

[HOME](#) » [IT World](#) » Cybersecurity, il governo firma il decreto

PRIMO PIANO

## Cybersecurity, il governo firma il decreto

Il provvedimento pone le basi per la definizione di un'architettura di sicurezza nazionale e di protezione delle infrastrutture critiche. Intanto la **Camera lancia l'appello: "Introdurre il reato di furto di identità digitale e creare Cert nazionali per battere il crimine informatico"**

di Federica Meta



L'Italia accelera sulla sicurezza informatica. Il presidente del Consiglio, Mario Monti, e i ministri membri del Comitato interministeriale per la sicurezza della Repubblica hanno firmato un decreto "per accrescere le capacità del Paese di confrontarsi con le minacce alla sicurezza informatica". Lo rende noto Palazzo Chigi sottolineando che "l'Italia si dota così della prima definizione di un'architettura di sicurezza cibernetica nazionale e di protezione delle infrastrutture critiche. Il decreto pone le basi per un sistema organico,

all'interno del quale, sotto la guida del presidente del Consiglio, le varie istanze competenti possono esercitare in sinergia le loro competenze".

La Presidenza del Consiglio spiega che "gli attacchi alla sicurezza informatica negli ultimi anni hanno avuto una crescita esponenziale". Assinform stima che il 40% degli attacchi richiedono almeno 4 giorni per essere risolti. Nel 90% dei casi l'attacco ha successo a causa dell'errata configurazione del sistema di sicurezza e per la mancanza di competenze specifiche. I costi sostenuti da privati e P.A. per proteggersi sono consistenti: Gartner li quantifica in 55 miliardi di dollari nel 2011, 60 nel 2012 e 86 (stimati) entro il 2016.

Il provvedimento risponde all'urgenza rappresentata lo scorso maggio in Senato con la cosiddetta "mozione Ramponi", che impegna il Governo a realizzare ogni iniziativa per precisare, nel rispetto delle responsabilità già individuate dalla legge, un'architettura istituzionale che assicuri coerenza d'azione per ridurre le vulnerabilità dello spazio cibernetico, accrescere le capacità d'individuazione della minaccia e di prevenzione dei rischi e aumentare quelle di risposta coordinata in situazioni di crisi. A luglio il Parlamento ha approvato la legge n. 133/2012, che pone in carico al sistema per la sicurezza nazionale e all'intelligence il ruolo di catalizzatore della protezione cibernetica del Paese".

Tre i livelli d'intervento individuati, "uno politico per l'elaborazione degli indirizzi strategici, affidati al Comitato interministeriale per la sicurezza della Repubblica; uno di supporto operativo ed amministrativo e a carattere permanente, il Nucleo per la Sicurezza Cibernetica presieduto dal Consigliere Militare del Presidente del Consiglio; uno di gestione di crisi, affidato al Tavolo interministeriale di crisi cibernetica. Il decreto prevede inoltre la messa a punto, in raccordo con il settore privato, di un quadro strategico nazionale, che si tradurrà nella prossima adozione di un Piano nazionale per la sicurezza dello spazio cibernetico". Il provvedimento sarà pubblicato nei prossimi giorni sulla Gazzetta Ufficiale.

Anche il Parlamento accende i riflettori sulla cybersecurity. La commissione Trasporti, poste e telecomunicazioni della Camera, chiudendo l'indagine conoscitiva sulla sicurezza informatica delle reti, chiede l'introduzione del reato di **furto di identità digitale**, prevedendo adeguate sanzioni penali, per combattere il **furto di identità digitale**. "I sistemi attualmente disponibili per la protezione dei dati che viaggiano sulle reti telematiche - si legge nel documento conclusivo - presentano numerosi aspetti di debolezza, sia dal punto di vista della security sia sotto il profilo della privacy, che rendono relativamente facile, anche per soggetti non particolarmente esperti di

 Cor.Com  Google 
**Cor.Com** la newsletter  
Newsletters di data
The news you need: **ISCRIVITI!**
[Archivio newsletter](#)

 FEED DA: **ICT4Executive**
**ANALISI**

Supply chain, quando la chiave è il data management

**SOFTWARE AS A SERVICE**

Otto applicazioni Cloud per le PMI "garantite" da Microsoft

**CULTURA**

I libri storici italiani diventano digitali

**ANALISI**

Logistica, le imprese italiane pensano poco alla scala internazionale

**SOLUZIONI VERTICALI**

Un ERP ad hoc per distribuire materiale elettrico

information technology mettere in chiaro comunicazioni riservate ed utilizzarle a fini dolosi e comunque illegali".

Banche e Poste italiane sono comunque attrezzate contro le minacce di perdita totale delle informazioni (disaster recovery). Nel settore bancario tuttavia, avverte la Commissione, non mancano "criticità" nel "rapporto con alcuni fornitori qualificati, in particolare, con gli operatori di telecomunicazioni".

Tra le minacce "che appaiono più significative per la sicurezza della rete figurano quelle consistenti nel **furto dell'identità** digitale e quelle rivolte ai cloud computing e alle reti wired e wireless facenti capo a organizzazioni pubbliche o private". Sul fronte del **furto di identità** la commissione Trasporti propone la individuazione di un "identity provider" nazionale, la realizzazione di una federazione degli "identity provider" "per garantire la circolarità dell'identificazione, a prescindere dallo strumento operativo utilizzato, su tutto il territorio nazionale, consentendo al cittadino di operare con un'unica **identità** digitale". E insieme a username e password l'utente dovrebbe essere garantito da "sistemi one-time-password, smart card o addirittura sistemi biometrici". La commissione Trasporti propone, infine, al termine di un'indagine condotta ascoltando esperti di aziende del settore e rappresentanti delle istituzioni, "la costituzione di squadre di livello nazionale per la risposta ad emergenze informatiche (CERT nazionali), l'adozione di una strategia di sicurezza informatica nazionale, l'elaborazione di piani di emergenza nazionali, l'organizzazione di esercitazioni nazionali e la partecipazione, come già avvenuto nel recente passato, ad esercitazioni europee".

23 Gennaio 2013

TAG: [mario monti](#), [Comitato interministeriale per la sicurezza, cybersecurity, commissione trasporti](#) [tlc camera](#), [furto identità digitale](#), [cert](#)

## Correlati

### IL FORUM DEL CORRIERE DELLE COMUNICAZIONI

Cybersecurity, serve un G20

La sicurezza informatica è strategica per garantire infrastrutture critiche e tutelare i dati dei cittadini. A dibattito Melissa Hathaway, Judy Baker, John N. Stewart e Andrea Rigoni, fra i massimi esperti mondiali di cybersecurity, al Forum del Corriere delle Comunicazioni

Quotidiano online d'informazione sull'ICT: notizie, approfondimenti e analisi sul mondo dell'Information Technology, il digitale nella pubblica amministrazione, i nuovi media, le telecomunicazioni e la sat economy.

[MAPPA DEL SITO](#) | [CHI SIAMO](#) | [CONTATTACI](#)

CORPO 10 SOC. COOP. A R.L. - LARGO DI TORRE ARGENTINA 11 - 00186 ROMA - P.IVA: 08650251005  
corrierecomunicazioni.it iscritto al Registro della Stampa del Tribunale di Roma n. 54/2009 in data 12/02/2009

Powered by



media agency