AGENZIA PER LA CYBERSICUREZZA NAZIONALE

CIRCOLARE 21 aprile 2022, n. 4336

Attuazione dell'articolo 29, comma 3, del decreto-legge 21 marzo 2022, n. 21. Diversificazione di prodotti e servizi tecnologici di sicurezza informatica. (22A02611)

(GU n.96 del 26-4-2022)

Vigente al: 26-4-2022

Alle amministrazioni pubbliche di cui all'articolo 1, comma 2 del decreto legislativo n. 165 del 2021 - Loro sedi

Oggetto: Attuazione dell'articolo 29, comma 3, del decreto-legge 21 marzo 2022, n. 21. Diversificazione di prodotti e servizi tecnologici di sicurezza informatica.

A) Premesse.

Con il decreto-legge 21 marzo 2022, n. 21, recante «Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina», il Governo ha ritenuto, tra l'altro, la straordinaria necessita' e urgenza di assicurare il rafforzamento dei presidi per la sicurezza, la difesa nazionale, le reti di comunicazione elettronica e degli approvvigionamenti di materie prime. A tale riguardo, l'art. 29, comma 1, del medesimo decreto-legge, prevede che, al fine di prevenire pregiudizi alla sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche di cui all'art. 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, derivanti dal rischio che le aziende produttrici di prodotti e servizi tecnologici di sicurezza informatica legate alla Federazione Russa non siano in grado di fornire servizi e aggiornamenti ai propri prodotti, in conseguenza della crisi in Ucraina, le medesime amministrazioni procedano tempestivamente alla diversificazione dei prodotti in uso.

Piu' nello specifico, il medesimo art. 29, secondo il combinato disposto dei commi 1 e 3, prevede che l'individuazione dei prodotti e servizi da diversificare avvenga in relazione alle categorie indicate con circolare dell'Agenzia per la cybersicurezza nazionale tra quelle volte ad assicurare le seguenti funzioni di sicurezza: a) sicurezza dei dispositivi (endpoint security), ivi compresi applicativi antivirus, antimalware ed «endpoint detection and response» (EDR); b) «web application firewall» (WAF).

La presente circolare e' volta, pertanto, ad indicare le categorie di prodotti e servizi tecnologici di sicurezza informatica per le quali le pubbliche amministrazioni dovranno procedere a diversificazione ai sensi dell'art. 29, del decreto-legge n. 21 del 2022.

B) Individuazione dei prodotti e servizi oggetto di diversificazione.

Ai fini dell'individuazione dei prodotti e servizi tecnologici di sicurezza informatica di aziende produttrici legate alla Federazione Russa, ai sensi dell'art. 29, commi 1 e 3, del decreto-legge n. 21 del 2022, ciascuna pubblica amministrazione destinataria della presente circolare procede alla diversificazione delle seguenti categorie di prodotti e servizi tecnologici di sicurezza informatica:

1) prodotti e servizi di cui all'art. 29, comma 3, lettera a), del decreto-legge n. 21 del 2022, della societa' «Kaspersky Lab» e della societa' «Group-IB», anche commercializzati tramite canale di rivendita indiretta e/o anche veicolati tramite accordi quadro o contratti quadro in modalita' «on-premise» o «da remoto»;

2) prodotti e servizi di cui all'art. 29, comma 3, lettera b), del decreto-legge n. 21 del 2022, della societa' «Positive Technologies», anche commercializzati tramite canale di rivendita indiretta e/o anche veicolati tramite accordi quadro o contratti quadro in modalita' «on-premise» o «da remoto».

C) Raccomandazioni procedurali.

Si raccomanda alle amministrazioni destinatarie della presente circolare - responsabili nella conduzione delle operazioni di configurazione dei nuovi servizi e prodotti acquisiti ai sensi dell'art. 29 del decreto-legge n. 21 del 2022, anche in relazione alla precisa conoscenza dei propri asset (reti, sistemi informativi e servizi informatici) e degli impatti degli stessi sulla continuita' dei servizi e della protezione dei dati - di adottare tutte le misure e le buone prassi di gestione di servizi informatici e del rischio cyber e, in particolare, di tenere conto di quanto definito dal Framework nazionale per la cybersecurity e la data protection, edizione 2019, realizzato dal Centro di ricerca di cyber intelligence and information security (CIS) dell'Universita' Sapienza di Roma e dal Cybersecurity national lab del Consorzio interuniversitario nazionale per l'informatica (CINI), con il supporto dell'Autorita' garante per la protezione dei dati personali e del Dipartimento delle informazioni per la sicurezza.

In particolare, si raccomanda di:

1) censire dettagliatamente i servizi e prodotti di cui al paragrafo B) della presente circolare, analizzando gli impatti degli aggiornamenti degli stessi sull'operativita', quali i tempi di manutenzione necessari;

2) identificare e valutare i nuovi servizi e prodotti, validandone la compatibilita' con i propri asset, nonche' la complessita' di gestione operativa delle strutture di supporto in essere;

3) definire, condividere e comunicare i piani di migrazione con tutti i soggetti interessati a titolo diretto o indiretto, quali organizzazioni interne alle amministrazioni e soggetti terzi;

4) validare le modalita' di esecuzione del piano di migrazione su asset di test significativi, assicurandosi di procedere con la migrazione dei servizi e prodotti sugli asset piu' critici soltanto dopo la validazione di alcune migrazioni e con l'ausilio di piani di ripristino a breve termine al fine di garantire la necessaria continuita' operativa. Il piano di migrazione dovra' garantire che in nessun momento venga interrotta la funzione di protezione garantita dagli strumenti oggetto della diversificazione;

5) analizzare e validare le funzionalita' e integrazioni dei nuovi servizi e prodotti, assicurando l'applicazione di regole e configurazioni di sicurezza proporzionate a scenari di rischio elevati (quali, ad esempio, autenticazione multi-fattore per tutti gli accessi privilegiati, attivazione dei soli servizi e funzioni strettamente necessari, adozione di principi di «zero-trust»);

6) assicurare adeguato monitoraggio e audit dei nuovi prodotti e servizi, prevendendo adeguato supporto per l'aggiornamento e la revisione delle configurazioni in linea.

Nella predisposizione, migrazione e gestione dei nuovi prodotti e servizi, si raccomanda l'adozione di principi trasversali di indirizzo, quali a titolo esemplificativo quello della «gestione del rischio», in termini di identificazione, valutazione e mitigazione dei rischi di diversa fattispecie che concorrono nell'attuazione della diversificazione dei servizi.

Infine, si raccomanda alle amministrazioni di controllare costantemente i canali istituzionali di comunicazione dell'Agenzia per la cybersicurezza nazionale https://www.acn.gov.it/ e https://csirt.gov.it

La presente circolare, che potra' essere oggetto di periodico aggiornamento, opera dalla sua pubblicazione nella Gazzetta Ufficiale

della Repubblica italiana e, al fine di assicurarne una diffusa conoscenza nell'intero territorio nazionale, la presente circolare sara' disponibile, dopo la pubblicazione, all'indirizzo https://www.acn.gov.it

Roma, 21 aprile 2022

Il direttore generale: Baldoni