Divisione Servizi

Direzione Centrale Servizi Istituzionali e di Riscossione
Settore Versamenti e rapporti con gli enti esterni
Ufficio Strategia dei rapporti con enti

ANCI - Associazione Nazionale
Comuni Italiani
PEC: anci@pec.anci.it

OGGETTO: Rafforzamento delle misure di consapevolezza e prevenzione in materia di protezione dei dati personali e cybersicurezza a seguito di una recente campagna di phishing rivolta agli utenti del servizio Siatel v2.0 Punto Fisco

A seguito di alcune recenti notizie che hanno messo in evidenza l'avvio di fraudolente campagne di *phishing* nei confronti degli utenti del servizio *Siatel v2.0 Punto Fisco*, è emersa la necessità per gli enti, tra cui i Comuni, di rafforzare le misure di prevenzione e contrasto ai rischi derivanti dalle minacce informatiche, che possono compromettere la sicurezza delle informazioni e la tutela dei dati personali.

Tali eventi confermano come il fattore umano continui a costituire uno dei principali elementi di vulnerabilità nell'ambito della sicurezza informatica e rendono, pertanto, indispensabile promuovere una campagna di sensibilizzazione tra il personale comunale autorizzato ad accedere all'Anagrafe Tributaria affinché sia accresciuta la consapevolezza nell'uso degli strumenti a disposizione.

Si ritiene opportuno richiamare, in tale contesto, i principali strumenti che questa Agenzia ha nel tempo realizzato e messo a disposizione degli enti per

consentire un'efficace ed efficiente gestione degli utenti e del monitoraggio delle operazioni:

- il cruscotto di gestione autonoma delle abilitazioni tramite l'applicazione Vitruvio;
- la consultazione - in ogni momento - dei log di tracciamento tramite il sistema Monade delle interrogazioni effettuate nell'ultimo anno;
- il sistema di *alerting* in caso di accessi potenzialmente anomali;
- la verifica di inattività da parte degli operatori e la conseguente cancellazione dell'utenza.

Oltre ai sopra menzionati strumenti, anche a seguito dei recenti tentativi di *phishing*, questa Agenzia ha invitato più volte i propri Referenti regionali interni a contattare i Responsabili e i Supervisori delle convenzioni di cooperazione informatica, al fine di informare e sensibilizzare il personale dell'Ente di appartenenza sul tema delle frodi tramite *social engineering* (tecniche di ingegneria sociale) e per scongiurare che tali iniziative fraudolente vengano perpetrate ai danni di altri Comuni o enti terzi che accedono alla banca dati. Al riguardo, si ricorda che:

- l'Agenzia non chiede mai né di fornire le credenziali e il certificato di postazione né di attivare sessioni di assistenza remota (ad esempio utilizzando i software *Windows Quick Assist - Assistenza rapida, AnyDesk, TeamViewer, VNC - Virtual Network Computing*) sui terminali dei Supervisori, dei Responsabili e degli operatori. In caso di dubbio, i Supervisori devono contattare i Referenti dell'Agenzia ai contatti istituzionali o il *call center* Sogei al numero 800863116;
- il Responsabile di convenzione, il Supervisore e il Supervisore operativo, il Responsabile dello scambio dati, l'Amministratore locale devono indicare in fase di registrazione una casella di posta elettronica personale nominativa su dominio istituzionale dell'Ente;
- la validazione degli operatori da parte dei Referenti regionali si conclude positivamente se e solo se gli operatori dispongono di una casella di posta

elettronica personale nominativa su dominio istituzionale dell'Ente e almeno un Supervisore risulta attivo. Si fa presente che, al fine di garantire continuità operativa e gradualità nell'applicazione delle misure di irrobustimento, attualmente i Referenti di Agenzia possono ancora temporaneamente accettare, per gli operatori, in via residuale, le caselle di posta elettronica "funzionali", purché su dominio istituzionale.

Per gli enti sono stati, altresì, pubblicati avvisi dedicati al tema della sicurezza direttamente sull'applicazione *Vitruvio*.

In tale contesto, si rappresenta, inoltre, che questa Agenzia avvierà ulteriori interventi per potenziare e rafforzare gli strumenti di accesso alle banche dati da parte degli enti esterni, prevedendo un piano di sostituzione delle attuali credenziali di accesso con gli strumenti SPID e CIE per l'identificazione personale degli utenti degli enti.

Si ricorda, inoltre, che:

- l'accesso alle informazioni è consentito, sotto la responsabilità dell'Ente, nell'esclusivo ambito delle finalità dichiarate e che l'accesso per fini non istituzionali costituisce illecito che può dare luogo a conseguenze civili, penali, amministrative e contabili;
- i servizi non possono essere utilizzati da soggetti esterni all'Ente, eccetto i soggetti che assumono la qualifica di Responsabili del trattamento ai sensi dell'articolo 28, comma 2, del Regolamento UE 2016/679;
- in nessun caso è consentita l'esposizione dei servizi dell'Agenzia verso l'esterno;
- l'Ente è tenuto ad effettuare controlli, anche a campione, per verificare la legittimità degli accessi e il rispetto delle disposizioni vigenti in materia di protezione dei dati personali.

Alla luce di quanto sopra, si chiede a codesta Associazione di voler valutare l'opportunità di informare i Comuni in merito ai temi segnalati nonché di promuovere specifiche iniziative di informazione, formazione e sensibilizzazione volte a:

- rafforzare la conoscenza dei rischi connessi alle campagne di *phishing* e ad altre tecniche di *social engineering*;
- richiamare l'attenzione sulla corretta gestione delle credenziali di autenticazione e delle *password* di accesso alle banche dati dell'Agenzia delle entrate, evitando pratiche non conformi ai princìpi di sicurezza, quali la condivisione delle credenziali o la conservazione delle stesse in modalità non protette;
- diffondere le migliori pratiche in materia di autenticazione forte, gestione degli accessi e protezione delle postazioni di lavoro, anche in vista del futuro passaggio all'autenticazione tramite SPID e CIE;
- favorire la tempestiva segnalazione alle competenti autorità (all'Autorità per la Cybersicurezza Nazionale, all'Autorità Garante per la protezione dei dati personali per le ipotesi di violazione dei dati personali ai sensi dell'articolo 33 del Regolamento UE 2016/679 e alle forze di polizia) di eventi sospetti, tentativi di compromissione o possibili incidenti di sicurezza, informando opportunamente degli stessi anche l'Agenzia delle entrate;
- promuovere la conoscenza degli obblighi derivanti dalla normativa vigente in materia di protezione dei dati personali e sicurezza dei sistemi informativi;
- rafforzare le procedure di controllo per la verifica della legittimità degli accessi.

Si ritiene, infatti, che un costante investimento nella formazione del personale e nella diffusione della cultura della sicurezza costituisca uno strumento essenziale per prevenire accessi abusivi alle banche dati pubbliche, ridurre il rischio di violazioni dei dati personali e garantire il corretto esercizio delle funzioni istituzionali affidate agli enti locali.

Confidando nella consueta collaborazione istituzionale di codesta Associazione e nella sensibilità verso tematiche di particolare rilievo per la tutela

dei dati personali e la sicurezza delle informazioni, si resta a disposizione per ogni utile iniziativa di supporto e approfondimento.

IL VICEDIRETTORE
CAPO DIVISIONE
Paolo Savini
Firmato digitalmente