONE CENTRALE SERVIZI PER LA RICERCA

UFFICIO ICT

Ai dipendenti del CNR

Oggetto: Elezioni Rappresentante personale CNR presso CdA

Allegati: 1 Votazioni CNR - Descrizione

Cari colleghi,

in accordo con la Direzione Generale del CNR, ritengo doveroso chiarire alcune questioni di carattere tecnico che sono state oggetto di illazioni sgradevoli in merito a una presunta gestione scorretta delle procedure utilizzate dall'Ente per l'elezione del rappresentante del personale CNR presso il Consiglio di Amministrazione.

Poiché l'operato dei tecnici dell'Ufficio ICT si è concentrato esclusivamente nelle attività di predisposizione e di gestione del sistema informatico, questa nota si pone l'obiettivo di rispondere esaustivamente e, si spera, in via definitiva, ai dubbi sollevati da alcuni candidati e/o colleghi dopo l'esito elettorale, dubbi che hanno innescato un clima intollerabile di sospetti tanto infondati quanto dannosi per l'Ente e per tutti coloro che vi operano con senso di responsabilità e notevole spirito di appartenenza e di collaborazione.
Tali sospetti hanno assunto la forma di insinuazioni e accuse gravi, come quelle riportate da articoli di quotidiani nazionali, e sembra siano anche alla base di un'azione legale annunciata in una e-mail del 27 dicembre a firma di alcuni candidati alle elezioni.

I firmatari di questa ultima e-mail parlano di "squilibri, violazioni e potenziali doli" e della "inerzia da parte dell'Ente a fornire chiarimenti". Sebbene **chiarimenti siano già stati forniti ad almeno uno dei suddetti firmatari, sia in via ufficiale sia per le vie brevi**, evidentemente non sono risultati sufficientemente chiari, in quanto la loro comprensione implica una puntuale conoscenza delle misure organizzative adottate dall'Ente e degli aspetti di profilo più specificatamente tecnico informatico.

Dal momento che dell'azione legale non conosco le motivazioni, reputo opportuno chiarire nel seguito alcuni argomenti trattati nei suddetti articoli giornalistici, soffermandomi più in particolare sulle questioni di carattere tecnico-informatico.

- Risposta alla seguente affermazione: *"Il 29 ottobre, giorno della sfida finale, accadono cose strane. Si scopre che un pacchetto consistente di voti (digitali)* ***destinati all'ingegner Fantini*** *proviene dagli stessi protocolli Ip, il sospetto è che possano essere partiti dallo stesso computer… Ci sono 1.080 voti partiti da 78 Ip: 1.080 voti sospetti su un totale di 5.382, un quinto."* (Corrado Zunino, *La denuncia di un candidato: "Brogli per le elezioni al Cnr"*, la Repubblica, 19 dicembre 2019)

  Da una rapida lettura del documento allegato, che descrive la piattaforma applicativa utilizzata (*Votazioni CNR*) tutti potranno comprendere che il sistema è concepito per rendere impossibile l'effettuazione delle operazioni di spoglio da parte di soggetti privi delle chiavi di criptazione. In questo caso sono state generate due chiavi, consegnate a due commissari designati dall'Ente.
  Un'importante caratteristica del sistema, fin dalla sua prima versione del 2015, consiste nella criptazione dell'espressione di voto che viene registrata in maniera univoca, unitamente alla registrazione

completamente disgiunta dell'effettuata votazione da parte di un utente. Ciò, oltre a garantire naturalmente l'impossibilità per un utente di esprimere più preferenze, garantisce l'assoluto anonimato delle preferenze stesse, le quali non possono essere in alcun modo riconosciute neanche dai tecnici addetti al mantenimento funzionale del Sistema.
Più in particolare, la procedura prevede che gli utenti possano accedere alla piattaforma utilizzando le proprie credenziali Siper ed esprimere la propria preferenza. Il sistema richiede conferma prima di registrare effettivamente l'espressione di voto. Una volta che l'utente ha confermato la sua scelta il sistema registra in maniera completamente disgiunta l'effettuazione del voto, con relativa data, ora e indirizzo IP, e l'espressione di voto viene criptata per renderla segreta e anonima. Ad ogni ulteriore accesso da parte dell'utente il Sistema non permette più di votare notificandogli con opportuna messaggistica di avere già espresso la propria preferenza.
Non si comprende quindi sulla base di quali elementi di fatto possa essere stata formulata un'affermazione tanto grave!

- Risposta alla seguente affermazione: "*Le irregolarità sono a catena: per un passaggio elettorale avvenuto online non c'è mai stato l'invio di una mail che attestasse all'avente diritto l'avvenuto voto… Lo sconfitto, Vito Mocella, raggiungerà il compartimento che si occupa delle investigazioni digitali e denuncerà tutto: "L'assenza di un'email di conferma poteva agevolmente consentire l'inserimento di voti in maniera abusiva, stanti le deboli misure di sicurezza informatica messe in campo nella procedura stessa".* (Corrado Zunino, *La denuncia di un candidato: "Brogli per le elezioni al Cnr"*, la Repubblica, 19 dicembre 2019)

  Sia in occasione del ballottaggio sia del primo turno elettorale non si è proceduto con l'invio di una mail - all'indirizzo istituzionale del dipendente - a conferma del voto effettuato, contrariamente a quanto avvenuto nelle precedenti votazioni (elezioni rappresentante personale CNR presso il CdA - 2015, elezioni membri interni dei Consigli Scientifici di Dipartimento - 2019).
  Questa, che apparentemente può sembrare una "irregolarità", si configura in realtà come una miglioria procedurale, in linea con quanto previsto dall'art. 4 del Decreto del Presidente del CNR, Prot. n. 0058734/2019, del 09.08.2019, "*Avvio delle consultazioni telematiche per l'elezione di un componente del Consiglio di Amministrazione tra ricercatori e tecnologi di ruolo dell'Ente*".
  È infatti naturale che a distanza di quattro anni siano stati effettuati perfezionamenti sia tecnici che di processo. Ad esempio, oltre a introdurre importanti miglioramenti tecnologici per garantire prestazioni più elevate del sistema informatico, sono stati più chiaramente formulati i messaggi presentati all'utente durante lo svolgimento della procedura di voto.
  La modalità utilizzata per la votazione prevede il riconoscimento degli utenti attraverso l'autenticazione, basata sul protocollo LDAP (che conserva le credenziali in forma criptata), con il proprio account CNR; la comunicazione tra browser utilizzato dall'utente e il server che ospita la piattaforma "Votazioni CNR" basata sul protocollo *https* (anch'esso cifrato); il salvataggio in modo completamente anonimo dell'espressione di voto. **Essa è comunque concettualmente e operativamente identica a quella utilizzata per la votazione di quattro anni fa.**
  Un elemento degno di nota consiste nel fatto che le contestazioni sul mancato invio della e-mail di conferma del voto non siano state sollevate subito dopo il primo turno elettorale.
  Comunque, **la ricezione di una e-mail non può di per sé attestare in modo certo e univoco l'avvenuto voto**.
  Un altro aspetto assai rilevante alla prova dei fatti è che **nessun utente ha mai segnalato malfunzionamenti o denunciato furti di identità e relative espressioni di voto a propria insaputa**.
  Il funzionamento complessivo delle procedure informatiche è inoltre **totalmente tracciato e conservato**, ciò a garanzia di trasparenza, anche nell'ipotesi di ispezioni da parte di autorità legittimamente preposte allo scopo.
  Non si comprende quindi quali elementi abbiano consentito di riscontrare "*le deboli misure di sicurezza informatica messe in campo nella procedura stessa*"!

- Risposta alla seguente affermazione: "*E il sistema allestito per l'intera tornata non aveva una certificazione adeguata, constaterà la polizia postale."* (Corrado Zunino, *La denuncia di un candidato: "Brogli per le elezioni al Cnr"*, la Repubblica, 19 dicembre 2019)

Il sistema non è certificato e non c'è bisogno della polizia postale per constatarlo (nonostante una sua visita potrebbe risultare auspicabile a questo punto, visto il clima che si è venuto a creare!).
Sarebbe importante comprendere a che tipo di certificazione si fa riferimento: gestione della qualità (ISO serie 9000 e Vision 2000), gestione della qualità del software (ISO serie 25000), gestione della sicurezza informatica (ISO 27001), etc.

Vale la pena precisare che **neanche il sistema utilizzato nelle precedenti votazioni era certificato!**
Ritengo inoltre doveroso sottolineare che il processo di certificazione è costoso, complesso e molto impegnativo per una pubblica amministrazione. Il CNR non ha mai ritenuto opportuno procedere con la certificazione per nessuno dei sistemi (e sono tanti!) sviluppati dallo stesso Ente.
Le Unità Funzionali (Software Factory e Centro Servizi) che operano all'interno dell'Ufficio ICT adottano, in ogni caso, strumenti, tecniche e principi tali da consentire di gestire tutto il processo di produzione, manutenzione e gestione del software conservando traccia e relativa documentazione degli interventi/operazioni effettuati sia a livello di sviluppo e/o sistemistico sia a livello utente.
Mi sembra comunque importante sottolineare che molti di questi sistemi (si vedano, ad esempio, SIGLA, Selezioni online, Scrivania digitale, etc.) sono oggetto da anni di ***riuso*** da parte di altre pubbliche amministrazioni, che li utilizzano senza essersi mai poste il problema della certificazione dei software resi disponibili dal CNR.
Tali realizzazioni, tra l'altro, rappresentano esempi significativi di software depositato presso il Repository gestito in collaborazione dall'Agenzia per l'Italia Digitale e dal Team per la trasformazione digitale della Presidenza del Consiglio dei Ministri, nell'ambito dell'iniziativa "Developers Italia".

- Risposta alla seguente affermazione: "*Vito Mocella fa notare che il Consiglio nazionale delle ricerche è membro fondatore del Garr, la rete italiana a banda ultralarga dedicata alla comunità dell'istruzione, della ricerca e della cultura, e allo stesso Cnr sono attribuite centinaia di migliaia di Ip: "La struttura non ha alcuna necessità di sopperire a una presunta scarsità di indirizzi pubblici", si legge nella denuncia."* (Corrado Zunino, *La denuncia di un candidato: "Brogli per le elezioni al Cnr"*, la Repubblica, 19 dicembre 2019)

  Non mi soffermo sulla questione della "denuncia" in quanto personalmente ne sono venuto a conoscenza unicamente dall'articolo citato e, più di recente, dalla già menzionata e-mail del 27 dicembre scorso.

  Dal punto di vista tecnico mi corre l'obbligo di precisare che da alcuni anni si dispone dell'IPv6, vale a dire la versione del protocollo IP che fornisce uno spazio di indirizzamento largamente superiore a quello dell'IPv4. L'adozione su larga scala dell'IPv6 consentirebbe di risolvere definitivamente il problema dell'esaurimento degli indirizzi resi disponibili dall'IPv4, ancora largamente utilizzato.
  Moltissime organizzazioni pubbliche e private, nazionali e internazionali, continuano infatti a utilizzare il sistema di indirizzamento dell'IPv4 che non mette a disposizione un numero di indirizzi pubblici sufficienti a soddisfare le esigenze degli utenti. Con la diffusione straordinaria di dispositivi mobili tali organizzazioni si trovano spesso nelle condizioni di dover ricorrere al cosiddetto meccanismo NAT "Network Address Translation", implementato da dispositivi *router* o *firewall*, i quali, attraverso tecniche di tipo diverso, permettono di utilizzare un unico indirizzo pubblico per più indirizzi privati.
  In ogni caso, trattandosi di un sistema di votazione di tipo telematico - che offre la possibilità di votare da qualsiasi postazione fissa o mobile, da qualsiasi parte del territorio nazionale e anche internazionale - il CNR ha ritenuto opportuno garantire esclusivamente il corretto funzionamento dei sistemi centrali che consentono di gestire le operazioni di voto. Non può essere certamente compito del CNR controllare infrastrutture di rete complesse gestite da diversi operatori e basate su tecnologie anche molto diversificate tra loro.
  Eventuali dubbi sul corretto utilizzo delle postazioni fisse e/o dei dispositivi mobili possono essere sciolti solo mediante indagini a cura delle autorità preposte alla verifica delle operazioni effettuate sulla rete, risalendo così a possibili azioni dolose. In una tale circostanza l'Ente potrà fornire elementi conoscitivi utili allo scopo delle indagini.

Considerato che coloro che nutrono dubbi sul corretto svolgimento delle operazioni di voto sembra abbiano attivato le autorità amministrative e giudiziarie preposte alla vigilanza e al controllo degli adempimenti in

questione, mi preme evidenziare che i miei collaboratori ed io personalmente siamo e saremo a totale disposizione di tutti coloro che saranno legittimamente delegati a qualsivoglia attività ispettiva.

A nome di tutto l'Ufficio di cui sono responsabile, auspico che eventuali ispezioni possano avvenire quanto prima, in modo da fare cessare tutti i sospetti e le polemiche di questi ultimi tempi.

Ritengo doveroso sottolineare che anche in questa occasione, come in altre precedenti, il personale ICT, designato a supportare l'Amministrazione nella gestione delle procedure tecnico-informatiche, ha operato in modo ineccepibile e, soprattutto, ha ancora una volta dimostrato considerevole competenza unita a grande senso del dovere e spirito di sacrificio.
Trovo quindi particolarmente deprecabile che vengano mosse accuse formulate in modo tanto generalizzato da colpire inevitabilmente tutti coloro che, a diverso titolo, si sono adoperati per l'efficace svolgimento delle elezioni del Rappresentante del personale CNR presso il CdA.

Spero di avere fornito chiarimenti utili a dirimere le questioni oggetto di polemiche/insinuazioni/accuse mosse da soggetti diversi in forme diverse.

Dal momento che tali questioni sono ormai di pubblico dominio, ritengo opportuno e doveroso informare coloro che intendessero formulare legittime richieste di ulteriori chiarimenti di profilo tecnico all'Ufficio ICT che, d'ora in poi, le risposte saranno sicuramente fornite e, al contempo, indirizzate a tutti i componenti della comunità CNR.
Si tratta quindi di una misura improntata a trasparenza effettiva, che può certamente contribuire a evitare l'utilizzo non corretto di informazioni.
Faranno ovviamente eccezione a questa misura le risposte fornite dall'Ufficio ICT a fronte di eventuali richieste da parte di autorità amministrative e giudiziarie.

A proposito delle modalità di comunicazione corre l'obbligo di segnalare che, analizzando l'intestazione del messaggio, la e-mail del 27.12.2019 sopra menzionata è stata inviata ad un indirizzo di posta elettronica inesistente del dominio CNR (**personaledipendente@cnr.it**) e, probabilmente in copia nascosta, ad una lista di indirizzi e-mail predisposta dal mittente che risulta anonimo, sollevando il dubbio che il messaggio potesse provenire da una lista di distribuzione ufficiale/istituzionale. Pur essendo stato più volte rivendicato da molti il mancato invio della e-mail di conferma del voto, i firmatari di questa ultima nota dimostrano essi stessi che l'utilizzo del servizio di posta elettronica tradizionale rappresenta di per sé un canale di comunicazione non idoneo a certificare provenienza e destinazione dei messaggi.
Tutti infatti dovrebbero sapere che, per coloro che possiedono una sufficiente familiarità con le tecnologie Internet, non è particolarmente difficile "manipolare" le informazioni del mittente di un messaggio e-mail e inviare un messaggio indicando un indirizzo contraffatto (reale o inesistente). I server che gestiscono servizi di distribuzione di e-mail spesso non filtrano tali messaggi e possono indurre in errore il destinatario.

Con lo spirito di appartenenza e di solidarietà tra colleghi, che da sempre caratterizza il personale dell'Ufficio ICT, a nome di tutti noi colgo l'occasione per formulare l'augurio per un 2020 stimolante, positivo e molto sereno.

Maurizio Lancia

LANCIA MAURIZIO
Date 30.12.2019 22:49:31 CET