

COMUNICATO STAMPA CONGIUNTO

Protezione informatica in *virtual appliance* con l'utilizzo di programmi *open source*

ICT: CNIPA E CONSIP VARANO UN PACCHETTO SOFTWARE PER AUMENTARE LA SICUREZZA DI APPARATI, DATI E SERVIZI DELLA P.A.

Si rafforza la blindatura dei servizi informatici interconnessi con l'SPC

Roma, 25 giu. – La Pubblica Amministrazione innalza ulteriori barricate per proteggere i propri sistemi informatici dagli attacchi e dagli incidenti. E lo fa grazie all'interconnessione e all'integrazione tra amministrazioni centrali e locali, realizzate con l'SPC-Sistema Pubblico di Connettività, la maggiore infrastruttura telematica pubblica d'Europa, già operativa e il cui network è stato costituito con le relative connessioni e i servizi di base, costituendo così uno dei cardini per lo sviluppo del processo di e-Government in atto. La Commissione di coordinamento dell'SPC ha appena deliberato l'avvio operativo di una specifica *Community* della sicurezza ICT nel settore pubblico. Per la prima volta in ogni amministrazione centrale aderente all'SPC, sulla base delle regole tecniche, viene individuata una **Unità Locale di Sicurezza**, cui è affidata sia la responsabilità di porre in atto tutte le fasi di prevenzione degli incidenti ICT, sia la gestione operativa degli eventuali incedenti informatici.

In particolare, dopo un anno di attività congiunta in questo specifico settore, il CNIPA e la CONSIP hanno annunciato di mettere a disposizione delle Pubbliche amministrazioni centrali il risultato di un progetto pilota per la sicurezza informatica, condotto dal CERT-SPC, il *Computer Emergency Response Team del Sistema Pubblico di Connettività* attivo al CNIPA sul modello adottato a livello internazionale, e dall'ULS MEF/CONSIP, l'Unità Locale di Sicurezza di CONSIP, primo soggetto in ambito pubblico ad aver attivato questo tipo di struttura, destinata a diventare progressivamente operativa in tutte le pubbliche amministrazioni aderenti all'SPC. Un'apposita piattaforma è stata presentata dal **prof. Fabio Pistella, presidente del CNIPA**, e dal **dott. Danilo Broggi, amministratore delegato della CONSIP**, in un incontro su «*Gli incidenti informatici nell'SPC: come difendersi*», presenti anche i Dirigenti dei Sistemi Informatici Automatizzati della Pubblica Amministrazione.

Si tratta dell'insieme di applicazioni (*suite*) "**RIM-Risorse per l'Incident Management**", inserita in un dvd e composta da programmi nativi *open source*, che consente di supportare rapidamente e in modo evoluto e semplificato le complesse attività di monitoraggio, protezione, assistenza e ripristino svolte delle varie ULS in caso di attacchi e, soprattutto, di incidenti informatici.

Simili iniziative assumono particolare rilievo soprattutto per favorire la cultura della sicurezza informatica sensibilizzando, così, ogni amministrazione a dotarsi di presidi efficienti. Nel 2007 sono state scoperte **6.437 nuove vulnerabilità** (fonte: ISS-XForce) e nella seconda metà dello stesso anno sono stati registrati non meno di **500 mila nuovi malware** (fonte: Symantec).

Fabio Pistella ha sottolineato che «*per la prima volta, con il sostegno di un'innovativa legislazione, viene posta al massimo livello di attenzione la sicurezza ICT nella PA con la costituzione di un dominio affidabile, costituito da una federazione di domini di sicurezza in cui diversi soggetti, grazie alle Unità Locali di Sicurezza individuate, si impegnano reciprocamente ad adottare tutte le necessarie misure preventive e operative che verranno resi disponibili a tutte le PA. È proprio di questi giorni, infatti, la pubblicazione in Gazzetta Ufficiale delle 'Regole tecniche' che costituiscono le ULS e definiscono la sicurezza ICT della PA su SPC. L'intensa collaborazione tecnologica sviluppatasi tra il CNIPA e la CONSIP, inoltre, ha consentito di mettere a punto gli strumenti amministrativi per garantire a cittadini ed imprese la sicurezza del trattamento dei loro dati personali*».

Danilo Broggi ha affermato che «*il progetto comune CNIPA-CONSIP s'inserisce nel solco di una collaborazione già avviata con successo nei mesi scorsi con l'accordo per l'istituzione dell'Osservatorio sui prezzi*

delle forniture ICT. Il tema della sicurezza è strategico per chi, come CONSIP, lavora al servizio delle Pubbliche amministrazioni. Garantire la massima affidabilità dei sistemi e la protezione dei dati è fondamentale per consentire loro di lavorare in modo sicuro, senza blocchi e ritardi e, quindi, fornire servizi sempre più efficienti. La sfida della sicurezza si vince anche unendo le forze contro gli attacchi e gli incidenti e condividendo conoscenze, in modo da realizzare sinergie fra soggetti che hanno sviluppato best practice in questo settore. Anche da questo punto di vista SPC è una grande risorsa per tutte le amministrazioni e un'infrastruttura strategica per la crescita di tutto il Paese, perché facilita queste sinergie».

La suite "RIM" rientra nelle iniziative volte a realizzare applicazioni ad alto valore aggiunto nell'ambito del programma di e-Government ed è stata progettata mettendo a fattor comune le specifiche esperienze di CNIPA e CONSIP. Lo scopo è quello di far agire l'intero sistema informatico pubblico come un'unica squadra, non solo condividendo informazioni, strategie e strumenti di sicurezza, ma anche implementando a loro volta le applicazioni per adeguarle a nuovi scenari. L'utilizzo di licenza d'uso di tipo *open source*, infatti, prevede espressamente la possibilità di modificare il codice del programma, di copiarlo, distribuirlo e di evolverlo, ma anche di sviluppare e condividere specifiche funzionalità di *backup* e *restore* delle applicazioni e informazioni per garantire una corretta ripartenza dei sistemi a fronte di eventuali "cadute" per incidenti e attacchi.

Per consentire una totale portabilità delle soluzioni, a prescindere dall'*hardware* e dai sistemi applicativi usati dagli utenti, la suite "RIM" è stata realizzata da CNIPA e CONSIP con la tecnica della "virtual appliance", ossia della "virtualizzazione" di un ambiente pre-configurato (sistema operativo ed applicazioni) per l'immediato impiego nel singolo ambiente di esercizio. In questo modo è stato possibile realizzare un dvd che contiene tutto l'ambiente virtuale realizzato e utilizzabile semplicemente su qualunque server.

Nel corso dell'ultimo anno il CERT-SPC ha inviato alla comunità della sicurezza in SPC **105 bollettini di sicurezza**, **50 segnalazioni** ed ha fornito supporto nella gestione di **6 incidenti di sicurezza**.

L'SPC si basa su una avanzata rete di telecomunicazioni realizzata in modo dedicato per la PA con il supporto dei maggiori operatori di mercato delle telecomunicazioni. Questa mega-Intranet pubblica è ormai pienamente operativa e vi hanno aderito le **60 amministrazioni centrali**. Non solo, ma sono stati già stipulati oltre **300 contratti** con le amministrazioni locali (Regioni, Province, Comuni, Asl) per la fornitura di servizi SPC, e siglati tre protocolli d'intesa con le Regioni Emilia Romagna, Toscana e Umbria, le cui reti così entrano a far parte dell'SPC, trasformandolo gradualmente in una "rete federale". Proprio per questo la *Community* della sicurezza ICT dell'SPC entro l'anno sarà estesa anche alle Amministrazioni territoriali.



Sul modello ormai adottato a livello internazionale, il **CERT-SPC Computer Emergency Response Team** del Sistema Pubblico di Connettività, è la struttura collocata presso il CNIPA con funzioni di referente centrale nazionale per la prevenzione, il monitoraggio, il coordinamento informativo e l'analisi degli incidenti di sicurezza in SPC. È formato da esperti di sicurezza informatica e, in primo luogo, assolve il compito di raccogliere e diffondere all'interno di SPC le informazioni utili per garantire il più elevato livello di sicurezza possibile.



Le **Unità locali di sicurezza**, una per ogni dominio connesso al SPC, concorrono insieme alla struttura centrale al coordinamento, al mantenimento e alla verifica del livello di sicurezza minimo garantito limitatamente al singolo dominio. La ULS Mef/Consip, costituita nel dicembre 2006, è stata la prima struttura a diventare operativa nell'ambito di SPC, dopo soli cinque mesi dalla costituzione.

Contatti:

CNIPA: Dario de Marchi
tel. 06 8526 4233 – fax 06 8526 4137
ufficiostampa@cnipa.it
www.cnipa.gov.it

CONSIP: Alessandro Grilli
tel. 06 8544 9267 – fax 06 8544 9636
alessandro.grilli@tesoro.it
corporateidentity.consip@tesoro.it
www.consip.it