



PALAZZI

SPREAD

FELUCHE

AL VERDE

JAMES BOND

PORPORA

POP-TECH

TRUMP

MOBILITÀ

Cyber security, che cosa cambia con la Direttiva Nis

Michele Pierri

JAMES BOND

0

FOTO

i, De Poli e Salisbury.
i c'era al Senato a
ere di Global Health.
Foto di Pizzi



La cerimonia di
vicendamento tra
assi e Falsaperna al
ariato generale della
Difesa. Le foto

Il decreto attuativo del provvedimento comunitario - che per la prima volta affronta in modo organico e trasversale gli aspetti in materia di sicurezza informatica rafforzando la resilienza e la cooperazione in Europa - è stato approvato oggi in via definitiva dal Consiglio dei ministri. I fatti e il commento di Giustozzi (esperto Enisa e Cert-PA)

Uno dei provvedimenti più attesi nel campo della cyber security ottiene il via libera definitivo anche in Italia. Si tratta della direttiva sulla sicurezza delle reti e dei sistemi informativi dell'Unione europea, meglio nota come Nis, che oggi ha visto approvato dal Consiglio dei ministri il suo decreto attuativo.

GLI OBIETTIVI DEL DECRETO

Il decreto, che complice il periodo post-elettorale è stato approvato con qualche giorno ritardo rispetto al limite per il recepimento fissato il 9 maggio, persegue – si legge nella nota diramata da Palazzo Chigi al termine del CdM – “tre obiettivi principali”: promuovere una cultura di gestione del rischio e di segnalazione degli incidenti tra i principali attori economici, in particolare gli operatori che forniscono servizi essenziali per il mantenimento di attività economiche e sociali e i fornitori di servizi digitali; migliorare le capacità nazionali di cyber security; e rafforzare la cooperazione a livello nazionale e in ambito Ue.

PROTEGGERE I SERVIZI ESSENZIALI

Lo scopo è, innanzitutto, quello di assicurare la continuità dei servizi essenziali come energia, trasporti, salute, finanza e così via (i cui operatori dovranno essere identificati entro il 9 novembre di quest'anno), e di quelli digitali, ad esempio motori di ricerca, servizi cloud, piattaforme di commercio elettronico. Per riuscire nel compito, il decreto prevede l'adozione di misure tecnico-organizzative per ridurre il rischio e limitare l'impatto di incidenti informatici, l'obbligo di notifica di incidenti con impatto rilevante sulla fornitura dei servizi, e anche delle sanzioni. Parallelamente, il testo individua le Autorità competenti Nis e i rispettivi compiti, svolti in cooperazione con le omologhe autorità degli altri Stati membri, nonché il Computer Security Incident Response Team (Csirt) nazionale, con compiti di natura tecnica nella prevenzione e risposta ad incidenti informatici svolti in cooperazione con gli altri Csirt europei.

L'APPROCCIO NECESSARIO

Per **Corrado Giustozzi** – esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale per lo sviluppo del Cert della Pubblica Amministrazione e membro del Permanent Stakeholders' Group dell'Agenzia dell'Unione Europea per la Sicurezza delle Reti e delle Informazioni (Enisa) – il provvedimento approvato oggi è “di rilevanza primaria”. Da tempo, ha sottolineato all'agenzia *Cyber Affairs*, “il settore auspicava questo cambiamento, che renderà il livello di protezione omogeneo e uniforme a livello europeo”. Secondo l'esperto, l'aspetto più interessante delle nuove norme è “la linea adottata dal legislatore



à, Giro, Provenzano e
garetti all'Agorà di
do Bettini. Le foto di
Umberto Pizzi



...africano di Melania
rump in 70 foto



loardo Vianello e
gherita Boniver alla
ntazione del libro di
nna Lambertucci al
o di Adriano. Foto di
Pizzi

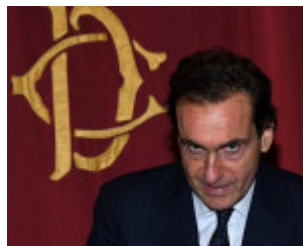
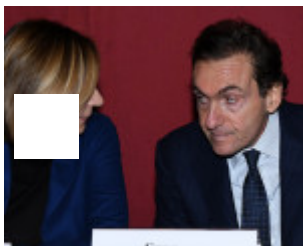
europeo, che ha usato lo stesso criterio del nuovo Regolamento Privacy, il Gdpr. Non si tratta più di un approccio prescrittivo", commenta, "con l'indicazione di cose precise da fare, ma si dà ai singoli Stati il compito di fare un'analisi del rischio, di scegliere le misure più idonee per raggiungere gli obiettivi indicati, e addirittura di autodenunciarsi in caso di problemi". Ciò, conclude l'esperto, segnala "l'assegnazione di una grande responsabilità, che segna davvero la necessità di una nuova sensibilità culturale sul tema della cyber security".

LE ULTIME MISURE

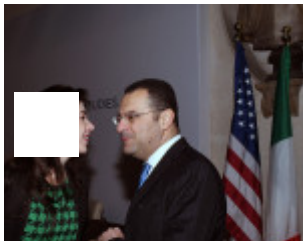
La direttiva Nis non è, in ogni caso, l'unica misura che inciderà sulla sicurezza informatica del Paese. Lo scorso anno, a febbraio, con il cosiddetto **Dpcm Gentiloni** che ha sostituito un analogo provvedimento del gennaio 2013 a firma dell'allora presidente del Consiglio **Mario Monti**, l'Italia ha rinnovato la sua architettura nazionale per la sicurezza cibernetica rafforzando il ruolo del Comitato interministeriale per la sicurezza della Repubblica e quello del Dipartimento delle informazioni per la sicurezza (diretto oggi dal prefetto **Alessandro Pansa**), creando un vicedirettore del Dis ad hoc per la cyber security (incarico che è poi andato al professor **Roberto Baldoni**). A ciò si è affiancato un nuovo piano nazionale sul tema, contenente diverse novità, come ad esempio un centro per la certificazione di software e hardware utilizzato dalla pubblica amministrazione.

0

Baldoni, Calipari, Dambruoso e Minniti discutono di cyber security alla Camera. Le foto



Chi sono gli esperti cyber che hanno incontrato Laura Galante al Csa. Le foto



Chi c'era a Roma Tre per parlare di cyber security e big data con Nimrod Kozlovski (Yale University). Le foto



**Lualdi si racconta
"Io Antonella, amata
Franco". Le foto di
Umberto Pizzi**



**Franceschini, Guerini,
D'Alema e Toschi al Senato
"Il caso Moro non è
uso". Foto di Pizzi**



ARCHIVIO FOTO